# Security



Document name: Security.docx
Last update: 04.11.2020
Autor: A. Balogh

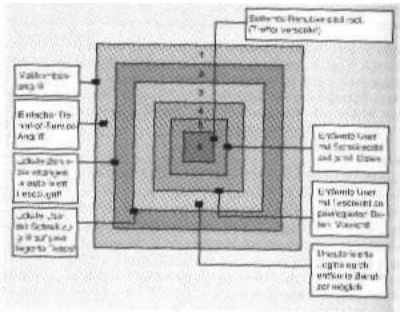
## Inhaltsverzeichnis

# INTRODUCTION

- Noch nicht geklärte Artikel sind mit ***???*** markiert!

Kontakt Verlag: maxsecii@altavista.net

Simple Check: Show all data modified after dd/mm/yyyy *.exe, *.com, *.dll



Open Platform for Security Enterprise Connectivity (OPSEC-Specification)
E3-Certification

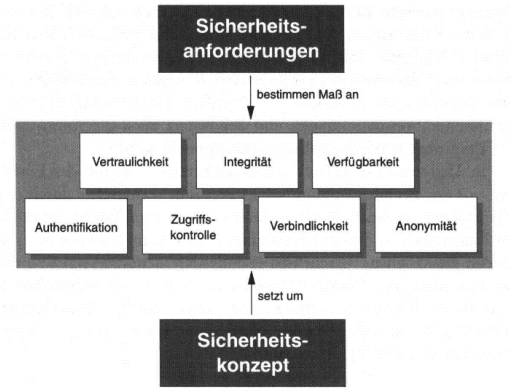
http://www.astalavista.net
http://www.packetstormsecurity.org/

**3 Grundanforderungen:**

- Vertraulichkeit, Integrität, und Verfügbarkeit.

**4 Sicherheitsdienste:**

- Authentifikation
- Zugriffskontrolle
- Verbindlichkeit
- Anonymität




**Begriffsdefinition Sicherheit**
Aus unternehmerischer Sicht sollte der Begriff Sicherheit als eine zentrale Eigenschaft von Geschäftsprozessen verstanden werden, die durch geeignete technische und organisatorische Massnahmen sicherstellt, dass das ***Restrisiko*** für die Organisation auf ein tragbares Mass reduziert wird.

**A network is only as secure as its weakest element.**

**As is often the case with security compromises, it's not a matter of if your company will be compromised, but when.**

# LINKS

**RSS-Feeds**
SANS https://www.sans.org/newsletters/newsbites/rss/

**Daily Security Reports**
Listinfo: https://lists.cert.at/cgi-bin/mailman/listinfo/daily

https://www.sans.org/ SANS
https://www.sans.org/security-resources/policies

https://www.mywot.com/
https://seclists.org/
http://www.trustedsource.org/
https://www.virustotal.com/en/
https://haveibeenpwned.com/ Account breaches
ebas.ch/zertifikatspruefung Certificate Check
zkb.ch/sicherheit General Security informations
https://asecuritysite.com/ Testing Blowfish and others
www.datenschutz.de/suche Datenschutz
www.mindcert.com/category/mind-maps/cissp
https://www.datenschutz-guru.de/datenschutzhinweise/
http://www.hackshop.com/
https://shop.hak5.org/
https://threatpost.com/

**NTT - Information Security and Risk Management (SOC)**
https://uk.portal.wideanglentt.com/wamss/services.php

Smarttech 247
Offers a 24/7 managed SOC, penetration testing and Data Classification Solutions.
Switzerland
+41 78 69 99 502

**PEN-Testing**
Oneconsult, Thalwil

**Exeon Analytics**
- Wurde im August 2016 von David Gugelmann gegründet.
- Das Spin-off der ETH Zürich bietet Lösungen zur Sicherung von Unternehmensnetzwerken an.
- Exeon Analytics beschäftigt aktuell neun Personen in der Forschung und Software-Entwicklung, wobei drei davon im Rahmen eines Forschungsprojekts mit der ZHAW beim Start-up mitarbeiten.
- Weitere Mitarbeiter sind im Marketing und Verkauf tätig.
- www.exeon.ch

# SECURITY CERTIFICATIONS

## *APP - Associate Protection Professional*

- The Associate Protection Professional (APP) designation provides the first "rung" on the security manager's career ladder.
- It is for those with 1-4 years of security management experience and measures the professional's knowledge of security management fundamentals, business operations, risk management, and response management.

## *CAMS - Certified Anti-Money Laundering Specialist*

- https://www.acams.org

## *CAP - Certified Authorization Professional*

See: www.isc2.org/cap

- CAP recognizes personnel responsible for formalizing processes used to assess risk and establish security requirements and documentation.

## *CAS - Information Security - Technology*

- Informationssicherheit mit Fokus Technik betrachten
- Das CAS Information Security - Technology vermittelt Grundlagen der Informationssicherheit. Es fokussiert auf technische Aspekte, thematisiert aber auch die Bereiche Management und Recht.
- Das CAS Information Security - Technology vermittelt zentrale Grundlagen der Informationssicherheit.
- In kleinerem Umfang werden auch Fragestellungen aus den Bereichen Informationssicherheits-Management und Recht vermittelt.
- Dadurch erhalten Personen mit technischem Hintergrund einen idealen Einstieg in die Themen Management und Recht.
- Gleichzeitig können sie technische Aspekte der Informationssicherheit vertiefen.
- Die entwickelten Kompetenzen befähigen Absolventinnen und Absolventen, kleinere Projekte in der Informationssicherheit selbstständig zu bearbeiten.
- Bei komplexen Fragestellungen sind sie kompetente Gesprächspartnerinnen und Gesprächspartner.
- Sie verfügen über eine gute Mitsprachekompetenz.

## *CCFP - Certified Cyber Forensic Professional*

- For individuals who wish to demonstrate advanced expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete and reliable digital evidence admissible to a court of law, as well as the ability to apply forensics techniques to other information security disciplines, such as e-discovery, malware analysis, or incident response.

## *CCISO - Certified Chief Information Security Officer*

- ECCU 523 - Executive Governance and Management

***Umfasst:***

- ❑ Governance (Policy, Rechtliches & Compliance)
- ❑ IS Management Kontrollen und Auditing Management
- ❑ Management - Projekte und Operations (Projekte, Technologie & Operations)
- ❑ Information Security Kernkompetenzen
- ❑ Strategische Planung & Finanzen

## *CCSA - Certification in Control Self Assessment*

- Dieses Zertifikat wurde speziell für Praktiker des ***Controll Self Assessment*** entwickelt. Jeder Praktiker wird, unabhängig von seinen tatsächlichen Erfahrungen, von diesem ausführlichen Programm profitieren.
- Bei der Auseinandersetzung mit dem geforderten Wissen auf dem Gebiet von Risiko- und Kontrollmodellen, die oftmals als Gebiete einzig für Revisoren gesehen werden, werden Konzepte vermittelt, die für eine effektive Nutzung des CCSA als Unterstützung der Kunden bei der Zielerreichung von grundlegender Bedeutung sind.
- Das IIA Global hat am 7. August 2018 bekannt gegeben, dass die bestehende CCSA Zertifizierung ab Jänner 2019 in die ***CRMA*** Zertifizierung integriert werden wird.

## *CCSP - Certified Cloud Security Professional*

- Securing the Power of the Cloud
- As powerful as cloud computing is for the organization, understanding its information security risks and mitigation strategies is critical.
- Legacy approaches are inadequate, and organizations need competent, experienced professionals equipped with the right cloud security knowledge and skills to be successful. They need CCSPs.
- Backed by the two leading non-profits focused on cloud and information security, the Cloud Security Alliance (CSA) and (ISC)², the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security.
- CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

## *CEH - Certified Ethical Hacker*

The first step before sending even one single packet to the target would be to have a signed agreement with clear ***rules of engagement*** and a ***signed contract***.

The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understands that some of the tests could lead to ***interruption*** of service or even ***crash*** a server. The client signs that he is aware of such risks and willing to accept them.

- ECCU 501 Ethical Hacking & Countermeasures
- CIS 404 Hacker Techniques, Tools, and Incident Handling
- A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).
- The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.
- "Improving the Security of Your Site by Breaking Into It".

***Keep Certified:***
You must earn ***60 PDU's /Year*** or ***180 PDU's in 3 Years***.
1 PDU equals 60 minutes of education.

***CEH Methodology / PHASES OF HACKING***
1. Reconnaissance (footprinting)
2. Scanning
3. Enumeration
4. Gaining access escalating privileges maintaining access
5. Covering tracks


***Hacking erste Schritte***

- ❑ Wie sieht das Netzwerk aus?
- ❑ Welche möglichen Schwachstellen gibt es?
- ❑ Wer betreibt das Netzwerk?
- ❑ Woher bekommt es seine Anbindung?

host -l -v -t any hostname.com
finger
showmount
rpcinfo
whois

Phrack Magazine : http://www.phrack.com
2600: http://www.2600.com

Zwei oder drei Befehlszeilen an Port 25. Dieser Befehl dient dazu, den Server zu veranlassen eine eine Kopie der Datei /etc/passwd an den Cracker zu senden.

**r-Utilities:**
rlogin remote login
rsh remote shell
rcp remote file copy
rcmd remote command

## *CHFI - Computer Hacking Forensic Investigator*

- ECCU 502 Investigating Network Intrusions and Computer Forensics
- CIS 406 System Forensics, Investigation, and Response

### *CIPT - Certified Information Privacy Technologist*

- The CIPT credential shows you've got the knowledge to build your organization's privacy structures from the ground up.
- With regulators worldwide calling for tech professionals to factor data privacy into their products and services, the job market for privacy-trained IT pros has never been stronger.
- Do you work in IT, security, or engineering?
- The CIPT is for you. How about privacy by design, software engineering, data management or audit? Ditto.
- Whether you work in the public or private sector, data privacy skills are quickly becoming a must-have—and that's a great opportunity for you.

### *CIPP/E - Certified Information Privacy Professional*

The CIPP credential says you know privacy laws and regulations and how to apply them. It also says you know how to secure your place in the information economy. No wonder it's our most popular program.

### *CIPM - Certificate in Investment Performance Measurement*

Make a difference in your organization and in your career. The CIPM designation says that you're a leader in privacy program administration and that you've got the goods to establish, maintain and manage a privacy program across all stages of its lifecycle.

### *CISA - Certified Information Systems Auditor*

- The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals.
- Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to ***assess vulnerabilities***, ***report on compliance*** and ***institute controls*** within the enterprise.

### *CISM - Certified Information Security Manager*

- Demonstrate your information security management expertise.
- The uniquely management-focused CISM certification promotes international security practices and recognizes the individual who manages designs, and oversees and assesses an enterprise's information security.

### *CISSP - Certified Information Systems Security Professional*

See: www.isc2.org/cap

- The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.
- Backed by (ISC)², the globally recognized, nonprofit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

***CISSP is recommended for following roles:***

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant

- Network Architect

***Concentrations***

In order to earn your ***CISSP concentration certification***, you must have first earned your CISSP certification and maintained it.

- Information Systems Security Architecture Professional (ISSAP)
- Information Systems Security Engineering Professional (ISSEP)
- Information Systems Security Management Professional (ISSMP)

***CISSP-ISSAP***

- Is concentrated only for professional who is an ***architect*** or security professionals who wants to specialise themselves as an architect.
- The CISSP-ISSAP certification deals specifically with information security architecture.
- It is designed for analysts, as well as chief security architects, consultants and others in the industry who develop, design and implement program security.
- According to (ISC)2, this concentration is ideal for system architects, chief technology officers, system designers, network designers, business analysts and chief security officers who want to "specialize in designing security solutions and providing management with risk-based guidance to meet organizational goals."

***The ISSAP CBK covers quite a few areas, including:***

1. Physical security considerations
2. Communications and network security
3. Cryptography
4. Technology-related business continuity planning
5. Disaster recovery planning
6. Security architecture analysis

***CISSP-ISSEP***

- Is concentrated only for professionals who is ***security product developer*** or developer who likes specialise in security development engineering with some best practices.
- The CISSP-ISSEP concentration deals with information systems security engineering, and is designed for senior systems engineers, information assurance systems engineers, information assurance officers, information assurance analysts, and senior security analysts along with others.
- According to (ISC)2, these professionals "specialize in the practical application of systems engineering principles and processes to develop security systems."

***The CBK for this concentration includes:***

1. US government information assurance related policies and issuances
2. Systems security engineering
3. Certification and accreditation
4. Risk management framework
5. Technical management

***CISSP-ISSMP***

- Is concentrated only for professionals who is in ***leadership role*** or in ***management roles*** to plan an efficient security projects.
- The ISSMP concentration deals with information systems security management, and it is designed for chief information officers, chief information security officers, senior security executives and chief technology officers, amongst many others.
- The organization says these professionals "specialize in establishing, presenting, and governing information security programs, and demonstrate management and leadership skills."

***The CBK for the ISSMP concentration includes:***

1. Law, ethics, and incident management
2. Security leadership and management
3. Contingency management
4. Security lifecycle management

5. Security compliance management

### *CND - Certified Network Defender*

- ECCU500 Managing Secure Network Systems
- CIS 403 Network Security, Firewalls and VPns

### *CompTIA Security+ -*

- CompTIA Security+ is the first security certification IT professionals should earn.
- It establishes the core knowledge required of any ***cybersecurity role*** and provides a springboard to intermediate-level cybersecurity jobs.
- Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills.
- Cybersecurity professionals with Security+ know how to address security incidents - not just identify them.
- Security+ is compliant with ***ISO 17024*** standards and approved by the US DoD to meet directive ***8140/8570.01-M*** requirements.

### *CPP - Certified Protection Professional*

- The Certified Protection Professional (CPP®) is considered the "gold standard" for security management professionals.
- This certification validates your knowledge in all areas of security management.
- Eligibility requirements include 7-9 years of security experience and 3 years in responsible charge of a security function.

### *CSSLP - Certified Secure Software Lifecycle Professional*

See: www.isc2.org/cap

- CSSLP recognizes the key qualifications of developers building secure software applications.

### *DEKRA - Datenschutzbeauftragter*

See: DSGVO

### *ECIH - EC-Council Certified Incident Handler*

- ECCU 522 - Incident Handling and Response

### *ECSA - ECCouncil Certified Security Analyst*

- ECCU 503 - Security Analysis and Vulnerability Assessment
- The ***next step*** after CEH.

### *ECSP - EC-Council Cerified Secure Programmer*

- ECCU 510 - Secure Programming

### *EDRP - EC-Council Disaster Recovery Professional*

- ECCU 513 - Disaster Recovery

### *EISM - EC-Council Information Security Manager*

- ECCU 523 Executive Governance and Management
- Alternative zum CCISO, falls die enrolment Bedingungen des Kandidaten nicht erfüllt sind.

### *F5 Certified Administrator*

- Exam 101 - Application Delivery Fundamentals
- Exam 201 - TMOS Administration

## *Fortinet NSE 4 - Network Security Professional*

- This designation recognizes your ability to install and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific ***corporate network security policies***.
- NSE 4 certification based on FortiGate Security and FortiGate Infrastructure courses are highly recommended to prepare you for the Fortinet NSE 4 - FortiOS 5.6 and Fortinet NSE 4 - FortiOS 6.0 exams.

## *Fortinet NSE 8 - Fortinet Network Security Expert*

The Fortinet NSE 8 designation recognizes a candidate's broad and in-depth knowledge of:

- Network security design
- Configuration
- Troubleshooting for complex networks.

This is the most complete and unique networking and security designation in the worldwide technology industry. Attaining the NSE 8 designation will make you part of a new elite group of professionals

## *GIAC - Global Information Assurance Certification*

- Global Information Assurance Certification (GIAC) is the leading provider and developer of Cyber Security Certifications.
- GIAC tests and validates the ability of practitioners in information security, forensics, and software security.
- GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment.

## *GCIA - Certified Intrusion Analyst*

- GIAC Certified Intrusion Analysts (GCIAs) have the knowledge, skills, and abilities to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files.

## *GCIH*

Incident handlers manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on detecting, responding, and resolving computer security incidents and covers the following security techniques:

- The steps of the incident handling process
- Detecting malicious applications and network activity
- Common attack techniques that compromise hosts
- Detecting and analyzing system and network vulnerabilities
- Continuous process improvement by discovering the root causes of incidents

*No Specific training is required for any GIAC certification. There are many sources of information available regarding the certification objectives' knowledge areas. Practical experience is an option; there are also numerous books on the market covering Computer Information Security. Another option is any relevant courses from training providers, including SANS.*

## *GCFA - Certified Forensic Analyst*

- The GCFA certification is for professionals working in the information security, computer forensics, and incident response fields.
- The certification focuses on core skills required to collect and analyze data from Windows and Linux computer systems.
- The GCFA certifies that candidates have the knowledge, skills, and ability to conduct formal incident investigations and handle advanced incident handling scenarios, including internal and external data breach intrusions, advanced persistent threats, anti-forensic techniques used by attackers, and complex digital forensic cases.

- *No Specific training is required for any GIAC certification.
- There are many sources of information available regarding the certification objectives' knowledge areas. Practical experience is an option; there are also numerous books on the market covering Computer Information Security.
- Another option is any relevant courses from training providers, including SANS.*

## *GISF - Security Fundamentals*

- See: sans.org
- SEC301: Introduction to Cyber Security

## *GISRA - Government Information Security Reform Act (2000)*

- The Government Information Security Reform Act (GISRA) of 2000, established information security program, evaluation, and reporting requirements for federal agencies.
- GISRA required agencies to perform ***periodic threat-based risk assessments*** for systems and data.
- GISRA requires agencies to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained either by the agency or for it by another agency or contractor.
- GISRA required that agencies develop a process for ensuring that remedial action is taken to address significant deficiencies. GISRA also required agencies to provide training on security awareness for agency personnel and on security responsibilities for information security personnel.
- GISRA required the agency head to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. The agency head was responsible for ensuring that the appropriate agency officials, evaluated the effectiveness of the information security program, including testing controls.
- In 2002, GISRA was replaced and strengthened with ***FISMA*** (Federal Information Security Management Act).
- Each requirement of the law relating to Information Security is broken down further into more specific sub-requirements that can be mapped back to both the Security Principles that drive them and the Design Patterns that satisfy them.

## *GREM - Reverse Engineering Malware*

- The GIAC Reverse Engineering Malware (GREM) certification is designed for technologists who protect the organization from malicious code.
- GREM-certified technologists possess the knowledge and skills to reverse-engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers.
- These individuals know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration.

## *ISO 27001 Lead Implementer*

- This training enables you to develop the necessary expertise to support an organization in establishing, implementing, managing and maintaining an Information Security Management System (ISMS) based on ISO/IEC 27001.

## *LPT - Licensed Penetration Tester (Master)*

- ECCU 506 - Conducting Penetration and Security Tests
- The ***next step*** after ECSA.

## *MAS - Master of Advanced Studies*

- Der Master of Advanced Studies (MAS) ist ein Abschluss im tertiären Weiterbildungsbereich auf Hochschulstufe, der hauptsächlich in der Schweiz und Liechtenstein sowie vereinzelt in Österreich, aber auch in Deutschland Anwendung findet.

z.B.***MAS Information Systems Management***

## *NIACAP - National Informational Assurance Certification and Accreditation Process*

- Establishes the ***minimum*** national standards for certifying and accrediting national security systems.

## *NIIPA - National Informational Infrastructure Protection Act (1996)*

- The National Information Infrastructure Protection Act (NIIPA), signed into law in October 1996, was a significant revision of U.S. computer crime law.
- It provides federal criminal liability for theft of trade secrets and for "anyone who intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage."
- The NIIPA is ***one of a number of laws*** enacted by the U.S. government to address the array of new cybercrimes that have emerged with the ongoing expansion and development of the Internet.
- The NIIPA represents the most ambitious amendments to the Computer Fraud and Abuse Act of 1984, which had previously been modified in 1986 and 1994.

## *OSCP - Offensive Security Certified Professional*

Link: https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/?utm_expid=.c0Ak2sVZTzWDYy-X0jCRzw.0&utm_referrer=https%3A%2F%2Fwww.offensive-security.com%2Finformation-security-certifications%2F

- The **Offensive Security Certified Professional (OSCP)** is the companion certification for our Penetration Testing with Kali Linux training course and is the world's first completely hands-on offensive information security certification.
- The OSCP challenges the students to prove they have a clear and practical **understanding of the penetration testing process and life-cycle** through an arduous twenty-four **(24) hour certification exam**.
- An OSCP has demonstrated their ability to be presented with an unknown network, enumerate the targets within their scope, exploit them, and clearly document their results in a penetration test report.
- The Offensive Security Certified Professional (OSCP) is the companion certification for our Penetration Regulatory Obligations

## *OSWP - Offensive Security Wireless Professional*

Link: https://www.offensive-security.com/information-security-certifications/oswp-offensive-security-wireless-professional/

## *PCI - Professional Certified Investigator*

- The professional Certified Investigator (PCI®) certification provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings.
- Requirements include a high school diploma or GED equivalent and five years of investigations experience, with at least two years in case management.

## *PRA - Paperwork Reduction Act (1995)*

- The Paperwork Reduction Act of 1980 (Pub. L. No. 96-511, 94 Stat. 2812, codified at 44 U.S.C. §§ 3501-3521) is a United States federal law enacted in 1980 designed to reduce the total amount of paperwork burden the federal government imposes on private businesses and citizens.
- The Act imposes procedural requirements on agencies that wish to collect information from the public.
- It also established the Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB), and authorized this new agency to oversee federal agencies' collection of information from the public and to establish information policies.

- A substantial amendment, the Paperwork Reduction Act of 1995, confirmed that OIRA's authority extended over not only agency orders to provide information to the government, but also agency orders to provide information to the public.

## *PSP - Physical Security Professional*

- The Physical Security Professional (PSP®) demonstrates your knowledge in physical security assessments, application, design, and integration of physical security systems, and implementation of security measures.
- Eligibility requirements include a high school diploma, GED equivalent, or associate degree AND six years of progressive experience in the physical security field OR a Bachelor's degree or higher AND four years of progressive experience in the physical security field.

## *SSCP - Systems Security Certified Practitioner*

- The (ISC)2 Systems Security Certified Practitioner (SSCP) is a terrific entry-level information security certification, and it is the ideal precursor for the much sought after Certified Information Systems Security Professional (CISSP).
- The SSCP certification focuses on seven (7) Common Body of Knowledge (CBK) domains:
    - Access Controls
    - Security Operations and Administration
    - Risk Identification, Monitoring, and Analysis
    - Incident Response, and Recovery
    - Cryptography
    - Networks and Communications Security
    - Systems and Applications Security

# ORGANIZATIONS

## *ACLU - American Civil Liberties Union*

- https://www.aclu.org/
- Die American Civil Liberties Union (kurz ACLU, englisch „Amerikanische Bürgerrechtsunion“) ist eine US-amerikanische Nichtregierungsorganisation mit Sitz in New York City, die seit 1920 besteht.
- Sie setzt sich für Bürgerrechte und generell für Anliegen des Liberalismus ein.

## *ASIS - International*

- See: https://www.asisonline.org/

## *ASP - Association for Strategic Planning*

- See: https://www.strategyassociation.org/
- ***Highly successful organizations*** report that strategic planning has high impact on overall organizational success.
- ***Low-success organizations*** do not report strategic planning as key to overall organizational success.

***Strategic Planning***

1. ***Goal-based planning*** is probably the most common method and starts with a focus on the organization’s mission. It includes reviewing the organization’s vision and values, goals to work toward the mission, strategies to achieve the goals, and action planning (who will do what and by when).
2. ***Issues-based strategic planning*** often starts by examining issues within the organization, strategies to address those issues, and action plans.
3. ***Organic strategic planning*** might start by articulating the organization’s vision and values, and then creating action plans to achieve the vision while adhering to those values.

***Strategic Planning Steps***

- Assessment
- Strategy formulation
- Strategy execution
- Evaluation

***TOOLS:***

***Balanced Scorecard***

- The Balanced Scorecard is a strategic planning and management system that is used to align business activities to the vision and strategy of the organization, improve internal and external communications, and monitor the organization’s performance against strategic goals.

## *CERT - Computer Emergency Response Team*

- 1988 gegründet nach dem "Morris-Wurm-Vorfall".
- Gibt Hinweise heraus, wann immer ein neues Sicherheitsloch auftaucht.
- 24 Stunden Notfalldienst für technische Ratschläge
- Website mit Sicherheitsinformationen
- Jahresbericht
- CERT veröffentlicht keine Informationen bevor nicht eine Abhilfe entwickelt wurde!
- Coordination Center Generic Security Information ***Checklist*** http://ird.security.mci.net/check/cert-sec.html

***CERT Mailing Liste:***

1. E-Mail senden an cert-advisory-request@cert.org
2. Schreiben Sie das Wort: subscribe + E-Mail Adresse

oder
http://www.cert.org/nav/alerts.html

CIAC-Virus-Datenbank http://ciac.llnl.gov
CIAC-Sicherheitsbulletins
CIAC-Sicherheitsdokumente

http://www-leland.stanford.edu/~llurch/win95netbugs/archives

**Mailing Listen**
majordomo@applicom.co.il Firewall 1 / Checkpoint
SUBSCRIBE firewall-1
listserv@listserv.nbugtraq.com Windows.NT
subscribe ntbugtraq Ihr_Vorname Nachname

**Newsgroups:**

| | |
|---|---|
| alt.2600 | Hacking, Cracking und Exploits |
| alt.2600.crackz | Hacking, Cracking und Exploits |
| alt.2600.hackerz | Hacking, Cracking und Exploits |
| alt.computer.security | Allg. Computer Sicherheit |
| comp.security.firewalls | Firewalls |

## *CIS - Center for Internet Security*

- The Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense1
- (CSC) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.
- The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources.

***CIS Controls***

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

## *CJIS - Criminal Justice Information Services*

- Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.

## *CNIL - Französische Datenschutzbehörde*

- ???

### *CompTIA - Computing Technology Industry Association*

- Provider of vendor-neutral IT Certifications.

### *COSO - Committee of Sponsoring Organizations of the Treadway Commission*

- Base for ***COBIT***.
- Is a joint initiative of the five private sector organizations listed on the left and provides thought leadership through the development of frameworks and guidance on ***enterprise risk management***, ***internal control*** and ***fraud deterrence***.
- Main purpose to help ensure ***fraudulent financial reporting*** cannot take place.

### *CPTED - Crime Prevention Through Environmental Design*

See: www.cpted.net
www.defexiblespace.com

- CPTED is the design, maintenance, and use of the built environment in order to enhance quality of life and to reduce both the incidence and fear of crime.
- Teritoriality means providing clear designation between public, private, and semi-private areas ans makes it easier for people to understand and participate in an area's intendes use.
- Sense of active "ownership".

### *CVE - Common Vulnerabilities and Exposures*

https://cve.mitre.org Common Vulnerabilities and Exposures (CVE)
https://www.lockedshield.com/cve-(nvd)

- CVE® is a list of entries.
- Each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.
- CVE Entries are used in numerous cybersecurity products and services from around the world, including the ***U.S. National Vulnerability Database (NVD)***.

### *DISA - Defense Information Systems Agency*

- Specific benchmarks for various infrastructure systems.

### *DoD - US Department of Defense*

https://www.defense.gov/

### *EKAS - Eidgenössische Koordinationskommission für Arbeitssicherheit*

### *FAR - U.S. Federal Acquisition Regulation*

- The FAR defines a standard set of security clauses in Part 52.204-2 - Security Requirements.
- This section of U.S. law defines a set of standard security requirements that are applicable to all vendors providing services to U.S. federal agencies.
- The clauses define the ***scope***, ***applicability***, and ***purpose*** of each clause.

### *FASB - Financial Accounting Standards Board*

- See: https://www.fasb.org

### *FATF - Financial Action Task Force*

- Combatting terrorist financing is the top priority for the FATF, the intergovernmental body responsible for understanding terrorist financing risks, developing global standards and evaluating countries' compliance.

### *FBI - Federal Bureau of Investigation*

- Zu Deutsch etwa „Bundesamt für Ermittlung“, ist die zentrale Sicherheitsbehörde der Vereinigten Staaten.

- In ihm sind sowohl ***Strafverfolgungsbehörde*** als auch ***Inlandsgeheimdienst*** der US-Bundesregierung zusammengefasst.
- Als Kriminalpolizei ist sie für die Verfolgung und Verhinderung von bundesrechtlichen Straftaten zuständig, soweit keine spezielle Zuständigkeit anderer Strafverfolgungsbehörden, etwa des ***ATF*** oder der ***DEA*** gegeben ist.
- Als Nachrichtendienst betreibt das FBI die ***Vorfeldaufklärung möglicher Bedrohungen*** unabhängig von konkretem Verdacht.
- Daneben leistet es im Wege der Amtshilfe technische Unterstützung für andere Ermittlungsbehörden.
- In Folge der Terroranschläge am 11. September 2001 wurde aufgrund einer Direktive des US-Präsidenten vom 28. Juni 2005 der „National Security Branch“ (NSB) geschaffen.
- In ihm wurden die bisher getrennten Abteilungen des FBI für Terrorbekämpfung, die Spionageabwehr und für die Bekämpfung von Massenvernichtungswaffen zusammengefasst und direkt einem stellvertretenden Direktor des FBI unterstellt.
- Hierdurch und durch eine enorme Steigerung des personellen und materiellen Einsatzes ist das FBI heute die ***grösste zivile Behörde zur Terrorbekämpfung***.
- Das FBI untersteht dem US-Justizministerium und hat seinen Hauptsitz im J. Edgar Hoover FBI Building in Washington, D.C.

## *FedRAMP - Federal Risk and Authorization Management Program*

- Cloud computing regulatory

## *FEMA - Federal Emergency Management Agency*

See: fema.gov

- National flood insurance program.

## *FS-ISAC - Financial Services Information Sharing and Analysis Center*

- The Financial Services Information Sharing and Analysis Center or (FS-ISAC) is the global ***financial industry's resource for cyber and physical threat intelligence analysis*** and sharing. FS-ISAC is a member-owned non-profit, created by and for the financial services industry to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector’s ability to provide services critical to the orderly function of the global financial system and economy.

## *FTC - Federal Trade Commission*

- Die Federal Trade Commission (FTC, zu Deutsch etwa „Bundeshandelskommission“) ist eine unabhängig arbeitende Bundesbehörde der Vereinigten Staaten von Amerika mit Sitz in Washington, D.C. Sie hat derzeit 1.200 Mitarbeiter. Die Behörde wird von fünf Commissioners geleitet, die vom Präsidenten der Vereinigten Staaten nominiert und vom Senat bestätigt werden. Gemäss der FTC Act dürfen nicht mehr als drei Commissioners derselben politischen Partei angehören.
- Sie wurde im Jahr 1914 als Nachfolgerin des Bureau of Corporations gegründet und ist zuständig für die Zusammenschlusskontrolle und den Verbraucherschutz. Sie wird bei direkten Beschwerden von Konsumenten oder Unternehmen gegen einzelne Unternehmen tätig. Sie kann weitergehende Untersuchungen auch bei Anfragen des Kongresses oder Veröffentlichungen in der Presse unternehmen.
- Die Aufgabenstellung der Behörde wird allgemein damit beschrieben, ***unfairen und täuschenden Praktiken*** zu begegnen, um das Funktionieren eines konkurrenzbestimmten Marktes sicherzustellen. Sie geht hier über die Aufgabenstellung einer Wettbewerbsbehörde hinaus, indem sie auch Aufgaben des Verbraucherschutzes wahrnimmt.

## *GovCERT - Swiss Governmental Computer Emergency Response Team*

Link: https://www.govcert.ch/

- Das GovCERT.ch wurde von ***MELANI*** geschaffen, um noch schneller auf Vorfälle reagieren zu können und ist seit dem 1. April 2008 operativ.

Report an incident: incidents@govcert.ch
General inquiries: outreach@govcert.ch

If you wish to ***communicate through a secure channel***, please either use PGP or SMIME:
GovCERT.ch PGP Key: 0x61624749
GovCERT.ch SMIME certificate: govcert_2021.crt

## *HIN - HEALTH INFO NET AG*

- HIN stellt allen Partnern im Schweizer Gesundheitswesen eine offene und gesicherte Extranet-Plattform für den E-Mail-Verkehr und andere Anwendungen zur Verfügung.
- Auch Geschäftsprozesse lassen sich mit HIN schützen.
- Ärztinnen und Ärzte, die Spitex, Physio- und Ergotherapeuten, Chiropraktiker und weitere Personen bilden die 13.000 Einzel-Abonnenten der HIN Extranet-Plattform.

## *Honeynet Project*

- The Honeynet Project is a leading international 501c3 ***non-profit security research organization***, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security.
- With Chapters around the world, our volunteers have contributed to fight against malware (such as Confickr), discovering new attacks and creating security tools used by businesses and government agencies all over the world. The organization continues to be on the cutting edge of security research by working to analyze the latest attacks and educating the public about threats to information systems across the world.
- Founded in 1999, The Honeynet Project has contributed to fight against malware and malicious hacking attacks and has the leading security professional among members and alumni. Our mission reads "to learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned" with three main pillars:

## *IAB - Internet Architecture Board*

- See: https://www.iab.org
- See also: ***Internet Advisory Board***
- A committee of the ***IETF*** and an advisory body of the ***ISOC***.
- Internet Advisory Board (IAB) was formed in 2015 to help organizations succeed in this disruptive era of digital transformation.
- IAB creates and manages proactive "Digital Advisory Boards" that align with the strategic goals of the stakeholders we serve.
- Our formula for success is simple; we believe that organizations that want to reduce digital risk and increase online performance need to implement a Digital Advisory Board.
- This strategic oversight helps organizations save time and money while increasing their opportunity for long-term success.
- Call us at 904-476-8890 to discuss how a Digital Advisory Board can help your organization succeed online.

## *IETF - Internet Engineering Task Force*

- Die Internet Engineering Task Force (IETF, englisch für Internettechnik-Arbeitsgruppe) ist eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern.
- Ihr Auftrag ist die Erstellung hochqualitativer, relevanter technischer Dokumente, welche die Art und Weise beeinflussen, wie Menschen das Internet weiterentwickeln, benutzen und verwalten.
- Diese Dokumente umfassen Internetprotokollstandards, Beschreibungen momentan bekannter Verfahren sowie verschiedener Dokumente mit eher informativem Charakter.
- Im Gegensatz zur eher forschungsorientierten Internet Research Task Force (IRTF) kümmert sich die IETF mehr um die kurzfristig zu lösenden Probleme des Internets, insbesondere um die Standardisierung der im Internet eingesetzten Kommunikationsprotokolle.

- Zur Internetprotokollfamilie gehören beispielsweise das Internet Protocol (IP), die Transportprotokolle UDP, TCP und SCTP sowie das Anwendungsprotokoll HTTP zur Übertragung von Web-Inhalten.
- Die IETF ist eine offene, internationale Freiwilligenvereinigung von Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern, die für Vorschläge zur Standardisierung des Internets zuständig ist.
- Sie steht jedem interessierten Individuum offen und es existiert keine förmliche Mitgliedschaft oder Mitgliedsvoraussetzung. Die IETF besitzt als lose Organisation keine Rechtsform.
- Das Sekretariat der Organisation befindet sich in Fremont, Kalifornien.

*Source: Wikipedia*

### *Infosec Institute*

See: infosecinstitute.com

### *INFRAGARD*

See: www.infragard.org

### *INTERPOL - International Criminal Police Organization*

- https://www.interpol.int/

### *IOCE - International Organization on Computer Evidence*

- See the six principals.

### *ISACA - Information Systems Audit and Control Association*

- www.isaca.org

### *ISC - International Information Systems Security Certification Consortium*

See: www.isc2.org

- The governing body that administers the CISSP certification.
- Stated the "***Code of Ethics***".

***HCISPP - HealthCare Information Security Privacy Practitioner***
See ISC
- Healthcare

***ISSAP - Information Systems Security Architecture Professional***
See ISC
***ISSEP - Information Systems Security Engineering Professional***
See ISC
***ISSMP - Information Systems Security Management Professional***
See ISC

### *ISIO - International Security Industry Organization*

- This international organization regulates billions of transactions daily and provides security guidelines protect personally identifiable information (PII).
- These security controls provide a baselin and prevent low-level hackers sometimes known a script kiddies from causing a data breach.

### *ITRC - Identify Theft Resource Center*

- Routinely tracks data breaches.

### *ITU-T - International Telecommunication Union*

- Home: https://www.itu.int

- The ITU Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications and Information Communication Technology such as ***X.509*** for cybersecurity, ***Y.3172*** for machine learning, and ***H.264/MPEG-4 AVC*** for video compression, between its Member States, Private Sector Members, and Academia Members.
- The standardization efforts of ITU started in 1865 with the formation of the International Telegraph Union (ITU).
- ITU-T has a permanent secretariat, the Telecommunication Standardization Bureau (TSB), based at the ITU headquarters in ***Geneva, Switzerland***.

### *KARTAC - Interessengemeinschaft der Zahlkartenindustrie Schweiz*

- www.kartac.ch

### *LEIU - Law Enforcement Intelligence Unit*

- Is an organization designed to facilitate ***intelligence sharing*** between state and local law enforcement agencies.
- It began in 1956 with 26 members and has since expanded to include roughly 250 members, mostly in the United States but also in Canada, Australia, and South Africa.
- The organization is divided into four zones:
  Eastern, Central, Northwestern, and Southwestern.
- According to its website, LEIU's purpose is to "gather, record, and exchange confidential information not available through regular police channels, concerning organized crime and terrorism."
- Since the LEIU is ***not a government agency***, it is not subject to the provisions of the U.S. Freedom of Information Act or its equivalents in other countries.

### *Locked Shield*

See: ***lockedshield.com***

- **Locked Shield** Headquarter is located in the capital of information technology and security leadership, ***Estonia***.
- The team is composed of high experts with at least an academic degree of Master of Science in Cyber Security, Information technology or with at least a field experience of 10 years as security researchers and technicians.
- Base see the ***Cyber War attack*** started on 26th April 2007.

### *Mandiant*

- **Mandiant** ist ein US-amerikanisches IT-Sicherheitsunternehmen.
- Es erlangte durch die Veröffentlichung eines Berichts im Februar 2013 öffentliche Aufmerksamkeit, der China in einen direkten Zusammenhang mit Cyber-Spionage stellt.
- Das Unternehmen wurde 2013 von FireEye, Inc. übernommen.

### *MELANI - Melde- und Analysestelle Informationssicherung*

- MELANI ist keine Strafverfolgungsbehörde. Entsprechend werden keine polizeilichen Ermittlungen im Zusammenhang mit den gemeldeten ***Phishing-Versuchen*** durchgeführt.
- Die Aufgabe von MELANI ist die ***Abwehr*** von akuten Gefahren für die Informationssicherheit, nicht die Verfolgung der Täter.
- Wenn Sie durch Phishing geschädigt wurden, empfehlen wir Ihnen, bei Ihrer Kantonspolizei Anzeige zu erstatten.

### *MITRE - MITRE Corporation*

See: www.cve.mitre.org

- Maintains the ***CVE database***.
- The founders do have a horsory as research engineers at the ***Massachusett's Institute of Technology (MIT)***.

## *NACD - National Association of Corporate Directors*

- The National Association of Corporate Directors (NACD) defines ***four essential information security governance practices***:

1. Place information security on the board's agenda.
2. Identify information security leaders, hold them accountable, and ensure support for them.
3. Ensure the effectiveness of the corporation's information security policy through review and approval.
4. Assign information security to a key committee and ensure adequate support for that committee

## *NIAP - National Information Assurance Partnership*

See: www.niap-ccevs.org

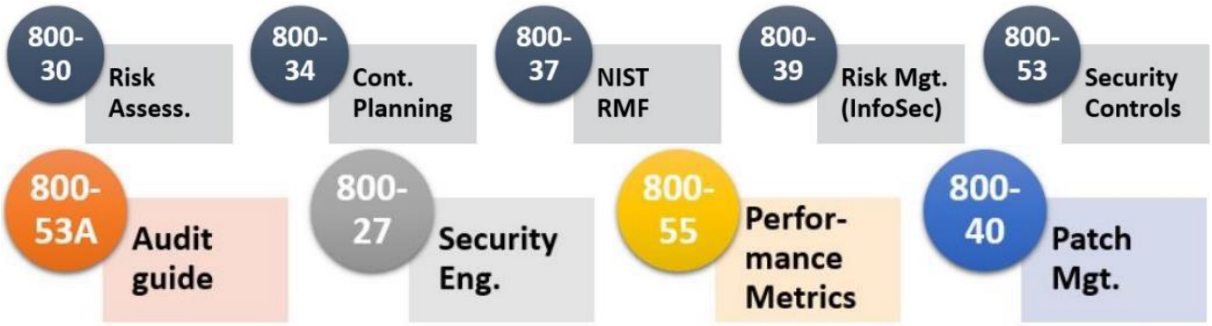
## *NISPOM - National Industrial Security Program Operating Manual*

- Regarding Forensics
- "TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations.

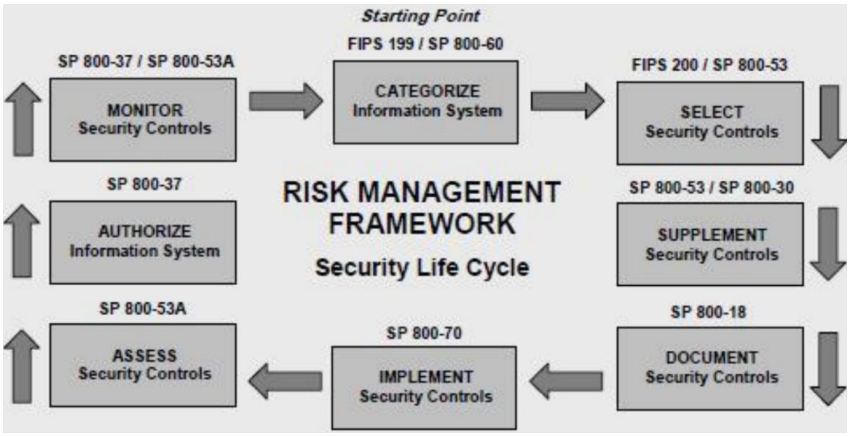
## *NIST - National Institute of Standards and Technology*

See: http://csrc.nist.gov

- ISS Vulnerability Database → http://www.iss.net/vd/library.html
  See: ***CVE Entries***
- The U.S. National Institute of Standards and Technology (NIST) publishes standards, guidelines, recommendations, and research on computers, cyber, information security, and privacy.
- The 800 series of Special Publications are the NIST's primary mode of publishing security guidelines, recommendations, and reference materials.
- Documents in the 800 series of NIST Special Publications outline the requirements for U.S. federal agencies or organizations managing information on behalf of the Federal Government; however, a CISO from any organization has the flexibility to use these documents to help develop, support, or enhance a security program.
- The documents provide foundational frameworks and are typically used to support security activities unrelated to the U.S. government.




***NIST Risk Management Framework (RMF)***




***NIST SP 800-14 Rev. 1 | Guide for Conducting Risk Assessments***

***NIST SP 800-27 Rev. A | Engineering Principles for Information Technology Security***

- A Baseline for Achieving Security
- SP 800-27 Rev. A is superseded in its entirety by ***SP 800-160*** (November 2016).

***NIST SP 800-30 Rev. 1 | Guide for Conducting Risk Assessments***

- Risk Management Process
- Risk Assessment
- Key Risk Concepts
- Applications of Risk Assessment
- Preparing for the risk assessment
- Conducting the risk assessment
- Communicating and sharing risk assessment information
- Maintaining the risk assessment

***NIST SP 800-34 Rev. 1 | Contingency Planning Guide for Federal Information Systems***

- NIST Special Publication 800-34 Rev 1., the Contingency Planning Guide for Federal Information Systems, provides instructions, recommendations, and considerations for federal information system contingency planning.

***NIST SP 800-37 Rev. 2 | Risk Management Framework for IS and Org's***

- The Guide for Applying the Risk Management Framework to Federal Information Systems, provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
- Companies usually categorize risks as ***operational***, ***financial***, ***strategic***, ***reputational***, or ***legal***.

***NIST SP 800-39 | Managing Information Security Risk***

***Key Elements:***

- Assignment of risk management responsibilities to senior leaders/executives.
- Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the nation arising from the operation and use of information systems.
- Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities.
- Accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organization-wide risk management programs.

***NIST SP 800-40 Rev. 3 | Guide to Enterprise Patch Management Technologies***

- Organizations should deploy patch management tools using a phased approach.

- Organizations should reduce the risks associated with enterprise patch management tools through the application of standard security techniques when deploying an enterprise-wide application.
- Organizations should balance their security needs with their needs for usability and availability.

***NIST SP 800-53A | Security Controls for Information Systems***

- NIST SP 800-53A is an audit guide that helps organizations evaluate the effectiveness of ***controls*** applied from the NIST SP 800-53 control catalog.
- This publication provides a catalog of ***security*** and ***privacy controls*** for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

**SECURITY CONTROLS & PRIVACY CONTROLS**

**ACCESS CONTROL**
AC-1 ACCESS CONTROL POLICY AND PROCEDURES
AC-2 ACCOUNT MANAGEMENT
AC-3 ACCESS ENFORCEMENT
AC-4 INFORMATION FLOW ENFORCEMENT
AC-5 SEPARATION OF DUTIES
AC-6 LEAST PRIVILEGE
AC-7 UNSUCCESSFUL LOGON ATTEMPTS
AC-8 SYSTEM USE NOTIFICATION
AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
AC-10 CONCURRENT SESSION CONTROL
AC-11 SESSION LOCK
AC-12 SESSION TERMINATION
AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
AC-15 AUTOMATED MARKING
AC-16 SECURITY ATTRIBUTES
AC-17 REMOTE ACCESS
AC-18 WIRELESS ACCESS
AC-19 ACCESS CONTROL FOR MOBILE DEVICES
AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
AC-21 INFORMATION SHARING
AC-22 PUBLICLY ACCESSIBLE CONTENT
AC-23 DATA MINING PROTECTION
AC-24 ACCESS CONTROL DECISIONS
AC-25 REFERENCE MONITOR

**AWARENESS AND TRAINING**
AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT-2 SECURITY AWARENESS TRAINING
AT-3 ROLE-BASED SECURITY TRAINING
AT-4 SECURITY TRAINING RECORDS
AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

**AUDIT AND ACCOUNTABILITY**
AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU-2 AUDIT EVENTS
AU-3 CONTENT OF AUDIT RECORDS
AU-4 AUDIT STORAGE CAPACITY
AU-5 RESPONSE TO AUDIT PROCESSING FAILURES
AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-7 AUDIT REDUCTION AND REPORT GENERATION
AU-8 TIME STAMPS

AU-9 PROTECTION OF AUDIT INFORMATION
AU-10 NON-REPUDIATION
AU-11 AUDIT RECORD RETENTION
AU-12 AUDIT GENERATION
AU-13 MONITORING FOR INFORMATION DISCLOSURE
AU-14 SESSION AUDIT
AU-15 ALTERNATE AUDIT CAPABILITY
AU-16 CROSS-ORGANIZATIONAL AUDITING

**SECURITY ASSESSMENT AND AUTHORIZATION**
CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
CA-2 SECURITY ASSESSMENTS
CA-3 SYSTEM INTERCONNECTIONS
CA-4 SECURITY CERTIFICATION
CA-5 PLAN OF ACTION AND MILESTONES
CA-6 SECURITY AUTHORIZATION
CA-7 CONTINUOUS MONITORING
CA-8 PENETRATION TESTING
…
**CONFIGURATION MANAGEMENT**
CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
CM-2 BASELINE CONFIGURATION
…
CM-11 USER-INSTALLED SOFTWARE
…
**CONTINGENCY PLANNING**
CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES
…
**IDENTIFICATION AND AUTHENTICATION**
IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
…
**INCIDENT RESPONSE**
IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES
…
**MAINTENANCE**
MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES
…
**MEDIA PROTECTION**
MP-1 MEDIA PROTECTION POLICY AND PROCEDURES
…
**PHYSICAL AND ENVIRONMENTAL PROTECTION**
PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
…
**PLANNING**
PL-1 SECURITY PLANNING POLICY AND PROCEDURES
…
**PERSONNEL SECURITY**
***(Operational Control)***
PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES
…
**RISK ASSESSMENT**
RA-1 RISK ASSESSMENT POLICY AND PROCEDURES
…
**SYSTEM AND SERVICES ACQUISITION**
SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
…
**SYSTEM AND COMMUNICATIONS PROTECTION**
SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
…
**SYSTEM AND INFORMATION INTEGRITY**
SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
…

**INFORMATION SECURITY PROGRAMS**
PM-1 INFORMATION SECURITY PROGRAM PLAN
…

***NIST SP 800-53, Rev. 4 | Security and Privacy Controls for Federal IS and Org's***

- The "Security and Privacy Controls for Federal Information Systems and Organizations", provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal Government.
- The guidelines apply to all components of information systems that process, store, or transmit federal information.
- Controls for Change Management

***Controls:***

- ❑ **PE-1** Physical and Environmental Protection Policy and Procedures requires consideration for controls that facilitate the implementation of physical and environmental protection controls.
- ❑ **PE-9** Power Equipment and Cabling requires consideration for protecting power equipment and cabling from damage or destruction.
- ❑ **PE-11** Emergency Power requires consideration for short-term uninterruptable power supplies to facilitate orderly shutdown of systems.
- ❑ **PE-13** Fire Protection requires consideration for fire suppression and detection systems.
- ❑ **PE-15** Water Damage Protection requires consideration for protecting systems from damage resulting from water leakage by master shutoff and isolation valves.

***NIST SP 800-55***

- ***Performance Measurement Guide*** for Information Security, highlights factors that must be considered during the development and implementation of an information security measurement program:

***Factors***

- ❑ Measures must yield quantifiable information (percentages, averages, and numbers);
- ❑ Data that supports the measures needs to be readily obtainable;
- ❑ Only repeatable information security processes should be measured; and
- ❑ Measures must be useful for tracking performance and directing resources.

***NIST SP 800-65 | Integrating IT Security into the Capital Planning and Investment Control Process***

- Withdrawn, but no superseding publication.
- Pre-dates important NIST guidance such as SP 800-53 Rev. 4, SP 800-53A Rev. 4, and the Cybersecurity Framework
-

***NIST SP 800-88 | Guidelines for Media Sanitization***

- Withdrawn, but no superseding publication.

***NIST SP 800-132 | Recommendation for Password-Based Key Derivation***

- X

***NIST SP 800-160 Systems Security Engineering***

- Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.
- SP 800-160 (1/3/18 update) is superseded in its entirety by the publication of ***SP 800-160 Volume 1*** (3/21/18 update).

***NIST SP 800-160 Vol. 1 Systems Security Engineering***

- Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure
- Is to present a list of system-level security principles to be considered in the design, development, and operation of an information system.

***The 10 Principales***

1. Establish a sound security policy as the “foundation” for design.
2. Treat security as an integral part of the overall system design.

3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
4. Ensure that developers are trained in how to develop secure software.
5. Reduce risk to an acceptable level.
6. Assume that external systems are insecure.
7. Identify potential tradeoffs between reducing risk and increased costs, and decrease in other aspects of operational effectiveness.
8. Implement tailored system security measures to meet organizational security goals.
9. Protect information while being processed, in transit, and in storage.
10. Consider custom products to achieve adequate security.

***NIST SP 800-162 ABAC - Attribute Based Access Control***

- Guide to Attribute Based Access Control (ABAC)
- Definition and Considerations

## *NPC - National Security Agency*

- Coordinates computer crime investigations throughout the United States.

## *NSA - National Security Agency*

http://csrc.nist.gov/publications/PubsSPs.html

- See: National Security Agency (NSA) Guides
- Can provide a starting point for organizations to define security configurations for common technology and systems.

## *NVD - National Vulnerability Database*

- See: **NIST**
- U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

## *OECD - Organization for Economic Co-operation and Development*

- The Organization for Economic Co-operation and Development (OECD) Privacy Principles provide the most commonly used privacy framework for confidentiality and data protection.
- Many countries leverage the OECD Privacy Principles as the model to develop their privacy laws.
- This is evident in the similarity of privacy laws in the U.S., the EU, Australia, and other developed nations that use the principles to serve as the basis for creating privacy programs and requirements.

***Pricipals:***

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

## *OISSG - Open Information Systems Security Group*

See: ISSAF

## *OSHA - Occupational Safety and Health Administration*

- Die **OSHA** ist eine Bundesbehörde in den Vereinigten Staaten, die zur Durchsetzung des Bundesarbeitssicherheitsgesetzes von ***1970*** als Folge einer neuen Arbeitssicherheitsgesetzgebung (dem OSH Act) gegründet wurde.
- Sie soll die Zahl und Folgen von Arbeitsunfällen vermindern helfen.

- Die Behörde untersteht dem US-Bundesarbeitsministerium.

## *OAK - Oberaufsichtskommission Berufliche Vorsorge*

- Die Oberaufsichtskommission Berufliche Vorsorge OAK BV ist eine unabhängige Behördenkommission für die berufliche Vorsorge, die so genannte 2. Säule.
- Sie hat die Oberaufsicht über die die kantonalen respektive interkantonalen Aufsichtsbehörden am Sitz der Vorsorgeeinrichtung.
- Direkt von der OAK BV beaufsichtigt werden die BVG-Anlagestiftungen sowie der Sicherheitsfonds und die Auffangeinrichtung.
- Ihr Ziel ist, die finanziellen Interessen der Versicherten verantwortungsbewusst und zukunftsgerichtet wahrzunehmen.
- Sie soll zu einer konsequenten Verbesserung der Systemsicherheit sowie von Rechtssicherheit und Qualitätssicherung betragen.

## *OWASP - Open Web Application Security Project*

- See: www.owasp.org

- Is a nonprofit security project focusing on improving ***security for online or web-based applications***.
- ***Testing methodology*** to secure web applications by providing a list of flaws and how to fix them.

### *Vulnerability Scanners*

- Link: Scanning Tools

***The Top 10 concerns as of 20xx are listed as follows:***

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Un-validated Redirects and Forwards

## *Ponemon Institute*

- See: https://www.ponemon.org/library

- Global Megatrends in Cybersecurity research.

***Result 2015***

- 75% of organization's senior leadership view security as a necessary cost instead of a competitive advantage
- 80% of boards do not receive briefings on their organization's security strategy
- 34% of organization's senior leadership views security as a strategic priority

## *SCADA - Supervisory Control and Data Acquisition*

- Unter SCADA versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.

***Typical SCADA Systems***

- Electricity transmission and distribution.
- Gas and water distribution networks.
- Oil and gas production operations.
- Gas and liquid transmission pipelines.
- …

## *SEC - U.S. Securities and Exchange Commission*

- The guidance from the U.S. Securities and Exchange Commission (SEC) applies to publicly traded companies within the SEC's jurisdiction.
- The guidance emphasizes the importance of ***information security*** within an organization and the financial impact incidents can have on financial accounting.

## *SERT - Solutionary Security Engineering Research Team*

- See: www.solutionary.com
- Works to provide the most comprehensive and informative ***threat analysis*** possible to clients.

## *SFAMA - Swiss Funds & Asset Management Association*

- See: **sfama.ch**

## *SWGDE - Scientific Working Group on Digital Evidence*

- See: **Forensic**

***Standards and Criteria 1.4***

- ❑ The agency must maintain written copies of the appropriate technical procedures.

***Standards and Criteria 1.5***

- ❑ The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.

***Standards and Criteria 1.6***

- ❑ All activities related to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

***Standards and Criteria 1.7***

- ❑ Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

## *TCG - Trusted Computing Group*

See also TPM.
See also RoT - Roots of Trust

## *U.S. Computer Security Incident Response Team (CSIRT)*

- Incident response services to any user, company, government agency, or organization in partnership with the ***Department of Homeland Security***.
- Provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

## *USC - United States Code*

- Criminal and civil law.

## *USPTO - United States Patent and Trademark Office*

- Das United States Patent and Trademark Office (PTO oder USPTO) ist das dem Handelsministerium der Vereinigten Staaten unterstellte Patentamt der Vereinigten Staaten, die Patente für Erfindungen vergibt und für die Etablierung von Marken- und geistigen Eigentumsrechten verantwortlich ist.
- Sie hat ihren Sitz seit 2006 in Alexandria (Virginia).

## *VHM - Virus Help Munich*

- Ist ein freiwilliger, privater Zusammenschluss von ***Antivirus-Forschern*** aus dem deutschsprachigen Raum.
- Ziel der VHM ist die Information und Hilfestellung für Betroffene von Computerviren sowie der Informationsaustausch der Mitglieder untereinander.

# ORGANIZATIONAL ROLES

> ***Security management*** is a responsibility of ***upper management***, not of the IT staff, and is considered a business operation issue rather than an IT administration issue.
>
> The ***security plan*** needs approval by senior management.
>
> If a company does not practice ***due care*** and ***due diligence***, ***managers can be held accountable*** for both asset and financial losses.

## *Board of Directors*

## *CEO - Chief Executive Officer*

- The CEO as the key role in the organization is expected to support information security initiatives as they relate to the mission of the business, ensure responsible funding is provided for ongoing security operations and new program initiatives, and to hold the components of the business accountable to adhering to information security policies and procedures as well as achieving their objectives in a secure manner.
- The responsibility of the CEO in regard to security is no different from the responsibility to any other part of the business or any other executive.
- As the CEO is responsible for making financial, operational, and business-risk decisions on a continuous basis, he or she needs to have enough information to make fact-based decisions that will not expose the organization to regulatory compliance issues, risk the business' reputation, or decrease the efficiency and effectiveness of the organization's capability to produce.
- Typically, the CEO of an organization reports to the ***board of directors***.

## *CFO - Chief Financial Officer*

- The chief financial officer (CFO) provides leadership through managing the integrity of the accounting procedures and records, providing financial reporting, analysis, and expertise to develop and implement the strategies to advance the organization's mission and vision into the future.
- The CFO provides oversight of the financial and accounting operations throughout the company, and handles accounts payable, accounts receivable, cash management, the processing of general ledger journal entries, and payroll, and reports directly to the CEO.

## *CIO - Chief Information Officer*

- The CIO is charged with managing the technology that supports information processing throughout the organization.
- Many of these activities fall within the scope of IT governance and IT service delivery, which support the business processes that, in turn, support an organization.
- The CIO must also ensure that servers and other IT resources are configured and managed appropriately, applications are created using secure coding techniques, access to the enterprise network is controlled, and both internal and external audit issues are addressed promptly by IT management.
- In addition to the information security responsibilities of the CEO, CIO duties include, but are not limited to:

***Duties***

- ❑ Overseeing the identification, implementation, and assessment of common security controls.
- ❑ Ensuring compliance with applicable information security requirements.
- ❑ Ensuring that personnel with significant responsibilities for system and program security assessments are trained.

- ❑ Assisting other senior officials with their responsibilities for system and program security assessments.
- ❑ Encouraging the maximum reuse and sharing of security-related information including: 1) Threat and vulnerability assessments; 2) Risk assessments; 3) Results from common security control assessments; and 4) Internal and external IT audits; 5) Any other general information that may be of assistance to information system owners and their team.
- ❑ Determining the appropriate allocation of resources dedicated to the protection of the organization's information systems based on organizational priorities.
- ❑ Ensuring that critical systems have the appropriate disaster recovery, business continuity/contingency plans and emergency operating procedures, recovery procedures, mechanisms, and that measures are developed, maintained, and tested on a periodic basis

## *CISO - Chief Information Security Officer*

- A Chief Information Security Officer (CISO) is an organizational leader who defines and directs the program that manages information security risks facing an organization.
- A CISO can operate as a corporate executive or as a non-executive specialist who directs the security program.
- The Chief Information Security Officer works closely with the Chief Information Officer and other managers and personnel involved in securing the organization's information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed.
- CISOs who operate as organizational executives have elevated influence in the organization, but they also take on more responsibility for the day-to-day operations of the organization and delivery of the organization's products, services, and objectives.
- Executive CISOs require broad knowledge of information security and risk management practices. They also require broad knowledge of business management and organizational leadership.
- Non-executive CISOs are not exempt from a fundamental knowledge of business practices.
- In fact, this knowledge is critical as they communicate information up to the organizational leaders and lead operations directing the work and activities within lower levels of the organization.

***Duties***

- ❑ Ensuring the development and maintenance of an organization-wide information security program including information security policies, procedures, and control techniques to address all applicable requirements in compliance with organizational policies and standards.
- ❑ Coordinating the implementation of security controls to protect organizational interests and assets.
- ❑ Conducting security audits, verifications and acceptance checks, and maintain documentation on the results.
- ❑ Coordinating an annual, formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- ❑ Reviewing contract and procurement vehicles to ensure they address appropriate security measures.
- ❑ Defining and implementing performance metrics to evaluate the effectiveness of information security programs.
- ❑ Making high-level decisions pertaining to the information security policies, as well as their content and their effectiveness--and approving exceptions to these policies in advance on a case-by-case basis.
- ❑ Annually reviewing information security policies and procedures to maintain adequacy in light of emergent business requirements, regulatory requirements, security threats, or other technology developments.
- ❑ Reviewing business cases and budget submissions to ensure that information security requirements are addressed and adequately resourced.
- ❑ The CISO should ensure that a plan for system and data disposal is documented and asset inventories provide the date of anticipated disposal.

***CISO's Information Security Program***

- Information security programs exist to provide risk awareness and management in an organization.


***Security Operations Program***


***SOC - Security Operations Center***

- The Security Operations Center (SOC) provides the foundation for a security operations program.
- The SOC is defined by the coordinated efforts of personnel, processes, and technology to identify information security events, and provide timely response and remediation.
- It is extremely important to define the mission, charter, objectives, and responsibilities when implementing a SOC.

***CPIC - Capital Planning and Investment Control***

## *CCO - Chief Compliance Officer*

- The chief compliance officer (CCO) is often the legal authority within a company, providing guidance and advice to improve the business's understanding of related laws and regulatory requirements.
- The responsibilities within the role typically consist of developing and maintaining the compliance portion of relationships with key external organizations, including regulators and other key business partners.

## *CMO - Chief Marketing Officer*

- The chief marketing officer (CMO) is responsible for providing strategic leadership as a member of the executive team and as a trusted advisor to inter-departmental and operational leaders throughout the organization.
- They are the lead on the business’s marketing strategy, from ideation to implementation to optimization, working with a team of marketing professionals to establish clear goals and key performance indicators (KPIs) aligned with the overall company goals and initiatives.
- They think strategically around creative objectives but will also be able to align the marketing strategy with the firm’s overall financial goals.

## *COO - Chief Operational Officer*

- The chief operations officer (COO) plans and directs all company operational policies and initiatives.
- They lead the business strategy, overseeing the business operations throughout the company, and lead the strategic planning and development activities.

- The COO is responsible for the functions and operational efficiency of the company as well as a host of other responsibilities.
- Additional duties can include supporting the strategic direction of the company and steering the collective executive suite. The COO reports to the CEO.

**Challenges:**
- Lack of visibility across the supply chain.
- Optimization of the supply chain to increase speed of products to market.
- Avoiding disruption and increase production efficiency and quality.
- Improving vendor collaboration.
- Improving the customer experience.

## *CRO - Chief Risk Officer*

- The Chief Risk Officer (CRO) position and role is largely dependent on the industry in which the CRO is positioned.
- For example, the CRO in the financial industry will likely be responsible for the risk associated with investments and investment strategies.

***Duties***
- ❑ Managing and developing a comprehensive process for assessing, identifying, monitoring, and reducing pertinent business risks that could interfere with the organization's objectives and goals.
- ❑ Ensuring that the organization is in substantial compliance with its internal operating policies and procedures and any external legal, regulatory, or contractual requirements.
- ❑ Managing the implementation of all aspects of the risk management program, including implementation of processes, tools, and systems to identify, assess, measure, manage, monitor, and report risks.
- ❑ Assisting in the development and management of processes to identify and evaluate business risks--as well as risk and control self-assessments.
- ❑ Conducting compliance and risk assessments.  Conducting and documenting audits of client compliance to industry standards.

## *CTO - Chief Technology Officer*

- The Chief Technology Officer (CTO) is responsible for system administrators and provides the direct link between information security policies and the network, systems, and data.

***Duties***
- ❑ Ensuring the application of information security policies and procedures, as applicable, to all information assets.
- ❑ Ensuring an up-to-date network diagram, including wireless networks, is maintained.  Ensuring physical access to publicly accessible network jacks, wireless access points, gateways, and handheld devices are restricted.
- ❑ Ensuring adding, removing, and maintaining system users, as well as configuring their access controls to provide the users necessary access is performed with the principle of least privilege.
- ❑ Ensuring system parameters within the documented security standards are configured using the applicable information security guidance and system lifecycle documentation.
- ❑ Ensuring current documentation is maintained that properly defines the technical hardware and software configuration of system and network connections for systems for which they are responsible.
- ❑ Ensuring the proper installation, testing, protection, and use of system software.
- ❑ Ensuring regular backups are performed and conducting recovery tests and other associated contingency planning responsibilities for systems for which they are responsible.
- ❑ Ensuring system audit logs/trails and system logs are captured for review.  Ensuring system/user access is monitored for performance and security concerns--and reporting any anomalies to the information security program, as appropriate.
- ❑ Ensuring patches and hot fixes are applied as directed, following configuration management policies and procedures (including security patch management).
- ❑ Providing support for internal and external audit activities.

## *SA - Security Administrator*

***Duties***

- ❑ Setting user clearances, initial passwords, and other security characteristics for new users
- ❑ Changing security profiles for existing users
- ❑ Setting or changing file sensitivity labels
- ❑ Setting the security characteristics of devices and communications channels
- ❑ Reviewing audit data

## *EA - Enterprise Architect*

- The Enterprise Architect (EA) has a broad and deep understanding of the organization's overall business strategy and general IT trends and directions. The role of CEA is to:

***Duties***

- ❑ Lead enterprise architecture development and implementation efforts.
- ❑ Collaborate with lines of business within the organization to ensure proper integration of lines of business into enterprise architecture.
- ❑ Participate in strategic planning and performance-planning activities to ensure proper integration of enterprise architecture.
- ❑ Facilitate integration of information security into all layers of enterprise architecture to ensure organization implementation of secure solutions.
- ❑ Work closely with the program managers, the CISO, and the business owners to ensure that all technical architecture requirements are adequately addressed.

# LAWS, REGULATIONS, AND COMPLIANCE

**Categories of Laws:**

- Criminal Law
- Civil Law / Tort law
- Administrative Law

***Administrative Law***

- Deals with regulatory standards that regulate performance and conduct.
- Government agencies creates these standards, which are usually applied to companies and individuals within those companies.

## *ACTA - Anti-Counterfeiting Trade Agreement*

- Proposes a framework for international enforcement of ***intellectual property protections***.

## *AIFMD - Alternative Investment Fund Managers Directive*

- As a general matter, AIFMD introduces a passport system for the *marketing of EU or non EU Alternative Investment Funds ("AIF") in the EU* ("**EU-marketing passport**") as well as the possibility for EU and non EU Alternative Investment Funds Managers ("**AIFM**") to manage EU or non EU AIF on a cross-border basis ("**EU-management passport**").

## *ASCLD - American Society of Crime Laboratory Directors*

- Is a nonprofit professional society of crime laboratory directors and forensic science managers dedicated to providing excellence in forensic science through leadership and innovation.
- The purpose of the organization is to foster professional interests, assist the development of ***laboratory management principles*** and ***techniques***; acquire, preserve, and disseminate forensic based information; maintain and improve communication among crime laboratory directors; and to promote, encourage, and maintain the highest standards of practice in the field.

## *BankG - Bankengesetz*

- Dem Bankengesetz unterstehen Banken, Privatbankiers und Sparkassen.
- Es regelt u.a. die Bewilligung zum Geschäftsbetrieb und beinhaltet Vorschriften über die Geschäftstätigkeit.

## *BASEL II*

- Der Terminus **Basel II** bezeichnet die Gesamtheit der Eigenkapitalvorschriften, die vom Basler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden.
- Die Regeln müssen gemäss den EU-Richtlinien 2006/48/EG und 2006/49/EG seit dem ***1. Januar 2007*** in den Mitgliedsstaaten der Europäischen Union für alle Kreditinstitute und Finanzdienstleistungsinstitute angewendet werden.
- Während in der Schweiz die Umsetzung durch die Eidgenössische Bankenkommission geleitet wird, erfolgt diese in Deutschland durch das Kreditwesengesetz, die Solvabilitätsverordnung und die MaRisk.

## *BASEL III*

- **Basel III** (or the **Third Basel Accord**) is a global, voluntary regulatory framework on bank capital adequacy, stress testing, and market liquidity risk.
- It was agreed upon by the members of the Basel Committee on Banking Supervision in 2010-11, and was scheduled to be introduced from 2013 until 2015; however, changes from 1 April 2013 extended implementation until 31 March 2018 and again extended to 31 March 2019.
- The third installment of the Basel Accords (*see Basel I, Basel II*) was developed in response to the deficiencies in financial regulation revealed by the financial crisis of 2007-08. Basel III is intended to strengthen bank capital requirements by increasing bank liquidity and decreasing bank leverage.

## *CALEA - Communications Assistance for Law Enforcement Act (1994)*

- The Communications Assistance For Law Enforcement Act is a U.S. federal wiretapping law passed by Congress and signed into law by President Bill Clinton in 1994.
- At the time, phone companies were transitioning from the old electromechanical switching equipment to newer digital switching equipment in their central offices.
- The Federal Bureau of Investigation and other law enforcement agencies in the U.S. were worried that the new digital switching equipment would make it difficult for them to conduct wiretaps.
- The law requires equipment manufacturers and telecommunications providers to allow law enforcement agencies to intercept communications on digital switching equipment.
- Not only do telcos have to cooperate with investigations, equipment manufacturers are required to provide access using hardware and software designs.

## *CCCA - Comprehensive Crime Control Act (1984)*

- The Comprehensive Crime Control Act of 1984 (Pub.L. 98-473, S. 1762, 98 Stat. 1976, enacted October 12, 1984) was the first comprehensive revision of the U.S. criminal code since the early 1900s. It was signed into law by President Ronald Reagan. Among its constituent parts and provisions were:
    - Armed Career Criminal Act
    - Sentencing Reform Act which created the United States Sentencing Commission
    - extension of the United States Secret Service's jurisdiction over credit card fraud and computer fraud
    - increased federal penalties for cultivation, possession, or transfer of marijuana
    - a new section in the criminal code for hostage taking
    - re-institution of the federal death penalty
    - Stipulations about using civil forfeiture to seize assets of organized crime.[1]

## *CFAA - Computer Fraud and Abuse Act (1986/1994)*

- The Computer Fraud and Abuse Act (CFAA) is a United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984.
- The law prohibits accessing a computer without authorization, or in excess of authorization.
- Prior to computer-specific criminal laws, computer crimes were prosecuted as mail and wire fraud, but the applying law was often insufficient.
-

## *COBIT - Control Objectives for Information and Related Technology*

- Guideline for auditors
- ***ISACA*** framework for IT management and IT governance.
- ***Security concept infrastructure*** used to organize the complex security solutions of companies.
- See also: "coopers and lybrand white paper on nt"
- See also: ***Security Risk Management***

**The four Domains are:**

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

***COBIT 4.1***

- Is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks.

***COBIT 4.1 PO1.2 Business IT-Alignment***

- Establish processes of education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration.
- Mediate between business and IT imperatives so priorities can be mutually agreed.

***COBIT 5.0 addresses 5 Principles, which are:***

- Principle 1: Meeting Stakeholder Needs
- Principle 2: Covering the Enterprise End to End
- Principle 3: Applying a Single, Integrated Framework
- Principle 4: Enabling a Holistic Approach
- Principle 5: Separating Governance from Management

***COBIT 5.0 AP002 Manage Strategy Process Description***

- Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment.
- Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable, and efficient response to strategic objectives.

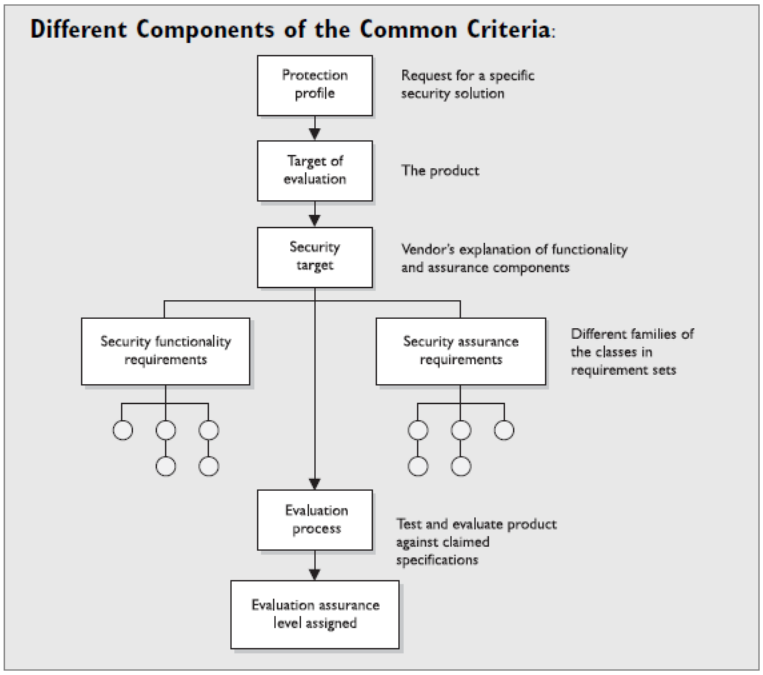
## *Common Criteria*

See: www.niap-ccevs.org

- See also ***ISO 15408***.
- Formally known as the "***Arrangement on the Recognition of Common Criteria in the Field of IT Security***".
- The Common Criteria was designe as a product evaluation model (***CC-evaluated*** products).
- The common criteria define various levels of ***testing*** and ***confirmation of systems security capabilities***, and the number of the level indicates what kind of testing and confirmation has been performed.

***EAL - Evaluation Assurance Levels***

- **EAL1:** Functionally Tested
- **EAL2**: Structurally Tested
- **EAL3**: Methodically Tested and Checked
- **EAL4**: Methodically Designed, Tested and Reviewed
- **EAL5**: Semi-formally Designed and Tested
- **EAL6**: Semi-formally Verified Design and Tested
- **EAL7**: Formally Verified Design and Tested




***PP - Protection Profile***

- A Protection Profile (PP) is a document used as part of the certification process according to ***ISO/IEC 15408*** and the ***Common Criteria (CC)***.
- As the generic form of a ***Security Target (ST)***, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.
- A PP is a combination of ***threats***, ***security objectives***, ***assumptions***, ***security functional requirements (SFRs)***, ***security assurance requirements (SARs) and rationales***.

***ST - Security Target***

- The document that identifies the security properties of the target of evaluation.
- The ST may claim conformance with one or more PPs.
- The TOE is evaluated against the ***SFRs*** (Security Functional Requirements).
- Again, see below) established in its ST, no more and no less.
- This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product.
- This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements.
- The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.

## *Copyrights*

- Copyright law protects only the actual text oft he sourece code and doesn't prohibit others from rewriting your code in a different form and accomplishing the same objective. If you treat your source code as a ***trade secret***, it keeps it out oft he hands of your competitors in the first place.

## *CalOPPA - California Online Privacy Protection*

- The first state law in the nation to require commercial websites and online services to post a privacy policy, the California Online Privacy Protection Act (CalOPPA) went into effect in 2004. It was amended in 2013 to require new privacy disclosures regarding tracking of online visits.
- CalOPPA applies to any person or company in the United States (and conceivably the world) whose website collects ***personally identifiable information*** from California consumers.
- CalOPPA requires the website to feature a conspicuous privacy policy stating exactly what information is collected and with whom it is shared; it also requires the operator of the website or online service to comply with the site's privacy policy.

- Those who fail to do so are at risk of civil litigation under the state's ***unfair competition law***.

## *CCPA - Cable Communications Policy Act*

- Amended by the USA PATRIOT ACT of 2001, and/or the Privacy Protection Act of 1980 (PPA).

## *COPPA - Children's Online Privacy Protection Act (1998)*

- Der Children's Online Privacy Protection Act (COPPA, deutsch: „***Gesetz zum Schutz der Privatsphäre von Kindern im Internet***“) ist ein Gesetz, welches am 21. April 2000 in den USA als Federal Trade Commission (FTC) Children's Online Privacy Protection Act (COPPA) in Kraft trat.
- Sein Gegenstand ist es, für die Betreiber von Websites Regeln zu schaffen, wie mit den persönlichen Daten von ***Kindern unter 13 Jahren*** umzugehen ist.
- In Deutschland wird man vor allem mit dem COPPA konfrontiert, wenn man sich in einem auf amerikanischer Software basierenden Webforum registrieren möchte.
- Während der Registrierung muss die Frage beantwortet werden, ob man unter 13 Jahre alt ist. Antwortet man mit ja, verlangt die Forensoftware eine Einverständniserklärung der Eltern, um die Registrierung durchzuführen.
- Da die COPPA-Richtlinien in Deutschland jedoch nicht gelten, ist eine Registrierung auch ohne Einverständniserklärung zulässig.

## *CRA - Canada Revenue Agency*

- The CRA has released some guidance for entities that could be subject to the US Foreign Account Tax Compliance Act (FATCA) regime - which came into effect on July 1, 2014.
- The guidance is intended to provide clarity to help financial institutions and their advisors understand and comply with their due diligence and reporting obligations under Canada's intergovernmental agreement (IGA) with the United States.

## *CSA - Computer Security Act (1987)*

- The Computer Security Act of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988), was a United States federal law enacted in 1987.
- It was intended to improve the security and privacy of sensitive information in federal computer systems and to establish minimally acceptable security practices for such systems.
- It required the creation of ***computer security plans***, and ***appropriate training of system users*** or ***owners*** where the systems would display, process or store sensitive information.

## *CSSF - Commission de Surveillance du Secteur Financier*

- See: http://www.cssf.lu/de/die-cssf/aufgaben-und-zustaendigkeitsbereich/
- Die Commission de Surveillance du Secteur Financier (CSSF) führt ihren Auftrag als Aufsichtsbehörde mit dem Ziel durch, die Solidität und Stabilität des Finanzsektors sicherzustellen.
- Dies erfolgt ausschliesslich im öffentlichen Interesse.
- Im Rahmen ihrer Befugnisse kontrolliert die CSSF, dass die zugelassenen Unternehmen und Emittenten die auf sie anwendbaren Rechtsvorschriften einhalten, einschliesslich der Rechtsvorschriften zum Verbraucherschutz im Finanzsektor und zur Verhinderung von ***Geldwäsche*** oder ***Terrorismusfinanzierung*** im Finanzsektor.
- Die CSSF vertritt die ***luxemburgische Aufsicht*** auf internationaler und europäischer Ebene.
- Bei der Verwirklichung ihrer Ziele verfolgt die CSSF einen aufsichtsrechtlichen Ansatz in Übereinstimmung mit internationalen Standards und unter Berücksichtigung des Verhältnismässigkeitsgrundsatzes, welcher mit Professionalität zur Gewährleistung einer unabhängigen, zukunftsorientierten und risikobasierten Überwachung umgesetzt wird.
- Die CSSF ist transparent und fördert einen effizienten Austausch mit den Stakeholders des Finanzsektors unter Berücksichtigung der Anforderungen des Berufsgeheimnisses.
- Sie misst der Integrität und Verantwortung grösste Bedeutung bei und versucht, mit Engagement und Anpassungsfähigkeit ihre Ziele zu erreichen.
- Die CSSF verpflichtet sich, eine ordnungsgemässe Verwaltung zu gewährleisten und ihre Aufgaben in effizienter Weise zu erfüllen.

- Dies erfolgt im Hinblick auf eine konstruktive Zusammenarbeit sowohl innerhalb der CSSF als auch auf nationaler, europäischer und internationaler Ebene.

## *DIACAP - DoD Information Assurance Certification and Accreditation Process*

- Is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply ***risk management to information systems (IS)***.

## *DIN EN 55159*

- Bahnanwendungen
- Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme
- Sicherheitsrelevante Kommunikation in Übertragungssystemen

## *DIN VDE 31000*

- General principles for the safe design of products.

## *DIN 66399 - Guidelines for Disposal of IT equipment*

- In case of shredding use DIN66399 specifications; security level 5 or higher.

## *DMCA - Digital Millenium Copyright Act*

- Copyright principals for ***webcasting***.

## *DoD - Rainbow Series (Outdated)*

Link: https://csrc.nist.gov/publications/detail/white-paper/1985/12/26/dod-rainbow-series/final
http://csrc.nist.gov/publications/secpubs/index.html

- A set of publications with colored covers.
- The Rainbow Series of Department of Defense standards is ***outdated***, out of print.
- See now TCSEC.

**Red Book**
- Trusted Network Interpretation (July 31, 1987)

**Orange Book** (based on Bell-LaPadula)
- DoD Trusted Computer System Evaluation Criteria (December 26, 1985)
- A Guide to Understanding Configuration Management in Trusted Systems (March 28, 1988)

***Defines:***
Operational assurance
Life cycle assurance

**Neon Orange Book**
- A Guide to Understanding Discretionary Access Control in Trusted Systems (September 30, 1987)

**Green Book**
- DoD Password Management Guideline (April 12, 1985)

**Light Yellow Book**
- Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (June 25, 1985)

**Yellow Book II**
- Technical Rationale Behind CSC-STD-003-85: Computer Security Requirement (June 25, 1985)

**Tan Book**

- A Guide to Understanding Audit in Trusted Systems (July 28, 1987)

**Bright Blue Book**
- Trusted Product Security Evaluation Program: a Guide for Vendors (March 1, 1988)

**Blue Book**
- Trusted Product Evaluation Questionnaire (October 16, 1989)

**Aqua Book**
- Glossary of Computer Security Terms (October 21, 1988)

**Lavender Book**
- A Guide to Understanding Trusted Distribution in Trusted Systems (December 15, 1988)

**Purple Book**
- Guidelines for Formal Verification Systems (April 1, 1989)

**Brown Book**
- Guide to Understanding Trusted Facility Management (June 1989)

## *DSGVO - Datenschutz-Grundverordnung*

- Links: https://deinedatendeinerechte.de/downloads/

- Die DSGVO beinhaltet Regelungen rund um die Sammlung, Speicherung und Verarbeitung personenbezogener Daten - beispielsweise:
  - die Verpflichtung zu regelmässigem Reporting und Monitoring
  - Meldepflicht bei Datenverletzungen und der Durchführung sogenannter Datenschutz-Folgeabschätzungen.

Kapitel 1: Allgemeine Bestimmungen
Gegenstand und Ziele, sachlicher und räumlicher Anwendungsbereich, Begriffsbestimmungen.

Kapitel 2: Grundsätze und Rechtmässigkeit
Grundsätze und Rechtmässigkeit der Verarbeitung personenbezogener Daten, Bedingungen für die Einwilligung, Verarbeitung besonderer Kategorien personenbezogener Daten.

Kapitel 3: Rechte der betroffenen Person
Transparenz und Modalitäten, Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten, Berichtigung und Löschung - das „Recht auf Vergessenwerden“ -, Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall einschliesslich Profiling

Kapitel 4: Verantwortlicher und Auftragsverarbeiter
Allgemeine Pflichten, Sicherheit personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Datenschutzbeauftragter, Verhaltensregeln und Zertifizierung.

Kapitel 5: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Kapitel 6: Unabhängige Aufsichtsbehörden

Kapitel 7: Zusammenarbeit und Kohärenz, Europäischer Datenschutzausschuss

Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen

Kapitel 9: Vorschriften für besondere Verarbeitungssituationen
u. a. Verarbeitung und Freiheit der Meinungsäusserung und Informationsfreiheit, Datenverarbeitung am Arbeitsplatz, Zugang der Öffentlichkeit zu amtlichen Dokumenten, Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften.

Kapitel 10: Delegierte Rechtsakte und Durchführungsrechtsakte

Kapitel 11: Schlussbestimmungen
u. a. Aufhebung der Richtlinie 95/46/EG und Inkrafttreten der DSGVO

## *ECPA - Electronic Communications Privacy Act (1986)*

- The Electronic Communications Privacy Act of 1986 (ECPA) was enacted by the United States Congress to extend restrictions on government wire taps of telephone calls to include transmissions of electronic data by computer (18 U.S.C. § 2510 et seq.), added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act (SCA, 18 U.S.C. § 2701 et seq.), and added so-called pen trap provisions that permit the tracing of telephone communications (18 U.S.C. § 3121 et seq.).
- ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications.
- The ECPA has been amended by the Communications Assistance for Law Enforcement Act (CALEA) of 1994, the USA PATRIOT Act (2001), the USA PATRIOT reauthorization acts (2006), and the FISA Amendments Act (2008).

## *eIDAS -*

- The eIDAS regulation allows the European Union to provide a legal framework for ***transnational digital transactions***.
- It is aiming for the enhancement of electronic exchanges' trust.
- It establishes a framework for electronic identification and trust services, including the topic of the ***electronic signature***.
- Thus, the eIDAS regulation enhances the transparency and reliability of transactions.
- Being compliant with the eIDAS regulation enables you to offer your suppliers and your customers an increased confidence in your services and a simplification of their procedures.

## *EMIR - European Market Infrastructure Regulation*

- Regulierung des ausserbörslichen Derivatehandels ist das Thema der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister.
- Über die Abkürzung EMIR für die inoffizielle englische Bezeichnung European Market Infrastructure Regulation hat die Kurzbezeichnung EMIR-Verordnung weite Verbreitung gefunden.
- Der deutsche Gesetzgeber spricht von ihr auch als Marktinfrastrukturverordnung.
- Die Verordnung regelt den ausserbörslichen Handel mit Derivaten.
- Kern der Regulierung ist die Verpflichtung der Marktteilnehmer zum Clearing ihrer ausserbörslichen Standard-Derivatgeschäfte über einen Zentralen Kontrahenten sowie die Meldung dieser Geschäfte an ein Transaktionsregister.
- Mit der Umsetzung der EMIR-Verordnung ist die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) betraut.

## *EP2 - EFT POS 2000*

- Ist der Spezifikationsstandard für die Abwicklung und den Aufbau von ***EFT-Transaktionszahlungen*** im bargeldlosen Zahlungsverkehr.
- EP2 stellt dabei sicher, dass für alle Karteninhaber im Schweizer Markt ein einheitlicher, moderner Kommunikationsstandard geschaffen und eingehalten wird.

## *EPPIA - Economic and Protection of Proprietary Information Act (1996)*

- This is a United States federal law addressing industrial and corporate espionage.
- It was introduced in 1996.
- The law stipulates that proprietary, economically valuable information shall be construed as property, allowing for the theft of such information to be prosecuted.

## *EUDPD - European Union Data Protection Directive (Directive 95/46/EC)*

- Restricts data transfers to countries outside oft he EU.

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA defines the standards for data management for citizens of the European Union.
- Commonly known as the EU Data Protection Directive, the law sets strict limits on the collection and use of personal data and demands that each member state set up an independent national body responsible for the protection of this data.
- The objective of this law, current as of May 2016, is to give citizens back control over of their personal data and to simplify the regulatory environment for business.
- Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose, and the Directive foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad.

***EU Data Protection Directive Features:***

- Notice: Data subjects should be given notice when their data is being collected.
- Purpose: Data should only be used for the purpose stated.
- Consent: Data should not be disclosed without the subject's consent.
- Security: Collected data should be kept secure from any potential abuses.
- Disclosure: Data subjects should be informed as to who is collecting their data.
- Access: Data subjects should be allowed to access their data and make corrections to any inaccurate data.
- Accountability: Data subjects should have an available method to hold data collectors accountable for following these six principles above.

## *EUPL - European Union Privacy Law (1995)*

- Every organizations based outside of Europe must consider the applicability of these rules due to ***trans-boarder data flow*** requirements.
- Deals with ***Electronic Signatures*** and ***Non repudiation***.

## *FATCA - Foreign Account Tax Compliance Act*

- Der Foreign Account Tax Compliance Act (FATCA) ist ein im Jahr 2010 in Kraft getretenes US-Gesetz, das in den USA steuerpflichtige Naturalpersonen und Unternehmen mit Sitz ausserhalb der USA zur Mitteilung steuererheblicher Daten, insbesondere von Auslandskonten gegenüber den US-Steuerbehörden verpflichtet.

- Durch bilaterale Abkommen mit anderen Staaten wollen die USA den gegenseitigen Datenaustausch gewährleisten.

- Ziel ist die Bekämpfung von Steuerflucht und die Förderung der Steuerehrlichkeit bei internationalen Sachverhalten.

## *FERPA - Family Educational Rights and Privacy Act*

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.
- The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
- FERPA gives parents certain rights with respect to their children's education records.
- These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

## *FFIEC - Federal Financial Institutions Examination Council*

- The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the

Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.
- In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

## *FINMA - Eidgenössische Finanzmarktaufsicht*

- Die Behörde verfolgt nach Massgabe der Finanzmarktgesetze den Zweck, Gläubiger, Anleger und Versicherte zu schützen (Anlegerschutz).
- Die Behörde bewilligt den Betrieb der ihrer Aufsicht unterstellten Unternehmen und Organisationen und überwacht sie.
- Sie ist zuständig für die Geldwäschereibekämpfung und wickelt bei Bedarf Sanierungsverfahren und Konkurse ab.

## *FISMA - Federal Information Security Management Act (2002)*

- FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems.
- In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.
- According to FISMA, the term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.
- The Federal Information Security Management Act (FISMA) of 2002 provides consistent security practices across the U.S. government. FISMA accomplishes this goal by standardizing the process for risk management and information security practices for all federal agencies and the contractors that do business with the government.
- The Federal Information Security Modernization Act (FISMA) of 2014 updated the cybersecurity practices defined in FISMA 2002 by codifying ***Department of Homeland Security (DHS)*** authority to administer the implementation of information security policies for non-national security federal Executive Branch systems.
- FISMA 2004 also amended and clarified the ***Office of Management and Budget's (OMB)*** oversight authority over federal agency information security practices by requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting".
- Regulations regarding: ***Log Management***

***Important FISMA Features:***

- Periodic risk assessments.
- Policies and procedures based on assessments.
- Qualitative risk rating—data-driven security model.
- Subordinate plans for information security for networks, facilities, and other sub-systems.
- Security awareness training for personnel.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls at least annually.
- A process to address deficiencies in information security policies (POAM).
- Procedures for detecting, reporting, and responding to security incidents.
- Procedures and plans to ensure continuity of operations for information systems that support the organization's operations and assets.

## *FIPS - Federal Information Processing Standard*

- Defines the ***hardware*** and ***software*** requirements for ***cryptographic modules*** that the federal government uses.

**Minimum requirement for Audit Data:**

- Create, protect and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity.

- Ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

***FIPS-140***
- NIST issues the 140-publication series to coordinate the requirement for cryptographic modules which include both ***hardware*** and ***software*** components for use by departments and agencies of th US federal government.
- Standard for ***hardware*** and ***software*** cryptographic modules.

***FIPS-140-2***
- The Federal Information Processing Standard Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
- The title is Security Requirements for Cryptographic Modules.
- Initial publication was on May 25, 2001 and was last updated December 3, 2002.
- FIPS 140-2 defines ***four levels of security***, simply named "Level 1" to "Level 4".
- It does not specify in detail what level of security is required by any particular application.

  **Level 1**
  Security Level 1 provides the lowest level of security.

  **Level 2**
  Security Level 2 improves upon the physical security mechanisms by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

  **Level 3**
  In addition to Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module.

  **Level 4**
  Security Level 4 provides the highest level of security.

***FIPS 153 | 3D graphics***

***FIPS-186***
- DSA - Digital Signature Algorithm
- DSS - Digital Signature Standard (asymmetric key algorithm)

***FIPS 197 | Advanced Encryption Standard (AES)***

***FIPS 199 | Std. for Security Categorization of Federal Information and Information Systems***

***FIPS 201 | Personal Identity Verification for Federal Employees and Contractors***

## *FOIA - Freedom of Information Act*

- Der Freedom of Information Act (FOIA) ist ein 1967 in den USA in Kraft getretenes Gesetz zur Informationsfreiheit und gibt jedem das Recht, Zugang zu Dokumenten von staatlichen Behörden zu verlangen.

## *FSC - Federal Sentencing Guidelines (1991)*

- The Federal Sentencing Guidelines are rules that set out a uniform sentencing policy for individuals and organizations convicted of felonies and serious (Class A) misdemeanors in the United States federal courts system.
- The Guidelines do not apply to less serious misdemeanors.
- States, that ***senior management*** could be responsible for monetary damages up to ***10 Mio. USD*** or twice the gain of the offender for nonperformance of due diligence in accordance with the U-S. Federal Sentencing Guidelines of 1991.

## *GAK - Government Access to Keys*

- The idea behind is simple: ensure the government has a way to decrypt encrypted communications so they can wiretap the bad guys when needed to keep the public safe

## *GASSP - Generally Accepted System Security Principles*

- See also: GAISP

## *GAISP - Generally Accepted System Security Principles*

- See: www.gaisp.org
- GAISP is the successor project to the GASSP, the Generally Accepted System Security Principles.
- The original GASSP project was formed in mid-1992 in response to Recommendation #1 of the report "Computers at Risk" (CAR), published by the United States of America's National Research Council in December of 1990.

Principles at all levels are developed by information security practitioners who fully understand the underlying issues of the documented practices and their application in the real world.
Then, these principles will be reviewed and vetted by skilled information security experts and authorities who will ensure that each principle is:

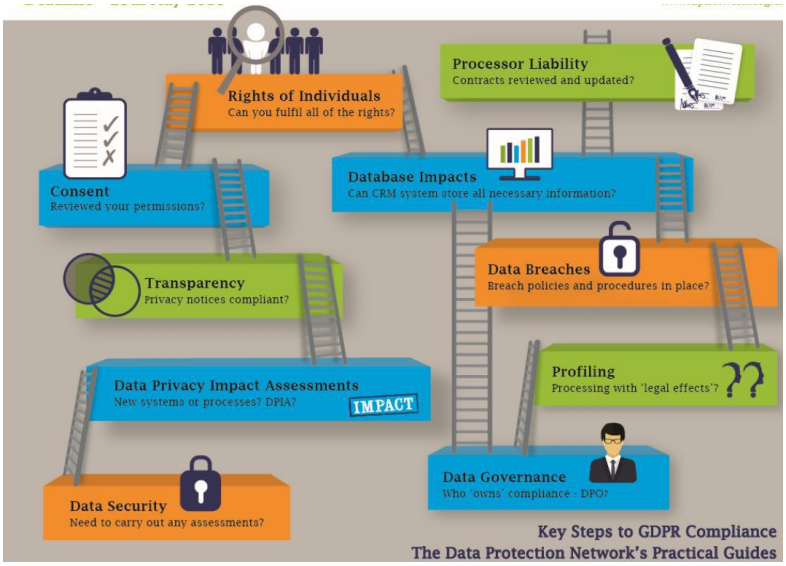
- Accurate, complete, and consistent
- Compliant with its stated objective
- Technically reasonable
- Well-presented, grammatically and editorially correct
- Conforms to applicable standards and guidelines

***The principles are:***

- Computer security supports the mission of the organization
- Computer security is an integral element of sound management
- Computer security should be cost-effective
- System owners have security responsibilities outside their own organization
- Computer security responsibilities and accountability should be made explicit
- Computer security requires a comprehensive and integrated approach
- Computer security should be periodically reassesed
- Computer security is constrained by societal factors

## *GDPR - General Data Protection Regulation (EU)*

- Deadline: 25.05.2018
- Auch bekannt unter ***RGPD*** (BE, FR, IT, LU, PT)
- Die ***DSGVO*** (AT, DE) beinhaltet Regelungen rund um die Sammlung, Speicherung und Verarbeitung personenbezogener Daten.
- Die Datenschutz-Grundverordnung (DSGVO, GDPR) zielt darauf ab, EU-Bürgern die Kontrolle über ihre persönlichen Daten zu geben. Insbesondere müssen neu Benutzer die explizite Zustimmung (Consent) zur Verwendung von persönlichen Daten geben.
- ***Airlock IAM 7*** unterstützt die Einhaltung der GDPR-Richtlinien durch die Verwaltung der Einverständniserklärungen von Benutzern für die Verwendung von Profildaten und für den Zugriff auf geschützte Applikationen oder Schnittstellen. Airlock IAM kann beispielsweise den Zugriff auf eine Applikation oder die Weitergabe von schützenswerten Profildaten so lange verhindern, bis der Benutzer die geforderte Einverständniserklärung akzeptiert hat. Durch den Einsatz von ***Self-Services*** kann der Benutzer jederzeit seine Einverständniserklärungen prüfen und widerrufen.




## *GLBA - Gramm-Leach-Bliley Act (1999)*

- The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
- The Act consists of three sections:
    - The Financial Privacy Rule, which regulates the collection and disclosure of private financial information;
    - the Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information; and the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses).
    - The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices

- Regulations regarding: ***Log Management***

## *GeBüV - Geschäftsbücherverordnung*

- Wer buchführungspflichtig ist, muss ein Hauptbuch und, je nach Art und Umfang des Geschäfts, auch Hilfsbücher führen.
- Das Hauptbuch besteht aus:
    - a) Den Konten (sachlogische Gliederung aller verbuchten Geschäftsvorfälle), auf deren Basis Betriebsrechnung und Bilanz erstellt werden;
    - b) Dem Journal (chronologische Erfassung aller verbuchten Geschäftsvorfälle).
- Die Hilfsbücher müssen in Ergänzung zum Hauptbuch die Angaben enthalten, die zur Feststellung der Vermögenslage des Geschäftes und der mit dem Geschäftsbetrieb zusammenhängenden Schuld- und Forderungsverhältnisse sowie der Betriebsergebnisse der einzelnen Geschäftsjahre nötig sind. Darunter fällt insbesondere die Lohnbuchhaltung, die Debitoren- und Kreditorenbuchhaltung sowie die fortlaufende Führung der Warenbestände bzw. der nicht fakturierten Dienstleistungen.

## *HIPAA - Health Insurance Portability and Accountability Act (1996)*

- Laws for HMOs.
- Die **Health Insurance Portability and Accountability Act** ( **HIPAA** ) wurde vom US-Kongress im Jahre ***1996*** erlassen.
- Laut der Website -Zentren für Medicare und Medicaid (CMS) Titel I der HIPAA schützt die Krankenversicherung Arbeitnehmer und ihre Familien, wenn Sie sich verändern oder ihren Arbeitsplatz verlieren.

- Titel II der HIPAA, bekannt als die Bestimmungen zur Administrativen Vereinfachung (AS), dies erfordert die Einrichtung von nationalen Normen für elektronische Gesundheitswesen Transaktionen und nationalen Bezeichner für Anbieter, Krankenversicherung Pläne und Arbeitgeber. Dient dem Datenschutz.
- Regulations regarding: ***Log Management***

Tool: ***Synedra*** (SW zum Schutz der Patienteninformationen)

***Important HIPAA Features:***

- ***Electronic Transaction and Code Sets Standards:*** Requires the same healthcare transactions, code sets, and identifiers.
- ***Privacy Rule:*** Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
- ***Security Rule:*** Specifies administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity and availability of electronic protected health information.
- ***National Identifier Requirements***: Requires that healthcare providers, health plans, and employers have standard national numbers that identify them on standard transactions.
- ***Enforcement Rule:*** Provides standards for enforcing all the Administration Simplification Rules.

## *HITECH - Health Information Technology for Economic and Clinical Health Act (2009)*

- Regulation of notifying affected individuals when the breach affects more than ***500 individuals***.
- The Health Information Technology for Economic and Clinical Health Act (HITECH) was created to promote the adoption and meaningful use of health information technology.
- The law significantly modifies HIPAA by adding new requirements concerning privacy and security for patient health information.
- The law also expands the scope of privacy and security protections available under HIPAA, increases the potential legal liability for non-compliance, and provides for more enforcement.

***Important HITECH Features:***

- Expansion of HIPAA security standards to “business associates” that perform activities involving the use or disclosure of individually identifiable health information.
- Increased civil penalties for “willful neglect.”
- Data-breach notification requirements for unauthorized uses and disclosures of “unsecured PHI.”
- Stronger individual rights to access electronic medical records and restrict the disclosure of certain information.
- New limitations on the sale of protected health information, as well as marketing and fundraising communications.

## *IFSF - International Forecourt Standards Forum*

- Is a UK-based European organisation which designs standards for ***connecting devices*** on a service station forecourt, such as dispensers, Tank Level Gauges, Price Signs, Car Washes and Outdoor Payment Terminals.
- In recent years additional standards have been added for ***Electronic Funds Transfer***.

Part 1-02 Retails Fuels Data Dictionary
Part 2-01 Communications over Lonworks
Part 2-02 Communications over TCP-IP
Part 2-03 Communications over HTTP REST
Part 3-01 Dispenser Standard
Part 3-02 Price Pole standard
Part 3-03 Tank Level Gauge Standard
Part 3-04 Car Wash Standard
Part 3-05 Card Handling Devices and Pin Pad Standard
Part 3-06 ***Magnetic Card Reader Standard***

Part 3-07 Bank Note Acceptor Standard
Part 3-09 Public Network Server Standard
Part 3-10 Card Handling Server Standard
Part 3-11 Delivery Control Standard
Part 3-12 Network Configuration Manager Standard
Part 3-13 Human Interface Device Standard
Part 3-14 Environmental Monitoring Sensor Standard
Part 3-15 Line Leak Detector Standard
Part 3-16 Customer Operated Payment Terminal (COPT) Standard
Part 3-17 Code Generating Device Standard
Part 3-18 POS to FEP V1 Interface Standard
Part 3-19 POS to EPS V1 Interface Standard
Part 3-20 Host to Host V1 Interface Standard
Part 3-21 Security Standard
Part 3-23 Security Use Cases
Part 3-24 Code Entry Device Standard
Part 3-25 Controller Device Standard
Part 3-26 Vapour Recovery Monitoring System Standard
Part 3-27 FDC POS Interface Standard
Part 3-28 Standard for Issuing EMV Based Fuel Cards
Part 3-29 Key Management Standard
Part 3-30 POS to EPS V3 Interface Standard
Part 3-40 POS to FEP V2 Interface Standard
Part 3-45 POS to FEP V3 (ISO 20022) Interface Standard
Part 3-50 Host to Host V2 Interface Standard
Part 3-60 Mobile Payment to Site Interface Standard
Part 3-70 POS to FDC V2 Interface Standard
Part 4-01 API Specification Design Rules
Part 4-02 API Specification Core Libraries
Part 4-03 API Implementation Guide
Part 4-04 IFSF Design Rules for APIs OAS3.0
Part 4-05 Remote Management and Control API
Part 4-10 Wet Stock Management API
Part 4-15 Pricing API

## *Intellectual Property*

## *Intellectual Property*

- Als geistiges Eigentum wird im Unterschied zum Eigentum an körperlichen Gegenständen (Sachen im Sinne des § 90 BGB) ein ausschliessliches Recht an einem immateriellen Gut, etwa einem Kunstwerk oder einer technischen Erfindung, bezeichnet.
- Das geistige Eigentum umfasst nach dem Willen des Konvents neben dem literarischen und dem künstlerischen Eigentum das Patent- und Markenrecht sowie die verwandten Schutzrechte.
- In historisch-rechtsvergleichender Hinsicht gibt es jedoch kein einheitliches Begriffsverständnis.

## *ISAE 3000*

- Reasonable Assurance
- Service Organisation Independent Assurance Report
- Kann mit dem ***SOC Typ II*** verglichen werden.
- Beschreibung des Systems der internen Kontrollen für die Dienstleistungen aus Sicht der Unterstützung zur Erfüllung der Anforderungen gemäss FINMA Rundschreiben 2008/7 (Outsourcing - Banken), 2018/3 (Outsourcing Banken und Versicherer) und 2008/21 Anhang 3 (Umgang mit elektronischen Kundendaten)

## *ISAE 3402*

- OrSuisse stellt höchste Anforderungen an die Sicherheitskontrollen und die Compliance.

- Der ISAE-3402 Standard (International Standard on Assurance Engagements) ist ein neuer internationaler Standard für Dienstleister.
- Er wurde 2009 vom International Auditing and Assurance Standards Board (IAASB), welches Teil der International Federation of Accountants (IFAC) ist, herausgegeben.
- Der damit verbundene Prüfbericht gibt Auskunft über die internen Kontrollen eines Unternehmens.
- Sie finden detaillierte Informationen zum ISAE 3402 Standard auf der folgenden Internetseite:
    - http://isae3402.com/

  There are two kinds of ISAE 3402 reports:
    - ***Type I***: Documenting a "snapshot" of the organisation's controls
    - ***Type II***: Documenting over a period of time (typically 6 months) showing controls have been managed over time.

## *ISF Standard of Good Practice for Information Security*

- The ISF Standard of Good Practice for Information Security (the Standard) is the most comprehensive information security standard in the world, providing more coverage of topics than the ISO.
- It covers the complete spectrum of information security arrangements that need to be made to keep the business risks associated with information systems within acceptable limits, and presents good practice in practical, clear statements.
- The current version of the standard, updated in 2014, features additional guidance on ***cyber resilience***, securing the ***supply chain***, mobile device security ($B\Psi O\Delta$), data privacy in the ***cloud***, and ***critical infrastructure***.

***The Standard is used by organizations to:***

- Improve resilience against the ever-changing threat landscape.
- Enable compliance with major information-security-related standards.
- Validate information security arrangements with external suppliers.
- Provide a foundation for information risk assessments.
- Form a basis for policies, standards, and procedures.
- Raise information security awareness.
- Form the basis of a detailed or high-level information security assessment.
- Develop or improve information security in response to changing threats.

## *ISO / BCM - Business Continuity Management Standards*


- In addition to the standards for information security in the ISO 27000 series, the International Organization for Standardization also documents important standards for business resilience.
- The ISO BCM standards provide guidance from both a strategy and planning perspective, and from a technical recovery perspective.

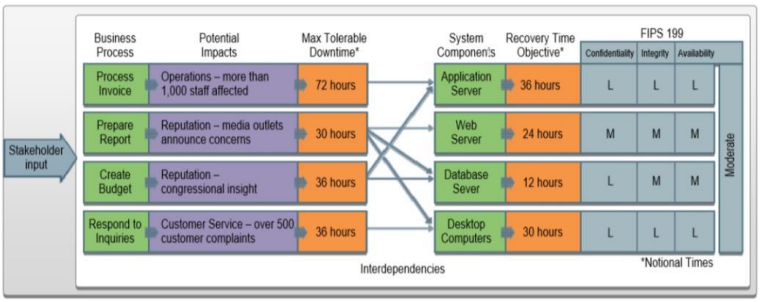
### *BIA - Business Impact Analysis*

- Supporting the mission of the organization.
- Determined wich systems and processes in use are ***critical*** to continued operation.
- **Step 1:** Identify and prioritize critical organization functions.
- Business Impact Analysis (BIA) ist ein unverzichtbarer Bestandteil des Planung einer Organisation für Business Continuity, also der Fortsetzung des Geschäftsbetriebs unter widrigen Umständen.
- Sie enthält eine explorative Komponente zum Aufdecken von Schwachstellen und eine Planungskomponente zum Entwickeln von Strategien zur Risiko-Minimierung.
- Das Ergebnis der Analyse ist der sogenannte ***Business Impact Analysis Report***, der die potenziellen Risiken für die untersuchte Organisation beschreibt.
- Eine der grundlegenden Annahmen bei BIA ist, dass jede Komponente einer Organisation zwar von der Funktion jeder anderen Komponente abhängig ist, aber einige davon weniger verzichtbar sind als andere.

- Letztere erfordern daher mehr finanziellen Aufwand, um Ausfällen vorzubeugen oder sie auszugleichen.
- Ein Unternehmen kann zum Beispiel in der Lage sein, den Geschäftsbetrieb mehr oder weniger normal aufrecht zu erhalten, wenn die Cafeteria geschlossen werden muss.
- Es würde aber gänzlich ins Stocken geraten, wenn das Informationssystem zusammenbricht.
- Als Teil eines Plans für Disaster Recovery wird BIA in der Regel die Kosten identifizieren, die sich durch Ausfälle ergeben. Beispiele hierfür wären:
    - Cashflow-Einbussen
    - Ersetzen von Ausstattung, für das Aufarbeiten des Arbeitsrückstands anfallende Gehälter, Gewinneinbussen und dergleichen.
- Ein BIA-Bericht quantifiziert die Bedeutung von geschäftlichen Komponenten und schlägt eine angemessene Massnahmen-Allokation zu deren Schutz vor.
- Die möglichen Ausfälle werden dabei im Hinblick auf ihre Auswirkungen auf Sicherheit, Finanzen, Marketing, Compliance und Qualitätssicherung bewertet.
- Wo es möglich ist, wird die Auswirkung für Vergleichszwecke in Geldeinheiten ausgedrückt.
- Ein Unternehmen kann zum Beispiel nach einem schweren Ausfall dreimal so viel für Marketing aufwenden müssen wie normalerweise, um das Vertrauen seiner Kunden zurück zu gewinnen.
- Die BIA sollte auch die langfristigen Auswirkungen eines Desasters ermitteln und dabei helfen, Prioritäten, Recovery-Strategien, Zeitaufwände und Ressourcenanforderungen zu bestimmen.
- The BIA is an important first step in BCM because the analysis identifies the ***recovery point objective (RPO)*** and ***recovery time objective (RTO)*** of each system or business process used by the organization.

***Recovery Point Objective (RPO)***
- RPO identifies the maximum tolerable timeframe in which data might be lost.
- This determines how much data the system can lose and defines the backup schedule.

***Recovery Time Objective (RTO)***
- RTO identifies the duration of acceptable downtime.
- This determines how quickly the system or business process must recover and defines recovery priority.
- BIA encourages active involvement and input from business leaders, IT, and security.
- Asset owners contribute by describing the business value of their systems.
- IT and security then transform this information into a prioritized plan to recover business processes and systems based on the context of their value and impact on business operations.




***The eight BIA steps are:***
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without theses resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

***BCP - Business Continuity Planning***

- A BCP is a ***corrective control***.
- BCP involves assessing the risks to organizational processes and creating ***policies***, ***plans***, and ***procedures*** to minimize the impact those risks might have on the organization if they were to occur.
- BCP is used to maintain the continuous operation of a business in the event of an emergency.
- The goal of the BCP process is to ensure that your ***RTOs*** are less than your ***MTDs***, resulting in a situation in which a function should never be unavailable beyond the maximum tolerable downtime (MTD).
- The BCP is concerned with monitoring ***threat activity***.
- Focuses on sustaining an organization's business functions ***during and after a disruption***.
- Contains ***strategy documents*** that provide detailed procedures that ensure critical business functions are maintained.
- Provides ***procedures*** for sustaining essential business operations ***while recovering*** from a significant disruption.
- Test your BCP at least ***once a year***.

***Principals:***

- ❑ The ***safety of people*** must always come before the organization's business goals.
- ❑ Depending on the nature of the ***cloud service***, the vendor's own business continuity arrangements may have a critical impact on your organization's business as well!
- ❑ Business continuity is ***everyone's responsibility***.
- ❑ ***Base question***: "If we need to rebuild the organizations today in a completely new location without access to any of our computer or files, what records would you need?"

**BCP contains the four main steps:**

- Project scope and planning
- Business impact assessment (BIA)
- Continuity planning
- Approval and implementation

**Executive succession planning**

- Organizations must ensure that there is ***always an executive is available*** to make decisions during a disaster.
- Executive succession planning determines an organization's line of succession.
- Executives may become unavailable due to a variety of disasters, ranging from injury and loss of life to strikes, travel restrictions, and medical quarantines.

## *ISO-IEC - International Organization for Standardization*

Link: www.iso.org

- Change management control is a mandatory element for some ***security assurance requirements (SARs)*** in the ***ISO Common Criteria***.

***ISO-IEC 8583***

- ???

***ISO-IEC 9001 | Grundsätze für Massnahmen zum Qualitätsmanagement***

- Qualitätsmanagement

***Sieben Grundsätze des Qualitätsmanagements:***

1. Kundenorientierung
2. Verantwortlichkeit der Führung
3. Einbeziehung der beteiligten Personen
4. Prozessorientierter Ansatz und (früher eigenständig) Systemorientierter Managementansatz
5. Kontinuierliche Verbesserung
6. Sachbezogener Entscheidungsfindungsansatz
7. Lieferantenbeziehungen zum gegenseitigen Nutzen

***ISO-IEC 12207 | Software Life Cycle Processes***

- Dient der besseren Verständigung bei Verhandlungen und Verträgen zwischen Kunden und Lieferanten von Projekten zur Entwicklung, dem Betrieb und der Wartung von Softwaresystemen.
- Dieser Standard ist nicht anwendbar beim Kauf von Standardsoftwarepaketen.

***ISO-IEC 14001 | ???***

***ISO-IEC 15489 | Records Management***

***ISO 15489-1:2001 General***

***ISO 15489-2:2001 Guidelines***

***ISO-IEC 17025 | Accreditation for Forensic Lab***

- ???

***ISO-IEC 17799 | ???***

***ISO-IEC 18028-1 | NETWORK SECURITY MANAGEMENT***

***ISO-IEC 20000 | INFORMATION TECHNOLOGY -- SERVICE MANAGEMENT***

- Die ***ISO 20000*** ist auf IT-Unternehmen und -Abteilungen ausgerichtet.
- Entscheidend für die Zertifizierung sind Definition und Nachprüfbarkeit aller Prozesse.
- Der Auditor schaut sich anhand der Dokumentationen an, auf welche Weise Störungen erfasst, qualifiziert und weitergegeben werden.

***ISO-IEC 22301 | BUSINESS CONTINUITY MANAGEMENT SYSTEMS***

- Standard for ***Business Continuity Management (BCM)***

***ISO-IEC 22301:2012 | BUSINESS CONTINUITY MANAGEMENT SYSTEMS***

- Specifies requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents when (or should) they arise.
- The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size, and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

***ISO-IEC 22313 : | GUIDELINES FOR INFORMATION AND COMMUNICATIONS***

- Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.

***ISO-IEC 24762:2008 | GUIDELINES FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY DISASTER RECOVERY SERVICES***

- Provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management, applicable to both "in-house" and "outsourced" ICT DR service providers of physical facilities and services.

***ISO/IEC 24762:2008 specifies:***

- The requirements for implementing, operating, monitoring, and maintaining ICT DR services and facilities.
- The capabilities outsourced ICT DR service providers should possess and the practices they should follow, to provide basic secure operating environments and facilitate organizations' recovery efforts
- The guidance for selection of recovery site.
- The guidance for ICT DR service providers to continuously improve their ICT DR services.

***ISO-IEC 27000 Family of Standards***


***ISO-IEC 27001 | Information Security Management***

Link : https://www.iso.org/isoiec-27001-information-security.html

- The ISO/IEC 27000 family of standards helps organizations ***keep information assets secure***.
- Using this family of standards will help your organization manage the security of assets such as ***financial information***, ***intellectual property***, ***employee details*** or information entrusted to you by third parties.
- ISO/IEC 27001 is the best-known standard in the family providing requirements for an ***information security management system (ISMS)***.

***ISO-IEC 27001:2005 | Information Security Management***

- Standard for Information Security Management (ISM).

***ISO-IEC 27001:2013 | Information Security Management***

- Ist der globale Standard von Information Security Management Systems (ISMS).
- Es wird ein Rahmen für die Einrichtung, die Implementierung, die Überprüfung und die Verbesserung von ISMS geboten.

***The standard includes ten clauses, plus an annex, which cover:***

1. Scope of the standard.
2. How the document is referenced.
3. Reuse of the terms and definitions in ISO/IEC 27000.
4. Organizational context and stakeholders.
5. Information security leadership and high-level support for policy.
6. Planning an information security management system; risk assessment; risk treatment.
7. Supporting an information security management system.
8. Making an information security management system operational.
9. Reviewing the system's performance.
10. Corrective action.

Annex A: List of controls and their objectives.

***ISO-IEC 27002 | Audit Controls***

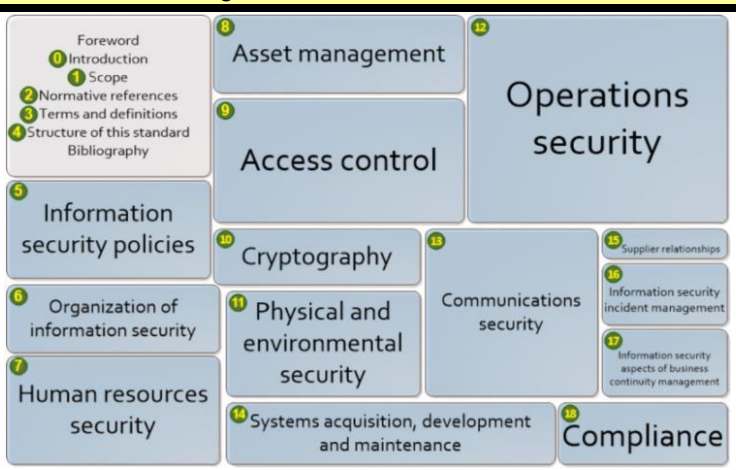
- The ISO/IEC 27000-series standards are descended from a corporate security standard donated by Shell to an ***UK government initiative in the early 1990s***.
- The Shell standard was developed into ***British Standard BS 7799*** in the mid-1990s and was adopted as ISO/IEC 17799 in 2000.
- The ISO/IEC standard was revised in 2005, and renumbered ISO/IEC 27002 in 2007 to align with the other ISO/IEC 27000-series standards. It was revised again in 2013.

***ISO-IEC 27002:2013 | Code of practice for information security controls***

- See also : https://www.iso27001security.com/html/27002.html
- This catalog provides guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s).
- It is designed to be used by organizations that intend to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001, implement commonly accepted information security controls, and develop their own information security management guidelines.

Eine wirkungsvolle Informationssicherheit verringert Risiken durch Schutz der Organisation vor Bedrohungen und Schwachstellen und vermindert dadurch die Auswirkungen auf organisationseigene Werte.

Die Einführung einer Reihe geeigneter Sicherheitsmassnahmen, darunter ***Richtlinien***, ***Prozesse***, ***Verfahren***, ***Organisationsstrukturen*** sowie ***Software***- und ***Hardwarefunktionen***, sorgt für Informationssicherheit.




***The 14 Chapters of 27002 :2013***

5 Information security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

***Die 14 Abschnitte von 27002 :2013***

1. Sicherheitsleitlinie
2. Organisation der Informationssicherheit
3. Personalsicherheit
4. Management der organisationseigenen Werten
5. Zugriffskontrolle
6. Kryptographie
7. Schutz vor physischem Zugang & Umwelteinflüssen
8. Betriebssicherheit
9. Sicherheit in der Kommunikation
10. Anschaffung, Entwicklung & Instandhaltung
11. Lieferantenbeziehungen
12. Management von Informationssicherheitsvorfällen
13. Informationssicherheitsaspekte des BCM
14. Richtlinienkonformität

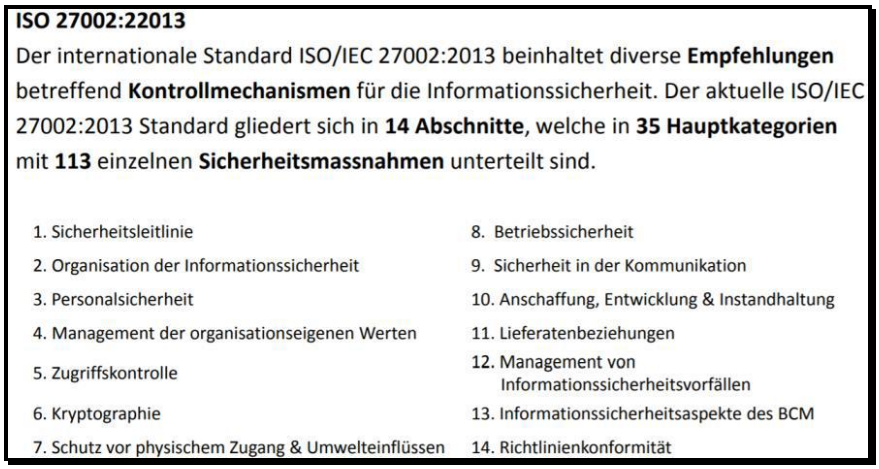



**Figure 1: ISO-IEC 27002:2013**

***ISO 27002 5.1 Information security policy (ISO 27001 Annex A A.5.1)***

- To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- A CISO who attempts to run an information security program without management will have difficulty implementing policies and processes to impact security behaviors in the organization.

***ISO-IEC 27003:2017 | Information security management system implementation guidance***

- The guidance in this document focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005.
- It describes the process of ISMS specification and design from inception to the production of implementation plans.
- It describes the process of obtaining management approval to implement an ISMS, outlines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project resulting in a final ISMS project implementation plan.

***ISO-IEC 27004:2009 | Information security management - Measurement***

- This document provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls, or groups of controls, as specified in ISO/IEC 27001. ISO/IEC 27004:2009 is applicable to all types and sizes of organization.

***ISO-IEC 27005 Risk Management***

- ISO 27005 provides information guidelines designed to provide broadly acceptable guidance for information security risk management.
- The standard applies globally, supports wide adoption across industries, and maps directly to the strategy and recommendations outlined in ISO 27001.
- The ISO 27005 risk management workflow directs a structured sequence of steps to manage information security risks for a process, a system, or an enterprise.

***ISO 27005 Risk Management Workflow***

1. Design controls based on risks clearly understood and measured (as much as possible) given existing threats that could potentially exploit vulnerabilities to organizational assets.
2. Systematic deployment of controls to reduce risks to an acceptable level of residual risk after approval by business leadership.
3. Manage controls to maintain an acceptable level of mitigation.
4. Provide ongoing analysis of controls to confirm continued effectiveness in light of changing operational conditions.

***Organizations should ensure that the following are continually monitored:***

- New assets that have been included in the risk management scope
- Necessary modification of asset values (e.g. due to changed business requirements)

- New threats that could be active both outside and inside the organization--and that have not been assessed
- Possibility that new or increased vulnerabilities could allow threats to exploit these different or changed vulnerabilities
- Identified vulnerabilities to determine those becoming exposed to new or re-emerging threats
- Increased impact or consequences of assessed threats, vulnerabilities, and risks in aggregation that result in an unacceptable level of risk
- Information security incidents

***Risk Communication should be carried out in order to achieve the following:***

- To provide assurance of the outcome of the organization's risk management
- To collect risk information
- To share the results from the risk assessment and present the risk treatment plan
- To avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision-makers and stakeholders
- To support decision-making
- To obtain new information security knowledge
- To coordinate with other parties and plan responses to reduce consequences of any incident
- To give decision-makers and stakeholders a sense of responsibility about risks
    - To improve awareness

***ISO-IEC 27005:2011 | Information security risk management***

- This document outlines the standards and guidelines for information security risk management.
- It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
- Knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011.
- ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) that intend to manage risks that could compromise the organization's information security.

***ISO-IEC 27017:2015 CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS***

- Gives guidelines for information security controls applicable to the provision and use of cloud services by providing :
  - additional implementation guidance for relevant controls specified in ISO/IEC 27002;
  - additional controls with implementation guidance

***ISO-IEC 27031 | BUSINESS CONTINUITY STANDARD***

- Suggests a structure or framework (a coherent set or suite of methods and processes) for any organization – private, governmental, and non-governmental.
- Identifies and specifies all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization's ISMS, helping to ensure business continuity.
- Enables an organization to measure its ICT continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

***ISO-IEC 27033 | NETWORK SECURITY***

***ISO/IEC 27033-1:2009 | NETWORK SECURITY OVERVIEW AND CONCEPTS***

***ISO/IEC 27033-2:2012 | GUIDELINES FOR THE DESIGN AND IMPLEMENTATION OF NETWORK SECURITY***

***ISO/IEC 27033-3:2010 | REFERENCE NETWORKING SCENARIOS - THREATS, DESIGN TECHNIQUES AND CONTOL ISSUES***

***ISO/IEC 27033-4:2014 | SECURING COMMUNICATIONS BETWEEN NETWORKS USING SECURITY GATEWAYS***

***ISO/IEC 27033-5:2013 | SECURING COMMUNICATIONS ACROSS NETWORKS USING VPN***

***ISO/IEC 27033-6 | SECURING WIRELESS IP NETWORK ACCESS***

***ISO-IEC 27037 | GUIDELINES FOR IDENTIFICATION, COLLECTION, ACQUISITION AND PRESERVATION OF DIGITAL EVIDENCE***

- Diese Norm enthält Leitlinien zur Identifizierung, Sammlung, Erfassung, Beschaffung, Handhabung und zum Schutz respektive zur Erhaltung digitaler forensischer Beweise.
- Gemeint sind damit digitale Daten, die von Beweiskraft sein können und somit für die Verwendung vor Gericht geeignet sind.
- Diese Norm betrifft die erstmalige Erfassung digitaler Beweismittel.

***ISO-IEC 27041 | GUIDANCE ON ASSURING SUITABILITY AND ADEQUACY OF INCIDENT INVESTIGATIVE METHOD***

- Sie bietet Leitlinien zu den Sicherheitsaspekten der digitalen Forensik.
- Mit diesen lässt sich etwa sicherstellen, dass die geeigneten Methoden und Werkzeuge ordnungsgemäss eingesetzt werden.

***ISO-IEC 27042 | GUIDELINES FOR THE ANALYSIS AND INTERPRETATION OF DIGITAL EVIDENCE***

- Dieser Standard deckt ab, was nach der Sammlung digitaler Beweise passiert.
- Sie beschreibt, wie diese sorgfältig zu analysieren und genau zu interpretieren sind.

***ISO-IEC 27043 | INCIDENT INVESTIGATION PRINCIPLES AND PROCESSES***

- Diese Norm liefert Leitlinien für gängige Untersuchungsverfahren von Vorfällen, bei denen digitale Beweismittel eine Rolle spielen.

***ISO-IEC 27050 | CODE OF PRACTICE FOR ELECTRONIC DISCOVERY***

- Dieser Standard besteht aus vier Teilen.
- Er beleuchtet alle Aspekte der elektronischen Entdeckung (Electronic Discovery) und deckt damit ungefähr ab, was die vorgängig erwähnten Normen schon adressieren.

***ISO-IEC 29115 | Entity Authentication Assurance***

- See also OpenID Connect.

***ISO-IEC 29990 | LEARNING SERVICES FOR NON-FORMAL EDUCATION AND TRAINING***

- Die ISO 29990:2010 wurde im September 2010 als ISO-Norm veröffentlicht und im Dezember 2010 als DIN-Norm DIN ISO 29990 „Lerndienstleistungen für die Aus- und Weiterbildung - Grundlegende Anforderungen an Dienstleister“ übernommen.
- Die Internationale Norm ist ein Servicestandard für Lerndienstleistungen und gleichzeitig ein Qualitätsmanagementsystem für ***Lerndienstleister*** in der Aus- und Weiterbildung.
- Das Ziel der ISO 29990 ist die Schaffung eines allgemeinen Qualitätsmodells für die berufliche Praxis und Leistungserstellung sowie einer gemeinsamen Referenz für Lerndienstleister und ihre Kunden zur Planung, Entwicklung und Durchführung von Aus- und Weiterbildung sowie zur Förderung von Entwicklung.
- Die Norm richtet den Fokus auf den Lernenden, die Lernergebnisse, die Lerndienstleistung und die Kompetenz des Lerndienstleisters.
- Organisationen und Individuen sollen durch die Internationale Norm bei der Auswahl eines geeigneten Lerndienstleisters unterstützt werden, der den Bedürfnissen und Erwartungen an die Entwicklung von Kompetenzen und Fähigkeiten entspricht.

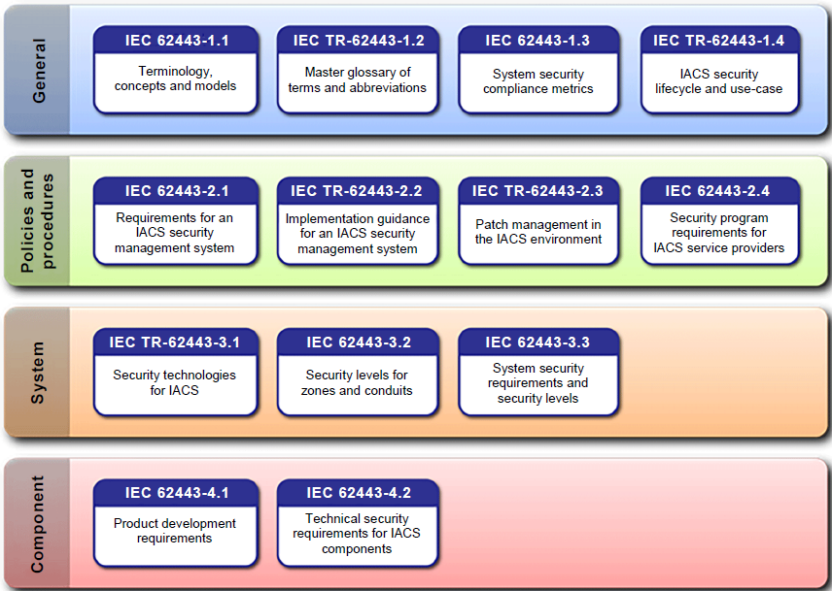
*Source: Wikipedia*

***ISO-IEC 31000 | Risk Management***

- ISO 31000 is a framework that provides ***generic guidelines for enterprise risk management*** with a universally recognized risk paradigm for practitioners and companies.

***ISO-IEC 62443 | Industrial communication networks***

- Ganzheitlichen Ansatz für Industrial Security im Produktions- und Automatisierungsbereich.




## *ITIL - Information Technology Infrastructure Library*

- ITIL is a public framework that describes ***best practices*** in IT service management.
- ITIL provides guidance on what should be done in order to offer the clients of an IT organization adequate IT services to support their business needs.
- See also: ***Risk Management***

***Benefits:***

- Increased user and customer satisfaction with IT services.
- Improved service availability, directly leading to increased business profits and revenue.
- Financial savings from reduced rework, lost time, improved resource management and usage.
- Improved time to market for new products and services.
- Improved decision-making and optimized risk.

## *ITSEC - Technology Security Evaluation and Criteria*

- Replaced by ***Common Citeria***.
- Represents an initial attempt to create security evaluation criteria in ***Europe***.
- It was developed as an ***alternative to the TCSEC*** guidelines.
- Addresses ***integrity, availability*** and ***confidentiality***.

## *KAG - Kollektivanlagengesetz*

- Dieses Gesetz bezweckt den Schutz der Anlegerinnen und Anleger sowie die Transparenz und die Funktionsfähigkeit des Marktes für kollektive Kapitalanlagen.

## *Licensing*

Four common types of software license agreements are in use today:

***Contractual license agreements***

- Use a written contract between the software vendor and the customer, outlining the responsibilites of each.
- These agreements are commonly found for high-priced and/or highly specialized software packages.

***Shrink-wrap license agreements***

- Are written on the doutside oft he software packaging.
- They connonly include a clause statin that you acknowledge agreement to the terms oft he conrract simply by breaking the shrink-wrap seal in the package.

***Click-through license agreements***

- Are becoming more connonplace than shrink-wrap agreements.
- In this type of agreement, the contract terms are either written on the software box or included in the software documentation.
- During the installation process, you are required to click a button indicating that you have read the terms oft he agreement and agree to abide by them.
- This adds an active consent to the process, ensuring that the individual is aware oft he agreement's existence prior to installation.

***Cloud services license agreements***

- Take cklick-through agreements to the extreme.
- Most cloud services do not require any form of written agreement and simply flash legal terms on the screen for review.
- In some cases, they may simply provide a link to legal terms ans a check box for users to confirm that they read and agree to the terms.
- Most users, in theird excitement to access a new service, simply click their way through the agreement without reading it and may unwittingly bind their entire organization to onerous terms and conditions.

## *MiFID II*

- Banks
- Conduct of business and organisational requirements for investment firms;
- authorisation requirements for regulated markets;
- regulatory reporting to avoid market abuse;
- trade transparency obligation for shares; and
- rules on the admission of financial instruments to trading.

## *Montreal Protocol*

- Refilling a Halon flooding system in the event that Halon is fully discharged, can be done by ordering a Non-Hydrochlorofluorocarbon compound from the manufacturer.

## *NERC - North American Electric Reliability Corporation*

- https://www.nerc.com
- NERC's compliance efforts are comprised of key activities such as:
    - Compliance Monitoring
    - Compliance Enforcement

## *NISTIR 8144 Assessing Threats to Mobile Devices & Infrastructure*

- https://csrc.nist.gov/publications/detail/nistir/8144/draft

## *NSAI - National Standards Authority of Ireland*

***EN 50159 | Railway applications***

- Communication, signalling and processing systems
- Safety-related communication in transmission systems

***CONTENTS***

- Reference architecture
- Threats to the transmission system
- Classification of transmission systems
- General aspects of classification
- Criteria for the classification of transmission systems
- Relationship between transmission systems and the threats
- Requirements for defences
- General requirements

- Specific defences
- Applicability of defences
- Threats
- A possible approach for building a safety case
- Choice and use of safety codes and cryptographic techniques
- Safety code
- Length of safety code
- Communication between safety-related and non safety-related applications

## *OEP - Occupant Emergency Plan*

- Many organizations adopt occupant emergency plans (OEPs) to guide and assist with sustaining personnel safety in the wake of a disaster.
- The OEP provides guidance on how to minimize threats to life, prevent injury, manage duress, handle travel, provide for safety monitoring, and protect property from damage in the event of a destructive physical event.
- The OEP does not address IT issues for business continuity, just personnel and general property.

## *OPC UA - Open Platform Communications United Architecture*

- Is a data exchange standard for industrial communication (machine-to-machine or PC-to-machine communication).

## *PCI DSS - Payment Card Industry Data Security Standard*

Link: www.pcisecuritystandards.org

Actual Version: **V3.2.1**

- Is a collection of requirements for improving the ***security of electronic payment transactions***.
- Requires that at least annually a ***web application vulnerability scan*** is performed.
- Doesn't allow organizations to ***outsource their responsibilities***.
- Any organization that sores credit card information must ***report any incident*** in which the disclosure of such information occurred.
- Regulations regarding: ***Log Management***

**The 12 main requirements:**

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regulary update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Maintain a policy that addresses information security for all personnel.
11. Track and monitor all access to network resources and cardholder data.
12. Regulary test security systems and processes.

**Die 12 Kapitel Deutsch:**

1. Installation und Pflege einer Firewall-Konfiguration, die Karteninhaberdaten schützt.
2. Keine von Lieferanten bereitgestellten Standardwerte/Standardeinstellungen für Systempasswörter und andere Sicherheitsparameter verwenden.
3. Gespeicherte Karteninhaberdaten schützen.
   Einbezogen werden zusätzlich Richtlinien, Methoden und Prozesse zur Aufbewahrung und Entsorgung von Daten, um sicherzustellen, dass sie aktuell und akkurat sind. Einige Daten

sollten nie gespeichert werden, wie z.B. der Inhalt des Magnetstreifens, die Kartenprüfnummer oder die persönliche Identifikationsnummer. Zusätzlich sollte verschlüsselt werden.

4. Übertragung der Karteninhaberdaten in offenen, öffentlichen Netzwerken verschlüsseln.
   Beispiele hierfür sind das Internet, drahtlose Technologien wie Bluetooth, GPRS und Satellitenkommunikation.
5. Antivirensoftware oder -programme verwenden und regelmässig aktualisieren.
   Systeme müssen vor Malware geschützt und Antivirenprogramme regelmässig aktualisiert werden, um Viren, Würmer und Trojaner abzuwehren. Dazu sollten Antivirentools implementiert, gepflegt und ausgeführt werden, wenn es notwendig ist.
6. Sichere Systeme und Anwendungen entwickeln und pflegen.
   Nach Updates suchen, um Software immer auf dem neuesten Stand zu halten. Nur dann ist ein Unternehmen vor aktuellen Datenschutzverletzungen weitgehend geschützt.
7. Den Zugang zu Karteninhaberdaten nach geschäftlichen Erfordernissen einschränken.
   Um diese Anforderungen zu gewährleisten benötigt man sowohl Systeme als auch Prozesse: WER hat Zugang zu diesen Daten und WARUM braucht er den Zugang. Nur die Personen sollten einen Zugang bekommen, die die Daten benötigen, um ihre Arbeit tun zu können.
8. Jeder Person mit Computerzugang eine eindeutige ID zuweisen.
   Das bedeutet sicherzustellen, dass Sie immer wissen, wer Zugang zu was hat. So sorgen Sie dafür, dass nur Personen mit der entsprechenden Berechtigung auf bestimmte Systeme und Komponenten zugreifen können. Eine Möglichkeit, eine ordnungsgemäße Autorisierung zu gewährleisten, ist die Zwei-Faktor-Authentifizierung bei der beispielsweise Smartcards, Token oder Biometrie verwendet werden, um den Sicherheitslevel zu erhöhen.
9. Physischen Zugang zu Karteninhaberdaten beschränken.
   Ein Datenverlust ist auch durch physische Sicherheitsverletzungen möglich. Daher sollte man sorgfältig darauf achten, dass der physische Zugang zu den betreffenden Datensätzen eingeschränkt und überwacht wird. Der Zutritt zu Serverräumen und Rechenzentren sollte begrenzt, Medien vernichtet und Datenträger vor Manipulation geschützt und überwacht werden.
10. Den Zugang zu Netzwerkressourcen und Karteninhaberdaten protokollieren und überwachen.
    Nur wenn man alle Zugangsmöglichkeiten protokolliert, erkennt man Risiken für Datenschutzverletzungen und kann sie minimieren. Dabei helfen sichere und kontrollierte Audit Trails, um alle Aktionen einzelner Benutzer zu protokollieren, wie z.B. den Zugang zu Daten, Berechtigungen, ungültige Anmeldeversuche und Änderungen an Authentifizierungsmechanismen, wie das Löschen von Objekten. Diese Protokolle sollte man regelmäßig überprüfen.
11. Sicherheitssysteme und -prozesse regelmässig überprüfen.
    Penetrationstests sind ein wichtiges Tool des IT-Sicherheits-Teams und sollten regelmäßig jährlich sowie nach allen wesentlichen Änderungen am Netzwerk durchgeführt werden. Dazu gehören Schwachstellen-Scans, Netzwerk-Topologie und Pflege der Firewall.
12. Eine Richtlinie pflegen, die sich mit der Informationssicherheit für Mitarbeiter und Auftragnehmer befasst.
    Sie sollte zweimal jährlich überprüft und aktualisiert werden. Dabei sollte man eine Risikobewertung durchführen, um Bedrohungen oder Schwachstellen zu identifizieren und einen Incident Response Plan aufstellen. Dazu kommen laufende Schulungen der Mitarbeiter, um neue Sicherheitsprotokolle zeitnah zu kommunizieren.

Es gibt ***vier*** verschiedene ***PCI-Compliance-Level***. Iin der Regel hängt die Einstufung Ihres Unternehmens davon ab, wie viele Kreditkartentransaktionen es über einen Zeitraum von 12 Monaten abwickelt.

| | TRIFFT ZU AUF | ANFORDERUNGEN |
|---|---|---|
| LEVEL 1 | 1 Organisationen, die jährlich mehr als 6 Millionen Transaktionen abwickeln; oder<br>2 Eine Datenschutzverletzung erfahren haben; oder<br>3 Werden von allen Kartenverbänden (Visa, Mastercard usw.) als Level 1 eingestuft | 1 Jährlicher Konformitätsbericht (ROC) durch einen qualifizierten Sicherheitsprüfer (Qualified Security Assessor) (QSA) - auch bekannt als Level 1-Standortprüfung oder interne Prüfung, wenn einer der Unternehmensleiter unterschreibt<br>2 Vierteljährlicher Netzwerk-Scan durch anerkannten Scan-Anbieter (Approved Scan Vendor) ASV<br>3 Konformitätsbescheinigung (AOC) für Standortprüfungen - es gibt bestimmte Formulare für Händler und Service-Anbieter |
| LEVEL 2 | Organisationen, die jährlich zwischen 1 und 6 Millionen Transaktionen abwickeln. | 1 Jährlicher PCI DSS Selbstbewertungsfragebogen (Self-Assessment Questionnaire) SAQ - in der Tabelle unten werden die 9 bestehenden SAQ-Typen kurz beschrieben<br>2 Vierteljährlicher Netzwerk-Scan durch anerkannten Scan-Anbieter (Approved Scan Vendor) (ASV)<br>3 Konformitätsbescheinigung ( AOC ) - es gibt ein entsprechendes Formular für jeden der 9 Selbtbewertungsfragebögen |
| LEVEL 3 | 1 Organisationen, die jährlich insgesamt **zwischen 20.000 und einer Million Transaktionen abwickeln**<br>2 Organisationen, die jährlich insgesamt **weniger als eine Million Transaktionen abwickeln** | |
| LEVEL 4 | 1 Organisationen, die jährlich insgesamt **weniger als 20.000 Transaktionen abwickeln; oder**<br>2 Organisationen, die jährlich **insgesamt bis zu einer Million Transaktionen abwickeln** | |

## *PSP - Personensicherheitsüberprüfung*

- See also: PSP 10 / PSP 11 / PSP 12
- Source: https://www.vbs.admin.ch
- Die Personensicherheitsprüfung (PSP) stellt eine präventive Massnahme zur Wahrung der inneren Sicherheit der Schweiz sowie zum Schutz ihrer Bevölkerung dar.
- Sie erfolgt bei Personen in sicherheitsempfindlichen Funktionen mit Zugang zu klassifizierten Informationen, Materialien oder Anlagen.
- Bei Angehörigen der Armee kann bezüglich Hinderungsgründe zur Überlassung der persönlichen Waffe ebenfalls eine PSP durchgeführt werden.
- Die PSP soll einen ***Missbrauch im klassifizierten Bereich*** sowie bezüglich der ***persönlichen Waffe*** verhindern, indem allfällige, von Personen ausgehende Risiken erkannt und auf ein Minimum reduziert werden.

**Grundsicherheitsprüfung (PSPV Art. 10 Abs. 1 Bst. a, b, d)**

- Im Rahmen der Grundsicherheitsprüfung werden verschiedene Register und Datenbanken abgefragt, wie beispielsweise das ***schweizerische Strafregister***.
- Bezieht sich auf die vergangenen ***5 Jahre***.

**Erweiterte Sicherheitsprüfung (PSPV Art. 11 Abs. 1 Bst. a - h)**

- Bei der erweiterten Personensicherheitsprüfung werden zusätzliche Informationen eingeholt. So werden hier auch die ***Betreibungsämter*** Ihrer Wohnorte angefragt.
- Bezieht sich auf die vergangenen ***10 Jahre***.

**Erweiterte Sicherheitsprüfung mit Befragung (PSPV Art. 12 Abs. 1 Bst. a, b)**

- Die erweiterte Personensicherheitsprüfung mit Befragung besteht ergänzend aus einem ***persönlichen Gespräch***, zu welchem die zu prüfende Person eingeladen wird.
- Dieses dient grundsätzlich dazu, die Person kennen zu lernen und sich ein besseres Bild von ihr machen zu können.

## *PTES - Penetration Testing Execution Standard*

- See: http://www.pentest-standard.org

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical gude can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

## *SCHUBAN - Schutzbedarfsanalyse*

- Mit Hilfe der Schutzbedarfsanalyse (SCHUBAN) wird untersucht, ob die minimalen Sicherheits-standards des Grundschutzes ausreichen oder ob ein ***erhöhter Schutzbedarf (ES)*** oder ***sehr hoher Schutzbedarf (SHS)*** vorliegt.
- Der ***Grundschutz (GS)*** gilt für alle Systeme, Services und Daten und definiert die auf jeden Fall einzuhaltenden Mindestanforderungen an die Informationssicherheit.
  Die entsprechenden Schutzmassnahmen müssen immer und überall umgesetzt werden.

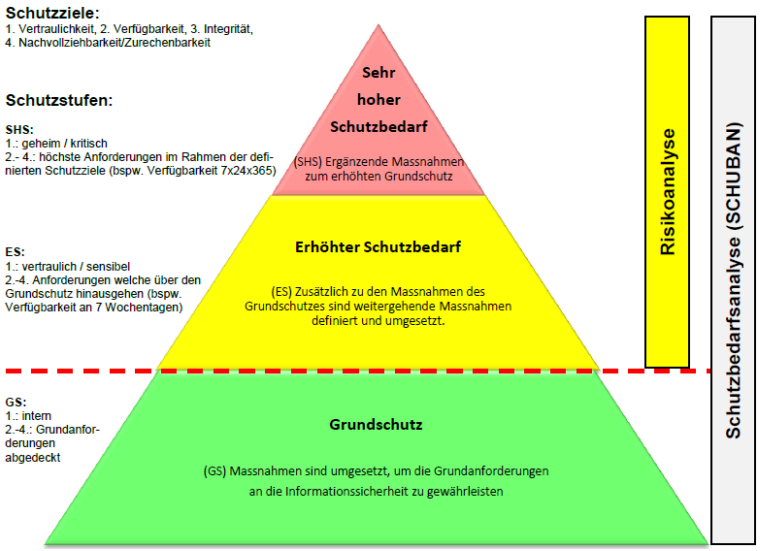
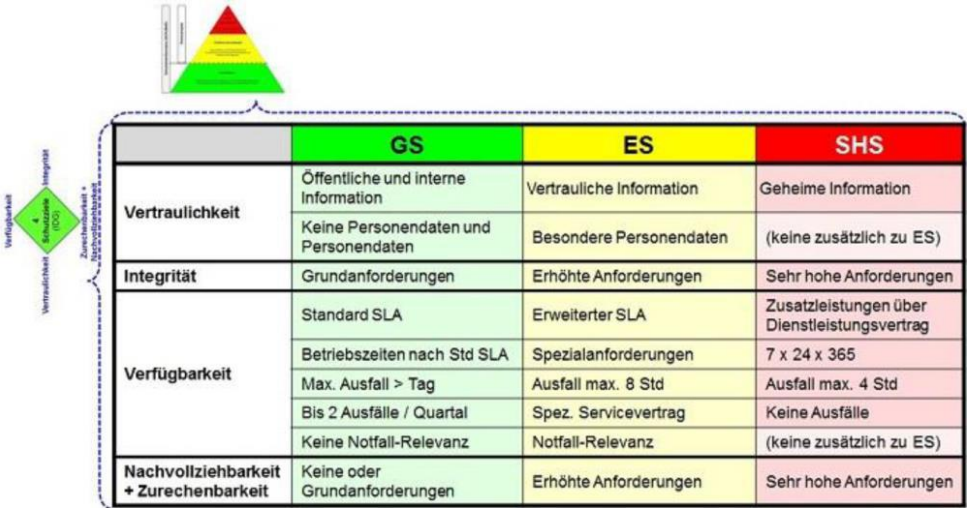



**Abbildung 1: Schutzbedarfsstufen, SCHUBAN und Risikoanalyse**



| | GS | ES | SHS |
|---|---|---|---|
| Vertraulichkeit | Öffentliche und interne Information | Vertrauliche Information | Geheime Information |
| | Keine Personendaten und Personendaten | Besondere Personendaten | (keine zusätzlich zu ES) |
| Integrität | Grundanforderungen | Erhöhte Anforderungen | Sehr hohe Anforderungen |
| Verfügbarkeit | Standard SLA | Erweiterter SLA | Zusatzleistungen über Dienstleistungsvertrag |
| | Betriebszeiten nach Std SLA | Spezialanforderungen | 7 x 24 x 365 |
| | Max. Ausfall > Tag | Ausfall max. 8 Std | Ausfall max. 4 Std |
| | Bis 2 Ausfälle / Quartal | Spez. Servicevertrag | Keine Ausfälle |
| | Keine Notfall-Relevanz | Notfall-Relevanz | (keine zusätzlich zu ES) |
| Nachvollziehbarkeit + Zurechenbarkeit | Keine oder Grundanforderungen | Erhöhte Anforderungen | Sehr hohe Anforderungen |

***Risikotypen:***
R01 Höhere Gewalt
R02 Unfallartige Ereignisse oder Defekte
R03 Menschliches Fehlverhalten und/oder unbeabsichtigte Weitergabe von Informationen
R04 Organisatorische Mängel und/oder Mängel in Beschaffung, Bereitstellung und Entsorgung
R05 Verstoss gegen rechtliche, vertragliche oder interne Bestimmungen
R06 Vorsätzliche Handlungen
R07 Ausfall von Personen

***Besondere Personendaten***
Es gelten strengere Regeln, wenn besondere Personendaten bearbeitet werden.

Als besondere Personendaten gelten einerseits Informationen, bei denen wegen ihrer Bedeutung, wegen der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere ***Gefahr einer Persönlichkeitsverletzung*** besteht (z.B. durch Stigmatisierung oder Diskriminierung), und anderseits Persönlichkeitsprofile.

In die erste Kategorie fallen insbesondere Informationen über ***religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten Gesundheit, Intimsphäre,***

***Rassenzugehörigkeit oder ethnische Herkunft Sozialhilfemassnahmen administrative und strafrechtliche Verfolgungen oder Sanktionen***.

***Daten über Einkommens- oder Vermögensverhältnisse*** sind keine besondere Personendaten; sie können aber Gegenstand besonderer Geheimhaltungspflichten sein (im Bereich des öffentlichen Rechts z.B. Steuergeheimnis, im privatrechtlichen Bereich z.B. Bankkundengeheimnis).

Zur zweiten Kategorie besonderer Personendaten gehören Zusammenstellungen von Informationen, die ***eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben*** - also das, was bisher im Datenschutzgesetz als ***Persönlichkeitsprofil*** bezeichnet wurde.

An die Zulässigkeit der Bearbeitung von besonderen Personendaten stellen die (Informations- und) Datenschutzgesetze in der Regel höhere Anforderungen — was hier unter «Grundsätze des Datenschutzes» noch vertieft wird.

***Audioaufnahmen***
Heimliche Audioaufnahmen unterliegen dem ***Beweisverwertungsverbot*** und sind ausserdem strafbar.

Schweizerisches StGB
Art. 179bis Abhören und Aufnehmen fremder Gespräche
Art. 201 Verletzung der Vertraulichkeit des Wortes.

Fernmeldegesetz (FMG)
Art. 50 Unbefugtes Verwerten von Informationen
Art. 13a1 Datenbearbeitung

## *SOC-1*

- Covers only internal controls over financial reporting.

## *SOC-2*

- SOC-2 assures clients we use systems to protect their data.
- It audits ***security***, ***availability***, ***process integrity***, ***privacy*** and ***confidentiality***.

## *SOC-3 - Service Organization Control 3*

- Ein Bericht nach Service Organisation Control 3 (SOC 3) enthält Informationen zu den internen Kontrollmechanismen einer Service-Organisation im Hinblick auf ***Sicherheit***, ***Verfügbarkeit***, ***Verarbeitungsintegrität***, ***Vertraulichkeit*** und ***Datenschutz***.
- Dies sind die fünf Fokus-Bereiche der AICPA Trust Services Principles and Criteria.
- SOC 3 berichtet über dieselben Informationen wie ein SOC 2-Bericht. Der Hauptunterschied zwischen beiden besteht darin, dass SOC 3 für ein ***allgemeines Publikum*** vorgesehen ist. Die Berichte sind also kürzer und gehen nicht so sehr ins Detail wie SOC 2-Berichte, die an ein informiertes Publikum aus interessierten Parteien verteilt werden. Aufgrund ihrer allgemeineren Natur können SOC 3-Berichte offen verbreitet und etwa - mit einem Siegel, das die Einhaltung bestätigt - auf der Webseite des Unternehmens veröffentlicht werden.

## *Solvency II*

- Solvabilität II, abgekürzt auch Solva II, englisch Solvency II, ist eine Richtlinie der Europäischen Union, mit der das europäische Versicherungsaufsichtsrecht grundlegend reformiert wurde.
- Schwerpunkte der Richtlinie bilden risikobasierte Solvabilitätsvorschriften für die Eigenmittelausstattung der Versicherungsunternehmen/-gruppen und qualitative Anforderungen an das Risikomanagement von Versicherungsunternehmen/-gruppen sowie erweiterte Publikationspflichten.
- Die Richtlinie wurde europaweit 2009 veröffentlicht und ist seit Januar 2016 in Kraft.

- Die Rahmenrichtlinie 2009/138/EG wurde am 25. November 2009 gültig - wobei die Umsetzung in den Staaten der EU sich noch lange hinzog - und wurde zwischenzeitlich mehrfach ergänzt und korrigiert.
- Bis zur Umsetzung von Solvabilität II galten die bisherigen Regelungen, die nachträglich als Solvabilität I (englisch Solvency I) bezeichnet wurden.
- Diese basieren auf den europäischen Richtlinien 2002/13/EG zur Schadensversicherung und 2002/83/EG zur Lebensversicherung.
- Sie bauen auf der Ersten Richtlinie 73/239/EWG (Aufnahme und Ausübung der Tätigkeit der Direktversicherung) auf.

## *SOX - Sarbanes-Oxley Act*

- Requires ***segregation of duties***.
- Der **Sarbanes-Oxley Act of 2002** (auch *SOX*, *SarbOx* oder *SOA*) ist ein US-Bundesgesetz, das als Reaktion auf Bilanzskandale von Unternehmen wie Enron oder Worldcom die Verlässlichkeit der Berichterstattung von Unternehmen, die den öffentlichen Kapitalmarkt der USA in Anspruch nehmen, verbessern soll.
- Kernstück: Die finanziellen Prozesse müssen gänzlich nach dem festgelegten Regelheft durchgeführt werden.
- Regulations regarding: ***Log Management***

## *SSAE 16*

- Statement on Standards for Attestation Engagements no. 16 (SSAE 16) is a largely ***American auditing standard*** for service organizations, superseding Statement on Auditing Standards no. 70 (***SAS 70***).
- The "service auditor's examination" of SAS 70 is replaced by a ***System and Organization Controls (SOC) report***.
- Many organizations that followed SAS 70 have now shifted to SSAE 16.
- Some service organizations use the SSAE 16 report status to show they are more capable, and also encourage their prospective end-users to make having an SSAE 16 a standard part of new ***vendor selection criteria***.
- Public companies in the United States fall under the Public Company Accounting Reform and Investor Protection Act, also known as ***Sarbanes-Oxley*** or SOX.
- SSAE 16 ***mirrors*** the International ***Standard on Assurance Engagements (ISAE) 3402***.
- SSAE 16 has two different kinds of reports. A ***SOC 1 Type 1*** report and a ***SOC 1 Type 2*** report adds a historical element, showing how controls were managed over time.
- The SSAE 16 standard requires a minimum of six months of operation of the controls for a SOC 1 Type 2 report.
- SSAE 16 provides ***guidance*** on an ***auditing method***, rather than mandating a specific control setand is in this respect like ***ISO 27001:2013***.

## *STIGS - Security Technical Implementation Guides*

- Can provide a starting point for organizations to define security configurations for common technology and systems.
- The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

## *TCSEC - Trusted Computer System Evaluation Criteria*

- Replaced by ***Common Citeria***.
- See also ***Orange Book***.
- According tot he TCSEC guidelines, ***trusted paths*** are required for higher trust level systems such as those at level ***B2*** or higher of TCSEC.
- Focuses ist concern entirely on ***confidentiality***.
- Was used ***to evaluate*** operating systems, applications, and different products.

***Categories:***

**A Verified protection**

- The highest level of security.

A1 Verified Protection
- Configuration Management is required.

**B Mandatory Protection**
- Based on the ***Bell-LaPadula*** security model and ***reference monitor***.

B1 Labeled Security
- Enforces using ***security labels***.
- Separate Operator and system administrator roles are not required at level B1.

B2 Structured Protection
- Separate Operator and system administrator roles are required at level B2.
- Configuration Management is required.
- Concerned about ***covert channels***.

B3 Security Domains
- Separate Operator and system administrator roles are required at level B2.
- Configuration Management is required.

**C Discretionary Protection**

C1 Discretionary protection

C2 Controlled Access protection
- Requires auditing mechanisms.

**D Minimal Protection.**
- Reserved for systems that have been evaluated but do not meet requirements to belong to any other category.

## *Trade Secrets*

- Trade secret protection is one oft he best ways to protect ***computer software***.

## *Trademarks*

- ***Words***, ***names***, ***symbols***, ***sounds***, ***slogans*** and ***logos*** to identify a company and ist products.
- The trademark should not be ***descriptive***.
- Trademarks, unlike patents can be ***renewed forever*** as long as they are being used in business.
- ™
- ®
- Intent to use application.

## *UCITA - Uniform Computer Information Transactions Act*

- Der Uniform Computer Information Transactions Act (UCITA) war ein umstrittener US-amerikanischer Gesetzesvorschlag aus dem Jahr 1999 zur Neuregelung des ***Vertragsrechtes für Software***.
- Es sah u. a. vor, dass Lizenzverträge auch dann gültig sind, wenn der Kunde sie erst nach dem Kauf des Produktes einsehen kann.
- Ausserdem sollten Softwarefirmen ein Recht zum „Ausschalten der Lizenz“ erhalten, beispielsweise bei Ablauf einer Lizenz durch Löschen per Internet auf dem Kundenrechner.
- Das Vorhaben wurde im August 2003 für gescheitert erklärt. Es wurde jedoch 2000 in den Bundesstaaten Virginia und Maryland ratifiziert und war dort auch 2008 noch geltendes Recht.

## *UCITS - Undertakings for Collective Investments in Transferable Securities*

- UCITS ist die internationale Bezeichnung für OGAW (Organismen für gemeinsame Anlagen in Wertpapieren).

## *UPA - USA Patriot Act (2001)*

- Der USA PATRIOT Act ist ein US-amerikanisches Bundesgesetz, das am 26. Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde.

- Es war eine direkte Reaktion auf die Terroranschläge am 11. September 2001 und die wenig später erfolgten Milzbrand-Anschläge. Das Gesetz bringt eine Einschränkung der amerikanischen Bürgerrechte in grösserem Masse mit sich, aber auch Auswirkungen für USA-Reisende, da die Anforderungen an Pässe erhöht wurden.
- USA PATRIOT Act steht als Apronym für Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, deutsch etwa:
    - „Gesetz zur Einigung und Stärkung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu verhindern“.
- Teile des Gesetzes sind am 1. Juni 2015 abgelaufen und wurden tags darauf ***am 2. Juni 2015 durch die Bestimmungen des USA Freedom Act*** ersetzt.

### *US-EU Safe Harbor*

- Safe Harbor is the name of an agreement between the United States Department of Commerce and the European Union that regulated the way that U.S. companies could export and handle the personal data of European citizens.
- The goal of Safe Harbor is to provide a single set of data protection requirements for transferring data across the borders of countries who joined the Safe Harbor collective.
- The agreement required that companies that collected ***personal data*** must inform people their data was being gathered, tell them what would be done with it, obtain permission to pass on the information to a third party, allow people access to the data gathered, ensure data integrity and security and provide a way to enforce compliance.
- Safe Harbor, which was established in 2000, is originally a compromise set up in response to the ***European Commission Directive on Data Protection***.

### *VKF - Brandschutznormen*

- Die Schweizerischen VKF-Brandschutzvorschriften bestehen aus der VKF-Brandschutznorm und den VKF-Brandschutzrichtlinien.
- Sie wurden durch das Interkantonale Organ Technische Handelshemmnisse IOTH als verbindlich erklärt und in Kraft gesetzt.
- Die VKF gibt für alle an der Umsetzung der VKF-Brandschutzvorschriften beteiligten Personen Erläuterungen, nutzungs- und themenbezogene Arbeitshilfen, Merkblätter und weitere Publikationen heraus.

### *WIPO - World intellectual Property Organization*

- https://www.wipo.int/portal/en/index.html

## ETHICS

### *Code of Ethics Preamble*

- The safety and welfare of society and the common good, duty to our principals and to each other requires that we adhere and be seen to adhere to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification as CISSP.

### *ISC2 CBK - Common Body of Knowledge*

- In security, Common Body of Knowledge (CBK) is a comprehensive ***framework*** of all the relevant subjects a security professional should be familiar with, including skills, techniques and best practices.
- CBK is organized by domain and it is annually gathered and updated by the ***International Information Systems Security Certification Consortium***, otherwise known as (ISC2).
- Discourage unsafe practices.

***Domains***

1. Information Security Governance and Risk Management
2. Access Control
3. Telecommunications and Network Security
4. Security Architecture and Design

5. Physical (Environmental) Security
6. Software Development Security
7. Cryptography
8. Business Continuity and Disaster Recovery Planning
9. Legal, Regulations, Investigations and Compliance
10. Operations Security

***ISC2 - Code of Ethics Canons***

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Security professionals have great social responsibility.
- We are charged with the burden of ensuring that our actions benefit the common good.
- Act honorably, honestly, justly, responsibly, and legally.
- Integrity is essential to the conduct of our duties.
- We cannot carry out our duties effectively if others within our organization, the security community, or the general public have doubts about the accuracy of the guidance we provide or the motives behind our actions.
- Provide diligent and competent service to principals.
- Although we have responsibilities to society, we also have specific responsibilities to those who have hired us to protect their infrastructure.
- We must ensure that we are in a position to provide unbiased, competent service to our organization.
- Advance and protect the profession.
- Our chosen profession changes on a continuous basis.
- As security professional, we must ensure that our knowledge remains current and that we contribute our own knowledge to the community's common body of knowledge.

## *Ethics and the Internet*

- See: ***RFC 1087***
- See also: ***IAB***

**The following purposes are unacceptable and unethical:**

- Seeks to gain unauthorized access to the resources of the internet.
- Disrupts the intended use of the Internet.
- Wastes resources (people, capacity, computer) through such actions.
- Destroys the integrity of computer-based information.
- Compromises the privacy of users.

## *Computer Ethics Institute*

**Defined 10 codes:**

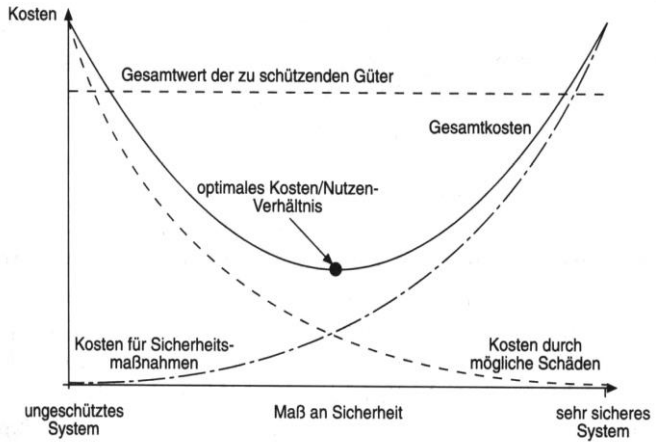
1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization nor proper compensation.
8. Thou shalt not appropriated other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

# FINANCIAL MANAGEMENT

- Defines the processes of planning, organizing, directing, and controlling the monetary activities of an organization and the use of its funds.
- In most companies the CISO-Department is a ***cost center***.

## *CISOs Role*

- The CISO plays an important role in financial planning for the information security program.
- Because most funding for the security program is allocated from the organizational operating budget, the CISO has a fiduciary responsibility to be a good steward of the funds invested in the program.
- Achieving good stewardship requires an understanding of fundamental financial management concepts.
- This understanding promotes the financial ***success of the security program*** and its mission.



# GPSP - GUIDELINES, PROCEDURES, STANDARDS and POLICY'S


## *GUIDELINE*

- Guidelines provide additional guidance to achieve all the steps outlined in a procedure that exists to support a policy.
- Guidelines can include ***best practices***, which will depend on the context of the associated or procedure.

***For example:***

- ***Full-disk encryption*** did not exist as a best practice until the compromise of 26.5 million records on a Veteran's Administration laptop. Since then, encryption of mobile devices is accepted as a standard guideline, or best practice, in most organizations.
- Best practices often support tailoring or customization.
- Whatever best practices an organization implements, the practices must be tailored to the requirements, resources, and culture of the organization.

## *PROCEDURE*

- Procedures are an ***extension of policies***.
- Procedures are ***step-by-step instructions*** that outline the proper steps to take to achieve the requirements defined by a policy.
- They are important because they explain how the organization will implement the policy.
- The CISO should work with the organization to develop procedures, where applicable, that define how the organization wants people to achieve compliance with the policies.
- Procedures should map directly to policies.
- Procedures are best developed when the input of each of the interfacing areas are included in the development of the procedure.
- This reduces the risk that important steps, communication, or required deliverables are left out of the procedure.
- Consistent documentation of the procedures facilitates an evaluation of effectiveness for future changes and improvements in the security procedures that support an organization.
- For example, if an organization documents a password policy that requires an 18-character password for authentication, the associated procedure should provide guidance for creating a password and offer a procedure for graceful and emergency password changes.
- Graceful changes occur naturally at the end of the password lifetime.
- Emergency password changes occur when the organization identifies a security event related to passwords that triggers a password change.

## *STANDARD*

- Standards extend policies to assign quantifiable measures that define the requirements for implementing the policy.
- Standards support consistent implementation of policies and reduce confusion, which can increase efficiency.
- Some organizations develop unique standards for information security.
- Some industries and the auditors within those industries treat standards with the same weight and influence as policies.

- This often occurs in regulated industries like financial services and energy where the “quantifiable measures” help establish the effectiveness of the controls implemented within an organization.
- Determination of which standards meet the organization’s needs must be driven by the security policies adopted by the organization.
- The standards provide the specification of the technology to effectively enable an organization to become successful in meeting the requirements of the policy.

## *POLICY*

- A policy is defined as a high-level document that oulines senior management's security directives.

***POLICY: PEN-Testing***

- "***CEH Terms of Engagement***" must be signed by CEH before PEN-Testing

***POLICY: Password***

- ❑ Passwords should not use personal information
- ❑ Passwords should be eight or more characters
- ❑ Passwords should be changed regularly
- ❑ Passwords should never be comprised of common words or names
- ❑ Passwords should be complex, use upper- and lower-case letters, and miscellaneous characters (e.g., !, @, #, $, %, ^, &)
- ❑ Limit logon attempts to three successive attempts
- ❑ Use a copy of the password database and standalone workstation to test password strength with password cracking program.
- ❑ Salted passwords should be used whenever possible.

***POLICY: VoIP***

- ❑ Encrypt VoIP traffic.

***POLICY: WLAN***

- ❑ Change the default value of the ***SSID***
- ❑ Perform Mandatory Access Control (MAC) filtering
- ❑ Turn off Dynamic Host Configuration Protocol (DHCP)
- ❑ Limit the access of wireless users
- ❑ Use port authentication such as ***802.1x***
- ❑ Perform periodic site surveys and scan for rogue devices
- ❑ Update policies to stipulate the requirements for wireless users
- ❑ Use ***encryption***
- ❑ Implement a second layer of authentication such as "***Remote Authentication Dial-In User Server (RADIUS)***"
- ❑ Use ***WTLS***

***POLICY: Network Security (Draft)***

***Checklist:***

- Focus on value rather than return on investment. Consider the harm a network security breach could do to the organization, such as lost revenue or customer litigation.
- Never assume security issues will originate from outsiders. Employees can accidentally create security vulnerabilities, and disgruntled or former employees can cause considerable damage.
- Do not address security issues with a piecemeal approach; use a single, unified strategy that protects the whole network.
- Collaborate within the organization to develop and implement security strategies, focusing on technology, training, and physical site security.
- Find the right balance between security and usability.
- The more secure the network is, the more difficult it can be to use.

***POLICY: IT System Security and Management Policy***

Excerpts see below:

Lifecycle Management Pricipals

- ❑ All systems are identified and included in service agreements, whter these services are provided in-house or outsourced.
- ❑ IT systems are inventoried

Change Log must contain:

- ❑ What was changed
- ❑ Who made the change
- ❑ When was the change made
- ❑ Why the change was made (reason/comment)

Vulnerability Management

- ❑ Identification
- ❑ Risk Assessment
- ❑ Treatment
- ❑ Monitoring

***POLICY: Remote Access (RAS)***

- ❑ Use CHAP instead of PAP

***POLICY: Mobile Device Management (MDM)***

- For ***BYOD - Bring Your Own Device*** systems, use ***device fingerprinting***.
- Providing capability for remote wiping, personal identity number (PIN) reset, and application authorization.
- Users must be ***educated*** on the dangers of leaving devices in plain view, as well as the benefit of storing devices securely when they are not in use.
- Evetually implement technologies to tracke the devices with ***GPS - Global Positioning Systems***.

# CIA TRIAD - CONFIDENTIALITY, INTEGRITY, and AVAILABILITY

- A guideline to judge all things related to security.
- Each organization needs to evaluate the nuances of confidentiality they wish to enforce.
- The ***CIA Triad*** is sometimes called the ***AIC Triad*** or ***Security Triad***.
- ***Identification*** and ***authentication*** always occur together as a ***single two-step process***.
- ***Identification*** and ***authentication*** are ***"all-or-nothing"*** aspects of access control.

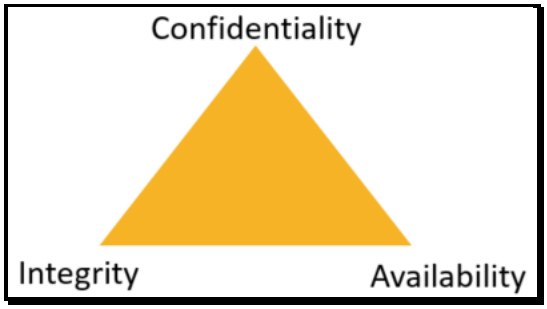



**Figure 2: The CIA Triad**

## *Confidentiality*

- Data must be ***protected from unauthorized access***, use, or disclosure while in ***storage***, in ***process***, and in ***transit***.
- ***Access controls*** help ensure that only authorized subjects can access objects.
- When unauthorized entities can access systems or data, it results in a ***loss of confidentiality***.

Sensitivity
Discretion
Criticality
Concealment
Secrecy
Privacy
Seclusion
Isolation

## *Integrity*

- For integrity to be maintained, objects must retain their veracity and be intentionally modified by only ***authorized subjects***.
- For integrity to be maintained on a system, controls must be in place to restrict access to data, objects and resources.
- Activity logging should be employed.

## *Availability*

- Authorized subjects are granted ***timely*** and uninterrupted access to objects.
- Prevention of ***Denial-of-Service attacks (DoS)***.
- Availability depends on both integrity and confidentiality.

## *AAA Services*

- ***Mobile IP***, which provides access to mobile users with smartphones, also uses AAA protocols.
- Common AAA protocols are: ***RADIUS***, ***TACACS+*** and ***Diameter***.

**The five elements of AAA services:**
Identification
Authentication
Authorization

Auditing
Accounting

***Identification***

- Without an identity, a system has no way to correlate an authentication factor with the subject.
- A ***subject*** must ***provide an identity*** to a system to state the authentication, authorization and accountability processes.
- A core principal with authentication is that ***all subjects must have unique identities***.
- Simplified ***username = Identity***.
- During the ***registration process*** the subject gets the identification (User ID).

***Authentication***

- The process of verifying or testing that the claimed identity is valid is called authentication.
- Authentication information used to verify identity is ***private information*** and needs to be protected.
- See also Multifactor Authentication (MFA)
- Simplified ***password = authentication***.

**Authentication factors:**

- Type 1 (Weakest): Something you know
- Type 2: Something you have
- Type 3 (Strongest): Something you are or something you do

***Authorization***

- Giving the rights and privileges assigned to the authenticated ***identity***.
- Indicates who is ***trusted*** to perform specific operations.

**Mechanisms and Concepts:**

Implicit Deny
Access Control Matrix
Capability Tables *(related/attached to a subject)*
Constrained Interface
Content-Dependent Control
Context-Dependent Control
Need to Know
Least Privilege
Separation of Duties and Responsibilities

***Auditing***

- Subject's actions are tracked and ***recorded*** for holding the subject accountable for their actions while authenticated on a system.
- Auditing ***tracks subjects*** and records when they access objects, creating an ***audit trail*** in one or more audit logs.
- ***Auditing provides accountability***.

***Accounting***

- Reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions.
- ***Auditing***, ***logging*** and ***monitoring*** provide accountability by ensuring that subjects can be held accountable for their actions.

**Remark:**

- If the organization is using ***shared/common user names*** and passwords no accountability is given.

***Products***

- NSP - Network Services Platform (Nokia)

## *Levels of Classification*

***GOVERNMENT***

| | |
|---|---|
| ***High*** | Top Secret<br>Secret<br>Confidential<br>Sensitive but unclassified (SBU) |
| ***Low*** | Unclassified |

***PUBLIC***

| | |
|---|---|
| ***Sensitive*** | Data that is to have the most limited access and requires a high degree of integrity. This is typically data that will do the most damage to the organization should it be disclosed. |
| ***Confidential*** | Data that might be less restrictive within the company but might cause damage if disclosed. |
| ***Private*** | Private data is usually compartmental data that micht not do the company damage but must be keep private for other reasons. Human resources data is one example of data that can be classified as private. |
| ***Proprietary*** | Proprietary data is data that is disclosed outside the company on a limited basis or contain information that could reduce the company's competitive advantage, such as the technical specifications of a new product. |
| ***Public*** | Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the company. |

## *Roles*

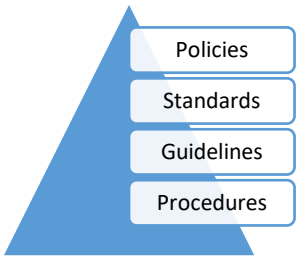
| | |
|---|---|
| Auditor | |
| CSIRT | Computer Security Incident Response Team |
| Data Custodian | |
| Data Owner | |
| Senior Manager | |
| Security Professional | |
| User | |

## *Security Policy*

- A security policy is a ***document*** that defines the security requirements for an organization.
- It identifies ***assets*** that need protection and the extent to which security solutions should go to protect them.
- ***Senior management*** must approve the security policy.
- Your security policy should ***specify steps*** to take for various types of incidents.

**Categories**

Regulatory
Advisory
Informative




***Guidelines***

- ❑ Make sure you know what incidents you must report.

- ❑ When should your report an incident?
- ❑ To whom should you report it?

***Procedures***

***Baselines***

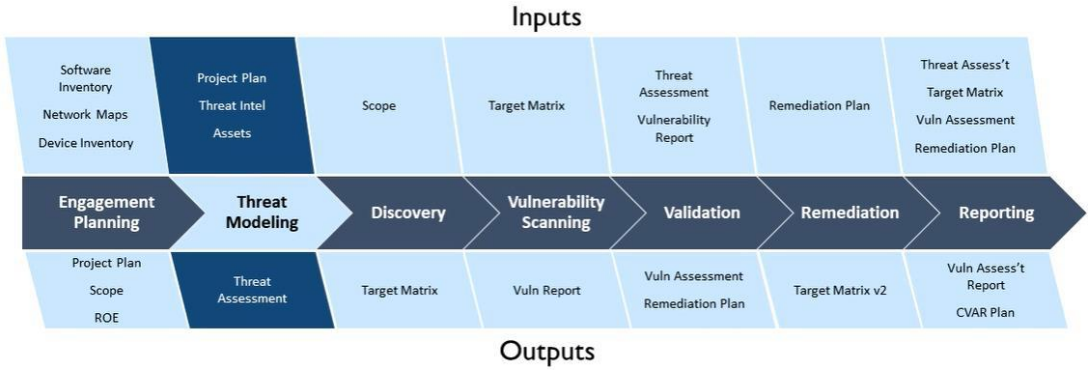
- CIS Benchmarks
- All non-Administrators should not have access due to the sensitive data and the rules of least privilege.
- Enable Multi-Factor Authentication (MFA).
- Block remembering MFA on trusted devices.

## *Threat Modeling*

- The ***ultimate goal*** of threat modeling is to ***prioritize the potential threats*** against an organization's asset.

**Approaches:**

- Focused on Assets
- Focused on Attackers
- Focused on Software



# PRINCIPALS of SECURITY MODELS, DESIGN and CAPABILITIES

- ***Computer security*** should be foremost ***cost-effective***.

## *Access Controls*

- CONTROLLING and MONITORING ACCESS
- The primary goal of controls is to ensure the ***confidentiality*** and ***integrity*** of data by disallowing unauthorized access by authorized or unauthorized subjects.

**Something a user knows**

- PASSWORDS
- One-time password (OTP)
- Static password
- Passphrase

**Something a user has**

- Key
- swipe card
- access card
- badge
- tokens

**Something a user is**

- What you physically are: ***BIOMETRICS***

***MAC - Mandatory Access Control***

- Limits the access to objects by ***subjects***.
- Relies on the use of ***classification labels / sensitivity labels***, which contains the ***classification*** and ***category set***.
- Each classification label represents a ***security domain***.
- Often referred as a ***lattice-based model***.
- The MAC model is ***more secure*** than the DAC model, but it isn't as flexible or scalable.
- Restriction: ***need to know*** can apply.
- ***Rule based*** access control
- Objects are ***files***, ***directories*** and ***devices.***

**Three types of environment:**

Hierarchical Environment
Compartmentalized Environment
Hybrid Environment

***DAC - Discretionary Access Control***

- Limits the access to objects by ***subjects***.
- Does not use ***classification labels***.
- A DAC model is implemented using ***ACLs on objects***.
- Ever object has an ***owner*** and the owner determines who has access.
- Allows the owner, creator or data custodian of an object to ***control and define access to that object***.
- Discretionary can also mean: Controlled access protection (object reuse, protect audit trail). User directed access control (identity based and hybrid based are also forms of discretionary) Identity Based AC

***Non-DAC - Non-Discretionary Access Control***

- Administrators ***centrally*** administer nondiscretionary access control and can make changes that affect the entire environment.
- Implies a ***central authority*** that defines ***rules*** and sometimes ***global rules***, dictating what subjects can have access to what objects.

Role based
Task based

lattice based → greatest lower, least upper bounds apply

***RBAC - Rule Based Access Control***

- ***Non-Discretionary Access Control*** (NDAC).
- Role-Based Access Control (RBAC) is a method of ***restricting*** or ***authorizing*** system access for users based on ***user roles*** and ***locales***.
- A ***role*** defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed to access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.
- A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the ***Server Administrator role*** in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.
- One common example of a RBAC model is a ***firewall***.

***TBAC - Task-Based Access Control***

- Under TBAC the focus is on controlling access by ***assigned tasks*** rather than by user identity.

***ABAC - Attribute-Based Access Control***

- Advanced implementation of a RBAC.
- The RBAC applies to all users, but the ABAC can be ***more specific***.

## *Security Models*

- In information security, models provide a way to ***formalize security policies***.
- A security model provides a way for designers to map abstract statements into a security policy that prescribes the algorithms and data structures necessary to build hardware and software.

***TCB - Trusted Computing Base***

- ***Life cycle assurance*** ensures, that TCB is designed, developed and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle.

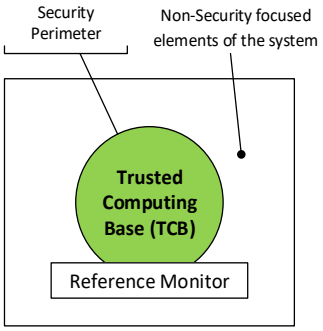



**Figure 3: TCB**

***Security Perimeter***

- The security perimeter of your system is an imaginary boundary that separates the TCB from the rest of the system.

***State Machine Model***

- The state machine model describes a system that is always secure no matter what state is in.
- Base ***Finite State Machine (FSM)***.
- A ***state*** is a snapshot of a system at a specific moment in time.
- If all aspects of a ***state*** meet the requirements of the security policy, that state is considered secure.

***Information Flow Model***

- The information flow model focuses on the ***flow of information***.

- Information flow models are based on a ***state machine model***.
- ***Bell-LaPadula*** and ***Biba*** are information flow models.
- Information flow models can also address ***type of flows***.

***Noninterference Model***

- Is loosely based on the ***information flow model***.
- Concerned with the ***actions of a subject*** at a ***higher security level*** affect the system stare or the actions of a subject at a ***lower security level***.
- Does not concern itself with the ***flow of data***.
- Provide a form of protection against damage caused by malicious programs such as ***Trojan horses***.
- If actions of a higher-level security subject is affecting a lower level security object it can create a ***covert channel***.

***Take-Grant Model***

- The Take-Grant model employs a directed graph to dictate how ***rights can be passed from one subject*** to another or ***from a subject to an object***.

| | |
|---|---|
| **Take rule** | Allows a subject to take rights over an object |
| **Grant rule** | Allows a subject to grant rights to an object |
| **Create rule** | Allows a subject to create new rights |
| **Remove rule** | Allows a subject to remove rights it has |

***Access Control Matrix***

- An access control matrix is a table of subjects and objects that indicates the actions or functions that each subject can perform on each object.
- Each column of the matrix is an ***ACL***.

***Bell-La Padula***

- Defined by ***David Bell*** and ***Leonard LaPadula***.
- ***Mandatory Access Control***
- ***Security Model***
- ***Information flow model***.
- ***Subject-to-Object model***
- Target to ***protect classified information***.
- Addresses only the ***confidentiality of data***.
- Does not address the aspects of ***integrity*** or ***availability*** for objects.
- Is a ***state machine*** model used for enforcing ***access control*** in ***government*** and ***military*** applications.
- Developed by the ***DoD***.
- Derived from the ***DoD multilevel security policy***.
- Preventing information flow from a ***high security level*** → ***low security level***.
- The first ***mathematical model*** of a multilevel security policy.
- Requires ***classification labels***.

***The tree main rules:***

**SS Rule - Simple Security rule**

- States that a subject may not read information at a higher sensitivity level
- ***no read up***
- ***Read down allowed***

**Discretionary Security rule**

- States, that the system uses an access matrix to enforce discretionary access control.

*** Star-Property**

- Also called ***confinement property***
- ***Write up allowed***
- ***Write down blocked***

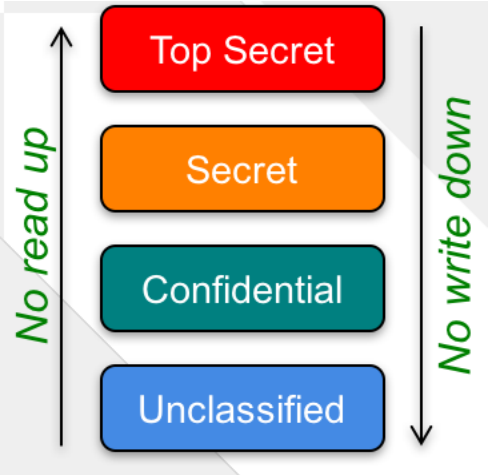



**Figure 4: Bell-LaPadula**

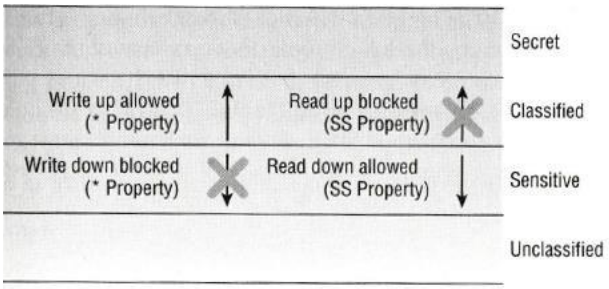



**Figure 5: Bell-LaPadula model**

***Lattice-Based Access Control***

- See also ***Mandatory Access Control*** (MAC).
- Can be used for complex access control decisions involving multiple objects and/or subjects.
- A lattice model is a ***mathematical structure*** that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

***Biba***

- ***Information flow model*** / ***state machine model*** like Bell-LaPadula.
- Preventing information flow from a ***low security level*** ➔ ***high security level***.
- Addresses ***integrity***.
- Requires ***classification labels***.

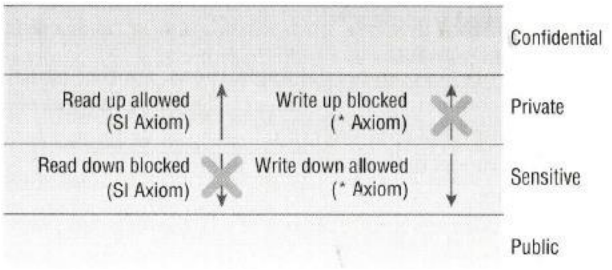



**Figure 6: Biba model**

***Target, prevent/protect:***

- Modification of objects by unauthorized subjects.
- Unauthorized modification of objects by unauthorized subjects.
- Internal and external object consistency.

***Three main rules:***

***-integrity axiom**

A subject cannot write data to an object at a higher integrity level (referred as "***no write up***")

**Simple integrity axiom**

A subject cannot read data from a lower integrity level (referred as "***no read down***")

**Invocation property**

A subject cannot request service (invoke) of higher integrity.

***Clark-Wilson Model***

- ***Integrity model***.
- Uses a ***multifaceted*** approach to enforcing ***data integrity***.
- Uses a three-part relationship of ***subject/program/object*** known as ***access control triple***.
- Uses ***security labels*** to grant access to objects.
- Enforces ***separation of duties***.
- Introduces ***access to objects only through programs***.

***The three goals are:***

1. Prevent unauthorized users from making modifications
2. Prevent authorized users from making improper modifications (separation of duties)
3. Maintain internal and external consistency (well-formed transaction)

**Clark-Wilson items:**

| | |
|---|---|
| CDI | Constrained Data Item |
| UDI | Unconstrained data item |
| IVP | Integrity verification procedure |
| TP | Transformation procedures |

***Brewer and Nash Model***

- Also known as ***Chinese Wall.***
- Uses the principal of ***data isolation***.
- This model applies to a ***single integrated database***.
- For example, someone who works for ***company C*** who has access to proprietary data for ***company A*** should not have access to data for ***company B***.
- Provides access controls that can ***change dynamically*** depending upon a user's previous actions.
- Main goal is to ***protect against conflicts of interest*** by user's access attempts.

***Goguen-Meseguer Model***

- ***Integrity model***.
- Foundation of ***noninterference conceptual theories***.
- Predetermining the set of domains.

***Sutherland Model***

- ***Integrity model***.

***Graham-Denning Model***

- Security creation and deletion of both subjects and objects.
- Consists of ***8 primary protection rules***.

## *System High Security Mode*

- A system is operating in ***system high-security mode*** when all users have a security clearance to access the information but not necessarily a need-to-know for all the information processed on the system.

## *Dedicated Security Mode*

- A system is operating in a ***dedicated security mode*** if all users have a clearance for and a formal ***need-to-know*** about all data processes within the system.

## *Certification*

- The ***first phase*** in a total evaluation phase is certification.

## *Accreditation*

- Is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards.

- If management decides the certification of the system satisfies their needs, the system is ***accredited***.

## *Security Capabilities of Information Systems*

- Includes ***memory protection***, ***virtualization***, ***Trusted Platform Module***, and ***fault tolerance***.

***Memory Protection***

- Memory protection is used to prevent an active process from interacting with an area of memory that was not specifically assigned or allocated to it.

***Virtualization***

Hyper-V
MS Virtual PC
MS Virtual Server
Oracle's VirtualBox
Parallels Desktop for Mac
VMware
XenServer

***TPM - Trusted Platform Module***

- A TPM is just one example of a ***Hardware Security Module (HSM)***.
- A TPM chip is used to store and process cryptographic keys for the purpose of a hardware supported/implemented ***hard drive encryption system***.

***Interfaces***

- The use of an interface is a practical implementation of the ***Clark-Wilson model of security***.
- Commands might be available to administrators via a menu or by right-clicking an item, but if a regular user doesn't have permissions, the ***command does not appear***.

***Fault Tolerance***

- Is the ability of a system to suffer a fault but continue to operate.

# PERSONNEL SECURITY

- Operational Control

## *Personnel Security Policies*

***Job Descriptions***

Constructing Job Descriptions requires:

- Separation of Duties
- Job Responsibilities
- Job Rotation

***Candidate Screening***

- ❑ Background checks
- ❑ Reference checks
- ❑ Education verification
- ❑ Security clearance validation

***Employment Agreement***

- ❑ Employee has to sign an employment agreement
- ❑ Sign a Nondisclosure Agreement (NDA)

***Employment Termination Process***

**Collect all:**

- Organization-specific identifications
- Access
- Security badges
- Cards
- Keys
- Access tokens
- Computer
- iPad
- iPhone
- User accounts

***SLAs***

- See Document Organization.

***Compliance***

- Employees need to be trained regarding what they need to do.

***Privacy***

- It is important to understand all government regulations that your organization is required to adhere to ensure compliance in the area of privacy protection.

## *Security Governance*

- Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.

# PROTECTING SECURITY of ASSETS

- One of the first steps in asset security is classifying and labeling assets.
- It is not uncommon for an ***email policy*** to require the deletion of all emails older than six months. These policies are often implemented using automated tools that search for old emails and delete them without any user or administrator intervention.

## *Email*

**Simple rules about encrypting email:**

- If you need confidentiality when sending an email message, ***encrypt*** the message.
- If your message must maintain integrity, you must ***hash*** the message.
- If your message needs authentication, integrity and/or nonrepudiation, you should ***digitally sign*** the message.
- If your message requires confidentiality, integrity and/or nonrepudiation, you should ***encrypt and digitally sign*** the message.

***PGP - Pretty Good Privacy***

- Designed by ***Phil Zimmerman.***
- PGP is available in two versions, ***commercial*** and ***freeware***.
- PGP uses its own type of ***digital certificates***.
- Uses ***symmetric*** encryption algorithm.

***Commercial version:***

- Uses ***RSA*** for key exchange
- ***IDEA*** for encryption/decryption for bulk encryption of data
- ***MD5*** for message digest production (Hashing).

***Freeware version:***

- Uses Diffie-Hellman key exchange the "Carlisle Adams/Stafford Tavares (CAST)" 128-bit encryption/decryption algorithm and the ***SHA-1*** hashing function.

***S-MIME***

- De facto standard for ***encrypting emails***.
- Uses ***RSA*** encryption algorithm.
- Relies on ***X.509 certificates*** for exchanging cryptographic keys.
- Supports ***AES*** and ***3DES*** symmetric encryption algorithm.
- Public key based, hybrid encryption schema.

## *Web Applications*

- For security, use SSL/TLS as transport channel.

## *PII - Personally Identifiable Information*

- Organizations have a responsibility to protect ***PII***.
- Any information that can be used to distinguish or trace an individual's identity, such as ***name***, ***social security number***, ***date*** and ***place of birth***, ***mother's maiden name***, or ***biometric records***.
- Use cryptographical storage to store PII.

## *PHI - Protected Health Information*

- Protected health information (PHI) under the US law is any information about ***health status***, ***provision of health care***, or ***payment for health care*** that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.
- This is interpreted rather broadly and includes ***any part of a patient's medical record or payment history***.
- PHI is often sought out in datasets for ***de-identification*** before researchers share the dataset publicly.

- Researchers ***remove individually identifiable PHI*** from a dataset to preserve privacy for research participants.

## *Destroying Sensitive Data*

- ***Data remanence*** is the data that remains on a hard drive as residual magnetic flux.

***INDUSTRY STANDARDS for DATA DESTRUCTION***

***(American) DoD 5220.22-M***

- This standard destroys the data on the drive's required area by overwriting that sector three times with ones and zeros, again verifying whether data is destroyed or not.

***(American) NAVSO P-5239-26 (RLL)***

- This is a three-pass overwriting algorithm that verifies in the last pass.

***(American) NAVSO P-5239-26 (MFM)***

- This is a three-pass overwriting algorithm that verifies in the last pass.

***(German) VSITR***

- This method overwrites in 6 passes with ones and zeros and then with the letter A.

***Russian Standard, GOST P50739-95***

- It is a wiping method that writes zeros in the first pass and then random bytes in the next pass.

***Erasing***

- Is the ***deletion*** of files or media.

***Clearing***

- Describes ***preparing media for reuse***.
- Renders information unrecoverable by a ***keyboard attack***.

***Purging***

- Is a ***more intensive form of clearing*** for reuse in lower security areas.
- Renders information unrecoverable against ***laboratory attack***.

***Declassification***

***Sanitization***

- Sanitization is disposing or erasing data in a ***secure manner***, ensuring the data is ***unrecoverable by any means***.

***Degaussing***

***Destruction***

- The best method of sanitizing SSDs is destruction.

# SOFTWARE DEVELOPMENT SECURITY

- It's much easier to build security into a system during development than it is to add security to an existing system.
- From a security point of view, ***object-oriented programming (OOP)*** provides a black-box approach to abstraction.

Compiled Languages
Interpreted Languages

1GL - First-Generation Languages
2GL - Second-Generation Languages
3GL - Third-Generation Languages
4GL - Fourth-Generation Languages
5GL - Fifth-Generation Languages

## System Development Life Cycle (SDLC)

***Conceptual Definition***

- The conceptual definition is a very high-level statement pf purpose and should not be longer than one or two paragraphs.
- Simply reading the concept statement periodically can assist in refocusing a team of developers.

***Functional Requirement Determination***

- In this phase, specific system functionalities are listed, and developers begin to think about how the parts of the system should interoperate to meet the functional requirements.
- Project managers should use this document as a checklist to ensure that all functional requirements are met.

***Control Specifications Development***

- Security-conscious organizations also ensure that adequate security controls are designed into every system from the earliest stages of development.

***Design Review***

- In this often-lengthy process, the designers determine exactly how the various parts of the system will interoperate and how the modular system structure will be laid out.

***Code Review Walk-Through***

- The meetings play an instrumental role in ensuring that the code produced by the various development teams performs according to specification.

***User Acceptance Testing***

- Most organizations perform the initial system tests using development personnel to seek out any obvious errors.

***Maintenance and Change Management***

- It's important that any changes to the code be handled through a formalized change management process.

## Life Cycle Models

***Waterfall Model***

See: Systems Engineering.docx

***Spiral Model***

See: Systems Engineering.docx

***Agile Software Development***

See: Scrum Master Handguide.docx

***Software Capability Maturity Model***

See: Systems Engineering.docx

***IDEAL Model***

See: Systems Engineering.docx

***Gantt Charts and PERT***

See: PMP.docx

## Change and Configuration Management

- Configuration management ensures that the technical settings of the hardware and software components are managed in a way that maintains secure operations
- To ensure that the required adjustments do not harm the security posture of a system, a well-defined ***configuration management process*** is needed that integrates information security principles

**Basic components:**
- Request Control
- Change Control
- Release Control

**Configuration Management:**
- Configuration Identification
- Configuration Control
- Configuration Status Accounting
- Configuration Audit

## *DevOps - Development and Operations Approach*

- The ***DevOps*** model is closely aligned with the ***Agile development*** approach and aims to dramatically decrease the time required to develop, test and deploy software changes.

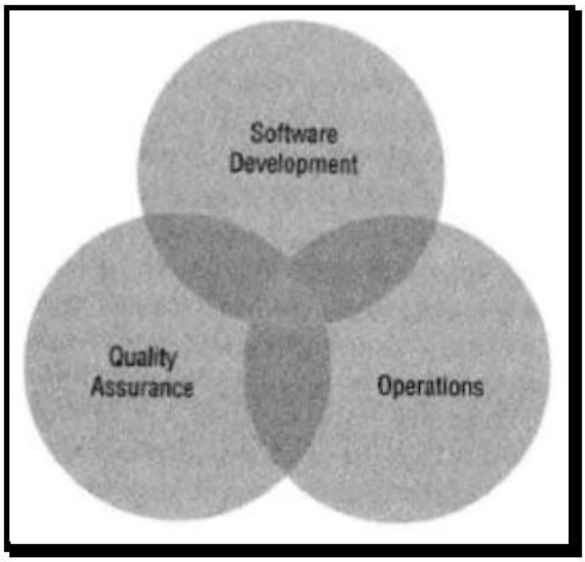



**Figure 7: DevOps Model**

## *API - Application Programming Interface*

- ***API keys*** are like passwords and should be trated as very sensitive information. they should always be stored in secure locations and transmitted only over encrypted communication channels. If someone gains access to your API key, they can interact with a web service as if they were you!

## *Software Testing*

- You should assign the testing of your software to someone other than the programmer who developed the code.

**White-Box Testing**
Examines the internal logical structures of a program and steps through the code line by line, analyzing the program for potential errors.

**Black-Box Testing**
Examines the program from a user perspective by providing a wide variety of input scenarios and inspecting the output. Black-Box testers do not have access to the internal code.

**Gray-Box Testing**
Combines the two approaches and is popular for software validation. In this approach, testers examine the software from a user perspective, analyzing inputs and outputs. They also have access to the source code and use it to help design their tests. They do not, however, analyze the inner workings of the program during their testing.

**Static Testing**
Evaluates the security of software without running it by analyzing either the source code or the compiled application. Usually involves the use of automated tools.

**Dynamic Testing**
Evaluates the security of software in a runtime environment. Testers often do not have access to the underlaying source code.

## *Code Repositories*

- Central storage point for developers to place their source code.
- They provide version control, bug tracking web hosting, release management and communications functions that support software development.

**Examples:**
- GitHub
- Bitbucket
- SourceForge

## *SLA - Service Level Agreements*

- Using SLAs is an increasingly popular way to ensure that organizations providing services to internal and/or external customers maintain an ***appropriate level of service*** agreed on by both the service provider and the vendor.
- SLA agreements also commonly include ***financial*** and other contractual remedies that kick in if the agreement is not maintained.

**Common addressed issues:**
- System uptime (as a percentage of verall operating time)
- Maximum consecutive downtime (in seconds/minutes/and so on)
- Peak load
- Average load
- Responsibility for diagnostics
- Failover time (if redundancy is in place)

## *SLO - Service Level Objective*

- Are the values of target metrics that are used to measure performance, reliability, or availability.
- These could be metrics defining the performance of request processing in milliseconds, the availability of services in minutes per month, or the number of requests processed per hour.

## *Software Acquisition*

- On premises
- Software-as-a-Service (SaaS)
- In the case of SaaS environments, most security responsibilities rests with the vendor, but the organization's security staff isn't off the hook, they have to monitor the vendor's security.

## *DBMS - Database Management System*

- Mixing data with different classification levels and/or need-to-know requirements is known as ***database contamination*** and is significant security challenge.

***Concurrency***
- ***Edit control*** is a ***preventive security mechanism*** that endeavors to make certain that information stored in the database is always correct or at least has its integrity and availability protected.
- When this recorded data is reviewed, concurrency becomes a ***detective control***.

***ODBC***

- Is a database feature that allows applications to communicate with different types fo databases without having to be directly programmed for interaction with each type.

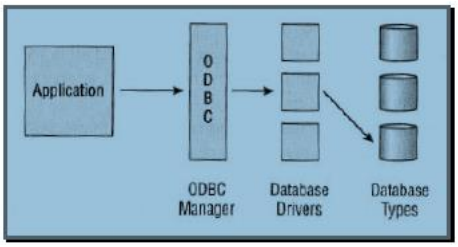



**Figure 8: ODBC interface**

## *Expert Systems*

- Every expert system has two main components: The ***knowledge base*** and the ***inference engine***.

## *Neural Networks*

- In neural networks, chains of computational units are used in an attempt to imitate the biological reasoning process of the human mind.
- Through the use of the ***delta rule***, neuronal networks are able to learn from experience.

## *DSS - Decision Supported System*

- A DSS is a knowledge-based application that analyzes business data and presents it in such a way as ***to make business decision easier for users***.
- It is considered more of an ***informational application*** than an operational application.
- Emphasizes flexibility in the decision-making approach.

# PHYSICAL SECURITY REQUIREMENTS

**Physical Threats**
- Fire, smoke, water earth movement, storms, sabotage/vandalism, explosion/destruction, building collapse, toxic material, utility loss, equipment failure, theft, personnel loss.

- Physical controls are the first line of defense, and people are the last.
- Create a ***secure facility plan*** with ***critical path analysis***.

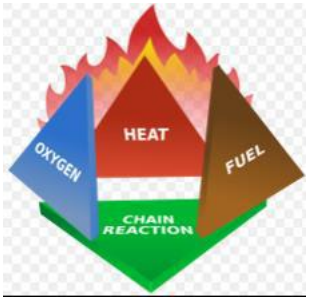



**Figure 9: The Fire Triangle**

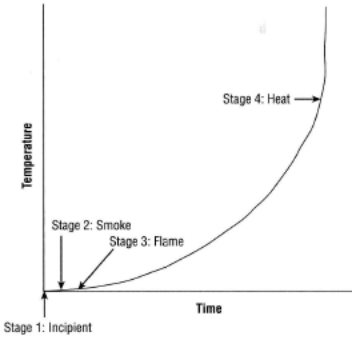



**Figure 10: The four primary stages of fire**

**Stage 1:** **The Incipient Stage**
At this stage, there is only ***air ionization*** but ***no smoke***.

**Stage 2:** **The Smoke Stage**
In Stage 2, smoke is visible from the point of ignition.

**Stage 3:** **The Flame Stage**
This is when a flame can be seen with the naked eye.

**Stage 4:** **The Heat Stage**
At Stage 4, the fire is considerably further down the timescale to the point where there is an intense heat buildup and everything tin the area burns.

## *Fire Extinguishers*

| Class | Type | Suppression material |
|---|---|---|
| A | Common Combustibles | Water, soda acid (a dry powder or liquid chemical) |
| B | Liquids | CO2, halon*, soda acid |
| C | Electrical | CO2, halon* |
| D | Metal | Dry powder |

* *Halon or an EPA-approved halon substitute*

### *Water Suppression Systems*

- Wet pipe system
- Dry pipe system (Clapper valve)
- Deluge system
- Preaction system (Most recommended)

### *Gas Discharge Systems*

See: www.epa.gov/oone/snap/fire/halonreps.html

- Gas discharge systems are usually ***more effective*** than water discharge systems.

### *Ventilation*

- Ventilation has several requirements that must be met to ensure a safe and comfortable environment.
- A closed-loop recirculating air-conditioning system should be installed to maintain air quality.
- "Closed-loop" means the air within the building is reused after it has been properly filtered, instead of bringing outside air in.
- ***Positive pressurization*** and ventilation should also be implemented to control contamination.
- ***Positive pressurization*** means that when an employee opens a door, the air goes out, and outside air does not come in.
- If a facility were on fire, you would want the smoke to go out the doors instead of being pushed back in when people are fleeing.

### *Privacy*

- Means protecting personal information from disclosure to any unauthorized individual or entity.
- Category Personally Identifiable Information (***PII***, see NIST)

### *Capacitance Detector*

- A "capacitance detector", emits a measurable magnetic field.
- The detector monitors this magnetic field, and an alarm sounds if the field is disrupted.
- These devices are usually used to ***protect specific objects*** (artworks, cabinets, or a safe) versus protecting a whole room or area.
- An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges.
- All objects have a static electric charge.
- They are all made up of many subatomic particles, and when everything is stable and static, these particles constitute one holistic electric charge.
- This means there is a balance between the electric capacitance and inductance.
- Now, if an intruder enters the area, his subatomic particles will mess up this balance in the electrostatic field, causing a capacitance change, and an alarm will sound.

# SECURE NETWORK ARCHITECTURE and SECURING NETWORK COMPONENTS

## *DNP3 - Distributed Network Protocol*

- Is a multilayer protocol that functions similarly to that of TCP/IP, in that it has link, transport, and transportation layers.
- Is primarily used in the electric and water utility and management industries.
- It is used to support communications between data acquisition systems and the system control unit.

## *DNS - Domain Name System*

See: www.dnssec.net

- See the Kaminsky DNS Vulnerability.

## *Converged Protocols*

### *FCoE - Fibre Channel over Ethernet*

- Converged Protocol.
- Layer 3 Protocol.
- Fibre Channel typically requires its own dedicated infrastructure (separate cables).
- A form of network data-storage solution (SAN or NAS).

### *MPLS - Multiprotocol Label Switching*

- Converged Protocol.
- MPLS is designed to handle a wide range of protocols through encapsulation.

### *iSCSI - Internet Small Computer System Interface*

- Converged Protocol.
- Is a networking storage based on IP.
- This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.
- Low-cost alternative to FCoE.

### *VoIP - Voice over IP*

- Converged Protocol.
- Is a tunneling mechanism used to transport voice and/or data over a TCP/IP network.
- Software based = ***Skype***.
- Hardware based = ***magicJack***.

### *SDN - Software Defined Networking*

- Converged Protocol.
- ***Vendor neutral*** and ***open standards*** based
- Using SDN frees an organization from having to purchase devices from a ***single vendor***.

## *CDN - Content Distributed Networks*

- A type of ***geographical*** and ***logical load balancing***.
- ***Providers:***
  CloudFlare, Akamai, Amazon, CloudFront, CacheFly and Level 3 Communications.
- The most widely recognized ***P2P CDN*** is ***BitTorrent***.

## *WIRELESS NETWORKS*

### *Securing Wireless Access Points (WAP)*

- You should adjust the strength of the wireless access point to maximize authorized user access and minimize intruder access.
- Use ***infrastructure mode*** rather than ***ad hoc mode***.

- ***Ad hoc mode*** means that any two wireless networking devices, including two wireless network interface cards, can communicate ***without a centralized control authority***.
- ***Power level*** adjustments should be performed carefully.

**WAP 1.0** was implemented 1999

**WAP 2.0** was released in 2002

***SSID - Service Set Identifier***
- ***SSID*** = Service Set Identifier
- Standard security practice dictates that the ***default SSID*** should be changed to something unique.
- For security reasons, the ***broadcasting*** (beacon frame) of the SSID should be disabled.
- The max. length of an SSID is ***32 characters***.
- ***WPA2*** must be used to secure Wireless LAN's.

***BSSID - Basic Service Set Identifier***

***ESSID - Extended Service Set Identifier***

***OSA - Open System Authentication***
- No real authentication is required.
- Typically transmits everything in clear text.

***OWA - Opportunistic Wireless Encryption***
- Bei Opportunistic Wireless Encryption nutzen WLAN-Client und WLAN-Zugangspunkt zuvor ausgehandelte, individuelle und einzigartige Schlüssel.
- Zur Aushandlung zwischen Client und Accesspoint kommt ein ***Diffie-Hellman-Key-Exchange***-Verfahren zum Einsatz.
- Die erhaltenen Pairwise Master Keys (PMKs) werden anstelle von WPA-PSKs im Vier-Wege-Handshake verwendet, um die eigentlichen Sitzungsschlüssel zu erzeugen und auszutauschen.
- Damit OWE funktioniert, müssen Client und Accesspoint das Verfahren unterstützen.
- Die Verschlüsselung der Daten erfolgt dann, ohne dass ein Passwort eingegeben werden muss.

***SKA - Shared Key Authentication***
- Some form of authentication must take place before network communications can occur.
- Authentications can be WEP. WPA, WPA2 and other.

***WEP - Wired Equivalent Privacy***
- Provides protection from ***packet sniffing*** and ***eavesdropping***. and ***integrity protection***.
- Uses a ***predefined shared secret key***.
- Today it is possible to ***crack WEP in less than a minute***.

***WPA - Wi-Fi Protected Access***
- Replacement for WEP.
- Based on the ***LEAP*** and ***TKIP*** cryptosystems.
- Vulnerable to ***brute-force attacks***.

***WPA2 - Wi-Fi Protected Access***
- Known as ***802.11i***.
- Uses the ***Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)*** based on ***AES*** encryption schema.

***802.1X***
- Supported by ***WPA*** and ***WPA2***.
- ***Port-based*** network access control (NAC).
- Is only ***one component*** of a complete NAC solution.

***EAP - Extensible Authentication Protocol***

- EAP is usually ***not encrypted***.
- A ***framework*** that supports multiple, optional authentication mechanisms for ***PPP***, including clear-text passwords, challenge-response and arbitrary dialog sequences.
- EAP is a protocol for wireless networks that expands on ***authentication methods*** used by the ***PPP protocol***, a protocol often used when connecting a computer to the internet.
- EAP can support ***multiple authentication mechanisms***, such as token cards, smart cards, certificates, OTP, and public key encryption authentication.
- ***Supports more than 40 methods:***
  LEAP, EAP-TLS, EAP-SIM, EAP-AKA and EAP-TTLS…

***PEAP - Protected Extensible Authentication Protocol***

- Encapsulates and encrypts EAP methods within TLS tunnel.

***LEAP - Lightweight Extensible Authentication Protocol***

- Cisco proprietary alternative to TKIP for WPA.
- LEAP ***should be avoided*** when possible.
- Use of ***EAP-TLS*** as an alternative is recommended otherwise a ***strong password*** is recommended.

***MAC Filter***

- Difficult to manage, eventually SDN could be used.

***TKIP - Temporal Key Integrity Control***

- Replacement for WEP.
- TKIP and WPA were officially replaced by WPA2 in 2004.

***CCMP - Counter Mode with Xipher Block Chaining Message Authentication Code Protocol***

- To replace ***WEP*** and ***TKIP/WPA***.
- Uses ***AES*** with a ***128-bit key***.
- Preferred standard security protocol of ***802.11***.

***ANTENNA TYPES***

**Base Antenna**

- ❑ Also called ***straight*** or ***pole antenna***.
- ❑ Sends and receives signals from all directions.

**Rubber Duck Antenna**

- ❑ Sends and receives signals from all directions.

**Yagi Antenna**

- ❑ Sending and receiving signals from one direction.

**Antenna Placement**

- First, ***site survey*** must be performed.
- Select ***directional antennas*** to avoid broadcasting in areas where they do not wish to provide signal.

***Captive Portals***

- A captive portal is an authentication technique that redirects a newly connected wireless Web client to a ***portal access control page***.
- Displays acceptable ***use policy***, ***privacy policy***, and ***tracking policy***.

***Wi-Fi Security Procedure***

- ❑ Use ***Infrastructure mode*** rather than Ad Hoc Mode
- ❑ Change the default administrator password.
- ❑ Disable the SSID broadcast.
- ❑ Change the SSID to something unique.
- ❑ Enable MAC filtering if the pool of wireless clients is relatively small (< 20) and static.
- ❑ Consider using static IP addresses, or configure DHCP with reservations.

- ❑ Turn on highest form of authentication and encryption supported.
- ❑ Treat wireless as external access and separate the WAP from the wired networking using a FW.
- ❑ Treat wireless as an entry point for attackers and monitor all WAP-to-wired-network communications with an IDS.
- ❑ Require all transmissions between wireless clients and WAPs to be encrypted (VPN-Link).
- ❑ Treat wireless as remote access, and manage access using 802.1X.
- ❑ Enforce security using a ***certificate-based*** system to authenticate the connecting device, following the standard ***802.1X***.
- ❑ Use the ***SRTP-Protokoll*** to secure further your communication.

## *NAC - Network Access Control*

- NAC is a concept of controlling access to an environment through strict adherence to an implementation of security policy.
- There are two versions: ***Agent*** based systems and ***agent-less*** systems.

**Target:**
- Prevent/reduce zero-day attacks
- Enforce security policy throughout the network
- Use identities to perform access control

***Preadmission*** philosophie
***Postadmission*** philosophie

**Some of the items NAC check would include:**
- ❑ Existence of an anti-virus program and whether a scan has been recently executed
- ❑ Determination if the endpoint has a configured firewall or IPS
- ❑ Determination if the corporate image for the device has been tampered with or changed
- ❑ Determination if the latest available virus signature updates are present
- ❑ Determination if there is an authorized version of the operating system
- ❑ Determination if the operating system and applications have been patched to an acceptable level

**NAC Challenges**
- Inconsistent access requirements affect the deployment.
- Network load increases as NAC evaluates hosts and supports the process of policy enforcement.
- Network devices like routers and switches must be compatible with the NAC solution.
- Establishing policies can be difficult in environments with a significant variety of devices.
- Scope and scalability are important concerns

## *FW - Firewalls*

- Essential tool to ***control network traffic***.
- Used to ***filter traffic***.

***USEFUL FEATURES***
Geo-Blocking
Rate Limiting
IP Reputation Detection
Signature Production

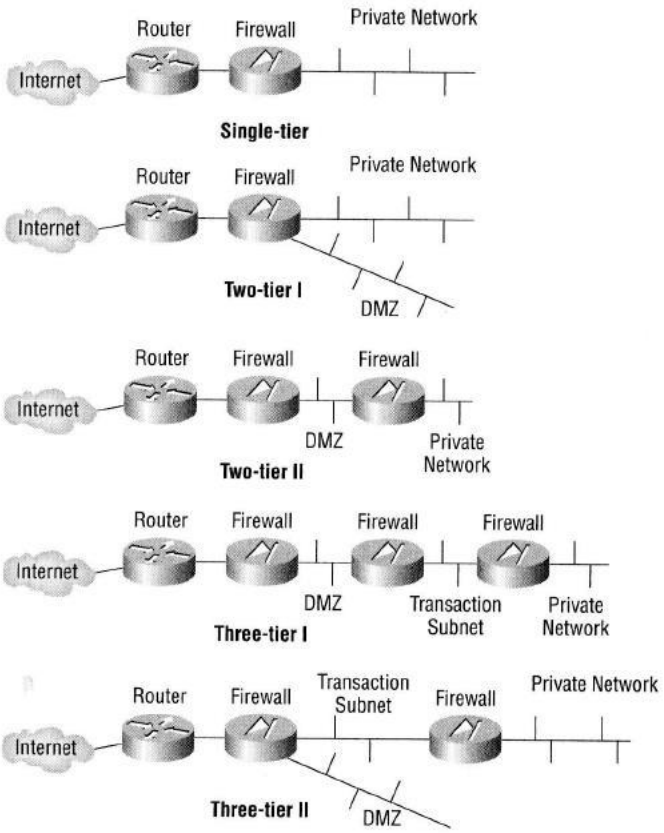



**Figure 11: Single- two- and three tier FW**

***Static Packet-Filtering FW***

- ***First-generation*** FWs.
- The most ***rudimentary*** type of all.
- Operates on ***Layer 3***.
- They are also called ***screening routers*** or ***common routers***.
- Filters traffic by examining data from a ***message header***.
- Rules are based on ***source***, ***destination*** and ***ports***.

***Stateful Inspection FW***

- Also called ***dynamic packet filtering FW***.
- Operates on ***Layer 3 and Layer 4***.
- Stateful inspection FWs generally operate more efficiently than application-level gateway FWs.

***Circuit Level Gateway FW***

- ***Second-generation*** FWs.
- Are used to establish ***communication sessions between trusted partners***.
- Operates on ***Layer 5***.
- Also called ***circuit proxies***.

***Application-Level Gateway FW***

- ***Second-generation*** FWs.
- Operates on ***Layer 7***.
- Also called a ***Proxy FW***.

***Multihomed FW***

- Filtering traffic coming into the private network as well as for protecting the identity of the internal client.

***Screened-Subnet FW***

- The screened subnet firewall is a ***variation of the dual-homed gateway*** and screened host firewalls.
- It can be used to locate each component of the firewall on a separate system, thereby achieving greater throughput and flexibility, although at ***some cost to simplicity***.
- But, each component system of the firewall needs to implement only a ***specific task***, making the systems less complex to configure.
- A screened subnet firewall is often used to establish a ***demilitarized zone (DMZ)***.

## *Endpoint Security*

- Expressed as "***the end device is responsible for its own security***."

## *IDPS - Intrusion Detection Prevention System*

- Sometimes called ***IPS***.
- An IPS system is placed ***in line*** with the traffic.
- Are network security appliances that monitor network or system activities for malicious activity.
- The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.
- Intrusion prevention systems are considered extensions of ***IDS*** because they both monitor network traffic and/or system activities for malicious activity.
- The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed ***in-line*** and are able to ***actively prevent or block intrusions*** that are detected. IDPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
- An IDPS also can ***correct cyclic redundancy check (CRC) errors***, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.
- An IPS includes all the capabilities of an IDS but can also take additional steps to stop or prevent intrusions.
- See NIST SP 800-94 this recommends placing all active IDS ***in line with the traffic*** so that they function as IPSs.

## *IDS - Intrusion Detection System*

- An IDS ***automates*** the inspection of logs and real-time system events to detect intrusion attempts and system failures.
- An IDS is intended as part of a ***defense-in-depth*** security plan.
- An IDS can have ***sensors*** or ***agents*** monitoring key devices such as routers and firewalls.
- The IDS use two methods of detecting intrusions. ***Knowledge-based detection*** and ***behavior-based detection*** (Profile-based systems).
- ***Knowledge-based detection*** is also called ***signature-based detection***.
- There are two types of IDS. ***Host-based IDS (HIDS)*** and ***network-based IDS (NIDS)***.
- An ***application-based IDS*** can monitor traffic between a web server and a database server looking for suspicious activity.
- If IP packets are detected with ***IP Source Address/Port*** are equal to ***IP Destination Address/Port***, the packets should be dropped.

## *Darknet*

- A darknet is a portion of allocated IP addresses within a network that are not used.
- It includes one device configured to capture all the traffic into the darknet.
- Since the IP addresses are not used, the darknet should not have any traffic at all.
- If an attacker is probing a network or malware is attempting to spread. the host in the darknet will detect and capture the activity.
- Domain-Names with the ending «***.onion***» are Darknets and can oly be visited with a special browser which hides any information about the visitors location (e.g TOR-Browser).

## *Honeypots/Honeynets*

- ***Honeypots*** are individual computers created as a trap for intruders.

- A ***honeynet*** is two or more network honeypots used together to simulate a network.
- They may be ***unpatched*** or have ***security vulnerabilities*** that administrators purposely leave open.
- Honeypots are also using ***Pseudo Flaws***.
- ***Padded Cells*** are similar to honeypots.

***Enticement***

- Placing a ***system*** on the @Internet with open security vulnerabilities and active services with known exploits is enticement.

***Entrapment***

- If you encourage someone into performing an illegal or unauthorized action, this is entrapment.

## *NIDES - Next Generation Intrusion Detection Expert System*

- Developed by Phillip Porras at the Information and Computing Sciences System Design Laboratory.

# SECURE COMMUNICATIONS and NETWORK ATTACKS

## *Secure Communication Protocols*

***SKIP - Simple Key Management for Internet Protocol***

- SKIP was ***replaced by IKE*** in 1998.
- This is an encryption tool used to protect ***sessionless datagram protocols***.
- SKIP was designed to integrate with ***IPSec***.
- It functions at ***Layer 3***.
- It is a ***hybrid Key distribution protocol***.
- Developed by the ***IETF*** Security Working Group for the ***sharing of encryption key***.

***swIPe - Software IP Encryption***

- ***Layer 3*** protocol.
- Provides ***authentication***, ***integrity*** and ***confidentiality***.

***S-RPC - Secure Remote Procedure Call***

- ***Authentication service***.
- Means to prevent ***unauthorized execution of code*** on remote systems.

***SSL - Secure Sockets Layer***

- ***Encryption protocol*** developed by Netscape.
- Session oriented protocol that provides ***confidentiality*** and ***integrity***.
- Uses Message Authentication Code (MAC) for ***Message integrity***.
- SSL is superseded by ***TLS***.
- Uses TCP port ***443***.
- Relies on the exchange of server ***digital certificates*** to negotiate encryption/decryption.
- A combination of symmetric and asymmetric cryptography.
- SSL encryption takes place at the ***transport layer***.

**Functionality:**

- When a user accesses a web site, the browser retrieves the web servers' certificate and extracts the server's public key from it.
- The browser then creates a random symmetric key, uses the servers public key to encrypt it, and then sends the encrypted symmetric key to the server.
- The server the decrypts the symmetric key using its own private key, and the two systems exchange all future messages using the symmetric key to the server.

***Videos:***
https://youtu.be/iQsKdtjwtYI

***TLS - Transport Layer Security***

- Uses TCP port ***443***.
- Nickname ***SSL 3.1***
- TLS is the ***successor*** to the Secure Sockets Layer (SSL) and is based on SSL version 3.
- ***End-to-end encryption***.
- TLS provides ***privacy*** and ***data integrity*** between two communicating applications on a network.
- TLS is made up of two protocols to secure the communications.
  ***TLS Handshake Protocols*** that creates the connection using asymmetric and symmetric keys.
  ***TLS Record Protocol*** maintains the integrity of the communications using a hash function.
- Uses stronger ***authentication*** and ***encryption*** protocols than SSL.
- Supports secure ***client-server communications*** by preventing ***tampering***, ***spoofing*** and ***eavesdropping***.
- Supports ***one-way authentication***.
- Supports ***two-way authentication*** using ***digital certificates***.
- Can be implemented at lower layers, such as ***Layer 3*** to operate as a VPN (***OpenVPN***).
- Can be used to ***encrypt UDP*** and ***SIP*** connections.

***DTLS - Datagram Transport Layer Security***

- Actual version 1.2
- RFC: 6347
- DTLS is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
- The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees.
- The DTLS protocol datagram preserves the semantics of the underlying transport—the application does not suffer from the delays associated with stream protocols, but because it uses UDP, the application has to deal with packet reordering, loss of datagram and data larger than the size of a datagram network packet.
- Because DTLS uses UDP rather than TCP, it avoids the "TCP meltdown problem", when being used to create a VPN tunnel.

***SET - Secure Electronic Transaction***

- SET is based on ***RSA*** encryption and ***DES***.
- Originated by ***VISA*** and ***MasterCard*** as an @Internet card protocol using ***digital signatures***.

## *Authentication Protocols*

***CHAP - Challenge Handshake Authentication Protocol***

- Used over ***PPP links***.
- Encrypts ***usernames*** and ***passwords***.
- Periodically ***reauthenticates*** the remote system.

***PAP - Password Authentication Protocol***

- PAP transmits usernames and passwords in ***clear text***.

***EAP - Extensible Authentication Protocol***

- Framework for authentication.
- Supports smart cards, tokens and biometrics.

***PEAP - Protected Extensible Authentication Protocol***

- Is used to secure communications over 802.11.

***LEAP - Lightweight Extensible Authentication Protocol***

- ***Cisco*** propriety.
- LEAP is crackable.

## *Secure Voice Communications*

***VoIP - Voice over Internet Protocol***

## *Social Engineering*

- It is the means to break into the perfectly technically secured environment.
- Is one of the most effective tools attackers use to gain access to a system.
- The only way to protect against social engineering attacks is to ***teach users*** how to respond and interact with any form of communications.

## *Email Security Solutions*

***S/MIME - Secure Multipurpose Internet Mail Extension***

- Die S/MIME Verschlüsslung ist eine asymetrische Verschlüsselung/Signatur für ein- und ausgehende E-Mails auf Basis RFC 5751.
- Sie basiert auf persönlichen S/MIME Zertifikaten deren Vertraulichkeit und Integrität von öffentlichen Stellen (sogenannten Certificate Authorities CAs) bestätigt werden.

- Certificate is needed.
- Offers ***authentication (X.509)*** and ***confidentiality***.

**Providers:**
- ***QuoVadis:*** Secure E-Mail Zertifikat
- ***Sectigo:*** Secure E-Mail Zertifikat
- ***Avantec:*** ***SEPPmail***
- ***Post:*** ***IncaMail***

***MOSS - MIME Object Security Services***
- Provides ***authentication***, ***confidentiality***, ***integrity*** and ***nonrepudiation***.

***PEM - Privacy Enhanced Mail***
- Provides ***authentication***, ***confidentiality***, ***integrity*** and ***nonrepudiation***.

***DKIM - DomainKeys Identified Mail***
- See: www.dkim.org

***PGP - Pretty Good Privacy***
- See www.gnupg.org

***OpenPGP***
- OpenPGP ist asymetrisches Verschlüsselungsverfahren für ein-und ausgehende E-Mails auf Basis der RFCs 4880 und 3156.
- Erfunden wurde diese Technologie unter dem Namen Pretty Good Privacy (PGP) 1991 von dem Amerikaner Phil Zimmermann und ist nach wie vor ein verbreitetes Public Key Verfahren.

## *Remote Access - Security Management*

- The most reliable authentication method for remote access is ***Synchronous Token***.

***Synchronous token***
A synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and if expires if not entered in the acceptable time frame.

**Consider the following:**
- ❑ Remote Connectivity Technology
- ❑ Transmission Protection
- ❑ Authentication Protection
- ❑ Remote User Assistance

***PPP - Point-to-Point Protocol***
- Is the transport protocol of choice for dial-up Internet connections.
- Uses ***PAP*** and ***CHAP***.
- Is a full-duplex protocol used for the transmission of TCP/IP packets over various non-LAN connections, such as modems, ISDN, VPNs, Frame Relay and so on.
- PPP permits multiple network layer protocols to operate on the same communication link.

***SLIP - Serial Line Internet Protocol***
- Older technology to support communications over asynchronous serial connections.

## *Logon Abuse*

- Logon abuse can refer to legitimate users accessing services of a higher security level that would normally be restricted to them.
- Unlike network intrusion, this type of abuse focuses primarily on those users who might be legitimate users of a different system or users who have a lower security classification.

## *Masquerading*

- Is the term used when one user ***pretends to be another user***.

- An attacker socially engineering passwords from an ISP could be an example of masquerading.

## *Virtualization*

- Virtualization technology is used to host one or more operating systems within the memory of a single host computer.
- ***Cloud computing*** is ultimately a form of virtualization.

VMWare, MS Virtual PC, MS Hyper-V

## *Security Boundaries*

- A security boundary is the line of intersection between any two areas, subnets, or environments that have ***different security requirements or needs***.
- Once you identify a security boundary, you need ***to deploy mechanisms to control the flow of information across those boundaries***.

# MANAGING IDENTITY and AUTHENTICATION

| | |
|---|---|
| DAC | Discretionary Access Control |
| MAC | Mandatory Access Control |
| Role-BAC | Role-Based Access Control |
| Rule-BAC | Rule-Based Access Control |

## *Permissions*

- In general, permissions refer to the access granted for an object and determine ***what you can do with it***.

## *Rights*

- A right primarily refers to the ability to ***take an action*** on an object.

## *Privileges*

- Privileges are the ***combination*** of ***rights*** and ***permissions***.

## *Access Control*

- Access control is any hardware, software, or administrative policy or procedure that controls access to resources.
- Organizations implement access controls using a ***defense-in-depth strategy***.

1. Identify and authenticate users or other subjects attempting to access resources.
2. Determine whether the access is authorized.
3. Grant or restrict access based on the subject's identity.
4. Monitor and record access attempts.

**Main control types:**

- Preventive Control
- Detective Control
- Corrective Control

**Detective Control**

- System Monitor
- IDS
- Monitor detector

**Further control types:**

- Deterrent
- Recovery
- Directive
  E.g. Policy stating that employees may not spend time on social media websites.
- Compensation

**Implementation categories:**

- Administrative control / Management control
- Logical control / Technical control
- Physical control

***Assets***

Includes:

- Information
- Systems
- Devices
- Facilities
- Personnel

***Subject***

- A subject is an active entity that accesses a passive object to receive information from, or data about, an object. Subjects can be users, programs, processes. computers, computers, or anything else that can access resource.
- The subject is always the ***active entity*** that receives information's about, or data from, the ***passive object***.
- Simplified ***subject = user*** (as example).

***Object***

- An object is a passive entity that provides information to active subjects. Some examples of objects include files, databases, computers, programs, processes, printers and storage media.
- Simplified ***object = file*** (as example).

***Passwords***

- Type 1 authentication (something you know)

**Creating Strong Passwords:**

- Maximum Age
- Password Complexity
- Password Length
- Password History

***Passphrase***

Example: ***"I passed the CISSP exam" = "IP@$$edTheCISSPEx@am"***

***Cognitive Passwords***

- What is your birthday?
- What is your mother's maiden name?

***Smartcards***

- ***Type 2*** authentication (something you have)
- Most smartcards include a microprocessor and one or more ***certificates***.

**Hybrid Cards**

- A ***smartcard*** with ***two chips*** and the capability of utilizing both contact and contactless formats.

***Tokens***

- ***Type 2*** authentication (something you have)
- ***Password-generating*** device.
- Provides ***multifactor authentication***.
- There are ***synchronous dynamic password tokens*** and ***asynchronous dynamic password tokens***.

***Static Password Tokens***

- The device contains a password which is physically hidden (not visible to the possessor), but which is ***transmitted for each authentication***.
- The token authenticates the ***identity of the owner*** to the information system.
- This type is vulnerable to ***replay attacks***.

***Synchronous dynamic password token***

- A timer is used to rotate through various combinations produced by a cryptographic algorithm.
- The token and the authentication server must have ***synchronized clocks***.

***Biometrics***

- ***Type 3*** authentication (something you are)
- Used in ***physical access controls*** and ***logical access controls***.
- You can compare the overall quality of biometric devices with the ***CER - Crossover Error Rate***.
  The lower the ***CER***, the better the biometric system.
- Subjects typically accept a throughput rate (identification) of about ***6 seconds*** or faster.

**Iris scan**

- Lowest ***CER***
- Mit einer speziellen Kameras werden Bilder der Iris (Regenbogenhaut) des Auges aufgenommen, mit algorithmischen Verfahren die charakteristischen Merkmale der jeweiligen Iris identifiziert, in einen Satz numerischer Werte (Merkmalsvektor, engl. „Template“) umgerechnet und für die Wiedererkennung durch einen Klassifizierungsalgorithmus wie z. B. ein Neuronales Netz gespeichert bzw. mit einem oder mehreren bereits gespeicherten Templates verglichen.

*Source: Wikipedia*

**Retina Scan**

- Has the ***highest accuracy*** and is least accepted by users.
- A retinal scan is a biometric technique that uses unique patterns on a person's ***retina blood vessels***.
- It is not to be confused with other ocular-based technologies: ***iris recognition***, commonly called an "iris scan", and ***eye vein verification*** that uses scleral veins.
- Low occurrence of false positives
- Extremely low (almost 0%) false negative rates
- Highly reliable because no two people have the same retinal pattern
- Speedy results: Identity of the subject is verified very quickly

**Facial Recognition**

- Gesichtserkennung.
- A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source (*Source: Wikipedia*).
- SW: Mirametrix, Cubera Solutions GmbH (Dominik B.)

**Hand geometry**

- Hand geometry is a biometric that identifies users by the shape of their hands.
- Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.
- Hand geometry is very reliable when combined with other forms of identification, such as ***identification cards*** or ***personal identification numbers***.

*Source: Wikipedia*

**Voice pattern**

- Has the highest ***CER***.

**Fingerprints**

- A fingerprint is an impression left by the friction ridges of a human finger.
- The recovery of partial fingerprints from a crime scene is an important method of forensic science.
- Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal.

*Source: Wikipedia*

**Behavioral Biometrics**

- Verification of web and mobile users through keystroke detection and more.

***Error Ratings:***

- **Type 1**:When a valid subject is not authenticated.
  - The ratio of Type 1 Errors to validate authentications is known as the ***FRR - False Rejection Rate***.

- **Type 2**:When an invalid subject is authenticated.
  - The ratio of Type 2 Errors to validate authentications is called the ***FAR - False Acceptance Rate***.
  - This is the most critical type of error.

***MFA - Multifactor Authentication***

- Multi-factor authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism.
- Typically, at least two of the following categories: ***knowledge*** (something they know), ***possession*** (something they have), and ***inherence*** (something they are).

***Device Authentication***

- For ***BYOD*** systems, use ***device fingerprinting***.

**Device Fingerprinting Tools:**

- ***SecureAuth*** Identity Provider (IdP).

## *Identity Management*

***Centralized Access Control***

- Administrative overhead is lower because all changes are made in a single location and a single change affects the entire system.

***Decentralized Access Control***

- Administrative overhead is higher because changes must be implemented across numerous locations.

***SSO - Single Sign-On***

- Is a ***centralized access control technique*** that allows a subject to be authenticated only once on a system and to access multiple resources without authenticating again.
- Is very convenient for users, but it also ***increases security***.
- The ***primary disadvantage*** to SSO is that once an account is compromised, an attacker gains unrestricted access to all the authorized resources.
- If the ***SSO Service*** is not available, the access to dependent services is also restricted.

- Ein SSO-System setzt darauf, dass ein Benutzer immer genau eine einzige ***physische Identität*** besitzt (was der realen Welt abgeschaut ist). Innerhalb eines Systems kann der Benutzer als Individuum aber unter verschiedenen Benutzernamen (***logische Identität***) gespeichert sein. Im SSO-System werden diese zusammengeführt und verknüpft – auftreten unter Pseudonym (ohne Bekanntgabe der anderen Benutzerkennungen) wird somit unmöglich.

***Federation Identity Management***

- Is a form of ***SSO***.
- ***Identity management*** is the management of user identities and their credentials and Federal Identity Management extends this ***beyond a single organization***.
- Users in each organization can log on once in their organization and their credentials are matched with ***federate identity***. They can then use the ***federated identity*** to access resources in any other organization within the group.
- Federation identity systems often use the ***SAML*** and/or the ***SPML*** to meet the need of a common language.
- A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored ***across multiple distinct identity management systems***.
- ***Windows Communication Foundation (WCF)*** provides support for building and deploying distributed systems that employ federated security.

***XML - Extensible Markup Language***

- Goes beyond describing how to display the data by actually ***describing the data***.

***SAML - Security Assertion Markup Language***

- Is an XML-based language that is commonly used to exchange ***authentication*** and ***authorization (AA)*** information between federated organizations.
- It is often used to provide ***SSO*** capabilities for browser access.

***SPML - Service Provisioning Markup Language***

- Based on the Directory Service Markup Language (DSML).

***XACML - Extensible Access Control Markup Language***

- To define access control policies within an XML format and it commonly implements role-based access controls.

***2FA -Two-factor authentication***

- Two-factor authentication (also known as 2FA) is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a ***type of multi-factor authentication***.
- A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.
- 2FA provides ***identification*** of users via the combination of two different components, which could be something that the user knows, something that the user possesses or something that is inseparable from the user.

***Managing Sessions***

- When using any type of authentication system, it's important to manage sessions to prevent unauthorized access.

***Provisioning***

- An initial step in identity management is the ***creation of new accounts*** (identities) and provisioning them with ***appropriate privileges***.
- Creation of new accounts are also called "***enrollment*** or ***registration***".
- After hiring a person, usually ***HR*** completes initial identification and forwards a request to the IT department to create an account.
- New employees should be ***trained*** on organization security policies and procedures, and should ***sign an agreement*** committing to uphold the organization's security standards.

***Account Review***

- Accounts should be ***reviewed periodically*** to ensure that security policies are being enforced.
- Use scripts to identify users which have not logged in since more than ***30 days***.

***Excessive Privileges*** are users which have more privileges tan their assigned work tasks dictate.

***Creeping Privileges*** are user accounts where users accumulating privileges over time as job roles ans assigned tasks change.

***Account Revocation***

- When employees leave the organization for any reason, it is important to disable their user accounts as soon as possible.
- Accounts should be disabled by HR during the ***exit interview***.

## *Directory Services*

- A ***directory service*** is a centralized database that includes information about subjects and objects.

***LDAP - Lightweight Directory Access Protocol***

- See also: LDAPv3

- LDAP and centralized access control systems can be used to ***support SSO capabilities***.

- Das LDAP Protokoll definiert nur das Zugangsprotokoll zu Verzeichnisdiensten.
- In welcher Art die Informationen vom LDAP Server gespeichert werden, ist abhängig von der Serverimplementation.
- Die Daten können in einer eigens entwickelten Datenbank untergebracht sein oder auf eine oder mehrere existierende Datenquellen zugreifen.

- Weitere Verzeichnisdienste: ***NIS***, ***X.500***, ***NT User DB***

***Kerberos - Authentication Protocol***

- ***Ticket system***.
- ***Symmetric key cryptography*** (No public key)***.***
- ***Kerberos 5*** relies on ***symmetric-key cryptography*** using ***AES***.
- Offers an ***SSO solution*** for users and providers protection for ***logon credentials***.
- Provides ***confidentiality*** and ***integrity*** for authentication traffic using ***end-to-end security*** and helps prevent, against ***eavesdropping*** and ***reply attacks***.
- A ***ticket*** is an encrypted message that provides proof that a subject is authorized to access objects.
- Kerberos requires a ***database of accounts*** (Key Distribution Center).
- Steams from ***Greek mythology***: "A three-headed dog named Kerberos guards the gates to the underworld. The dog faces inward, preventing escape rather than denying entrance."
- Kerberos validates the ***timestamp***.
- The user sends their ***identification information*** and a ***timestamp*** and ***sequence number encrypted*** with the shared session key to the requested service, which then decrypts this information and compares it with the identification data the ***KDC*** sent it about this requesting user. If the data matches, the user is allowed access to the requested service.

**KDC - Key Distribution Center**

- The Key Distribution Center is the most important component within a Kerberos environment as it holds all ***users and services secret keys***.
- Jeder Active Directory-Domänencontroller dient als **Key Distribution Center** (KDC).

**TGT - Ticket Granting Ticket**

**TGS - Ticket Granting Service**

***Begriffe beim Kerberos:***

- Principal
- Bereich
- Geheimer Schlüssel
- Sitzungsschlüssel
- Echtheitsbestätigung
- Schlüsselverteilungscenter
- Privilege Attribute Certificate(PAC)
- Ticket

***Kerberos Authentication Flow***

- Nachdem ein Benutzer authentifiziert wurde erhält er ein **TGT** (Ticket Granting Ticket).
- Anhand des **Service Principal Name** (SPN) des angeforderten Servers stellt der **KDC** fest, dass der Dienst sich in derselben Domäne befindet.
- Das **KDC** stellt dem Benutzer anschliessend ein **Sitzungsticket** (TGT) für den Dienst bereit.

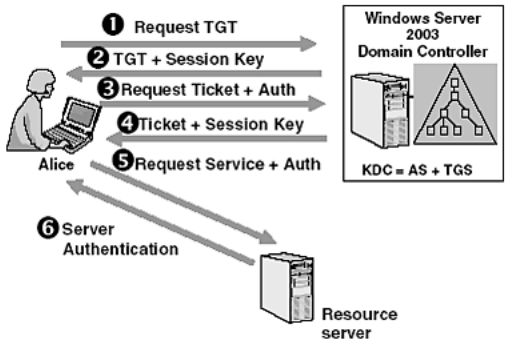



**Figure 12: Kerberos Authentication Flow**

***SESAME - Secure European System for Applications in a Multivendor Environment***

- Ticket based authentication system, developed by ***IBM***.
- In the professional security world SESAME is ***no longer a viable product***.
- Was developed to address some of the weaknesses in Kerberos and uses ***public key cryptography*** for the distribution of secret keys and provides ***additional access control support***.

***OAuth***

- Is an ***Access Granting Protocol***.
- Is an open standard designed to work with ***HTTP*** and it allows users to log on with ***one account (SSO)***.
- ***Google*** supports OAuth 2.0.

***Roles***
User, Application, API

***Grant Types***
Authorization Code Grant
Password Grant
Client Credntials Grant
Implicit Grant

***Video:*** OAuth 2.0 Introduction https://www.youtube.com/watch?v=CPbvxxslDTU

***Credential Management Systems***

- Storage space for credentials.

# PKI and CRYPTOGRAPHIC APPLICATIONS

**Key length:**

| | | | |
|---|---|---|---|
| RSA | 1024 bits | Public key | |
| DSA | 1024 bits | Public key | |
| Elliptic curve | 160 bits | Public key | El Gamal |
| FIPS 186-2 | | Public key | |

## *Key Management*

- The weakest link in the current encryption chain is the security of the keys.
- Keys may be stored centrally and use a facility such as a ***Key Distribution Center (KDC)***, whereby cryptography is used to distribute session keys in an encrypted manner.
- If a key is lost, there may not be the means to recover, unless the keys were provided to someone in the IT department as part of a policy.
- Some encryption products provide alternate means of retrieving data in the event of a lost key.
- Keys should also be protected while in storage by using strong access controls and should be securely archived for future retrieval.
- External providers of IT services may not want to take the legal liability of losing encryption keys.
- They sometimes establish clauses in their contracts designating a department, usually the IT service delivery or the information security program, to be responsible for managing the keys.

***Enrollment***

***Verification***

***Revocation***

- Certificate revocation List (CRL)
- CRLs are maintained by the various CAs.

## *ACME - Automatic Certificate Management Environment*

- Ist ein Protokoll zur automatischen Prüfung der Inhaberschaft einer ***Internet-Domain*** und dient der vereinfachten Ausstellung von digitalen Zertifikaten für ***TLS-Verschlüsselung***.
- Ziel der Umgebung ist es, die Zertifikate automatisiert und sehr kostengünstig auszustellen.
- Es wurde von der Internet Security Research Group (ISRG) für den Einsatz im Let's-Encrypt-Dienst definiert
- Das Protokoll basiert auf JSON-formatierten Meldungen, die über HTTPS ausgetauscht werden.
- Das Protokoll ist im März 2019 als RFC 8555 standardisiert worden.

## *PKI - Public Key Infrastructure*

**PKI haben die Aufgabe, in einer nicht vertrauenswürdigen Umgebung Vertrauen zu schaffen.**

- Single authority.
- Two Key (Asymmetric) Cryptosystem.
- Supports worldwide secure communication between parties that don't necessarily know each other prior to the communication.
- A PKI uses LDAP when integrating ***digital certifications*** into transmissions.
- A PKI is a group of technologies used to ***manage digital certificates*** during the certificate lifecycle.

**Provides:**

- Confidentiality
- Access control
- Integrity
- Authentication
- Nonrepudiation

**Cross certification**

- Allows entities in one PKI to trust entities in another PKI.
- This mutual trust relationship is typically supported by a cross-certification agreement between the CAs in each PKI.
- This agreement determines the responsibilities and liability of each party.
- A mutual trust relationship between two CAs requires that each CA issue a certificate to the other to establish the relationship in both directions.
- The path of trust is not hierarchal even though the separate PKIs may be certificate hierarchies.

***Entities and functions***

- CA - Certification Authority
- Registration Authority
- Certificate Repository
- Certificate Revocation System
- Key Backup and Recovery System
- Automatic Key Update
- Management of Key Histories
- Timestamping
- Client-Side Software

***Products:***

- GlobalSign
- PrimeKey - EJBCA PKI
  Open Source Certificate Authority (CA).
  EJBCA is platform independent and can easily be scaled out to match the needs of your PKI.
- SwissSign

***true-Xtender***

- Supplier: ***Keyon***
- true-Xtender Suite für Enterprise PKI
- Die true-Xtender Suite von Keyon ist eine umfassende Sammlung von Modulen, welche die Eigenschaften der Enterprise PKI erweitern.
- Alle Module werden auf Windows 2012 R2, 2016 und 2019 unterstützt und bieten volle Enterprise Funktionalität.
- Eine Schemaerweiterung ist nicht notwendig.
- Webbasierte, mandantenfähige Registrierungsstellen- und Service-APIs
- Zertifikatsverwaltung von Drittanbietern und automatische Registrierung für öffentliche CAs
- Durchsetzung von Richtlinien und Kontrolle des gesamten Zertifikatsmanagements

## *RSA - Rivest Shamir Adleman*

- See ***ANSI X9.31***
- ***Asymmetric algorithm***.
- ***Ronald Rivest***, ***Adi Shamir*** and ***Leonard Adleman*** proposed the ***RSA public key algorithm*** that remains a worldwide standard today.
- Developed in 1978 at ***MIT***.
- Does not deal with ***discrete logarithms***.
- Used for ***digital signatures***, ***key exchange*** and ***encryption***.
- Provides ***authentication*** and ***key encryption***.
- The security of this algorithm comes from the difficulty of factoring large numbers into their original ***prime numbers***.
- The public and private keys are functions of a pair of ***large prime numbers***, and the necessary activity requires to decrypt a message from ciphertext to plaintext using a private key is comparable to factoring a product into two prime numbers.

***RSA Key generation:***

- Choose two large prime numbers, **p** and **q**, of equal length, compute **p3q5n**, which is the public modulus.
- Choose a random public key, **e**, so that **e** and **(p-1)(q-1)** are relatively prime.
- Compute **e * d=1 mod(p-1)(q-1)**, where **d** id the private key.
- Thus, **d=e-1 mod((p-1)(q-1))**

## *Merkle-Hellman Knapsack*

- Merkle-Hellman was proven ineffective when it was broken in 1984.
- Is an ***asymmetric key*** algorithm.

## *DSS - Digital Signature Standard*

- Is an ***asymmetric key*** algorithm.
- Digital signatures do not provide ***encryption***.
- Detecting unauthorized modifications of data (integrity) and authenticate the identity of the signatories plus no-repudiation.

## *El Gamal*

- ***Asymmetric key*** encryption algorithm based on ***Diffie-Hellmann*** key exchange.
- ***DSA*** is a variant of El Gamal.
- ***Explicit signature.***
- Has a major disadvantage: "***The algorithm doubles the length of any message it encrypts.***"

## *ECC - Elliptic Curve Cryptography*

- The Elliptic Curve algorithm computes ***discrete logarithms*** of elliptic curves.
- A ***1088 bit RSA key*** is cryptographically equivalent to a ***160 bit elliptic curve*** cryptosystem key.

## *ECDSA - Elliptic Curve Digital Signature Algorithm*

- See ANSI x9.62
- ECDSA ist eine Variante des "Digital Signature Algorithm (DSA)", der Elliptische-Kurven-Kryptographie verwendet.

## *Digital Signatures*

- Digital signature process does not provide any privacy in and of itself.
- It only ensures that the cryptographic goals of ***integrity***, ***authentication*** and ***non-repudiation*** are met.
- Digital signatures provide a mechanism to verify that a message came from the sender, providing non-repudiation.
- This means someone sending a file or providing a digital signature cannot later claim they did not.

***BASIC PROCESS:***

1. A ***hash***, or ***message digest***, is created from the message that the person wants to send.
2. The ***message digest*** is encrypted with the ***sender's private key***.
3. The recipient decrypts the message digest using the ***sender's public key***.
4. The message digest is ***recomputed*** for the file.
5. The on-system message digest is compared to the message digest that was sent earlier.

***USE CASE:***

- Asymmetric algorithms are more computing intensive than symmetric algorithms.
- For this reason, asymmetric and symmetric algorithms are used in conjunction with each other.
- For example, if a message requires non-repudiation, the digital signature can be generated by creating the message digest much faster than encrypting the entire message using the private key.
- The contents of the message can be encrypted using the symmetric algorithms.

- Then the symmetric key can be provided using public/private key encryption.
- In this manner, the entire message is encrypted, and the symmetric or secret key is delivered securely.

## *Digital Timestamp*

- A digital timestamp binds a document to its creation at a particular time.
- Trusted timestamping is the process of securely keeping track of the creation and modification time of a document.
- According to RFC 3161 and ANSI ASC X9.95 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA).
- Used for contracts, research data, medical records…

## *MAC - Message Authentication Code*

- In order to protect against fraud in electronic fund transfer, the "Message Authentication Code (MAC)", ***ANSI X9.9***, was developed.
- A MAC is appended to the message before it is transmitted.

## *HMAC - Hashed Message Authentication Code*

- Implements a partial digital signature.
- It guarantees the ***integrity*** of a message during transmission.
- HMAC relies on a ***shared key*** and does not provide any ***nonrepudiation***.

## *UMAC - Universal Hashing Based MAC*

- Message authentication code

## *DES-CBC*

- Message authentication code

## *CERTIFICATE - Definition*

- Digital certificates provide communicating parties with the assurance that the people they are communicating with truly are ***who they claim to be***.

**Serverzertifikate:** Werden auf Hostnamen ausgestellt.
**Applikationszertifikate:** Werden für eine Domain ausgestellt.

***Certificate Errors***

| Fehlermeldung | Bedeutung |
|---|---|
| Das Zertifikat dieser Website wurde gesperrt. | BedeutungSie sollten dieser Website nicht vertrauen. Dies bedeutet häufig, dass das Sicherheitszertifikat von der Website in betrügerischer Weise abgerufen oder verwendet wurde. |
| Die Adresse dieser Website entspricht nicht der Adresse im Sicherheitszertifikat. | BedeutungEine Website verwendet ein Zertifikat, das für eine andere Webadresse ausgestellt wurde. Dies kann auftreten, wenn eine Firma verschiedene Websites besitzt und dasselbe Zertifikat für mehrere Websites verwendet. |
| Das Zertifikat dieser Website ist veraltet. | BedeutungDas aktuelle Datum liegt entweder vor oder nach dem Zeitraum, für den das Zertifikat gültig ist. Die Zertifikate von Websites müssen bei einer Zertifizierungsstelle verlängert werden, damit sie ihre Gültigkeit nicht verlieren. Veraltete Zertifikate können ein Sicherheitsrisiko darstellen. |
| Das Sicherheitszertifikat dieser Website stammt nicht von einer vertrauenswürdigen Quelle. | BedeutungDas Zertifikat wurde von einer Zertifizierungsstelle ausgestellt, die von Internet Explorer als nicht vertrauenswürdig eingestuft wird. Auf Phishingwebsites werden oft gefälschte Zertifikate verwendet, die diesen Fehler verursachen. |
| Internet Explorer hat ein Problem mit dem Sicherheitszertifikat dieser Website festgestellt. | BedeutungInternet Explorer hat ein Problem mit einem Zertifikat festgestellt, das nicht den in dieser Tabelle aufgeführten anderen Fehlern entspricht. Mögliche Ursachen hierfür wären, dass ein Zertifikat beschädigt ist, verfälscht wurde, in einem unbekannten Format vorliegt oder nicht gelesen werden kann. |

| Fehlermeldung | Bedeutung |
|---|---|
| | Wenn dieser Zertifikatfehler auftritt, sollten Sie der Identität der Website nicht vertrauen. |

***CA - Certificate Authorities***

- CAs are the glue that binds the PKI together.
- Choose a CA that is ***widely trusted***.
- If you do not recognize and trust the name of the ***CA*** that issued the certificate, you shouldn't place any trust in the certificate at all.
- If you configure your ***browser*** to trust a CA, it will automatically trust all the digital certificates issued by that CA.
- See the ***CPS*** - Certificate Practice Statement

**Widely Trusted CAs:**

- DigiCert
- Comodo Limited
- Entrust
- GeoTrust
- GlobalSign
- GoDaddy
- Network Solutions, LLC
- Symantec
- Starfield Technologies
- Thawte

***CPV - Certification Path Validation***

- ***RFC 5280*** defines a standardized path validation algorithm for ***X.509*** certificates, given a certificate path.

## *RAS - Registration Authorities*

## *TPM - Trusted Platform Module*

- Is an international standard for a ***secure crypto processor***, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
- TPM's technical specification was written by a computer industry consortium called Trusted Computing Group (TCG). International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standardized the specification as ISO/IEC 11889 in 2009.
- Software can use a Trusted Platform Module to ***authenticate hardware devices***. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it can perform ***platform authentication***.

## *OCSP - Online Certification Status Protocol*

- Provides ***real-time certification verification***.
- Is a standard for checking the revocation status of ***X.509 digital certificates***.
- It is described in ***RFC 6960***
- Formally known as the ***TLS Certificate Status Request extension***.
- Appends a ***time stamped OCSP response*** signed by the CA to the initial TLS handshake, eliminating the need for clients to contact the CA, with the aim of ***improving both security and performance***.

## *SCEP - Simple Certificate Enrollment Protocol*

- Is a protocol standard used for ***certificate management***.
- The protocol is designed to make the ***issuing of digital certificates as scalable as possible***.
- The idea is that any standard network user should be able to request their digital certificate electronically and as simply as possible.

- These processes have usually required intensive input from network administrators, and so have not been suited to large-scale deployments.

### *Steganography*

- Is the art of using cryptographic techniques to embed secret messages within another message.
- Often used for ***espionage*** and ***child pornography***.

### *DRM - Digital Rights Management*

- To enforce copyright restrictions on digital media such as music, movies and books.

#### *Music DRM*

- ***Napster*** and ***Kazaa*** are using DRM to revoke a user's access to download music when their subscription period ends.

#### *Movie DRM*

CSS - Content Scrambling System
AACS - Advanced Access Content System

#### *Video Game DRM*

#### *Document DRM*

- Organizations may also use DRM to protect the security of sensitive information stored in PDF files.

***Common permissions restricted by document DRM solutions:***

- Reading a file
- Modifying the contents of a file
- Removing watermarks from a file
- Downloading/saving a file
- Printing a file
- Taking screenshots of a file content

#### *E-Book DRM*

- Adobe offers Adobe Digital Experience Protection Technology (ADEPT) for E-Books.

## CRYPTOGRAPHY and SYMMETRIC KEY ALGORITHMS

- All cryptography relies on algorithms.
- Kerchoff principal
- Security through obscurity.

| | |
|---|---|
| P | Plaintext |
| C | Ciphertext |
| Keys | |
| Key Space | |
| Bit Size | |

### *Encryption - Definition*

- Encryption is the process of making data unreadable and unusable.
- To use or read the encrypted data, it must be decrypted, which requires the use of a secret key.
- There are two top-level types of encryption: ***Symmetric*** and ***Asymmetric***.
- Encryption is typically approached in two ways: encryption at ***rest*** and encryption in ***transit***.

Use Industry standard algorithms, such as: ***DES***, ***IDEA***, ***Blowfish***, or ***RC5***.

**Basic rule e.g. Encrypted Email:**
- If you want to ***encrypt a message***, use the ***recipient's public key***.
- If you want to ***decrypt a message*** sent to you, use your ***private key***.

**Basic rule e.g. Digital Signature:**
- If you want to ***digitally sign a message*** you are sending to someone else, use your ***private key***.
- If you want to ***verify the signature*** on a message sent by someone else, use the ***sender's public key***.

### *Transport Encryption*

SSL → Unsecure
TLS
IPSec

### *Circuit Encryption*

- ***Link-encryption*** and ***end-to-end encryption***.
- The critical ***difference*** between ***link-encryption*** an ***end-to-end encryption*** is that in ***link-encryption***, all the data, including the trailer, address and routing data is also encrypted.

### *Link Encryption*

- Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit.
- Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted.
- The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods.
- Link encryption, which is sometimes called online encryption, is ***usually provided by service providers*** and is incorporated into network protocols.
- All of the information is encrypted, and the packets must be decrypted at each hop so the router, or other intermediate device, knows where to send the packet next.
- The router must decrypt the header portion of the packet, read the routing and address information within the header, and then re-encrypt it and send it on its way.

### *CBC - Cipher Block Chaining Mode*

### *CFB - Cipher Feedback Mode*

### *OFB - Output Feedback Mode*

### *CTR - Counter Mode*

### *Blowfish*

- ***Bruce Schneier's*** Blowfish ***block cipher*** is another ***alternative*** to ***DES*** and ***IDEA***.
- This ***symmetric cipher*** splits messages into ***blocks of 64 bits*** and encrypts them individually.

### *Skipjack*

- Is an algorithm used for ***encryption***.

### *Twofish*

- Is an algorithm used for ***encryption***.

- ***Symmetric block cipher*** used for encryption.

## *RC - Rivest Cipher*

- ***Symmetric***-key cipher
- Designed by ***Ronald Rivest***

## *Symmetric Encryption*

- Symmetric key encryption utilizes an algorithm that uses a single, shared key to encrypt and decrypt the message.
- Symmetric key encryption is also called private key, shared key, secret key, single key, or same key encryption.
- One party encrypts the message using a key and the receiving party decrypts the message using the same key.
- The limitation of this approach is that the key must be securely shared with the party that will be decrypting the message.
- This usually means supplying an unencrypted message, typically through a different means than the message was delivered, such as fax, voicemail, overnight delivery, or in person.
- Relay on a "***Shared Secret***"
- ***Key distribution*** is a major problem
- Does not implement ***nonrepudiation.***
- ***Not scalable***.
- Key must be ***regenerated*** often.

***Examples of symmetric key algorithms:***

AES - Advanced Encryption Standard

128, 192, or 256-bit key length.
Replaced the DES and the 3DES (known as Triple DES)
standard is stronger and used in many products today.

DES - Data Encryption Standard

64-bit block cipher, 56 bits make up the true key and 8 bits are used for parity.
DES modes:
ECB - Electronic Code Book
CBC - Cipher Block Chaining
CFB - Cipher Feedback
CTR - Counter Mode

3DES - Triple DES

Blowfish (often used in SSH)

| Name | Block Size | Key Size |
|---|---|---|
| AES | 128 | 128, 192, 256 |
| Blowfish | 64 | 32-448 |
| DES | 64 | 56 |
| 3DES | 64 | 112 or 168 |
| IDEA (used in PGP) | 64 | 128 |
| RC2 - Rivest Cipher 2 | 64 | 128 |
| RC4 - Rivest Cipher 4 | Streaming | 128 |
| RC5 - Rivest Cipher 5 | 32, 64, 128 | 0-2'040 |
| Skipjack | 64 | 80 |
| Rijndael | Variable | 128, 192, 256 |
| Twofish | 128 | 1-256 |

**Figure 13: Symmetric memorization chart**

## *Asymmetric Encryption*

- ***Public key algorithms***.
- Every user maintains both a ***public key*** and a ***private key***.

- Asymmetric encryption was successfully demonstrated with the Public Key Diffie-Hellman Algorithm introduced in 1976 and then the RSA Algorithm (Rivest, Shamir, and Adelman) in 1977.
- Asymmetric encryption is also known as ***public/private key encryption***.
- It uses keys in pairs to encrypt and decrypt information.
- One of the keys is kept secret and is called the ***private key***, while the other is made public and known as the ***public key***.

***Functionality:***

- An individual can send a message to another individual by encrypting the message with the ***recipient's public key***.
- Since the keys are in pairs that are mathematically linked by factors of very large prime numbers, the only key that can decrypt the message is the recipient's private key for that public/private key pair.
- This provides integrity and confidentiality, as the message cannot be decrypted with only the private key.
- This differs from the symmetric key encryption, where only one key is used to encrypt and decrypt.
- The advantage of this approach is that a secret key does not have to be shared, thus taking care of the problem of sharing the symmetric keys.

## *Hash*

- Hash functions are used to guarantee ***communication integrity***.

***Hashing Algorithms***

- ***MD2***, ***MD4*** and ***MD5*** algorithms are no longer accepted as suitable ***hashing functions***.

| | |
|---|---|
| SHA-0 | |
| SHA-1 | Weak |
| SHA-2 | |
| SHA-512 | |
| MD2 | Should no longer be used. |
| MD4 | |
| ***MD5*** | |
| HMAC | |
| HAVAL | |

## *Goals of Cryptography*

- ***Confidentiality***
- ***Integrity***
- ***Authentication***
- ***Nonrepudiation:*** Preventive Control

## *Caesar Cipher*

- Rotate 3 (ROT3)
- To encrypt a message, you simply shift each letter of the alphabet three places to the right.
- ***Stream cipher***.

## *Flag Signals*

- Developed by Dr. Albert J. Myer

## *Enigma*

- This machine used a series of three to six rotors to implement an extremely complicated substitution cipher.
- The Allied forces started ***Ultra*** to attack the Enigma codes.

### *Logical Operations*

| | |
|---|---|
| ^ | AND |
| v | OR |
| ~ or ! | NOT |
|  | XOR |
| mod | Modulo Function |

### *Transposition Ciphers*

### *Substitution Ciphers*

### *One-Time Pads*

- Are also known as ***Vernam Ciphers***.
- Each one-time pad must be used ***only once***.
- One-time pads are awkward to implement because they require the physical exchange of pads.
- Each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition.
- ***Practical problems*** have prevented one-time pads from being widely used.

### *Running Key Ciphers*

### *Digital Envelope*

- A ***digital envelope*** is another term used to describe ***hybrid cryptography***.
- A message encrypted with a ***secret key*** attached with the message.
- The ***secret key*** is encrypted with the ***public key of the receiver***.

### *Block Ciphers*

- See also ***IDEA***.
- The ***IDEA*** algorithm is patented by its ***Swiss developers***.
- Block ciphers use ***symmetric keys***.

### *DEA - Data Encryption Algorithm*

- Is the algorithm that fulfills ***DES***, which provides ***encryption***.

### *IDEA - International Data Encryption Algorithm*

- Developed by ***ETH Zürich*** and ***Ascom Systems AG***
- ***Block Cipher***
- ***Symmetric-key*** algorithm
- Operates on ***64-bit blocks***, which is divided into ***16 smaller blocks***, and each has ***eight rounds*** of mathematical functions performed on it.

### *Stream Ciphers*

- Operate on ***one character*** or ***bit*** of a message at a time.
- ***Caesar cipher*** is an example of a stream cipher.
- Can also operate as a type of ***block cipher***.

***RC4*** is a stream cipher.

### *Polyalphabetic Cipher*

- A polyalphabetic cipher makes use of more than one alphabet to conquer ***frequency analysis***.

### *Diffie-Hellman Algorithm*

- Is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle.
- D-H is one of the earliest practical examples of public key exchange implemented within the field of cryptography.
- Traditionally, secure encrypted communication between two parties requires that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier.
- The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.
- This key can then be used to encrypt subsequent communications using a symmetric key cipher.

# SECURITY VULNERABILITIES, THREATS and COUNTERMEASURES

- Most of the ***security architectures*** and design elements are based on a ***solid understanding*** and implementation of ***computer hardware***.

## *Assess and Mitigate Security Vulnerabilities*

### *Hardware*

- The term hardware encompasses any tangible part of a computer that you can reach out and touch, from the keyboard and monitor to its CPU, storage media and memory chips.

**Data Storage Media**

**Viability Control concerns:**

- Marking
- Handling
- Storage

### *Processor*

**Multitasking**

In computing, multitasking means handling two or more tasks simultaneously.
Is normally coordinated by the OS.

**Multiprocessing**

More than one CPU available.
A single computer with more than one CPU is called symmetric multiprocessing (SMP).
Massively Parallel Processing (MPP) different systems with own OS.

**Multiprogramming**

Requires specially written software that coordinates its own activities and execution through OS:

**Multithreading**

Permits multiple concurrent tasks to be performed within a single process.

**Protection Rings**

- From a security standpoint protection rings ***organize code and components*** in an operating system into concentric rings.
- The deeper inside the circle, the higher the privilege level.
- Most modern OS use a four-ring model (0 - 3).

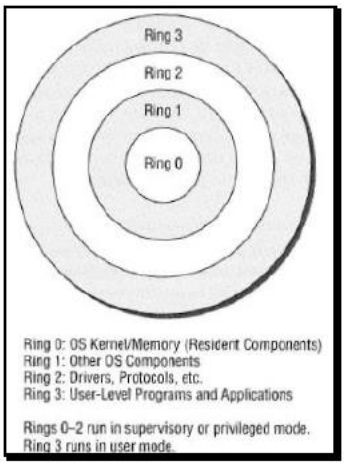



**Figure 14: Four Ring Model**

## *Database Security*

- Aggregation
- Inference
- Data Mining and Data Warehousing
- Data Analytics
- Large Scale Parallel Data Systems

## *Distributed Systems*

- In general, safeguarding distributed environments means understanding the vulnerabilities to which they're subject and applying appropriate safeguards.

### *Cloud Computing*

- The biggest concern with grid computing is that the content of each work packet is potentially exposed to the world.

**Hybrid Cloud**

- Mix of private cloud and public cloud service.

### *Grid Computing*

See: Systems Engineering.docx

### *P2P - Peer to Peer*

## *ICS - Industrial Control Systems*

- An industrial control system is a form of computer-management device that controls industrial processes and machines.

## *Web-Based Systems*

- See: OWASP - Open Web Application Security Project

### *SAML - Security Assertion Markup Language*

- Is often used to provide a "***Web-Based SSO***" solution.
- Is an XML-based open standard data format for ***exchanging authentication and authorization data*** between parties between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.
- The single most important requirement that SAML addresses is ***web browser single sign-on (SSO).***
- Single sign-on solutions are common at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies.

The SAML specification defines three roles:

- the ***principal (typically a user)***
- ***the identity provider (IdP)***
- ***and the service provider (SP)***.

## *Mobile Systems*

- Mobile devices are common targets of hackers and malicious code.

### *Android*

- Based on Linux
- Source code is made open source by Apache license.

### *iOS*

- Mobile device OS from Apple.

## *Mobile Device Management (MDM)*

- Due to the growth of malware an ***application whitelisting*** approach is one of the few options remaining that shows real promising in protecting devices and data.

***BYOD - Bring Your Own Device***

- Although BYOD may improve employees moral and job satisfaction, it ***increases security risk*** to the organization.
- The ***BYOD policy*** should define what support will be provided by the company and ehat support is left to the individual an if relevant, their service provider.
- The ***BYOD policy*** should address ***privacy*** and ***monitoring***.

## *Embedded Devices and Cyber-Physical Systems*

- An ***embedded system*** is a computer implemented as part of a larger system.
- ***Cyber-Physical systems*** refer to devices that offer a computational means to control something in the physical world.

**Examples:**

- Printer
- Smart TVs
- HVAC Controls
- Smart Appliances
- Smart Thermostats

## *Essential Security Protection Mechanisms*

## *Common Architecture Flaws and Security Issues*

- Covert Channels
- Attacks Based on Design or Coding Flaws

# SECURITY ASSESSMENT and TESTING

## *Security Testing*

- Security test ***verify*** that a control is functioning properly.
- The test includes ***automated scans***, ***tool-assisted penetration tests*** and ***manual attempts*** to undermine security.
- First develop the testing strategy.

## *Security Assessments*

- Security assessments are ***comprehensive reviews*** of the security of a system, application or other tested environment.
- The main ***work product*** of a security assessment is normally an ***assessment report*** addressed ***to management*** that contains the results of the assessment in ***nontechnical language*** and concludes specific ***recommendations*** for improving the security of the tested environment.

## *Security Audits*

- Must be performed by ***independent auditors***.
- Auditors generally have ***carte blanche*** access to all information within an organization and security staff should comply with those requests, consulting with management as needed.

**Internal Audits**

**External Audits**

- Enst & Young
- Deloitte & Touche
- PricewaterhouseCoopers
- KPMG

## *Vulnerability Assessment*

- Vulnerability assessments are some of the most important ***testing tools*** in the information security professional's toolkit.
- ***Vulnerability scans*** and ***penetration tests*** provide security professionals with a perspective on the weakness in a system or application's technical controls.

***Vulnerability Scans***

- ***Automatically probe systems***, applications and networks looking for weaknesses that may be exploited by an attacker.
- Probe for the presence of a vulnerability and do not normally ***take offensive*** action against the targeted system.
- ***Vulnerability scanners*** are software tools used to test systems and networks for known security issues.
- ***Attackers*** use vulnerability scanners to detect weaknesses in systems and networks, such as ***missing patches*** or ***weak passwords***.
- Vulnerability scanners use large ***repositories*** of vulnerabilities to identify ***misconfigurations*** or ***exploitable software***.

**Network Discovery San**

- See: nmap, nessus

TCP SYN Scanning
TCP Connect Scan
TCP Ack Scan
Xmas Scan

**Network Vulnerability Scan**

- Network vulnerability scans go deeper than discovery scans.
- This tools contain databases of thousands of known vulnerabilities.

- One way to improve the accuracy of the scanning and reduce false positive and false negative reports is to perform ***authenticated scans*** of systems.

**Web application vulnerability scan**

See: Nessus

- ***Web vulnerability scans*** are an important component of an organization's security assessment and testing program.

**Detecting:**
SQL injection attacks
Cross site scripting (XSS)
Cross site forgery (XSRF)

## *Penetration Testing*

- Often shortened as ***pentest***.
- See also ***NIST SP 800-115***.
- The penetration test goes beyond vulnerability testing techniques because it attempts to ***exploit systems***.
- Require focused attention from ***trained security professionals***, to a much greater extent than vulnerability scans.
- Penetration testers commonly use a tool called ***Metasploit***.
- Penetration tests are ***time consuming*** and require ***specialized resources***.
- Many penetration tests start with a ***vulnerability assessment***.
- ***Preventive measure*** an organization can use to counter attacks.
- Penetration tests need ***approval of senior management***.
- Penetration testing is the process of attempting to gain access to resources ***without knowledge*** of usernames, passwords, and other normal means of access.
- Penetration testing can occur in the form of ***external tests*** conducted by a third party or as ***internal tests***.

**Risks of Penetration Testing**

- Some methods can cause outages.
- Ideally, penetration tests should stop before they cause any actual damage.
- Whenever possible. testers perform penetration tests on a test system instead of a live production system.

***White Box Penetration Test***

- Provides the attackers with detailed information about the systems they target.

***Grey Box Penetration Test***

- Partial knowledge test.

***Black Box Penetration Test***

- Does not provide any information prior to the attack.

***Guide for Pentesting:***

- ❑ How often to test
- ❑ Defining goals
- ❑ Team considerations
- ❑ Creating response plans
- ❑ Know your targets
- ❑ Understand the attack path
- ❑ Consultant or self-assessment choices
- ❑ Which assets are at risk

## *Software Testing*

- One of the most critical components of a software testing program is conducting ***code review*** and ***testing***.

***Code Review***

- Is the ***foundation*** of software assessment programs.
- Also known as ***peer review***.
- See also the ***Fagan inspection***.
- ***Each company*** should adopt a code review process that suites its business requirements and software development culture.

***Static Testing***

- Static testing evaluates the security of software ***without running it*** by analyzing either the source code or the compiled application.
- Usually automated tools are used to detect for example ***buffer overflows***.

***Dynamic Testing***

- Dynamic testing evaluates the security of software in a ***runtime environment*** and is often the only option for organizations deploying applications written by someone else.

***Fuzz Testing***

- Fuzz testing is a specialized ***dynamic testing technique*** that provides many different types of input to software to stress its limits and find previously undetected flaws.

**Mutation (Dumb) Fuzzing**

**Generalization (Intelligent) Fuzzing**

***Interface Testing***

**Application Programming Interfaces (APIs)**

**User Interfaces (UIs)**

GUIs and command line interfaces.

**Physical Interfaces**

***Misuse Case Testing***

- Also called ***abuse case testing***.

***Test Coverage Analysis***

- To estimate the ***degree*** of testing conducted against the new software.

$$test\ coverage = \frac{\text{number of use cases tested}}{total\ number\ of\ use\ cases}$$

***Top-Down Testing***

- In this approach testing is conducted from main module to sub module. if the sub module is not developed a temporary program called STUB is used for simulate the submodule.

**Advantages:**

- Advantageous if major flaws occur toward the top of the program.
- Once the I/O functions are added, representation of test cases is easier.
- Early skeletal Program allows demonstrations and boosts morale.

**Disadvantages:**

- Stub modules must be produced
- Stub Modules are often more complicated than they first appear to be.
- Before the I/O functions are added, representation of test cases in stubs can be difficult.
- Test conditions ma be impossible, or very difficult, to create.
- Observation of test output is more difficult.

- Allows one to think that design and testing can be overlapped.
- Induces one to defer completion of the testing of certain modules.

***Bottom-Up Testing***

- In this approach testing is conducted from sub module to main module, if the main module is not developed a temporary program called DRIVERS is used to simulate the main module.

**Advantages:**

- Advantageous if major flaws occur toward the bottom of the program.
- Test conditions are easier to create.
- Observation of test results is easier.

**Disadvantages:**

- Driver Modules must be produced.
- The program as an entity does not exist until the last module is added.

## *Security Management Processes*

### *Log Reviews*

- ***SIEM*** systems play an important role in these processes.

### *Account Management*

- Account management reviews ensure that users only retain authorized permissions and that unauthorized modifications do not occur.
- One way to perform account management is to conduct a full review of all accounts.

### *Backup Verification*

- Inspecting the results of backups.

### *KPI - Key Performance Indicators*

- KPIs are performance measures that ***indicate progress toward a desirable outcome***.
- In strategic planning, KPIs monitor the implementation and effectiveness of an organization's strategies by highlighting gaps between actual and targeted performance.
- Ultimately, KPIs are a metric used to evaluate critical success factors.
- KPIs defined for the security program must reflect the organization's goals and objectives.
- The organization should develop a unique set of KPIs to define the expected outcome in each domain.
- For example, the CIO will have outcomes defined for IT service delivery, the CFO will have outcomes defined for enterprise financial management, and sales will have outcomes defined in terms of quotas and revenue generation.
- Each of these programs provides input into the KPIs developed for security.
- Like any evaluation in the security program, the quality of the measurements is important.
- The KPIs that measure performance of the information security strategy must yield quantifiable information.
- The data must also be readily obtainable, and the data collection process to support the evaluation should be repeatable.
- Finally, the KPI measurements must be useful for tracking performance and directing resources.
- KPI must be quantifiable because the measurements of performance cannot be subjective if the organization intends to determine if performance gaps exist, which would require adjustments in the strategy.
- Beyond the general characteristics of good metrics, KPIs must be ***verifiable*** and ensure data collection ***accuracy***.

#### *Good KPIs*

- ❑ Objective methods to see if the strategy is working
- ❑ Comparison to gauge performance change over time
- ❑ Tools to focus attention on what matters most to success
- ❑ Measurement of accomplishments, not just of the work that is performed
- ❑ Common language for communication
- ❑ Tools to reduce intangible uncertainty
- ❑ Measurement of the right things

### *Key Performance and Risk Indicators*

- Useful is a manager ***dashboard*** with all the key information's.

- ❑ Number of open vulnerabilities
- ❑ Time to resolve vulnerabilities
- ❑ Number of compromised account
- ❑ Number of software flaws detected in preproduction scanning
- ❑ Repeat audit findings
- ❑ User attempts to visit known malicious sites

# MANAGING SECURITY OPERATIONS

- The primary purpose for security operations practices is to safeguard information assets that reside in a system.
- ***Senior management*** has a direct responsibility to exercise ***due care*** and ***due diligence***.
- ***Separation of duties and responsibilities*** ensures that no single person has total control over a critical function or system.

## *Need to Know*

- Imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks.
- The primary purpose is to keep secret information secret.
- Limit the people who know, and you increase the chances of keeping it secret.

## *Least Privilege*

**Everyone can do everything they need to do, and NOTHING MORE!**
*Source: SANS*

- The principle of ***least privilege*** states that subjects are granted only the privileges necessary to perform assigned work tasks and no more.
- ***Privileges*** in this context includes both ***permissions*** to data and ***rights*** to perform tasks on the system.
- The principle of least privilege relies on the assumption that all users have a ***well-defined job description*** that personnel understand.
- Means an individual should have ***just enough permissions and rights to fulfill his role in the company*** and no more.

## *Separation of Privilege*

## *Segregation of Duties*

- Ensuring that the user alone does not have sufficient rights to subvert an important process.

## *Two-Person Control*

- Often called the ***two-man rule or dual control or "Vier-Augen Prinzip".***
- Similar to ***segregation of duties***.
- It requires the ***approval of two individuals*** for critical tasks.

## *Job Rotation*

- ***Detective administrative control***.
- Using job rotation as a security control provides ***peer review***, ***reduces fraud*** and enables ***cross-training***.

## *Mandatory Vacations*

- This provides a form of ***peer review*** and helps detect ***fraud*** and ***collusion***.
- Similar to the benefits of ***job rotation***.

## *Monitor Special Privileges*

- Helps to ensure that users granted with special privileges do not abuse them.

## *Managing the Information Life Cycle*

## *MSA - Master Service Agreement*

- An MSA is a contracting artifact that details the responsibilities and obligations of two parties to each other.
- MSAs are the general operating rules for all contracts.
- Rates and terms are found in the individual contracts.
- MSAs provide guiding legal requirements for all contracts and services.
- Subordinate agreements like SLAs, purchasing agreements, purchase orders, and SOWs provide additional details.

## *SLA - Service Level Agreements*

- A SLA is an agreement between an organization and an outside entity, such as a vendor.
- Organizations sometimes use a ***memorandum of understanding (MOU)***. MOUs document the ***intention*** of two entities to work together toward a ***common goal***. MOUs are ***less formal*** and doesn't include any ***monetary penalties***.
- Organizations use also ***interconnection security agreements (ISAs)***. ISAs define the ***technical requirements*** of a connection. See the ***NIST*** regulation.

## *SOW - Statement of Work*

- A Statement of Work (SOW) is a document that defines the scope of a project, specific deliverables, scheduling, and additional responsibilities as required by the purchasing company.
- A SOW is a binding contract between two parties that is more specialized in scope, language, and deliverables.

## *VMgmt - Vendor Management*

- The term vendor management is used when describing the activities included in ***researching*** and ***sourcing*** vendors, ***obtaining quotes*** with pricing, ***capabilities***, ***turnaround times***, and ***quality of work***, ***negotiating contracts***, ***managing relationships***, ***assigning jobs***, ***evaluating performance***, and ***ensuring payments are made***.
- The organization should evaluate the capabilities of the vendor to ensure satisfactory sanitization and destruction of data is possible.

## *Addressing Personnel Safety*

## *Provisioning and Managing Resources*

## *Managing Hardware and Software Assets*

- Use inventories.

#### *Hardware Inventories*

- Bar-Codes
- RFID

#### *Software Licensing*

- Any type of license key is highly valuable to an organization and should be protected.
- See Microsofts ***ConfigMgr*** tool.

#### *Protecting Physical Assets*

- Fences, barricades, locked doors, guards, CCTV systems and much more.

#### *Managing Virtual Assets*

- Virtual Machines (VMs)
- Software Defined Networks (SDNs)
- Virtual Storage Area Networks (VSANs)

***Managing Cloud Based Assets***

- One of the primary challenges is that these resources are outside the direct control of an organization, making it more difficult to manage the risk.
- When storing data in the cloud, organizations must ensure security controls are in place to prevent unauthorized access to data.
- The ***NIST*** provides standard definitions fo many cloud-based services.

***Media Management***

- Media management refers to the steps taken to protect media and data stored on media.

**SSDs**

**USB Flash Drives**

- To secure your USB Flash Drives you may use "***Hardware Encryption***" or "***Software Encryption***".

***Hardware Encryption:***

- Is more secure.

***Software encryption:***

- BitLocker

**Tape Media**

**Mobile Devices (Includes SmartPhones and tablets)**

***Managing Media Life Cycle***

- Once backup media has reached its ***MTTF***, they should be destroyed.

## *Managing Configuration*

- Configuration management helps ensure that systems are deployed in a secure consistent state and maintain this state throughout their lifetime.

***Baselining***

- When systems are deployed in a secure state with a secure baseline, they are much more likely to stay secure.

***Using Images for Baselining***

- It's common to combine imaging with other automated methods for baselining.

## *Managing Change*

- Change management helps reduce unanticipated outages caused by unauthorized changes.
- Most of the change management concepts are derived from ***ITIL***.

***Security Impact Analysis***

***Versioning***

- Versioning typically refers to version control used in ***software configuration management***.

***Configuration Documentation***

- Configuration documentation identifies the ***current configuration*** of systems.
- It identifies who is ***responsible*** for the system and the ***purpose*** of the system and lists ***all changes*** applied to the baseline.
- The challenge with the documentations is to have it accessible during an ***outage***.

## *Managing Patches and Reducing Vulnerabilities*

- ***Patch management*** and ***vulnerability management*** work together to help protect an organization against emerging threats.

- A ***vulnerability*** is a ***weakness*** which could potentially be exploited.

***System Hardening***

- System hardening is the application of security configurations, software, or other protections.
- Operating systems, such as Windows, UNIX, Linux, iOS, Android, are typically configured to operate on a ***least functionality principle***.
- This provides assurance that only those services that are needed to provide the required functionality are available.
- Because software operating systems contain millions of lines of code and introduce complexity in development and testing, errors are prone to occur.
- This potentially allows vulnerabilities to be present, and exploits can be developed after the software is released.
- Services, permissions, ports, protocols, and remote connection service are defined as part of the standard configuration and are applied during the baseline process.
- Also, unnecessary ports and protocols are removed to prevent unauthorized connection between devices.

❑ Application Hardening
❑ Database Hardening

***Patch Management***

- See: ***NIST SP 800-40***
- Patches are sometimes referred to as ***updates***, ***quick fixes*** and ***hot fixes***.
- Many security incidents occur simply because ***organizations don't implement*** a patch management policy.
- Whenever possible, administrators test patches on an ***isolated system*** to determine if the patch causes any unwanted side effects.
- ***Microsoft*** regularly releases patches on the ***second Tuesday of every month***, commonly called ***patch Tuesday***.
- ***Out-of-band*** patches are released by Microsoft in case of urgency.
- ***Timing***, ***prioritization***, and ***testing*** are critical aspects of an effective patch management program because up to ***85% of targeted attacks*** are preventable with appropriate patch management.
- An organization must create a ***patching schedule***.
- An organization should establish a ***testing environment*** to evaluate the impact of patches on systems before installing patches.

***Vulnerability Management***

- Vulnerabilities represent ***weaknesses*** that can be ***exploited*** to gain unauthorized access to information.
- Vulnerabilities can apply to ***physical*** as well as ***logical aspects*** of security.
- Vulnerability management refers to regularly identifying vulnerabilities, evaluating them and taking steps to mitigate risks associated with them.
- Two common elements of a vulnerability management program are ***routine vulnerability scans*** and ***periodic vulnerability assessments***.
- One of the most common vulnerabilities within an organization is an ***unpatched system***.
- The presence of a vulnerability does not necessarily cause harm by itself.

***Vulnerability Assessment***

- A vulnerability assessment can look at how sensitive information is ***marked***, ***handled***, ***stored*** and ***destroyed*** throughout its lifetime to address potential vulnerabilities.
- Vulnerability assessment is a ***tool-based approach*** using scanners to identify weaknesses in a system.

***Common Vulnerabilities and Exposures***

- Vulnerabilities are commonly referred to using the ***Common Vulnerability and Exposures (CVE)*** dictionary.

***CVSS - Common Vulnerability Scoring System***

- Provides a way to capture the principal characteristics of a vulnerability, and produce a ***numerical score*** reflecting its severity, as well as a textual representation of that score.
- The numerical score can then be translated into a qualitative representation (such as ***low***, ***medium***, ***high***, and ***critical***) to help organizations properly assess and prioritize their vulnerability management processes.

# INCIDENTS

## *Operational Investigations*

- Operational investigations have the ***loosest standards*** for collecting information.
- They are ***not intended to produce evidence*** because they are for internal operational purposes only.
- ***Resolving the issue*** is the primary goal.
- Normally a ***root cause analysis*** must be conducted.

## *Criminal Investigations*

- Criminal investigations may result in charging suspects with a crime and the ***prosecution*** of those charges in criminal court.
- Most criminal cases must meet the ***beyond a reasonable doubt*** standard of evidence.

## *Civil Investigations*

- Civil investigations typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team.
- They prepare the evidence necessary to present a case in civil court resolving dispute between two parties.
- They use the ***preponderance of the evidence*** standard.

## *Regulatory Investigations*

- Government agencies may conduct regulatory investigations when they belive that an individual or corporation has violated administrative law.

## *eDiscovery - Electronic Discovery*

- Refers to discovery in ***legal proceedings*** such as ***litigation***, ***government investigations***, or ***Freedom of Information Act requests***, where the information sought is in electronic format (often referred to as electronically stored information or ESI).
- Electronic discovery is subject to rules of civil procedure and agreed-upon processes, often involving review for privilege and relevance before data are turned over to the requesting party.

**Has nine steps:**

1. Information Governance
2. Identification
3. Preservation
4. Collection
5. Processing
6. Review
7. Analysis
8. Production
9. Presentation

## *Trade Secret Law*

- The Trade Secret Law protects the expression of the idea of the resource.

## *Evidence*

**Five Rules for Evidence (AAACC):**

- Admissible
- Authentic
- Accurate
- Complete
- Convincing

**Admissible evidence:**

- The evidence must be ***relevant*** to determining a fact.
- The fact that the evidence seeks to determine must be ***material*** to the case.
- The evidence must be ***competent***, meaning it must have been obtained legally. Evidence that results from illegal search would be inadmissible because it is not competent.

***Real Evidence***

- Also known as ***object evidence***.
- Consists of things that may be brought into court of law.
- Seized computer equipment, such as keyboard with fingerprints on it or hard drive from a hacker's computer system.
- Real evidence may also be ***conclusive evidence***, such as DNA.

***Documentary Evidence***

- Any ***written items*** brought into court to prove a fact at hand.
- This type of evidence must also be authenticated.
- ***Copies*** or ***descriptions*** of original evidence will not be accepted as evidence unless certain exceptions to the rule apply.
- The ***parol evidence rule*** states that, when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements my modify the written agreement.

***Testimonial Evidence***

- Testimonial evidence is quite simple, evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition.
- Witness may offer an ***expert opinion***.
- Computer log files that are not authenticated by a system administrator can also be considered ***hearsay evidence***.

***Evidence Collection and Forensic Procedures***

- Collecting digital evidence is a tricky process and should be attempted only by professional forensic technicians.
- As you conduct forensic evidence collection, it is important to ***preserve the original evidence***.
- It's best to work with a ***copy of the actual evidence*** whenever possible.

**Six principals (IOCE):**

1. When dealing with digital evidence, all the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access, storage or transfer of digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

**Media Analysis**

- Identification and extraction of information from storage media.
- Hard disks, tapes, CDs, DVDs, Blu-ray discs, RAM, solid state storage etc.

**Network Analysis**

- Forensic investigators are often interested in the activity that took place over the network during a security incident.
- The task of the network forensic analyst is to collect and correlate information from thes disparate sources and produce as comprehensive a picture of network activity as possible.

**Software Analysis**

- Forensic analysts may also be called on to conduct forensic reviews of applications or the activity that takes place within a running application.

**Hardware/Embedded Device Analysis**

- Finally, forensic analysts often must review the contents of hardware and embedded devices.
- Personal computers, Smartphones, Tablet computers, Computers in cars, security systems and others.
- The discipline of hardware analysis requires skill in both media analysis and software analysis.

## *Investigation Process*

- First assemble a team of competent analysts to assist with the investigation.
- The ***scope*** of the investigation has to be clearly defined.

### *Calling in Law Enforcement*

- One of the first decisions is whether law enforcement authorities should be called in.
- This decision should involve senior management officials.

### *Conducting the Investigation*

**Key principles:**

- Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.
- Never attempt to "hack back" and avenge a crime. You may inadvertently attack an onnocent third party and find yourself liable for computer crime charges.
- If in doubt, call in expert assistance. If you don't want to call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations.
- Usually, it's best begins the investigation process using informal interviewing techniques. These are used to gather facts and determine the substance of the case. When specific suspects are identified, they should be questioned using interrogation techniques. Interviewing typically involves open-ended questions to gather information. Interrogation often involves closed-ended questioning with a specific goal in mind and is more adversarial in nature. This is an area best left untouched without specific legal advice.

## *Major Categories of Computer Crime*

- An individual who violates one or more of your security policies is considered as an attacker.

### *Military and Intelligence Attacks*

- Are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources.
- You can be sure that serious attacks to acquire military or intelligence information are carried out by professionals.

### *Business Attacks*

- Focus on illegally obtaining an organization's confidential information.
- It's also called ***industrial espionage***.
- A business that has suffered an attack of this type can be put into a position from which it might not ever recover.

### *Financial Attacks*

- Are carried out to unlawfully obtain money or services.
- The goal of financial attack could be to steel credit card numbers, increase the balance in a bank account or place "free" long-distance telephone calls.

### *Terrorist Attacks*

- The purpose of a terrorist attack is to disrupt normal life and instill fear.

### *Grudge Attacks*

- Are attacks that are carried out to damage an organization or a person.

- As soon as an employee is terminated, all system access for that employee should be terminated.

***Thrill Attacks***
- Are launched only for the fun of it.
- Some of these attackers are ***script kiddies***.
- ***Hacktivists*** combine political motivations with the thrill of hacking.

## *Incident Handling*
- The most common reason incidents are not reported is that they are ***never identified***.
- Law dictates that some incidents must be reported.
- Many companies have contractual obligations to report different types of security incidents to business partners (see PCI DSS).

**Event**
Any occurrence that takes place during a certain period of time.

**Incident**
An event that has a negative outcome affecting the confidentiality, integrity or availability of an organization's data.

**Incident categories:**
- Scanning
- Compromises
- Malicious code
- Denial of Service

***Scanning***
- Scanning attacks are ***reconnaissance attacks*** that usually precede another, more serious attack.
- Attackers will gather as much information about your system as possible before launching a ***directed attack***.
- Look for a high number of ***SSH packets on port 22***.

***Compromise***
- A system compromise is ***any unauthorized access*** to the system or information the system stores.
- A compromise could originate inside or outside the organization.
- A compromise could come from a valid user.
- The more you know about the normal operation of your system, the better prepared you will be to detect abnormal system behavior.

***Malicious Code***
- The most effective way to protect your system from malicious code is to implement virus and spyware scanners and keep the signature database up to date.

***DoS - Denial of Service***
- Often the easiest to detect.
- It is theoretical possible to dynamically alter firewall rules to reject DoS network traffic.
- A DoS attack is a type of cyber attack in which a computing environment is bombarded with specially crafted messages designed to overload systems, applications, and networks, exhausting them of resources until they become unresponsive and unavailable.

**DoS - Types**
Amplification
DNS amplification attack
HTTP flooding
ICMP flood
Ping of death
Slowloris

SYN flood
TCP SYN flood
UDP flood

***Response Teams***

- These teams are commonly known as computer incident response team (***CIRT***) or computer security incident response team (***CSIRT***).

**Responsibilities:**

- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident-related damages.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.
- Management of the ***network logs***, including collection, retention, review, and analysis of data.

**Potential Team Members:**

- Representative(s) of senior management
- Information security professionals
- Legal representatives
- Public affairs/communications representatives
- Engineering representatives (development, system and network)

***IRP - Incident Response Plan/Process***

- A well-designed IRP provides step-by-step instructions for handling an incident and ensures that the security team responds using an established set of procedures, that the right people are involved, and that proper communication channels are informed.
- Many organizations use a ***three-step incident response process***, consisting of the following phases:

1. Detection and identification
2. Response and reporting
3. Recovery and remediation

**Step 1: Detection and identification**

- ***Goals***, detecting security incidents and notifying appropriate personnel.
- ***Prerequisite***, monitoring any relevant events that occur and notice when they meet the organization's defined threshold for a security incident.
- The key is to ***detect abnormal*** or ***suspicious activity*** that may constitute evidence of an incident.
- ***Abnormal or suspicious activity*** is any system activity that does not normally occur on your system.
- Once the initial evaluator identifies that an event or events meet the organization's security incident criteria, the evaluator ***must notify the incident response team***.

**Tools to detect abnormal or suspicious activities:**

- IDS/IPS
- Antivirus software
- Firewall logs
- System logs
- Physical security systems
- File integrity monitoring software

**Step 2: Response and reporting**

- Once you determine that an incident has occurred, the next step is to choose an ***appropriate response***.
- Always proceed with the assumption that an incident will end up in a court of law.
- Treat any evidence you collect as if it must pass admissibility standards.

- Once you taint evidence, there is no going back.
- You must ensure that the chain of evidence is maintained.

**Chain of Custody**

- A chain of custody is a history that shows how evidence was collected, analyzed, transported and preserved to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.
- Documentation of ***who***, ***what***, ***when***, ***where*** and ***how***.

***Chain of Custody Steps:***

- ❑ Recording the name and contact information of those charged with maintaining a chain of custody
- ❑ Details of the timing of the event
- ❑ Purpose for moving the data
- ❑ Identification of evidence through recording of serial numbers and other details
- ❑ Sealing the evidence with evidence tape
- ❑ Documenting the location of storage
- ❑ Documenting the movement of the information

**Isolation and Containment**

- The first actions you take should be dedicating to limiting the exposure of your organization and preventing further damage.
- In the case of a potential compromised system, you should disconnect it from the network to prevent intruders from accessing the compromised system and also to prevent the compromised system from affecting other resources on the network.
- It is important to keep the compromised system running, not to destroy evidences.

**Gathering Evidence**

- It is common to confiscate equipment, software or data to perform a proper investigation.

**Analysis and Reporting**

- Once you finish gathering evidence, you should analyze it to determine the most likely course of events leading up to your incident.
- Summarize those findings in a written report to management.
- In your report, you should be careful to distinguish ***fact*** from ***opinion***.
- It is acceptable to theorize about possible causes, but you should be certain to state which of your conclusions are based entirely on fact and which involve a degree of estimation.

**Step 3: Recovery and remediation**

- After completing your investigation, you have two tasks remaining: Restoring your environment to its normal operating state and completing a "lesson learned" process to improve how to handle future incidents.

***Interviewing Individuals***

- Interview and interrogating individuals are specialized skills and should be performed only by trained investigators.

**Interview**

- If you seek only to gather information to assist with your investigation.

**Interrogation**

- If you suspect the person of involvement in a crime and intend to use the information gathered in court.

***Reporting Incidents***

**Report following information's:**

- ❑ What is the nature of the incident, how was it initiated and by whom?
- ❑ When did the incident occur, as precise as possible.

- ❑ Where did the incident occur?
- ❑ If known, what tools did the attacker use?
- ❑ What was the damage resulting from the incident?

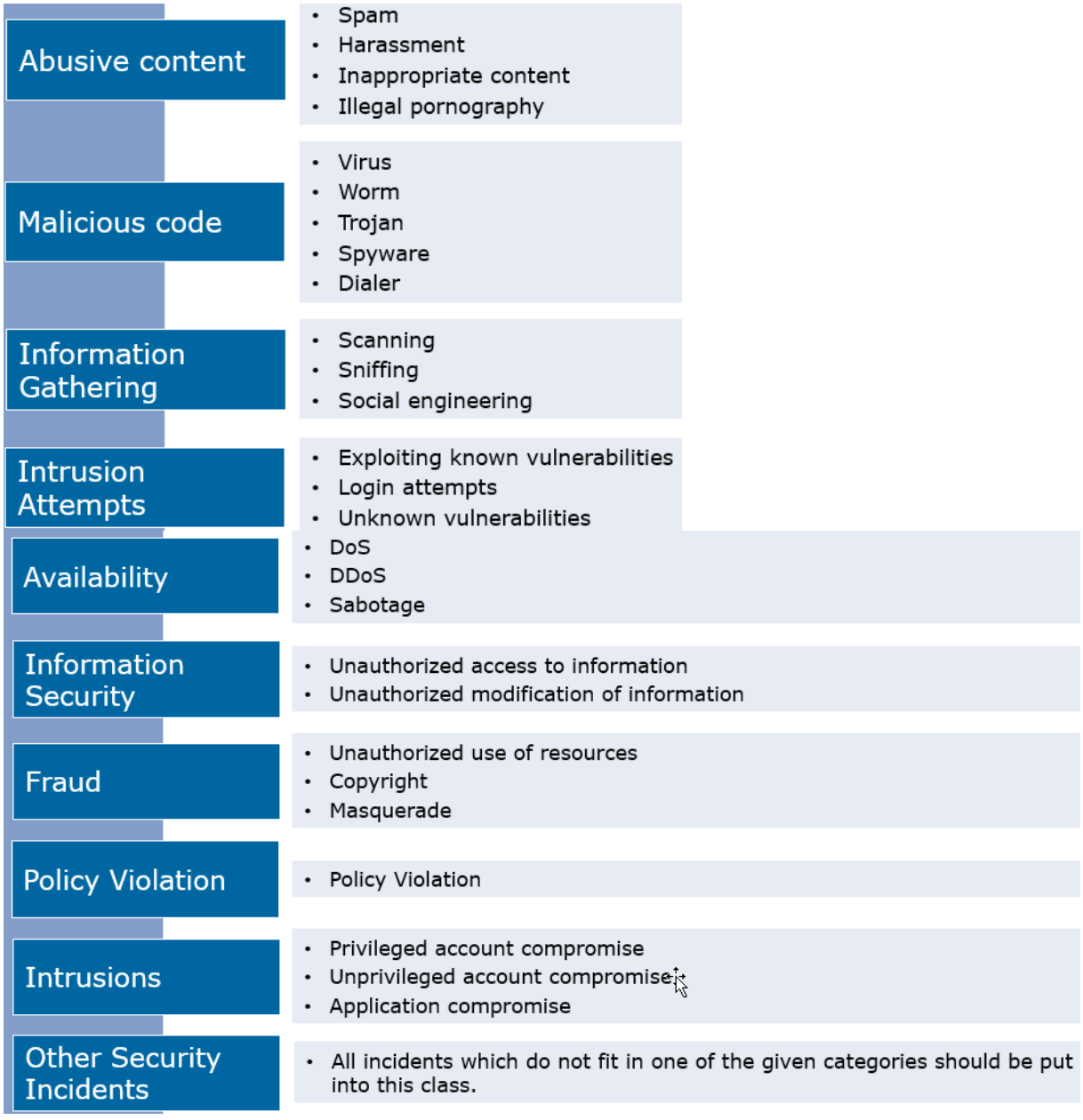
# PREVENTING and RESPONDING TO INCIDENTS

- Effective incident management helps an organization respond appropriately when attacks occur to limit the scope of the attack.
- The primary goal of ***incident response*** is to minimize the impact on the organization.

## *Defining an Incident*

- An ***incident*** is any event that has a negative effect in the confidentiality, integrity or availability of an organization's asset.
- According ***ITIL***: "An unplanned interruption to an IT Service or a reduction in the quality of an IT Service."
- A ***computer security incident*** commonly refers to an incident that is the result of an ***attack*** or the result of malicious or intentional actions on the part of users.
- ***RFC 2350*** defines both a security incident and a computer security incident as: "Any adverse event which comprises some aspect of computer or network security."
- ***NIST*** defintion: "A violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices."

## *Incident Types*



## *Incident Response Steps*

- See also ***NIST SP 800-61***
- Many organizations have a ***designated incident response team (CIRT)*** or ***computer security incident response team (CSIRT)***.
- The ***quicker*** an organization can respond to an incident, the better chance they have at limiting the damage.

1. Detection
2. Response
3. Mitigation
4. Reporting
5. Recovery
6. Remediation
7. Lessons Learned

## *Basic Preventive Measures*

- Keep systems and applications up-to-date.
- Remove or disable unneeded services and protocols.
- Use intrusion detection and prevention systems.
- Use up-to-date anti-malware software.
- User firewalls.
- ***Sensitivity labels*** are a kind of ***preventive security controls***.

## *Anti-Malware*

- The most important protection against malicious code is the use of ***anti-malware software*** with up-to-date ***signature files***.

## *Sandboxing*

- Provides a ***security boundary*** for applications and prevents the application from interacting with other applications.

## *Logging*

- Logging is the process of recording information about events to a log file or database.
- Logging captures ***events***, ***changes***, ***messages*** and other data that describe activities that occurred on a system.
- Standards like ***BSI***, ***ISO 27001***, ***PCI-DSS***, ***NIST 800-171*** or ***OWASP*** require to have a functioning ***Log-Infrastructure*** in place.
- It's important to define the ***retention time*** for logs in advance.

Windows Events
Security Logs (Windows)
System Logs
Application Logs
Firewall Logs
Proxy Logs
Change Logs

***Products:***
Datadog
Kiwi

## *Monitoring*

- Monitoring is the process of ***reviewing information logs*** looking for something specific.
- Provides several benefits for an organization, including increasing accountability, helping with investigations and basic troubleshooting.

## *Audit Trails*

- Using audit trails is a passive form of ***detective security control***.
- Audit trails are records created when information about events and occurrences is stored in one or more database or log files.
- Audit trails provide a record of ***system activity*** and can reconstruct activity leading up to and during security events.

## *Clipping Levels*

- Clipping is a form of ***nonstatistical sampling***.
- It selects only events that exceed a clipping level, which is predefined ***threshold*** for the event.
- The system ignores events until they reach this threshold.
- Clipping levels are widely used in the process of auditing events to establish a baseline of routine system or user activity.

# MALICIOUS CODE and APPLICATION ATTACKS

## *Adware*

- It uses a variety of techniques to display advertisements on infected computers.

## *Dynamic Web Applications*

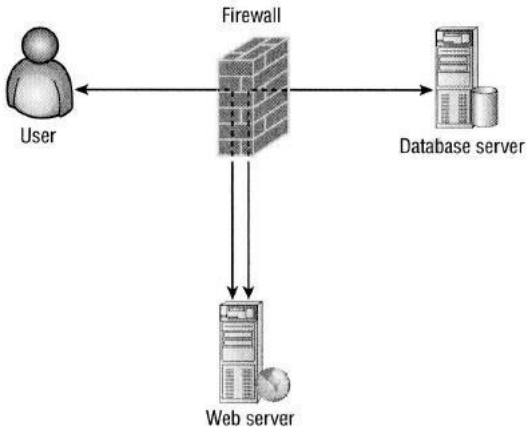



**Figure 15: Typical website architecture**

## *Hoaxes*

- Falschmeldung.
- A hoax is a falsehood deliberately fabricated to masquerade as the truth.

## *Logic Bombs*

- Reacts on conditions such as time. program launch, website logon.

## *Ransomeware*

- Bei Ransomware-Trojanern handelt es sich um eine Art von Malware, die Geld von Opfern erpressen soll.
- Oftmals fordert Ransomware eine Zahlung vom Benutzer, damit die Änderungen rückgängig gemacht werden, die der Trojaner auf dem Computer des Opfers vorgenommen hat.
- Diese Änderungen können Folgendes umfassen:
    - Verschlüsselung der auf der Festplatte befindlichen Daten, sodass die Informationen nicht länger verfügbar sind
    - Blockierung des normalen Zugriffes auf das System

**Example:**

- WannaCry
- Petya
- Cryptolocker

**Countermeasure:**

- E-Mail Security and sandboxing.
- Network scan and analysis.
- Protect your Servers with actual patches.
- Protect your endpoints with Antivirus software.
- Educate your staff regarding Phishing E-Mails.

## *Spyware - Definition*

- Monitors your actions and transmits important details to a remote system that spies on your activity.

- Is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- Is mostly classified into four types: ***system monitors***, ***trojans***, ***adware***, and ***tracking cookies***.

## *Virus - Definition*

- As with biological viruses, computer viruses have two main functions, ***propagation*** and ***destruction***.
- It lives inside other programs and requires ***human interaction to spread***.
- By definition, a virus must contain technology that enables it to spread from system to system, aided by unsuspecting computer users seeking to share data by exchanging disks, sharing networked resources, sending electronical mail, or using some other means.

**Master Boot Recorded Viruses**

- ***MBR*** virus is one of the earliest known forms of virus infection.

**File Infector Viruses**

- Many viruses infect different types of executable files and trigger when the operating system attempts to execute them.

**Macro Viruses**

**Service Injection Viruses**

**Multipartite Viruses**

- See Marzia virus

**Stealth Viruses**

- Stealth viruses hide themselves by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally.

**Polymorphic Viruses**

- Modify their own code as they are travel from system to system.

**Encrypted Viruses**

- Quite similar to polymorphic viruses.

## *Worm - Definition*

- They propagate themselves ***without*** requiring any human intervention.
- The behavior of a worm is similar to a virus in that it is designed to duplicate itself, but instead of hiding in existing files, a worm is a separate program that can infect other computers without human involvement.
- A worm often travels over the computer network, running in the background on an infected computer and using known vulnerabilities in computer software to locate and infect other connected devices.
- Some examples of worms have been ***Melissa***, ***Code Red***, and ***Stuxnet***.

# RISK MANAGEMENT

- Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
- Oversight for risk management, is a critical activity that should occur within an organization.
- Risk management begins at the ***corporate governance level*** of an organization, but the CISO has significant responsibilities concerning the implementation and executions of an organization's risk management strategy.

***The Essentials of Risk Management***

1. Understand risks to the organization.
2. Use an accepted process or framework to measure risk (and risk impact) meaningfully.
3. Communicate identified risks to the right people.
4. Select an appropriate risk treatment plan.
5. Obtain executive buy-in or endorsement of the risk treatment plan.
6. Implement the approved risk treatment plan, including respective controls.
7. Measure effectiveness of the risk treatment plan and consider residual risk to the organization.
8. Communicate effectiveness of risk treatment and the risk management program.
9. Discuss the opportunities for additional risk mitigation for residual risk and new risks identified for the organization.

## *Risk Assessment*

- ***Risk*** is the probability that a threat agent (cause) will exploit a system vulnerability (weakness) and thereby create an effect detrimental to the system.
- The CISO must understand the risks facing an organization before an appropriate response for addressing those risks can be identified.
- The effort to understand the risks facing the organization begins with ***risk assessment***.


**Figure 16: Risk Assessment**

***Risk assessments consist of the following activities:***

- Risk identification
- Risk analysis
- Risk evaluation


**Figure 17: Risk Assessment Workflow**

***Forensic Point of View***

1. Identify the incident and the problems caused by it
2. Characterize the incident according to its severity
3. Determine the data loss or damage caused to the computer due to the incident
4. Determine the possibility of other devices and systems being affected by the incident
5. Break the communications with other devices to prevent the incident from spreading

| | Likelihood of incident scenario | Very Low (Very Unlikely) | Low (Unlikely) | Medium (Possible) | High (Likely) | Very High (Frequent) |
|---|---|---|---|---|---|---|
| Business Impact | Very Low | 0 | 1 | 2 | 3 | 4 |
| | Low | 1 | 2 | 3 | 4 | 5 |
| | Medium | 2 | 3 | 4 | 5 | 6 |
| | High | 3 | 4 | 5 | 6 | 7 |
| | Very High | 4 | 5 | 6 | 7 | 8 |

**Figure 18: Generic Level of Risk Determination Chart**

| Likelihood | Consequences | | | | |
|---|---|---|---|---|---|
| | **Insignificant** (Minor problem easily handled by normal day to day processes) | **Minor** (Some disruption possible, e.g. damage equal to $500k) | **Moderate** (Significant time/resources required, e.g. damage equal to $1 million) | **Major** (Operations severely damaged, e.g. damage equal to $10 million)) | **Catastrophic** (Business survival is at risk damage equal to $25 million) |
| **Almost Certain** (e.g. >90% chance) | High | High | Extreme | Extreme | Extreme |
| **Likely** (e.g. between 50% and 90% chance) | Moderate | High | High | Extreme | Extreme |
| **Moderate** (between 10% and 50% chance) | Low | Moderate | High | Extreme | Extreme |
| **Unlikely** (e.g. between 3% and 10% chance) | Low | Low | Moderate | High | Extreme |
| **Rare** (e.g. <3% chance) | Low | Low | Moderate | High | High |

**Figure 19: Risk Assessment Matrix**

**FRAP - Facilitated Risk Analysis Process**

- Risk assessment methodology
- It allows organizations to implement risk management techniques in a highly cost-effective way.
- The FRAP process examines the qualitative risk analysis process and then provides tested variations on the methodology.

## *Risk Sources*

| Busienss Risks | External Sources |
|---|---|
| • Economic downturns<br>• Losing key employees<br>• Quality of customer service<br>• Regulatory changes<br>• Lack of capital to meet growth<br>• Optimization of capacity<br>• Strategic errors<br>• Economic inflation<br>• Market restructuring<br>• Accounting and tax issues<br>• Product obsolescence<br>• Currency fluctuations | • Clients<br>• Suppliers<br>• Competitors<br>• Regulatory Agencies<br>• Political, Social, Economic<br>• Environmental<br>• *Force majeure* |

## *Risk Tolerance*

- Tolerance is the most common description used to evaluate feelings about information security risk.
- It marks the boundaries of risk-taking outside of which an organization is not prepared to venture in the pursuit of its long-term objectives.

- The concept helps to define the level of risk an organization is willing to assume based upon the perception of risk related to the desire to achieve some outcome or objective.

## *Risk Appetite*

- Risk appetite evaluates how much risk an organization is willing to seek or accept in the pursuit of its long-term objectives.
- Risk tolerance evaluates how much risk an organization is willing to endure, and aversion evaluates the extent of the efforts exercised by an organization to avoid risk altogether.

## *Risk Aversion*

- Risk aversion defines the reluctance of a person to accept a bargain with an uncertain payoff.
- This is preferable to accepting another bargain with a more certain, but possibly lower, payoff.
- Psychologically, the concept applies to the behavior people demonstrate while exposed to uncertainty and the extent to which they will attempt to reduce that uncertainty to accomplish their goals.
- Although aversion is a valid driver that influences feelings about risk, it is rarely used to describe the emotional influences that affect the decision-making process.

## *Risk Management Concepts*

- Managing risk is an element of sustaining a secure environment.
- Target to ***reduce a risk*** to an acceptable level.


**Figure 20: Elements of risk**

**Risk Management Process**

- Identify assets
- Identifying threats
- Identifying vulnerabilities.

**Asset**

- An asset is anything within an environment that should be protected.

**Asset Valuation**

- Is a dollar value assigned to an asset based on actual cost and nonmonetary expenses.

**Threats**

- Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset is a threat.
- A threat is a potential occurrence that can result in an undesirable outcome.
- It also includes natural occurrences such as ***floods*** or ***earthquakes***.

**Vulnerability**

- The known ***weakness*** in an asset or ***the absence or weakness of a safeguard*** or countermeasure is a vulnerability.
- A vulnerability is any type of ***weakness***.

**Exposure**

- Experienced exposure
- Exposure doesn't mean that a realized threat is occurring.

**Risk**

- It is an assessment of probability, possibility and chance.
- There is no way to eliminate 100 percent of all risks.
- A ***risk report*** should be accurate, timely, comprehensive of the entire organization, clear and precise to support decision making, and updated on a regular basis.
- A risk is the possibility or likelihood that a threat will exploit a vulnerability resulting in a loss such as harm to an asset.
- Any losses that occur from accepting risks (residual risk) are the ***responsibility of management***.

**risk** = threat * vulnerability
**total risk** = threats * vulnerabilities * asset value
**residual risk** = total risk - control gap

**Safeguards**

- A ***safeguard*** or ***countermeasure*** is anything that removes or reduces a vulnerability or protects against one or more specific threats.
- The best of all possible safeguards would reduce the ***ARO*** to zero.
- If the cost of the countermeasure is greater than the value of the asset, then you should accept the risk.
- As a rule, the annual cost of safeguards should not exceed the expected annual cost of asset loss.

**Attack**

- Insider attacks
  These involve a brach of trust from employees within an organization.
- External attack
  These onvolve hackers hired by either an insider ir an external entity whose aim ist o destroy a competitor's reputation.

**Breach**

- A security breach is any incident that results in ***unauthorized access*** of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
- A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter.
- A security breach is also known as a ***security violation***.

***Quantitative Risk Analysis***

- ***Loss of revenue*** is an example of quantitative loss.
- The quantitative impact can be determined by evaluating financial losses such as ***lost revenue***, ***assets***, or ***productive units*** and salary paid to an idled workforce.

**ALE - Annualized Loss Expectancy**

- Mathematical measurement of the cost of replacing or repairing a specific resource.

ALE = SLE * ARO

**ARO - Annualized Rate of Occurrence**

x Failure / x Years = x Percent

**AV - Asset Value**

**SLE - Single Loss Expectancy**

- The monetary value expected from the occurrence of a risk on an asset.

SLE = AV * EF

**EF - Exposure Factor**

- The proportion of an asset's value that is likely to be destroyed by a particular risk, expressed as a percentage.
- For example, if the value of a building would be reduced from $1,000,000 to $250,000 by a fire, the exposure factor for the risk of fire to the building is 75%.

**Risk Equation**

- See: http://www.icharter.org/articles/risk_equation.html
- This equation is fundamental to all that we do in information security.

Risk = Threat x Vulnerability x Cost

***Qualitative Risk Analysis***

- Qualitative risk analysis is more scenario based than it is calculator based.
- Qualitative impact includes such factors as ***reputation***, ***goodwill***, ***value of the brand*** and ***lost opportunity***, among others.

### *Risk Information*


**Figure 21: Risk Information**

### *Identifying Assets*

- ***Asset valuation*** refers to identifying the actual value of assets with the goal of prioritizing them.

### *Identifying Threats*

- An essential part of risk management is identifying and examining threats.
- ***Threat modeling*** refers to the process of identifying, understanding and categorizing potential threats.

### *Identifying Vulnerabilities*

- Perform vulnerability analysis.

## *Audit Management*

- An information security audit is a systematic evaluation of the security of an organization's processes or systems by measuring how well they conform to a set of established criteria or controls.
- The purpose of an audit is to evaluate the effectiveness of controls used to mitigate risk in an organization or to measure alignment to a framework, internal compliance requirement, or external regulatory requirement.

- Organizations invest significant time and effort to build risk management and compliance programs.
- After applying controls to mitigate risks, organizations must evaluate the effectiveness of those controls.

## *Risk Treatment*

***Options:***

- Accept
- Mitigate
- Avoid
- Transfer

***Transfer***

- ***Crime Insurance Policy*** protects organizations from loss of money, securities, or inventory resulting from crime.
- ***Valuable Paper Insurance***.

## *Risk Register*

- The risk register is the most common tool used for tracking and communicating risks.
- The risk register is typically a spreadsheet that contains details of a risk.

***Common information included in the register follows:***

- ❑ A risk item identifier
- ❑ Who discovered it
- ❑ Impacted system(s)
- ❑ Nature of the risk/description
- ❑ Vulnerability
- ❑ Threat vectors
- ❑ Probability
- ❑ Risk rating
- ❑ Compensating controls
- ❑ Residual risk rating
- ❑ Recommendations
- ❑ Treatment decision
- ❑ Treatment status
- ❑ Risk acceptance

# DRP - DISASTER RECOVERY PLANNING

- DRP steps in where BCP leaves off.
- ***Business continuity management (BCM)*** encompasses BCP, DRP and incident management under a single umbrella.
- Any event that stops, prevents, or interrupts an organization's ability to perform its work tasks is considered a disaster.
- If the continuity is broken, the business processes have stopped and the organization is in ***disaster mode***.
- A disaster recovery plan should be set up so that it can almost run on ***autopilot***.
- The DRP should also be designed to ***reduce decision-making activities*** during a disaster as much as possible.
- The DRP should fully address the ***backup strategy*** pursued by your organization.
- Your DRP should specify the criteria used to determine when it is appropriate to return to the primary site and guide the DRP recovery and salvage teams through an orderly transition.
- Every DRP must be tested on a periodic basis to ensure that the plan's provisions are viable and that it meets an organization's changing needs.
- ***Disaster recovery responsibilities*** should be included in job descriptions.
- An organization's DRP is one of the ***most important documents*** under the purview of secutity professionals.

***Natural Disasters***

**Avalanches**

**Earthquakes**

See: http://www.seismo.ethz.ch

- Earthquakes are caused by the ***shifting of seismic plates*** and can occur almost anywhere in the world without warning.

**Fires**

**Floods**

- It's important that your DRP make appropriate response plans for the eventuality that a flood may strike your facility.

**Hailstorms**

**Hurricanes**

**Monsoons**

**Mudslides**

**Storms**

- Storms come in many forms and pose diverse risks to a business.

**Tornados**

**Tsunamis**

**Volcanic Eruptions**

**Windstorms**

***Man-Made Disasters***

**Acts of Terrorism**

**Bombing/Explosions**

**Fires**

**Power Outages**

**Strikes**

**Theft**

**Vandalism**

***System Resilience and Fault Tolerance***

- A primary goal of system resilience and fault tolerance is ***to eliminate single points of failure***.
- ***Fault tolerance*** is the ability of a system to suffer a fault but continue to operate.

**Protecting Hard Drives**

- See RAID.

**Protecting Servers**

- Fault tolerance can be added for critical servers with ***failover clusters***.
- Although network load balancing is primarily used to increase the scalability of a system so that it can handle more traffic, it also provides a measure of ***fault tolerance***.

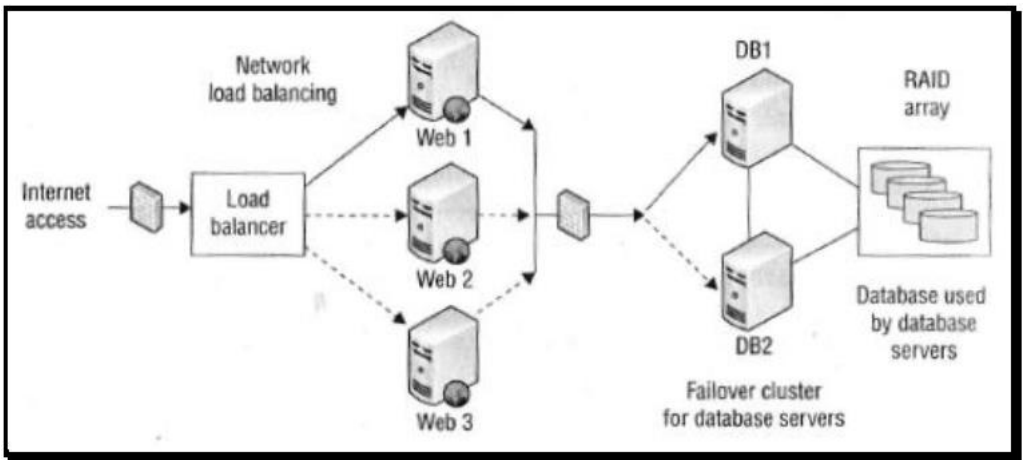



**Figure 22: Failover Cluster**

**Protecting Power Sources**

- Fault tolerance can be added for power sources with an ***uninterruptable power supply (UPS)***, a ***generator*** or both.
- A ***UPS*** provides power for a short period of time between ***5 and 30 minutes***.
- Static charge of ***>= 1500 volts*** causes disk drive data loss.

| | |
|---|---|
| **Spike** | Is a quick instance of an increase in voltage. |
| **Sag** | Is a quick instance of a reduction in voltage. |
| **Surge** | Is a longer period of high voltage. |
| **Brownout** | Is a longer period of a reduction in voltage. |
| **Blackout** | When the voltage drops to zero. |
| **Transients** | Noise on a power line. |

**Static electrical charge and damage:**

| | |
|---|---|
| 40 volts | Sensitive circuits and transistors |
| 1000 volts | Scramble monitor display |
| 1500 colts | Disk drive data loss |
| 4000 volts | Printer Jam |
| 17000 volts | Permanent chip damage |

**Trusted Recover**

- Trusted recovery provides assurance that after a failure or crash, the system is just as secure as it was before the failure or crash occurred.

| | |
|---|---|
| **Fail-Safe** | A ***fail-safe*** electrical lock will be unlocked when power is removed. |
| **Fail-Secure** | A ***fail-secure*** electrical lock will stay locked when power is removed. |

**The four types of trusted recovery:**

- Manual Recovery
- Automated Recovery
- Automated Recovery without Undue Loss
- Function Recovery

**QoS - Quality of Service**

- Controls protect the integrity of data networks under load.

Bandwidth
Latency
Jitter
Packet Loss
Interference

**Recovery Strategy**

- When a disaster interrupts your business, your DRP should kick in nearly automatically and begin providing support for recovery operations.

**Crisis Management**

- If a disaster strikes your organization, panic is likely to set in.
- Crisis management is a science and an art form.
- Crisis training for your key employees is a good idea.
- Ensure that at least some of your employees know how to handle emergency situations properly and can provide all-important "on-the-scene" leadership to panic-stricken co-workers.

**Emergency Communications**

- When a disaster strikes, it is important that the organization be able to communicate inernally as well as with the outside world.

**Workgroup Recovery**

- One important consideration in your DRP should be the restoration of workgroups to the point that they can resume their activities in their usual work locations.

**Alternate Processing Sites:**

- **Cold Sites**
- **Warm Sites**
- **Hot Sites**
  A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment and UPS.
- **Mobile Sites**
- **Service Bureaus**
- **Multiple Sites**
- **Cloud Computing**

**Database Recovery**

- Backup and restoration activities can be bulky and slow.

**Backup Medias:**

- Digital Data Storage (DDS)
- Digital Audio Tape (DAT)
- Digital Linear Tape (DLT)
- Super DLT
- Linear Tape Open (LTO)
- Disk-to-Disk (D2D)

**Tape Rotation:**

- Grandfather-Father-Son (GFS) strategy
- Tower of Hanoi strategy
- Six Cartridge Weekly Backup strategy

**Electronic Vaulting**

- In an ***electronic vaulting*** scenario database backup is moved to a remote site using ***bulk transfers***.

**Remote Journaling**

- With ***remote journaling***, data transfers are performed in an ore expeditious manner.
- Data transfer will occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour and sometimes more frequently.
- The data is stored on ***backup devices*** not on live databases.

**Remote Mirroring**

- The most advanced and most expensive database backup solution.

**Full Backup**

**Incremental Backup**

- Fastest backup method daily.

- It's fast, because it copies only the files that have been modified since the previous backup.

**Differential Backup**

- Does not reset the archive bit on files that are backed up.

**Recovery Plan Development**

- Use checklists.
- ***Recovery*** and ***restoration*** are separate concepts.

**Recovery**

- Involves bringing business operations and processes back to a working state.

**Restoration**

- Involves bringing a business facility and environment back to a workable state.

**Read-Through Test**

- The simplest test to conduct.

**Structured Walk-Through**

- In this type of test, often referred to as a table-top exercise, members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.

**Simulation Test**

- In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response.

**Parallel Test**

- Involves relocating personnel to the alternate recovery site and implementing site activation procedures.

**Full-Interruption Test**

- Involves actually shutting down operations at the primary site and shifting them to the recovery site.
- For obvious reasons, full-interruption tests are extremely difficult to arrange, and you often encounter resistance form management.

**Maintenance**

| Site | Cost | Hardware Equipment | Telecommunications | Setup Time | Location |
|---|---|---|---|---|---|
| **Cold Site** | Low | None | None | Long | Fixed |
| **Warm Site** | Medium | Partial | Partial/Full | Medium | Fixed |
| **Hot Site** | Medium/High | Full | Full | Short | Fixed |

# THREAT MANAGEMENT

- Threat management begins by identifying and understanding the threats facing an organization.
- Threat actors can be ***natural*** or ***human***, and their intentions can be ***accidental*** or ***deliberate***.

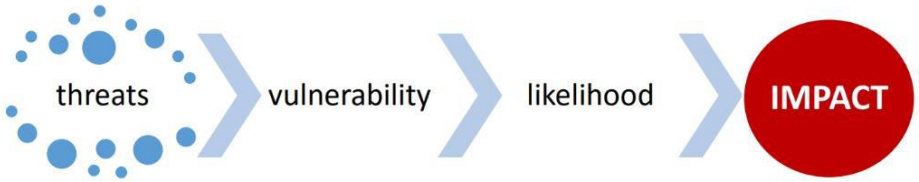



**Figure 23: Threat Management Evaluation Workflow**

***Thread Types:***

- Human Threats
- Physical and Environmental Threats
- Technical Threats

***Threat Analysis***

- The examination of threat-sources against system vulnerabilities to determine the threats for a particular operational environment.

# THREATS & ATTACKS

- Brute-force password attack
- Client-side attack
- Clone-Phising
- Denial of Service Attacks (DoS)
- Destruktive Methoden, wie z.B. Denial-of-Service-Tools
- Display name spear-phishing attack
- Email Attacks
- Fraggle DoS Attack
- FTP Exploits
- Max Age Attack ( → Router )
- NEMESIS
- Phlashing (BIOS attack)
- Probing Attacks
- Popular Service Exploits
- Password-spray attack
- Passwort - Knacker
- Route Table poisoning ( → Router )
- Sequence++ Attack ( → Router )
- Sniffer
- Split-response attack
- Trojanische Pferde
- Tools, die eine Verschleierung der Identität ermöglichen
- Temporary Internet files
- Unauthorized Network Traffic
- Windows Network Attacks
- WEBMITM

Weil der ***UNIX-Source Code*** weithin bekannt und verfügbart ist, werden auch mehr Fehler in der Sicherheitsstruktur des Systems bekannt.
Im Gegensatz dazu stehen ***proprietäre Systeme***, deren Hersteller meist nicht bereit sind, Source-Codes zu offenbaren und damit viele Fragen in Bezug auf Ihre Sicherheit aufwerfen.

## *DEFINITION THREAT*

- A threat refers to a new or newly discovered incident with the potential to do harm to a system or your overall organization.
- There are three main types of threats:
  - ***natural threats*** (e.g., floods or a tornado)
  - ***unintentional threats*** (such as an employee mistakenly accessing the wrong information), and
  - ***intentional threats***. There are many examples of intentional threats including spyware, malware, adware companies, or the actions of a disgruntled employee. In addition, worms and viruses are also categorized as threats, because they could potentially cause harm to your organization through exposure to an automated attack, as opposed to one perpetrated by humans.

***Examples of intentional Threats:***

- Spear-Phishing attacks
- Malicious Codes in App
- DDos
- DDos-Botnet
- Man-in-the-Middle
- Buffer Overflow
- ArpFlooding
- BadUSB
- Ransomware

- Rogue QR Codes

## *Access Aggregation Attacks*

- Is the act of ***combining information*** from separated sources.
- Refers to collecting multiple pieces of nonsensitive information ans combining them to learn sensitive information.
- The combination of the data forms new information, which the subject does not have the necessary rights to access.
- The combined information has a sensitivity that is greater than that of the individual parts.

## *Access Control Attacks*

- Attempt to bypass or circumvent access control methods.
- Often try to ***steal user credentials***.

## *APT - Advanced Persistent Thread*

- An ***APT*** refers to a group of attackers who are working together and are highly motivated, skilled and patient.
- The attackers are ***well funded*** and have ***advanced technical skills*** and resources.
- They act on behalf of a nation-state, organized crime, terrorist group, or other sponsor.
- See the ***Mandiant APT1*** report.

## *ARP Cache Poisoning*

- Base for ***man-in-the-middle*** attacks.
- Creates ***static ARP entries***.
- ***Static ARP entries*** are permanent, even across system reboots.
- ARP Cache Poisoning ***does not cross router boundaries***.

**Countermeasure:**
Physical Security

## *ARP Spoofing*

- See: Ettercap, Cain & Abel and arpspoof

## *Backdoors*

- Are shortcuts in a system that allow a user to bypass security checks to log in.

## *BEAST-Attacke*

- Vulnerability in ***TLS 1.0***
- BEAST ist die Ausnutzung einer vorhandenen Sicherheitslücken und Fehlverhalten innerhalb des sog. ***Cipher Block Chaining (CBC)***, dass das Secure Sockets Layer (SSL) Protokoll nutzt.
- Mit dieser Anfälligkeit von ***CBC*** kann gegen SSL ein sog. "Man-in-the-Middle“-Attacke gestartet werden.
- Dadurch kann ein Dritter im Verborgenen den Authentifizierungs-Token erhalten und entschlüsseln und damit Zugriff auf den eigentlich per SSL-gesicherten Datenaustausch zwischen einem Webserver und dem Browser erhalten.
- Die zugrunde liegende Schwachstelle wurde bereits 2002 das erste Mal benannt und wäre mit dem Einsatz von ***TLS 1.1*** seit 2006 auch nicht mehr problematisch.
- Bis zur Vorstellung des Angriffs-Mechanismus „BEAST (***Browser Exploit Against SSL/TLS***)“ gab es jedoch keine praktische Demonstration, wie man diese Lücke ausnutzen konnte.

## *BlueKeep*

- ???

## *Boot Sector Virus*

- Moves the ***MBR*** to another location on the hard disk and copies itselt tot he original location oft he MBR.

## *Brain*

- First computer virus that infected the boot sector oft he ***MS-DOS***.

## *Cavity Viruses*

- A cavity virus attempts to install itself ***inside*** of the file it is infecting.
- Most viruses take the easy way out when infecting files; they simply attach themselves to the end of the file and then change the start of the program so that it first points to the virus and then to the actual program code.
- Many viruses that do this also implement some stealth techniques, so you don't see the increase in file length when the virus is active in memory.
- A cavity virus, on the other hand, attempts to be clever.
- Some program files, for a variety of reasons, have empty space inside of them. This empty space can be used to house virus code.
- A cavity virus attempts to install itself in this empty space while not damaging the actual program itself.
- An advantage of this is that the virus then does not increase the length of the program and can avoid the need for some stealth techniques.
- The ***Lehigh virus*** was an early example of a cavity virus.
- Because of the difficulty of writing this type of virus and the limited number of possible hosts, cavity viruses are ***rare***.

## *Clickjacking Attack*

- Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.
- This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
- Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an ***iframe***, on top of the page the user sees.
- The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.
- The invisible page could be a malicious page, or a legitimate page the user did not intend to visit – for example, a page on the user's banking site that authorizes the transfer of money.
- Variations of ***clickjacking***:
    - ***Likejacking*** – a technique in which the Facebook "Like" button is manipulated, causing users to "like" a page they did not intend to like.
    - ***Cursorjacking*** – a UI redressing technique that changes the cursor for the position the user perceives to another position.
      Cursorjacking relies on vulnerabilities in Flash and the Firefox browser, which have now been fixed.

**Countermeasure:**

- Use the ***X-Frame-Options HTTP header*** to avoid this kind of attack.

## *GHOST CVE-2015-0235 28.01.2015*

- Hole in the ***Glibc-Library***.

## *IDORs - Insecure Direct Object References*

- A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a ***file***, ***directory***, or ***database*** key ***without any validation*** mechanism which allows attackers to manipulate these references to access unauthorized data.

### *Intel CSME bug*

- CVE-2019-0090
- Attacks are impossible to detect, and a firmware patch only partially fixes the problem.
- Only the latest Intel ***10th generation chips*** are not vulnerable.
- CSME is basically a «root of trust» for every other technology running o Interl chipsets.
- The malware has to have OS-level (root privileges) or BIOS-level code execution access.
-

### *Low Orbit Ion Cannon*

- DoS Attack

### *Lucky Thirteen*

- Heartbleed

### *Malicious Code*

- Malicious code is any script or program that performs an unwanted, unauthorized, or unknown activity on a computer system. This are viruses, worms, trojan horses, documents with destructive macros and logic bombs.
- Also called ***malcode***.

### *Meltdown / Spectre*

| | Meltdown | Spectre |
|---|---|---|
| Allows kernel memory read | Yes | No |
| Was patched with KAISER/KPTI | Yes | No |
| Leaks arbitrary user memory | Yes | Yes |
| Could be executed remotely | Sometimes | Definitely |
| Most likely to impact | Kernel integrity | Browser memory |
| Practical attacks against | Intel | Intel, AMD, ARM |

### *Multipartite Virus*

- Infects the ***system boot sector*** and the ***executable files***.

### *NBA - Network Behavior Analysis*

http://rules.emergingthreats.net/open

- NBAD - Network Behaviour Anomaly Detection (NBAD)

### *PHP*

- ***PHP 5.6*** steht kurz vor dem Ende seiner Lebenszeit. Mit 31.12.2018 endet der Security-Support für die letzte Version der PHP 5 Familie, ab dann wird nur noch ***PHP 7*** weiterentwickelt.
- Das bedeutet, dass ab dem Jahreswechsel neu entdeckte Sicherheitslücken in PHP 5.6 Upstream nicht mehr gepatcht werden.

### *Pinkslipbot (Qakbot/QBot)*

- ???

### *Privilege Escalation*

- Privilege escalation vulnerabilities allow an attacker with (typically limited) access to be able to access additional resources.

- ***Vertical escalation*** leverages non-privileged access into higher level access. One example is escalating privileges from a normal Unix user into root access (UID 0).
- ***Horizontal escalation*** allows an attacker to access other accounts, such as pivoting from one non-privileged account to another (with access to different resources).
- Improper software configurations and poor coding and testing practices often cause privilege escalation vulnerabilities.

**Countermeasure:**
- Privileged Account Management (PAM)

## *POODLE Vulnerability CVE-2014-3566 [1]*

- "Padding Oracle On Downgraded Legacy Encryption (POODLE, 2014)".
- Demonstrated a significant flaw in the SSL 3.0 fallback mechanism.
- To remediate this vulnerability, many organizations completely dropped SSL support and now rely solely on TLS security.

**Countermeasure:**
- Don't use SSL

## *QBot*

- ProLock
- Bank Trojan

## *Ramen*

- Worm

## *Ransomware*

- Ransomware entschlüsseln: https://www.heise.de/security/meldung/Erpressungstrojaner-Everbe-Hidden-Tear-und-InsaneCrypt-kostenlos-entschluesseln-4254364.html

## *Slammer Worm*

- SQL-Slammer ist der Name eines Computerwurms, der einen ungepatchten ***Microsoft SQL Server 2000*** befallen kann.
- Er begann am 25. Januar 2003, sich zu verbreiten, und infizierte innerhalb einer halben Stunde 75.000 Opfer, den Grossteil davon in den ersten 10 Minuten.
- Der SQL-Slammer nutzt zwei Pufferüberläufe.
- Microsoft hatte schon ein halbes Jahr davor einen Patch veröffentlicht, der allerdings auf vielen Systemen nicht installiert war.
- Das Besondere an diesem Wurm ist, dass er aus einem einzigen ***UDP-Paket mit nur 376 Bytes*** besteht, was für seine enorme Verbreitungsgeschwindigkeit sorgte.
- In einigen Quellen wird der Wurm auch Sapphire, MS-SQL Slammer, WORM_SQLP1434.A, SQL Hell oder Helkern genannt.
- Nach einem Bericht der Nuclear Regulatory Commission der USA drang noch im Januar 2003 der Wurm über eine ungesicherte Leitung in das IT-System des Davis-Besse Atomkraftwerks in Ohio ein und legte das Sicherheitssystem für fast fünf Stunden lahm.
- Im November 2004 wurden zwei Mitglieder der Virenschreibergruppe 29A von der Polizei zur Verbreitung des Wurms befragt.

## *Stealth Virus*

- Tries to hide from anti-virus programs by altering and corrupting the chosen service call interruptions when they are being run.

## *Stuxnet*

- Worm.
- Rootkit to a SCADA system.

## *Trickbot*

- ***Trojan***
- Von ***Emotet*** nachgeladenes Schadprogramm.
- Die ***Kernkomponente*** von Trickbot – der Loader – deaktiviert zunächst die Windows-Dienste und laufende Prozesse von Windows Defender und verschiedener anderer Antivirus-Programme.

## *Wanna Cry*

- ***Ransomeware***
- WannaCry, auch bekannt als Wcrypt, WCRY, WannaCrypt oder Wana Decrypt0r 2.0, ist ein Schadprogramm für Windows, das im Mai 2017 für einen schwerwiegenden Cyberangriff genutzt wurde.
- WannaCry befällt Windows-Betriebssysteme, die nicht mit einem bestimmten, seit März 2017 von Microsoft angebotenen Patch nachgebessert wurden.
- Nach Befall eines Computers verschlüsselt das Schadprogramm bestimmte Benutzerdateien des Rechners und fordert als Ransomware den Nutzer auf, einen bestimmten Betrag in der Kryptowährung Bitcoin zu zahlen, nach ungenutztem Ablauf einer Frist droht das Programm mit Datenverlust.
- Ausserdem versucht das Programm, als Computerwurm weitere Windows-Rechner zu infizieren, und installiert die schon länger bekannte ***Backdoor DoublePulsar***.

## *Interne Angriffe*

- Dass interne Angriffe häufiger vorkommen als entfernte Attacken hat verschiedene Gründe.
- Ein sehr offensichtlicher Grund ist, dass es viel leichter ist, ein Netzwerk von innen anzugreifen.
- Verärgerte Mitarbeiter?

Policies: Integrieren in Arbeitsverträge.
Verbieten jeglicher Aktivitäten, die die interne Sicherheit gefährden können.

## *Interne Sicherheitsscanner*

- SysCAT
- SQLAuditor
- System Security Scanner
- RSCAN
- Comodo

## *Birthday Attack*

- A birthday attack focuses on finding ***collisions***.
- Usually applied to the probability of ***two different messages*** using the ***same hash function*** that produces a common ***message digest***.

## *Blackjacking Attack*

- Use BBProxy

## *Blind SQL injection (SQLi)*

- This occurs when the attacker knows the database is susceptible to injection, but the error messages and screen returns don't come back to the attacker.
- Because thers's a lot of guesswork and trial and error, ***this attack takes a long while to pull off***.

## *Bluejacking*

- Bluetooth attack.
- Bluejacking bezeichnet das Senden unangeforderter Nachrichten über Bluetooth an Bluetooth-fähige Geräte, z. B. Mobiltelefone, PDAs oder Laptops.

- Dabei wird eine sogenannte vCard, welche normalerweise eine Nachricht im Namensfeld (z. B. für Bluedating oder Bluechat) enthält, an ein anderes Bluetooth-fähiges Gerät über das OBEX-Protokoll gesendet.

## *Bluesnarfing*

- Bluesnarfing ist eine spezielle Form von Snarfing über eine Bluetooth-Verbindung, oftmals von Mobiltelefonen unter Verwendung eines anderen Mobiltelefons, Computers, Laptops oder PDAs.
- Bluesnarfing erlaubt den Zugang auf den Kalender, das Adressbuch, E-Mails und Textmitteilungen.
- Es ist ein grösseres Problem als Bluejacking. Programme wie ***Blooover*** nutzen ohne Wissen des Anwenders eine Sicherheitslücke aus.
- Jedes Gerät, das die Bluetooth-Verbindung eingeschaltet hat und auf „für Andere sichtbar" eingestellt ist, kann angegriffen werden.
- Bei ausgeschalteter Sichtbarkeitsfunktion ist das betreffende Gerät vor Bluesnarfing etwas besser geschützt, Sicherheit gewährleistet jedoch nur eine Deaktivierung der Bluetooth Funktion.
- Bluesnarfing greift in die Privatsphäre ein und ist in vielen Ländern illegal.
- Entdeckt wurde die Möglichkeit des „Bluesnarfing" im November 2003 durch Adam Laurie von A.L. Digital, einer englischen Sicherheitsfirma.
- Basiert auf einem Fehler im ***Object-Exchange(OBEX)-Protokoll*** von Bluetooth.

## *Bluebugging*

- Bluebugging erlaubt es versierten Benutzern von Mobiltelefonen, auf fremden Mobiltelefonen, die für diese Art des Angriffs offen sind, (interne) Befehle auszuführen, ohne dass es die Zielperson mitbekommt.
- Diese Angriffsvariante auf Bluetooth-fähige Mobiltelefone wurde von Martin Herfurt im März 2004 auf der CeBIT in Hannover publik gemacht. Als anfällig gelten vor allem Mobiltelefone älterer Generationen.
- Falls der Angreifer keine besondere Ausrüstung hat, muss er sich in einem Abstand von maximal ***10 m vom Ziel-Mobiltelefon*** befinden. Durch spezielle Ausrüstung lassen sich auch grössere Entfernungen überwinden.
- Dem Angreifer stehen verschiedene Nutzungsmöglichkeiten des Mobiltelefons offen, zum Beispiel das Lesen und Versenden von SMS, das Tätigen und Mithören von Anrufen, das Bearbeiten des Adressbuchs oder das Verbinden mit dem Internet

## *Bluesmacking*

- Bluetooth attack
- Is an example of Denial of Service Attack for Bluetooth enabled devices.
- It works like Ping of Death. It uses L2CAP layer to transfer an oversized packet to Bluetooth enabled devices, resulting in a Denial of Service attack.

## *Botnets*

- The computers in abotnet are ***like robots*** (often called ***zombies***) and will do whatever attackers instruct them to do.
- A ***bot herder*** is typically a criminal who controls all the computers in the botnet via one or more command and control servers.
- Botnets of over ***40'000 computers*** are relatively common.

**Examples:**

- Gameover Zeus (GOZ)
- Simda
- Esthost (also called DNSChanger)

**Countermeasure:**

- Ensure ***anti-malware software*** is running and the definitions are up-to-date.
- Keeping ***browsers and their plug-ins*** up-to-date.
- Use browser which are supporting ***sandboxing***.

## *Brute-Force Attacks*

- A brute-force attack is an attempt to ***discover passwords*** for user accounts by systematically attempting all possible combinations of letters, numbers and symbols.
- The longer and more complex a password is, the more costly and time consuming a brute-force attack becomes.

**Countermeasure:**

- Disabling the public IP address and using one of these connection methods:
  Use a point-to-site virtual private network (VPN)
  Create a site-to-site VPN
  Use ***Azure ExpressRoute*** to create secure links from your on-premise network to Azure
- Require two-factor authentication
- Increase password length and complexity
- Limit login attempts
- Implement Captcha
- Limiting the amount of time that the ports are open

## *BREACH Attack*

- “Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext”, is a security exploit against HTTPS when using HTTP compression.
- BREACH is built based on the CRIME security exploit.
- BREACH was announced at the August 2013 Black Hat conference by security researchers Angelo Prado, Neal Harris and Yoel Gluck.
- The idea had been discussed in community before the announcement.

*Source: Wikipedia*

**Example**

```
<script type="text/javascript" src="https://appB.com/appB.js"></script>
```

## *Buffer Overflow Attack*

- E.g. A packet containing a long string of ***NOPs (0x90)*** followed by a command.

## *Business Attack*

- A competitive intelligence attack is a business attack.

## *Chosen-Ciphertext Attack*

- Cryptographic Attack
- Portions oft the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext.

## *Chosen-Plaintext*

- Cryptographic Attack
- Chosen plaintext is encrypted and the output ciphertext is obtained.

## *Ciphertext-Only Attack*

- Cryptographic Attack
- When the attacker has only encrypted messages to work with, this is known as "Ciphertext Only Attack.

## *Collision Attacks*

- Tries to find two inputs producing the same hash.

## *Covert Channel Attacks*

- Storage and timing threat.
- See also CCTT - Covert Channel Tunneling Trojan.
- See also Orange Book.

## *Cryptographic Attacks*

- Analytic Attack
- Implementation Attack
- Statistical Attack
- Brute Force
- Frequency Analysis
- Meet in the middle
- Man in the Middle
- Birthday
- Replay

## *CSRF - Cross Site Request Forgery*

- Also known as ***one-click attack*** or ***session riding*** or ***XSFR.***
- A browser making a request to a server without the user's knowledge.

**Countermeasure:**

- The web application should not use ***random tokens***

## *CSPP Attack*

- Connection Stream Parameter Pollution (CSPP)
- Injection of parameters into a connection string using ***semicolons*** as a separator

## *Cybere War*

- See 26th of April 2007 where ***Estland*** was attacked by a botnet.

## *Data Diddling*

- ***Active attack***.
- Data Diddling is an attack that ***alters data***.
- It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits.

## DB Browser for SQLite

- See: Forensics
- Source: https://sqlitebrowser.org/
- DB Browser for SQLite (DB4S) is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite.

***Features:***

- Create and compact database files
- Create, define, modify and delete tables
- Create, define, and delete indexes
- Browse, edit, add, and delete records
- Search records
- Import and export records as text
- Import and export tables from/to CSV files
- Import and export databases from/to SQL dump files
- Issue SQL queries and inspect the results
- Examine a log of all SQL commands issued by the application
- Plot simple graphs based on table or query data

## *DDoS - Distributed Denial-of Service*

- Attacks involving ***zombied systems (botnets)***.
- A DDoS attack occurs when ***multiple systems*** attack a single system at the same time.
- A ***botnet*** may include infected PCs, security cameras, or a vast array of insecure IoT (Internet of Things) devices.

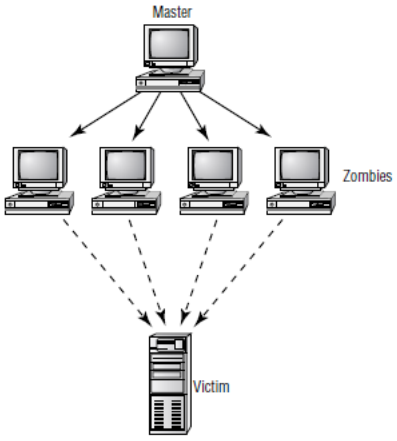



**Figure 24: DDoS Attack**

## *DHCP Starvation Attacks*

- See: **DoS attack**

**Countermeasure:**

- dhcp snooping
- Dynamic ARP Inspection (DAI)

## *Dictionary Attacks*

- A dictionary attack is an attempt to discover passwords by using every possible password in a ***predefined database*** or list of common or expected passwords.

## *DNS cache poisoning*

- See: Kaminsky DNS Vulnerability at: http://unixwiz.net/techtips/iguide-kaminisky-dns-vuln.html
- ***Resolution attack***.

**Countermeasure:**

- ❑ Upgrading to ***DNSSEC***.
- ❑ Restrict the amount of time DNS record can stay in cache.

## *DNS-Spoofing*

**Countermeasure:**

- Install DNS Anti-Spoofing

## *DoS - Denial-of Service*

- A DoS attack is a ***resource consumption attack*** that has the primary goal of preventing legitimate activity on a victimized system.
- DoS attacks can result in ***system crashes***, ***system reboots***, ***data corruption***, ***blockage of services*** and more.
- DoS attacks are not common for internal systems that are not directly accessible via the @Internet.

Commercial DoS & DDoS protection services:

- ***CloudFlare*** or ***Prolexic***

Article http://www.crime-research.org/library/grcdos.pdf

## *DRDoS - Distributed Reflective Denial-of-Service*

- Is a variant of a DoS.
- ***DNS poisoning*** and ***smurf attack*** are examples.

Article: http://www.cs.washington.edu/homes/arvind/cs425/doc/drdos.pdf

## *DROWN Attack*

- See ***SSL v2*** vulnerability

## *Drive-by-download*

- A drive-by-download is code downloaded and installed on a user's system ***without the user's knowledge***.

- Drive-by download means two things, each concerning the ***unintended download of computer software*** from the Internet.
- Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically.
- Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.
- Drive-by downloads may happen when visiting a website, opening an e-mail attachment or clicking a link, or clicking on a deceptive pop-up window: by clicking on the window in the mistaken belief that, for example, an error report from the computer's operating system itself is being acknowledged or a seemingly innocuous advertisement pop-up is being dismissed.

*Source: Wikipedia*

**Examples:**
Zeus, Gumblar

## *Dumpster Diving*

- See: **Passive Reconnaissance Activity**
- Type: Access Control Threat
- Simple tactic of rooting through trash to obtain enough information to make conclusion and create a strategy for attacking a target.

## *Eavesdropping*

- See: **Passive Attack**
- Listening to communication traffic for the purpose of ***duplicating it***.
- Usually requires ***physical access*** to the IT infrastructure.
- Difficult to detect.

***Eavesdropping Tools:***

- T-Sight, Zed Attack Proxy (ZAP) and Cain & Abel.

## *Emanation Attack*

- People can know what you are typing on your keyboard just by analysing the small differences the ***sound of the keys*** on your keyboard make.
- In fact, a computer can quite accurately determine what you are typing ***- just by listening - from 20 meters away***, if it has been trained on the keyboard you're using. The light reflected from your screen, onto the walls and out the window, can even be reconstituted, to a certain degree.
- The idea that an attacker can compromise your computer's security by ***analysing the emanations*** from it - and thus completely bypass most conventional security measures - may come as a shock.

***Source: Daniel Flower***

## *Emotet*

- Emotet ist im Wesentlichen ein "***Banking-Trojaner***", der lokal Transaktionen des Online-Bankings angreift.
- Besteht aus einer Kaskade mehrerer Schadprogramme.
- Das Besondere an Emotet ist die Vielseitigkeit, die sowohl die Schadsoftware an sich als auch deren Verwendung betrifft.

- Emotet greift sowohl Firmen als auch Endbenutzer an
- Der initiale Angriff ist immer eine ***Phishing-Mail***
- Emotet kann andere Schadsoftware nachladen (TrickBot, …) und sich in Netzwerken verbreiten
- Emotet missbraucht Kontakt-Informationen aus ***Outlook***
- Emotet verwendet verschiedene Methoden, um Zugangsdaten für E-Mail-Clients und Browser auszulesen
- Meist verbreitet durch Word Attachments, welche ***makros*** enthalten.

***Countermeasure:***

- Keine Makros ausführen bei ***Office-Products*** attachments aus E-Mails!
- Die Ausführung von Makros einschränken und notwendige Applikationen explizit Whitelisten, siehe ***Office Trust Center***.
- Nur ***signierte Makros*** zuzulassen.
- Keine ***Makros aus dem Internet*** ausführen aktivieren.
- Vertrauenswürdige Speicherorte über ***GPO's*** steuern.

## *Espionage*

- Espionage is the malicious act of gathering proprietary, secret, private, sensitive or confidential information about an organization.

## *Evil Twin Attack*

- Is an attack type for a rogue Wi-Fi access point that appeara to be a legitimate one offered on the premises, but has ben set up to eavesdrop on wireless communications.
- It is the wireless version of the phising scam.
- An attacker fools' wireless users into connecting a laptop or mobile phone toa a tainted hotspot by posing as a legitimate provider.
- This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

## *Fraggle Attack*

- Like smurf attack.
- Instead of ICMP fraggle is using ***UDP packets on port 7 and 19***.

## *Fuzzing Attack*

- To determine if a software program properly handles a wide range of invalid input you may perform a "Fuzzing Attack" with Burp.

## *FREAK Attack*

- Server accepts "***export-grade***" encryption (RSA_EXPORT).

## *Freaking*

- To crack phone systems.

## *Heartbleed*

- Discovered March 2014
- An attacker sends one byte, telling the target system, it sent 64 KB.
  The target machine returns 64 KB data from the memory
- Can expose the ***private key.***

## *Hijacking*

- ***Session-Hijacking:*** Einklinken eines Angreifers in eine autorisierte Browser Session
- ***Browser-Hijacking:*** unbemerktes Ändern der Startseite und der Standardsuche
- ***Domain-Name-Hijacking:*** Entführung fremder Domainnamen
- ***Network-Hijacking:*** Angriff auf einen Server mit dem Ziel, dessen Inhalte zu manipulieren

**Countermeasure:**

- Continuous authenticaton

## *Honeyspot attack*

- A honeyspot attack is when an attacker is using a ***wifi hotspot*** with the same name as the target network to entice client to connect to it.
- A good example would be a WiFi Pineapple from hak5.org.

## *HOSTS poisoning*

- Entries from the ***HOSTS file*** are permanent.

## *IIS Attacks*

- Telnet <Zielrechner> 80 Senden einer GET .../... Anweisung kann einen MS-IIS zum Absturz bringen

## *IP Probes*

- See: **Reconnaissance Attack**
- Also called ***IP sweeps*** or ***Ping sweeps***.

## *Jailbreaking*

- Removes restrictions on iOS devices and permits root-level access to the underlaying operating system.

## *Known-Plaintext*

- Cryptographic Attack
- The attacker has a copy of the plaintext corresponding to the ciphertext.

## *Land Attack*

- Layer 4 Denial of Service (***DoS***) attack
- A land attack occurs when the attacker sends ***spoofed SYN packets*** to a victim using the victim's IP address as both the source and destination IP address.
- This tricks the system into ***constantly replying to itself*** and cause it to freeze, crash or reboot.

Send a spoofed packet with the SYN flag set from a host, on an open port (such as 113 or 139), setting as source the SAME host and port
ie: 10.0.0.1:139 to 10.0.0.1:139)

***Countermeasure:***

- Create access-lists to avoid equal sender and destination address in on packet.

```
interface ethernet 0
ip address 1.2.3.4 255.255.255.0
ip access-group 101 in

interface ethernet 1
ip address 5.6.7.8
ip access-group 101 in

access-list 101 deny tcp 1.2.3.4 0.0.0.0 1.2.3.4 0.0.0.0
access-list 101 deny tcp 5.6.7.8 0.0.0.0 5.6.7.8 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

## *LDAP Injection*

- Username: user1)(&))

**Operators:**
=

>=
<=
~=
*
AND (&)
OR (|)
NOT (!)

## *List-Linking*

- Der Angreifer registriert Sie bei dutzenden von Mailing-Listen als Abonnent.

Zwei derivate: ***Kaboom*** und ***Avalanche***

## *LOGJAM attack*

- Against ***TLS***
- See also ***DHE_EXPORT***
- Action: Disable support for "export cipher suites" and use 2048-bit Diffie-Hellman group

## *Masquerade Attack*

- A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.
- If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.
- Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process.
- The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network.
- The amount of access masquerade attackers get depends on the level of authorization they've managed to attain.
- As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they’ve gained the highest access authority to a business organization.
- Personal attacks, although less common, can also be harmful.

**Countermeasure:**

- Biometric identification

## *MitB - Man-in-the-Browser*

- Der Man-in-the-Browser-Angriff ist eine Sonderform des Man-in-the-middle-Angriffs.
- Man-in-the-Browser (MitB, MITB, MIB, MiB) ist eine Angriffsform auf Rechner, bei der ein Trojaner den Browser des Nutzers infiziert und dann bei Nutzung des Onlinebankings oder eines sozialen Netzwerks die Darstellung von Webseiten verändert und Transaktionen eigenständig durchführen kann.
- Im Gegensatz zum Phishing können die Eingriffe des Schadprogramms dabei vom Nutzer im Normalfall nicht bemerkt werden, da der Nutzer sich auf den echten Seiten der Anbieter bewegt, korrekt eingeloggt ist und die unerwünschten Transaktionen für den Nutzer wie normale Vorgänge angezeigt werden.
- Bekannte Trojaner, die diese Form des Angriffs nutzen sind:
    - Zeus, SpyEye, Carberp, Gozi und Clampi

## *MITC - Man-in-the-Cloud*

- Major cloud services such as ***Box***, ***Google Drive***, ***Dropbox***, and ***Microsoft OneDrive*** are at risk of ‘man-in-the-cloud' (MITC) cyber attacks, according to a research paper published by ***Imperva***.

## *MitM - Man-in-the-Middle*

- A man-in-the-middle attack occurs when a malicious user is able to gain a position logically between the two endpoints of an ongoing communication.

## *Morris-Wurm*

- See: **DoS Attack / Worm**
- Disconnect the target host from the net.

## *MS Blaster*

- See: **Worm**
- Is a computer worm that spread on computers running operating systems Windows XP and Windows 2000 during August 2003.
- Attacks ***Port 135 and 445***.

Countermeasure: **snort**
alert tcp <x> any → <y> 135 (msg: "NETBIOS DCERP ISystemActivator bind attempt")
alert tcp <x> any → <y> 445 (msg: "NETBIOS SMB DCERP ISytemActivator bind attempt")

## *Network Address Hijacking*

- Allows an attacker to ***reroute data traffic*** from a network device to a personal computer.
- Also referred to as ***session hijacking***.
- Network address hijacking enables an attacker to capture and analyze the data addressed to a target system.
- This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.

## *OSINT Attack*

- Source:Github
- Find information from a phone number.

Python 3
Pip 3
PhoneInfoga

## *Pass-the-hash - Attack*

- ???

## *Pass-the-ticket - Attacks*

- ???

## *Password Attacks*

- Brute-force
- Rainbow table
- Sniffing methods
- Password guessing
- Dictionary attacks
- Social engineering attacks
- Hybrid

***Passwort Crack***

Password Change Utility: NT / W2K
hoem.eunet.no/~pnordahl/ntpasswd

Password capturing utility

Amiecod, Ami.com,Aw.com

## *Pharming*

- Pharming is a cyber attack intended to ***redirect a website's traffic*** to another, fake site.
- Pharming can be conducted either by changing the ***hosts file*** on a victim's computer or by exploitation of a vulnerability in ***DNS server software***.
- Compromised DNS servers are sometimes referred to as "***poisoned***".
- Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.
- The term "pharming" is a neologism based on the words ***"farming"*** and ***"phishing"***. Phishing is a ***type of social-engineering attack*** to obtain access credentials, such as usernames and passwords.
- In recent years, both pharming and phishing have been used to gain information for ***online identity theft***.
- Pharming has become of major concern to businesses hosting ecommerce and online banking websites.
- Sophisticated measures known as ***anti-pharming*** are required to protect against this serious threat.

**Countermeasure:**

- Use ***DNSSEC***.
- Secure the ***hosts file***
- Antivirus software and spyware removal software cannot protect against pharming.

## *Phising*

- Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln') versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

***Countermeasure against Macro-Virus:***

- First, never turn macros on, and never trust a document that asks you to turn macros on, especially if it's a Microsoft® Office file that wants you to show hidden content.
- Macros are a very common attack vector.
- Second, always make sure to keep your operating system up to date, especially Microsoft Office programs.
- Third, you likely already mistrust emails from people you don't know. Now, it's time to turn that suspicion onto trusted senders too.
- Attackers commonly try to spoof email addresses to look like those you're familiar with and may even gain control of an email account belonging to a person you know.
- Always err on the side of caution when it comes to emails asking you to download attachments.
- Fourth, it's important to protect your own email account from being hijacked.
- Attackers can use techniques like alternate inboxing to send messages from your account without your knowledge.
- Be sure to secure your account with strong passwords, 2-factor authentication, or use a secure password manager.
- Encourage friends and colleagues to do the same.
- Finally, if you're suspicious of an email, the best way to check its legitimacy is to pick up the phone. If you know the sender personally, ask them about the message in person or via phone.
- Or, if you receive a message from a company, look up their publicly listed phone number (do not use the number provided in the email) and call them.

## *Phreaker*

- Telefon Cracker
- Phreaking is a specific type of attack directed toward telephone systems.

***Black boxes***

- are used to manipulate line voltages to steal long distance services.

***Red boxes***

- are used to simulating inserting coins in a pay phone to get free calls.

***Blue boxes***

- are used to to simulate a telephone operator's console to bypass the normal switching mechanism.

***White boxes***

- are simply portable Touch-Tone Kepads.

## *Ping Floods*

- Are a basical denial of service attack relying on consuming all the bandwidth that a target has available.

## *Ping of Death*

- See: **DoS Attack**
- Sends a malformed ping (ICMP packet) larger than ***65'535 bytes*** to a computer to attempt to crash it.
- When a system received a ping packet larger than 64 KB, it resulted in a problem.
- A ping of death attack is ***rarely successful today*** because patches and updates remove the vulnerability.

Article: http://support.microsoft.com/support/kb/articles/Q132/4/70.asp

## *Port Scans*

- See: **Reconnaissance Attack**
- Layer 4 Attack.
- Also called ***port knocking***.

**Countermeasure:**
Firewall
scanlogd daemon

## *Rainbow Table Attack*

- Uses precomputed hash tables.

## *Replay Attack*

**Countermeasure:**

- Use challenge/response authentication

## *Rubber Hose Attack*

- In cryptography, rubber-hose cryptanalysis is a euphemism for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture.
- Such as beating that person with a rubber hose, hence the name.
- In contrast to a mathematical or technical cryptanalytic attack.
- Without computer

## *RPC Attack*

**RFC's**
1050 (See also RFC 1014, and VMTP for trasnport)
5531
7861

The RPC protocol is independent of transport protocols.

- Transaction_ID (mapping replies to requests

**Ports:**
111 TCP & UDP SUNPRC
121 EPRC
1352 LN RPC (IBM Lotus Notes/Domino)
Portmap (Part of the ONC-RPC protocol family)

**Fields to identify an RPC:**
Remote program number
Remote program version number
Remote procedure number

Check RPC-Language (identical to XDR-Language)

Commands: ***rpcapd.exe***

## *Session Hijacking*

- Involves assuming control of an existing connection after the user has successfully created an authenticated session.
- Session hijackint is the act of unauthorized insertion of packets into a data stream.
- It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.

## *TCP Reset Attack*

- Attackers can spoof the source IP address in a RST packet and ***disconnect active legitimate sessions***.

## *TCP sequence prediction attack*

- A **TCP sequence prediction attack** is an attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets.

## *Teardrop Attack*

- See: **DoS Attack**
- In a ***teardrop attack***, an attacker ***fragments traffic*** in such a way that a system is unable to put data packets back together.
- ***Older systems*** couldn't handle this situation and crashed.
- ***Current systems*** are not susceptible to teardrop attacks.
- Takes advantage of the ***weak fragment assembly functionality*** of the TCP/IP protocol stack.

## *TOCTTOU Attack*

- ***State attack***.
- Attacks in between ***time of check (TOC)*** and ***time of use (TOU)***.
- Also called "***Race Conditions"***.

## *Sabotage*

- Employee sabotage is a criminal act of destruction or disruption committed against an organization by an employee.

## *Salami Attack*

- Steeling very thin slices from an amount.

## *Scavenging*

- See: ***Passive attack***.
- A kind of ***Dumpster Diving***.

- Scavenging is the process of searching through data residue in a system or a network to gain unauthorised knowledge of sensitive information.

## *Shellshock*

- Discovered ***September 2014***
- To gain access to a server.
- Affected many internet-facing services, ***except Windows***.
- goto fail;

***Example:***

```
env x='(){ :;};echo exploit' bash -c 'cat/etc/passwd'
```

## *Shoulder Surfing*

- ***Passive Attack***.

## *Side channel attack*

- An attempt to decode RSA key bits using power analysis.
- In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs).
- Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.
- Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks.
- The rise of Web 2.0 applications and SaaS has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g., through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University.
- Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher.

## *Smishing*

- Mobile device attack with SMS

## *SMTP Attack*

- See: Backscatter

## *Smurf Attack*

- A kind of ***DoS attack***.
- It floods the victim with ***ICMP echo packets***.
- Generate enormous amounts of traffic on a target network by ***spoofing broadcast pings***.
- The attacker sends the ICMP as a broadcast to all systems on the network and ***spoofs the source IP address***.
- Smurf attacks take advantage of an amplifying network by sending a ***direct broadcast*** through a router.

**Countermeasure:**

- Disabling the router from accepting ***broadcast ping messages***
- Configure the routers according ***RFC 2644***

## *Sniffer Attack*

- ***Passive Attack***.
- Also called ***snooping*** or ***eavesdropping attack***.

## *SPIT - Spam over Internet Telephony*

- SPIT ist Telefon-Spam, der über das Internet Protocol mit Hilfe der IP-Telefonie (Voice-over-IP) übertragen wird.
- Als Telefon-Spam bezeichnet man unerwünschte Telefonanrufe, die ***automatisiert*** und in grosser Anzahl eingespielt werden.
- Telefon-Spam ist vergleichbar mit E-Mail-Spam, zurzeit aber ***weniger verbreitet*** und erfordert aufgrund der synchronen Kommunikation andere Schutzmassnahmen.

## *SQL Injection*

- Use unexpected input to a web application.
- Is an ***input validation problem***.

**Three techniques to protect your web applications:**

- Perform Input Validation
- Limit Account Privileges
- Use Stored Procedures

**Example**
Eve'); DROP TABLE Users;--

### *XSS- Cross-Site Scripting*

See:
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

- ***XSS Attacks*** are a type of injection.
- Common XSS attacks use ***HTML tags***, such as ***<script></script>***, ***<IMG>***, ***<INPUT>***, ***<BODY>***, etc.

**Example**
Enter following code in a textbox on a webserver.

```
Test1<SCRIPT>alert(Test2)</SCRIPT>
```

Enter text with brackets like `<, >, {, }` etc. in the application form and double check if the input is displayed correctly in the browser.

**For example, all the scripts below mean the same:**

```
<script>alert(“XSS”)</script>
<sCRipT>alert(“XSS”)</ScRiPt>.............................(Toggle case)
%3cscript%3ealert(”XSS”)%3c/script%3e>...................(Hex encoding)
%253cscript%253ealert(1)%253c/script%253e.................(Double encoding)
```

### *XXE*

- XML External Entity (XXE) Processing

## *SSRF - Server-Side Request Forgery*

- Server-Side Request Forgery (SSRF) vulnerabilities let an attacker send crafted requests from the back-end server of a vulnerable web application.
- Criminals usually use SSRF attacks to target internal systems that are behind firewalls and are not accessible from the external network.
- An attacker may also leverage SSRF to access services available through the loopback interface (127.0.0.1) of the exploited server.
- SSRF vulnerabilities occur when an attacker has full or partial control of the request sent by the web application.
- A common example is when an attacker can control the third-party service URL to which the web application makes a request.

## *SYN Flood Attack*

- See: **DoS Attack / *SYN attack***.

- It disrupts the standard ***three-way handshake*** process.
- In a SYN Flood attack, the attacker sends multiple SYN packets but never completes the connection with an ACK.
- Servers often wait for the ***ACK*** for as long as ***three minutes*** before aborting the attempted session.
- It's common for the attacker to ***spoof the source address***, with each SYN packet having a different source address.

**Countermeasure:**
- Reduce the time a server will wait for an ACK.

## *Tautology*

- This is an overlay complex term used to describe the behavior of a database system when deciding whether a statement is true.
- Because user IDs and passwords are often compared, and the "true" measure allows access, if you trick the database by providing something that is already true (1 does, indeed, equal 1), then you can sneak by.

## *Vulnerability Scans*

- See: **Reconnaissance Attack**

## *Vishing*

- Is a variant of phising that uses the phone system or VoIP.

## *War Dialing*

- War dialing means using a modem to search for a system that accepts inbound connection attempts.

## *Wardriving*

- Ist das systematische Suchen nach Wireless Local Area Networks mit Hilfe eines Fahrzeugs.

## *Whaling*

whaling attack (whaling phishing)

- Is a variant of phishing that targets senior or high-level executives such as CEO's and presidents within a company.
- A whaling attack, also known as whaling phishing or a whaling phishing attack, is a specific type of phishing attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company, as those that hold higher positions within the company typically have complete access to sensitive data.
- In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.
- The term whaling stems from the size of the attacks, and the whales are thought to be picked based on their authority within the company.
- Due to their highly targeted nature, whaling attacks are often more difficult to detect than standard phishing attacks.
- In the enterprise, security administrators can help reduce the effectiveness of whaling attacks by encouraging the corporate management staff to undergo information security awareness training.

## *WinNuke*

- See: **DoS Attack**
- Der Begriff WinNuke bezeichnet eine über Netzwerk ferngesteuerte DoS-Attacke (denial-of-service attack), gegen die folgende Microsoft-Betriebssysteme anfällig sind/waren: Windows 95 (Version A), ***Windows NT*** und Windows 3.1x.

- Das Senden eines TCP-Paketes mit gesetztem ***URG-Flag*** auf den ***TCP-Port #139*** (NetBIOS; als aktiver Bestandteil des Betriebssystems) hat einen „Blauen Bildschirm“ (sogenannter Bluescreen, „blue screen of death“) zur Folge oder verursacht einen Neustart des Rechners.
- Dieser Exploit verursacht keinen primären Schaden am angegriffenen Computer, aber alle nicht gespeicherten Daten sind mit dem Absturz des Systems verloren.

**Exploits:**
Dateiname: winnuke.c
http://winnuke.linkdesign.com/winnuke
http://cvinc.tierranet.com/hacking/files/nukers/WinNuke2.zip
http://www.magmacom.com/~sbrule/winnu95.zip

## *Wrapping Attack*

- See: **SOAP attack**

## *Zero-day*

- A zero-day vulnerability is one the application vendors either don't know about or have not released a patch to remove the vulnerability.

# TOOLS

**Minimum Toolkit for Security Professionals (*Draft*)**

**HARDWARE**

- Intel Core I7 / 20 GB RAM / 512 SSD
- USB-Sticks > 8 GB (for Linux Distributions, Hiren's Boot CD)
- Airpcap
- Mobile capture equipment

**SOFTWARE**

- Windows 10 Professional
- Hyper-V | VirtualBox
  - Kali Linux
    - Metasploit
    - Meterpreter
  - Parrot Security OS
- Notepad++
- Hex Editor Neo
- Nmap
- Visio
- Nessus
- OWASP ZAP (or Burp Suite)
- Wireshark
- Colasoft Packet Builder
- FileZilla
- Snort

### *### SEARCH TAGS ###*

Anti-Forensics
Attack Tool
Compliancy Checker
Disk Management
Encryption
File Recovery (MAC)
Forensics
Forensics Mobile
Forensics Network
Linux Emulation
MDM
Monitoring ARP
Monitoring Registry
Monitoring Windows Services
Online Malware Analysis
Partition Recovery
Password Cracker
Penetration Testing
Privileged Access Management
Reconnaissance
Vulnerability Scanner
Vulnerability Scanner Code
Vulnerability Scanner Webserver
Web Attack Investigation
WHOIS Desktop Tool

### *321Soft Data Recovery*

- See: **File Recovery (MAC)**
- http://www.321soft.com

### *7-Data Partition Recovery*

- See: **Partition Recovery**
- http://7datarecovery.com

### *Accent WORD Password Recovery*

- See: **Password Cracker**
- Source: http://www.passwordrecoverytools.com
- Accent WORD Password Recovery tool recovers lost Microsoft Word passwords.
- It provides full support for all versions of Microsoft Word with lightning-fast recovery of Microsoft Word passwords.

### *Accent EXCEL Password Recovery*

- See: **Password Cracker**
- Source: http://www.passwordrecoverytools.com
- Accent EXCEL Password Recovery recovers lost or forgotten passwords for opening documents and modifying worksheets in Microsoft Excel 95-2010 workbooks.
- It uses three password recovery methods: an advanced dictionary-based attack, a brute-force attack, and a brute-force attack using an advanced mask to recover the passwords.

### *Accent ZIP Password Recovery*

- See: **Password Cracker**
- http://passwordrecoverytools.com

### *Accent RAR Password*

- See: **Password Cracker**
- Recovery http://passwordrecoverytools.com

### *Ace Password Sniffer*

- See: **Forensics Network**
- Source: http://www.effetech.com
- Ace Password Sniffer is a password recovery utility that captures the forgotten passwords.
- It is used to monitor the web activities and monitor password abuse.
- The tool supports and captures passwords through http, ftp, smtp, pop3, and telnet, including some web mail password.
- Ace Password Sniffer ***works passively and does not generate any network traffic***; therefore, it is very hard for others to detect it.
- The tool requires any additional software on the target PCs or workstations if the network is connected through switch, thereby allowing the user to run the sniffer on the gateway or proxy server, which bears all network traffic.
- It also acts as a stealth-monitoring utility and is useful to recover the network passwords, to receive network passwords of children for parents, and to monitor passwords abuse for server administrators.

### *AccessData's FTK*

- See: **Forensics**
- Source: http://accessdata.com
- FTK is a court-cited digital investigations platform.
- It provides processing and indexing up front, so filtering and searching is fast.
- FTK can be setup for distributed processing and incorporate web-based case management and collaborative analysis.

### *AccessData FTK Imager*

- See: **Forensics Mobile**
- Source: http://accessdata.com
- FTK Imager is a standalone disk-imaging program distributed by AccessData, which has the ability to create and save a forensic image of a disk drive in one file or in segments that you can reconstruct later.
- The tool scans the entire hard disk 220ort he required information.
- It also locates the deleted files.
- The FTK Imager is a simple but concise tool.
- It can calculate MD5 hash values and ensures the integrity of the data before closing the files, which results in an image file.
- You can save these image files in several formats.

### *AccessData Mobile Phone Examiner (MPE) Plus*

- See: **SIM Data Acquisition Tools**
- Source: http://accessdata.com
- Mobile Phone Examiner Plus (MPE+) is a mobile device investigation tool that performs smart device acquisition and analysis.
- It contains tools to collect, identify and obtain the data pertaining to a mobile device or a SIM card.

### *Aceso*

- See: **iPhone Data Acquisition Tools**
- Source: http://www.radio-tactics.com
- Aceso is a sound data extraction utility for mobile phones, GPS devices, SIM, and media cards

### *Active@ Disk Image*

- See: **Forensics**
- Source:http://www.lsoft.net
- Data acquisition

### *Active@ File Recovery*

- See: **File Recovery**
- http://www.file-recovery.net

### *Active@ Partition Recovery*

- See: **Partition Recovery**
- Source: http://www.partition-recovery.com

### *Active@ Password Changer*

- See: **Password Cracker**
- Is designed for resetting local administrator and user passwords on Windows XP/Vista/2008/2003/2000, and Windows 7 systems in case an administrator's password is forgotten or lost.
- Forgotten password recovery software has a simple user interface, supports multiple hard disk drives, detects several SAM databases (if multiple OS were installed on one volume), and provides the opportunity to pick the right SAM before starting the password recovery process.
- Active@ Password Changer displays a list of all local users.
- The software user simply chooses the local user from the list to reset the password.
- With Active@ Password Changer you can log in as a particular user with a blank password.

### *Active@ UNDELETE*

- See: **File Recovery**
- http://www.active-undelete.com

### *Active LogView*

- See: **Web Attack Investigation**
- Source: http://www.softcab.com
- Active LogView is a log analysis program that provides analysis of total requests, unique visits, advanced referrers list, hourly summary, user agents list, OS list, advanced filtration, advanced search and more.

### *Active Registry Monitor*

- See: **Monitoring Registry**
- Source: http://www.devicelock.com
- Active Registry Monitor (ARM) is a utility designed for analyzing the changes made to Windows registry - by making the "snapshots" of it and keeping them in the browsable database.
- You can compare any two snapshots and get the list of keys/data which are new, deleted or just changed.
- ARM can do comparing not only in the entire registry but also in any key of the registry.

### *ActiveWhois*

- See: **Web Attack Investigation / WHOIS Desktop Tool**
- Source: http://www.johnru.com
- Price: ?
- ActiveWhois is a network tool for Windows which is used to find any information about the owners of IP address or Internet domain.
- You can determine the country, personal and postal addresses of the owner, and user of IP address and domains. ActiveWhois also allows users to explore DNS aliases.

***Features:***

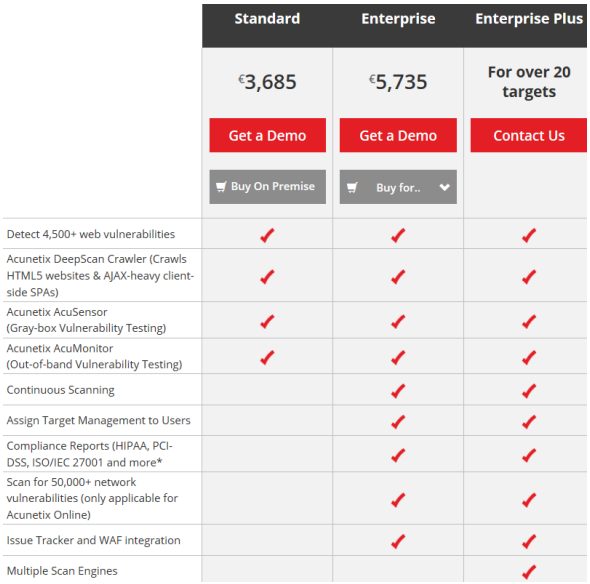
- The WHOIS-hyperlink feature allows you to explore domain databases
- It allows to investigate even international domains.
- Active Whois provides direct links to the domain registrars for each country.
- ActiveWhois can also be used in offline mode.
- All the completed WHOIS requests will be saved to disk and can be instantly retrieved without the need for a live internet connection.
- The NetStat feature allows you to check who is connected to your computer.

### *Acronis Disk Director Suite*

- See: **Partition Recovery**
- http://www.acronis.com

### *Acunetix*

- See: **Vulnerability Scanner**
- Link: https://www.acunetix.com/
- **On premise** or **online**.



| | Standard | Enterprise | Enterprise Plus |
|---|---|---|---|
| | €3,685 | €5,735 | For over 20 targets |
| | Get a Demo | Get a Demo | Contact Us |
| | Buy On Premise | Buy for.. | |
| Detect 4,500+ web vulnerabilities | ✓ | ✓ | ✓ |
| Acunetix DeepScan Crawler (Crawls HTML5 websites & AJAX-heavy client-side SPAs) | ✓ | ✓ | ✓ |
| Acunetix AcuSensor (Gray-box Vulnerability Testing) | ✓ | ✓ | ✓ |
| Acunetix AcuMonitor (Out-of-band Vulnerability Testing) | ✓ | ✓ | ✓ |
| Continuous Scanning | | ✓ | ✓ |
| Assign Target Management to Users | | ✓ | ✓ |
| Compliance Reports (HIPAA, PCI-DSS, ISO/IEC 27001 and more* | | ✓ | ✓ |
| Scan for 50,000+ network vulnerabilities (only applicable for Acunetix Online) | | ✓ | ✓ |
| Issue Tracker and WAF integration | | ✓ | ✓ |
| Multiple Scan Engines | | | ✓ |

## *Adler-32*

- See: **Checksum algorithm for files**
- RFC 1950
- Source: https://hash.online-convert.com/de/adler32-generator
- Hochladen und Erzeugen einer ***ADLER32-Prüfsumme*** einer Datei:

## *ADMmutate*

- See: **IDS evasion**
- ADMutate is an API that is designed to change around the code structure of buffer overflow exploits.
- This polymorphism of the code structure is done in order to mask the signatures of the attack from IDSs by giving the hacker the ability to create variants on the fly.

## *Advanced Archive Password Recovery tool*

- See: **Password Cracker**
- Source: https://www.elcomsoft.com
- Recovers protection passwords or unlocks encrypted ZIP and RAR archives created with all versions of popular archivers.
- The tool recovers passwords for plain and self-extracting archives created with PKZip, WinZip, RAR, and WinRAR automatically or with your assistance.

## *Advanced Disk Recovery*

- See: **File Recovery**
- http://www.systweak.com

## *Advanced EFS Data Recovery tool*

- See: **File Recovery**
- Decrypts the protected files and works on all versions of Windows 2000, XP, 2003, Vista, Windows 7, 8, 8.1, and Windows Server 2008 and 2012.
- Recovery of the data is still possible even when the system is damaged, is not bootable, or when some encryption keys have been tampered with.
- Advanced EFS Data Recovery tool recovers ***EFS-encrypted data*** that becomes inaccessible because of the system administration errors such as removing users and user profiles, misconfiguring data recovery authorities, transferring users between domains, or moving hard disks to a different PC.

### *Advanced Win Service Manager*

- See: **Monitoring Windows Services**
- Source: http://securityxploded.com
- Advanced Win Service Manager is software for smarter analysis of Windows Services.
- It offers many features which set it apart from built-in Service Management Console as well as other similar software.
- Some of the features include Detection of Malicious/Rootkit Services, Automatic Threat Analysis, Service Filter mechanism, Integrated Online Virus/Malware Scan, Color based Threat Representation, and HTML/XML based Service Report, etc.

### *ADExplorer*

- See: **AD Explorer**
- Source:https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer
- Sysinternals / ADExplorer.exe
- LDAP Enumeration with Active Directory Explorer
- In fact, a penetration test begins before testers have even contacted victim systems.
- During enumeration, information is systematically collected, and individual systems are identified.
- Pen testers examine the systems in their entirety, which allows them to evaluate security weaknesses.

### *ADS Spy*

- See: **Reconnaissance**
- Source:https://adspy.com
- Searching for ADS on ***Facebook*** and ***Instagramm***
- The powerful software that keeps top advertisers innovating and holds social media organizations to account for their content.
- Using our unparalleled array of data and innovative search functionality, uncovering the ads that you need to see becomes a simple task.

### *Advanced Disk Recovery*

- See: **Forensics**
- Source: http://www.systweak.com
- Advanced Disk Recovery scans the entire system for deleted files and folders and provides an opportunity to recover them.
- Hard drives, partitions, external devices, and even CDs and DVDs can be scanned for recoverable files using Advanced Disk Recovery.
- The software offers two types of scans.
- The Quick Scan uses the Master File Table to find all files with the same filename.
- The Deep Scan uses file signatures to search for deleted files or folders.
- After either type of scan, one can preview the deleted files and folders, and restore any or all of them to the location of choice.
- With just a few clicks, one can locate and restore most of the deleted files.

### *Advance Data Recovery Software Tools for NTFS*

- See: **Partition Recovery**
- http://www.recoverdatatools.com

### *Advanced Office Password Recovery*

- See: **Password Cracker**
- Source: http://www.elcomsoft.com
- Advanced Office Password Recovery unlocks documents created with all versions of Microsoft Office.
- It recovers passwords for Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher, and OneNote.

### *Advanced IP Scanner*

- See: **Scanner**
- Source: https://www.advanced-ip-scanner.com/de/
- Pricing: ***Freeware***
- Zuverlässiger und kostenloser Netzwerk-Scanner zur Analyse lokaler Netzwerke.
- Das Programm scannt alle Netzwerkgeräte, ermöglicht Ihnen den Zugriff auf freigegebene Ordner und FTP-Server sowie die Fernsteuerung von Computern (über RDP und Radmin).
- Zudem ermöglicht es Ihnen, Computer aus der Ferne auszuschalten.
- Es ist einfach zu bedienen und wird als portable Edition ausgeführt.
- Das Programm sollte für jeden Netzwerkadministrator die erste Wahl sein.

### *Advanced PDF Password Recovery*

- See: **Password Cracker**
- Source: https://www.elcomsoft.com
- Advanced PDF Password Recovery recovers password-protected or locked PDF documents created with all versions of Adobe Acrobat or any other PDF application.

### *AFICK (Another File Integrity Checker)*

- See: **File and Folder Integrity Checkers**
- Source: http://afick.sourceforge.net
- Afick is a portable utility which acts as an aid in intrusion detection as well as helping to monitor the overall integrity of the system.
- It also monitors changes in the file system of your machine and reports them back to you, thereby letting you decide whether any given change was expected.

### *Aid4Mail Email Forensic software*

- See: **E-Mail Forensics**
- Source: http://www.aid4mail.com
- Aid4MailTMis used to quickly and reliably migrate email accounts, easily transfer messages between email apps and web-based services.

### *AIM Sniffer*

- See: **Forensics Network**
- Source: http://www.effetech.com
- AIM Sniffer is a network utility to capture and log AIM (AOL Instant Messenger) chat from computers within the same LAN.
- The tool supports messaging through AIM server and direct connection messaging.
- All intercepted messages are well organized by AIM user with buddies and shown instantly on the main window.
- It provides a features report system to export captured AIM conversations as HTML files for later analyzing and reference.

### *Aircrack-NG*

- See: **WiFi Password Cracker**
- See also: Kali Linux
- Source: https://www.aircrack-ng.org/
  https://github.com/aircrack-ng/aircrack-ng
- Price: GENERAL PUBLIC LICENSE (GPL)
- CLI or GUI
- Complete suite of tools to assess WiFi network security.
- Password cracker
- Default cracking method is ***PTW***
- Can also use the ***FMS/KoreK*** method

**Features**

❑ Monitoring: Packet capture

- ❑ Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- ❑ Testing: Checking WiFi cards and driver capabilities
- ❑ Cracking: WEP and WPA PSK (WPA 1 and 2)

***Example:***

```
Aircrack-ng <..cap> -w <pwdfile.txt>
```

## *Aireplay-ng*

***Example:***

```
aireplay-ng -0 50 -a <C8:...> -c <c8:..> <wlan0mon>
aireplay -ng -0 0 -a 0A:00:2B:40:70:80 -c mon0
```

## *Airgeddon*

- See: **WiFi Cracking**
- Source: Kali Linux

## *Airmon-ng*

***Example:***

```
airmon-ng start <wlan0mon>
PID killen
Kill xxx
```

## *Airodump-ng*

***Example:***

```
Airodump-ng <wlan0mon>
Airodump-ng -bssid <bssid> -c <channel> -w <Testfile> <wlan0mon>
```

## *AiroPeek NX*

- See: **WiFi Sniffer**
- Source: www.techrepublic.com
- Supplier: WildPackets
- Wireless sniffer

## *Airsnarf*

- See: **WiFi**
- Stealing usernames and passwords from an AP.

## *AirSnort*

- See: **WiFi Password Cracker**
- Source: airsnort.soft112.com
  sourceforge.net
- Supplier: SNAX
- Further development of AirSnort ***stopped in 2004***
- ***Cracking*** wireless encryption keys WEP on an 802.11b network
- Operates by passively monitoring transmissions, computing the encraption key when enough packets have been gathered.

## *AirWatch*

- See: **Enterprise Mobile Management**
- See also: Workspace ONE
- Source: https://www.air-watch.com/
- Mobile Device Management (MDM)

## *Alert Logic Log Manager*

- See: **Forensics Network**

- Source: https://www.alertlogic.com
- Alert Logic Log Manager with ActiveWatch is a Security-as-a-Service (SaaS) solution that meets compliance requirements and identifies security issues across the entire environment, including public cloud.
- It collects, processes, and analyzes data.

### *Alchemy Network Monitor*

- See: **Forensics Network**
- Source: http://www.mishelpers.com
- Alchemy Eye monitors network server availability and performance.
- It supports over 50 monitoring types, including, but not limited to ICMP ping, NT Event Log monitoring, HTTPS/FTP URL checking, free disk space monitoring, etc.
- Alchemy Eye notifies the Network Administrator about server malfunction events.
- It logs application events to a log file.
- Different log file detail levels (none/normal/full) and log file formats (text, HTML, CSV, SQL database) can be configured using the application.

### *Alien Registry Viewer*

- See: **Monitoring Registry**
- Source: http://lastbit.com
- Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files.
- While RegEdit shows the contents of the system registry, Alien Registry Viewer works with registry files copied from other computers.
- Alien Registry Viewer can be extremely useful for system administration and forensic computer examination purposes.

### *AlienVault Unified Security Management*

- See: **Forensics Network**
- Source: https://www.alienvault.com
- AlienVault Unified Security ManagementTM (USM) is a platform that provides unified, coordinated security monitoring, security event management and reporting, continuous threat intelligence and multiple security functions without multiple consoles.

### *Andriller*

- See: **Forensics Mobile**
- Andriller allows Android smartphone users to retrieve data from their smartphones by using powerful forensic tools.
- These tools provide the means to extract data automatically from the non-rooted devices by using a set of decoders.
- Andriller enables investigators to import several database files processed by the application and used to generate reports.
- Investigators can use the decoders for Android devices that can obtain account information, messages, contacts, call history, browser data, and much more for investigation.

### *Angry IP Scanner*

- See: **IP Scanner**
- Source: https://angryip.org/
- Price: Freeware
- Angry IP scanner is a fast, simple, and efficient IP address and ***port scanner***.
- It simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc.
- The amount of gathered data about each host can be extended with plugins.

### *Anubis*

- See: **Online Malware Analysis**
- Analyzing Unknown Binaries

- Source: http://anubis.iseclab.org
- Anubis is a tool for analyzing the behavior of ***Windows PE-executables***, with a focus on malware analysis.
- It generates a report file that contains enough information about the purpose and the actions of the analyzed binary.
- The generated report includes detailed data about modifications made to the Windows registry or file system, about interactions with the Windows Service Manager or other processes, and of course it logs all generated network traffic.

## *AnVir Task Manager*

- See: **Monitoring Windows Services**
- Source: http://www.anvir.com
- AnVir Task Manager controls everything running on the user's computer.
- It offers all of its features in a single interface instead of releasing multiple packages to perform a family of related tasks.

***Features:***

- Monitors processes, services, startup programs, etc.
- Replaces Windows Task Manager
- Gets rid of spyware and viruses
- Speeds up the system and Windows startup

## *ArchiMate*

- See: **Enterprise Architecture Modeling Tool**
- Is an open and independent ***enterprise architecture modeling language*** to support the description, analysis and visualization of architecture within and across business domains in an unambiguous way.

## *Archive.org*

- See: **Reconnaisance**
- Shows past versions of a website

## *Armitage*

- See: **Penetration Testing**
- Armitage is a fantastic Java-based GUI ***front-end for the Metasploit Framework*** developed by Raphael Mudge.

## *Apache Logs Viewer (ALV)*

- See: **Web Attack Investigation**
- Source: http://www.apacheviewer.com
- Apache Logs Viewer (ALV) enables you to view, monitor, and analyze the ***Apache*** / ***IIS*** / ***nginx*** logs.

## *ApexSQL Audit*

- See: **Database Forensics**
- ApexSQL Audit is a SQL Server auditing tool, which provides auditing access, changes, and security on SQL Server instances, databases, and objects.
- It audits queries, DDL and DML operations, security events (authentication changes, permissions changes, and attempted logins), events on stored procedures and functions.
- ApexSQL Audit saves captured information in a centralized auditing repository and provides comprehensive reports.
- Analyzing the volatile data with ApexSQL Audit helps forensic investigators gain insight on the login activities, the client connected to the server and the database on which the transactions occurred.

## *ApexSQL Log*

- See: **Forensics Network / Database Forensics**

- Source: http://www.apexsql.com
- ApexSQL Log is a SQL Server database transaction log reader that can present all the information in a human readable format.

### *API Monitor*

- See: **API Calls Monitor**
- API Monitor is a software that allows you to spy and display Win32 API calls made by applications.
- It can trace any exported APIs and displays a wide range of information, including function name, call sequence, input and output parameters, function return value and more.
- It's a useful developer tool for seeing how win32 applications work and learn their tricks.

### *AppleXsoft File Recovery for Mac*

- See: **File Recovery (MAC)**
- http://www.applexsoft.com

### *APKTool*

- See: **Pentesting**
- The APKTool utility for decompiling Android applications.

### *ArcSight ESM*

- See: **Forensics Network**
- Source: http://www8.hp.com
- HPE Security ArcSight ESM is a security management application that combines event correlation and security analytics to identify and prioritize threats in real time, thereby facilitating immediate response and remediation.

### *ARPWALL*

- See: **Countermeasure for ARP attacks**
- Source: https://sourceforge.net/projects/arpwall/
- Price: Freeware
- This tools will give early warning when arp attack occurs and simply block the connection.

### *ARPWatch*

- See: **Monitoring ARP**
- To detect ARP Poisoning.

### *Asleap*

- See: **Penetration Testing**
- Source: https://tools.kali.org/wireless-attacks/asleap
- See also: Kali Linux
- Exploits weak protection provided by Cisco LEAP networks.

### *Assuria Log Manager*

- See: **Forensics Network**
- Source: http://www.assuria.com
- This tool is used for the collection of forensically sound logs from almost any source into a central store.
- It allows enterprise-wide automated management of logs, including log rotation.

### *Athena*

- See: **iPhone Data Acquisition Tools**
- Source: http://www.radio-tactics.com
- Athena enables the investigator to extract and process communication and positioning information from GPS, satellite handsets, phones, and other portable devices.

## *Atola Insight Forensic*

- See: **Forensics**
- Source: http://atola.com
- Atola Insight Forensic provides complex data retrieval functionalities with utilities for accessing hard drives at the lowest level, wrapped in an efficient user interface.
- The tool is designed by recovery engineers, law enforcement agencies, and forensic experts.

## *Auditpol*

- See: **AD Tool**
- Viewing, Enabling and Clearing Audit Policies

***Features***

- Set and query a system audit policy.
- Set and query a per-user audit policy.
- Set and query auditing options.
- Set and query the security descriptor used to delegate access to an audit policy.
- Report or back up an audit policy to a comma-separated value (CSV) text file.
- Load an audit policy from a CSV text file.
- Configure global resource SACLs.

## *Autopsy*

- See: **Forensics**
- Source: http://www.sleuthkit.org
- Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools.
- It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.
- You can even use it to recover photos from your camera's memory card

```
http://localhost:9999/autopsy
```

## *AutoRuns for Windows*

- See: **Startup Programs Monitoring**
- Source: http://technet.microsoft.com
- Autoruns for Windows has the knowledge of auto-starting locations of any startup monitor, shows what programs are configured to run during system bootup or login, and shows the entries in the order Windows processes them.
- These programs include ones in the startup folder, Run, RunOnce, and other Registry keys.
- One can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

## *AWStats*

- See: **Web Attack Investigation**
- Source: http://www.awstats.org
- AWStats is a graphical tool that generates the web, streaming, ftp or mail server statistics.
- This log analyzer works as a CGI or from the command line and shows all possible information your log contains.

## *BASE - Basic Analysis and Security Engine*

- Source:sourceforge.net
- BASE is the ***Basic Analysis and Security Engine***.
- It is based on the code from the Analysis Console for Intrusion Databases (ACID) project.
- This application provides a web front-end to query and analyze the alerts coming from a ***SNORT IDS system***.

### *Backtrack*

- See: **Exploit Tool**

### *Batch IP Converter*

- See: **WHOIS Desktop Tool**
- Source: https://www.softpedia.com
- Source: http://www.sabsoft.com
- Batch IP Converter is a network tool to work with IP addresses.
- It combines Domain-to-IP Converter, Batch Ping, Tracert, Whois, Website Scanner and Connection Monitor into a single interface as well as an IP-to-Country Converter.

### *BatchPurifier*

- See: **Anti Forensics Tool**
- http://www.digitalconfidence.com

### *BBProxy*

- See: **Penetration Testing**
- For blackjacking attack

### *BCTextEncoder*

- BCTextEncoder simplifies ***encoding and decoding text data***.
- Plain text data are compressed, encrypted and converted to text format, which can then be easily copied to the clipboard or saved as a text file.

### *BeEF*

- See: **Penetration Testing**
- Source: https://beefproject.com/
- Kali Linux (Beef xss Framework)
- BeEF is short for The **Browser Exploitation Framework**.
- It is a penetration testing tool that focuses on the ***web browser***.
- Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using ***client-side attack vectors***.
- Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system and examines exploitability within the context of the one open door.
- The web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context

### *Belkasoft Browser Analyzer*

- See: **Forensics**
- http://belkasoft.com

### *Belkasoft Evidence Center*

- See: **Forensics**
- http://belkasoft.com

### *Belkasoft Live RAM Capturer*

- See: **Forensics**
- Source: http://belkasoft.com
- Data acquisition

### *Bettercap*

- See: **WiFi Attack**
- Source: bettercap.org

- Bettercap is the Swiss Army knife for ***WiFi***, ***Bluetooth Low Energy***, wireless HID ***hijacking*** and ***Ethernet networks reconnaissance*** and ***MITM attacks***.

### *BetterWhois*

- See: **WHOIS OnlineTool**
- Source: http://www.betterwhois.com
- BetterWhois offers a unified WHOIS search allowing you to check the domain availability, display domain ownership, and verify nameserver information across hundreds of domain registrars.

### *Bhavesh Virus Maker*

- See: **Virus**
- Source:https://sourceforge.net/projects/bhavesh-virus-maker/

### *Big Mother*

- See: **Forensics Network**
- Source: http://www.tupsoft.com
- Big Mother is a switchsniff with zero configurations used as an internet activity monitoring tool.
- Big Mother is an ***eavesdropping*** program that uses a switch sniffer to capture and analyze communication traffic over a network.
- The tool not only logs in real time URL visits, email, chats, games, FTP, and data flows but also takes webpage snapshots, duplicates email and FTP copies, records MSN messenger content, and gives statistical reports.
- It freely restricts online activities with time schedules and according to customized filtering Internet rules.
- The program will set up itself and perform content monitoring and access control to keep family members or employees accountable for their actions

### *Bitdefender QuickScan*

- See: **Online Malware Analysis**
- Source: http://quickscan.bitdefender.com
- Bitdefender QuickScan is an online virus scanner that detects hidden threats, malware, and keyloggers.
- It uses in-the-cloud scanning technology to detect active malware on a system.

### *BitGlass*

- See: **CASB**
- Source:https://www.bitglass.com
- Agentless cloud security
- Agentless security broker on any device
- Bitglass' Next-Gen Cloud Access Security Broker (***CASB***) solution enables your enterprise to embrace the cloud while ensuring data security and regulatory compliance.
- Bitglass secures your data across any cloud app and any device.

### *BitLocker*

- See: **Defense**
- Encrypts an entire volume

1. Open Windows File Explorer
2. Navigate to “This PC”
3. Right mouse click on the drive you would like to turn on BitLocker
4. Choose “Turn on BitLocker”
5. Choose the way you would like to unlock the drive:
   “Password” or “Smart Card” protected.
6. Backup your recovery key:
   Either save it to a file or print it

7. Decide how to encrypt the drive:
   Either only the used disk space or the entire drive
8. Choose encryption mode:
   XTS-AES if the disk is only used on one device

### *BlackIce Defender*

- See: **HIDS**
- Source: Pearson Software
- Personal FW

### *BlackStratus LOGStorm*

- See: **Forensics Network**
- Source: http://www.blackstratus.com
- LOGStormTM is a log management and log monitoring solution that combines log management with correlation technology, real-time event log correlation and log monitoring, and an integrated incident response system.

### *Blade® Professional v1*

- See: **Forensics Mobile**
- Source: http://www.digital-detective.net
- Blade is the perfect tool for the retrieval of data from a mobile phone.
- Equipped with the latest technology, this software is tremendously effective in recovering MPEG-4/3GP/ISO Base video files.
- Blade supports all the major forensic image formats.
- The professional modules have inbuilt Intelli-Carve validation and interpretation routines to facilitate accurate data recovery.

### *Blancco Flash*

- See: **Anti Forensics Tool**
- http://www.blancco.com

### *Blue Coat*

- See: **Web-Security**
- Supplier: Symantec
- Network ***visibility***, ***acceleration*** and ***security***.

### *Blue Coat Data Loss Prevention (DLP)*

- See: **Data Loss and Leakage Prevention**

### *Boomerang Data Recovery*

- See: **File Recovery (MAC)**
- https://www.boomdrs.com

### *Brutus*

- See: **Password cracker**
- Source: www.darknet.org.uk
- No UNIX/LINUX version is available

### *Bulk extractor*

- See: **Forensics**
- Source: http://www.forensicswiki.org
- The bulk extractor is a computer forensics tool that scans a disk image, a file or a directory of files and extracts useful information without parsing the file system or file system structures.

## *Buster Sandbox Analyzer*

- See: **Monitoring Registry**
- Source: http://bsa.isoftware.nl
- Buster Sandbox Analyzer is a tool that has been designed to analyze the behavior of processes and the changes made to the system and then evaluate if they are malware suspicious.

## *Burp Suite*

- See: **Web Attack**
  **Vulnerability Scanner Webserver**
- Source: https://portswigger.net/burp

***Enterprise Version***
- USD 3999/Year
- Web vulnerability scanner
- Scheduled & repeated scans
- Unlimited scalability
- CI integration

***Professional Version***
- USD 399/Year
- Web vulnerability scanner
- Advanced manual tools
- Essential manual tools

***Community Version***
- Free
- Essential manual tools

***Usage***
cmd>java -jar -Xmx2G <Burp location> → Expand memory for Burp suite
Cert: http://burp

## *Cain & Abel*

- See: **Forensics**
- Source: oxid.it
- Supplier: Oxid
- Password cracker.
- Password recovery tool for ***MS OS Systems***.
- Uses ***Brute force*** attacks with dictionary
- Recording ***VoIP*** conversations
- Decoding ***VoIP traffic***
- Decoding scrambled passwords
- Decoding ***Cisco VPN config files***, ***.PCF*** files
- Recovering ***WLAN keys***

## *Caine-Live-CD und -usB*

- See: ***IT-Forensik***
- Caine (***C***omputer ***A***ided ***IN***vestigative environment) kann auf einen bootfähigen Datenträger kopiert werden.
- Die Tool-Sammlung mit italienischen Wurzeln verwendet als Betriebssystem die GNU/Linux-Distribution Ubuntu.
- Zu den Hauptmerkmalen gehört eine anwenderfreundliche Benutzeroberfläche, die mit einer grossen Anzahl von Forensik- und Incident-Response-Werkzeugen gekoppelt ist.
- Die Umgebung wird laufend angepasst und erhält Updates.
- Ein schönes Feature ist zudem ein halbautomatischer Report-Generator.
- Infos: www.caine-live.net

## *CallerIP*

- See: **IP and Port monitoring Tool**
- Source: http://www.callerippro.com
- ***Desktop installation*** required
- CallerIP informs you when someone has connected to your computer and can report the IP address. It also runs a trace on that IP address.
- See all incoming and outgoing connections made to your computer. Including process names, remote and internal port numbers and much more. Learn more.
- Automated alerts bring your attention to illegal connections
- Automated Alerting
- Set up alerts to warn you of intruders and hack attempts. CallerIP can send an email, display a warning dialog and/or append a log file. Learn more.
- CallerIP server allows you to view all incoming and outgoing connections to your computer from any browser in the world. Learn more.
- CallerIP plots all connecting IP locations on a world map.
- IP origin and connecting IP addresses shown on world map

## *Capsa*

- See: **Forensics Network**
- Source: http://www.colasoft.com
- Price: 30 days Trial
- Capsa is a ***portable network analyzer*** application for both LANs and WLANs which performs real-time packet capturing capability, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis.
- It goes one step ahead of sniffing by intuitively analyzing network packets and ***generating meaningful information***.
- Network administrators can use Capsa's comprehensive high-level window view for monitoring entire network, quick insight to network administrators or network engineers that allows rapidly pinpointing and resolving application problems.

***Features:***

- ❑ Extended network security analysis
- ❑ Versatile traffic & bandwidth statistics
- ❑ Advanced network protocol analysis
- ❑ Multiple network behavior monitoring
- ❑ Automatic expert network diagnosis

## *Ccleaner*

- See: **Startup Programs Monitoring**
- Source: https://www.piriform.com
- CCleaner is a utility for computers running Microsoft Windows that cleans out the 'junk' that accumulates over time: temporary files, broken shortcuts, and other problems.
- CCleaner protects your privacy.
- It cleans your browsing history and temporary internet files, allowing you to be a more confident Internet user and less susceptible to identity theft.
- CCleaner can clean unneeded files from various programs saving you hard disk space, removes unnecessary entries in the Windows Registry, help you uninstall software and select which programs start with Windows.

## *Cellebrite UFED Logical Analyzer*

- See: **SIM Data Acquisition Tools**
- Source: http://www.cellebrite.com
- The Cellebrite UFED Logical extracts and analyzes data from mobile devices and has a built-in SIM reader that allows the device to obtain data such as call logs, phonebooks, SMS, IMSI, and the ICCID.
- The device even supports SIM card cloning.

### *Chanalyzer*

- See: **WiFi**
- Source.metageek.net
- Extension: (.wsx)
- You can download a trial version, but registration is required.

### *Chameleon Startup Manager*

- See: **Startup Programs Monitoring**
- Source: http://www.chameleon-managers.com
- Chameleon Startup Manager can control the programs that run at Windows startup, which makes Windows start faster, operate with increased stability, and lower the HDD usage.
- It also offers program launch options with fixed or automatic delayed startup (each program is initiated in sequence after the previous one finishes starting), allowing the computer to be started as quickly and smoothly as possible.
- Programs run according to various functions including startup order change, priority, consecutive program launch, and day selection.
- A user can create and select the configurations at Windows startup or applied without restarting Windows.

### *Change Tracker Enterprise*

- See: **File and Folder Integrity Checkers**
- Source: https://www.newnettechnologies.com
- Change Tracker is a system integrity monitoring tool used for real-time breach detection.
- Closed-Loop Intelligent Change Control (CLICC) reconciles the benefits of forensic-level change control with the hitherto onerous workload associated of reviewing and acknowledging reported changes.
- Change Tracker learns the difference between good and bad changes, automatically promoting legitimate changes to Planned Changes, leaving behind only potentially harmful, unplanned changes for review.

### *CHIRP*

- See: **WiFi**
- Source: Kali Linux

### *CHKROOTKIT*

- See: **Defense**
- Source: Kali Linux
  chkrootkit.org
- CLI
- To check promiscuous mode
- Shell script that checks system binaries for rootkit modifications.
- Chrootkit is a simple command line utility that scans your system for known rootkits.
- Chkrootkit doesn't remove rootkits.
- Chances are, if you're infected with one, you're going to be doing a fresh install unless you get lucky enough to be able to remove it manually.
- That said, it's still an amazing tool for detecting potential breaches.

### *CHNTPW*

- See: **Password Cracker**
- Is a SW utility for resetting or blanking local passwords used by WNT, W2K, WXP, WVista, W8, and W8.1

### *Cisdem DataRecovery 3*

- See: **File Recovery (MAC)**
- http://www.cisdem.com

### *Clang*

- See: **Vulnerability Scanner Code**
- Source: https://clang-analyzer.llvm.org/
- The Clang Static Analyzer is a source code analysis tool that finds bugs in C, C++, and Objective-C programs.

### *CloudInspect*

- See: **Penetration testing tool**
- Penetration tests for Amazone Web Services (AWS).

### *CloudPassage Halo*

- See: **Vulnerability Scanner**
- Source: www.cloudpassage.com
- "CloudPassage Halo" is a security automation platform that delivers comprehensive visibility, protection, and continuous compliance monitoring to reduce cyber security risks.
- Unlike other solutions that provide limited coverage, CloudPassage Halo finds critical risks in your ***AWS*** and ***Azure*** deployments that another tools miss.

### *CmosPwd*

- See: **Password Cracking**
- Source: http://www.cgsecurity.org
- CmosPwd is CMOS/BIOS password recovery tool.
- It decrypts passwords stored in CMOS used to access BIOS SETUP.
- CmosPwd works and compiles under Dos-Win9x, Windows NT/W2K/XP/2003, Linux, FreeBSD, and NetBSD.

### *Code Compare*

- See: **Vulnerability Scanner Code**
- Source: https://www.devart.com/codecompare/download.html
- Price: ***Open-source***, Free version available or paid version
- Resolves merge conflicts and deploys source code changes
- Integrates with TFS, SVN, Git, Mercurial and Perforce
- Standalone diff tool or Visual Studio extension
- Supports C#, C++, Visual Basic, JavaScript, Java and XML
- It is designed to compare and merge files and folders.
- You can use it as a standalone tool or as a ***Visual Studio extension***.
- When identifying issues, you will see colored blocks for inserted, deleted or modified text.
- You can edit files on the fly and click for a quick merge.

### *CommView*

- See: **Forensics Network**
- Source: http://www.alchemy-lab.com
- CommView is a network monitor and analyzer designed for LAN administrators, security professionals, network programmers, home users, and anyone who wants a full picture of the traffic flowing through a PC or LAN segment.
- The application captures every packet on the wire to display important information such as a list of packets and network connections, vital statistics, and protocol distribution charts.
- CommView allows the users to examine, save, filter, import, and export captured packets, view protocol decodes down to the lowest layer with full analysis of supported protocols.
- With the information, CommView can help the users pinpoint network problems and troubleshoot software and hardware.

### *ConfigMgr*

- See: **Monitoring**
- Microsofts inventory monitoring tool.
- See also MS System Center Configuration Manager

### *Colasoft Packet Builder*

- See: **Forensics Network & Packet Crafting**
- Source: www.colasoft.com
- Pricing: Free Edition
  Professional Edition $
- Colasoft Packet Builder enables creating custom network packets; users can use this tool to check their network protection against attacks and intruders.
- Colasoft Packet Builder includes a very powerful editing feature.
- Besides common HEX editing raw data, it features a Decoding Editor allowing users to edit specific protocol field values much easier.
- Users are also able to edit decoding information in two editors - Decode Editor and Hex Editor. Users can select one from the provided templates Ethernet Packet, ARP Packet, IP Packet, TCP Packet and UDP Packet, and change the parameters in the decoder editor, hexadecimal editor or ASCII editor to create packets.
- Any changes will be immediately displayed in the other two windows. In addition to building packets, Colasoft Packet Builder also supports saving packets to packet files and sending packets to network.
- Packet replayer!

### *Comodo Cloud Scanner*

- See: **Monitoring Registry**
- Source: https://www.comodo.com
- Comodo Cloud Scanner (CCS) is a system scanning tool that identifies malware, viruses, suspicious processes and other problems with your computer.
- Apart from identifying the viruses and malware, CCS also identifies other problems like Windows Registry errors that cause system instability, issues that threaten your privacy and junk or garbage files that occupy your valuable disk space.

### *Core Impact*

- See: **Penetration Testing**
  **Vulnerability Scanner**
- Source: https://www.coresecurity.com
- Supplier: Core Security
- Pentest like results.
- Used for penetration testing.

### *CorreLog*

- See: **Forensics Network**
- Source: https://correlog.com
- CorreLog is a solution for cross-platform IT security log management and event log correlation.
- It allows real-time event log collection across both distributed and mainframe systems.
- Event logs generated from CorreLog Agents are ready format for the CorreLog SIEM Correlation Server or any SIEM correlation engine.

### *Coverity*

- See: **Vulnerability Scanner Code**
- Source: https://scan.coverity.com/
- Find and fix defects in your ***Java***, ***C/C++, C#***, ***JavaScript***, ***Ruby***, or ***Python*** open source project for free.

### *Covert_TCP*

- Using ***Covert Channels***
- Networks use network access control permissions to permit/deny the traffic through them.
- Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, web proxies to allow certain traffic.
- Covert channels can be made by inserting data into unused fields of protocol headers.

- There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.
- Covert_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination.
- It can act like a server as well as a client and can be used to hide the data transmitted inside a IP header.
- This issue fule when bypassing firewalls and sending data with legitimate looking packets that contain no data for sniffers to analyze.

## *Cppcheck*

- See: **Vulnerability Scanner Code**
- Source:http://cppcheck.sourceforge.net/
- Is a static analysis tool for ***C/C++*** code.
- It provides unique code analysis to detect bugs and focuses on detecting undefined behaviour and dangerous coding constructs.
- The goal is to detect only real errors in the code (i.e. have very few false positives).

## *cRARk 5.1*

- See: **Password Cracker**
- http://www.crark.net

## *Crowdstrike Falcon*

- See: **Endpoint Protection**
- Cloud-native endpoint protection platform.
- OS version on the endpoints needs to be part of Compatibility matrix
- Machine must have ENS installed
- Falcon has received third-party validation for the following regulations:
  ***PCI DSS v3.2*** | HIPAA | NIST | FFIEC | PCI Forensics | NSA-CIRA | SOC 2 | CSA-STAR | AMTSO | AV Comparatives.

## *Crunch*

- See: **Wordlist Creator**
- Create password-List

***Example***

```
crunch 8 8 abcABC0123456789 -o pwd.txt
```

## *CryptaPix*

- See: **Anti Forensics Tool**
- http://www.briggsoft.com

## *Cryptcat*

- See: **Encryption**
- Cryptcat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol while encrypting the data being transmitted with ***twofish***.
- Enables to communicate between two systems and encrypts the communication between then with ***twofish***.
- It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.
- At the same time, it is a feature-rich ***network debugging*** and ***exploration tool***, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

## *CryptoForge*

- See: **File and Text Encryption**

- CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages, by encrypting them with strong encryption algorithms.

## *CrypTool*

- See: **Basic Disk Encryption**
- CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms.
- It has the typical look and feel of a modern Windows application.
- CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

## *CSP File Integrity Checker*

- See: **File and Folder Integrity Checkers**
- Source: https://www.cspsecurity.com
- CSP File Integrity Monitor provides granular monitoring of changes to specified disk files.
- By storing unique fingerprints for selected disk files based on particular attributes (contents, security settings etc.) and then monitoring for change, FIC enables strict compliance to security policies, including “PCI DSS” regulations.
- Any detected changes are flagged in reports and can be used to generate alerts.

***Key Features:***

- Monitors Guardian and OSS files.
- Meets PCI DSS regulation 11.5.
- Unique file fingerprint.
- GUI display for file management.
- Full audit reporting capability.
- Audit database of change history.
- Alerts for unauthorized change.
- Easily integrated with enterprise compliance tools.
- Easy setup and intuitive GUI.

## *CurrPorts*

- See: **Port Monitor**
- CurrPorts is network monitoring software that displays a list of all currently opened TCP/IP and UDP ports on a local computer, along with the processes running on its ports.

## *CyberArk*

- See: **Privileged Access Management**
- Source: https://www.cyberark.com/de/
- Centralized management and controlling of credentials and accounts.
- >= 80% of serious security incidents involve the ***misuse of privileged accounts***.
- >= 51% of companies have suffered ***SSH*** key-related compromises.

## *Cygwin*

- See: **Linux Emulation**
- Linux-like environment for Windows
- A large collection of GNU and Open Source tools which provide functionality similar to a Linux distribution on Windows.
- A DLL (cygwin1.dll) which provides substantial POSIX API functionality.

## *DAEMON Tools Pro 7*

- See: **Forensics**
- Source: https://www.daemon-tools.cc
- Data acquisition

### *DaveGrohl*

- See: **Password Cracker**
- Source: http://davegrohl.org
- DaveGrohl is a multi-threaded distributed password cracker aiming at brute-forcing OS X user passwords.
- Initially created in early 2011 as a password hash extractor and companion tool but has since evolved into a standalone or distributed password cracker.
- It supports the entire standard Mac OS X user password hashes (MD4, SHA-512, and PBKDF2) used since OS X Lion and also can extract them formatted for other popular password crackers such as John the Ripper.
- The latest stable release is designed specifically for Mac OS X Lion and Mountain Lion.

### *Data Acquisition Toolbox*

- See: **Forensics**
- Source:https://www.mathworks.com
- Data acquisition

### *Data Extractor*

- See: **Forensics**
- Source:http://www.deepspar.com
- Data acquisition

### *Data Pilot Secure View Kit*

- See: **Forensics Mobile**
- Source: http://www.datapilot.com
- Data pilot secure view kit helps in analyzing data, synchronization, and backing up of the data.
- It also allows for the recovering of deleted data from the mobile.

### *Data Rescue 4*

- See: **File Recovery (MAC)**
- http://www.prosofteng.com

### *Data Rescue PC*

- See: **File Recovery**
- http://www.prosofteng.com

### *Data Recovery for Mac*

- See: **File Recovery (MAC)**
- https://www.binarybiz.com

### *Data Recovery Pro*

- See: **File Recovery**
- http://www.paretologic.com

### *Data Stash*

- See: **Anti Forensics Tool**
- http://www.skyjuicesoftware.com

### *DBAN*

- See: **Anti Forensics Tool**
- http://www.dban.org

### *DataNumen Outlook Repair*

- See: **E-Mail Forensics**

- Source: https://www.datanumen.com
- DataNumen Outlook Repairscans the corrupt Outlook personal folders (.pst) files and recovers mail messages, folders, posts, calendars, appointments, meeting requests, contacts, distribution lists, tasks, task requests, journals, notes, etc. in them, thereby minimizing the loss in file corruption.

### *DataThief*

- See: **Pentesting**
- To automate SQL injections and exploit databases.
- DataThief III is a program to extract (reverse engineer) data points from a graph.
- Typically, you scan a graph from a publication, load it into DataThief, and save the resulting coordinates, so you can use them in calculations or graphs that include your own data.

### *DDR Professional Recovery Software*

- See: **File Recovery**
- http://www.recoverybull.com

### *Deep Log Analyzer*

- See: **Web Attack Investigation**
- Source: http://www.apacheviewer.com
- The Deep Log Analyzer is a web analytics solution for small and medium size websites.
- It analyzes web site visitors' behavior and gets the complete website usage statistics in easy steps.

***Features:***

- It provides website statistics and web analytics reports presentation with interactive navigation and hierarchical view
- It analyzes logs from popular web servers, such as ***IIS*** on Windows, ***Apache*** or ***Nginx*** on Unix/Linux, etc.
- It enables viewing of aggregated reports and allows its comparison reports for different intervals

### *DeepSound*

- See: **Anti Forensics Tool**
- http://jpinsoft.net

### *DeepSpar*

- See: **Forensics**
- Source:http://www.deepspar.com
- DeepSpar Disk Imager is a disk imaging system specifically built to ***handle damaged drives***.

### *DevBug*

- See: **Vulnerability Scanner Code**
- Source:http://www.devbug.co.uk/
- ***PHP*** Static Code Analysis.

### *Device Seizure*

- See: **Forensics**
- "Device Seizure is a ***forensic acquisition*** and ***analysis tool*** used for examining ***cell phones***, ***PDAs***, and ***GPS devices***.
- The program also comes with ***hardware***, so you are well-equipped for ***mobile forensics***.
- Device Seizure has been upheld in dozens of court cases. There is a new feature in the system: Paraben's Point 2 Point, which takes data points and converts them into a format that can be read by Google Earth.
- The program has ***low system requirements***, meaning it can be run on older machines.

- Depending on the model, the tool can acquire the following types of data: ***SMS messages***, including deleted messages, ***phonebook*** information, ***call history***, received calls, dialed numbers, missed calls, call dates and durations, ***datebook*** information, scheduler, calendar, to-do list information, filesystem, system files, multimedia files, java files, deleted data, quicknotes, GPS, RAM/ROM, PDA databases, e-mail, and registry data.

### *Directory Monitor*

- See: **File and Folder Integrity Checkers**
- Source: https://directorymonitor.com
- Directory Monitor can be used by the investigators for the surveillance of certain directories and network shares and will notify the investigator of file changes/access, deletions, modifications, and new files in real-time.
- Users and processes making the changes can also be detected. It provides text logs, automation via script/application execution, emailing, writing to a database, sound notifications, etc.
- The tool monitors local directories or network shares including hidden/private shares, enable snapshots to ensure changes can be detected while the network is down and even during power outages.

### *DiskDigger*

- See: **File Recovery**
- Source:http://diskdigger.org

### *Disk Drill*

- See: **File Recovery**
- http://www.cleverfiles.com

### *Disk Drill for Mac*

- See: **File Recovery (MAC)**
- http://www.cleverfiles.com

### *Disk Doctors Mac Data*

- See: **File Recovery (MAC)**
- Recovery http://www.diskdoctors.net

### *DiskInternals Mail Recovery*

- See: **E-Mail Forensics**
- Source: http://www.diskinternals.com
- DiskInternals Mail Recovery can automatically locate, recover and fix broken Outlook Express, Vista Mail, Microsoft Outlook, Server Storage Archive and The Bat email databases on severely corrupted and damaged disks in one action.

### *Disk Imager Forensic Edition*

- See: **Forensics**
- Source:http://www.deepspar.com
- Data acquisition

### *Disk Jockey PRO*

- See: **Forensics**
- Source:http://www.diskology.com
- Data acquisition

### *DiskPulse*

- See: **Monitoring**
- Source: http://www.diskpulse.com

- DiskPulse is a ***disk change monitoring solution*** allowing investigators to monitor changes in one or more disks and directories, send E-Mail notifications, save various types of reports, generate statistical pie charts, export detected changes to an SQL database, send error messages to ***the*** system event log and execute custom commands when a user-specified number of changes detected.
- The tool intercepts file system change notifications issued by the operating system and detects newly created files, modified files, deleted files and renamed files.
- All file system changes are detected in real-time allowing one to send an E-Mail notification, execute a custom command and save a disk change monitoring report within a couple of seconds after one or more critical changes detected.
- The Investigator is provided with the ability to review, categorize and filter detected file system changes, generate various types of statistical reports showing the number of changes per file extension, the number of changes per change type, the number of changes per user, etc.

## *Ditto Forensic FieldStation*

- See: **Forensics**
- Source. https://www.cru-inc.com
- Data acquisition

## *Dmitry - Deepmagic Information Gathering Tool*

- See: **Reconnaissance**
- Source: Kali Linux
- Author: James Greig
- License: GPLv3
- Command Line Tool
- Deepmagic Information Gathering Tool
- DMitry is a UNIX/(GNU)Linux Command Line Application coded in C.
- DMitry can gather as much information as possible about a host.

**Features:**

- Port scanning
- Gather subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more

**Options:**

`-o filename`
Create an ascii text output of the results to the "filename" specified. If no output filename is specified then output will be saved to "target.txt". If this option is not specified in any form output will be sent to the standard output (STDOUT) by default. This option MUST trail all other options, i.e. "./dmitry -winseo target".

`-i`
Perform an Internet Number whois lookup on the target. This requires that the target be in the form of a 4 part Internet Number with each octal seperated using the '.' notation. For example, "./dmitry -i 255.255.255.255".

`-w`
Perform a whois lookup on the 'host' target. This requires that the target be in a named character format. For example, "./dmitry -w target" will perform a standard named whois lookup.

`-n`
Retrieve netcraft.com data concerning the host, this includes Operating System, Web Server release and UpTime information where available.

`-s`
Perform a SubDomain search on the specified target. This will use serveral search engines to attempt to locate sub-domains in the form of sub.target. There is no set limit to the level of sub-domain that can be located, however, there is a maximum string length of 40 characters (NCOL 40) to limit memory usage. Possible subdomains are then reversed to an IP address, if this comes back positive then the resulting subdomain is listed. However, if the host uses an asterisk in their DNS records all resolve subdomains will come back positive.

`-e`

Perform an EmailAddress search on the specified target. This modules works using the same concept as the SubDomain search by attempting to locate possible e-mail addresses for a target host. The e-mail addresses may also be for possible sub-domains of the target host. There is a limit to the length of the e-mail address set to 50 characters (NCOL 50) to limit memory usage.

`-p`

Perform a TCP Portscan on the host target. This is a pretty basic module at the moment, and we do advise users to use something like nmap (www.insecure.org/nmap/) instead. This module will list open, closed and filtered ports within a specific range. There will probably be little advancement upon this module, though there will be some alterations to make it a little more user friendly. There are also other options for this module that can affect the scan and its relative output.

`-f`

This option will cause the TCP Portscan module to report/display output of filtered ports. These are usually ports that have been filtered and/or closed by a firewall at the specified host/target. This option requires that the '-p' option be passed as a previous option. For example, "./dmitry -pf target".

`-b`

This option will cause the TCP Portscan module to output Banners if they are received when scanning TCP Ports. This option requres that the '-p' option be passed as a previous option. For example, "./dmitry -pb target".

`-t`

This sets the Time To Live (TTL) of the Portscan module when scanning individual ports. This is set to 2 seconds by default. This is usually required when scanning a host that has a firewall and/or has filtered ports which can slow a scan down.

```
dmitry [IP]
dmitry -e [IP] Search for possible E-Mail addresses
dmitry -n [IP] Retrieve Netcraft.com information about a host
dmitry -f [IP] Shows open ports
dmitry -p [IP] Shows open ports
dmitry -pb [IP]       TCP Portscan + banner
dmitry -pf [IP]       TCP Portscan
dmitry -s [IP] Search for subdomains
```

### *dnmap*

- See: **Nmap Tool**
- Source: Kali Linux
- Is a ***framework*** to distribute nmap scans among several clients.
- It reads an already created file with nmap commands and send those commands to each client connected to it.
- The framework uses a client/server architecture.
- The server knows what to do and the clients do it.
- All the logic and statistics are managed in the server. Nmap output is stored on both server and client.
- Usually you would want this if you have to scan a large group of hosts and you have several different internet connections (or friends that want to help you).

```
dnmap_client <ip>
dnmap_server <ip>
```

### *DNS Tunnel*

- See: **DNS-Tool**
- TCP over DNS

### *DNSQuerySniffer*

- See: **DNS Monitoring**

### *DNSstuff*

- See: **WHOIS Online Tool**
- See: DNS Monitoring

- Source: http://tools.dnsstuff.com
- It allows forensic analysis of name and email servers, path analysis, authenticating and locating domains.

### *Domain Dossier*

- See: **WHOIS Online Tool**
- Source: http://centralops.net
- Domain Dossier is an online tool used to investigate domains and IP addresses.

### *DumpSec*

- See: **Enumeration tool**

### *Dr. Web Online Scanners*

- See: **Online Malware Analysis**
- Source: http://vms.drweb.com
- Dr. Web Online Scanner is an online tool that needs a suspicious file or link to scan.
- This tool allows file scan, link scan, and virus database search.
- After the analysis of the suspicious file or links, the tool generates a detailed report of detected viruses, worms, and various kinds of adware, and sends it to the requester

### *Driver Detective*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.drivershq.com
- Driver Detective removes guesswork in resolving driver problems by providing instant access to the most relevant content for your computer's hardware.

***Features:***

- Scans your PC to determine the manufacturer, family, model, and motherboard
- Easy Migrator will automatically scan your computer's hardware, download all of the latest drivers for any destination operating system that you choose, and then creates a device-driver migration CD
- Ensures that the downloads do not contain viruses
- Possess tools necessary to keep the computer running at its best
- Provides accurate recommendations for user's computer
- Has a built-in wizard that allows you to copy (backup) your downloaded drivers to a CD, network drive, or USB flash drive

### *Driver Fusion*

- See: **Device Drivers Monitoring Tool**
- Source: https://treexy.com
- Driver Fusion is the complete device and driver solution for your PC that can manage and monitor your devices and their drivers.
- You can install and uninstall drivers with Driver Fusion, including the ability to backup, restore and download drivers with ease.
- The effortless health check, including an automatic driver updater to update outdated drivers and install missing drivers, lets you scan and fix detected issues quickly.
- Furthermore, you can disable, enable and restart devices while Windows is running.
- With our cloud-powered removal engine, you can delete the driver entries that are left behind by the normal uninstallers, which is especially useful when you are updating a driver or changing a device.

### *Driver Magician*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.drivermagician.com
- Driver Magician allows device drivers backup, restoration, update and removal in Windows operating system.

- It identifies all the hardware in the system, extracts their associated drivers from the hard disk and backs them up to a location of your choice.
- It has a built-in database of the latest drivers with the ability to go to the Internet to receive the driver updates.
- If there are unknown devices in the PC, Driver Magician helps to detect them with its built-in hardware identifier database.

### *Driver Reviver*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.reviversoft.com
- Driver Reviver restores maximum performance and functionality to the user PC's hardware and its components.

***Features:***

- Ensures that the user PC and its components are performing at their optimum levels
- It tracks down each driver for each single piece of hardware connected to the PC
- Scans for drivers downloads them and installs them correctly
- Prevents users from incorrectly using the wrong driver
- Eliminates the risk of downloading a faulty driver or even malware
- Ensures that if there are any problems with an update, the changes can be reversed to get the system back up and running

### *DriverEasy*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.drivereasy.com
- DriverEasy tool automatically scans and analyzes users' systems.

***Features:***

- Fixes driver issues
- Detects unknown device drivers
- Keeps drivers up-to-date with latest versions
- Secures user's system with backup of Installed drivers, easy to roll back or restore them
- Uninstalls removed device drivers to speed up booting

### *DriverGuide Toolkit*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.driverguidetoolkit.com
- DriverGuide Toolkit identifies and lists drivers installed on the computer and when connected to the Internet, allows one to search DriverGuide.com (and other sources) for driver updates and manufacturer sites.
- In addition, it allows to take a backup of currently installed drivers for safe keeping.

### *DriverView*

- See: **Device Drivers Monitoring Tool**

### *DriveSpy*

- See: **Device Drivers Tool**
- Link: digitalintelligence.com
- Supplier: Digitalintelligence
- See: Forensics
- DOS application, does not run under Windows
- Drive forensics

### *dSniff*

- See: **Forensics Network**
- Source: Kali Linux
- Sniffing passwords, Email and HTTP traffic.

- arpredirect, macof, tcpkill, tcpnice, filesnarf, mailsnarf.
- Sniffs both switched and shared networks.
- Uses the arpredirect and macof tools.
- Capture authentication information for FTP, telnet SMTP, HTTP, POP, NNTP, IMAP.

## *E-Mail Bomben*

Serie von Nachrichten (tausende)!
Grösse, in der Regel 2 Mbyte.

**E-Mail-Bomben-Pakete**

| | |
|---|---|
| Up Yours | UPYOURS3.zip, UPYOURS3.exe, MAIL-CHECK.exe, UPYOURSX |
| Kaboom | KABOOM3.zip, KABOOM3.exe, KABOOM3!.zip, WSERR.DLL |
| The Unabomber | UNA.exe, KWANTAM.nfo |
| The Windows Email Bomber | BOMB.exe, BOMB.txt, BOMB02B.zip |
| Gatemail | GATEMAIL.c |
| Unix Mail-Bomber | MAILBOMB.C |

**Abhilfe:**

Kill Files
Exclusionsschemen
Mail-Filter

**SPAM-Filter Applications:**

| | |
|---|---|
| Advanced E-Mail Protector | http://wwwantispam.org |
| E-Mail Chomper | http://www.sarum.com/echomp.html |
| SPAM Attack Pro | http://www.softwiz.com |
| SPAM Buster | http://www.contactplus.com |
| SPAM Killer | http://www.spamkiller.com |
| DCC | Distributed Checksum Clearinghouses<br>The Distributed Checksum Clearinghouses or DCC is an anti-spam content filter that runs on a variety of operating systems. The counts can be used by SMTP servers and mail user agents to detect and reject or filter spam or unsolicited bulk mail. DCC servers exchange or "flood" common checksums. The checksums include values that are constant across common variations in bulk messages, including "personalizations."<br>Does not need to check the content. |

## *EASEUS Data Recovery Wizard*

- See: **Forensics**
- Source: http://www.easeus.com
- It is hard drive data recovery software to recover data lost from PCs, laptops, or other storage media because of deleting, formatting, partition loss, OS crash, virus attack etc.

***Features:***

- Supports large hard disk.
- Specify your recovery file types before scanning for precise searching results.
- Filter your search by file name, type, and date to find files.
- Preview the files to check their details and quality before you decide to recover them.

## *EASEUS Email Recovery Wizard*

- See: **E-Mail Forensics**
- Source: http://www.wisecleaner.com
- EaseUS Email Recovery Wizard is an email recovery software to recover deleted or lost emails, folders, calendars, appointments, meeting requests, contacts, tasks, task requests, journals, notes and attachments from corrupted .pst file.
- It is a safe and read-only utility which reads the lost/deleted mail items without modifying the existing content and restores the lost data into a new file.

### *EDGAR Database*

- See: **Footprinting tool**
- Source: https://www.sec.gov/edgar.shtml

### *EFF DES Cracker*

- See: **DES Brute Force**
- Source:w2.eff.org
- Supplier: Electronic Frontier Foundation
- Performs ***brute force attack*** of the DES cipher key space.

### *EffeTech HTTP Sniffer*

- See: **Forensics Network**
- Source: http://www.effetech.com
- EffeTech HTTP Sniffer is a HTTP packet sniffer, protocol analyzer, and file reassembly software based on windows platform.
- Unlike most other sniffers, this sniffer dedicates itself to capture IP packets containing HTTP protocol, rebuild the HTTP sessions, and reassemble files sent through HTTP protocol.
- Its smart real-time analyzer enables on-the-fly content viewing and captures, analyzes, parses, and decodes HTTP protocol.
- By delivering an easy to use and award-winning HTTP monitoring utility, the EffeTech HTTP sniffer has become the preferred choice of managers, network administrators, and developers worldwide.
- Information about HTTP traffic can received by all via LAN.

### *EFS - Encrypting File System*

- See: **Defense**
- Encrypts individual files and directories

### *Elcomsoft iOS Forensic Toolkit*

- See: **iPhone Data Acquisition Tools**
- Source: https://www.elcomsoft.com
- Elcomsoft iOS Forensic Toolkit performs the complete forensic acquisition of user data stored on the iPhone/iPad/iPod devices running any version of iOS.

### *ELM Enterprise Manager*

- See: **Forensics Network**
- Source: http://tntsoftware.com
- ELM Enterprise Manager elevates Windows event log monitoring to real-time.
- Events logs are collected reliably after they are written.

### *Email Address Verifier*

- See: **E-Mail Forensics**
- Source: https://tools.verifyemailaddress.io
- This email address verification technology connects to mailboxes to check whether an email address exists or not.

### *Email Checker*

- See: **E-Mail Forensics**
- Source: http://email-checker.net
- Email Checker is a simple tool for verifying an email address.
- It's free and quite easy to use.
- Just enter the email address and hit check button.
- Then it tells you whether the email address is real or not.

- It extracts the MX records from the email address and connect to mail server (over SMTP and also simulates sending a message) to make sure the mailbox really exist for that user/address.

### *EMail Detective - Forensic Software Tool*

- See: **E-Mail Forensics**
- Source: http://www.hotpepperinc.com
- This application is used to extract any MBOX or AOL email that has been cached or saved on a user's disk.
- Additionally, a comprehensive report is produced that contains all the emails for a user.
- This report can then be instantly viewed and searched for any specific words or phrases by the investigator.

### *emailTrackerPro*

- See: **E-Mail Forensics**
- Source: http://www.emailtrackerpro.com
- EmailTrackerPro not only offers the ability to trace an email using the email header but it also comes with a spam filter (advanced edition), which scans each email as it arrives and warns the user if it is suspected spam.
- Stops spam email before it reaches its intended recipient.

### *Empire*

- CCTV
- Access Controls
- Barriers
- Visitor Management System
- Walkie Talkies

### *EnCase Forensic*

- See: **Forensics / E-Mail Forensics**
- Supplier: Guidance Software
- Source: https://www.guidancesoftware.com

- ***EnCase Forensic Software*** is designed for law enforcement and security analysts who need to investigate all types of digital storage devices. It facilitates the search, identification, collection, preservation, analysis and reporting of digital evidence in a court-approved manner. It is the only computer forensic application that has withstood numerous court challenges worldwide.
- EnCase has been used in hundreds of thousands of cases worldwide and mentioned in more than 70 published court cases. The EnCase Evidence File, a container for digital evidence that maintains and verifies the chain-of-custody of digital evidence, is a robust evidence container. Tens of thousands of users have worked with EnCase software. Thousands of people have attained EnCase Certified Examiner status. Millions of cases have used EnCase Evidence Files. Nearly every ***eDiscovery*** service provider uses EnCase Evidence File. This level of court validation, and the fact that EnCase Evidence Files are a leading preservation/authentication mechanism for digital evidence, makes it the most credible way to collect forensically sound electronic data in the industry today.
- EnCase's passive ***servlet (agent)*** is simply installed on all machines on the network and awaits instructions. Moreover, it provides a secure way to manage IT/legal personnel's access to network assets. Through the use of Secure Authentication for EnCase (SAFE), users can be restricted from performing search and collect activities in a number of different ways, including by subnetwork, time of day, region, etc. Additionally, all user activity is logged, ensuring compliance with regulatory guidelines.
- With EnCase, an enterprise can expect to see a significant reduction in costs associated with electronic data collection. The software's ability to search and collect information over the network in a non-intrusive way allows enterprises to avoid expensive travel costs since it eliminates the need to have personnel travel to remote locations to gather data. Positive

customer return on investment (ROI) generally occurs in the short term after implementing EnCase.
- Though no analyst firm tracks computer forensic shipments, many professionals in the computer forensics community say Guidance Software is the market leader in this space with more than 33,000 copies of EnCase Forensic sold.

### *ENUM-Tool*

- See: **Enumeration**
- Enum Tool is a Python application designed to digest OME XML schema and produce meaningful output about enumerations.

### *Enum4linux*

- See: **Enumeration**
- Enumerating information from Windows and Samba host.
- Enum4linux is a tool for enumerating information from Windows and Samba systems.
- As a security expert you have to secure process where the attacker can establish an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.
- You should know what info is available to the attacker and secure that info before anyone misuses it.

### *ESET SysInspector*

- See: **Monitoring**
- Source: http://www.eset.com
- ESET SysInspector is a diagnostic tool that helps troubleshoot a wide range of system issues. It tracks down the presence of malicious code.

### *EtherApe*

- See: **Forensics Network**
- Source: http://etherape.sourceforge.net
- EtherApe is a graphical network monitor for UNIX modeled after etherman.
- The tool features link layer, IP and TCP modes, and graphically displays network activity.
- Hosts and links change in size with traffic.
- Color-coded protocols display.
- EtherAPE supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus several encapsulation formats.
- It can filter traffic and can read packets from a file as well as live from the network.
- It can also export node statistics.

### *EtherDetect Packet Sniffer*

- See: **Forensics Network**
- Source: http://www.etherdetect.com
- EtherDetect Packet Sniffer is a sniffing tool that can capture full packets organized by TCP connections or UDP threads and passively monitor the network, with any program installations on target PCs.
- The tool enables packet viewing in Hex format and syntax highlighting viewer.

***Features:***

- Organizes captured packets in a connection-oriented view
- Captures IP packets on the LAN with nearly no packets losing.
- Functions as a real-time analyzer, enabling on-the-fly content viewing while capturing and analyzing.
- Enables parse and decode a variety of network protocol.
- Supports saving captured packets for reopening afterward.
- Allows syntax highlighting for application data in the format of HTML, HTTP, and XML.

### *Ettercap*

- See: **Forensics Network**
- Source: http://ettercap.sourceforge.net
- Mainly for Unix based systems!
- Injection of HTML code
- Ettercap is a comprehensive suite for ***man-in-the-middle attacks***.
- The tool features sniffing of live connections, content filtering on the fly, and many other interesting tricks.
- Ettercap supports active and passive dissection of many protocols and includes many features for network and host analysis.
- Check out for ➔ IPv4 Identification: 0xe77e

### *Event Log Explorer*

- See: **Forensics Network**
- http://eventlogxp.com
- Event Log Explorer is a software solution for viewing, analyzing and monitoring events recorded in Microsoft Windows event logs.
- Event Log Explorer simplifies the analysis of event logs (security, application, system, setup, directory service, DNS, and others).

### *EventLog Analyzer*

- See: **Forensics Network**
- Offers log management for network security
- Monitors application Logs and generates reports
- Stays informed on event activities in real-time
- Offers holistic approach for network IT security
- Checks if audit is ready and compliant

### *EventReporter*

- See: **Forensics Network**
- Source: http://www.eventreporter.com
- EventReporter is a Windows event log processor and syslog forwarder.
- It is used to consolidate multiple event logs and create a central repository.

### *EventSentry*

- See: **Forensics Network**
- Source: http://www.eventsentry.com
- It receives critical alerts and consolidates all your logs in one place with real-time event log, log file, and Syslog monitoring.
- It offers sophisticated rule sets to ensure you only get the alerts you need.
- It also offers web-based reporting which gives you a unique insight into all of your logs.

### *EventTracker Enterprise*

- See: **Forensics Network**
- Source: http://www.eventtracker.com
- EventTracker Enterprise is a log management tool and includes features such as File Integrity Monitoring, Change Audit, Config Assessment, Cloud Integration, Event Correlation, and writeable media monitoring.

### *ExactFile*

- See: **File and Folder Integrity Checkers**
- Source: http://www.exactfile.com
- ExactFile is checksum calculation that supports multiple files.
- ExactFile (both the console and GUI versions) fully support Unicode.
- ExactFile also supports extremely large files.

- ExactFile supports a one-step process for “stamping” a deployment folder with a checksum digest and GUI file scanner that can be burned to the CD along with the rest of your files.
- Run the scanner, and it will automatically start checking the integrity of the files on the CD, telling you once-and-for-all if the disc is damaged.
- This makes it easy for your customers and clients to find out if their disc has been damaged, or if there is some other problem that needs to be worked out.

### *Exchange Deleted Email Recovery*

- See: **E-Mail Forensics**
- Source: http://www.emaildoctor.org
- This Product features MS Exchange Server Email Data EDB File recovery from any extent of file corruption, protection and deletion thus eliminating server downtime.

### *Exiv2*

- See: **Anti Forensics Tool**
- http://www.exiv2.org

### *F-Response Imager*

- See: **Forensics**
- Source:https://www.f-response.com
- Data acquisition

### *Faraday IDE*

- See: **Penetration Testing**
- Kali Linux

### *FastSum*

- See: **Monitoring**
- Source: http://www.fastsum.com
- FastSum, built upon the MD5 checksum algorithm, is a tool for checking the integrity of the files.
- FastSum computes checksums according to the MD5 checksum algorithm, which gives easy to compare and store outputs.

### *FCIV*

- See: **Encryption**
- Source:http://download.microsoft.com
- CLI
- It is a command line utility that computes ***MD5*** or ***SHA1*** cryptographic hashes for files.

### *Fern WiFi Cracker*

- See: **WiFi**
- Source:Kali Linux
- GUI

Kali Linux built in wordlists
`/computer/usr/share/wordlists`


## *fgdump*

- See: **Password Cracker**
- Source: http://foofus.net
- Fgdump is basically a utility for dumping passwords on Windows NT/2000/XP/2003/Vista machines.
- It comes with an inbuilt functionality that has all the capabilities of PWdump and can also do several other crucial things, such as executing a remote executable, dumping the protected storage on a remote or local host, and grabbing cached credentials

## *Fiddler*

- See: **http Monitoring**
- Source:http://www.telerik.com/download/fiddler
- Fiddler hilft beim Protokollieren, Debuggen und Beeinflussen von HTTP-Verkehr zwischen Netz und Gerät.

## *File Scavenger*

- See: **File Recovery**
- http://www.quetek.com

## *File Viewer*

- See: **Forensics**
- Source: http://www.accessoryware.com
- File Viewer is a ***Disk/File Utility*** that helps to locate, view, print, organize, and exchange files over the internet using e-mail components.
- It can search for many common file types, or groups of file types, display, print, organize or send files over the internet, find and display pictures, videos, sounds, music, text files, documents, spread sheets, database, and system files, locally over the LAN or on the internet.
- Picture file types supported by the file viewer are JPG, JPG2000, GIF, uncompressed TIF, TIFF, BMP, ICO, CUR, PCX, DCX, PCD, FPX, WMF, EMF, FAX, RAW, XPB, XPM, IFF, PBM, CUT, PSD, PNG, TGA, EPS, RAS, WPG, PCT, PCX, CLP, XWD, FLC, ANI, SGI, XBM, etc.

## *File-Wiping Utilities*

- See: **Anti Forensics Tool**
- BCWipe, R-Wipe & Clean, Eraser, CyberScrubs PrivacySuite

## *FileMerlin*

- See: **Forensics**
- Source: http://www.file-convert.com
- Converts word processing, spreadsheet, presentation and database files between a wide range of file formats.
- Widely regarded as the premier ***document conversion product***, it is suitable for straightforward as well as complex documents, and is the most accurate, complete and flexible such solution that we know of.

### *FILERECOVERY® 2016*

- See: **File Recovery (MAC)**
- http://filerecovery.com

### *FileSalvage*

- See: **File Recovery (MAC)**
- http://subrosasoft.com

### *FileVerifier++*

- See: **File and Folder Integrity Checkers**
- Source: http://www.programmingunlimited.net
- FileVerifier++ is a Windows application for verifying the integrity of files.
- FileVerifier supports various algorithms using dynamically loadable hash libraries.
- It uses the Windows API and doesn't have any dependencies other than what comes with Windows (WinFVC excluded).
- Permanent installation is not required

***Some of its feature are listed below:***

- Can load and save results to and from various formats
- Hash algorithms can be added through the dll interface
- Can load hash results and compare to what is actually on your disk
- Color coding of validity states
- Verification considers file size, file attributes, and modification date to be significant
- Drag and drop support
- Recursive directory processing

### *FileZilla*

- See: **FTP Client**

### *FINALeMail*

- Supplier Finaldata
- Source:finaldata.com
- Windows application
- To recover deleted e-mails
- MS Outlook Express, Netscape Mail, Eudora

Pricing:

- Free version available

### *Firebug*

- See: **Reconnaisance**

### *FireEye*

- See: **Thread detectionForensic Sorter**
- Supplier: Paraben
- Designed for computer forensic examiners to help organize and speed up the examination of the contents of a hard drive.
- Forensic Sorter allows you to sort the contents of entire hard drives into categories such as video, audio, spreadsheets, etc. so you can easily find what you're looking for.
- Filter out common Windows files, recover deleted files or file fragments in slack, deleted, and unallocated space.

### *Firewalk*

- See : **Penetration Testing**
- See also : Kali Linux

- Command Line Tool (CLI)
- ***Firewalk*** is a software tool that performs ***Firewalking***.
- Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass.
- Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway.
- If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message.
- If the gateway hostdoes not allow the traffic, it will likely drop the packets on the floor and we will see no response.

***Examples:***

```
root@kali:~# firewalk -h
root@kali:~# firewalk -S8079-8081  -i eth0 -n -pTCP 192.168.1.1 192.168.0.1
```

## *Firewall Analyzer*

- See: **Forensics Network**
- Source: https://www.manageengine.com
- ManageEngine Firewall Analyzer is a log analytics and configuration management software that helps network administrators to collect, archive, analyze their security device logs and subsequently generate forensic reports.

## *Flash Retriever Forensic Edition*

- See: **Forensics**
- Source:http://www.infinadyne.com
- Data acquisition

## *Flawfinder*

- See: **Vulnerability Scanner Code**
- Link: https://dwheeler.com/flawfinder/
- A simple program that examines ***C/C++*** source code and reports possible security weaknesses (“flaws”) sorted by risk level.

## *Forensic Email Recovery Tools Kit*

- See: **E-Mail Forensics**
- Source: http://www.forensicsoftware.org
- This kit looks into suspect's mailbox even if he/she played the trick to corrupt/delete the relevant emails from his/her email database of Outlook application, Exchange email system or from Mac Outlook email program.

## *Forensic Falcon*

- See: **Forensics**
- Source:http://www.logicube.com
- Data acquisition

## *Forensic Replicator*

- See: **Forensics**
- Source:https://www.paraben.com
- Data acquisition

## *Forensic Toolkit (FTK)*

- See: **E-Mail Forensics**
- Source: http://accessdata.com
- FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
- It provides comprehensive processing and indexing up front, so that filtering and searching is fast.
- This means we can “zero-in” on the relevant evidence quickly, increasing the analysis speed.

### *Forensic Tower IV Dual Xeon*

- See: **Forensics**
- Source: http://www.forensiccomputers.com
- Data acquisition

### *Forensic UltraDock*

- See: **Forensics**
- Source: https://www.cru-inc.com
- Data acquisition

### *Fort Knox*

- See: **Firewall**
- Supplier: Fortknox
- Link: fortknox-firewall.com

### *FortKnox 3.55*

- See: **Steganography**
- Supplier: Guillermito
- Link: http://www.guillermito2.net/stegano/fortknox/

### *Fpipe v2.1*

- See: ***TCP source port forwarder/redirector***
- Supplier: McAfee
- It can create a TCP stream with a source port of your choice.
- This is useful for getting past firewalls that allow traffic with source ports of say 23, to connect with internal servers.

### *FPort v2.0*

- See: **Scanner**
- Supplier: McAfee
- Identify unknown open ports and their associated applications
- Fport supports Windows NT4, Windows 2000 and Windows XP
- fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the '***netstat -an***' command, but it also maps those ports to running processes with the ***PID***, process name and path.
- Fport can be used to quickly identify unknown open ports and their associated applications.

### *Fragroute*

- See: **Penetration testing tool / Packet Crafting**
- See: Kali Linux
- Command line tool
- Fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection” paper of January 1998.
- It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour.
- This tool was written in good faith to aid in the testing of network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour.
- Please do not abuse this software.

### *FRED - Digital Intelligence Forensic Hardware*

- See: **Forensics**
- https://www.digitalintelligence.com
- FRED systems are optimized for stationary laboratory acquisition and analysis.

- Simply remove the hard drive(s) from the suspect system, plug them into FRED, and acquire the digital evidence.
- FRED will acquire data directly from IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/USB hard drives and storage devices and save forensic images to Blu-Ray, DVD, CD, or hard drives.

## *FREDDIE*

- See: **Forensics**
- Source:http://www.digitalintelligence.com
- Data acquisition

## *Free Windows Service Monitor Tool*

- See: **Windows Services Monitoring Tool**
- Source: http://www.manageengine.com
- Free Windows Service Monitor helps to monitor Exchange Server, SharePoint services, MySQL services, MSSQL services, DHCP services, etc.
- It allows users to monitor up to five custom services simultaneously.

***Features:***

- Monitors the Windows services for up to three devices simultaneously
- Allows to know the status and startup type of the Windows services
- Configures the startup type and updates the status of Windows services
- Allows to fetch the status of Windows services by refreshing

## *FSUM Frontend*

- See: **File and Folder Integrity Checkers**
- Source: http://fsumfe.sourceforge.net
- Source: http://www.slavasoft.com
- Fsum Frontend is a free and easy-to-use tool that allows computing message digests checksums and HMACs for files and text strings.
- It supports drag-and-drop, and you can handle multiple files at once.
- The checksum generated can be used to verify the integrity of the files It is a command line utility for file integrity verification.
- It offers a choice of 13 hash and checksum functions for file message digest and checksum calculation.

***Few of features enlisted below:***

- Calculate the checksums, message digest and HMAC of files and text strings.
- Verify files using a SFV/MD5/SHA1/SHA2 file and notify you if a file is corrupted or missing.

## *Ftk Imager*

- See: **Forensics**
- Dieser ist einerseits Teil der kompletten FTK (Forensics Toolkit) von AccessData, andererseits kann das Werkzeug als Stand-alone gratis heruntergeladen werden.
- Es dient der Erstellung von Images und sollte in keiner gepflegten Tool-Sammlung fehlen.
- Infos: accessdata.com

## *FTPExplorer*

- See: **FTP Client**
- Source: http://www.ftpx.com

## *G-Lock Software Email Verifier*

- See: **E-Mail Forensics**
- Source: http://www.glocksoft.com
- G-Lock SoftwareE-mail Verifier will check every email address from a database or a mailing list and determine if the e-mails are still valid.

### *GamaSec*

- See: **Vulnerability Scanner Code**
- Source: http://www.gamasec.com
- Is a remote online web vulnerability-assessment service delivered via ***SaaS*** (software-as-a-service) and is designed to identify security weaknesses in web applications.
- The scanner identifies application vulnerabilities e.g. ***Cross Site Scripting (XSS)***, ***SQL injection***, ***Code Inclusion*** etc.. as well as site exposure risks.
- It also ranks threat priority, produces highly graphical, intuitive HTML reports, and indicates site security posture by vulnerabilities and threat exposure.

### *Gargoyle Investigator Forensic Pro*

- See: **Steganography Detection Tool**
- Is a tool that conducts quick searches on a given computer or machine for known contraband and malicious programs.
- This tool finds remnants in a removed program as it conducts the search for the individual files associated with a particular program.
- Its signature contains botnets, Trojans, steganography, encryption, and keyloggers.
- It helps in detecting stego files created by using BlindSide, WeavWav, and S-Tools.
- It has the ability to perform a scan on a stand-alone computer or network resources for known malicious programs and the ability to scan within archived files.

### *GeekSn0w*

- See: **iOS Jailbreaking Tools**
- Source: http://geeksn0w.it
- GeekSn0w is a free tool developed by Andrea Bentivegna for jailbreaking iPhones running on iOS 7.1.
- It is available only for Windows OS as of now.

### *GetDataBack*

- See: **File Recovery**
- http://www.runtime.org

### *GFI EventsManager*

- See: **Forensics Network**
- Analysis of log data, including SNMP traps, Windows® event logs, W3C logs, text-based logs, Syslog, SQL Server®, and Oracle® audit logs
- Provides specific reports for some of the major compliance acts as well as other standard reports
- Filter-enabled charts provide access to the important data you need  GFI EventsManager offers deep granular control of log data to easily classify the information from the system.
- GFI EventsManager offers safe storage of log data according to industry standards and security best practices.

### *GiliSoft File Lock Pro*

- See: **Anti Forensics Tool**
- http://gilisoft.com

### *Glary Undelete*

- See: **File Recovery**
- http://www.glarysoft.com

### *Global Network Inventory*

- Is one of the de facto tools for security auditing and testing of firewalls and networks.
- It is also used for ***Idle Scanning***.

## *Gnu WGET*

- See: **Website Mirroring**
- Price: Freeware
- For retrieving files using HTTP, HTTPS, FTP and FTPS the most widely-used Internet protocols.
- It is a non-interactive ***commandline tool***, so it may easily be called from scripts, cron jobs, terminals without X-Windows support, etc.

## *GoAccess*

- See: **Web Attack Investigation**
- Source: https://goaccess.io
- GoAccess is an open source real-time web log analyzer and interactive viewer that runs in a terminal in *nix systems or through your browser.
- It provides HTTP statistics for system administrators that require a visual server report.

## *Golismero*

- See: **Vulnerability scanner**
- Link: http://www.golismero.com
- ***Free*** software framework for security testing.
- It's currently geared towards web security, but it can easily be expanded to other kinds of scans.
- It can run their own security tests and manage a lot of well-known security tools (OpenVas, Wfuzz, SQLMap, DNS recon, robot analyzer...) take their results, feedback to the rest of tools and merge all of results.
- And all of this automatically

***EXAMPLES***

```
golismero <IP>
golismero scan <IP>
golismero -p quick <www.xxx.com>
```

## *Gopher*

- Hgopher
- ws_gopher
- ***Informationsdienst***, der über das Internet mit Hilfe eines Gopherclients abgerufen werden kann.
- Arbeitet auf ***Port 70***.

## *Guaranteed PDF Decrypter*

- See: **Password Cracker**
- http://www.guapdf.com

## *Graylog*

- See: **Forensics Network**
- Source: https://www.graylog.org
- It is an open-source log management tool used to search, analyze, and generate alerts across all log files.

## *Griffeye CS Operations*

- See: **Forensics**
- Supplier: Griffeye
- Link: https://www.griffeye.com
- For group efforts on individual cases, gives you and your colleagues a digital base of operations for reviewing and analyzing materials.

### *GSView*

- See: **Tool**
- Utility zum lesen von PostScript Dateien.
- Source: http://www.cs.wisc.edu/~ghost/gsview/index.html

### *Hackbot*

- See: **Vulnerability Scanner**
- Link: scuriteam.com
- Hackbot is a vulnerability and banner grabber meant as auditory tool for remote and local hosts.
- Requires PERL (http://www.perl.org), IO::Socket, Net::hostent and Getopt::Std that should come with your default PERL installation.
- Scans over 300 CGI's, scans for banners of several services, does Unicode checks, checks for open relays, outsmarts Cisco PIX MailGuard, can do ripe checkup, SpamCOP DB checkup, X connect test and lots more.

### *Handy Recovery*

- See: **File Recovery**
- Source: http://www.handyrecovery.com

### *HardCopy 3P*

- See: **Forensics**
- Source: http://www.digitalintelligence.com
- Data acquisition

### *Hash Buster*

- See: **Penetration Testing**
- Link: github.com
- A hash buster is a program which randomly adds characters to data in order to change the data's hash sum.
- This is typically used to add words to spam e-mails, to bypass hash filters. As the e-mail's hash sum is different from the sum of e-mails previously defined as spam, the e-mail is not considered spam and therefore delivered as if it were a normal message.
- Hash busters can also be used to randomly add content to any kind of file until the hash sum becomes a certain sum. In e-mail context, this could be used to bypass a filter which only accepts e-mails with a certain sum.
- Initially spams containing "white noise" from hash busters tended to simply exhibit 'paragraphs' of literally random words, but increasingly these are now appearing somewhat grammatical.

### *HashCalc*

- See: **Forensics**
- Calculating One-Way Hashes
- HashCalc is a fast and easy-to-use calculator that allows computing message digests, checksums, and HMACs for files, as well as for text and hex strings.
- It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

**Video:** https://www.youtube.com/watch?v=qDxGoRuVQwk

### *HashMyFiles*

- See: **Forensics**
- Source: https://www.nirsoft.net/utils/hash_my_files.html
- HashMyFiles is small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system.
- You can easily copy the MD5/SHA1 hashes list into the clipboard or save them into text/html/xml file.

- HashMyFiles can also be launched from the ***context menu of Windows Explorer*** and display the MD5/SHA1 hashes of the selected file or folder.

### *Hash Suite*

- See: **Password Crack**
- http://hashsuite.openwall.net

### *Helix Live for Windows / Helix3 Pro*

- See: **Forensics**
- Supplier: E-Fense
- Source: e-fense.com
- **Helix3** is a Live CD built on top of Ubuntu.
- It focuses on **incident response** and ***computer forensics***.
- Reveals passwords of ***MDB files***.
- MessenPass → To recover messenger passwords

### *Hetman Partition Recovery*

- See: **Partition Recovery**
- https://hetmanrecovery.com

### *Hex Editor Neo*

- See: **Forensics**
- Source: http://www.hhdsoftware.com
- Freeware Hex Editor Neo allows viewing, modifying, analyzing hexadecimal data and binary
- files, editing, exchanging data with other applications through the clipboard, inserting new data and deleting existing data, as well as performing other editing actions.

### *Hiren's Boot CD*

- See: **Troubleshooting**
- Source: https://www.hirensbootcd.org/download/
- A whole bunch of tools.

### *HijackThis*

- See: **Monitoring**
- Source: http://sourceforge.net
- HijackThis is a utility that generates an in depth report of registry and file settings from the computer.
- It makes no separation between safe and unsafe settings in its scan results giving the ability to selectively remove items from the machine.
- In addition, HijackThis comes with several tools useful in manually removing malware from a computer.

### *HOIC*

- See: **DDoS**
- "High Orbit Ion Cannon" or HOIC for short is a network stress testing tool for launching DDoS attacks.
- HOIC causes DoS through the use of HTTP floods.
- HOIC has a built-in scripting system that accepts.hoic files called "boosters," allowing a user to implement some anti-DDoS randomization countermeasures, as well as increase the magnitude of the attack.

### *HotWhois*

- See: **WHOIS Desktop Tool**
- Source: http://www.tialsoft.com
- HotWhois allows you to get all IP Whois and Domain whois information about IP addresses and domain names.

- This IP tracking tool can reveal valuable information, such as country, state, city, address, contact phone numbers and e-mail addresses of an IP provider.

## *Hping*

- See: **Packet Crafting**
- Source: hping.org
- Source: Kali Linux
- Hping is no longer actively developed!
- To get a response from a host if ***ICMP*** isn't working.
- Needs ***libcap*** (Packet Capture Library)
- ***hping*** command is a -line oriented TCP/IP packet assembler/analyzer.
- The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests.
- It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.
- While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts.
- A subset of the stuff you can do using hping:

**Features:**

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- hping can also be useful to students that are learning TCP/IP.

Countermeasure:

- Block ICMP type 13 messages

### *hping2*

```
hping2 -1 host.domain.com            → ICMP Scan
```

### *hping3*

```
hping3 10.10.10.10 --udp --rand-source --data 500
hping3 10.10.10.10 --flood
hping3 -A 192.168.2.x -p 80
hping3 -c 3 10.10.10.10
hping3 -S 10.10.10.10 -p 80 -c 5
hping3 --scan 1-3000 -S 10.10.10.10
hping3 -V -c 1000 -d 100 -S -p 21 --flood <DST_IP>   → SYN Flood
hping3 -V -c 1000 -d 100 -S -p 21 -s 80 -k -a <SRC_IP> <DST_IP> → Land Attack
```

## *HSM - Hardware Security Module*

- FIPS 140-2 Level 4
- Many certificate authority systems (CAs) use HSMs ***to store certificates***.
- A hardware security module (HSM) is a dedicated crypto processor that is specifically designed for the protection of the ***crypto key lifecycle***.
- Specialized HSMs are used in the ***payment card industry***.
- HSMs support both general-purpose functions and specialized functions required to process transactions and comply with industry standards.

## *HSM - Hierarchical Storage Management*

- Provides a continuous ***on-line backup*** by using optical or tape "***jukeboxes***", similar to ***WORMs***.

- It appears as an ***infinite disk*** to the system and can be configured to provide the closest version of an available real-time backup.
- This is commonly employed in ***very large data retrieval systems***.

### *HstEx*

- See: **Forensics**
- http://www.digital-detective.net

### *HTTP-ANALYZE*

- See: **Web Attack Investigation**
- Source: http://http-analyze.org
- The http-analyze is a logfile analyzer for web servers.
- It runs on any platform conforming to the ANSI C and POSIX standards ranging from personal computers to high-performance systems.

### *HTTPWatch*

- See: **HTTP Monitoring**
- Source: https://www.httpwatch.com

### *HTTP RAT*

- See: **Penetration Testing**
- A kind of ***Remote Access Trojan*** which utilizes web interfaces and port 80 to gain access.
- It can be understood simply as an HTTP Tunnel, except it works in the reverse direction.
- These Trojans are comparatively more dangerous as these work on the web and thus work almost everywhere where you can find internet.

### *HTTrack Web Site Copier*

- See: **Reconnaissance / Web Site Mirroring**
- Price: Freeware
- Web site mirroring creates a replica of an existing site.
- It allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos and other files from the server on your computer.

### *HXD*

- See: **Hex Editor**
- Source: https://mh-nexus.de
- HXD is a ***hex editor*** allowing users to edit, modify the raw binary content of a file or a disk of any size.
- The tool features; operations such as searching, replacing, exporting, checksums/ digests, insertion of byte patterns, a file shredder, concatenation or splitting of files, statistics, analyze malware, patch programmers, repair hard drive tables, perform file comparisons, create cheats, etc.
- The tool assists investigators in finding out information of evidentiary value such as email ID, display name, filecache.dbx path, Server_time, file list, and updated/deleted files. Investigators can track the logged in credentials of the required Dropbox account by searching the RAM dump using the string AUTHENTICATE and the logged in user's name can be obtained using the string DisplayName.

### *Hybrid Analysis*

- See: **Online Malware Analysis**
- Source: https://www.hybrid-analysis.com
- Supplier: CrowdStrike
- This is an online malware analysis service powered by Payload Security that detects and analyzes unknown threats.

- The service is running VxStream Sandbox v5.50 in the backend that supports PE, Office, PDF, APK and more such files.

### *Hyena*

- See: **Penetration testing tool**
- Enumerating Resources
- Hackers enumerate applications and banners in addition to identifying user accounts and shared resources.
- Hyena uses an Explorer-style interface for all operations. Management of users, groups (local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported.
- To be an Expert Ethical Hacker and Penetration Tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked.

### *IBM Security MaaS360® with Watson™*

- See: **MDM**
- Vereinfacht und beschleunigt die Unterstützung einer vielschichtigen, komplexen Endpunkt- und mobilen Umgebung, die auf KI und Analyse basiert und in Ihre bestehende IT-Infrastruktur integriert ist.

### *ICMP Shell*

- See: **Penetration Testing**
- ICMP Shell (ISH) is a telnet-like protocol.
- It allows users to connect to a remote host and to open a shell using only ICMP to send and receive data.
- ICMP Shell was written in C for the UNIX environment.

### *ICQ Sniffer*

- See: **Forensics Network**
- Source: http://www.etherboss.com
- ICQ Sniffer is a network utility that can capture and log ICQ chat from computers within the same LAN.
- It supports messaging through ICQ server with format of plain text, RTF, or HTML. It provides a report system to export captured ICQ conversations as HTML files for later analysis and reference.

### *IDA - VirusAnalysis*

- See: **Malware Analysis**
- Virus Aktivitäten analysieren

### *IDS - Intrusion Detection Systems*

***HIDS***
***NIDS***
***Hybrid***
***WIPS***

- Locating rogue access points (APs)

***Types:***

- Anomaly-based detection
  Behavioral-based systems / Profile-based systems
- Signature-based detection

### *IM Solo-4 G3 Forensic*

- See: **Forensics**
- Enterprise Super Kit http://ics-iq.com
- Data acquisition

### *IMAGE MASSTER WIPEPRO*

- See: **Forensics**
- Supplier: ICS
- Link: ics-iq.com
- The Image MASSterTM Wipe PRO is a ***hard Drive Sanitization Station***.
- It can erase up to 8 Hard Drives simultaneously at speeds exceeding 7 GB/min.

### *ImageMASSter Solo-3*

- See: **Forensics**
- Supplier: ICS
- Link: ics-iq.com
- Capturing data from IDE, SATA, SCSI and flash card.
- Produces ***MD5*** and CRC32 hashes.
- Professional disk eraser

### *ImgStegano*

- See: **Steganography Detection Tool**
- http://www1.chapman.edu

### *InstalledDriversList*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.nirsoft.net
- InstalledDriversList is a tool for Windows that lists all device drivers that exists on the system.
- For every device driver, it displays the following information: Driver Name, Display Name, Description, Startup Type, Driver type, Driver Group, Filename, File Size, Modified/Created Time of the driver file, and version information of the driver file.
- If the driver is currently running on Windows kernel, it also displays the following information: Base Memory Address, End Address, Memory Size, and Load Count.

### *Intella TEAM*

- See: **E-Mail Forensics**
- Source: https://www.vound-software.com
- Intella TEAM enables multiple individuals to review evidence independently.
- It is an email investigation and eDiscovery software tool for an agency, law firm or investigative team that needs to coordinate the search and analysis of ESI and files that exceed 250 gigabytes.
- Investigators can quickly and easily process, search, review and analyze email and ESI as well as process and search multiple email sources, file types and metadata.
- It allows viewing results in a visual layout of choice and exporting the documents of interest in a wide variety of file formats.

### *Internet Worm Maker*

- See: **WORM Tool**
- Internet Worm Maker Thing is a tool to ***create worms***.
- It can also convert a virus into a worm.
- Internet Worm Maker Thing is an automated scripting tool used to generate malicious code.
- It enables you to specify criteria down to the most basic element, including the actions you want it to perform, its display language, and its launch date.
- As an ethical hacker and pen-tester, you can use Internet Worm Maker Thing as a proof of concept to audit perimeter security controls in your organization.

### *Invisible Secrets 4*

- See: **Anti Forensics Tool**
- http://www.invisiblesecrets.com

### *IGHASHGPU*

- See: **Password Cracker**
- Source: darknet.org.uk
- GPU based hash cracking - ***SHA-1***, MD4, ***MD5***

### *Ike-Scan*

- See: **Reconnaissance**
- Source: Kali Linux
- ***Fingerprinting*** VPN Firewalls.
- Portscanner

### *ILook Investigator*

- See: **Forensics**
- Data acquisition

### *inetmgr*

- See: **IIS Tool**
- CLI
- inetmgr is a command that can be used to open the ***IIS Manager***, it is actually a shortcut to open the IIS Manager.

### *InFixi® Email Recovery Tools*

- See: **E-Mail Forensics**
- Source: http://www.infixi.com
- InFixi Software group offers a great range of software product for "Email Recovery", "Email Conversion", "File Repair", "File Recovery" and "Password Recovery".

### *InsidePro*

- See: **Password Cracker**
- http://www.insidepro.com

### *InSSIDer*

- See: **WLAN Tool**
- Supplier: MetaGeek
- See: https://www.metageek.com/products/inssider/
- WiFi Troubleshooting and Optimization.

### *InTrust*

- See: **Forensics Network**
- Source: http://software.dell.com
- InTrust enables the secure collection, storage, search, and analysis of massive amounts of IT data from numerous data sources, systems, and devices in one place.

### *Inundator*

- IDS Evasion

### *IObit Cloud*

- See: **Online Malware Analysis**
- Source: http://cloud.iobit.com
- IObit Cloud is an automated threat analysis system that uses Cloud Computing technology and Heuristic Analyzing mechanic to analyze the behavior of spyware, adware, trojans, keyloggers, bots, worms, hijackers and other security-related risks.

### *Iodine*

- See: **DNS-Tool**
- TCP over DNS

### *ioos*

- See: **Compliancy Checker**
- Python tool to check your ***datasets*** vs compliance standards.
- The IOOS Compliance Checker is a python based tool for data providers to check for completeness and community standard compliance of local or remote ***netCDF*** files against ***CF*** and ***ACDD*** file standards.
- The python module can be used as a command-line tool or as a library that can be integrated into other software.

### *IP-Tools*

- IP-Tools offers many TCP/IP utilities in one program and is indispensable for anyone who uses the Internet or Intranet.
- It can perform activities such as network monitoring, spoofing, filtering, decoding and parsing from a single place.
- The Adapter Statistics program can provide not only textual but graphical data with support of the most network protocols.

### *IPgrab*

- See: **Forensics Network**
- Source: http://ipgrab.sourceforge.net
- IPgrab is a verbose packet sniffer for UNIX hosts.

### *Ipswitch Log Management*

- See: **Forensics Network**
- Source: https://www.ipswitch.com
- The Ipswitch Log Management Suite is an automated tool that collects, stores, archives, and backs-up ***Syslog***, ***Windows events***, or ***W3C*** / ***IIS logs***.
- It analyzes for suspicious activities and automatically generates compliance reports.

### *IPTables*

- Source:debian.org

- FW for Linux

### *IPTraf*

- See: **Traffic monitoring tool (Linux)**
- Source:optraf.seul.org

### *IQCOPY FOR FORENSIC*

- See: **Forensics**
- Source:http://ics-iq.com
- Data acquisition

### *iRecovery Stick*

- See: **Forensics**
- Source:https://www.paraben.com
- Data acquisition

### *IrfanView*

- See: **Forensics**

- Source: http://www.irfanview.com
- IrfanView is a small FREEWARE (for non-commercial use) ***graphic viewer*** for Windows 9x, ME, NT, 2000, XP, 2003 , 2008, Vista, Windows 7, Windows 8, Windows 10.

### *iSunshare Windows Password Genius*

- See: **Password Cracker**
- http://www.isunshare.com

### *iSteg*

- See: **Steganography tool**
- Supplier: hanynet.com

### *iXAM*

- See: **iPhone Data Acquisition Tools**
- Source: http://www.ixam-forensics.com
- iXAM is used for mobile forensics investigation to provide any information from a stored contact or text message to an email, photograph, or specific map location.

### *IXimager*

- See: **Forensics**
- Data acquisition

### *John the Ripper*

- See: **Password Cracker**
- Source: http://tms.netrom.com/~cassidy/utils/john-15w.zip
  www.openwall.com/john
- Works on Unix and Linux.
- Runs ***dictionary attack***.

***Example:***

```
john <file.txt>
```

### *Jotti's Malware Scan*

- See: **Online Malware Analysis**
- Source: https://virusscan.jotti.org/de
- Investigators can scan malware using online tools like Jotti for well-known malwares.
- Numerable anti-virus vendors would have analyzed and sorted the malware files.

### *JPlag*

- See: ***software plagiarism***
- Source:http://jplag.ipd.kit.edu/
- JPlag is a system that finds similarities among multiple sets of source code files.
- This way it can detect ***software plagiarism***.
- JPlag does not merely compare bytes of text, but is aware of programming language syntax and program structure and hence is robust against many kinds of attempts to disguise similarities between plagiarized files.
- JPlag currently supports Java, C#, C, C++, Scheme and natural language text.
- JPlag is typically used to detect and thus discourage the unallowed copying of student exercise programs in programming education. But in principle it can also be used ***to detect stolen software parts*** among large amounts of source text or modules that have been duplicated (and only slightly modified). JPlag has already played a part in several intellectual property cases where it has been successfully used by expert witnesses.
- JPlag has a powerful graphical interface for presenting its results. See our example.
- Just to make it clear: JPlag does not compare to the internet! It is designed to find similarities among the student solutions, which is usually sufficient for computer programs.

### *JPS Virus Maker*

- JPS Virus Maker is a tool to create viruses.
- It also has a feature for converting a virus into a worm.

### *Juggernaut*

- See: **Network Sniffer**
- Source: infonexus.com
- View active telnet sessions
- Hijacking of TCP sessions

### *jv16 PowerTools*

- PC System Utilities Software designed to make your computer work fast and smoothly.

### *Kali Linux*

- See: **Tools**
- Source: www.kali.org
- Must have for security professionals.

***Built-In password list:*** ***rockyou.txt***

```
/usr/share/wordlist/rockyou.txt.gz
```

### *Kernel Email Recovery Software*

- See: **E-Mail Forensics**
- Source: http://www.nucleustechnologies.com
- Kernel data recovery group presents an wide range of email recovery products, which recover the lost and deleted emails, email attachments, images, files and email properties.
- This recovery software is developed to restore and repair files of MS Outlook (OST and PST), Outlook Express (DBX), IncrediMail (.IMM, .IMH, .IMB) which might get corrupt due to accidental deletion of emails, virus attacks, emails corrupted in the transit and even when the emails are emptied from the 'Deleted Items' folder of the email clients.

### *Kernel for PST Recovery*

- See: **E-Mail Forensics**
- Source: http://www.pstrecoverytools.com
- Kernel for PST Recovery is a enables to repair corrupted PST file and recover all email items from them.
- It successfully fixes errors resulted due to damaged or corrupted PST file, virus attacks, deleted emails, broken PST files, header corruption, disk corruption, errors due to large PST file size and others.

### *KFSensor*

- See: **Honeypot / IDS**
- KFSensor is a commercial host based Intrusion Detection System (IDS), it acts as a honeypot to attract and detect hackers by simulating vulnerable systems.

### *Kibana*

- See: **Forensics Network**
- Source: https://www.elastic.com
- Kibana is an open-source data visualization platform that allows interaction with the data through a graphical user interface.

### *KillProcess*

- See: **Monitoring**
- Source: http://orangelampsoftware.com

- KillProcess can terminate almost any process on a Windows machine, including any service and process running in the system.
- It can even terminate the protected Microsoft system processes.
- It can kill multiple processes, either by multi-select or by use of “kill lists.”
- Using these techniques it is possible to batch-terminate processes.
- It can also scan the running processes on the computer, and kill them on sight, much like an anti-spyware application would.

### *Kingo Android ROOT*

- See: **Android Rooting Tools**
- Source: https://www.kingoapp.com
- This is a simple and direct utility to root android devices and suitable for novice users.

***Features are as follows:***

- Enhanced performance
- Saves battery life
- Provides access to root apps and can uninstall them
- Customized appearance
- Gain administration of the device

### *Kippo*

- See: **Forensics Network**
- Is one of the commonly used Honeypots to fool the attackers and understand their methodology thereby minimizing the risk of attack.

### *KisMet*

- See: **Forensics Network**
- Source: https://www.kismetwireless.net/
- Passive discovery tool
- Kismet ist ein freier passiver WLAN-Sniffer zum Aufspüren von Funknetzwerken.

### *Kiwi Log Viewer*

- See: **Forensics Network**
- Source: http://www.kiwisyslog.com
- Kiwi Log Viewer enables the monitoring of a log file for changes.
- It can display changes in real-time and allows automatic monitoring of log file entries for specific keywords, phrases, or patterns.

### *Kiuwan*

- See: **Vulnerability Scanner Code**
- Source: https://www.kiuwan.com/
- Find and fix security vulnerabilities in your code at every stage of the SDLC.

### *Kon-Boot*

- See: **Password Cracker**
- Source: http://www.thelead82.com

### *Kroll Ontrack Email Recovery*

- See: **E-Mail Forensics**
- Source: http://www.krollontrack.com
- It is an email management tool that helps IT administrators granularly search and restore mailboxes, messages, attachments and other Microsoft® Office Outlook items without restoring the entire database.

### *KRyLack ZIP Password*

- See: **Password Cracker**

- Recovery http://www.krylack.com

### *KRyLack RAR Password*

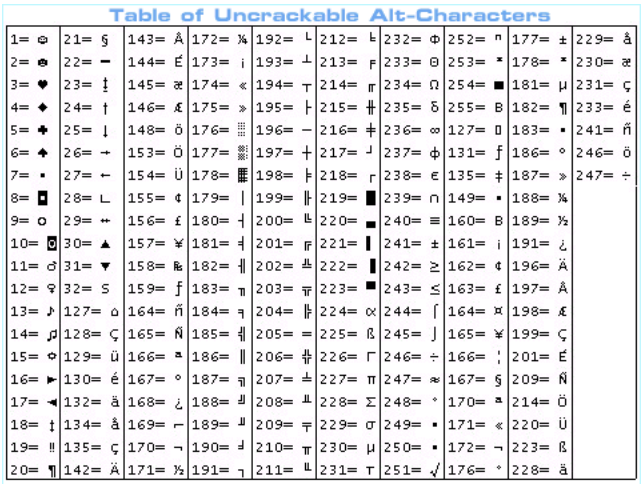
- See: **Password Cracker**
- Recovery http://www.krylack.com

### *KSE - Kane Security Analyst for WNT*

- Source: http://www.intrusion.com/
- Supplier: Security Dynamics
- KSA uses built-in security intelligence to examine system configurations and find areas that pose risks or need adjustment.
- The tool is well suited for small shops and large enterprise networks.

### *L0phtCrack*

- See: **Forensics / Password cracker**
- Source: Kali Linux
- http://www.l0phtcrack.com
- Can crack ***Windows SMB passwords*** simply by listening to network traffic.




| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1= ☺ | 21= § | 143= Å | 172= ¼ | 192= └ | 212= ╘ | 232= Φ | 252= ⁿ | 177= ± | 229= å | | |
| 2= ☻ | 22= ▬ | 144= É | 173= ¡ | 193= ┴ | 213= ╒ | 233= Θ | 253= ² | 178= ² | 230= æ | | |
| 3= ♥ | 23= ↨ | 145= æ | 174= « | 194= ┬ | 214= ╓ | 234= Ω | 254= ■ | 181= µ | 231= ç | | |
| 4= ♦ | 24= ↑ | 146= Æ | 175= » | 195= ├ | 215= ╫ | 235= δ | 255= B | 182= ¶ | 233= é | | |
| 5= ♣ | 25= ↓ | 148= ö | 176= ▒ | 196= ─ | 216= ╪ | 236= ∞ | 127= ⌂ | 183= · | 241= ñ | | |
| 6= ♠ | 26= → | 153= Ö | 177= ▓ | 197= ┼ | 217= ┘ | 237= ϕ | 131= ƒ | 186= ° | 246= ö | | |
| 7= • | 27= ← | 154= Ü | 178= ▓ | 198= ╞ | 218= ┌ | 238= ∈ | 135= ‡ | 187= » | 247= ÷ | | |
| 8= ◘ | 28= ∟ | 155= ¢ | 179= │ | 199= ╟ | 219= ▉ | 239= ∩ | 149= • | 188= ¼ | | | |
| 9= ○ | 29= ↔ | 156= £ | 180= ┤ | 200= ╚ | 220= ▄ | 240= ≡ | 160= B | 189= ½ | | | |
| 10= ◙ | 30= ▲ | 157= ¥ | 181= ╡ | 201= ╔ | 221= ▌ | 241= ± | 161= ¡ | 191= ¿ | | | |
| 11= ♂ | 31= ▼ | 158= ₧ | 182= ╢ | 202= ╩ | 222= ▐ | 242= ≥ | 162= ¢ | 196= Ä | | | |
| 12= ♀ | 32= S | 159= ƒ | 183= ╖ | 203= ╦ | 223= ▀ | 243= ≤ | 163= £ | 197= Å | | | |
| 13= ♪ | 127= ⌂ | 164= ñ | 184= ╕ | 204= ╠ | 224= ∝ | 244= ⌠ | 164= ¤ | 198= Æ | | | |
| 14= ♫ | 128= Ç | 165= Ñ | 185= ╣ | 205= ═ | 225= ß | 245= ⌡ | 165= ¥ | 199= Ç | | | |
| 15= ☼ | 129= ü | 166= ª | 186= ║ | 206= ╬ | 226= Γ | 246= ÷ | 166= ¦ | 201= É | | | |
| 16= ► | 130= é | 167= º | 187= ╗ | 207= ╧ | 227= π | 247= ≈ | 167= § | 209= Ñ | | | |
| 17= ◄ | 132= ä | 168= ¿ | 188= ╝ | 208= ╨ | 228= Σ | 248= ° | 170= ª | 214= Ö | | | |
| 18= ↕ | 134= å | 169= ⌐ | 189= ╜ | 209= ╤ | 229= σ | 249= • | 171= « | 220= Ü | | | |
| 19= ‼ | 135= ç | 170= ¬ | 190= ╛ | 210= ╥ | 230= µ | 250= · | 172= ¬ | 223= ß | | | |
| 20= ¶ | 142= Ä | 171= ½ | 191= ┐ | 211= ╙ | 231= τ | 251= √ | 176= ° | 228= ä | | | |

### *LADS*

- Searching for ADS

### *LAN Turtle*

- See: Penetration testing tool
- Source: https://www.hak5.org/gear/lan-turtle
- The LAN Turtle is a covert Systems Administration and Penetration Testing tool providing stealth remote access, network intelligence gathering.

### *Lantern*

- See: **iPhone Data Acquisition Tools**
- Source: http://katanaforensics.com
- The Lantern allows the user to parse and triage a Mac running OSX or a Mac OSX image and allows for data extraction, analysis, and auditing.

### *LanWhoIs*

- See: **WHOIS Desktop Tool**
- Source: http://lantricks.com

- The LanWhoIs program helps you find out who, where, and when registered the domain or site you are interested in, and the information about those who supports it currently.

## *Last SIM Details*

- See: **Forensics Mobile**
- Source: http://lastsimdetails.blogspot.co.uk
- Last SIM Details offers the following

***Features:***

- LSD parses physical flash dumps and Nokia PM records to find details of previously inserted SIM cards.
- Able to parse both .bin and .pm file types.
- The Regex customiser allows investigators to define the country and network parameters to eliminate false positives.

## *LCP*

- See: **Password Cracker**
- http://www.lcpsoft.com

## *Leafpad*

## *LIBNIDS*

- See: **NIDS**
- Libnids is an implementation of an E-component of Network Intrusion Detection System.
- It emulates the IP stack of Linux 2.0.x. Libnids offers ***IP defragmentation***, ***TCP stream assembly*** and ***TCP port scan detection***.
- The most valuable feature of libnids is reliability. A number of tests were conducted, which proved that libnids predicts behaviour of protected Linux hosts as closely as possible.
- Libnids is highly configurable in run-time and offers a convenient interface.
- Currently it compiles on Linux, *BSD and Solaris. WIN32 port is maintained separately here.
- Using libnids, one has got a convinient access to data carried by a TCP stream, no matter how artfully obscured by an attacker.
- You may have a look at a sample application.
- Libnids is designed by Rafal Wojtczuk.

## *Libwhisker*

- See: **Vulnerability scanning**
- exploitation
- IDS evasion

## *Log and Event Manager*

- See: **Forensics Network**
- Source: http://www.solarwinds.com
- Log & Event Manager is an SIEM that makes it easy to use logs for security, compliance, and troubleshooting.

## *Log Management Utility*

- See: **Forensics Network**
- Source: http://www.biz.konicaminolta.com
- Log Management Utility enables one to collect, save, browse, and search MFP Audit Logs smoothly and for a longer period of time from a PC, giving more time to manage and analyze the conditions of each MFP.

## *Logcheck*

- See: **Forensics Network**

- Source: http://logcheck.org
- Logcheck is a utility that allows system administrators to view the log files, which are produced by hosts under their control.
- This is done by mailing summaries of the log files to the hosts, after first filtering out “normal” entries.
- Normal entries are entries that match one of the many regular expression files contained in the database.

### *LogCruncher*

- See: **Web Attack Investigation**
- Source: https://logentries.com
- LogCruncher is a tool for analysis and data visualization of web server log files.
- It allows the user to see and understand the website analytics based on key metrics.

### *Loggly*

- See: **Forensics Network**
- Source: https://www.loggly.com
- Loggly offers a cloud-based service that mines log data in real time and reveals what is required, so that you have the insights you need to produce.

### *LogMeister*

- See: **Forensics Network**
- http://www.logmeister.com
- This tool monitors Windows event logs, syslog, and text logs on servers throughout a network, providing notifications of key events and allowing for appropriate and timely action.
- It consolidates, archives, transforms, and exports the log data to meet the required compliance needs.

### *LogRhythm*

- See: **Forensics Network**
- Source: https://www.logrhythm.com
- The LogRhythm security intelligence and analytics platform enables organizations to detect, prioritize, and neutralize cyber threats that penetrate the perimeter or originate from within.

### *Logscape*

- See: **Forensics Network**
- Source: http://logscape.com
- This tool allows searching, visualizing, and analyzing log files and operational data.

### *Logsene*

- See: **Forensics Network**
- Source: https://www.sematext.com
- Using Logsene, all logs are accessible in one place.
- It allows to inspect logs via UI or Elasticsearch API and correlate logs with performance metrics via SPM

### *Logstash*

- See: **Forensics Network**
- Source: http://www.netwrix.com
- Logstash is a data pipeline that helps the processing of logs and other event data from a variety of systems.
- Logstash can connect to a variety of sources and stream data at scale to a central analytics system.
- It provides a convenient way to custom logic for parsing these logs at scale.

## *Loki ICMP Tunneling*

- See: **Penetration Testing**
- Provides shell access over ICMP.

## *Lotus Notes Forensics Tool*

- See: **E-Mail Forensics**
- Source: http://www.mailproplus.com
- It recovers and extracts evidence from NSF Files.

***Features:***

- Forensically Analyze Lotus Notes mails with several preview modes for carving out evidence
- Multiple search types like general expression available to look for available trails
- Recursive listing option enables collective email preview displaying all emails

## *LSASecretsView*

- See: **Password Cracker**
- http://www.nirsoft.net

## *Lucent Personalized Web Assistant*

- Lösung zum Schutz der Privatsphäre
- Cookies, IP-Addresses

## *Lynis*

- See: **Vulnerability scanner**
- Link: https://cisofy.com/lynis
- Source: Kali Linux
- ***Open Source security auditing tool.***
- Its main goal is to audit and harden ***Unix*** and ***Linux*** based systems.
- It scans the system by performing many security controls checks.
- Examples include searching for installed software and determine possible configuration flaws.
- Many tests are part of common security guidelines and standards, with on top additional security tests.
- After the scan, a report will be displayed with all discovered findings.

```
lynis audit
```

## *MaaTec Network Analyzer*

- See: **Forensics Network**
- Source: http://www.maatec.com
- The MaaTec Network Analyzer is a tool that allows capturing, saving, and analyzing network traffic on a LAN or a DSL internet connection.
- We can use this tool for network troubleshooting, to analyze the existing network infrastructure, or for long-term network monitoring.

***Features:***

- Unique new packet information display in split window
- Supports multiple network cards in one or multiple windows
- Reports with charts and multiple data tables
- Provides support for files that are larger than 2 GB
- Enables online view of incoming packets

## *MacQuisition*

- See: **Forensics**
- Source: https://www.blackbagtech.com
- Data acquisition

### *MAC Flood*

- See: **Penetration Testing**
- Vielleicht auch eine gleichnamige SW?

### *Mac Data Recovery Guru*

- See: **File Recovery (MAC)**
- http://macosxfilerecovery.com

### *Mac Data Recovery*

- See: **File & Partition Recovery (MAC)**
- http://mac.powerdatarecovery.com
- http://www.kerneldatarecovery.com

### *MacKeeper Files Recovery*

- See: **File Recovery (MAC)**
- http://www.data-retrieval.net

### *MAGNET IEF*

- See: **Forensics**
- Source: https://www.magnetforensics.com
- Can be used by forensics professionals to find, analyze, and report on the digital evidence from computers, smartphones, and tablets
- It can recover evidence from a variety of data sources (ex: here ***Dropbox***) and integrate them into a single Magnet IEF case file
- The tool processes the raw, unstructured and disparate data in the forensic image, or file dump and extracts the meaningful data for each supported artifact type.
- It searches for the artifacts of multiple categories from allocated and unallocated space over the computer devices.
- Investigators use Magnet IEF to find, analyze and report on the digital evidence from computers, Smartphones, and tablets.
- It automates the digital forensic evidence.
- The tool can recover artifacts from unallocated space by extracting data from the files that are not sequential, out of order, or missing entirely irrespective of the disk sizes and integrates them into a single Magnet IEF case file.
- All the digital evidence recovered by a MAGNET IEF search is organized and stored in an IEF Case File, a database comprised of distinct artifact tables for each supported artifact type.

### *Macrium Reflect Free*

- See: **Forensics**
- Source:http://www.macrium.com
- Data acquisition

### *Macronit Disk Partition Expert*

- See: **Disk Management**

### *Magnet Axiom*

- See: **Forensics**
- Source:https://www.magnetforensics.com
- Ist ein „All-in-One“-Tool für forensische Ermittlungen, mit dem Sie in ein und demselben Fall Beweise auf Computern und mobilen Geräten untersuchen können.
- Egal, ob Sie forensische Bilder sichern oder Bilder von anderen Tools laden – mit der hohen Verarbeitungskapazität von Magnet AXIOM finden Sie Beweise, die anderen Tools entgehen würden.

### *MailXaminer*

- See: **Forensics E-Mail**
- Source: https://www.mailxaminer.com
- It is used to search and uncover relevant information by conducting, coordinating, and real-time monitoring of a case with an investigative team to get thorough and unambiguous evidence in a ***court admissible file format***.
- Is an e-mail searching, reporting, and exporting tool that enables the law enforcement agencies to execute investigations and detailed analyses of the suspected e-mails

### *Maltego*

- See: **Penetration testing tool**
- Source: paterva.com
- Supplier: Paterva
- See also: Kali Linux
  beenverified.com
- GUI Tool
- Interactive ***data mining tool***
- ***Penetration testing tool***
- Finding relatshionships between pieces of information from various internet sources
- To find informations about people
- ***E-Mail Addresses*** per domain

Pricing: Free community edition (Limited functionalities)

***Example 1***

1. Run Machine
2. Footprint L1
3. Run Transforms

### *Magnet RAM Capture*

- See: **Forensics**
- Source: https://www.magnetforensics.com
- Data acquisition

### *Masker*

- See: **Anti Forensics Tool**
- http://www.softpuls.com

### *McAfee Enterprise Log Manager*

- See: **Forensics Network**
- Source: http://www.mcafee.com
- McAfee Enterprise Log Manager collects, compresses, signs, and stores all original events with a clear audit trail of activity that cannot be repudiated.

### *MD5 Calculator*

- See: **Forensics**
- MD5 Calculator is a bare-bones program for calculating and comparing MD5 files.
- While its layout leaves something to be desired, its results are fast and simple.

### *MD5SUM*

- RFC 1321
- To check the value of 128-bit ***MD5*** hashes.

### *Medusa/Mendax*

- See: **Password Cracker**
- Source: Kali Linux (Julian Paul Assage)

- CLI
- Packet crafting

### *MegaPing for Windows*

- Complete network information and supervision pack
- MegaPing is a good, trial version software only available for Windows, that belongs to the category Networking software.
- MegaPing is a light software that takes up less storage than many software in the section Networking software.
- It's a very popular program in Germany, Zambia, and Myanmar.Since the program has been added to our selection of programs and apps in 2005, it has achieved 12,744 downloads, and last week it gained 3 downloads.MegaPing is available for users with the operating system Windows 95 and previous versions, and you can get it only in English.

### *Memory Viewer*

- See: Forensics
- http://www.rjlsoftware.com

### *Metadata Assistant*

- See: **Forensics**
- http://www.thepaynegroup.com

### *Metagoofil*

- See: **Reconnaissance**
- Source:https://tools.kali.org/information-gathering/metagoofil
- Metagoofil is an ***information gathering tool*** designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.
- Extracting metadata from files, collected.

```
Metagoofil -d <domain> -t doc,docx -l 50 -n 20 -f <output.html>
```

### *Metasploit*

- See: **Penetration Testing**
- Link: **metasploit.com**
- Source:Kali Linux
- The preferred tool/Framework for penetration testing.

**Modules:**

- **Rex** (Ruby Extension Library) library
- psexec → to obtain access to a system that you already know the credentials
- msfencode
- msfpayload
- War dialing with: ***WarVOX***

Start: https://localhost:3790

### *Metascan Online*

- See: **Online Malware Analysis**
- Source: https://www.opswat.com/blog/tag/metascan-online
- Metascan Online is an online file scanning service powered by OPSWAT's Metascan technology, a multiple-engine malware scanning solution.

### *Microsoft Security Compliance Toolkit 1.0*

- See: **Compliancy Checker**
- The ***Security Compliance Toolkit (SCT)*** is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products.

### *MiniTool Power Data Recovery Enterprise*

- See: **Forensics**
- Source: http://www.minitool.com
- MiniTool Power Data Recovery Enterprise Edition can ***recover data*** including images, texts, videos, music, and emails.
- It supports different data loss situations like important data lost because of deletion by mistake, formatting, logical damage, etc.

### *MiniTool Power Data*

- See: **Partition Recovery**
- Recovery Free http://www.powerdatarecovery.com

### *MiniTool Partition Wizard*

- See: **Disk Management**

### *MJ Registry Watcher*

- See: **Monitoring Registry**
- Source: http://www.jacobsm.com
- MJ Registry Watcher is a registry, file and directory hooker that safeguards the most important startup files, registry keys and values, and other registry locations commonly attacked by trojans.

### *MobiControl*

- MDM

### *Mobile Field Kit*

- See: **Forensics**
- Source:https://www.paraben.com
- Data qcquisition

### *MOBILedit! Forensic*

- See: **SIM Data Acquisition Tools**
- Source: http://www.mobiledit.com
- MOBILedit Forensic allows the investigator to view, search, or retrieve data from a mobile device, including call history, phonebook, text messages, multimedia messages, files, calendars, notes, reminders, and raw application data.
- It will also retrieve device information such as IMEI, operating systems, firmware including SIM details (IMSI), ICCID, and location area information.
- This tool facilitates access to the SIM card status information (IMSI, ICCID, LAI, PIN, PUK, and call costs) as well as review and export a list of all SIM card applications.
- It can also read deleted messages from the SIM card.

### *Mobilyze*

- See: **iPhone Data Acquisition Tools**
- Source: http://www.blackbagtech.com
- Mobilyze is a mobile data triage tool, designed to give users immediate access to data from iOS and Android devices.

### *MONIT*

- See: **Monitoring**
- Source: http://mmonit.com
- Monit is an open source utility for managing and monitoring UNIX systems.
- It conducts automatic maintenance and repair and can execute meaningful causal actions in error situations.

### *MoSucker*

- See: **Penetration Testing**
- MoSucker is a powerful backdoor - hacker's remote access tool.

### *MRTG*

- See: **Traffic monitoring tool**
- Linux
- Monitors SNMP traffic

Pricing:

- Free Software

### *MS Outlook PST Recovery Tool*

- See: **E-Mail Forensics**
- Source: http://quickdata.org
- It is a reliable solution to repair corrupted PST files, recover shift deleted emails, contacts, tasks, and save data in the different formats like; PST, MSG, or EML.

### *MSFVENOM*

- See: **Penetration Testing**
- Msfvenom is the combination of **payload generation** and encoding.
- It replaced ***msfpayload*** and ***msfencode*** on June 8th 2015.

### *MultiMon*

- See: **Forensics**
- http://www.resplendence.com

### *MxToolBox Email Header Analyzer*

- See: **E-Mail Forensics**
- Source: http://mxtoolbox.com
- This tool will make email headers human readable by parsing them according to RFC 822.

### *My Drivers*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.zhangduo.com
- My Drivers enables to detect, backup and restore all hardware device drivers currently on the system.
- In addition, it allows finding the latest drivers for the hardware and installing them onto the computer.
- One can back up the list of all hardware devices extracted, into the desired folder and restore them after reinstalling or upgrading the system.

### *MyEventViewer*

- See: **Forensics Network**
- Source: http://www.nirsoft.net
- MyEventViewer allows the users to watch multiple event logs in one list. Additionally, MyEventViewer allows easy selection of multiple event items and saving them to HTML/Text/XML file or copying them to the clipboard (Ctrl+C) and pasting them into Excel.

### *N-Stalker Tool*

- See: **Vulnerability Scanner**
- Web applications are tested for implementing security and automating vulnerability assessments.
- Doing so prevents ***SQL injection*** attacks on web servers and web applications.
- Websites are tested for embedded malware and by employing multiple techniques.

### *Nagios Log Server*

- See: **Web Attack Investigation**
- Source: https://www.nagios.com
- Nagios Log Server is a Centralized Log Management, Monitoring and Analysis Software.
- It simplifies the process of searching your log data.
- It sets up alerts to notify you when potential threats arise or simply query your log data to audit any system.
- Here, all log data are present in one location.

### *Nagios XI*

- See: **Monitoring Windows Services**
- Source: http://www.nagios.com
- Nagios XI monitors the state of any Microsoft Windows service such as ***IIS***, ***Exchange***, and ***DHCP***, and alerts whenever the service stops or crashes.

***Features:***

- Increased server, services, and application availability
- Detects network outages and protocol failures
- Detects failed processes and batch jobs

### *Service+*

- Source: http://www.activeplus.com
- Service+ provides advanced features to manage Windows services (custom views, specific properties, monitoring, etc.).

***Features:***

- Implements multiple services such as startup, account, dependencies, name, and path simultaneously
- Monitors services installation and un-installation in real time
- Terminates un-responding services without any reboot
- Allows all authenticated users to start a service
- Prohibits all users, including administrators to stop critical services such as backup and critical applications
- Manages the services on a remote computer
- Sorts services by standard and advanced properties such as name, status, startup, and type
- Imports or exports the configuration of services as an XML file to duplicate them, to backup settings, or to mirror the same configuration on several computers

### *Neotrace*

- See: **Reconnaissance / *Footprinting***
- NeoTrace ist ein Allrounder wenn's um Internet-Informationen geht.
- Damit Sie wissen, mit welchen Internet-Servern Sie es zu tun haben, setzen Sie NeoTrace ein.
- Damit spüren Sie alle Zwischenstationen von Ihrem Provider bis zur Zielhomepage auf.
- Bei Nichterreichen einer Webseite können Sie mit TraceRoute schnell herausfinden, ob das Problem bei Ihrem Provider liegt oder der Webserver der Homepage down ist.

### *Nessus*

In Greek mythology, ***Nessus*** (Ancient Greek: Νέσσος) was a famous ***centaur*** who was killed by Heracles, and whose tainted blood in turn killed Heracles. He was the son of Centauros. He fought in the battle with the Lapiths and became a ferryman on the river, Euenos.
*Source: Wikipedia*

- See: **Vulnerability Scanner**
- See: **Compliancy Checker**

- Source: www.tenable.com
  www.nessus.org
  www.youtube.com/tenablesecurity Videos
- See also: **Tenable Security Center (TSC)**
- Hybrid tool.
- Network ***vulnerability scanner*** managed by ***Tenable Network Security***.
- **Web** vulnerability scan.
- Can be used for ***session splicing.***

**Versions:**

| | |
|---|---|
| Nessus Essentials | Free (Scan 16 IPs) |
| Nessus Professional | USD 2'190/Year |
| Nessus Manager | USD 2'920/Year |
| | |
| Nessus for W10Pro: | 6.11.2 |
| Nessus for WVista | 5.2.5 |
| Nessus for WXP: | 5.2.1 (unable to install under WXP SP3. Tried 4 times) |
| | |
| Start: | https://localhost:8834 |

**Remark:**
Takes very long to install (2 h).

## *NetBIOS Enumerator*

- See: **Network Enumeration**
- Enumeration is the first attack on a target network, used to gather the information by actively connecting to it.
- You must have sound knowledge of enumeration, a process that requires an active connection to the machine being attacked.
- A hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab, we enumerate a target's user name, MAC address, and domain group.

## *Netbus*

- Price: Shareware
- NetBus ist ein Fernwartungstool für Microsoft Windows, das meist illegal eingesetzt wird.
- In seiner Funktionalität entspricht es ***Back Orifice (Port: 31337)***, verfügt allerdings über mehr Möglichkeiten.
- Es wurde von dem Schweden Carl-Fredrik Neikter in Delphi geschrieben, der die erste Version Mitte März 1998 veröffentlichte.
- Derzeit liegt das Programm in den Versionen 1.60, 1.70 und als NetBus 2.01 Pro vor.

## *Netcat*

- See: **Tool**
- Command Line Tool (CLI)
- "Swiss Army Knife" for hackers.
- Collect volatile data over a network
- Netcat, auch ***nc*** genannt, ist ein einfaches Werkzeug, um Daten von der Standardein- oder -ausgabe über Netzwerkverbindungen zu transportieren.
- Es arbeitet als Server oder Client mit den Protokollen TCP und UDP.
- Supports SSL, IPv6, SOCKS, http proxies, connection brokering, and more …

***EXAMPLES***

```
-e                                → to execute a program
nc -l -u -p55555 < /etc/passwd    → Grabs the passwd file when connected to
                                    UDP port 55555
```

```
nc -l -p 2222 | nc x.x.x.x 1234   → Listen on port 2222 and output anything
received
                                     to x.x.x.x port 1234
nc -u -v -w2 x.x.x.x 1-1024       → UDP port scan
nc x.x.x.x -p <port>              → Establish a connection to a listening port
```

## *Netcross*

- See: **DNS-Tool**
- TCP over DNS

## *NetDiscover*

- See: **ARP Reconnaissance Tool**
- Source: Kali Linux

```
netdiscover -f <IP>             → Fast Mode
netdiscover -r <IP/24>          → Returns IP / MAC / MAC Vendor (LONG RUN!)
```

## *NetHunter*

- See: **Penetration testing tool**
- Kali NetHunter is an Android ROM overlay that includes a mobile penetration testing platform.
- It is officially available for download on newer Nexus devices and the OnePlus One, as well as some Samsung Galaxy models.
- It also works unofficially on other phones.
- Started in 2014, the Kali Linux NetHunter project is the first Open Source Android penetration testing platform for Nexus devices, created as a joint effort between the Kali community member “BinkyBear” and Offensive Security, the company behind the Kali Linux desktop distribution.
- The overlay includes a custom kernel, a Kali Linux chroot, and an accompanying Android application, which allows for easier interaction with various security tools and attacks.
- In addition to the penetration testing tools featured on desktop Kali Linux, NetHunter also Wireless 802.11 frame injection, one-click MANA Evil Access Points, HID keyboard (Teensy-like attacks), as well as BadUSB man-in-the-middle attacks.
- It is based on Kali Linux distribution and tool sets. NetHunter is an open-source project developed by Offensive Security and the community.

## *Netcraft*

- See: **Anti Phishing**
- Source: toolbar.netcraft.com
- Against Phishing

## *NetScan Tools Pro*

- See: **Reconnaissance**
- Source: www.netscantools.com
- NetScanTools Pro is an integrated collection of internet information gathering and network troubleshooting utilities for Network Professionals.
- Research IPv4 addresses, IPv6 addresses, hostnames, domain names, email addresses and URLs automatically** or with manual tools.
- It is designed for the Windows operating system. **Automated tools are started interactively by the user.
- Affectionately called "NetScan" by our users, this software has a long user-driven development history and is used by thousands of network professionals and persons involved in 'ethical hacking'

***Features***

- ARP Scan
- ARP Ping
  Search for duplicate IP Addresses

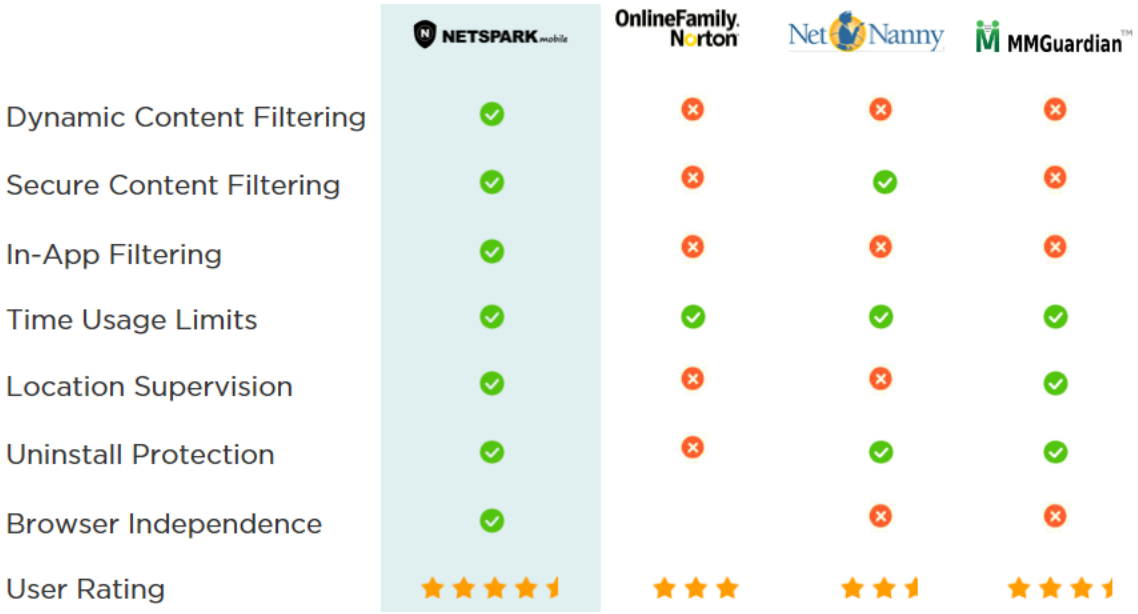
- Graphical Ping
- Multitrace
- Tracertoute
- DNS Tools

**Price:**

- Installed version is ***$249*** for a single license that you can install on a desktop and laptop.
- USB version is ***$299*** for a license on a high speed USB 3.0/2.0 Flash Drive.

## *Netspark Mobile*

- Source: https://www.netsparkmobile.com/en/
- Access the Web, Facebook, Youtube, Whatsapp, and keep access to your favourite apps with NetSpark Mobile.
- Let our real-time inspection and filtering protection keep unwanted content off your phone/tablet so you can focus on what really matters




## *NetStumbler*

- See: **WiFi**
- Source: netstumbler.com
- ***Detect*** Wireless LAN's.
- Cannot monitor traffic on ***802.11n*** networks
- Can be used as ***IDS*** on wireless networks
- ***Collect*** wireless packets

## *NetSurveyor*

- See: **WiFi**
- ***WLAN-Scanner*** mit grafischer Auswertung; benötigt .NET 3.5

## *NetWitness Investigator*

- See: **Forensics Network**
- Captures live traffic and processes packet files from virtually any existing network collection device for analysis.
- The tool can locally process packet files and record in real time from a network tap or span port with immediate insight into network traffic.
- The tool is the primary interactive application of the NetWitness AppSuite.

### *NetworkMiner*

- See: **Forensics Network**
- Source: http://www.netresec.com
- NetworkMiner is a Network Forensic Analysis Tool for Windows/Linux/Mac OS X/FreeBSD used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports, etc., ***without placing any traffic strain on the network***.
- NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

### *Network Probe*

- See: **Forensics Network**
- Source: http://www.objectplanet.com
- Network Probe is the network monitor and protocol analyzer to monitor network traffic tool.
- It can find the sources of any network slow-downs.
- The tool displays the protocols used on your network, which hosts are sending and receiving data, where the traffic is coming from, and when all this happens.
- The Network Probe allows configuring in such a way that it can notify if anything out of the ordinary happens and can proactively fix the problem before it grows into a serious one

### *Network Solutions Whois*

- See: **WHOIS Online Tool**
- Source: http://www.networksolutions.com
- Network Solutions Whois is an online tool used to look for domain availability.

### *Network Topology Mapper*

- ***SolarWinds Network Topology Mapper*** automatically discovers your network and produces a comprehensive network diagram that can be easily exported to Microsoft Office or Visio.
- Network Topology Mapper automatically detects new devices and changes to network topology.
- It simplifies inventory management for hardware and software assets, addresses reporting needs for PCI compliance and other regulatory requirements.

### *Network-Tools.com*

- See: **WHOIS Online Tool**
- Source: http://network-tools.com
- Network-Tools.com is an online tool used to perform whois lookup on a target website.

### *Netwrix Auditor in Action*

- See: **Compliancy Checker**

### *Netwrix Service Monitor*

- See: **Windows Services Monitoring Tool**
- Source: http://www.netwrix.com
- Netwrix Service Monitor is a tool to monitor critical Windows services and optionally restart them after failure.
- The tool tracks all automatic startup services on multiple servers at a time and sends e-mail alerts when one or more services stops unexpectedly.
- The optional automatic restart feature ensures that all monitored services are up and running without downtime.

### *NetResident*

- See: **Forensics Network**
- Source: http://www.tamos.com
- NetResident is a network content analysis application designed to monitor, store, and reconstruct network events and activities, such as e-mail messages, web pages, downloaded files, instant messages, and VoIP conversations.

- NetResident saves the data to a database, reconstructs it, and displays the content in a simple format.

***Features***

- In-depth, real-time view of network traffic and storage of data in a database
- Deep packet inspection: state-of-the-art technology for searching, identifying, and reconstructing many protocols and data types: HTTP, POP3, SMTP, FTP, News, VoIP (SIP, H.323), IM (MSN, Yahoo, ICQ, etc.), Web Mail (Gmail, Hotmail, etc.), Telnet.
- Customizable alerts: pop-ups, e-mail notifications, SNMP traps, to name a few
- Log file import in popular formats for post-capture forensic analysis: PCAP, CommView, etc.

## *NetXRay Analyzer*

- Protocol Analyzer and Network Monitor

## *Nexpose*

- See: **Vulnerability Scanner**
- Link: rapid7.com
- Installation: ***On-prem***

## *Nikto*

- See: ***Vulnerability Scanner Webserver***
- Source: Kali Linux
- ***Command Line Tool***
- Nikto is an ***Open Source (GPL)*** web server scanner which performs comprehensive tests against ***web servers*** for multiple items, including over 6700 potentially dangerous files/programs, ***checks for outdated versions*** of over 1250 servers, and version specific problems on over 270 servers.
- Nikto Web Scanner is a Web server scanner that tests Web servers for ***dangerous files/CGIs***, ***outdated server software*** and other problems.
- It performs generic and server type specific checks.
- It also captures and prints any ***cookies*** received.
- The Nikto code itself is Open Source (GPL), however the data files it uses to drive the program are not.
- It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.
- Scan items and plugins are frequently updated and can be automatically updated.
- Nikto is ***not designed as a stealthy tool***.
- It will test a web server in the quickest time possible and is obvious in log files or to an IPS/IDS.
- However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).
- Not every check is a security problem, though most are.
- There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server.
- These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

**Features**

SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)

- Full HTTP proxy support
- Checks for outdated server components
- Save reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scan multiple ports on a server, or multiple servers via input file (including nmap output)
- LibWhisker's IDS encoding techniques
- Easily updated via command line

- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Mutation techniques to "fish" for content on web servers
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guess credentials for authorization realms (including many default id/pw combos)
- Authorization guessing handles any directory, not just the root directory
- Enhanced false positive reduction via multiple methods: headers, page content, and content hashing
- Reports "unusual" headers seen
- Interactive status, pause and changes to verbosity settings
- Save full request/response for positive tests
- Replay saved positive requests
- Maximum execution time per target
- Auto-pause at a specified time
- Checks for common "parking" sites
- Logging to Metasploit
- Thorough documentation

***EXAMPLES: <nikto …>***

```
--help                          → Shows the options
-dbcheck
-Format+
-F                              → File type of -o
-host <IP>                      → Scanns by default on port 80
-host <IP> -port 443            → Searches on port 443
-host <IP> -port 1-1024         → Searches the given port range
-host <IP> -output ./x.txt      → Output to x.txt
-host <domain>                  → San on port 80
-o                              → Ouput
-port
-update
```

## *njRAT*

- See: **RAT**
- njRAT is a **Remote Access Trojan (RAT)** intensive in its data-stealing capabilities.
- In addition to logging keystrokes, this malware can access target computers' cameras, stealing credentials stored in browsers, uploading/downloading files, manipulating processes and files, and viewing their desktops.
- The njRAT Trojan remains one of the most successful RATs in the wild because of the widespread online support and tutorials available to cyber-criminals.
- There are a variety of .NET obfuscation tools that make detection difficult for antivirus solutions and hinders analysis by security researchers.
- njRAT utilizes dynamic DNS for command and control (C2) servers and communicates using a custom TCP protocol over a configurable port.
- The njRAT, developed in .NET, allows attackers to take complete control of an infected device.
- The malware can log keystrokes, downloading and executing files, providing remote desktop access, stealing application credentials, and accessing the infected computer's webcam and microphone.
- PhishMe reports that njRAT has been distributed over the past period with the aid of spam emails advertising a car changer hack for the "Need for Speed: World" video game.
- Zscaler also noted that video game cracks and application key generators are often used as lures.
- Being a security administrator or an ethical hacker, your job responsibilities include finding machines vulnerable to Trojan attacks, protecting the network from malware, Trojan attacks,

stealing valuable data from the network, and identity theft.

The C&C callback from the infected system includes following information:

- Bot identifier (based off configurable string in builder and volume serial number)
- Computer name (base-64 encoded)
- Operating system information
- Existence of attached webcam (“Yes”/“No”)
- Bot version
- Country code
- Title of the active process window

## *Nmap*

- See: ***Vulnerability Scanner***
- See also: SW Nmap.docx
- Source: nmap.org
  Sectools.org

**Remark:** Easy installation and handling.
Host **scanme.nmap.org** is allowed to be scanned with nmap!!!

nmap -v -A [IP]

## *NowSecure Forensics*

- See: **iPhone Data Acquisition Tools**
- Source: https://www.nowsecure.com/forensics
- NowSecure Forensics extracts, parses, and analyzes the device data and aids investigators by providing with mobile security solutions.

## *NPING*

- May discover NAT-Devices and Transparent-Proxy.

***EXAMPLES***

nping --echo-client "public" echo.nmap.org -udp → NAT Devices
nping --echo-client "public" echo.nmap.org --tcp -p80 → Transparent Proxy

## *NTBugTraq*

http://www.ntbugtraq.com/

## *NT Crack*

http://www.secnet.com/

## *NT Locksmith*

http://www.winternals.com/

## *NTFSDOS Tools*

http://www.winternals.com/

## *NTFS Data Recovery Toolkit*

- See: **Partition Recovery**
- http://www.ntfs.com

## *TestDisk for Windows*

- See: **Partition Recovery**
- http://www.cgsecurity.org

### *NTHandle*

http://www.sysinternals.com

### *Ntopng*

- See: **Forensics Network**
- Source: http://www.ntop.org
- Ntopng is a network traffic probe that shows the network usage, similar to what the popular top Unix command does.
- Ntopng is based on libpcap, and it runs on every Unix platform, MacOSX and on Windows.
- Ntopng users utilize a web browser to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status.
- In the latter case, ntopng acts as a simple RMON-like agent with an embedded web interface.

***Features***

- Sorts network traffic according to many criteria, including IP address, port, L7 protocol, throughput, AS.
- Shows network traffic and IPv4/v6 active hosts.
- Produces reports about various network metrics such as throughput, application protocols
- Stores on disk persistent traffic statistics in RRD format
- Geo-locates hosts and displays reports according to host location
- Characterizes HTTP traffic by leveraging on characterization services provided by Google and HTTP Blacklist.
- Shows IP traffic distribution among the various protocols
- Analyses IP traffic and sorts it according to the source/destination.
- Produces HTML5/AJAX network traffic statistics.

### *NTRecover*

http://www.winternals.com/

### *NTUndelete*

http://www.winternals.com/

### *ntopng*

Link: www.ntop.org

- Traffic monitoring tool (Linux).

### *NTSECURITY.COM*

http://www.ntsecurity.com/default.htm

### *Nuix Corporate Investigation Suite*

- See: **Forensics**
- Source:http://www.nuix.com
- The Nuix Corporate Investigation Suite is used to collect, process, analyze, review, and report on electronic evidence.

### *Nuix Investigator Lab*

- See: **E-Mail Forensics**
- Source: http://www.nuix.com
- Nuix Investigator Lab is for organizations looking to set up a dedicated facility that can rapidly ingest and process terabytes of digital evidence per day and make it available for timely analysis.

- It enables multiple investigators and subject matter experts simultaneously to review and collaborate on an investigation with secure remote access, and produce comprehensive reports on your findings.

### *Observer*

- See: **Forensics Network**
- Is a software used for troubleshooting in a network.
- It has features such as expert analysis, VoIP tools, in-depth application analysis, connection dynamics, stream reconstruction, and more, in addition to offering support for SNMP and RMON device management.
- Users can generate and share reports via the web, add custom decode modules for use in proprietary environments, and extract data from external sources using SOAP.

### *Office Multi-document Password Cracker*

- See: **Password Cracker**
- Office Multi-document Password Cracker cracks lost passwords to multiple MS Office documents.
- It scans the drives for protected documents and restores passwords from all Word, Excel, PowerPoint, Access, and Outlook documents it finds.

### *Office Password Recovery*

- See: **Password cracker**
- Source: http://www.passwordrecovery.in
- Office Password Recovery tool recovers lost or forgotten passwords for Microsoft Word, Excel, Access, PowerPoint, OneNote, Outlook email accounts, and personal folder files.
- It recovers all types of passwords, including instant recovery of passwords to modify, database passwords, workbook passwords, pst passwords, and email account passwords.

### *Office Password Recovery Lastic*

- See: **Password Cracker**
- http://www.passwordlastic.com

### *Office Password Genius*

- See: **Password cracker**
- http://www.isunshare.com

### *Offline NT Password &*

- See: **Password Cracker**
- Registry Editor http://pogostick.net

### *OllyDbg*

- OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is not available.
- It traces registers, recognizes procedures, API calls, switches, tables, constants, and strings, and locates routines from object files and libraries.

### *OmniHide PRO*

- See: **Anti Forensics Tool**
- http://omnihide.com

### *OmniPeek*

- Gives network engineers real-time visibility and expert analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and video to remote offices.

- By using OmniPeek's intuitive user interface and the "top-down" approach to visualize network conditions, network engineers can analyze, drill down and fix performance bottlenecks across multiple network segments, maximizing uptime and user satisfaction.

***Features***

- Network performance management and monitoring of networks, including network segments at remote offices
- Monitoring of key network statistics in real time, aggregating multiple files, and instantly drilling down to packets using the "Compass" interactive dashboard
- Seamless management of all OmniEngine software probes, and Omnipliance and TimeLine network recorders in the network
- Integrated support for Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless (including 3-stream), VoIP, video, MPLS, and VLAN
- Intuitive drill-down to understand which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- Complete voice and video over IP real-time monitoring, including high-level multimedia dashboard, call data record (CDR) and comprehensive signaling and media analyses.

## *OneClickRoot*

- See: **Android Rooting Tools**
- Source: https://www.oneclickroot.com
- This utility allows the users to root their Android mobile devices without having a good understanding or its firmware and kernel.

***Features:***

- Access full potential of your device
- Install compatible custom firmware
- Access the blocked features of device administration
- Preserves battery life by freezing unnecessary applications running in the background
- Enhances the performance of the device

## *Online Password Recovery*

- See: **Password Cracker**
- http://www.password-find.com

## *Ontrack EasyRecovery*

- See: **Forensics**
- Source: https://www.krollontrack.com
- Ontrack EasyRecovery is a data recovery software ready to retrieve missing files.
- It recovers data and also protects it.

## *Onion routing*

- See: **Anti Forensics Tool**
- Attackers use virtual routers such as, the Onion routing approach, which provides ***multiple layers of protection***.
- Onion routing is the technique used for ***secret communication*** over a computer network.
- This network encapsulates messages in layers of encryption, similar to the layers of an onion and employs a worldwide volunteer network of routers that serve to anonymize the source and destination of communications.
- Therefore, ***tracing this type of communication*** and attributing it to a particular source is very difficult for investigators.

## *Ontrack® EasyRecovery*

- See: **File Recovery**
- http://www.krollontrack.com

## *Ontrack Eraser Degausser*

- See: **Anti Forensics Tool**
- http://www.krollontrack.co.uk

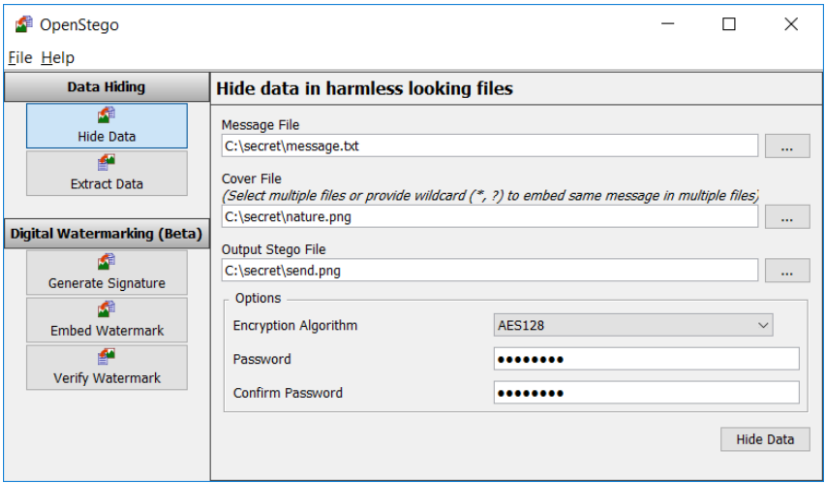
## *OpenSSL*

- See: **Tool**
- For testing ***TLS***.

```
openssl <client> -connect <domain>:443>
```

## *OpenStego*

- See: **Steganography Tool**
- Source: https://www.openstego.com/




## *OpenVAS*

- See: **Vulnerability Scanner**
- Source: www.openvas.org
- ***Open Source***
- In ***2005***, the developers of the vulnerability scanner Nessus decided to discontinue the work under Open Source licenses and switch to a proprietary business model.
- See also ***Greenbone Vulnerability Management (GVM)*** and ***Greenbone Source Edition (GSE).***

## *Ophcrack*

- See: **Forensics / Password cracker**
- Source: Kali Linux
  http://ophcrack.sourceforge.net
- CLI
- Free Windows password cracker based on rainbow tables.
- It comes with a Graphical User Interface and runs on multiple platforms.

## *OpManager*

- See: **Monitoring**
- Source: http://www.manageengine.com
- ManageEngine OpManager is a network and data center infrastructure management software that helps large enterprises, service providers, and SMEs manage their data centers and IT infrastructure efficiently and cost-effectively.
- Automated workflows, intelligent alerting engines, configurable discovery rules, and extendable templates enable IT teams to setup a “24x7” monitoring system.

- Do-it-yourself plug-ins extend the scope of management to include network change and configuration management and IP address management as well as monitoring of systems, applications, databases, virtualization, and NetFlow-based bandwidth.

### *Orion File Recovery Software*

- See: **File Recovery**
- http://www.nchsoftware.com

### *OSFClone*

- See: **Forensics**
- Source: http://www.osforensics.com
- Data acquisition

### *OSForensics*

- See: **Forensics**
- See: E-Mail Forensics
- Source: http://www.osforensics.com
- Extract forensic data from computers, and uncover the ***data hidden*** inside a PC.
- It helps discover relevant forensic data faster with high performance file searches and indexing as well as restores deleted files.
- It identifies suspicious files and activity with hash matching, drive signature comparisons and looks into e-mails, memory and binary data.
- It also manages digital investigation, organizes information and creates reports about collected forensic data.

### *OSSEC*

- See: **Forensics Network / File and Folder Integrity Checkers**
- Source: http://ossec.github.io
- OSSEC is an open-source host-based intrusion detection system (HIDS).
- It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting, and active response.
- It runs on operating systems such as Linux, OpenBSD, FreeBSD, Mac OS X, Solaris, and Windows.
- OSSEC watches it all, actively monitoring all aspects of UNIX system activity with file integrity monitoring, log monitoring, root check, and process monitoring.
- With OSSEC you won't be in the dark about what is happening to your valuable computer system assets.
- When attacks happen, OSSEC lets you know through alert logs and email alerts sent to you and your IT staff so you can take quick actions.
- OSSEC also exports alerts to any SIEM system via syslog so you can get real-time analytics and insights about your system security events.

### *OSSIM*

- Open Source Security Information Management.

### *OWASP LAPSE Project*

- See: **Vulnerability Scanner Code**
- Link: OWASP LAPSE Project
- Is LAPSE+ the Security Scanner for ***Java EE Applications***.

### *OWASP O2 Project*

- See: **Tool**
- OWASP O2 Platform

- The O2 platform represents a new paradigm for how to perform, document and distribute Web Application security reviews.
- O2 is designed to Automate Security Consultants Knowledge and Workflows and to Allow non-security experts to access and consume Security Knowledge.

### *OWASP Orizon Project*

- See: **Vulnerability Scanner Code**
- OWASP Orizon Project
- Is a ***source code security scanner*** designed to spot vulnerabilities in J2EE web applications, Android code and in Java written source code.

### *OWASP SonarQube Project*

- See: **Vulnerability Scanner Code**
- Source: OWASP SonarQube Project
- SonarQube is one of the world's most popular continuous ***code quality tools*** and it is actively used by many developers and companies.

### *OWASP WAP-Web Application Project*

- See: **Vulnerability Scanner Code**
- Link: OWASP WAP-Web Application Protection
- Web Application Protection (WAP) is a tool to detect and correct input validation vulnerabilities in web applications written in ***PHP*** and predicts false positives.

### *OWASP ZAP*

- See: **Penetration Testing**
- Link: https://www.zaproxy.org
- OWASP ZAP (short for Zed Attack Proxy) is an open-source ***web application security scanner***.
- It is intended to be used by both those new to application security as well as professional penetration testers.
- It is one of the most active OWASP projects and has been given Flagship status.
- It is also fully internationalized and is being translated into over 25 languages.
- When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using https.
- It can also run in a 'daemon' mode which is then controlled via a REST Application programming interface.
- This cross-platform tool is written in Java and is available in all of the popular operating systems including Microsoft Windows, Linux and Mac OS X.
- ZAP was added to the ToughtWorks Technology Radar in May 2015 in the Trial ring

### *Oxygen Forensic® Kit*

- See: **Forensics**
- Source: http://www.oxygen-forensic.com
- The Oxygen Forensic® Kit is a ready-to-use and customizable mobile forensic solution for field and in-lab usage.
- It allows not only extraction of data from the device but also ***creates reports*** and ***analyzes data in the field***.

### *Oxygen Forensic Detective*

- See: **Forensics Mobile**

### *P0f-Tool*

- Passive ***OS fingerprinting tool***

### *PA File Sight*

- See: **File and Folder Integrity Checkers**
- Source: https://www.poweradmin.com
- PA File Sight is a file monitoring software that will help you determine who is reading from and writing to important files.
- It can tell you when a new file or folder is created or renamed.
- And, with our file watcher, when a file or folder gets deleted, PA File Sight can tell you who did it and which computer they did it from (IP address and computer name).

### *Packers*

- UPX, PECompact, BurnEye, Exe Stealth Packer, Smart Packer Pro

### *PageNest offline browser*

- See: **Website Mirroring**
- OS: Windows
- Price: Free Edition & Pro Edition $

### *PALADIN Forensic Suite*

- See: **Forensics**
- Source: https://www.sumuri.com
- PALADIN is a modified “live” ***Linux distribution*** based on Ubuntu used to fulfill various forensics tasks in a forensically sound manner via the PALADIN Toolbox.
- PALADIN is available in 64-bit and 32-bit versions.

### *Pandora Recovery*

- See: **File Recovery**
- http://www.pandorarecovery.com

### *PANGU JAIL BREAK*

- See: **iOS Jailbreaking Tools**
- Source: http://en.pangu.io
- The Pangu jailbreak tool allows the user to jailbreak iOS devices by running the click-to-jailbreak app and removes the jailbreak by rebooting the iOS devices.

### *Papertrail*

- See: **Forensics Network**
- Source: https://papertrailapp.com
- Papertrail is used for its time-saving log tools, flexible system groups, team-wide access, long-term archives, charts, analytics exports, and monitoring webhooks.

### *Parasoft*

- See: **Vulnerability Scanner Code**
- Source:https://www.parasoft.com
- Use Parasoft to validate that you’ve built a secure application by leveraging penetration testing and fuzzing.
- Then combine security testing with deep coverage analysis to pinpoint internal attack vectors and ensure you have thoroughly protected your application.

### *Paragon Hard Disk Manager 15 Suite*

- See: **Forensics**
- Source:https://www.paragon-software.com
- Data acquisition

### *Paraben's DP2C*

- See: **Forensics**
- Source: https://www.paraben.com
- DP2C is a data targeted collection tool for triage forensics.
- DP2C is special software that runs from a USB drive and allows the collection of specific type of data from Windows-based systems to the evidence drive.

### *Paraben's Email Examiner*

- See: **E-Mail Forensics**
- Source: https://www.paraben.com
- Email Examiner forensically examines email formats including Outlook (PST and OST), Thunderbird, Outlook Express, Windows mail and more.
- It allows to analyze message headers, bodies and attachments.
- It recovers email in the deleted folders, supports advanced searching, reporting and exporting to PST and other formats and supports all major email types that are stored on local computers for analysis, reporting, and exporting/conversion.

### *Paraben's P2C (P2 Commander)*

- See: **Forensics**
- Source: https://www.paraben.com
- P2C is a digital investigation tool used by forensic examiners.
- It has an integrated database with multi-threading.
- P2C was built on Paraben's trusted email examination tools for unparalleled network email and personal email archive analysis.

### *Paraben's SIM-Card Seizure*

- See: **Forensics Mobile**
- Source: https://www.paraben.com
- Paraben's SIM-Card Seizure is useful in recovering deleted SMS/ text messages.
- It also performs comprehensive analysis of SIM card data.

### *ParetoLogic Privacy Controls*

- See: **Anti Forensics Tool**
- http://www.paretologic.com

### *Partition Find & Mount*

- See: **Partition Recovery**
- http://findandmount.com

### *Pathping*

- A combination of ICMP & Tracert.

### *Passware Kit Forensic*

- See: **Password Cracking**
- Source: http://www.lostpassword.com
- This complete electronic evidence discovery solution reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms.

### *Passware Kit Standard*

- See: **Password Cracker**
- https://www.passware.com

### *Password Cracker*

- See: **Password Cracker**
- Source: http://www.amlpages.com

### *Password Unlocker Bundle*

- See: Password Cracker
- http://www.passwordunlocker.com

### *Path Analyzer Pro*

- Network route tracing can determine the intermediate nodes traversed towards the destination and can detect the complete route (path) from source to destination.

### *Pavuk*

- See: **Website Mirroring**
- OS: Linux

### *Malware Protection Center*

- See: **Online Malware Analysis**
- Source: https://www.microsoft.com/en-us/wdsi
- The Malware Protection Center is a service provided to protect computers from malware.
- Users submit the file containing malware or potentially unwanted software, and then Microsoft analyzes the file and generates a complete report of its findings.

### *Malwr*

- See: **Online Malware Analysis**
- Source: https://www.cyberdb.co/vendor/malwr/
- Supplier: CyberDB
- Malwr is a free malware analysis service and community that allows users to submit files to it and receive the results of a dynamic analysis.

### *PC Firewall 1.02*

- Supplier: McAfee
- Link: http://www.nai.com/

### *PC Services Optimizer*

- See: **Windows Services Monitoring Tool**
- Source: http://www.smartpcutilities.com
- PC Services Optimizer is a tweaking solution that enables to optimize Windows Services automatically.
- It turns off unneeded Windows services without affecting the normal function, which will make PC to run faster and more securely.

***Features:***

- Gaming Mode: It gives users' systems an immediate performance boost.
- Services Profiles: It saves user services settings in profiles, enabling the user to apply different settings in seconds, saving time especially when dealing with multiple computers or users.
- Services Manager: It enables advanced users to master Windows services including third party services by providing several tools for performing advanced functions

### *PCTuneUp Free Startup Manager*

- See: **Startup Programs Monitoring**
- Source: http://www.pctuneupsuite.com
- PCTuneUp Free Startup Manager is a system startup entry monitor and management tool.

- It displays the configuration of applications and processes to run automatically during startup or login and helps to disable or enable startup items from system boot.
- It displays the detailed information of the exact applications such as the name, type, and arguments, and it makes possible to process some operations of each item in the activated registry editor, such as import/export, modification, renaming, and copy, as needed.

***Features:***

- Speeds up system boot and Windows login process
- Removes unneeded programs in the startup list
- Allows to set programs to launch at startup
- Allows to acquire more available memory, such as RAM and other system resources

## *PDBEDIT*

- Link: samba.org
- To store contents of a TDB (Trivial Database).
- Manage the SAN database

## *PDF Password Cracker*

- See: **Password Cracker**
- Source: http://www.crackpdf.com
- PDF Password Cracker is a utility to remove the security on PDF documents.

## *PDF Password Genius*

- See: **Password Cracker**
- http://www.isunshare.com

## *PDF Password Recovery*

- See: **Password Cracker**
- http://www.top-password.com

## *PDS Excel Password Recovery*

- See: **Password Cracker**
- Source: http://www.excelpasswordcracker.com
- PDS Excel Password Recovery is used to crack password-protected documents created in MS Excel 97/2000/XP/2003/2007/2010 (*.xls, *.xlsx files).
- The application is a quick algorithm-based Excel Password Breaker.
- The program allows cracking “open,” “write,” “workbook,” “shared workbook,” and “worksheet” passwords.

## *PE Explorer*

- See: **Malware Analysis**

## *PEBrowse*

- See: **Malware Analysis**

## *PEiD*

- See: **Malware Analysis**
- Investigators can use tools like PEid to find if the file has packed programs or obfuscated code.
- This tool also displays the type of packers used in packing the program.

## *Pendrivelinux.com*

- See: **Linux on a USB Stick**

Get www.kali.org
Download Kali Linux

Get pendrivelinux Universal USB Installer (UUI) Installer
Start Universal USB Installer and select Kali Linux
Select the correct USB Drive
Set the Boot device in the BIOS as USB first

## *PEScan*

- See: **Malware Analysis**

## *PEView*

- See: **Malware Analysis**

## *Responder*

- See: **Penetration Testing**
- Active Online Attack
- LLMNR and NBT-NS are enabled by default in Windows and can be used to extract the password hashes from a user.
- Since the awareness of this attack is fairly low, there is a good chance of acquiring the user credentials on an internal network penetration test.
- By listening for LLMNR/NBT-NS broadcast requests, it is possible for an attacker to spoof itself as the server and send a response claiming to be the legitimate server.
- After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool like Responder.py.
- When a DNS name server request fails, Link-Local Multicast Name Resolution (LLMNR) and Net-BIOS Name Service (NBT-NS) is used by the windows systems as a fallback.
- If the DNS name still remains unresolved, the windows system performs an unauthenticated UDP broadcast to the whole network.
- Any masquerading machine, claiming to be the server then sends a response and captures the victim's credentials during the authentication process.

## *Phishtank*

- Source: www.phishtank.com
- Against Phishing

## *Phone Image Carver*

- See: **Forensics Mobile**
- Source: http://www.phoneimagecarver.com
- Phone Image Carver is an easy-to-use segment-by-segment data carver for mobile phone image files.
- Phone image carver currently supports Hex, DD, Bin, RAW, DMG, and XRY.
- Its design is helpful in a mobile forensic investigation.
- It does not search on sector boundaries, but analyzes the mobile image file sector-by-sector for select user file types.

## *PhotoRec*

- See: **File Recovery**
- http://www.cgsecurity.org

## *Pipl.com*

- See: **People search**
- Source:www.pipl.com
- Pipl is an information services company with the world's largest people search engine.
- The best place to find the real person behind the online identity.

***Pricing:***

| | |
|---|---|
| 200 searches per user/month | 99 USD |
| 500 searches per user/month | 199 USD |
| Unlimited searches user/month | 299 USD |

## *Plaso*

- Ehemals ***log2timeline***
- Das Tool dient dem Extrahieren von Timestamps verschiedener Files und zur Aggregierung dieser zu einer Timeline.
- Infos: github.com/log2timeline/plaso/wiki

## *PortMon*

- See: **Port Monitor**

## *PORTSENTRY*

- See: **Port Scanner**
- Source: Psionic

## *PowerSploit*

- See: **Penetration testing tool**
- PowerSploit is an offensive security framework for **penetration testers** and **reverse engineers**.
- It was born out of the realization that PowerShell was the ideal post-exploitation utility in Windows due to its ability to perform a wide range of administrative and low-level tasks all without the need to drop malicious executables to disk, thus, evading antivirus products with ease.

**Functions:**

- ❑ CodeExecution - Perform low-level code execution and code injection.
- ❑ ScriptModification - Modify and/or prepare scripts for execution on a compromised machine.
- ❑ Persistence - Add persistence capabilities to a PowerShell script.
- ❑ PETools - Parse/manipulate Windows portable executables.
- ❑ Capstone - A PowerShell binding for the Capstone Engine disassembly framework.
- ❑ ReverseEngineering - A wide range of reverse engineering tools
- ❑ AntivirusBypass - Defeat AV byte signatures in executables.
- ❑ Exfiltration - Steal sensitive data from a compromised machine.
- ❑ Mayhem - Perform destructive actions.
- ❑ Recon - Tools to aid in the reconnaissance phase of a penetration test

## *Power Spy*

- Web Activity Monitoring and Recording

## *PowerBroker Event Vault*

- See: **Forensics Network**
- Source: https://www.beyondtrust.com
- BeyondTrust PowerBroker Event Vault automates and streamlines the collection and management of standard Microsoft Windows event logs.

## *PowerPoint Password*

- See: **Password Cracker**
- Source: http://lastbit.com
- PowerPoint Password recovers lost or forgotten passwords to PowerPoint (*.ppt) files.
- It supports brute-force, dictionary, hybrid dictionary, and smartforce (TM) attacks.
- PowerPoint Password supports brute-force attack, dictionary attack, hybrid dictionary attack and SmartForce (TM) attack.
- The tool recovers simple passwords.

## *Privacy Eraser*

- Is an ***anti-forensic solution*** to protect the privacy of the user by deleting the browsing history and other computer activities.

- This tool supports multiple web browsers such as Internet Explorer, Microsoft Edge, Firefox, Google Chrome, Safari, and Opera.
- Privacy Eraser erases all digital footprints: web browser cache, cookies, browsing history, address bar history, typed URLs, autocomplete form history, saved passwords, index.dat files, Windows' run history, search history, open/save history, recent documents, temporary files, recycle bin, clipboard, DNS cache, log files, error reporting, etc.
- Privacy Eraser supports plugins to extend the software's cleaning features.
- It supports programs such as ACDSee, Adobe Reader, Microsoft Office, WinZip, WinRAR, Windows Media Player, VLC Player, BitTorrent, and Google Toolbar.
- It works with Windows 10/8.x/7/Vista/2012/2008 (32/64-bit), and also supports Windows FAT16/FAT32/exFAT/NTFS file systems.
- The software implements and exceeds the US Department of Defense and NSA clearing and sanitizing standards, giving you the confidence that once erased, your file data is gone forever and can never be recovered.

## *Proactive System Password*

- See: **Password Cracker**
- Recovery https://www.elcomsoft.com

## *Proc Heap Viewer*

- See: **Forensics**
- http://securityxploded.com

## *ProDiscover*

- See: **Forensics**
- Source: http://www.arcgroupny.com
- Data acquisition

## *Process Explorer*

- See: **Forensics**
- https://technet.microsoft.com
- Process Explorer shows information about which handles and DLLs processes have opened or loaded.
- The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

## *Process Hacker*

- See: **Windows Services Monitoring Tool**
- Source: http://processhacker.sourceforge.net
- Process Hacker is a multi-purpose tool that helps to monitor system resources, debug software, and detect malware.
- It is an open source alternative to programs such as Task Manager and Process Explorer.

***Features:***

- Provides a detailed overview of system activity with highlighting
- Offers graphs and statistics to track down resource hogs and runaway processes
- Allows discovery of which processes are using the file that cannot be edited or deleted
- Permits seeing what programs have active network connections, and close them if necessary
- Provides real-time information on disk access
- Allows viewing of detailed stack traces with kernel-mode, WOW64, and .NET support
- Permits going beyond services.msc: create, edit, and control services

## *Process Monitor*

- See: **Monitoring Tool**
- Source: Sysinternals
- procmon.exe

- Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.
- It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.
- Its uniquely powerful features will make ***Process Monitor*** a core utility in your ***system troubleshooting*** and ***malware hunting*** toolkit.

## *ProRat*

- See: **RAT**
- ProRat is a ***Remote Administration Tool*** written in C programming language and capable of working with all Windows operating systems.

## *PsTools*

- See: MS Sysinternals
- PsTools

***PsGetsid***

- PsGetsid allows you to translate SIDs to their display name and vice versa. It works on builtin accounts, domain accounts, and local accounts.

***PsKill***

- PsKill is part of a growing kit of Sysinternals command-line tools that aid in the adminstration of local and remote systems named PsTools

***PsLIST***

- PsList is part of a growing kit of Sysinternals command-line tools that aid in the adminstration of local and remote systems named PsTools.

## *Public VPN*

- Avira Phantom VPN
- CyberghostVPN
- ExpressVPN
- HideMyAss
- IPVANISH
- NordVPN
- Private Tunnel/OpenVPN
- PrivateVPN
- PureVPN
- TorGuard
- VikingVPN

## *Project-A-Phone*

- See: **Forensics**
- Source: http://www.project-a-phone.com
- Data acquisition

## *PST Outlook Repair*

- See: **E-Mail Forensics**
- Source: http://www.pstoutlookrepair.com
- Outlook PST stores the Outlook files and maintains the Outlook data till the space does not gets consumed or the MS Outlook itself does not encounter some technical glitches.

## *PVS-Studio*

- See: **Vulnerability Scanner Code**
- Source: https://www.viva64.com/en/pvs-studio/

- PVS-Studio is a tool for detecting bugs and security weaknesses in the source code of programs, written in **C, C++, C#** and **Java**.
- It works under 64-bit systems in Windows, Linux and macOS environments, and can analyze source code intended for 32-bit, 64-bit and embedded ARM platforms.

## *PWDUMP / PWDUMP7*

- See: **Password cracker**
- Source: https://www.openwall.com/passwords/windows-pwdump
- Outputs the LM and NTLM password hashes
- Can be used to dump protected files.
- You can always copy a used file by executing:

```
pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat.
```

## *Pyrit*

- See: **WiFi Password Cracking**

***Example:***

```
Pyrit -r <x.cap> analyze
Pyrit -r <x.cap> -o <x.cap> strip
```

## *Qualys*

- See: **Vulnerability Scanner**
- Link: https://www.qualys.com
- Automatically identify all known and unknown assets on your global hybrid-IT—on prem, endpoints, clouds, containers, mobile, OT and IoT—for a complete, categorized inventory, enriched with details such as vendor lifecycle information and much more.

## *Queso*

- See: **Reconnaissance**
- OS guessing

## *QuickCrypto*

- See: **Encryption**
- Link: http://quickcrypto.com
- Is advanced Windows-based ***privacy*** and ***encryption software***.
- It is a program that will hide and encrypt files, emails, and passwords. It uses the most powerful algorithms and techniques to ensure your email communication, passwords, all confidential files, and information are kept completely secure.

**Features**

- Secure Volume & File Encryption
- Powerful Easy Email Encryption
- Multi-Use Password Manager
- Secure File Shredder

## *Quick Recovery*

- See: **File Recovery**
- http://www.recoveryourdata.com

## *Quick Recovery for Linux*

- See: **Partition Recovery (Linux)**
- http://www.recoveryourdata.com

## *Quick Stego*

- Image Steganography

### *R-Drive Image*

- See: **Forensics**
- Source: http://www.drive-image.com
- R-Drive Image is a potent utility that provides ***creation of disk image files for backup or duplication purposes***.
- R-Drive Image restores the images on the original disks, on any other partitions, or even on a hard drive's free space.
- Using R-Drive Image, one can restore the system after heavy data loss caused by an operating system crash, virus attack, or hardware failure.

***Features:***

- ❑ A simple wizard interface
- ❑ Image file compression
- ❑ Removable media support
- ❑ Image files splitting
- ❑ Image Protection

### *R-Mail*

- Link: rmail.com
- To recover deleted e-mails.

### *R-Studio for Mac*

- See: **File Recovery (MAC)**
- http://www.r-tt.com

### *R-Tools / R-Studio*

- See: **Forensics & File Recovery**
- Source: http://www.r-studio.com
- http://www.data-recovery-software.net
- Data acquisition

### *R-Undelete*

- See: **File Recovery**
- http://www.r-undelete.com

### *RAID Recovery for Windows*

- See: **Forensics**
- Source: https://www.runtime.org
- Data acquisition

### *RainbowCrack*

- See: **Password Cracker**
- Source: Kali Linux
  project-rainbowcrack.com
- CLI
- Hash cracker tool
- There are LM, NTLM, ***MD5*** and ***SHA-1*** rainbow tables available

### *RAM Capturer*

- Source: https://belkasoft.com
- Investigators can find out the information about the sessions of a Dropbox client from the RAM analysis.
- For this, the investigator can run RAM Capturer tool to dump the RAM contents, and then use a hex editor tool to analyze the captured RAM contents.

- RAM Capturer allows investigator to reliably extract the entire contents of computer's volatile memory to the required drive - even if protected by an active anti-debugging or anti-dumping system.
- The tool allows investigators with the ability to take snapshots of the computer's volatile memory (memory dumps) even if an anti-dumping protection is active for the drive.

### *RAPID IMAGE 7020 X2 IT*

- See: **Forensics**
- Source: http://ics-iq.com
- Data acquisition

### *RAR Password Genius*

- See: **Password Cracker**
- http://www.isunshare.com

### *RAT - Router Audit Tool*

- See: **Network Auditing**
- Source: http://ncat.sourceforge.net/

### *Recon-ng*

- See: **Reconnaissance**
- OS: Linux
- Recon-ng is a ***reconnaissance tool*** with an interface like Metasploit.
- Running recon-ng from the ***command line*** you enter a shell-like environment where you can configure options, perform recon and output results to different report types.
- The interactive console provides several helpful features such as command completion and contextual help.

### *Recover4all Professional*

- See: **File Recovery**
- http://www.recover4all.com

### *Recovery Toolbox for Outlook*

- See: **E-Mail Forensics**
- Source: https://outlook.recoverytoolbox.com
- Recovery Toolbox for Outlook helps to restore emails, attachments, contacts and other from damaged .PST or .OST file. PST repair software helps to fix errors detected in Outlook.

### *Recover My Files*

- See: **Forensics**
- Source: http://www.recovermyfiles.com
- Recover My Files data recovery software will recover deleted files emptied from the Windows Recycle Bin, or lost because of the format or corruption of a hard drive, virus or Trojan infection, and unexpected system shutdown or software failure.

***Features:***

- Recover files even if they are emptied from the Recycle Bin.
- Recover files after accidental format, even if you have reinstalled Windows.
- Recover disks after a hard disk crash.
- Get back files after a partitioning error.
- Get data back from RAW hard drives.
- Recover documents, photos, video, music, and email.
- Recover from a hard drive, camera card, USB, Zip, floppy disk, iPod, and other media.

### *RECUVA*

- See: **Forensics**

- Source: https://www.piriform.com
- Recuva can ***recover lost pictures, music, documents, videos, emails or any other file type*** and it can also recover data from any rewriteable media like memory cards, external hard drives, USB sticks, etc.

## *Redsn0w*

- See: **iOS Jailbreaking Tools**
- Source: http://www.redsn0w.us
- RedSn0w allows the investigator to jailbreak into an iPhone, iPod Touch, or iPad by running a variety of firmware versions.
- Maintained and created by the Dev-Team, RedSn0w has become one of the most used jail-breaking tools to jailbreak iOS firmware.

## *Reg Organizer*

- See: **Monitoring Registry**
- Source: http://www.chemtable.com/organizer.htm
- Reg Organizer is a set of tools to tweak, optimize, and clean Windows, designed to free up system resources and rev performance to the max.
- The set includes a visual autostart manager, an advanced uninstaller featuring search for leftovers of the uninstalled programs in the system, functions to purge unnecessary data, a powerful registry editor to quickly search and replace keys and data quickly, and much more - all to keep your system healthy.

## *Regedit*

- To check out password file of the user in "HKEY_LOCAL_MACHINE"

**Navigate to:**
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon."
Look at the "DefaultPassword" line to view the password.

## *Registry Cleaner*

- See: **Monitoring Registry**
- Is part of the jv16 PowerTools, which detects errors and unneeded that can have a measurable adverse effect on general system performance.

## *Registry Viewer*

- See: **Forensics / Monitoring Registry**
- http://accessdata.com
- Source: http://www.gaijin.at/en/dlregview.php
- Registry Viewer allows you to view the contents of Windows® operating system registries.
- Registry Viewer lets you view registry files from any computer.
- Registry Viewer gives you access to a registry's protected storage.
- The protected storage can contain passwords, usernames, and other information that is not accessible in Windows Registry Editor.

## *RegScanner*

- See: **Forensics / Monitoring Registry**
- Source:http://www.nirsoft.net
- Is a utility that allows you to scan the Registry, find the desired Registry values that match the specified search criteria, and display them in one list.
- After finding the Registry values, you can jump to the right value in RegEdit by double-clicking the desired Registry item.
- You can also export the found Registry values into a .reg file that can be used in RegEdit.

***Advantages over RegEdit find of Windows***

- RegScanner allows you to make a case sensitive search

- While scanning the Registry, RegScanner displays the current scanned Registry key, as opposed to RegEdit, that simply display a boring "Searching the registry" dialog-box
- Standard string search (Like in RegEdit), RegScanner can also find Registry values by data length, value type (REG_SZ, REG_DWORD, and so on), and by modified date of the key
- RegScanner can find a unicode string

## *Regshot*

- See: **Monitoring Registry**
- Source: https://sourceforge.net
- Regshot is a registry compare utility which helps to compare the changes in registry entries after installing/uninstalling a program or modifying the registry manually.
- The purpose of this utility is to compare your registry at two separate points by taking a snapshot of the registry before and one after any program/settings are added/removed or modified.
- Regshot is an open-source (LGPL) registry compare utility that allows you to take a snapshot of your registry quickly and then compare it with a second one - done after doing system changes or installing a new software product.

***Tip***

- Use the <***Regshot-x64-Unicode.exe***> for multilanguage systems.

## *Remo Recover (Mac) - Pro*

- See: Partition Recovery
- http://www.remosoftware.com/

## *Repair PST - Outlook PST Recovery*

- See: **E-Mail Forensics**
- Source: http://www.emailrecovery.in
- Repair PSTis an Outlook PST Recovery Software to recover emails from corrupt PST files of Microsoft Outlook.
- It successfully recovers emails from Outlook PST with tasks, contacts, calendar, journal, notes and attachments.

## *RescuRoot*

- See: **Android Rooting Tools**
- Source: http://rescueroot.com
- It is a one click utility to root most of the Android mobile devices from the brands Samsung, HTC, Motorola, LG, and Sony Ericsson.

***Features are:***

- Simple to use
- Supports almost every android device
- Provides data Backup and Restore functionality
- Enhanced support

## *RIPS*

- See: **Vulnerability Scanner Code**
- Link: https://www.ripstech.com
- Static application security testing.

## *ROADMASSTER-3 X2*

- See: **Forensics**
- Source:http://ics-iq.com
- Data acquisition

### *RUDY - R-U-Dead-Yet*

- ***DoS*** Tool to attack a web server.

### *RS Partition Recovery*

- See: **Partition Recovery**
- http://recoverhdd.com

### *RSYSLOG*

- See: **Forensics Network**
- Source: http://www.rsyslog.com
- RSYSLOG is a system for log processing.
- It offers security features and a modular design.
- It accepts inputs from a variety of sources, transforms them, and outputs the results to diverse destinations.

### *rtgen*

- See: **Password Cracker**
- Source: http://project-rainbowcrack.com
- RainbowCrack is a general purpose implementation tool that takes advantage of the time-memory trade-off technique to crack hashes.
- This project allows you to crack a hashed password.
- The rtgen tool of this project helps to generate the rainbow tables.
- The rtgen program needs several parameters to generate a rainbow table.

### *S.M.A.R.T.*

- See: **Forensics**
- Self-Monitoring, Analysis and Reporting Technology.
- Forensic tool suite for Linux.
- Especially f or Harddisk forensics.

### *SafeBack*

- See: **Forensics**
- Data acquisition (Tape)

### *Sam Spade*

- See: **DNS footprinting tool**
- A Windows software tool designed to assist in tracking down sources of e-mail spam.

***Main Features:***

- Zone Transfer - ask a DNS server for all it knows about a domain
- SMTP Relay Check - check whether a mail server allows third party relaying
- Scan Addresses - scan a range of IP addresses looking for open ports
- Crawl website - search a website, looking for email addresses, offsite links, etc.
- Browse web - browse the web in a raw http format
- Check cancels - search your news server for cancel messages
- Fast and Slow Traceroute - find the route packets take between you and a remote system
- S-Lang command - issue a scripting command; useful for debugging scripts
- Decode URL - decipher an obfuscated URL
- Parse email headers - read email headers and make a guess about the origin of the email

### *SaaS Log Management*

- See: **Forensics Network**
- Source: http://www.cloudaccess.com
- SaaS Log Management is a solution that works with CloudAccess SIEM Log management to provide secure storage and full lifecycle management of event data.

### *SATAN - Security Administrator Tool for Analyzing Networks*

- See: **Vulnerability Scanner**
- Link: http://www.porcupine.org/satan
- Tool to automatically detect vulnerabilities.

### *Sawmill*

- See: **Forensics Network**
- Source: https://www.sawmill.net
- Sawmills helps analyze, monitor, and alert a wide range of systems.
- It provides log processing and reporting features to gain insight into the network data.

### *SCANLOGD*

- See: **Reconnaissance**
-
- Source: openwall.com
- Port scan detection tool

### *ScanNT Plus*

- Source: http://www.ntsecurity.com/

### *Scapy*

- See: **Packet Crafting**
- Primarly developed for ***Unix based systems***.
- Scapy is a powerful interactive packet manipulation tool, ***packet generator***, ***network scanner***, ***network discovery tool***, and ***packet sniffer***.

### *Seagate File Recovery Software*

- See: **File Recovery**
- http://www.seagate.com

### *Secure4U*

- Ist ein Tool gegen die Gefahren von schädlichen ActiveX- und Java-Applets, Trojanischen Pferden und Viren. Herkömmliche Firewalls oder Antiviren-Software sind bei Angriffen von unbekanntem ausführbarem Code, d.h. von Daten mit aktivem Web-Inhalt, wirkungslos.
- Hier setzt Secure4U von Sandbox Security AG ein. Die Software des 1999 in München gegründeten Start-up-Unternehmens arbeitet mit der Sandbox-Technologie: Anstatt Daten zu blockieren oder nach bekannten Code-Mustern zu suchen, baut Secure4U um jeden ausführbaren Code eine geschlossene Umgebung (Sandbox) auf. Aktiv wird der Code nur in dieser Umgebung, auf bestehende Applikationen und Daten kann er nicht zugreifen.

### *Secure IT*

- See: **Anti Forensics Tool**
- http://www.cypherix.com

### *SecureView*

- See: **iPhone Data Acquisition Tools**
- Source: http://mobileforensics.susteen.com
- Secure View is a forensic data recovery tool.
- It also helps with forensic investigations and forensic analysis.

### *Securing Windows NT Installation*

http://www.microsoft.com/ntserver/guide/secure_ntinstall.asp?A=2&B=10

### *Security Onion*

- Source:https://securityonion.net/
- Is a free and open source Linux distribution for ***intrusion detection***, ***enterprise security monitoring***, and ***log management***.
- It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools.
- The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

### *Security Task Manager*

- See: **Forensics**
- http://www.neuber.com
- Security Task Manager shows comprehensible information about programs and processes running on the computer.

For each Windows process, it improves on Windows Task Manager, providing:

- unique security risk rating
- full directory path and file name
- process description
- CPU usage graph
- embedded hidden functions (e.g., keyboard monitoring, browser supervision, or manipulation)
- process type (e.g., visible window, systray program, DLL, IE-plugin, startup service)

### *SecurityCenter CV*

- See: **Forensics Network**
- Source: https://www.tenable.com
- SecurityCenter Continuous View (SecurityCenter CV) collects data from multiple sensors to provide advanced analysis of vulnerability, threat, network traffic, and event information and delivers a continuous view of IT security across the environment.

### *ServiWin*

- See: **Device Drivers Monitoring Tool**
- See: Windows Services Monitoring Tool
- Source: http://www.nirsoft.net
- ServiWin utility displays the list of installed drivers and services on the system.
- For some of them, it shows additional useful information: file description, version, product name, company that created the driver file, and so on.
- In addition, ServiWin allows one to stop, start, restart, pause, and continue service or driver, change the startup type of service or driver (automatic, manual, disabled, boot or system), save the list of services and drivers to file, or view HTML report of installed services/drivers in the default browser.

### *Sentinel Log Manager*

- See: **Forensics Network**
- Source: https://www.netiq.com
- SentinelTM Log Manager is a software appliance that enables the collection, storage, analysis, and management of IT infrastructure event and security logs.

### *SET - Social Engineering Toolkit*

- See: **Penetration Testing**
- The Social Engineering Toolkit is an open-source Python-driven tool aimed at penetration testing.
- The SET is specifically designed to perform advanced attacks against human by exploiting human behavior.
- The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

## *Sfind*

- See: **Reconnaissance**
- Searching for ADS.

## *SHA1SUM*

- To check the hash value.

## *Shadow 3*

- See: **Forensics**
- Source: http://www.voomtech.com
- It helps to ***view suspect computers at the scene of the investigation in real time*** without prior need to image hard drives and without the need for clumsy virtual viewing software.
- All without corrupting the evidence.

## *Shodan*

- See: **Reconnaissance**
- Source: https://www.shodan.io
- Price: Freelancer 59$/Mth, Small Business 299$/Mth, Corporate 899$
- Shodan is the world's first search engine for ***Internet-connected devices (IoT)***.

***Search Words:***
IPCamera_Logo, router, switch, webcam, scada systems, power plants, netgear

webcam city:"Zuerich"
webcam country:"CH"

shodan count vuln:cve-2019-0708
shodan stats vuln:cve-2019-0708
shodan count net:x.x.x.x/24

org:"UPC Schweiz"

os:"Linux"
os:"windows xp"

port:21 → FTP
port:"23" → Telnet
port:"554" → CCTV
port:"3389" → Remote Desktop (MSTSC)

product:"xxx"

## *SID2USER*

- See: **Enumeration tool**

## *sift - SANS Investigative Forensic toolkit*

- See: **Forensics**
- Ist eine IT-Forensik-Tool-Sammlung, die entweder als VMware-Appliance gestartet oder auf der GNU/Linux-Distribution Ubuntu 16.04 ausgeführt werden kann.
- Die Werkzeugkiste wird unter anderem in den vom Sans-Institute angebotenen Kursen zur Incidence Response und IT-Forensik verwendet.
- Sift unterstützt hauptsächlich für forensische Untersuchungen verwendete Beweismittelformate (Evidence Format) wie das Expert Witness Format (E01), Advanced Forensic Format (AFF) und RAW (dd).
- Infos: digital-forensics.sans.org

## *SIGVERIF.EXE*

- See: **Analyze drivers**
- It checks integrity of critical files that have been digitally signed by Microsoft.

## *SIM Brush*

- See: **Forensics Mobile**
- Source: https://code.google.com
- It is an open-source implementation of (U) SIM investigation and (forensic) analysis and offers the following

***Features:***

- Recovery of call-list information
- Recovery of text message information
- Preparation of detailed report in HTML format

## *SIMiFOR*

- See: **Forensics Mobile**
- Source: http://www.forensicts.co.uk
- SIMiFOR tool helps in acquiring, analyzing, and reporting the data.
- It also helps in recovering the deleted data from the mobile.

## *Sleuth Kit*

- See: **Forensics**
- Source: http://www.sleuthkit.org
- The Sleuth Kit® is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them.
- It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

```
fsstat -f ntfs "<file>"

istat -f ntfs "<file>" 0
istat -f ntfs "<file>" 1
istat -f ntfs "<file>" 2
istat -f ntfs "<file>" 3
istat -f ntfs "<file>" 4
istat -f ntfs "<file>" 6
istat -f ntfs "<file>" 7
istat -f ntfs "<file>" 8
istat -f ntfs "<file>" 9

fls -f ntfs "<file>"
fls -d ntfs "<file>"

img_stat "<file>"
```

## *SMAC*

- See: **Penetration Testing**
- MAC duplicating or spoofing attack involves sniffing a network for MAC addresses of legitimate clients connected to the network.
- In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port.
- Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client.
- Once the spoofing is successful, the attacker can receive all traffic destined for the client.
- Thus, an attacker can gain access to the network and take over the identity of a network user.
- If an administrator does not have the working packet-sniffing skills, it is hard to defend intrusions.
- So, as an Expert Ethical Hacker and Penetration Tester, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning.

### *SmartKey Password Recovery Bundle Standard*

- See: **Password Cracker**
- Source: http://www.recoverlostpassword.com
- SmartKey Password recovery bundle Standard is multi-functional password recovery software.
- It recovers passwords for Windows Excel, Word, Access, PowerPoint, Outlook, Outlook Express, PDF, RAR/WinRAR, ZIP/WinZIP, MSN, AOL, Google Talk, Paltalk, Trillian, Miranda, Opera, Firefox, IE Browser, etc.

### *Smart Undeleter*

- See: **File Recovery**
- http://www.recoverdeletedfilestool.com

### *SmartSniff*

- See: **Forensics Network**
- Source: http://www.nirsoft.net
- SmartSniff is a network monitoring utility that captures TCP/IP packets that pass through the network adapter and displays the captured data as a sequence of conversations between clients and servers.
- The tool allows viewing the TCP/IP conversations in Ascii or as hex dump.

### *SmartWhois*

- See: **Web Attack Investigation / Whois Desktop Tool**
- Source: http://www.tamos.com
- Price: 35 EUR (1 License)
- SmartWhois is a network information utility that allows you to look up all the available information about an IP address, hostname or domain, name of the network provider, administrator and technical support contact information.
- It supports Internationalized Domain Names (IDNs) and also fully supports IPv6 addresses.

***Features:***

- It saves results into an archive.
- Allows batch processing of IP addresses or domain lists.
- Enables caching of obtained results, hostname resolution, and DNS.
- It provides the customizable interface.

### *Sn0wbreeze*

- See: **iOS Jailbreaking Tools**
- Source: www.ih8sn0w.com
- Sn0wbreeze is a jailbreak application developed by iH8sn0w for Apple devices running on iOS such as iPhone, iPad, and iPod Touch.

### *SnapBack*

- See: **Forensics**
- Data acquisition (Tape)

### *Snare*

- See: **Forensics Network**
- Source: https://www.intersectalliance.com
- Snare helps in gathering and filtering IT-event data for critical security monitoring, analysis, auditing, and archiving.

### *Sniffer*

http://www.packet-sniffer.co.uk/
http://www.axial.co.uk/sniffer/sniff.html
http://www.tlic.com/analysis/snifferethernet.htm Demo Licence key: TLICWORLDWID4

http://www.enertec.com/

Sniffer sind Vorrichtungen die Prozesse überwachen können. Ein Sniffer ist eine Vorrichtung - Hardware oder Software-, die jedes Paket lesen kann, das über das Netzwerk versandt wird. Sniffer können ein erhebliches Sicherheitsrisiko darstellen.
Sniffer bestehen immer aus einer Kombination von Hardware und Software.

Legitimer Zweck:
- Analyse von Netzwerkverkehr und die Identifizierung von potentiellen Gefahrenbereichen.
- Administrationstools

Das Netzwerk-Interface wird mittels dem Sniffer in den "**Promiscuous Mode**" gesetzt.

- Sniffer können Passwörter abfangen.
- Sniffer können vertrauliche oder proprietäre Informationen abfangen.
- Sniffer können dazu benutzt werden, Sicherheitsmassnahmen angrenzender Netzwerke zu durchbrechen oder Einflussnehmenden Zugang zu erhalten.
- Sniffer können Daten nur auf dem augenblicklichen Netzwerksegment abfangen.
- Es gibt drei Netzwerk-Interfaces die ein Sniffer nicht überqueren kann:
  Switches, Router, Bridges

***Abwehr:***
- Daten gegen Sniffer schützen, Sniffer aufdecken und beseitigen.
  Programme: ***Snifftest***, ***Nitwit***, ***Promise***, ***cpm***
- Eine sichere Netzwerktopologie
- Verschlüsselte Arbeitssitzungen

***Kommerzielle Sniffer***
- ATM Sniffer Network Analyzer von Network Ass. http://www.networkassociates.com
- NAI Sniffer Pro LAN http://www.comsoft.ch price: CHF 17990.--
- Shomiti System Century LAN Analyzer http://www.shomiti.net
- PacketView von Klos Technologies http://www.klos.com ftp://ftp.clos.com/demo/pvdemo.zip
- Network Probe 8000 http://www.netcommcorp.com
- LanWatch http://www.guesswork.com
- EtherPeek ricki@aggroup.com
- NetMinder Ethernet http://wwwneon.com
- Dataglance Network Analyzer von IBM http://www.redbooks.ibm.com/GX288002/x800206.htm
- LinkView Internet Monitor http://www.wg.com
- ProConvert http://www.net3group.com
- LANdecoder32 (W95) http://www.triticom.com
- NetXRay Analyzer (WNT) http://cinco.com oder http://www.cinco.com
- NetAnt Protocol Analyzer (W95) http://www.people-network.com
- NeoTrace 2.0 Christophe!

***Kostenlose Sniffer***
- sniffit (Unix)
- Ethereal http://ethereal.zing.org
- Esniff (Unix)
- Gobbler (W95) ftp://ftp.tordata.se/www/hokum/gobbler.zip
- ETHLOAD http://www.computercraft.com/noprogs/ethld104.zip
- Netman http://www.ndg.com.au
- LinSniff (Linux)
- Sunsniff (Sunos)
- linux_sniffer.c

***Atm Sniffer Network Analyzer von Network Associates***
Network Associates, Inc.
Tel. +1 408 988 3832
http://www.networkassociates.com/

***Shomiti System Century LAN Analyzer***
http://www.shomiti.com/
***DatagLANce Network Analyzer von IBM***
http://www.redbooks.ibm.com/GX288002/x800206.htm

***EtherPeek***

***LANWatch***
http://www.guesswork.com/

***LANdecoder32***
http://www.triticom.com/

***LinSniff***
http://www.rootshell.com/archive-1d8dks1x1xja/199804/linsniff.c

***LinkView Internet Monitor***
http://www.wg.com/

***NetAnt Protocol Analyzer***
Windows 95
http://www.people-network.com/

## sniffit

http://sniffit.rug.ac.be/sniffit/sniffit.html.

***NetWitness***
***Network Probe 8000***
http://www.netcommcorp.com/

***NetMinder Ethernet***
http://www.neon.com

***NetXRay Analyzer***
http://www.cinco.com/

***ProConvert***
http://www.net3group.com/

***Ethereal***
http://ethereal.zing.org/.

***Esniff***
http://www.asmodeus.com/archive/IP_toolz/ESNIFF.C
http://www.rootshell.com/archive-1d8dks1x1xja/199707/Esniff.c
http://www.chaostic.com/filez/exploites/Esniff.c

## Gobbler (Tirza von Rijn)

- Windows 95
- DoS Attack
- Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope.

ftp://ftp.tordata.se/www/hokum/gobbler.zip

***ETHLOAD***

http://www.computercraft.com/noprogs/eth1d104.zip

## Netman (Schulze, Benko und Farrell)

http://www.ndg.com.au/

***PacketView von Klos Technologies***

ftp://ftp.klos.com/demo/pvdemo.zip.
http://www.klos.com/

***Sunsniff***

http://www.7thsphere.com/hpvac/files/hacking/sunsniff.c
http://www.zerawarez.com/main/files/csource/sunsniff.c
http://www.jabukie.com/Unix_Sourcez/sunsniff.c

## linux_sniffer.c

http://www.rootshell.com/archive-1d8dks1x1xja/199707/linux_sniffer.c
http://www.society-of-shadows.com/security/linux_sniffer.c
http://www.asmodeus.com/archive/linux/linsniffer.c

***Snifftest***

http://www.unitedcouncil.org/c/snifftest.c

## Nitwit.

http://www.7thsphere.com/hpvac/files/hacking/nitwit.c

## Promisc.

http://geek-girl.com/bugtraq/1997_3/0411.html.

## cpm.

ftp://info.cert.org/pub/tools/cpm/cpm.1.2.tar.gz.

## *Snow*

- Simple Steganography Tool

## *SnowBatch*

- See: **Forensics**
- Source: http://www.snowbound.com
- SnowBatch® is a Windows-based ***image conversion and file conversion application*** that converts large batches of image or document files from one format to another.

## *Snyk*

- See: **Vulnerability Scanner Code**
- Open source
- Unique combination of developer-first tooling and best in class security depth enables businesses to easily build security into their continuous development process.

## *Sguil*

- See: **Forensics Network**
- Link: https://bammv.github.io/sguil/index.html
- Sguil (pronounced sgweel or squeal) is a collection of free software components for Network Security Monitoring (NSM) and event driven analysis of IDS alerts.

- The sguil client is written in Tcl/Tk and can be run on any operating system that supports these.
- Sguil integrates alert data from ***Snort***, session data from SANCP, and full content data from a second instance of Snort running in packet logger mode.
- Sguil is an implementation of a Network Security Monitoring system.
- NSM is defined as "collection, analysis, and escalation of indications and warnings to detect and respond to intrusions."
- What makes this particularly interesting is that this is basically a suite of tools which one can use as the foundation of an organization's Security Operations Center (SOC).
- Sguil is released under the GPL 3.0.

*Source Wikipedia*

### *SIM Card Data Recovery*

- See: **Forensics Mobile**
- Source: http://www.datadoctor.in
- It recovers lost or deleted text messages and contact numbers from a mobile phone SIM card.

### *SIM Explorer*

- See: **Forensics Mobile**
- Source: http://www.dekart.com
- SIM Explorer is a SIM card forensic tool designed to find, view, and edit files on GSM SIM, 3G USIM or CDMA R-UIM cards.
- SIM Explorer targets mobile operators, content providers, detectives, developers, reverse engineers, and others who need flexible access to the structure of a SIM card.

### *SIM Query*

- See: **Forensics Mobile**
- Source: http://vidstrom.net
- SIMQuery is a tool that retrieves the ICCID and IMSI from a GSM SIM card and also retrieves the user information provided during the purchase of the mobile phone along with the SIM card owner details.

### *SIMIS 2.0*

- See: **Forensics Mobile**
- Source: http://www.crownhillmobile.com
- SIMIS is capable of forensically extracting data from a SIM card and providing that data in an easy to read HTML report.
- SIMIS 2 is mainly targeted for forensic interrogation of Phase 2 GSM SIM Cards, now commonly referred to as 2G.

### *SIMIS 3G*

- See: **Forensics Mobile**
- Source: http://www.crownhillmobile.com
- SIMIS 3G provides the examiner with broadly similar features and facilities to SIMIS 2; however, the 3G SIM holds a vast amount of user and network information.
- SIMIS 3G is a comprehensive tool for recovery and clear, precise presentation of the data.
- SIMIS 3G presents the recovered data in its original language and in an easily browseable format.

### *Simple Event Correlator (SEC)*

- See: **Forensics Network**
- Source: https://simple-evcorr.github.io
- SEC is an event correlation tool for event processing, which can be harnessed for event log monitoring, network and security management, fraud detection, and any other task that involves event correlation.

### *SIMulate*

- See: **Forensics Mobile**
- Source: http://www.crownhillmobile.com
- SIMulate Mobile provides the features of SIMulate2G and SIMulate3G on a mobile platform, allowing the examiner to generate a duplicate of the 2G or 3G card within or outside the lab environment.
- It is ideal for scene of crime work or intelligence.

### *SIMXtractor*

- See: **Forensics Mobile**
- Source: http://www.cyberforensics.in
- SIMXtractor 2.0 is a forensic tool used for imaging and analyzing SIM cards.
- SIMXtractor suite contains a SIM Card Reader, SIM Imager (Imaging of SIM cards), and SIM Analyzer (Analysis of SIM cards), which can be used to take an image of the SIM and read and analyze the data contained in it.

### *Slowloris*

- See: **DoS Attack**
- Script
- The ***Slowloris*** script opens two connections to the server, each without the final CRLF.
- After 10 seconds, second connection sends additional header.
- Both connections then wait for server timeout.
- If second connection gets a timeout 10 or more seconds after the first one, we can conclude that sending additional header prolonged its timeout and that the server is vulnerable to Slowloris DoS attack.

### *SMART for Linux*

- See: **Forensics**
- Source:http://www.asrdata.com
- Data acquisition

### *SmartKey PowerPoint Password Recovery*

- See: **Password Cracker**
- Source: http://www.recoverlostpassword.com
- PowerPoint Password Recovery tool is designed to recover lost or forgotten MS PowerPoint presentation passwords.
- It uses three different searching methods: advanced dictionary attack, brute-force attack, and advanced brute-force with mask attack.

### *SmartKey ZIP Password*

- See: **Password Cracker**
- Recovery http://www.recoverlostpassword.com

### *SmashGuard*

- ***Hardware Solution***
- A buffer overflow attack is perhaps the most common attack used to compromise the security of a host.
- This attack can be used to change the function return address and redirect execution to the attacker's code.
- We present a hardware-based solution, called SmashGuard, to protect against all known forms of attack on the function return addresses stored on the program stack.
- With each function call instruction, the current return address is pushed onto a hardware stack.
- A return instruction compares its address to the return address from the top of the hardware stack.
- An exception is raised to signal the mismatch.

- Because the stack operations and checks are done in hardware in parallel with the usual execution of instructions, our best-performing implementation scheme has virtually no performance overhead (because we are modifying hardware, it is impossible to guarantee zero overhead without an actual hardware implementation).
- While previous software-based approaches' average performance degradation for the SPEC2000 benchmarks is only 2.8 percent, their worst-case degradation is up to 8.3 percent.
- Apart from the lack of robustness in performance, the software approaches' key disadvantages are less security coverage and the need for recompilation of applications.
- SmashGuard, on the other hand, is secure and does not require recompilation of applications

## *snmp_enum*

- See: **Enumeration**
- ***SNMP enumeration*** is the process of enumerating the users' accounts and devices on a SNMP enabled computer.
- SNMP service comes with two passwords, which are used to configure and access the SNMP agent from the management station.
- They are: Read community string and Read/Write community string.
- These strings (passwords) come with a default value, which is same for all the systems.
- Hence, they become easy entry points for attackers if left unchanged by the administrator.
- Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc., and network information such as ARP tables, routing tables, device specific information, and traffic statistics.

## *SNMPUtil*

- See: **Enumeration**
- SNMP Enumeration

## *SNMPWALK*

- SNMPWALK is a Simple Network Management Protocol (SNMP) application present on the Security Management System (SMS) CLI that uses SNMP GETNEXT requests to query a network device for information.
- An object identifier (OID) may be given on the command line. This OID specifies which portion of the object identifier space will be searched using GETNEXT requests.
- All variables in the subtree below the given OID are queried and their values presented to the user.

## *SNORT*

- See: **IDS**
- Source:https://www.snort.org/downloads
- Signature-based ***IDS***.
- Snort is a ***security application*** that serves as a packet sniffer, packet logger and ***NDIS***.
- Snort can ***alert*** and ***log*** matching events.
- Integrated in the ***Cisco ASA***
- Can be used in conjunction with:
  Basic Analysis and Security Engine (BASE, Web Frontend)
  sguil
  OSSIM
- Limit the packets captured to the snort configuration file!

***snort modes:***

- Sniffer
- Packet Logger
- Network Intrusion Detection System

***Install on Kali Linux***

```
apt update
apt install snort
```

***EXAMPLES***

```
snort -dev -I eth 0            → Display ARP packets
snort -dev -l ./log            → Run snort in packet logger mode
snort -v -i eth 0
```

### *Snadboys*

- Mit Stern (*, Asterisk) verdeckte Passwörter werden damit angezeigt.

### *SNScan*

- See **SNMP**
- SNMP Enumeration

### *Sobolsoft*

- See: **WHOIS Online Tool**
- Source: http://www.sobolsoft.com
- Sobolsoft is an online whois lookup tool.

### *SoftFuse Whois*

- See: **WHOIS Desktop Tool**
- Source: http://www.softfuse.com
- SoftFuse Whois is a desktop domain lookup utility.
- It does a lookup search for a domain and presents you with all available information, such as administrative, technical or billing contacts, domain location, hosting provider, creation, and expiration date.

### *SoftPerfect Network Scanner*

- See: **Penetration Testing**
- Network enumeration
- To be an Expert Ethical Hacker and Penetration Tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked.
- A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.
- Resolve host names and auto-detect your local and external IP range.
- Enumeration involves an active connection so that they can be logged.
- Typical information that attackers look for includes user account names for future password guessing attacks.

### *Solarwinds IP Network Browser*

- See: **SNMP**
- SNMP Enumeration

### *Somarsoft DumpSec*

- Source:http://www.somarsoft.com/
- SomarSoft's DumpSec is a security auditing program for Microsoft Windows® NT/XP/200x.
- It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent.
- DumpSec also dumps user, group and replication information.

### *Somarsoft DumpEvt*

- Source:http://www.somarsoft.com/

### *Somarsoft DumpReg*

- Source:http://www.somarsoft.com/

### *Somarsoft RegEdit*

- Source: http://www.somarsoft.com/

### *Sparta*

- See: **Brute Force Attack**
- Source: Kali Linux

### *SpiderFoot*

- Free open source domain footprinting tool.

### *Splunk Enterprise*

- See: **Forensics Network / Web Attack Investigation**
- Source: http://www.splunk.com
- Splunk Enterprise allows investigators to collect, analyze, and act upon the untapped value of the big data generated by the technology infrastructure, security systems, and business applications—giving them insights to drive operational performance and business results.

### *Spytech SpyAgent*

- System Monitoring and Surveillance

### *sqlmap*

- See: **Penetration Testing**
- Zum Finden und Ausnutzen von SQL-Injection-Lücken.
- Ist zudem in der Lage, neben der Datenbank auch das zugrunde liegende Betriebssystem zu infiltrieren.
- Unterstützt MySQL, Oracle, PostgreSQL und Microsoft SQL Server;
- Achtung: einige der beiliegenden Exploits lösen Virenalarm aus

### *SQLite Viewer*

- See: **Forensics**
- Source: https://www.systoolsgroup.com/sqlite-viewer.html
- Online: https://inloop.github.io/sqlite-viewer/
- SQLite Viewer allows forensic investigators to explore the database files with the following extensions:
- .sqlite, .sqlite3, .sqlitedb, .db, and .db3

### *SSL FREAK Check*

- See: **Encryption**
- See also RSA_EXPORT

### *SSL Manager*

- Free

### *SSL Security Test!*

- See: **Encryption**
- See: https://www.ssllabs.com/ssltest

### *sslcaudit*

- See: **Penetration Testing**
- Source: Kali Linux
- The goal of sslcaudit project is to develop a utility to automate testing ***SSL/TLS*** clients for resistance against ***MITM attacks***.
- It might be useful for testing a thick client, a mobile application, an appliance, pretty much anything communicating over SSL/TLS over TCP.

```
sslcaudit -l 0.0.0.0:443 -v 1
```

## *sslscan*

- See: **Encryption**
- Source: Kali Linux
- sslscan queries SSL/TLS services, such as HTTPS, in order to determine the ciphers that are supported.

```
sslscan www.x.com
sslscan --no-failed www.x.com
sslscan --show-certificate www.x.com
sslscan --starttls-ftp www.x.com
```

## *Stacheldraht (DDOS)*

- See: **DDoS Tool**

Communication between clients, handlers and agents use these ports by default:

```
16660 tcp
65000 tcp
ICMP ECHO
ICMP ECHO REPLY
```

## *StartEd Pro*

- See: **Startup Programs Monitoring**
- Source: http://www.outertech.com
- StartEd is a utility that helps to manage the Windows startup procedure. It recognizes obsolete or memory-hogging startup programs and enables the option of disabling them to increase the quality of system performance.

***Features:***

- View, edit, delete, disable, and add entries to the Windows startup configuration
- Backup and Restore startup configurations
- Manage System Services with detailed notes and description
- Filter Service List with keywords
- See new startup items and services since last StartEd use
- Show detailed information about every startup entry
- Create shortcuts on desktop which is useful for temporarily disabled items
- Recognize Trojan Horses in startup configuration

## *Startup Delayer*

- See: **Startup Programs Monitoring**
- Source: http://www.r2.com.au
- Startup Delayer optimizes startup process by delaying applications from starting up as soon as a user logs into the computer.
- Because of the delay, the computer becomes usable a lot faster.
- Startup Delayer will then start launching the delayed applications when the computer is idle.

***Features:***

- Provides automatic delay engine
- Possess advanced launch options, which let to modify various launch options such as launching on a specific day.
- Monitors running tasks and services
- Creates backups of startup applications and restores them when required
- Recovers deleted applications

## *Stellar Phoenix Deleted Email Recovery*

- See: **E-Mail Forensics**

- Source: http://www.stellarinfo.com
- It is a software that safely recovers lost or deleted emails from MS Outlook data (PST) files and Outlook Express data (DBX) files.

### *SteelCentral Packet Analyzer*

- Is a packet analysis and reporting solution with an intuitive graphical user interface.
- We can use this tool with locally-presented trace files or remote SteelCentralTM NetShark devices, or SteelHead/SteelFusion running NetShark.
- SteelCentral Packet Analyzer identifies and troubleshoots network and application performance issues down to the bit level through Packet Analyzer's full integration with Wireshark.

***Features:***

- High-speed packet analysis to rapidly detect problems
- Analyze multi-terabyte files quickly
- Professional reporting that everyone can understand
- No charge for multi-segment analysis
- Seamless integration with Wireshark

### *StegAlyzerAS*

- See: **Steganography Detection Tool**
- http://www.sarc-wv.com

### *Steganography Studio*

- See: **Steganography Detection Tool**
- http://stegstudio.sourceforge.net

### *Steganos Privacy Suite 17*

- See: **Anti Forensics Tool**
- https://www.steganos.com

### *Stegdetect*

- See: **Steganography Detection Tool**
- https://github.com

### *StegExpose*

- See: **Steganography Detection Tool**
- https://github.com

### *Stellar Phoenix Mac Data*

- See: **File Recovery (MAC)**
- Recovery http://www.stellarinfo.com

### *Stellar Phoenix Windows Data*

- See: **File Recovery**
- Recovery http://www.stellarinfo.com

### *Stellar Phoenix Linux Data*

- See: **Partition Recovery (Linux)**
- Recovery Software http://www.stellarinfo.com

### *Stellar Phoenix Office Password*

- See: **Password Cracker**
- Recovery http://www.stellarinfo.com

### *Stellar Phoenix Zip Password*

- See: **Password Cracker**
- Recovery http://www.stellarinfo.com

### *Stellar Phoenix Outlook PST Repair Software*

- See: **E-Mail Forensics**
- Source: http://www.stellarinfo.com
- Stellar Phoenix® Outlook PST Repair is a reliable solution to repair and recover Outlook personal storage file '.PST'.
- After repair, the contents are restored to a new importable PST file.
- The application also facilitates the recovery of folders.

### *StackRox*

- ***Container Security*** for Docker and Kubernetes.

### *Startup Booster*

- See: **Startup Programs Monitoring**
- Source: http://www.smartpctools.com
- Startup Booster classifies all of the programs that are executed at startup as system programs, suspicious applications (such as viruses, etc.), and the unwanted programs for startup.
- This tool helps to remove programs from startup list or to add them when needed.

***Features:***

- Configures Windows to perform maximum by simple tweaks that suggest which options are to be activated and deactivated
- Cleans up the registry of outdated data or wrong values
- Instructs on how to configure the BIOS

### *Starus Partition Recovery*

- See: **Partition Recovery**
- http://www.starusrecovery.com

### *Steps for Evaluating the Security of a Windows NT Installation*

http://www.ntresearch.com/ntchecks.htm

### *Stunnel*

- Stunnel ist eine kostenlose ***SSL-Codiersoftware***.
- SSL (Secure Socket Layer) steht für eine verschlüsselte Verbindung, die in der Regel auf der Seite des Providers steht.
- Die Software muss auf ***Client*** und ***Server*** installiert werden.
- Anschliessend können Daten verschlüsselt übertragen werden.

### *Sumo Logic*

- See: **Forensics Network**
- Source: https://www.sumologic.com
- Sumo Logic is used to build, run, and secure modern applications.
- It is a cloud-native, machine data analytics service for log management and time series metrics.

### *SuperOneClick*

- Android

### *SuperScan*

- See: **Enumeration**

- Source:McAfee
- Performing Network Enumeration.
- Does IP Scanning, host and service discovery, port scanning, zone transfers and Windows enumeration.

### *SuperNetwork Tunnel*

- See: **DNS-Tool**
- Source:http://www.networktunnel.net/
- TCP over DNS
- Super Network Tunnel is professional ***http tunneling software***, which includes http tunnel client and server software.

### *SurfOFFLINE*

- See: **Website Mirroring**
- OS: Windows

### *Suricata*

- See: **NIDS**
- Source:https://suricata-ids.org/
- Ist ein ***Network Intrusion Detection System (NIDS).***
- Es wird durch die Open Information Security Foundation (OISF) entwickelt und betreut.
- Die Software steht unter einer ***freien GPLv2 Lizenz***.
- Neben dem Betrieb als IDS bietet Suricata auch einen Network Intrusion Prevention System (NIPS) Modus an der direkt in den Datenverkehr eingreift und Pakete blockieren kann.

### *Swatch*

- See: **Forensics Network**
- Source: https://sourceforge.net/projects/swatch
- Swatch is a tool used for monitoring log files produced by UNIX's syslog facility.

### *SwayzCryptor*

- See: **Attack Tool**
- Source:https://guidedhacking.com/threads/swayzcrypter.5778/
- ***Obfuscating a Trojan***
- At present, there have been numerous anti-virus software programs configured to detect malware such as Trojans, viruses and worms.
- Though security specialists keep updating the virus definitions, hackers try to evade/bypass them by some or the other means.
- One method which attackers use to bypass AVs is to “crypt” (an abbreviation of “encrypt”) the malicious files using fully undetectable crypters (FUDs).
- Crypting these files allow them to achieve their objectives and thereby taking complete control over the victim machine.
- As an expert security auditor or ethical hacker, you need to ensure that your organization’s network is secure from such encrypted malware files, and anti-virus tools are properly configured to detect and delete such files.
- A crypter is software used to hide viruses, keyloggers, or any RAT tool from antiviruses so that they are not detected and deleted by antiviruses.
- It simply assigns hidden values to each individual code within source code.
- Thus, the source code becomes hidden, making it difficult for the anti-virus tools to scan it.

### *Syslog-ng*

- See: **Forensics Network**
- Source: https://syslog-ng.org
- syslog-ng allows the collection, parsing, classification, and correlation of logs from across the infrastructure and store or route them to log analysis tools.

### *System Explorer*

- See: **Forensics**
- http://systemexplorer.net
- System Explorer is software for exploration and management of system Internals.
- It includes many tools, which help to keep the system under control.
- With System Explorer, one can get fast access to file database, which helps to determine unwanted processes or threats.

### *SysAnalyzer*

- See: **Port Monitor**

### *SysTracer*

- See: **Monitoring Registry**
- Source: http://www.blueproject.ro
- SysTracer is a system utility tool that can scan and analyze your computer to find changed (added, modified or deleted) data into registry and files.
- SysTracer can scan your system and record information about changed files and folders, modified registry entries, installed programs, etc.

### *T-Sight*

- See: **DDoS Tool**

### *T3iu Forensic SATA Imaging Bay*

- See: **Forensics**
- Source: https://www2.guidancesoftware.com
- It is built for write-blocked acquisitions of 3.5" and 2.5" SATA hard drives.

### *TAFT*

- See: **Forensics**

### *Tamper Data*

- See: **Penetration Testing**
- Monitor live requests
- Edit headers on live requests
- Cancel live requests
- Redirect live requests

### *TCP-over-DNS*

- Evade firewall inspection

### *TCPDUMP*

- OS: Unix, Linux
- Can be used for ***passive OS fingerprinting***
  http://geek00l.blogspot.com/2007/04/tcpdump-privilege-dropping-passive-os.html

### *TCPflow*

- See: **Penetration Testing**
- tcp-ip-reassembler

### *TCPTRACE*

- To ***analyze*** files, produced by tcpdump, WinDump, Wireshark and EtherPeek.
- Is a tool written by ***Shawn Ostermann*** at Ohio University, for analysis of TCP dump files.
- It can take as input the files produced by several popular packet-capture programs, including tcpdump, snoop, etherpeek, HP Net Metrix, and WinDump.

- *tcptrace* can produce several different types of output containing information on each connection seen, such as elapsed time, bytes and segments sent and received, retransmissions, round trip times, window advertisements, throughput, and more.
- It can also produce several graphs for further analysis.

### *TCPTRACEROUTE*

- To detect ***round-robin-load-balancing***.

### *TCPView*

- See: **Port Monitor**
- Tells real time, which ports are listening or in another state.

### *TD2u Forensic Duplicator*

- See: **Forensics**
- Source:https://www2.guidancesoftware.com
- Data acquisition

### *TEMPEST*

- See: **Penetration Testing**
- Can compromise the security of data displayed on a ***monitor***.
- See: ***Van Eck radiation***, ***Van Eck phreaking***.
- ***Keyboards*** and ***mice*** are also vulnerable to TEMPEST monitoring.
- TEMPEST countermeasures include ***Faraday cages***, ***white noise*** and ***control zones***.
- TEMPEST project, researching of ***emanation security*** since 1950s.

### *TestDisk*

- To recover data and partitions on Win, Linux, SunOS and MAC OS X.

### *TestDisk for Mac*

- See: **Partition Recovery**
- http://www.cgsecurity.org

### *Tenorshare PDF Password*

- See: **Password Cracker**
- Recovery http://www.tenorshare.com

### *TFN / TFN2K (DDOS)*

- See: **DDoS Tool**
- Communication between clients, handlers and agents does not use any specific port, for example, it may be supplied on run time or it is chosen randomly by a program, but is a combination of UDP, ICMP and TCP packets.

### *THC-Hydra*

- See: **Password Cracker**
- Source:Kali Linux
- https://www.thc.org

### *Theef*

- See: **Penetration Testing**
- Theef is a Windows-based application for both a client and a server.
- The Theef server is a ***virus*** that you install on a target computer, and the Theef client is what you then use to control the virus.

### *The Elastic Stack*

- See: **Forensics Network**
- Source: https://www.elastic.co
- The open-source Elastic Stack, that is Elasticsearch, Kibana, Logstash, and Beats, helps procure data from any source in any format and search, analyze, and visualize it in real time.

### *TheFatRat*

- See: **Penetration Testing**
- Creating Malicious Office Documents
- Social Engineering is one of the most typically used attacks by a hacker.
- As the recent trends suggest, many big organizations fall victim to this attack vector.
- The attackers trick the staff of a workplace to click links in a legitimate looking document which turn out to be malicious and even able to evade the anti-virus programs.
- TheFatRat is an exploiting tool which compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac. TheFatRat provides an easy way to create backdoors and payloads which can bypass most anti-virus systems.

### *ThreatAnalyzer*

- See: **Online Malware Analysis**
- Source: http://www.threattracksecurity.com
- ThreatAnalyzer is a malware analysis tool that provides defense against Advanced Persistent Threats (APTs), Zero-days, and custom-targeted attacks.
- This tool analyzes malware samples, generates report analyses to aid in the understanding of each threat, and improves response time to remediate threats.

### *Thumbcache Viewer*

- See: **Forensics**

### *ThumbsDisplay*

- See: **Forensics**
- http://www.infinadyne.com
- ThumbsDisplay is a tool for examining and reporting on the contents of Thumbs.db files used by Windows.
- The tool prints a full-page version of thumbnail images without any other graphics programs.
- It will copy individual thumbnails and print three different format reports.

### *TIBCO LogLogic*

- See: **Forensics Network**
- Source: http://www.tibco.com
- This tool is used to harness log and machine data to provide insight into IT operational efficiencies.

### *TigerBreach Penetrator*

- See: **Penetration Testing**
- Source:https://www.freeforumzone.com/discussione.aspx?idd=5737328
- Is part of ***TigerSuite***.
- Penetrating ***whois*** databases.

### *TOR proxy*

- See: **Anti Forensics Tool**
- To hide your true identity when performing almost anything online.

### *Total Recall*

- See: **File Recovery**
- http://www.totalrecall.com

### *Towelroot*

- See: **Android Rooting Tools**
- Source: http://towelroot.org
- The Towelroot app provides one click root to most of the existing and popular Android smart phones.
- Towelroot.apk is an easy and convenient rooting apk for Android devices like nexus 5.
- You can download the towelroot.apk file to computer and transfer it to mobile to get Android towel root download software for mobile.

### *Triage-Responder*

- See: **Forensics**
- Source: http://www.adfsolutions.com
- Triage-Responder is designed particularly for nontechnical first responders.
- It uses an easy two-step process to scan, analyze and extract evidence from a digital device.
- It searches the whole target drive in four categories and integrates different technologies, like, ActivitySensorTM, which enables the investigators to find and collect valuable files quickly

### *Trinoo (DDOS)*

- See: **DDoS Tool**

Communication between clients, handlers and agents use these ports by default:

```
1524 tcp
27665 tcp
27444 udp
31335 udp
```

### *Tripwire Log Center Source*

- See: **Forensics Network / Monitoring**
- Source:www.tripwire.org
- HIDS
- Open source.
- Allows you to monitor a system for changes.
- Maintains a database of ***hash values*** for all files stored on the system and reports to you periodically.
- Tripwire Log Center normalizes data from servers, security and network devices, as well as applications, integrating them with Tripwire Enterprise and Tripwire IP360TM to provide ***endpoint protection*** and security.
- Tripwire Log Center ensures that regulations are met with complete, secure, and reliable log collection.

### *Troubleshooting Windows NT*

- http://www.ntsystems.com/nts110fe.htm

### *Tufin Suite*

- Source:www.tufin.com
- Tufin Security Policy Orchestration for Today's Enterprise Networks.
- Visualize and ***control your network security policy*** across all on-premise environments and cloud platforms.

### *UFED Cloud Analyzer*

- See: **Cloud Forensics**
- Source: http://www.cellebrite.com
- Cloud data sources represent a virtual goldmine of potential evidence for forensic investigators.
- Together with mobile device data, they often capture the details and critical connections investigators need to solve crimes.
- However, access remains a challenge.

- The tool provides forensic practitioners with instant extraction, preservation, and analysis of private social media accounts --Facebook, Twitter, Kik, Instagram --file storage and other cloud-based account content that can help speed investigations.
- The tool automatically collects both existing cloud data and metadata and packages it in a forensically sound manner.
- Allows investigators to search, filter and sort data and identify the required details to advance their investigations.

### *UFED Pro Series*

- See: **Forensics**
- Source.http://www.cellebrite.com
- Data acquisition

### *UFED Touch*

- See: **Forensics**
- Source.http://www.cellebrite.com
- Data acquisition

### *UFED Touch2*

- See: **iPhone Data Acquisition Tools**
- Source: http://www.cellebrite.com
- UFED Touch2 is a device used to perform physical, file system, password and logical extractions of evidentiary data

### *UltraKit*

- See: **Forensics**
- Source:https://www.digitalintelligence.com
- Data acquisition
- Hardware write blocker

### *UltraTools*

- See: **WHOIS Online Tool**
- Source: https://www.ultratools.com/whois/home
- UltraTools is an online tool that shows you information about the domain you enter, including the Whois registration data, the Site Profile, and IP information.

### *UndeletePlus*

- See: **Forensics & File Recovery**
- Source: http://www.undeleteplus.com
- Recovers documents, photos, video, music, and email.
- Recover files - even those emptied from the Recycle Bin.
- File recovery after accidental format - even if one has reinstalled Windows.
- Recover files from hard drives, USB thumb drives, camera media cards, floppy disks, and other storage devices.

### *Unistal Email Recovery Software*

- See: **E-Mail Forensics**
- Source: http://www.unistal.com
- This software tool helps recover and restore MS Outlook Files, Lotus Notes email files, Incredimail as well as MS Exchange email files.

### *Universal Shield*

- See: **Anti Forensics Tool**
- http://www.everstrike.com

### *unix-privesc-check*

- See: **Vulnerability Scanner / Penetration Testing**
- Source: Kali Linux

### *Unknown Device Identifier*

- See: **Device Drivers Monitoring Tool**
- Source: http://www.zhangduo.com
- Unknown Device Identifier enables one to identify the yellow question mark labeled “Unknown Devices in Device Manager.”
- It reports a detailed summary for the manufacturer name, OEM name, device type, device model and even the exact name of the unknown devices.
- With the collected information, one might contact the hardware manufacturer for support or search the Internet for the corresponding driver.

### *US-LATT PRO*

- See: **Forensics**
- Source: https://www.wetstonetech.com
- Data acquisition

### *USB Dumper*

- See: **Forensics**
- To copy silently files from USB devices.

### *USER2SID*

- See: **Enumeration tool**

### *USIM Detective*

- See: **Forensics Mobile**
- Source: http://www.quantaq.com
- It provides features such as data integrity, fast throughput, and advanced data imaging.
- USIM Detective can view acquired information (including phonebook contacts and numbers, SMS text messages, deleted text messages, and call records) in a number of report formats.

### *USM Anywhere*

- See: **Vulnerability Scanner**
- Source: Alien Vault
- Unified Security Monitor

### *URLScan*

- See: **Reconnaissance**
- UrlScan is a security tool that restricts the types of HTTP requests that ***IIS*** will provide, by blocking specific HTTP requests.
- Helps to prevent potentially harmful requests from reaching applications on the server.

### *Valkyrie*

- See: **Online Malware Analysis**
- Source: https://valkyrie.comodo.com
- Valkyrie is a signature-based malware detection system that conducts analysis using run-time behavior and hundreds of features from a file.
- It can also warn users against malwares undetected by other Anti-Virus products.

### *Vault*

- See: **Credential Management**
- Source: https://vaultsecurity.io

### *Veracode*

- See: **Vulnerability Scanner Code**
- Link: https://www.veracode.com/security/application-vulnerability
- Application Vulnerability code scanner.

### *VeraCrypt*

- See: **Disk Encryption**
- Basic Disk Encryption
- VeraCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost, and the source code is available.
- It can create a virtual encrypted disk within a file or encrypt a partition or entire storage device.

### *Veriato Server Manager*

- See: **Forensics Network**
- Source: http://www.veriato.com
- This tool allows the viewing and reporting of event log data and isolates pertinent log entries by merging multiple logs into a single view, hiding duplicate entries, and filtering the results.
- It easily exports, prints, or emails the results for clear and concise event log analysis.

### *Verisys*

- See: **File and Folder Integrity Checkers**
- Source: https://www.ionx.co.uk
- Verisys is file integrity monitoring solution for Windows and Linux that allows you to maintain the integrity of business critical files and data by detecting unauthorized changes.
- Verisys is configurable to suit your requirements using the interface and includes many templates for common systems and applications to help you get started quickly.

### *VirtualLab*

- See: http://www.vlab.co.in/
- Source: http://www.binarybiz.com
- See: File Recovery
- Locate lost files and partitions
- restore data from formatted, damaged or lost patition on Windows and Mac

### *Virtual Steganographic*

- See: Steganography Detection Tool
- Laboratory (VSL) http://vsl.sourceforge.net

### *Virtuosity*

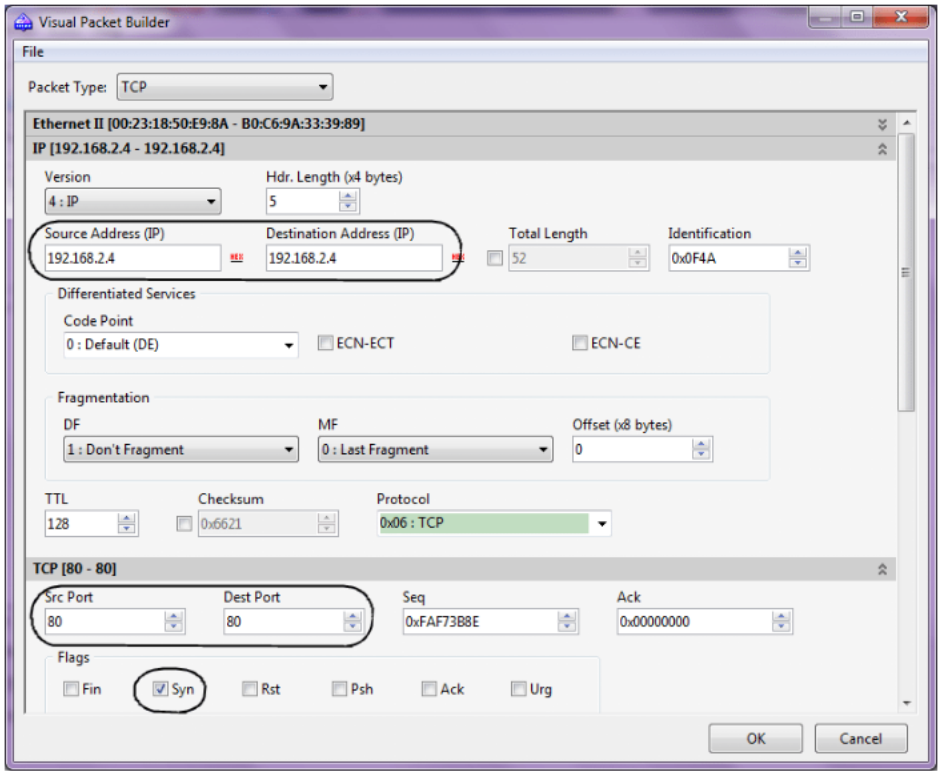
http://www.ntsecurity.com

### *VirusTotal*

- See: **Online Malware Analysis**
- Source:https://www.virustotal.com/gui

### *Visual Packet Builder*

- See: **Packet Crafting**
- Source:tamos.com




An example of a Land attack packet A packet generator tool can be used to customarily build the Land attack traffic packets. This can be done by using an online command tool, such as FrameIP Packet Generator (FrameIP Packet Generator, 2013), or a more friendly and easy to use GUI tool, such as Engage Packet Builder (Engage Packet Builder, 2013) or CommView Visual Packet builder (CommView Network Monitor, 2013). For instance, from the attack host "A" and using CommView Visual Packet Builder, Figure 4 shows a spoofed TCP SYN packet used to generate Land attack traffic. The packet has the source IP address equals to the destination IP address (Host B's IP: 192.168.2.4), and the source port equals to the destination port 80. The destination MAC address is set to the MAC address of the target Host "B".

## *Visual TimeAnalyzer*

- From A. & M. Neuber Software: Visual TimeAnalyzer is an extensive reporting timesheet, project and time tracking software. The easy to use application automatically ***tracks all computer activities***, working time, pauses, projects, costs, software and Internet use and presents detailed, richly illustrated reports.
- You learn which programs were used for how long, when, and by whom. Parents have control over their children's PC use.
- The logger runs invisible in the background and monitors all activities on family's PC or company's network.
- Visual TimeAnalyzer analyses software usage at individual workstations or across the network.
- You can choose detailed reports and analysis graphs for time tracking, time management, project tracking, project management, project cost or attendance.
- Select user and time periods and see: Weekly statistics, hourly computer use, most used programs, online time, active working time, pause times, opened documents, projects, daily summary (diary), history and intensity of program usage (ideal for project overview), extent of the use of available programs, visited web pages (time, URL, title), and TopTen of the most popular web pages. Visual TimeAnalyzer analyzes PC activities in Family or Business.
- You can compare all users (e.g. most active users, most used programs, most visited websites). Keep user data (like passwords and personal documents) safe: Visual TimeAnalyzer does not record keyboard inputs or run background screencaptures.

## *VisualCodeGrepper*

- See: **Vulnerability Scanner**

### *Volatility Framework*

- See: ***IT-Forensik***
- Dieses Rahmenwerk dient der Analyse flüchtiger Speicher.
- Es untersucht beispielsweise die Runtime-Prozesse und den Systemstatus anhand der Daten, die es im RAM findet.
- Das Framework wurde an der Black Hat entwickelt und wird mittlerweile weltweit von Strafverfolgungsbehörden verwendet.
- Infos: www.volatilityfoundation.org

### *vRealize Log Insight*

- See: **Forensics Network**
- Source: http://www.vmware.com
- vRealize Log Insight delivers heterogeneous and scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility, thereby providing operational visibility and faster troubleshooting.

### *wbStego*

- See: **Anti Forensics Tool**
- http://wbstego.wbailer.com

### *Web Data Extractor*

- See: **Reconnaissance / Web Mirroring Tool**
- Source:www.webextractor.com
- Price: 199 USD
- Web Data Extractor Pro is a web scraping tool specifically designed for mass-gathering of various data types.
- It can harvest ***URLs***, ***phone*** and ***fax numbers***, ***email addresses***, as well as ***meta tag information*** and ***body text***.
- Special feature of WDE Pro is ***custom extraction of structured data***.

### *Web Wiz*

- See: **WHOIS Online Tool**
- Source: http://www.webwiz.co.uk/domain-tools/whois-lookup.htm
- WebWiz is an online tool used to look up the whois information for domains and IP addresses.

### *Webalizer*

- See: **Web Attack Investigation**
- Source: http://www.webalizer.org
- The Webalizer is a web server log file analysis program.
- It produces detailed, configurable usage reports in HTML format, for viewing with a standard web browser.

### *WebBrowserPassView*

- See: **Password**
- Source: http://www.nirsoft.net
- Investigators can use tools such as WebBrowserPassView, a ***password recovery tool*** that reveals the passwords stored by the following Web browsers:
  Internet Explorer (Version 4.0 - 11.0)
  Mozilla Firefox
  Google Chrome
  Safari
  Opera
- The tool can also be used to recover the lost/forgotten password of any website be it Facebook, Google, Yahoo as long as it is stored in the user's browser.

- The retrieved passwords can be saved in text/html/csv/xml file by using the Save Selected Items.

### *WebGoat*

- See: **Penetration Testing**
- WebGoat is a platform independent environment.
- Black-box testing
- Maintained by OWASP
- Can use Java or .NET
- It utilizes Apache Tomcat and the JAVA development environment.
- Installers are provided for Microsoft Windows and UN*X environments, together with notes for installation on other platforms

### *WebLog Expert*

- See: **Forensics Network / Web Attack Investigation**
- Source: https://www.weblogexpert.com
- WebLog Expert is an access log analyzer.
- It provides information about a website's visitors: activity statistics, accessed files, paths through the site, information about referring pages, search engines, browsers, operating systems, and more.
- WebLog Expert can analyze logs of Apache, IIS and Nginx web servers.
- It can even read GZ and ZIP compressed log files, which precludes the need for manually unpacking them.

***Features:***

- It provides general statistics, activity, and access statistics
- It gives information about visitors: hosts, top-level domains, countries, states, cities, authenticated users, screen resolutions, color depths and languages
- It gives information about errors
- It supports custom reports

### *Web Log Storming*

- See: **Web Attack Investigation**
- Source: http://www.weblogstorming.com
- Web Log Storming is a web server log file analyzer (IIS, Apache, and Nginx) for Windows.

### *Webroot's Internet Security Complete*

- See: **Anti Forensics Tool**
- http://www.webroot.com

### *WebSiteSniffer*

- See: **Forensics Network**
- Source: http://www.nirsoft.net
- WebSiteSniffer is a packet sniffer tool to capture all Web site files downloaded by the Web browser while browsing the Internet and stores them on your hard drive under the base folder that you choose.
- WebSiteSniffer allows the users to capture any required type of Web site files: HTML Files, Text Files, XML Files, CSS Files, Video/Audio Files, Images, Scripts, and Flash (.swf) files.
- While capturing the Web site files, the main window of WebSiteSniffer displays general statistics about the downloaded files for every Web site/host name, including the total size of all files (compressed and uncompressed) and total number of files for every file type.

### *WebToolHub*

- See: **WHOIS Online Tool**
- Source: http://www.webtoolhub.com/tn561381-whois-lookup.aspx
- WebToolHub is an online whois lookup service to check the owner of the domain name or IP address.

### *Wfuzz*

- See: **Password cracker**
- Capability of injection via multiple points with multiple dictionary
- Output in colored HTML
- Post, headers and authentication data brute forcing
- Proxy and SOCK Support, Multiple Proxy Support
- Multi Threading
- Brute force HTTP Password
- POST and GET Brute forcing
- Time delay between requests
- Cookies fuzzing

### *WhatChanged*

- See: **Dropbox Investigation / Monitoring Registry**
- Source: http://portableapps.com
- WhatChanged portable is useful for checking program installations.
- It is a system utility that scans for modified files and registry entries.
- It uses the 'brute-force method' to check files and the registry.

***There are two steps for using WhatChanged Portable software:***

- First, take a snapshot to get the current state of the computer before installing Dropbox client;
- Second, run it again to check the differences since the previous snapshot, after installing Dropbox client. By comparing both the screen shots, investigators can find out the list files modified in the registry and the entries made to the registry.

### *What's Running*

- See: **Malware Analysis**
- Supplier: https://whats-running.en.softonic.com
- A user can use What's Running to explore processes, services, modules, IP-connections, and drivers, among others.
- It finds relevant information such as what modules are involved in a partiular process.

### *WhatInStartup*

- See: **Startup Programs Monitoring**
- Source: http://www.nirsoft.net
- This utility displays the list of all applications that are loaded automatically when Windows starts up.
- For each application, the following information is displayed: Startup Type (Registry/Startup Folder), Command-Line String, Product Name, File Version, Company Name, Location in the Registry or file system, and more.
- It allows you to easily disable or delete unwanted programs that run in your Windows startup.
- You can use it on your currently running instance of Windows, as well as you can use it on external instance of Windows in another drive.

### *Whisker*

- See: **Anti-Forensics**
- Anti IDS Tactics, Evasion Tactics.
- Can be used for ***session splicing attack***.

### *WhoIs Analyzer Pro*

- See: **WHOIS Desktop Tool**
- Source: http://www.whoisanalyzer.com
- WhoIs Analyzer Pro grants you access to contact records and other information from registrars and routing registries worldwide without you having to know which one to visit.
- It gives accurate information for any IP address, email address, URL, or Autonomous System Number (ASN) by giving you access to contact records from every country worldwide.

### *Whois*

- See: **WHOIS Online Tool**
- Source: http://tools.whois.net
- Whois performs the registration record for the domain name or IP address specified by you.

### *Whois Online*

- See: **WHOIS Online Tool**
- Source: http://whois.online-domain-tools.com
- Whois Online is a tool that allows you to get information about various Internet resources, such as domain names, networks, IP addresses, domain registrants or autonomous systems.
- It queries WHOIS databases to get information that you are looking for.
- WHOIS record contains human-readable information about the organization (or person) that owns or administers the queried resource and the associated contact information.

### *WhoisThisDomain*

- See: **WHOIS Desktop Tool**
- Source: http://www.nirsoft.net
- Pricing: ***Freeware***
- WhoisThisDomain is a domain registration lookup utility allows you to easily get information about a registered domain.
- It automatically connects to the right WHOIS server, according to the top-level domain name, and retrieves the WHOIS record of the domain.

### *WiFite*

- See: **WiFi**
- Source: Kali Linux

```
Wifite → Start WiFite
<x>    → Select SSID
```

### *WinAgents EventLog Translation Service*

- See: **Forensics Network**
- Source: http://www.winagents.com
- The WinAgents EventLog Translation Service is a server that monitors Windows event logs and forwards the events that appear for further processing.
- The program can forward events to a Syslog server or to an SNMP management station.

### *WinDump*

- See: **Forensics Network**
- Source: http://www.winpcap.org
- Kostenlose alternative zu TCPDUMP.
- WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX.
- WinDump is fully compatible with tcpdump and is used to watch, diagnose, and save to disk network traffic according to various complex rules.

### *Windows Data Recovery Software*

- See: **File Recovery**
- http://www.diskdoctors.net

### *Windows Forensic Toolchest (WFT)*

- See: **Forensics**
- http://www.foolmoon.net
- The Windows Forensic Toolchest (WFT) is designed to provide a structured and repeatable automated live forensic response, incident response, or audit on a Windows system while collecting security-relevant information from the system.

- WFT is essentially a forensically enhanced batch processing shell, capable of running other security tools and producing HTML-based reports in a forensically sound manner.

### *Windows NT Security FAQ*

http://www.it.kth.se/~rom/ntsec.html

### *Windows NT Security Issues bei Somarsoft*

http://www.somarsoft.com/security.htm

### *Windows NT Magazine Online*

http://www.winntmag.com/

### Defense Information Infrastructure Common Operating Environment (DII COE), Version 3.1

- Gesammelte Dokumente zu NT 4.0
- http://spider.osfl.disa.mil/cm/dii31/dii31_nt40.html

### *Windows Password Recovery Lastic*

- See: **Password Cracker**
- Is a password recovery tool used to recover the password in Windows OSs.
- This tool requires rebooting into another OS.
- Run the tool on another computer to create a bootable USB stick or CD/DVD disk and then Boot from it on the computer and the program lists all user accounts it finds, thereby offering an easy way to remove a password of any of them.
- Once Windows Password Recovery Lastic loads its boot part from a bootable, it offers the user a choice to either remove a password of some particular Windows user account or to save its hash. Removing a password is done instantly.
- Therefore, this is a preferable way to access the computer.

### *Windows Password Unlocker*

- See: **Password Cracker**
- https://www.passwordunlocker.com

### *Windows Password Breaker*

- See: **Password Cracker**
- Enterprise http://www.recoverwindowspassword.com

### *Windows Password Recovery Tool*

- See: **Password Cracker**
- http://www.windowspasswordsrecovery.com

### *Windows Service Manager (SrvMan)*

- See: **Windows Services Monitoring Tool**
- Source: http://tools.sysprogs.org
- SrvMan has both GUI and Command-line modes.
- It can also be used to run arbitrary Win32 applications as services (when such service is stopped, the main application window is closed automatically).

***Features:***

- Allows creating driver and Win32 services without restarting
- Supports both GUI and Command Line
- Supports all modern 32-bit and 64-bit versions of Windows
- Allows running arbitrary Win32 applications as services
- Allows installing & running legacy driver services in a single command line call

### *Windows Service Manager Tray*

- See: **Windows Services Monitoring Tool**
- Source: http://winservicemanager.codeplex.com
- Windows Service Manager Tray allows selecting the necessary services and controlling them from the tray.
- This tool also optimizes the default Windows service manager and permits to start, stop, or restart required services.

### *WinGate*

- See: **Tool**
- WinGate Proxy Server is a highly capable HTTP Proxy server, SOCKS server, integrated Internet gateway and communications server designed to meet the access control, security and communications needs of today's businesses.
- In addition to a comprehensive range of features.

### *WinHex*

- See: **Forensics**
- Powerful tool to recover files
- All File Type signatures can be displayed.

***Examines:***

- Recovered deleted files
- Fragmented files
- Corrupted data

### *WinMD5*

- See: **Monitoring**
- Source: http://www.winmd5.com
- WinMD5Free is a utility to compute MD5 hash value for files.
- It works with Microsoft Windows 98, 2000, XP, 2003, Vista, 7 and later versions.

### *WinPatrol*

- See: **Startup Programs Monitoring**
- Source: http://www.winpatrol.com
- WinPatrol provides the user with 14 different tabs to help in monitoring the system and files.
- This security utility gives the user a chance to look for the programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate/malicious programs.
- WinPatrol is a system utility that helps users to monitor changes made to files and folders, startup programs, hidden files, scheduled tasks, and services.

### *WinTools.net 16.7.1 Premium*

- See: **Startup Programs Monitoring**
- Source: http://www.wintools.net
- It is a suite of tools for increasing MS Windows operating system performance.
- WinTools.net cleanly removes unwanted software from disk drives and dead references from the Windows registry.
- WinTools.net puts you in control of the Windows start up process, memory monitoring and gives you the power to customize desktop and system settings to fit your needs.
- Adds more speed and stability for your connection.
- Ensures your privacy and keep sensitive information secure.

### *WinTrinoo (DDoS)*

- See: **DDoS Tool**

### *WriteProtect-DESKTOP*

- See: **Forensics**
- Source: http://www.logicube.com
- The WriteProtect-DESKTOP provides digital forensic professionals with a secure, read-only write-blocking of suspect hard drives.
- It is a ***portable write-blocker*** that provides support for 5 different interfaces in one device.

### *Winrtgen*

- See: **Password Cracking**
- Source: http://www.oxid.it
- Winrtgen is a graphical Rainbow Tables Generator that helps attackers to create rainbow tables from which they can crack the hashed password.
- Generate Rainbow Tables Using Winrtgen

### *WinUndelete*

- See: **File Recovery**
- http://www.winundelete.com

### *Wise Data Recovery*

- See: **File Recovery & E-Mail Forensics**
- http://www.wisecleaner.com
- Wise Data Recovery is a data recovery program to get back deleted photos, documents, videos, emails etc. from your local or removable drives for free.

### *Word Extractor*

- See: **Forensics**
- http://www.soft.tahionic.com

### *Word Password Recovery Master*

- See: **Password Cracker**
- Source: http://www.rixler.com
- Word Password Recovery Master is used to crack password-protected documents created in MS Word 97/2000/XP/2003/2007/2010/2013.
- The program allows the user to crack “open,” “protection,” and “write” passwords.

### *WS_FTP Pro*

- See: **FTP Client**
- Professionelle Art Files mit FTP zu transferieren.

### *X-ray*

- See: **Vulnerability Scanner**
- For Android devices.

### *X-Ways Forensics*

- See: **Forensics**
- Dabei handelt es sich um eine integrierte kommerzielle Arbeitsumgebung für IT-Forensiker, die laut Herstellerangaben nicht so ressourcenhungrig ist wie vergleichbare Tools.
- Das Werkzeug ist anwenderfreundlich, mobil und läuft von einem USB-Stick aus auf jedem Windows-System ohne vorherige Installation.
- Source: www.x-ways.net

***Features:***

- Access logical memory of running processes
- Gather slack space, free space, inter-partition space, and generic text from drives and images

- Ability to read partitioning and file system structures
- Memory analysis for local RAM or memory dumps
- Disk cloning and imaging

### *xARP*

- Detection of ***ARP poisoning***

### *XenMobile*

- MDM

### *Xplico*

- See: **Forensics**
- Source: http://www.xplico.org
- The goal of Xplico is to extract the applications data contained from an ***internet traffic capture***.
- For example, from a ***pcap*** file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on.
- Xplico is an open source Network Forensic Analysis Tool (NFAT).

### *XpoLog Log Management*

- See: **Forensics Network**
- http://xpolog.com
- The XpoLog log management platform helps in the analysis, visualization, monitoring, and automated in-depth mining of log data.
- XpoLog allows the optimization of IT operations and visibility for any type of system log data.

### *XRY Office*

- See: **Forensics**
- Source: https://www.msab.com
- XRY Office provides both logical and physical support for mobile forensic examiners.
- It provides full access to thousands of mobile devices with all the required tools supplied.
- XRY is a software-based solution and is built for a purpose with all the required hardware to recover data from ***mobile devices*** in a secure way.

### *Yersinia*

- Yersinia is a framework for performing layer 2 attacks.
- It is designed to take advantage of some weaknesses in different network protocols.
- It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Attacks for the following network protocols are implemented in this particular release:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- 802.1q
- 802.1x
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Source: https://github.com/tomac/yersinia
Yersinia Homepage | Kali Yersinia Repo
Author: Alfredo Andres Omella, David Barroso Berrueta
License: GPLv2

### *Yet Another (remote) Process Monitor*

- See: **Tool**
- Source: http://yaprocmon.sourceforge.net
- Yet Another (remote) Process Monitor (YAPM) is an application that allows to view and manage running tasks, processes, threads, and modules, and the services on a local or on a remote machine.

### *Zamzar*

- See: **Forensics**
- Source: http://www.zamzar.com
- Zamzar supports over 1200 different ***conversions*** such as Video Converter, Audio Converter, Music Converter, eBook Converter, Image Converter, and CAD Converter.

### *zAnti*

- See: **Penetration Testing**
- Mobile Penetration Testing Toolkit & Risk Assessment.

### *ZAR Windows Data*

- See: **Partition Recovery**
- Recovery http://www.z-a-recovery.com

### *ZClone®Xi*

- See: **Forensics**
- Source:http://www.logicube.com
- Data acquisition

### *ZIP Password Genius*

- See: **Password Cracker**
- http://www.isunshare.com

### *ZoneAlarm*

- FW

### *Xstegsecret*

- See: **Steganography Detection Tool**
- http://stegsecret.sourceforge.net

### *Zzuf*

- SW ***Fuzz testing*** tool.
- Uses ***bit flipping***.

# TECHNIQUES

- Packet crafting
- Distortion Technique to encrypt messages.
- Text Semagrams
- Linguistic Steganography
- ***Bastion Host***
  Exposed to the @Internet
  Hardened - You expect an attack, its your front line.
- BPF-Based filtering
- 5nine Cloud Security
- ***Screened Subnet***
  A Bastion Host between an internal and an external firewall
  MOST SECURE

AATP - Azure Advanced Threat Protection
OATP - Office Advanced Threat Protection
WDATP - Windows Defender Advanced Threat Protection

## *Firewalking*

- Determing what port or protocol is open on a Firewall is known as ***Firewalking***.
- Firewalking is a technique developed by Mike Schiffman and David Goldsmith that ***utilizes traceroute techniques*** and ***TTL values*** to analyze IP packet responses in order to ***determine gateway ACL*** (Access Control List) filters and ***map networks***.
- It is an ***active reconnaissance*** network security analysis technique that attempts to determine which layer 4 protocols a specific firewall will allow.
- To find out which ***ports*** and ***protocols*** is the firewall letting go through.

***Countermeasure:***

- To protect a firewall / gateway against firewalking one can ***block ICMP Time Exceeded messages***.

## *Incident Response*

| | |
|---|---|
| **Vorbereitung**<br>Aufbauen, Erhalten und verbessern der Reaktionsfähigkeit bei sicherheitsrelevanten Vorfällen | |
| **Identifikation**<br>Bestätigen, Kategorisieren, Eingrenzen und Priorisieren von sicherheitsrelevanten Vorfällen | |
| **Eindämmen**<br>Minimieren des Schadens durch Datenverlust, Informationsdiebstahl oder Serviceunterbruch | |
| **Beseitigung**<br>Enfernen der Bedrohung | |
| **Wiederherstellung**<br>Sicheres und schnelles Wiederherstellen der Système und Services | |
| **Lessons Learned**<br>Identifizieren von prozessualen sowie organisatorischen und technischen Massnahmen für die Verbesserungd der Abläufe beim nächsten Event | |

## *IT-Forensik*

- Chain of Custody bewahren und jeden Schritt dokumentieren.
- Hashing anwenden um integrität der gesicherten Daten zu gewähren.

- «Computer-Forensik - Computerstraftaten erkennen, ermitteln, aufklären»
  ISBN 978-3-86490-133-2

## *MM - Open Source Testing Methodology Manual*

- Maintained by ***ISECOM***
- ***Addresses controls***.
- Recognizes ten types of controls, divided in two classes:
  Class A: ***Interactive***
  Class B: ***Process***

**Recognizes three types of compliancy:**

- Legislative
- Contractual
- Standard based

## *Pivoting Method*

- Pivoting is the exclusive method of using an instance also known by 'foothold' to be able to "move" from place to place inside the compromised network.
- It uses the first compromised system foothold to allow us to compromise other devices and servers that are otherwise inaccessible directly.
- Is a method that makes ***use of a compromised system*** to attack other systems on the same network to avoid restrictions that might prohibit dierect access to all machines.

**Example:**
An Attacker has an IP (192.168.1.104).
The attacker compromises a Windows XP system having IP 192.168.1.131 and 10.128.0.3.
Now the attacker scan 10.128.0.x network and found an IP 10.128.0.1 (Linux) to be live and then he goes ahead and tries to compromise it as well.
Now Point to be noted is that the IP 10.128.0.1 (Linux) is not directly accessible to the attacker, but still, it can be compromised by the technique "Pivoting."

## *Steganography*

- For Images
- For Documents

## *CMM - Software Capability Maturity Model*

- Also called: SW-CMM, SCMM
- Developed by: Software Engineering Institute (SEI) at Carnegie Mellon University
- The CMM is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes.

The five Software Capability Maturity levels have been defined as:

**1. Initial**
The software process is characterised as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.

**2. Repeatable**
Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

**3. Defined**
The software process for both management and engineering activities is documented, standardised, and integrated into all processes for the organisation. All projects use an approved version of the organisation's standard software process for developing and maintaining software.

**4. Managed**

Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

**5. Optimising**
Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

# COUNTERMEASURES

- Ensure systems are not running ***unneeded services*** and ***protocols*** to reduce a system's attack surface.
- Enable both, ***network-based firewalls*** and ***host-based firewalls***.
- Use ***honeypots***.
- Keep systems "***up-to-date"***.
- Use ***sandboxing***.
- Use ***postmortem review***.
- The primary means of ***defense against malicious code*** is the use of antivirus-filtering software.
- Every ***server system*** on a network should have updated antivirus software searching the local file system for malicious code.
- Use ***content filter*** system to scan inbound and outbound electronic mail and web traffic for signs of malicious code.
- Use ***Tripwire (IDS)*** to monitor your systems.
- The cornerstone of any security program is ***education***.
- The best technique to authenticate to a system is:
  To authenticate the person by ***something he knows*** and ***something he has***.
- Use ***SSH*** when connecting to devices.
- For secure SNMP traffic use ***SNMPv3***.
- If your IDS detect IP packets with ***IP Source Address/Port*** are equal to ***IP Destination Address/Port***, the packets should be dropped.
- Always delete the ***browser-chache***.

# CHECKLISTS

### *CEH - Check Abuse List*

https://www.abuseipdb.com/check/<x.x.x.x>
https://www.abuseipdb.com/check/124.65.18.102

### *LAN Security Self-Assessment*

http://www.utoronto.ca/security/lansass.htm//lansass

### *Generic Password Security Checklist*

http://delphi.colorado.edu/~security/users/access/goodprac.htm

### *TCP/IP Security Checklist*

http://ird.security.mci.net/check.html

### *Cisco IP Security Checklist*

http://www.cisco.com/c/en/us/solutions/small-business/resource-center/secure-my-business/network-security-checklist.html

### *Security Policy Checklist*

http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

# WIRELESS NETWORKING

## *WEP - Wired Equivalent Privacy*

In 2003 the Wi-Fi Alliance announced that **WEP** had been superseded by Wi-Fi Protected Access (**WPA**). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 have been deprecated
*Source: Wikipedia*

- Provides 64- and 128-bit encryption.
- See ***802.11***
- Significant ***flaws*** exist in the WEP algorithm.
- You should ***never use WEP*** encryption to protect a wireless network.

## *WPA - WiFi Protected Access*

- ***WPA2*** with ***802.1x*** authentication provides best security.
- Implements Temporal Key Integrity Protocol (***TKIP***).
- Does not provide an end-to-end security solution. It encrypts traffic only between a mobile computer and the nearest wireless access point. Once the traffic hits the wired network, it's in the clear again.
- WPA is designed to interact with 802.1x authentication servers.

## *WPA2 - WiFi Protected Access*

- Adds ***AES*** cryptography.
- Encryption level: 128 bit and ***CCMP***

## *WTLS - Wireless Transport Layer Security*

- Provides ***authentication***, ***encryption*** and ***data integrity*** for wireless devices.

## *IEEE 802.1x*

- Authenticates devices before allowing them to access the LAN.
- Implements identity-based networking on wired and wireless hosts by using client/server access control.
- The client runs a piece of software known as the ***supplicant***.

***Components:***

| | |
|---|---|
| **Client** | Supplicant<br>Communicates with the authentication server. |
| **Authenticator** | Switch as proxy between client and authentication server. |
| **Authentication server** | RADIUS |

# ANTIVIRUS

- VCloud Based
- Behaviour Based
- Heuristics Based

## *Anti-Virus Scanner für Linux*

| Name | Link | Preis |
|---|---|---|
| Network Associates Virus Scan | www.nai.com | $12’500.00 |
| H+BEDV AntiVir/X | http://www.hbedv.com/infos/prices.htm | €138.04 |

| | | |
|---|---|---|
| Sophos Sweep | http://www.sophos.com/products/software/antivirus/savunix.html | ?? konnte Programm aber downloaden |
| Kaspersky Lab AntiViral Toolkit Pro (AVP) | http://www.kaspersky.com/de/buyonline.html?chapter=944395 | $49.95 |
| CyberSoft VFind | http://www.cybersoft.com/products/vfind.shtml | $895.00 |
| CAI InoculateIT | http://www3.ca.com/Solutions/Product.asp?ID=3049 | ?? konnte Programm aber downloaden |
| F-Secure Inc. (former DataFellows) F-Secure AV | http://www.f-secure.com/estore/fsavlinuxwks.shtml | $80.00 |

### *AVAST*

- CZ: http://www.trendmicro.de
- OS: W95/NT

### *Avira AntiVir*

- Freeware

***Products:***

- AntiVir Personal Edition; W9x, NT, deutsch, ca. 4,1 MByte, H+BEDV
- AntiVir Vollversion: H+BEDV

### *Bitdefender*

- Freeware

### *ClamAV*

- See: **Antivirus Tool**
- Securing ownCloud
- ClamAV is an open-source, multi-platform ***antivirus*** which supports multiple file formats with file and archive unpacking.
- It detects multiple singnature languages and is the only antivirus program supported by ownCloud.
- It also has command line utilities for an on-demand file support with automatic signature updates.
- It is a versatile antivirus with multi-threaded daemon which makes it a great tool to keep your system secure.

### *Clamwin*

- See: **Antivirus Tool**
- **Source:** http://www.clamwin.com/
- Clamwin is a highly effective and widely used ***malware removal program*** which can detect and remove the latest variants of multiple malware.
- ClamWin is a Free Antivirus program for Microsoft Windows 10 / 8 / 7 / Vista / XP / Me / 2000 / 98 and Windows Server 2012, 2008 and 2003.

### *Cylance*

- See: **Antivirus Tool**
- Supplier: Paraben Corporation
- Source: paraben.com
- Virus, Worms and Trojan detection
- Advantage, very low CPU usage.

### *McAfee*

- US: https://www.mcafee.com

- OS: Microsoft Windows, Mac OS X, Linux
- Total Virus Defence für Unternehmen Network Associates (McAfee)
- Formerly known as ***Intel Security***, and ***Network Associates (NIA)***.

### *Norton Internet Security*

- See: http://www.symantec.ch

### *ScanGuard*

- Freeware

### *Symantec*

- Symantec AntiVirus Prod.

### *ThunderByte Antivirus (TBAV)*

- Norman ASA hat das Produkt übernommen.

### *Total AV*

- Source:www.totalav.com
- Freeware (Nicht wirklich, der Echtzeitschutz muss gekauft werden)

### *Trend Micro Products*

- USA: http://www.trendmicro.de
- OS: Windows/Linux

***Products:***
Trend Micro E-Mail VirusWall
Trend Micro FileScanner
Trend Micro InterScan VirusWall
Trend Micro ScanMail für cc:Mail / Lotus Notes / MS Exchange
Trend Micro ServerProtect für NT-Server / Novell NetWare
Trend Micro DeskTop VirusWall (ehem. PC-Cillin)
Trend Micro OfficeScan (Corporate / SBS)
Trend Micro Virus Control System

Vet Computer Associates, Sydney
Virex für Macintosh Dr Solomon's
virus utilities Windows 9x Ikarus Software, Wien
virus utilities Windows NT Ikarus Software, Wien
VirusScan Emergency für Windows 95 und 98 Dr Solomon's
VirusScan Toolkit für W9x, NT, DOS und OS/2 Dr Solomon's
VirusScan 4.x (VScan) für Win95/98, McAfee
VirusScan 5.x (VScan) für Win95/98, McAfee
VirusScan Deluxe 5.0 für W95/98/NT3.51/4.0/3.1x/DOS,OS/2, McAfee

### *Windows Defender Antivirus*

- Reached ***EOL,*** the replacement is called ***MS Security Essentials***.
- Previousely called ***MS AntiSpyware***
- ***Realtime*** malware protecten after first start of Windows.

### *Others*

AVG für W9x/NT, Grisoft

Clinic (VirusScan) McAfee.com
Command AntiVirus für Windows, Command Software Systems

F-Prot DOS, W9x/NT, engl., 2,3 MByte, Frisk Software International
F-Secure Anti-Virus 5 für Windows, Data Fellows

InocuLAN für Windows NT- Computer Associates
InocuLAN AntiVirus für Windows 95 - Computer Associates

InVircible für Windows, NetZ Computing

Panda Antivirus Platinum für W9x, NT, OS2, Panda Software
Global Virus Insurance für Unternehmen, Panda Software

Norman Virus Control (NVC) Norman ASA
Norton Antivirus für W9x, NT, 2000 Symantec
Norton Antivirus für Macintosh Symantec
Norton AV f. kleine Netzwerke Symantec

Sophos Anti-Virus for Windows NT/2000 Sophos GmbH
Sophos Anti-Virus for Windows 95/98 Sophos GmbH
Sophos Anti-Virus for Macintosh Sophos GmbH
Sophos Anti-Virus for Unix Sophos GmbH

KAOS AntiVirus

Michelangelo Anti-Virus Area
NCSA Anti-Virus Vendor Forum

# DOS-SECURITY

| | |
|---|---|
| BIOS-Passwort: | Kann von jedem deaktiviert werden, der physikalischen Zugang zum Rechner hat! |
| | CMOS-Batterie entfernen oder kurzschliessen.<br>Pgm: Password Capturing Utility<br>Amiecod, Ami.com, Aw.com |
| Tastatur Recorder: | Verzeichnis verbergen alt+2+5+5<br>keycopy, Playback, Phantom2, Keytrap |

# WINDOWS-SECURITY

**Microsoft Windows Security Checklist**

- http://kumi.kelly.af.mil/wincheck.html

PWL Password.
Path in System.ini. ( \windows ).
Boot with F5 or F8 abändern der System.ini etc.
GLIDE, dient zum knacken von PWL-Dateien ( http://morehouse.org/hin/blckrwl/hack/glide.zip )

**Crack:**

| | |
|---|---|
| ARJ-Archive | http://www.10pht.com/pub/blckrwl/hack/brkarj10.zip |
| MS-Excel | http://www.net-security.sk/crack/ostatne/excelCrack.zip |
| MS Word | http://www.net-security.sk/crack/ostatne/wpl.zip |
| ZIP-Archive | http://morehouse.org/hin/blckrwl/hack/fzc104.zip |

### *Schwachstellen*

OOB
Port 1031 Telnet auf 1031 + Müll senden
NTCrash WNT

### *WINDOWS NT*

- NT immer NTFS verwenden und alle Patches laden!

rdsik /s
c:\winnt/repair

ftp://ftp.iss.net/pub/lists/ntsecurity-digest.archive

Windows NT ist eine ausgezeichnete Server Plattform. Wie seine Entsprechungen ist jedoch auch Windows NT nicht von sich aus sicher. Um einen sicheren Server zu betreiben, müssen Sie drei Dinge tun:

- Die Patches laden
- Sicherheitstools/-methoden anwenden
- Die neuseten Entwicklungen verfolgen

## WINDOWS NT-SECURITY

**in Verbindung mit dem Internet und im Intranet:**
Alle Hinweise ohne Gewähr!
Sie sollten unbedingt vor der Installation eines Live-Systems an einer speziellen Maschine getestet werden!

**Oberste Regeln:**

- Jeder Administrator sollte unbedingt wissen, *was* auf seinem Server für Dienste angeboten werden. Das heisst, dass zumindest der Administrator wissen muss, welche Dienste eingerichtet sind und damit, welche möglichen Sicherheitsrisiken bestehen können.

- Es sollten nur die für den Betrieb des Servers unbedingt notwendigen Services angeboten werden. Jeder überflüssig angebotene Dienst kann wieder ein Sicherheitsrisiko in sich bergen. Die Dienste, die angeboten werden, sollten auch dokumentiert sein.

- Als Regel, von der ausgegangen wird, sollte angesetzt werden:
  **Alles, was nicht explizit erlaubt ist, ist verboten!**
  Nur mit diesem Ansatz kann sichergestellt werden, dass bei der Einrichtung der Maschine nicht vergessen wird, einen Dienst zu verbieten. Der Administrator befindet sich bei diesem Ansatzpunkt immer auf der 'sicheren Seite'. Es ist besser, dass interne Benutzer feststellen, dass ein benötigter Dienst u.U. nicht funktioniert als eine Öffnung aller Dienste, die dann auch in Richtung Internet angeboten werden.

- **Bennennen Sie den Usernamen des Administrators um:**
  Unter NT sind die einzelnen User-Accounts vor Angriffen in der Weise geschützt, dass sie nach einer festgelegten Anzahl falsch eingegebener Passworte gesperrt werden. Dieses gilt nicht für den Account 'Adminstrator'. Er kann im Normalfall nicht gelöscht, ausser Betrieb gesetzt oder wegen mehrfach falsch eingegebener Passworte gesperrt werden. Daher ist dieser Account, den es per Voreinstellung auf allen Systemen gibt, brute-force Angriffen auf diesem Bereich (z.B. Raten von Passworten mit Lexikon) ausgeliefert.
  Besser ist es, diesen Account umzubenennen: Dann ist für potentielle Angreifer neben dem Passwort zusätzlich der für die Administration eingerichtete Account herauszufinden (z.B. 8Hkm§kH&Vr!). Zum Umbenennen dieses Accounts ist in

der Menüauswahl des UserManagers die Option User>Rename auszuwählen und der neue Name einzugeben.
Bei Windows NT 4.0 kann mit Hilfe des Resource Kit der Administrations-Account gegenüber Angriffen aus dem Netzwerk geschützt werden, indem die Möglichkeit genutzt wird, auch diesen Account nach X falschen Passworten zu sperren - der Zugang zur Maschine ist in einem solchen Fall nur noch über die Console möglich.

- Löschen Sie alle Accounts, die für den Betrieb der Maschine nicht zwingend notwendig sind:
  Jeder Account, der auf einer Maschine eingerichtet ist, birgt wegen der Passwortproblematik ein potentielles Sicherheitsrisiko. Besonders gilt dieses für Maschinen, die für die Öffentlichkeit Dienste im Internet anbieten. Hier sollte neben dem für die Adminstration eingerichteten Account möglichst kein anderer eingerichtet sein - auch nicht der Gast-Account. Dieser wird bei der Default-Installation genauso wie der Administratior-Account eingerichtet.

- **Benutzen Sie das Dateisystem NTFS und** *nicht* **das FAT-System:**
  NTFS bietet neben der auch für FAT eingesetzten Möglichkeit, die freigegebenen Verzeichnisse zu schützen, zusätzlich die ACLs (Access Control Lists). Mit diesen können, ähnlich wie bei UNIX, die genauen Schreib- und Leserechte für Verzeichnisse und auch einzelne Dateien eingestellt werden. Damit lässt sich auch der Nur-Lese Zugriff auf einzelne Dateien verhindern. Und: Doppelt hält besser ;-)
  Wenn Sie bereits FAT einsetzen, können Sie bei x86-Systemen eine Boot-Partition einrichten, die dann unter NTFS läuft (CONVERT). Vorher sollte allerdings unbedingt ein Backup gemacht werden.
  Wichtig ist aber, dass Sie sich nicht alleine darauf verlassen können, dass der Zugriffschutz unter NT gewährleistet ist: Es gibt einige Tools, mit denen von einer DOS-Bootdiskette auf NTFS-Partitionen zugegriffen werden kann.

- **Legen Sie verschiedene NTFS Partitionen an:**
  Es sollten aus Sicherheitsgründen die NT Systemdateien nicht auf der gleichen Partition sein wie z.B. die Dateien, die vom Web Server abgerufen werden können. Gleiches gilt für die Dateien des FTP Servers oder CGI-Skripten.
  Falls ein Einbruch erfolgreich gewesen sein sollte, ist es leicht, auf der gleichen Partition in andere Verzeichnisse zu gelangen. Schwieriger ist es, als Einbrecher auf eine andere Partition bzw. Festplatte zu kommen.

- **Benutzen Sie ein reines TCP/IP Netzwerk und schalten Sie NetBIOS aus**
  Die Nutzung von NetBIOS, auch über TCP/IP, ist gefährlich, speziell wenn Ihr Netzwerk auch an das Internet angeschlossen ist. Alle freigegebenen Services sind im Prinzip für jede Maschine erlangbar, die über das Netzwerk erreichbar ist (also u.U. auch das gesamte Internet). Wenn es nicht vermeidbar ist, beides zu nutzen und Sie einen Firewall gegenüber dem Internet einsetzen, sollten die Ports 137/udp, 138/udp und 139/tcp nicht hindurchgelassen werden. Zusätzlich sollten Sie durch den Einsatz eines Proxy Servers die interne TCP/IP-Struktur des Netzwerkes verstecken.
  Wenn Sie NetBIOS nicht unbedingt brauchen, sollten Sie dieses auf jeden Fall komplett entfernen. Hierzu ist neben dem Löschen aller nicht benötigter Dienste auch gemeint, dass Sie den WINS Client sowie den TCP/IP NetBIOS Helper deaktivieren. Keine Sorge, wenn Sie über Systemsteuerung/Netzwerk vom NT die Meldung bekommen, dass kein Netzwerk installiert ist! Auf die Frage von NT, ob es jetzt installiert werden soll, einfach mit "nein" antworten und dann TCP/IP konfigurieren.

- **Vermeiden Sie möglichst, den FTP Serverdienst anzubieten**
  Gerade FTP Server bergen immer wieder Sicherheitsrisiken in sich. Ausserdem gibt bei einer Standardinstallation die Begrüssungsmeldung Aussenstehenden bereits Informationen über das System (z.B. welcher FTP Server, welches Betriebssystem). Damit können dann bekannte (Ihnen aber unbekannte) Sicherheitslücken für einen Einbruch genutzt werden. Zusätzlich ist bei vielen

FTP Servern die Anzahl der Versuche, mit Usernamen und Passwort in das System zu kommen, nicht beschränkt. Daher kann über FTP z.T. beliebig lange nach einer passenden Kombination gesucht werden. Wurde eine gefunden, ist das System offen - mit allen Folgen.
Wenn wirklich ein FTP Server notwendig ist, dann sollte sich dieser auf einer speziellen Partition befinden und im Root-Verzeichnis des Servers keine Schreibrechte für Benutzer eingerichtet sein. Besser wäre, den FTP Server auf einer dedizierten Maschine zu betreiben, die sich nicht direkt im internen Netzwerk des Unternehmens befindet.

- **Benutzen Sie den Web Server nicht als File Server**
  Auch Web Server können Sicherheitsrisiken in sich bergen. Falls auf die Maschine, auf der der Web Server läuft, eingebrochen werden sollte, sind damit gleichzeitig Ihre unternehmensinsternen Daten kompromittiert. Die Maschine mit dem öffentlichen Web Server sollte in einem Netzwerk betrieben werden, das vom internen Netzwerk durch einen Firewall oder zumindest einem Router mit entsprechenden Paketfiltern abgegrenzt ist.

- **Schalten Sie das Mapping für .bat- und .cmd-Dateien aus und benutzen Sie diese nicht als CGI-Skripten**
  Dieses gilt insbesonders, wenn Sie den IIS benutzen: Hier sind bereits einige Sicherheitslücken offengelegt worden.

- **Entfernen Sie Programme, die gefährlich werden können (z.B. rasdial.exe, telnet.exe, ftp.exe)**
  Jeder Serverdienst, der angeboten wird, kann Sicherheitsrisiken in sich bergen. Auch wenn heute das System nach dem neuesten Stand der Technik sicher ist, kann bereits Minuten später eine neue Sicherheitslücke bekannt sein. Daher sollten wirklich nur die notwendigsten Serverdienste angeboten und die Diskussionen über Sicherheit verfolgt werden.

- **Installieren Sie auf einer Maschine im Internet niemals Beispielprogramme**
  Hier sind in letzter Zeit einige Sicherheitslücken bekanntgeworden, durch die von aussen "eingestiegen" werden kann. Ein Beispiel hierfür ist der IIS: Wenn hier z.B. die Beispiele für asp's installiert sind, kann ein geschickter Besucher des Servers aus dem abgetrennten Bereich herauskommen und sämtliche Dateien, die sich auf der Maschine befinden, lesen.

- **Überwachen Sie die Maschine**

  Durch das Einschalten der Loggingmechanismen ist die Möglichkeit gegeben, die sich auf der Maschine ereignenden Vorkommnisse zu dokumentieren. Die Logs sollten regelmässig kontrolliert werden. Da Einbrecher meist versuchen, ihre in den Logfiles hinterlassenen Spuren zu verwischen, sollten kurz aufeinander folgende, regelmässige Backups dieser Dateien erfolgen. Die Lagerung der gesicherten Dateien sollte aus den obigen Gründen nicht auf der gleichen Maschine geschehen.

- **Verlassen Sie sich nicht darauf, dass alle Angriffe von aussen kommen**
  Es sind im Internet sowie im Buchhandel sehr viele Tools bekannt, die Sicherheitslücken auch für Laien ausnutzbar machen. Der Anteil "interessierter Mitarbeiter", die im Grunde nicht wissen was sie tun, ist sehr hoch und keinesfalls zu unterschätzen. Auch im Intranet sollten die Maschinen so sicher wie möglich aufgesetzt sein. Starten Sie als Administrator selber derartige Tools und beheben Sie die gefundenen Sicherheitslücken - bevor ein Mitarbeiter von Ihnen oder gar ein Unbekannter von aussen dieses tut!

# UNIX-SECURITY

**Zitat aus Hacker's Guide:**
Ein Unix-Netzwerk zu sichern, ist sogar für erfahrene Anwender eine furchteinflössende Aufgabe. Seltsamerweise sind heutzutage sogar nicht Unix vertraute Anwender bereit, dies zu versuchen.

Trotz hervorragender Tools ist Sicherheit in Unix nur schwer zu erreichen (Hackers Guide Seite 57)

- Physikalische Sicherheit
- Sicherheit an der Konsole
- Passwortsicherheit
- Patches
- Verschlüsselte Passwörter
- Starke Zugriffskontrollen zu Dateien und Directories
- Authentifizierungsverfahren auf Systemebene
- Raffinierte Systemeinrichtungen zur Protokollierung
- Sicherheitsüberwachungstools
- Systemprotokollierungs-Tools
- Intrusion-Detection-Tools (Tools zum Aufspüren unerlaubten Eindringens)
- Many Unix operating systems store encrypted versions of a user's password in the: <***etc/passwd***> file.

Datei: passwd Feld: Login-ID, Passwort Verschlüsselungsprozess: crypt(3)

## *Physikalische Sicherheit*

- Eine Grundlegende Tatsache bei der Computersicherheit ist, dass, wenn der Rechner selbst nicht physikalisch sicher ist, das ganze System nicht mehr als sicher angesehen werden kann.
- Ein Nutzer mit physikalischem Zugang zum Rechner kann ihn anhalten, ihn im privilegierten Modus wieder hochfahren, die Festplatte austauschen oder verändern, Trojanische Pferde einschleusen oder eine Vielzahl anderer unerwünschter (und schwer zu verhindernder) Aktionen durchführen.
- Kritische Datenübertragungsverbindungen, wichtige Server und andere wichtige Rechner müssen an physikalisch sicheren Standorten stehen.

## *FTP*

Kapitel: 18.11
Wenn man anonymes FTP auf demselben Rechner erlaubt wie der Web-Server läuft, kann ein Eindringling eine Datei im "Anonymous-FTP-Bereich" platzieren und den http-Server dazu bringen, sie auszuführen.

Attacken: FTP-Bounce-Attacke

Test: **telnet 21**
Befehl: **SITE_EXEC** Falls die Shell angezeigt wird gibt es ein Sicherheitsproblem!

## *TFTP*

- ( Kapitel: 18.12.1 )
- Der beste Rat, den ich Ihnen zu TFTP geben kann ist, es zu deaktivieren. TFTP ist ein selten genutztes Protokoll und birgt erhebliche Sicherheitsrisiken, selbst wenn Sie ein als sicher angesehen Version verwenden.

Securing "Internet Information Servers" Leitfaden:
- http://ciac.llnl.gov/ciac/documents/CIAC-2308_Securing_Internet_Information_Servers.pdf

## *Hoch Privilegierte Accounts*

Root(UNIX)
QSECOFR(AS400),Administrator (NT)
Supervisor(NOVELL), und Operator

## *Shellshock*

- Shellshock ist eine Sicherheitslücke - oder eine Familie von Sicherheitslücken, CVE-Nummern CVE-2014-6271, …-7169, -7186, -7187, -6277, -6278 - in der Unix-Shell Bash.
- In der Bash kann der Wert einer Zeichenkettenvariablen eine Funktionsdefinition enthalten.
- Durch die Sicherheitslücke kann nach der Auswertung einer solchen Variablen ungeprüft Programmcode ausgeführt werden.

# CHFI - Computer Forensics in Today's World

Exam 312-49
Total 1458 pages

Computer forensics refer to a ***set of methodological procedures and techniques*** that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal and/or administrative proceeding.

Organizations need to employ the services of a ***computer forensics agency*** or ***hire a computer forensics expert*** to guard against computer incidents or solve crimes that involve the use of computers and related technologies.

***Forensic readiness*** refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs.

**O.S.C.A.R.**

- Obtain information: Who what, when, where …
- Strategize: What evidence may exist; how to collect it (legally)
- Collect Evidence: Capture traffic, copy, Capinfos
- Analyze: Filter, extract, insert comments
- Report: Clear and concise, easy-to-understand (if possible)

***Objectives***

- To track and prosecute perpetrators of a cyber crime
- To gather evidence of cyber crimes in a forensically sound manner
- To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
- To minimize the tangible and intangible losses to the organization
- To protect the organization from similar incidents in future

***Process***

- The forensic examiner must make ***duplicate copies*** of the original evidence and start by ***examining only the duplicates***.

***Locard's Exchange Principle***

- According to Locard's Exchange Principle, "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave".

***Sources***

Computer Technology Investigators Network ➔ http://www.ctin.org
High Technology Crime Investigation Association ➔ https://www.htcia.org

## *ETI - Enterprise Theory of Investigation*

- Has become the ***standard investigative model*** used by the FBI when conducting investigations against major criminal organizations.

# CHFI - Computer Forensics Investigation Process

The ***computer forensics investigation process*** includes a ***methodological approach*** for preparing for the investigation, collecting and analyzing digital evidence, and managing the case right from the time of reporting to the conclusion.

- ❑ The investigators must follow a repeatable and well documented set of steps such that every iteration of analysis provides the same findings.
- ❑ The forensics investigation process must comply with local laws and established standards

***PHASES***
- Pre-investigation Phase
- Investigation Phase
- Post-investigation Phase

## *CFL - Computer Forensics Lab*

- A Computer Forensics Lab (CFL) is a location designated for conducting computer-based investigation with regard to the collected evidence.

***Required Accreditations***
- ISO/IEC 17025 Accreditation
- ASCLD/LAB Accreditation

***EQUIPMENT***
- ❑ Two forensic workstations and one ordinary workstation with Internet connectivity.
- ❑ Take care for humidity, airflow, ventilation, and room temperature.
- ❑ One entrance, video observed.
- ❑ Log register: Name, date and time of visit
- ❑ Badges for visitors.
- ❑ Intrusion alarm system.
- ❑ Fire extinguishers within and outside the lab.
- ❑ Photocamera

***ROLES***
- lab coordinator
- lab director
- forensic technician
- forensic analyst
- forensic scientist
- Photographer
- Incident Responder
- Decision Maker
- Incident Analyzer
- Evidence Examiner/Investigator
- Evidence Documenter
- Evidence Manager
- Evidence Witness
- Attorney
- System-/Network-Administrator

***Computer Forensics Workstation***
- Create the toolkit before commencing an investigation, as the investigating team needs to be familiar with these tools before performing the investigation.

- ❑ High Speed CPU
- ❑ >= 8 GB RAM
- ❑ DVD-ROM & Blu-ray
- ❑ IDE, SCSI, USB, FireWire
- ❑ LAN/WAN card
- ❑ Tape drive, USB drive, and removal drive bays.
- ❑ 2 hard drives for loading two different OSs on each (Windows, Linux)
- ❑ Support hardware-based local and remote network drive duplication
- ❑ Validate the image and the file's integrity
- ❑ Identify the date and time of creation, access and modification of a file
- ❑ Identify deleted files
- ❑ Support removable media

- ❑ Isolate and analyze free drive space

***Computer Forensics Hardware***

- Create the toolkit before commencing an investigation, as the investigating team needs to be familiar with these tools before performing the investigation.

- ❑ Specialized cables
- ❑ Write-blockers
- ❑ Drive duplicators
- ❑ Archive and Restore devices
- ❑ Media sterilization systems
- ❑ Paraben's First Responder Kit: https://www.paraben.com

***Computer Forensics Software***

- Create the toolkit before commencing an investigation, as the investigating team needs to be familiar with these tools before performing the investigation.

- ❑ Operating Systems
- ❑ Data discovery tools
- ❑ Password-cracking tools
- ❑ Acquisition tools
- ❑ Data analyzers
- ❑ Data recovery tools
- ❑ File viewers (Image and Graphics)
- ❑ File type conversion tools
- ❑ Security and Utilities software
- ❑ Paraben's Examination SW: https://www.paraben.com

## *CHFI FACTS*

***Copying HD***

- ❑ Use a brandnew HD to copy on it.
- ❑ Make bit by bit copy.
- ❑ Create hash valus of the original and the copy (must match).

***Social Medias***

Facebook, WhatsApp, Twitter, LinkedIn, Google+, Snapchat etc.
RAM, browser cache, page files, unallocatedclusters, and system restore point of a computer.
Tools: Netvizz, twecoll, divud, Digitalfootprints, Netlytic, X1 Social Discovery, Facebook Forensic Software, H&A forensics, Geo360 , Navigator by LifeRaft Social, Emotive, etc.

***Dropbox***

W10
C:\Users\Admin\AppData\Roaming\
C:\Program Files (x86) or C:\Program Files

***Startup Folders***

Windows: \system32
Linux: rc.local

## *FIRST QUESTIONS*

1. What happened?
2. Who is the incident manager?
3. What is the case name or title for the incident?
4. What is the location of the incident?
5. Under what jurisdiction are the case and seizure to be conducted?
6. What is to be seized (make, model, location, and ID)?
7. What other work will need to be performed at the scene (e.g., full search and evidence required)?
8. Is the search and seizure required to be overt or covert, and will local management be informed?

### *METHODOLOGY*

1. First response
2. Search and Seizure
3. Collect the Evidence
4. Secure the Evidence
5. Data Acquisition
6. Data Analysis
7. Evidence Assessment
8. Documentation and Reporting
9. Testify as an Expert Witness

## CHFI - Understanding Hard Disks and File Systems

HDD - Hard Disk Drive
SSD - Solid-state Drive
CHS - Cylinders, heads and sectors
LBA - Logical Block Address
GUID - Global Unique Identifier

- Is a 128-bit unique reference number used as an identifier in computer software

GPT - GUID Partition Table

- GPT allows users to partition disks larger than 2 terabytes
- It allows users to have 128 partitions in Windows using GPT partition layout
- GPT partition and boot data is more secure than MBR, as GPT stores data in multiple locations across the disk
- It use Cyclic Redundancy Check (CRC) to ensure data integrity
- Uses CRC32 checksums that detect errors in the header and partition table

UEFI - Unified Extensible Firmware Interface

- Replace legacy BIOS firmware interfaces.
- UEFI uses partition interfacing systems that overcome the limitations of the MBR partitioning scheme.

MBR - Master Boot Record

- Refers to a hard disk's first sector or sector zero that specifies the location of an operating system for the system to load into the main storage.
- Backing up the MBR In UNIX/Linux, dd helps to create backup and restore the MBR.
- Back up the MBR
  dd if=/dev/xxx of=mbr.backupbs=512 count=1
- Restore the MBR
  dd if=mbr.backup of=/dev/xxx bs=512 count=1

Slack space

- Is the wasted area of the disk cluster lying between end of the file and end of the cluster when the file system allocates a full cluster to a file, which is smaller than the cluster size.

Lost cluster

- Is a FAT file system error that results from in what manner the FAT file system allocates space and chains files together.
- It is mainly the result of a logical structure error and not a physical disk error.

Bad sectors

- Refer to the portions of a disk that are unusable due to some flaws in them and do not support the read or write operations.

EFS - Encrypting File System

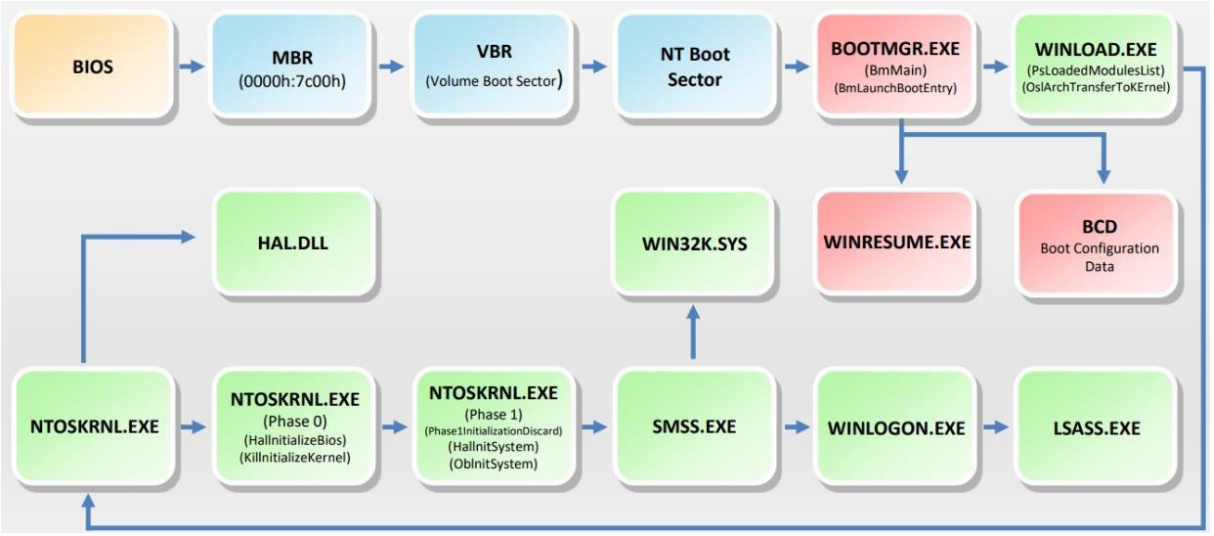
***File systems***
FAT, FAT32, NTFS, EXT, EXT2, 3 and 4, EFS

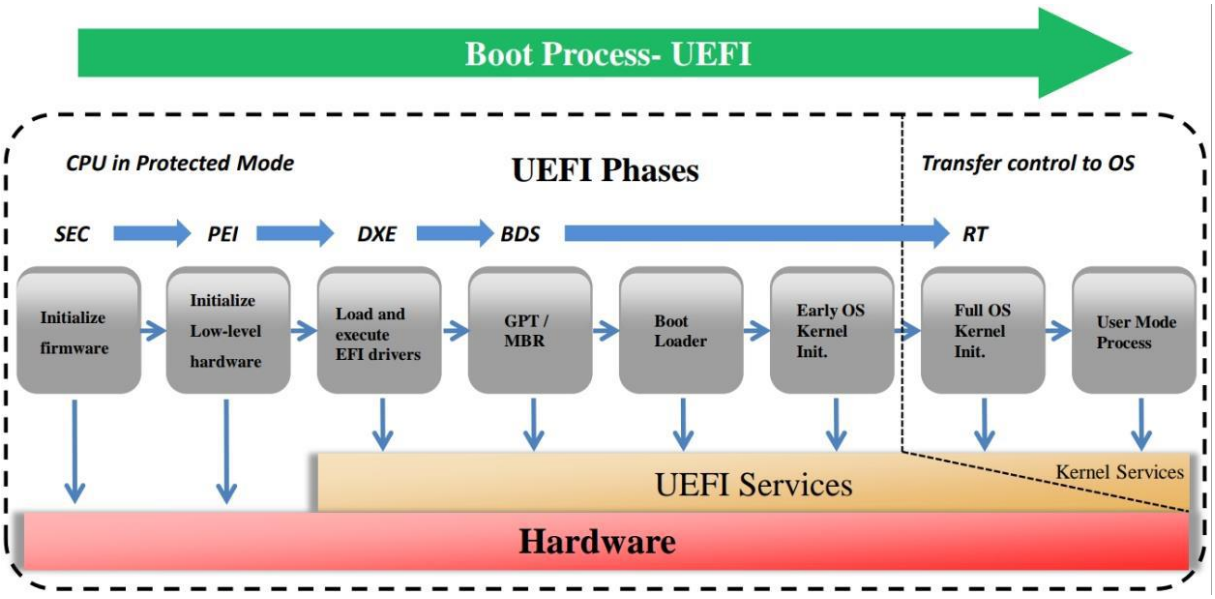
### *Essential Windows System Files*

| FILE NAMES | DESCRIPTION |
|---|---|
| Ntoskrnl.exe | Executive and kernel |
| Ntkrnlpa.exe | Executive and kernel with support for Physical Address Extension (PAE) |

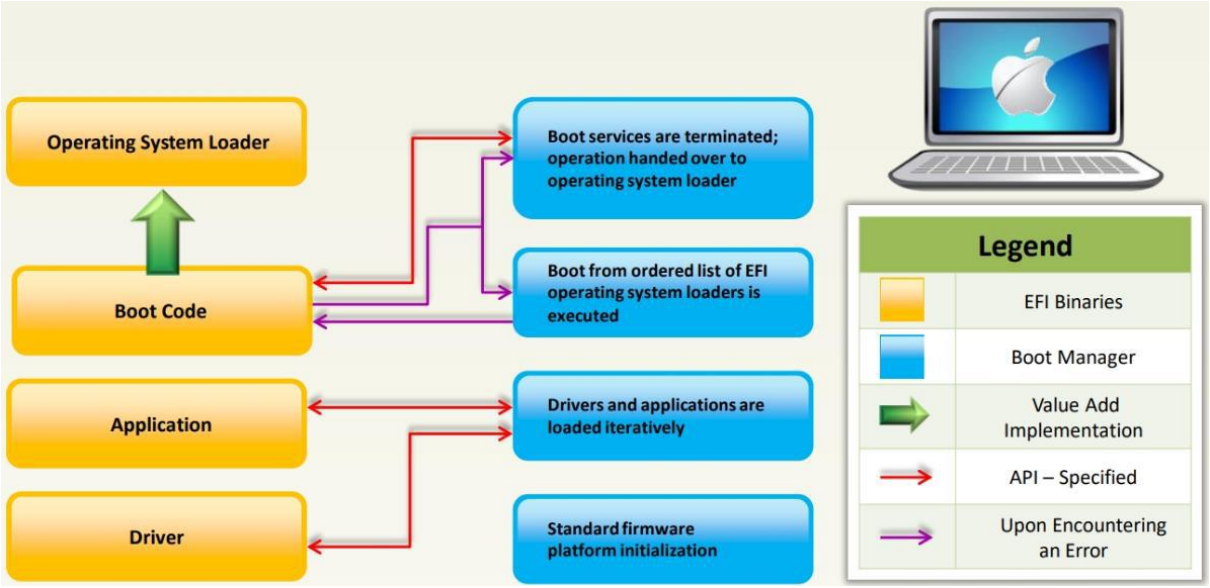
| | |
|---|---|
| Hal.dll | Hardware abstraction layer |
| Win32k.sys | Kernel-mode part of the Win32 subsystem |
| Ntdll.dll | Internal support functions and system service dispatch stubs to executive functions |
| Kernel32.dll | Win32 subsystem DLL files |
| Advapi32.dll | |
| User32.dll | |
| Gdi32.dll | |
| DHCP logs | ***C:\Windows\System32\dhcp*** folder on DHCP servers |

## *Windows Boot Process*

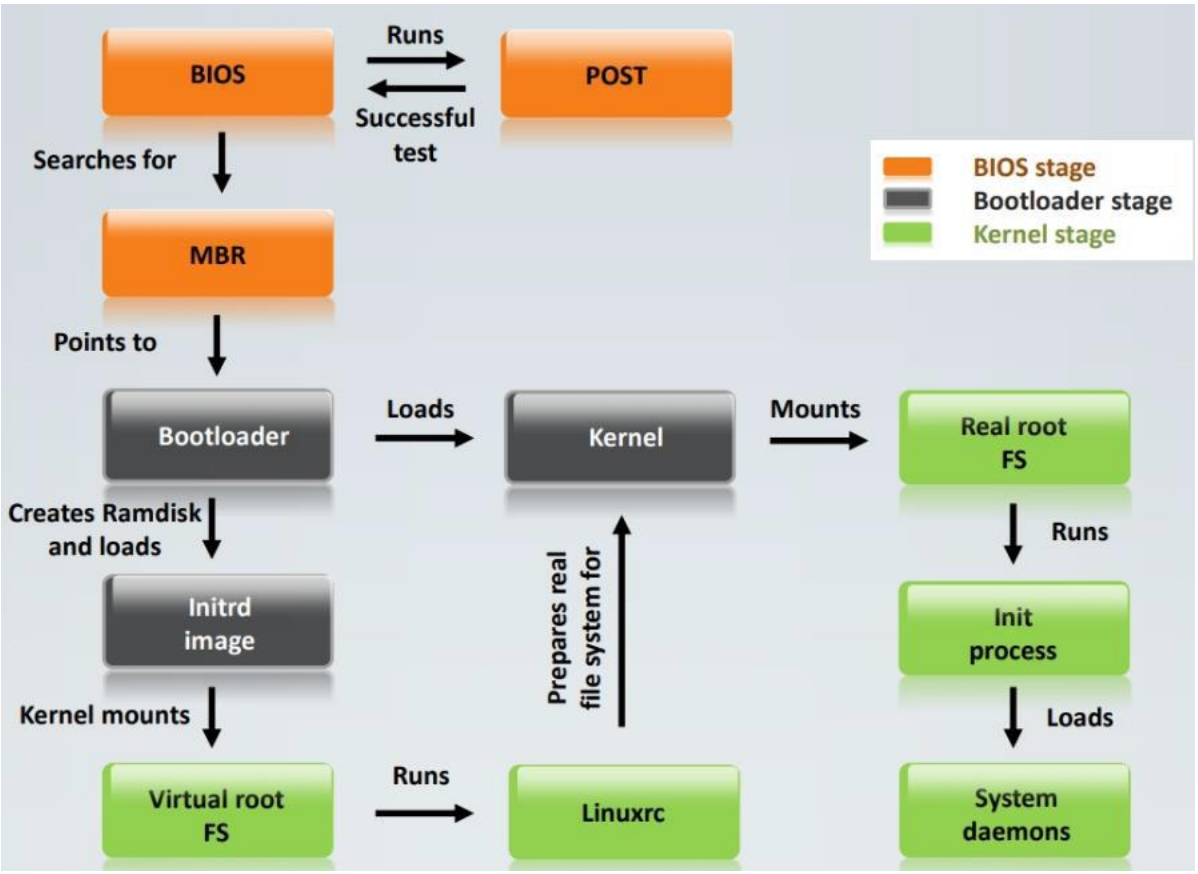



## *Macintosh Boot Process*




## *Linux Boot Process*



### *NTFS System File*

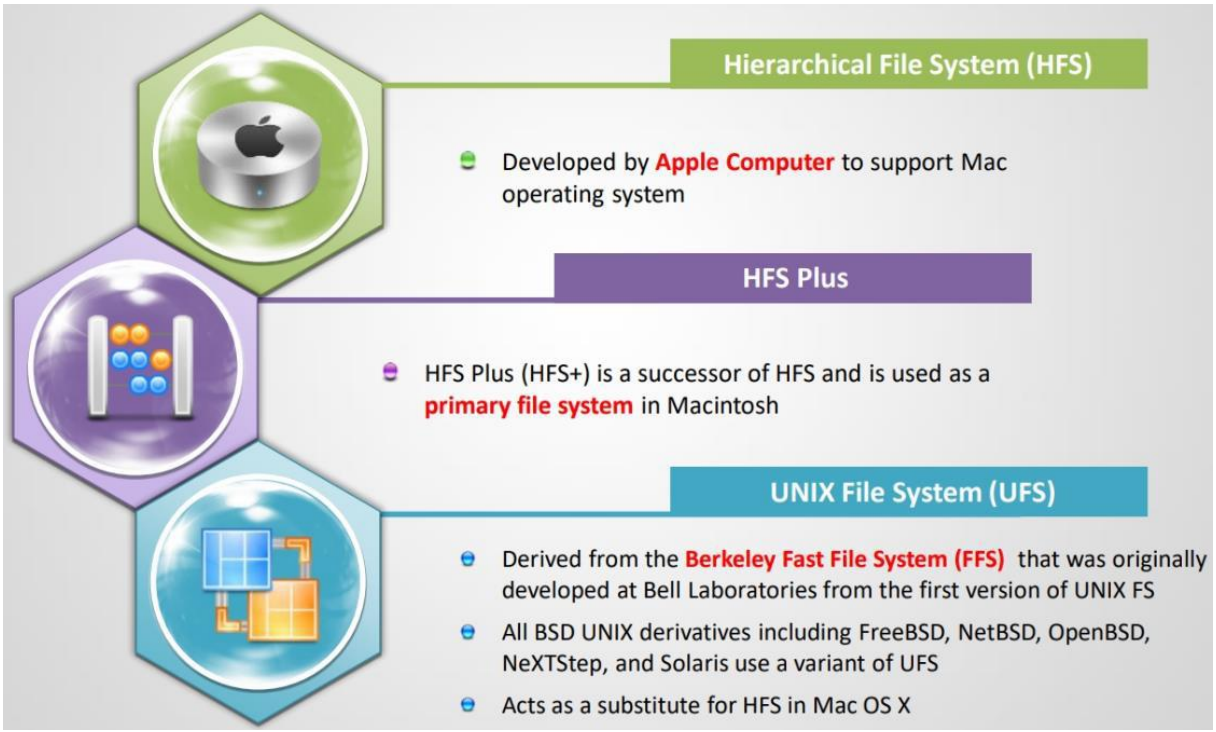
| File Name | Description |
|---|---|
| $attrdef | Contains definitions of all system-and user-defined attributes of the volume |
| $badclus | Contains all the bad clusters |
| $bitmap | Contains bitmap for the entire volume |
| $boot | Contains the volume's bootstrap |
| $logfile | Used for recovery purposes |
| $mft | Contains a record for every file |
| $mftmirr | Mirror of the MFT used for recovering files |
| $quota | Indicates disk quota for each user |
| $upcase | Converts characters into uppercase Unicode |
| $volume | Contains volume name and version number |

### *Linux File System*

FHS - Filesystem Hierarchy Standard

| Directory | Description |
|---|---|
| /bin | Essential command binaries. Ex: cat, ls, cp. |
| /boot | Static files of the boot loader. Ex: Kernels, Initrd |
| /dev | Essential device files. Ex: /dev/null |
| /etc | Host-specific system configuration files |
| /home | Users' home directories, holding saved files, personal settings, etc. |
| /lib | Essential libraries for the binaries in /bin/ and /sbin/ |
| /media | Mount points for removable media |
| /mnt | Temporarily mounted filesystems |
| /opt | Add-on application software packages |
| /root | Home directory for the root user |
| /proc | Virtual file system providing process and kernel information as files |
| /run | Information about running processes. Ex: running daemons, currently logged-In users |
| /sbin | Contains the binary files required for working |
| /srv | Site-specific data for services provided by the system |
| /tmp | Temporary files |
| /usr | Secondary hierarchy for read-only user data |
| /var | Variable data. Ex: logs, spool files, etc. |

### *MAC OS X File Systems*




### *Oracle Solaris 11 File System ZFS*

- ZFS is the default **disk-based and root file system** used in the Oracle Solaris 11
- It **provides a simple management interface**, which is robust, scalable, and easy to administer

**Features:**

- ZFS Pooled Storage Model
- Data integrity Model
- Simplified Administration
- Copy-on-Write transactional model
- End-to-End Checksums
- Self-Healing Data
- Unparalled Scalability
- ZFS and Solid-State Storage
- Snapshots and Clones
- Encryption
- Deduplication
- Compression

**Benefits:**

- Simplifies and reduces storage management tasks
- Increases storage agility and data protection
- Delivers superior performance and availability

### *File Type Signatures*

- See: WinHex
- Can show all signatures

| | |
|---|---|
| ACI | |
| AIFF | |
| BMP | 42 4D |
| DOC | |
| DOCX | |

| | |
|---|---|
| EPUB | |
| FLV | |
| GIF | 47 49 46 38 |
| JNT | |
| JPEG | FF D8 FF |
| MP3 | |
| MP4 | |
| OGG | |
| PNG | 89 50 4E |
| PDF | 25 50 44 46 |
| PPT | |
| PPTX | |
| RAR | |
| WAV | |
| WMV | |
| XLS | |
| XLSX | |
| ZIP | |

# CHFI - Data Acquisition and Duplication

***Data Collection Priority***

1. Registers, cache
2. Routing table, process table, kernel statistics, and memory
3. Temporary file systems
4. Disk or other storage media
5. Remote logging and monitoring data related to the target system
6. Physical configuration, network topology
7. Archival media

***Live Data Acquisition***

- One chance to collect!

***Includes***

- Registries
- Cache
- RAM

***Linux***

```
dd if/dev/mem of/home/sam/mem.bin bs1024
dcfldd if=/dev/sdb of=sdb_image.img
```

***Static Data Acquisition***

- Acquisition of data that remains unaltered even if the system is powered off.
- Create two copies bit-by-bit of the original HD
- Use brand new HD's so you do not have to sanitize them.

***Includes***

- Temporary (temp) files
- System registries
- Event/system logs
- Boot sectors
- Web browser cache
- Cookies
- Hidden files

***AFF - Advanced Forensics Format***

- AFF is an open source data acquisition format that stores disk images and related metadata.
- The aim was to make a disk imaging format that could not lock users into a proprietary format.
- The AFF File extensions are ***.afm*** for AFF metadata and ***.afd*** for segmented image files.
- There are no AFF implementation restrictions on forensic investigators, as it is an open source format, but it can limit its analysis.
- AFF supports two compression algorithms: 1) zlib, faster but less efficient and 2) LZMA, slower but more efficient.
- The actual AFF is a single file which has segments with drive data and metadata.
- AFF file contents can be compressed and uncompressed.
- AFFv3 supports AFF, AFD, and AFM file extensions.

***gfzip - Generic Forensic Zip***

- gfzip file format is usable for the compressed yet randomly accessible storage of disk image data for computer forensics purposes.

# CHFI - Defeating Anti-forensics Techniques

Video: Module 5 DONE
Weiterlesen: 614 DONE
Lab:

## *Anti-Forensics Techniques*

- Data/File Deletion
- Password Protection
- Steganography
- Data Hiding in File System Structures
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption
- Encrypted Network Protocols
- Program Packers
- Rootkits
- Minimizing Footprint
- Exploiting Forensics Tool Bugs
- Detecting Forensics Tool Activities

***FAT File System***

- The OS replaces the first letter of a deleted file name with a hex byte code : ***E5h***

***NTFS File System***

- When a user deletes a file, the OS marks the file as deleted in the ***master file table (MFT)***

***Recycle Bin***

Drive:\$Recycle.Bin
Drive:\RECYCLED
Drive:\RECYCLER

***Desktop.Ini***

- If the Desktop.ini file is not present or is damaged, you can re-create it by adding the following information to a blank Desktop.ini file:
  [.ShellClassInfo]CLSID={645FF040-5081-101B-9F08-00AA002F954E}

***Cleartext Passwords***

HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft \Windows NT\ CurrentVersion\ Winlogon

***Microsoft Authentication***

SAM
    c:\windows\system32\config\SAM
    %SystemRoot%/system32/config/SAM
NTLM
Kerberos

***AFT - Anti-forensics tools***

Have the capability to change their behavior on detecting the use of CFT.
Ex: A Worm may not propagate if it discovered that the network is under surveillance

# CHFI - Operating System Forensics

- "Operating System Forensics" refers to the process of finding, extracting and analyzing evidences present in the operating system of any computerized device used by the victim, or suspected computer system involved in any security incident.
- Most commonly used operating systems include ***Microsoft Windows***, ***Linux***, and ***MAC***.
- They are often the most common target and source of criminal activities.

## *Windows Forensics*

### *Collecting Volatile Information*

- The investigators follow the ***Locard's Exchange Principle*** and collect the contents of the RAM right at the onset of investigation, so as to minimize the impact of further steps on the integrity of the contents of the RAM.
- Investigators are well aware of the fact that the tools they are running to collect other volatile information cause ***modification of the contents of the memory***.

- ❑ System time
  date /t & time /t
  net statistics workstation
  C++
  void GetSystemTime(
  LPSYSTEMTIME lpSystemTime
  );

- ❑ Logged-On user(s)
  PsLoggedOn
  net sessions
  LogonSessions

- ❑ Open files
  net file
  PsFile
  Openfiles

- ❑ Network information
  nbtstat -c
  nbtstat -a <IP>
  netstat -ano
  netstat -r

- ❑ Network connections

- ❑ Network status
  Ipconfig /all
  PromiscDetect tool
  Promqry too

- ❑ Process information
  TaskManager
  Tasklist /V
  Pslist
  pslist -x
  Listdlls
  listdlls64
  Handle
  Process Explorer (procexp.exe, procexp64.exe)
  PMDump
  ProcDump
  Process Dumper (PD)
  Memory Dump

- %SystemRoot%\Memory.dmp
- %SystemRoot%\Minidump directory
Dumpchk
EProcess block
- Microsoft Debugging tools
- LiveKD.exe
Lsproc.pl
Lspd.pl
Lspi.pl
pmdump.exe
Process Dumper (pd.exe)
Userdump.exe
adplus.vbs
BinText
Handle.exe
listdlls.exe
Volatility Tool

- ❑ Print Spool Files
  C:\Windows\System32\spool\PRINTERS*.SHD
  C:\Windows\System32\spool\PRINTERS*.SPL

- ❑ Clipboard
  Free Clipboard Viewer

- ❑ Process-to-port mapping
- ❑ Mapped drives
- ❑ Shares
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanman Server\Shares

- ❑ Clipboard contents
- ❑ Service/driver information
  wmic

- ❑ Command history
  doskey /history

***Collecting Non-Volatile Information***

- ❑ Examine File Systems
  dir /o:d
  Check Registry:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown → pagefile.sys
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\"NTFSDisableLastAccessUpdate"
  fsutil behavior query disablelastaccess
  Autoruns Tool
  Fsutil Tool

- ❑ Microsoft Security ID (SID)
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

- ❑ Microsoft Edge Browser
  ***ESE database:***
  \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxx\AC\MicrosoftEdge\User\Default\DataStore\ Data\nouser1\xxxxx\DBStore\spartan.eb
  ***Edge cached files location:***
  \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\
  ***Edge last active browsing session data location:***
  \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Ac tive\

Edge stores history records
Cookies, HTTP POST request header packets and downloads in:
\Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat If the last browsing session open was in PrivacIE mode then the browser stores these recordsin:
\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge
\User\Default\Re covery\Active\{browsing-session-ID}.dat

- ❑ Computer Name
  HKEY_LOCAL_MACHINE\SYSTEM\Cu rrentControlSet\Control\Comp
  uterName\ActiveComputerName
- ❑ Shutdowntime
  HKEY_LOCAL_MACHINE\SYSTEM\Contro lSet001\Control\Windows
- ❑ Product Information
  HKEY_LOCAL_MACHINE\SOFTWARE\Microso ft\Windows NT\CurrentVersion
- ❑ Time Zone
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- ❑ SSIDs
  SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{GUID}
- ❑ Connected Devices
  DevCon Tool

- ❑ Slack Space
- ❑ Web Cache
  Windows Thumbcache thumbcache.db
  - C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\Explorer
  - Thumbcache Viewer
  - ThumbsDisplay

- ❑ VHD - Virtual Hard Disk

- ❑ USB Devices
  HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\USBSTOR
  USBDeview - Tool

- ❑ Cookies
  ChromeCookiesView

- ❑ Temporary Files
- ❑ Volume Shadow Copy Service-based backup (VSS)
  Internet Evidence Finder (IEF) - Tool

- ❑ Autostart Files
  AutoRuns - Tool

- ❑ Most Recently Used (MRU) list
  HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\ Windows\CurrentVersion
  \Explorer\RecentDocs
  HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\RunMRU
  HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\TypedURLs
  HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\ComDlg32
  \OpenSavePidIMRU
  HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\FileExts
  HKEY_CURRENT_USER\Software\Microsoft \Windows\CurrentVersion\Explorer\ Map
  Network Drive MRU
  HKEY_CURRENT_USER\Software\Microsoft \Windows\CurrentVersion\Explorer\
  MountPoints2
- ❑ Metadata Analysis
  Metashield Analyzer - Tool

***Windows Memory Analysis***

- ❑ Virtual Memory
  X-Ways Forensics Tool

- ❑ Hibernate Files
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power
- ❑ Pagefile.sys
- ❑ Windows Search index
  Passware Search Index Examiner
- ❑ Hidden Partition
  Partition Logic
  Partition Find & Mount
- ❑ Hidden ADS Streams
  Stream Armor tool

***Windows Registry Analysis***

- ❑ ProDiscover
- ❑ RegRipper
- ❑ Restore Point Registry
  HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore
  Rp.log - Tool
  change.log - Files
- ❑ Prefetch Files
  HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\Session Manager\Memory Management\PrefetchParameters

***Event Logs Analysis***

- ❑ Psloglist Tool
- ❑ Copy the event log files ***(.evt files)*** themselves off the system
- ❑ wevtutil - Tool
- ❑ C:\Windows\System32\winevt\Logs

Metadata Investigation
Windows File Analysis

***Cache, Cookie, and History Analysis***

- ❑ Cache Location:
  C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2
- ❑ Cookies Location:
  C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite
- ❑ History Location:
  C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\places.sqlite
- ❑ MZHistoryView - Tool
- ❑ MozillaCacheView - Tool
- ❑ MozillaCookiesView - Tool
- ❑ MozillaHistoryView - Tool
- ❑ C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default
- ❑ ***Google Chrome <Internet Cache>***
  *Tip : Use CCleaner to analyze*
  C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache
  C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Storage
  C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\File System
  C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Service Worker
  …
- ❑ Microsoft Edge
  C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
  C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies
  C:\Users\Admin\AppData\Local\Microsoft\Windows\History
- ❑ IE
  IECacheView - Tool
  IECookiesView - Tool
- ❑ BrowsingHistoryView - Tool

## *Linux Forensics*

***dmesg***

- The command dmesg is the short for display message or 'Driver Message'.
- The command displays the kernel ring buffers, which contains the information about the drivers loaded into kernel during boot process and error messages produced at the time of loading the drivers into kernel.
- These messages are helpful in resolving the restoring the device's driver issues.

***fsck***

- The command fsck, is meant for File System Consistency Check.
- It is a tool to check the consistency of Linux file system and repair.

***Stat***

- Displays file or file system status.

***history***

- The command history checks and lists the Bash shell commands used.
- This command helps the users for auditing purposes.

***mount***

- The command mount causes mounting of a file system or a device to the directory structure, making it accessible by the system.

***pstree***

- Displays the processes on a system in the form of a tree

***top***

- Displays system summary information as well as a list of processes or threads Linux kernel is currently managing

***ps***

- Used to report the status of current process

***grep***

- Searches for presence of text or an expression or pattern in files

***pgrep***

- Stands for "Process-ID Global Regular Expressions Print", searches through the current processes and lists the process IDs which match the selection criteria to stdout

***kill***

- Terminates the processes without logging out or rebooting the system

***file***

- Displays the type of data contained in a computer file

***su***

- Allows user to run a command with substitute user and group ID

***dd***

- Copies a file, converts and formats it according to the operands

***ls***

- Lists directory contents

***Useful Commands:***

```
df -h
uname -a
sudo su
lshw -short
```

w
last -a
netstat
ifconfig -a
`lsblk`
lshw
lsof
lsmod
aureport
id root
ausearch
arp
gedit <file>

| Log Location | Description |
|---|---|
| /var/log/auth.log | System authorization information, including user logins and authentication mechanism |
| /var/log/kern.log | Initialization of kernels, kernel errors or informational messages sent from kernel |
| /var/log/faillog | Failed user login attempts |
| /var/log/lpr.log | Stores printer logs |
| /var/log/mail.* | All mail server message logs |
| /var/log/mysql.* | MySQL server logs |
| /var/log/apache2/* | Apache web server logs |
| /var/log/apport.log | Application crash report / log |
| /var/log/lighttpd/* | Lighttpd web server log files directory |
| /var/log/daemon.log | Running services such as squid, ntpd, etc. |
| /var/log/debug | Debugging log messages |
| /var/log/dpkg.log | Package installation or removal logs |
| /var/log/messages | Global system messages |
| /var/log/dmesg | Kernel ring buffer information |
| /var/log/cron | Information about the cron job in this file |
| /var/log/user.log | All user level logs |
| /var/log/lastlog | Recent login information |
| /var/log/boot.log | Information logged on system boots |

## *MAC Forensics*

# CHFI - Network Forensics

- Network forensics is the implementation of sniffing, recording, acquisition, and analysis of network traffic and event logs to investigate a network security incident.

***Most Common Network Attacks***
- Eavesdropping
- Data Modification
- IP Address Spoofing
- Denial of Service Attack
- Man-in-the-Middle Attack
- Packet Sniffing
- Enumeration
- Session Hijacking
- Buffer Overflow
- Email Infection
- Malware attacks
- Password-based attacks
- Router Attacks

***Most Common Wireless Network Attacks***
- Rogue Access Point Attack
- Client Mis-association
- Misconfigured Access Point Attack
- Unauthorized Association
- Ad Hoc Connection Attack
- HoneySpot Access Point Attack
- AP MAC Spoofing
- Jamming Signal Attack

***Rule 803, Federal Rules of Evidence***
A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regulary conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or a statute permitting certification, unless the source of information or the methode of circumstances of preparation indicate lack of trustworhiness.

***Jamming Signal Attack***
- A kind of ***Denial of Service attack (DoS)***, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on.

  **Countermeasure:**
  1. Power: Speak louder.
  2. Tightening: Try to use directional radio beams.
  3. Frequency hopping: Switch frequencies over a large range of possible frequencies.

  ...

# CHFI - Investigating Web Attacks

SQL Injection
Cross Site Scripting
Local File Inclusion (LFI)
Remote File Inclusion (RFI)

***Indicators of a Web Attack***

- Customers being unable to access services
- Suspicious activities in user accounts
- Leakage of sensitive data
- Correct URLs redirecting to incorrect sites
- Web page defacements
- Unusually slow network performance
- Frequent rebooting of the server
- Anomalies in log files
- Error messages such as 500 errors, “internal server error,” and “problem processing your request”

***Buffer Overflow:***

- Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the adjacent memory locations. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack. The purpose of these attacks is to corrupt the execution stack of the web application.

***Cookie Poisoning:***

- Cookie Poisoning refers to the modification of a cookie for bypassing security measures or gaining unauthorized information. The attackers bypass the authentication process by altering the information present inside a cookie. Once the attackers gain control over a network, they can modify its content, use the system for a malicious attack, or steal information from the users’ systems.

***Insecure Storage:***

- The sensitive information, such as account records, credit card numbers, passwords or other authenticated information are generally stored by the web applications either in a database or on a file system.
- If the developers make any mistakes while enforcing the encryption techniques on a web application or ignore the security aspects of some parts of the application, this sensitive information might be at risk.
- Insecure storage of such data can allow the attacker to gain access to the web application as a legitimate user.
- Hence, the forensics investigators need to understand the process of storing the data.

On Windows Server 2012, the log files are stored by default in the
***%SystemDrive%\inetpub\logs\LogFiles***

REGEX
Regular expression for detection of SQL meta-characters:
/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix

Modified Regular expression for detection of SQL meta-characters:
/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/i

Regular expression for typical SQL injection attack:
/\w*((\%27)|(\'))((\%6F) |o|(\%4F))((\%72)|r| (\%52))/ix

Regular expression for detecting SQL injection with the UNION keyword:
/((\%27)|(\'))union/ix

Regular expression for detecting SQL injection attacks on a MS SQL Server:

/exec(\s|\+)+(s|x)p\w+/ix

Snort signature alert tcp $EXTERNAL_NET any ->
$HTTP_SERVERS $HTTP_PORTS(msg: "SQL Injection - Paranoid"; flow:to_server, established;
uricontent:“.pl";pcre:"/ (\%27)|(\')|(\-\-)|(%23) |(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)

SELECT * from userinfo where username = '" & Request.Form("username") & "' and pwd = '" & Request.Form("pwd") & "'")

Attack:  blah' or 1=1--
SELECT * from userinfo where username = 'blah' or 1=1-- " & Request.Form("username") & "' and pwd = '" & Request.Form("pwd") & "'")
SELECT * from userinfo where username = 'blah' or 1=1

# CHFI - Database Forensics

Video: Module 9 DONE
Weiterlesen: 1021 DONE
Lab: DONE

- Database forensics deals with the examination of databases and its associated metadata.
- The process involved in database forensics is similar to the ones followed in computer forensics.

There are two phases in database analysis:
- Evidence collection
- Evidence examination

## *MSSQL Forensics*

- MSSQL forensics take action when a security incident has occurred and detection and analysis of the malicious activities performed by criminals over the SQL database file are required.
- A forensic investigator needs to examine the ***Primary Database Files (MDF)*** and ***Secondary Database Files (NDF)*** and ***Transaction Log Files (LDF)*** for investigation purpose.

***Primary Database Files (MDF)***
- The primary data file is the starting point of a database and points to other files in the database.
- Every database has a primary data file.
- The primary data file stores all the data in the database objects (tables, schema, indexes, etc.).
- The file name extension for primary data files is .mdf.

***Secondary Database Files (NDF)***
- The secondary data files are optional.
- While a database contains only one primary data file, it can contain zero/single/multiple secondary data files.
- The Secondary data file can be stored on a hard disk, separate than the primary data file.
- The file name extension for secondary data files is .ndf.

***Transaction LOG Database Files (LDF)***
- The transaction log files hold the entire log information associated with the database.
- The transaction log file helps a forensic investigator to examine the transactions occurred on a database, and even recover data deleted from the database.
- The file name extension for transaction log date files is .ldf and each file is divided into virtual log files.

***SQL Server Error Logs***
- C:\Program Files\Microsoft SQL Server\MSSQLxx.MSSQLSERVER\MSSQL\LOG

***TOOLS***
- ApexSQL
- sqlcmd
- SQL Server Management Studio (SSMS)
- Undocumented functions: ***fn_dblog ()***, ***fn_dump_dblog ()***
- Database Consistency Checker (DBCC)

## *MySQL Forensics*

- As per the information security policies, administrators need to audit high-performance databases regularly to ensure the data integrity and data security.

- They should even be able to detect database manipulations. Information auditing needs to be performed on regularly to find out if any part of the database is altered intentionally or accidentally by users at any point of time through bypassing auditing system.
- Such suspected behavior is to be inspected and analyzed by Database forensic investigators.
- The forensic approach for MySQL databases varies with the database engine used in the db server.

***Data directory is located at:***
Windows: C:\ProgramData\MySQL\MySQL Server 5.n
Linux: C:\mysql\data.

***Mysqldump***
- The utility allows you to dump a database or a collection of databases for backup purposes
- It generates a .sql file with CREATE table, DROP table and INSERT into the SQL statement of the source database
- It executes the .sql file on the destination database to restore the original database.
  Syntax: mysqldump [options] [db_name [tbl_name ...]]

***mysqlaccess***
- Checks the access privileges defined for host name, user name, etc.
- Validates access using the user, db, and host tables
- Syntax: mysqlaccess [host_name [user_name [db_name]]] [options]

***myisamlog***
- Processes the contents of MyISAM log file and perform recovery operation, display version information, etc., depending on the situation
- The default operations of the utility are update(-u) and recovery(-r)
- Syntax: myisamlog [options] [logfile-name [tbl_name] ...]

***myisamchk***
- Views the status of the MyISAM table or checks, repairs, or optimizes them.
- Syntax: myisamchk [options] tbl_name ...

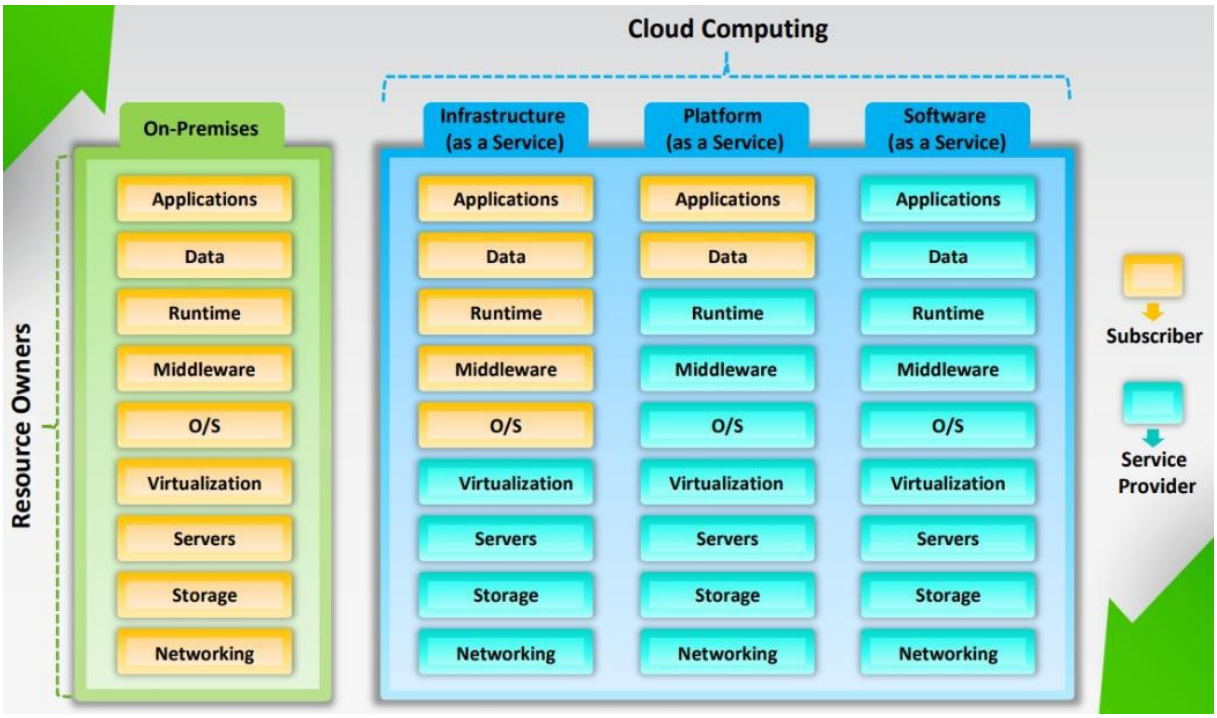
***mysqlbinlog***
- Reads the binary log files directly and displays them in text format
- Displays the content of bin logs (mysql-bin.nnnnnn) in text format
- Syntax: mysqlbinlog [options] log-file ...

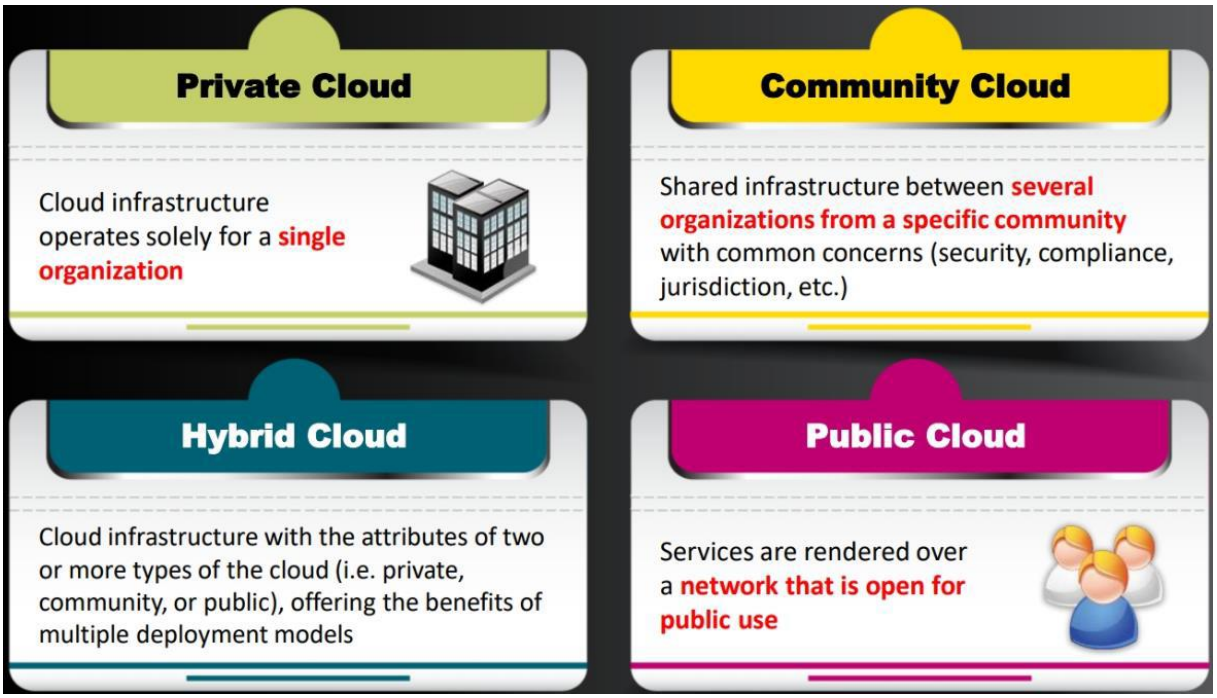
***mysqldbexport***
- Export metadata/data definitions
- Produces output in a variety of formats by making data extraction easier and suitable for the external application
- Syntax: mysqldbexport --server=user:pass@host:port:socket db1, db2, db3

# CHFI - Cloud Forensics

Video: Module 10 DONE
Weiterlesen: 1102 DONE
Lab: DONE

- Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet.
- Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, and, so on.
- As many enterprises are adopting the cloud, attackers make cloud as their target of exploit in order to gain unauthorized access to the valuable data stored in it.
- Therefore, one should perform ***cloud pen testing regularly*** to monitor its security posture.



***Limitations of Cloud Computing:***

- Organizations have limited control and flexibility
- Prone to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Depends on network connections

***Cloud Computing Threats***

1. Data breach/loss
2. Abuse of cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Inadequate infrastructure design and planning
8. Conflicts between client hardening procedures and cloud environment
9. Loss of operational and security logs
10. Malicious insiders
11. Illegal access to cloud systems
12. Privilege escalation
13. Loss of business reputation due to co-tenant activities
14. Natural disasters
15. Hardware failure
16. Supply chain failure
17. Modifying network traffic
18. Isolation failure
19. Cloud provider acquisition
20. Management interface compromise
21. Network management failure
22. Authentication attacks
23. VM-level attacks
24. Lock-in
25. Licensing risks
26. Loss of governance
27. Loss of encryption keys
28. Risks from changes of Jurisdiction
29. Undertaking malicious probes or scans
30. Theft of computer equipment
31. Cloud service termination or failure
32. Subpoena and e-discovery
33. Improper data handling and disposal
34. Loss or modification of backup data
35. Compliance risks
36. Economic Denial of Sustainability (EDOS)

***Cloud Computing Attacks***

1. Service Hijacking using Social Engineering Attacks
2. Session Hijacking using XSS Attack
3. Domain Name System (DNS) Attacks
4. SQL Injection Attacks
5. Wrapping Attack
6. Service Hijacking using Network Sniffing
7. Session Hijacking using Session Riding
8. Side Channel Attacks or Cross-guest VM Breaches
9. Cryptanalysis Attacks
10. DoS and DDoS Attacks

***CSPs***

- Amazon
- Dropbox

- Google
- AT&T
- Iron Mountain
- Microsoft
- Nirvanix
- Rackspace
- Swisscom myCloud

## *Investigating Dropbox Cloud Storage Service*

- Dropbox is an online application that allows users to store their files on a cloud and share them when required.
- Users can access and use Dropbox through the following methods, website, desktop or mobile application.
- In both ways, the Dropbox creates artifacts on a system that may provide relevant information for the forensic investigation.
- Besides, the Dropbox servers also save information such as account history, a user's file history, and logs.
- These artifacts and log files can help the investigator in conducting a detailed forensic analysis.
- Unter Einhaltbg des Bug-Bounty-Programms, können Schwachstellenüberprüfungen vorgenommen werden.

OnWindows 10 OS, by default Dropbox client is installed at
C:\Program Files (x86)\Dropbox

Executable and libraries are stored at:
C:\Program Files (x86)\Dropbox\Client

The default folder used for syncing files is
C:\Users\<username>\Dropbox

Dropbox installation creates various keys and values inside the ***registry***:

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\DropboxExt(n)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
HKLM\SOFTWARE\Classes\DropboxUpdate.ProcessLauncher HKLM\SOFTWARE\Dropbox\InstallPath
HKLM\SOFTWARE\Dropbox\Client\Version

Configuration files are saved inside the Appdata folder in the user profile
C:\Users\<username>\AppData\Local\Dropbox\instance(n)

Files created during Dropbox client installation:

LINK files or Shortcut files:
C:\Users\<username>\Desktop\Dropbox.lnk
C:\Users\<username>\Links\Dropbox.lnk

Prefetch Files:
C:\Windows\Prefetch\DROPBOX.EXE-1AFC8E96.pf
C:\Windows\Prefetch\DROPBOX.EXE-BC41F124.pf
C:\Windows\Prefetch\DROPBOXCLIENT_3.14.7.EXE-67CA8E4C.pf
C:\Windows\Prefetch\DROPBOXCLIENT_3.14.7.EXE-68E912D2.pf
C:\Windows\Prefetch\DROPBOXCRASHHANDLER.EXE-3D55A98C.pf
C:\Windows\Prefetch\DROPBOXINSTALLER.EXE-1EDCCE18.pf
C:\Windows\Prefetch\DROPBOXUNINSTALLER.EXE-A866A871.pf
C:\Windows\Prefetch\DROPBOXUPDATE.EXE-59B5AB7D.pf
C:\Windows\Prefetch\DROPBOXUPDATE.EXE-48534C67.pf
C:\Windows\Prefetch\DROPBOXUPDATE.EXE-AA3CC021.pf
C:\Windows\Prefetch\DROPBOXUPDATEONDEMAND.EXE-229B2726.pf

## *Investigating Google Drive Cloud Storage Service*

- Google drive is ***online file storage and sharing service*** from Google that supports sharing of different types of files such as pictures, videos, documents, spreadsheets, presentations, etc.
- The service supports various devices including desktops, mobiles, etc. through different modes such as desktop client, web portal, mobile application, etc.

- The users can also invite others to view, download and collaborate on the files.
- The storage works in collaboration with Google Docs, Sheets, and Slides, an office suite that allows users to editing the documents, spreadsheets, presentations, drawings, forms, and more online.

***Previous versions of files available to the files modified during the security incident.***

- In the Google Drive account homepage, right click on the required file
- Select Manage versions... option from the drop down menu
- In the Manage versions window, select the version required to analyze
- Click the options button present at the end of the file name
- Click the Download option from the list

On Windows 10 OS, by default Google Drive client is installed at

C:\Program Files (x86)\Google\Drive

The default folder used for syncing files is

C:\Users\<username>\Google Drive

Google Drive installation creates various keys and values inside the registry:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
HKCU\SOFTWARE\Google\Drive
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync
HKCU\SOFTWARE\Classes

Configuration files are saved inside the installation folder in the user profile
C:\Users\<username>\AppData\Local\Google\Drive\user_default

Executable and libraries are stored at:
C:\Program Files (x86)\Google\Drive

Files created during Google Drive client installation: LiNK files or Shortcut files:
C:\Users\<username>\Desktop\Google Drive.lnk
C:\Users\<username>\Links\Google Drive.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk

Prefetch Files: Located at
C:\Windows\Prefetch

An additional 4 files are created in the default database path directory
C\Users\<username>\AppData\Local\Google\Drive\user_default

# CHFI - Malware Forensics

During malware analysis, pay attention to the ***key features*** instead of understanding each and every detail.

- Currently, malicious software, commonly called malware, is the most efficient tool used in compromising security of the computer or any other electronic device connected to the internet.
- This has become a menace owing to the rapid progress in technologies such as easy encryption and data hiding techniques.
- Malware is the major source of various cyber-attacks and internet security threats, which is why computer forensic analysts need to have expertise in dealing with it.
- Malware forensics is the method of finding, analyzing and investigating various properties of malware to find the culprits and reason for the attack.
- The process also includes tasks such as finding out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use, etc.
- Investigators conduct forensic investigation using different techniques and tools.

***Types of Malware***

- Backdoor
- Botnet
- Downloader
- Launcher
- Rootkit
- Scareware Spam-sending malware
- Worm or virus
- Credential-stealing program

***Ways to get infected***

- Instant Messenger applications
- Browser and e-mail software bugs
- Internet Relay Chat (IRC)
- NetBIOS (File Sharing)
- Removable devices
- Fake programs
- Links and Attachments in e-mails
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

| Malware Components | Description |
|---|---|
| Crypter | Software that protects malware from undergoing reverse engineering or analysis, thus hardening the task of security mechanism its detection |
| Downloader | A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system |
| Dropper | A type of Trojan that installs other malware files on to the system either from malware package or internet |
| Exploit | A malicious code that breaches the system security via software vulnerabilities to access information or install malware |
| Injector | A program that injects its code into other vulnerable running processes and changes the way of execution in order to hide or prevent its removal |
| Obfuscator | A program via various techniques that conceals its code and intended purpose, and thus, makes it hard for security mechanisms to detect or remove it |
| Packer | A program that allows to bundle all files together into a single executable file via compression in order to bypass security software detection |

| | |
|---|---|
| Payload | A piece of software that allows to control a computer system after it has been exploited |
| Malicious Code | A command that defines malware's basic functionalities such as stealing data and creating backdoor |

## *Preparing Testbed*

1. Allocate a physical system for the analysis lab
2. Install Virtual machine (VMware, Hyper-V, etc.) on the system
3. Install guest OSs in the Virtual machine(s)
4. Isolate the system from the network by ensuring that the NIC card is in "host only" mode
5. Simulate internet services using tools such as iNetSim
6. Disable the 'shared folders' and the 'guest isolation'
7. Install malware analysis tools
8. Generate hash value of each OS and tool
9. Copy the malware over to the guest OS

## *Supporting Tools for Malware Analysis*

***Virtual Machines Tools***

- ❑ Virtual Box (https://www.virtualbox.org)
- ❑ Parallels Desktop 11 (http://www.parallels.com)
- ❑ Boot Camp (https://www.apple.com)
- ❑ VMware vSphere Hypervisor (http://www.vmware.com)

***Screen Capture and Recording Tools***

- ❑ Snagit (https://www.techsmith.com)
- ❑ Jing (https://www.techsmith.com)
- ❑ Camtasia (https://www.techsmith.com)
- ❑ Ezvid (http://www.ezvid.com)

***Network and Internet Simulation Tools***

- ❑ NetSim (http://tetcos.com/netsim_gen.html)
- ❑ ns-3 (https://www.nsnam.org)
- ❑ Riverbed Modeler (http://www.riverbed.com)
- ❑ QualNet (http://web.scalable-networks.com)

***OS Backup and Imaging Tools***

- ❑ Genie Backup Manager Pro (http://www.genie9.com)
- ❑ Macrium Reflect Server (http://www.macrium.com)
- ❑ R-Drive Image (http://www.drive-image.com)
- ❑ O&O DiskImage 10 (https://www.oo-software.com)

## *Static Malware Analysis*

- Also known as code analysis, involves going through the executable binary code without actually executing it to have a better understanding about the malware and its purpose Disassemblers such as ***IDA Pro***, can be used to disassemble the binary file.

## *Dynamic Malware Analysis*

- Also known as behavioral analysis, involves executing the malware code to know how it interacts with the host system and its impact on it.
- This type of analysis requires virtual machines and sandboxes to deter the spreading of malware Debuggers such as ***GDB***, ***OllyDbg***, ***WinDbg***, etc., are used to debug malware at the time of execution to study its behavior.

## *Steps to detect malware in PDF and MS Office document files*

1. Enlist the common vulnerabilities and exploits :
   Study and list the common vulnerabilities and their impact on the document structure.

2. Examine the file for suspicious elements or pointers of malware :
   Using the common vulnerability, investigators should be able to scan the document for suspicious elements that can confirm presence of malicious code, strings, commands, etc.

3. Inspect the metadata :
   Metadata may include time of creation and modification, author and moderator names, an application used for creation, etc.
   Gather the metadata and inspect it for any mistakes.

4. Verify the structure and content :
   Analyze the structure and contents of the document for suspicious elements such as objects, streams, scripts, and shellcode.

5. Extract the uncertain scripts or code :
   Search and extract the suspicious scripts and code from the document.

6. Search for encrypted scripts and decrypt:
   Find if the document contains any encrypted elements, as the attackers encode the malicious code, scripts, and objects to avert detection. Extract such elements and decrypt them.

7. Analyze the suspicious element:
   Evaluate the impact of the suspicious element by finding their course of action, propagation, and modification they make on the system.

8. Scan with malware scanner: Scan the suspicious documents with malware scanner or scan them using online and offline tools to find if they contain any malicious content.

***TOOLS***

- PDFStreamDumper
- PDFID
- OffVis

# CHFI - Investigating Email Crimes

***TERMS***
mail user agent (MUA)
mail transfer agent (MTA)

***Components***
POP3 110
SMTP 25
IMAP 143

***POP3 Commands***
 USER - enter your user ID
 PASS - enter your password
 QUIT - quit the POP3 server
 LIST - list the messages and their size
 RETR - retrieve a message, according to a message number
 DELETE - delete a message, according to a message number

***RFCs***
RFC 5322 defines the Internet email message format
RFC 2045 through RFC 2049 defines multi-media content attachments MIME

***E-mail crime can be categorized in two ways:***

***Crimes committed by sending e-mails***

- Spamming
- Phishing
- Mail bombing
- Mail storms

***Crimes supported by e-mails***

- Identity Fraud
- Cyber-stalking
- Child pornography
- Child abduction

***Steps involved in investigating e-mail crimes and violations:***

1. Obtain a Search Warrant
2. Examine e-mail messages
3. Copy and print the e-mail messages
4. View the e-mail headers
5. Analyze the e-mail headers
6. Trace the e-mail
7. Acquire e-mail archives
8. Examine e-mail logs

***Steps to copy an e-mail message using Microsoft Outlook:***
1. Insert a formatted USB key into the machine's USB port
2. Navigate to My Computer or Windows Explorer to access the USB key
3. Open Microsoft Outlook
4. Click the folder that contains the offending message, while keeping the folders list open.
5. A list of messages in the selected folder will be displayed in the mid-section of the panel. Click the message you want to copy
6. Resize the Outlook window to see both the message to be copied and the USB drive icon
7. Drag the message from the Outlook window to the USB drive icon
8. The next step after copying the e-mail message is to print it. Go to File menu  click Print  click Print Options. Select the settings for printing in the Print dialog box and then click the Print button
9. You can include the printed e-mail copy in your final report

***Received headers*** of an email message provide information about the ***message origin***, the route it took to reach the recipient, and the cause of delivery delays.

It is important to examine this part of the email header once we identify that the email is spam.

When the SMTP Server receives an email message, a received Header gets ***added to the email***. Therefore, ***Received Headers are essentially in reverse order***; in other words, the last Received Header added is the first one at the top.

***To understand the Received Headers correctly, read from the bottom (first Received Header) to the top (last Received Header).***

***Tools to check e-mail validity:***

| | |
|---|---|
| Email Address Vérifier | https://tools.verifyemailaddress.io |
| Email Checker | http://email-checker.net |
| G-Lock Software Email Vérifier | http://www.glocksoft.com |
| e-Mail Validator Tool | http://e-mailvalidator.com |

www.freeality.com
This site provides the various options for searching such as ***email address***, ***phone numbers***, and ***names***. One can do a reverse email search, which could reveal the subject's real name. This site can do other searches such as reverse phone number searches and address searches

***IBM Notes***
Gather the *.NSF file
Gather the associated *.ID file for the archive.
It functions as the encryption key that allows you to open encrypted mails

***MS Exchange***
Follow these guidelines when dealing with MS Exchange:
In an organization, various employees connect with each other through servers such as the Microsoft Exchange Server. Therefore, the investigators should not access an active Exchange server. The best way is to create a backup of the server, which will be available for users to connect to the Exchange server. Investigators must collect all the data files associated with the server, as there is more than one file associated with Exchange email. The archive file consists of the PRIV.EDB file, PUB.EDB file, and PRIV.STM file.
The files available will vary according to the Exchange server you are dealing with.

- ***PRIV.EDB***: It is a rich text database file that contains message headers, message text, and standard attachments.
- ***PUB.EDB***: It is a database file to store public folder hierarchies and contents.
- ***PRIV.STM***: It is a streaming Internet content file containing video, audio, and other media that are streams of MIMEs.

***CAN-SPAM's main requirements meant for senders:***

- ❑ Do not use false or misleading header information
- ❑ Do not use deceptive subject lines
- ❑ The commercial e-mail must be identified as an ad
- ❑ The email must have your valid physical postal address
- ❑ The email must contain the necessary information regarding how to stop receiving e-mails from the sender in future
- ❑ Honor recipients' opt-out request within 10 business days
- ❑ Both the company whose product is promoted in the message and the e-mailer hired on contract to send messages must comply with the law

# CHFI - Mobile Forensics

- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.
- It involves the examination and reporting of all possible sources of digital evidence in a forensically sound manner.
- The investigator reports and presents the evidence in the court of law to prove the incident. Mobile phone forensics includes extraction, recovery, and analysis of data from the internal memory, SD cards, and SIM cards of mobile devices.
- Forensics experts analyze the phone by examining the incoming and outgoing text messages, pictures stored in the memory of the phone, call logs, email messages, SIM data, deleted data, etc., in an attempt to trace the perpetrators of crimes that involve the use of mobile phones.Mobile forensics is the science of recovering digital evidence from mobile devices under forensically sound conditions.
- With the increase in the usage of mobile devices every day, there is growing importance of mobile forensics.
- This module highlights the precautions that a forensic analyst must take when collection, preserving, and acquiring mobile devices such as smartphones, PDAs, digital cameras, Internet of Things, etc.
- This module will familiarize you with the topics mentioned in the slide

***Components of a Mobile Device***

???

***TERMS***

- DFU - Device Firmware Upgrade
- SIM: Subscriber Identity Module
- MSC: Mobile Services Switching Center
- HLR: Home Location Register
- BTS: Base Transceiver Station
- AuC: Authentication Center
- VLR: Visitor Location Register
- BSC: Base Station Controller
- ME: Mobile Equipment
- EIR: Equipment Identity Register

## *Booting iPhone in DFU Mode*

1. Connect the iPhone to a computer and launch ***iTunes***
2. Turn the iPhone ***off***
3. Hold down the ***sleep/power*** button and home button together for exactly ***10 seconds***, then release the power button
4. Continue to hold down the ***Home*** button until a message appears in iTunes saying that "iTunes has detected an ***iPhone in recovery mode***"

- The display completely turns OFF while running in DFU mode; this confirms that the mobile is connected in the DFU mode.
- If it displays any of the logo on the screen, it represents that the mobile is connected in the standard recovery mode; then, it repeats the steps again to connect the device in DFU mode.
- To exit from the DFU mode, the user must press and hold the FK and ***sleep/power*** buttons together on the device when connected.

## *Creating Disk Image of an iPhone Using SSH*

What you need before creating the image:

1. iPhone should be jailbroken
2. SSH should be installed on both iPhone and workstation running Linux OS
3. iPhone's IP address
4. Computer's IP address

Then Run following command on Linux:
ssh -l <username> <your Linux box host address> dd if=/dev/disk0 | dd of=~/myiphoneback.img

***Mobile forensic workstation:***

- ***A laptop or a desktop computer***
  The forensic examiner requires a computer to retrieve, store, and process the information from the mobile phone.
- ***A USB connector***
  The USB connector establishes communication between a computer and mobile phone, memory card reader, etc.
- ***FireWire***
  A FireWire connection allows data transfer from high-bandwidth digital devices such as digital camcorders.
- ***Mobile forensics toolkit***
  Mobile forensics toolkits such as EnCase, FTK, etc. facilitate forensic investigation and data recovery from mobile devices.
- ***Cables (including Bluetooth and IR)***
  The investigator requires supporting cables and wires that provide communication between devices.
- ***Micro SD Memory card Reader***
  The forensic investigator requires an SD Memory card Reader (with micro option) to access the data from a memory card.
- ***SIM card Reader***
  The SIM card reader is a small device that is used to access the information on a SIM card. The investigator carefully secures the SIM card found at the crime scene and uses a SIM card reader to access the information on the SIM card.

## *Hardware Tools*

- ❑ Cellebrite UFED System
- ❑ Secure ViewKit for Forensics
- ❑ DS-Device Seizure & Toolbox
- ❑ USB reader for SIM cards
- ❑ iGo
- ❑ DC Lab Power Supply 0-15V/3A
- ❑ Digital Display with Backlight
- ❑ Paraben's Phone Recovery Stick

## *Software Tools*

- ❑ SEARCH Investigative Toolbar
- ❑ BitPim
- ❑ Oxygen Forensics Analayst
- ❑ Paraben's Sim Card Seizure
- ❑ MOBILedit! Forensic
- ❑ TULP2G
- ❑ iDEN Phonebook Manager
- ❑ SUMURI's PALADIN
- ❑ floAt's Mobile Agent
- ❑ XRY Logical & XRY Physical
- ❑ AccessData FTK Imager
- ❑ ViaExtract

***Bypassing Android Phone Lock Password Using ADB***

- Connect the device to the forensics workstation through USB
- Launch adb shell using ***ViaExtract***
- Remove password.key file from android directory

***Bypassing the iPhone Passcode Using IExplorer***

- Connect the device to the workstation
- Browse the iPhone file system with IExplorer

- Navigate to the directory /var/mobile/Library/Preferences/ and delete com.apple.springboard.plist
- Navigate to the directory /var/Keychains/ and delete keychain-2.db
- Reboot the iPhone

Note: This technique works for jailbroken devices only

## *Cellular Networks*

***Code Division Multiple Access (CDMA)***
This is one of the dominant types of cellular networks used. It employs spread-spectrum technology where channels for communication are defined in terms of codes.

***Enhanced Data Rates for GSM Evolution (EDGE)***
Improved data transmission rates are possible through backward-compatible digital mobile phone technology. It delivers high bit-rates per radio channel that is used for any of the packet-switch applications.

***Integrated Digital Enhanced Network (iDEN)***
iDEN, developed by Motorola, is the mobile communication technology that provides its users with the benefit of a trunked radio and cellular telephone.

***General Packet Radio Service (GPRS)***
This is a packet-oriented mobile data service. It is available to the users of GSM and IS-136 mobiles. It uses the technology of frequency-division duplex and time-division multiple access.

***Global System for Mobile communications (GSM)***
This is a major and popularly used cellular network.

***High-Speed Downlink Packet Access (HSDPA)***
This third generation mobile telephony communication protocol allows high data transfer speed for networks based on UMTS.

***Time Division Multiple Access (TDMA)***
In this communication, a single-frequency channel is provided to multiple users over a divided time slot.

***Universal Mobile Telecommunications System (UMTS)***
This is a 3-G mobile phone technology (upgrade to 4-G) that use W-CDMA as the underlying air interface.

***Unlicensed Mobile Access (UMA)***
- UMA or the Generic Access Network (GAN) enables mobile services such as voice, IP Multimedia Subsystem/Session Initiation Protocol (IMS/SIP applications), and data to access IP networks.

# CHFI - Forensics Report Writing and Presentation

- An investigative report contains all the findings of a forensic investigation that are presented in a written form.
- It contains only facts, and there is no room for any personal opinions of a forensic investigator.

## *Forensics investigation report template*

***1. Executive summary***

Case number
Names and Social Security Numbers of authors, investigators, and examiners
Purpose of investigation
Significant findings
Signature analysis

***2. Investigation objectives***

***3. Details of the incident***

Date and time the incident allegedly occurred
Date and time the incident was reported to the agency's personnel
Details of the person or persons reporting the incident

***4. Investigation process***

Date and time the investigation was assigned
Allotted investigators
Nature of claim and information provided to the investigators

***5. Evidence information***

Location of the evidence
List of the collected evidence
Tools involved in collecting the evidence
Preservation of the evidence

***6. Evaluation and analysis Process***

Initial evaluation of the evidence
Investigative techniques
Analysis of the computer evidence (Tools involved)

***7. Relevant findings***

***8. Supporting Files***

Attachments and appendices
Full path of the important files
Expert reviews and opinion

***9. Other supporting details***

Attacker's methodology
User's applications and Internet activity
Recommendations

# CISM - Information Security Governance

# CISM - Information Risk Management

# CISM - Information Security Program Development

# CISM - Information Security Program Management

# CISM - Incident Management and Response

- An incident is described as any event where the service is, or could be, disrupted. For information security, the service provided is the provision of accedd to information resources and the prevention of unauthorized access to information systems. An incident, in these terms, would identify a failure to provide such access or a breach in the system rending a leak of information.
- Incident mangement is a process used to control the activities related to identifying, managing and overcoming an incident. Many incidents are reocurring and, therefore, use pre-defined incident models. These methods describe the steps for handling an incident. Specifically, the model defines :

  - The steps to be taken
  - Order of steps, including dependencies
  - Responsible parties
  - Timelines and thresholds for completing steps
  - Escalation procedures
  - Activities for preserving evidence

- The process for incident management is similar to problem management. A couple of steps are extensive because of the immediacy of the incident, such as escalations and closure. Escalation serves two functions in incident management. The first is functional escalation when the Service Desk is unable to resolve an incident entirely or within a specific timeframe and requires the incident rcord to be sent to another level of support. Hierarchical escalation is performed for incidents with a high severity, when IT and business management must be notified.
- Resolution, reovery, and closure of an incident can be more involved in incident management. A request in change management is usually nor required. Potential resolutions are applied and tested. Typically, closure is initiated when both the incident is resolves and the user is satisfied with the resolution. As a result, the Service Desk usually checks the following before closing the record :

  - Closure categorization - ensure the incident is properly categorized, or has been changed from initial understanding
  - Use satisfaction survey - to determine the satisfaction of th euser and find potential service improvements
  - Incident documentation - ensure al information related to the incident, including the description of th event and resoulution attempts, are documented
  - Recurring problem determination - making the decision to introduce the incident details to problem management
  - Formal closure - provides th fina closing procedure for the incident

# REGISTRY

Microsoft Description of Registry: http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986

## *HKCR - HKEY_CLASSES_ROOT*

**Enthält: Softwarekonfigurationsdaten**

Diese Teilstruktur enthält Softwarekonfigurationsdaten, d.h. Daten zu OLE (Object Linking and Embeding) und den Dateiverknüpfungen. Diese Teilstruktur verweist auf den Unterschlüssel Classes in der Teilstruktur HKEY_LOCAL_MACHINE\SOFTWARE.

### *Cannot View Thumbnail Image W2K*

1. Click **Start**, click **Run**, type regedit in the **Open** box, and then click **OK**.
2. Locate and click the **HKEY_CLASSES_ROOT\.jpg** registry key.
3. Right-click the **HKEY_CLASSES_ROOT\.jpg** registry key, point to **New**, and then click **Key**. Name the new key **ShellEx**.
4. Right-click the **ShellEx** registry key that you created, point to **New**, and then click **Key**. Name the new key **{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}**.
5. Click the **{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}** registry key that you created, right-click the **Default** value in the right pane, click **Modify**, and then type the following value data in the **Value data** box:

   {7376D660-C583-11d0-A3A5-00C04FD706EC}

   oder .REG-Datei erstellen

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\.jpg]
@="jpegfile"
"Content Type"="image/jpeg"
[HKEY_CLASSES_ROOT\.jpg\jpegfile]
[HKEY_CLASSES_ROOT\.jpg\jpegfile\ShellNew]
[HKEY_CLASSES_ROOT\.jpg\PersistentHandler]
@="{098f2470-bae0-11cd-b579-08002b30bfeb}"
[HKEY_CLASSES_ROOT\.jpg\ShellEx]
[HKEY_CLASSES_ROOT\.jpg\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"

ALL THUMBNAILS ( allthumb.reg )
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\.BMP\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.art\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.dib\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.GIF\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.jfif\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.jpe\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.jpeg\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.jpg\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
[HKEY_CLASSES_ROOT\.wmf\ShellEx\{BB2E617C-0920-11d1-9A0B-00C04FC2D6C1}]
@="{7376D660-C583-11d0-A3A5-00C04FD706EC}"
```

## *HKCU - HKEY_CURRENT_USER*

**Enthält: Benutzerkonfiguration**

USER.DAT ( User-Profile )

Diese Teilstruktur enthält Daten über den aktuellen Benutzer. Es wird eine Kopie für jedes Benutzerkonto abgerufen, das zur Anmeldung beim Computer verwendet wird, und im Schlüssel Windows2000\Documents And Settings\Benutzername gespeichert.

| | |
|---|---|
| NoSaveSettings = 01 | Der Desktop wird beim Verlassen nicht mehr gespeichert |
| NoFind = 01 | Im Startmenü wird "Suchen" nicht mehr angezeigt |
| NoRun = 01 | Im Startmenü wird "Ausführen" nicht mehr angezeigt |
| NoSetTaskbar = 01 | Die Taskbar ist nicht mehr veränderbar |
| NoStartBanner = 01 | "Klicken Sie hier..." erscheint nicht mehr |
| NoClose = 01 | Windows kann nicht mehr beendet werden |
| NoSetFolder = 01 | Unter "Einstellungen" im "Startmenü" ist nur noch das Icon für die "Task-Leiste" vorhanden. Kein Drucker und Systemsteuerung |
| NoStartMenuSubFolders = 01 | Im "Startmenü" sind einige Ordner nicht mehr sichtbar |
| NoNetHood = 01 | Das Icon "Netzwerk" wird nicht mehr angezeigt |

## *HKLM - HKEY_LOCAL_MACHINE*

**Enthält:** **Computerkonfiguration**

SYSTEM.DAT ( %SystemRoot%)

| Registry Path | File Path |
|---|---|
| HKEY_LOCAL_MACHINE\System | Windows\System32\config\SYSTEM |
| HKEY_LOCAL_MACHINE\SAM | Windows\System32\config\SAM |
| HKEY_LOCAL_MACHINE\Security | Windows\System32\config\SECURITY |
| HKEY_LOCAL_MACHINE\Software | Windows\System32\config\SOFTWARE |
| HKEY_USERS\.Default | Windows\System32\config\DEFAULT |

Diese Teilstruktur enthält alle Konfigurationsdaten für den lokalen Computer, einschliesslich der Hardware- und Betriebssystemdaten ( z.b. Bustyp, Systemspeicher, Gerätetreiber und zur Startsteuerung). Anwendungen, Gerätetreiber und das Betriebssystem verwenden diese Daten zur Ermittlung der Computerkonfiguration. Die Daten in dieser Teilstruktur bleiben konstant und sind vom jeweiligen Benutzer unabhängig.

**Autostart Programme:**
**HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion**
hier gibt es folgende Ordner (es sind nicht immer alle vorhanden):
**Run** = beim Starten ausführen...
**RunOnce** = Nur beim nächsten Start ausführen...
**RunOnceEx** = Nur beim nächsten Start aber vor RunOnce ausführen...
**RunServices** = Programm wird vor der Passworteingabe/Netzwerk ausgeführt.
**RunServicesOnce** = Programm wird einmal vor der Passworteingabe/Netzwerk ausgeführt.
Ausserdem gibt es im Windows-Verzeichnung noch die **'Win.ini'**. Hier können im Abschnitt [Windows] unter 'run=' und 'load=' auch Einträge stehen, die Programme starten. Den Start dieser Programme kann man durch voranstellen eines Semikolons oder Hashes verhindern.

Vorsicht: Einträge nur löschen, wenn sicher ist, dass Windows oder andere Programme sie nicht zum Start brauchen.

**DIENSTE**
**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**

**Microsoft PhotoEditor**
*Problem:*

No File Format Information Can be found in the Registry
Keine Dateiformat-Informationen in der Registrierung gefunden

***Lösung:***
Start/Run/Regdt32
HKEY_LOCAL MACHINE\Software\Microsoft\Shared Tools\Graphic Filters
Security/Permissions
Users = Full Control
=======

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"=hex:95,00,00,00
"NoSaveSettings"=hex:00,00,00,00
"NoStartBanner"=hex:01,00,00,00
"SpecifyDefaultButtons"=dword:00000001
"Btn_Back"=dword:00000001
"Btn_Forward"=dword:00000001
"Btn_Stop"=dword:00000001
"Btn_Refresh"=dword:00000001
"Btn_Home"=dword:00000001
"Btn_Search"=dword:00000002
"Btn_History"=dword:00000002
"Btn_Favorites"=dword:00000002
"Btn_Media"=dword:00000002
"NoBandCustomize"=dword:00000001
"NoToolbarCustomize"=dword:00000001
"NoWindowsUpdate"=dword:00000001
"NoFileUrl"=dword:00000001
"Btn_Edit"=dword:00000002
"Btn_MailNews"=dword:00000002
"Btn_Discussions"=dword:00000002
"NoExpandedNewMenu"=dword:00000001

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Toolbars\Restrictions]
"NoAddressBar"=dword:00000001
"NoLinksBar"=dword:00000001

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Restrictions]
"NoBrowserOptions"=dword:00000001
"NoFileNew"=dword:00000001
"NoFileOpen"=dword:00000001
"NoFindFiles"=dword:00000001
"NoBrowserBars"=dword:00000001
"NoFavorites"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]
"Start Page"=http://our.intranet

**MODEM**
http://support.microsoft.com/default.aspx?scid=kb;de;250649
HKEY_LOCAL_MACHINE\System\CurrentControlSet00.\Control\Class\{…}\Settings

Blind_Off Wählton vor dem Wählen abwarten X4

## *HKU - HKEY_USERS*

**Enthält: Systemstandardeinstellungen**
Diese Teilstruktur enthält die Systemstandardeinstellungen (Systemstandardprofile) für die Identitäten und Arbeitsumgebungen der einzelnen Benutzer. Hierzu gehören die Einstellungen für den Desktop, für die Fensterumgebung bzw. die Benutzeroberfläche sowie für Benutzerspezifische Software.

### *HKCC - HKEY_CURRENT_CONFIG*

**Enthält:** **Hardwareprofil**

Diese Teilstruktur enthält Daten zum aktiven Hardwareprofil, die aus den Zweigen SOFTWARE und System extrahiert werden. Mithilfe dieser Informationen werden bestimmte Einstellungen festgelegt (z.B. die zu ladenden Gerätetreiber und die Bildschirmauflösung).

Der Command Scanreg /fix bewirkt unter Win98, dass die Registry auf eventuelle Fehler überprüft wird und leere Einträge gelöscht werden.
Der Command Scanregw bewirkt unter WinME, dass die Registry auf eventuelle Fehler überprüft wird und leere Einträge gelöscht werden.

## FTP-Sites

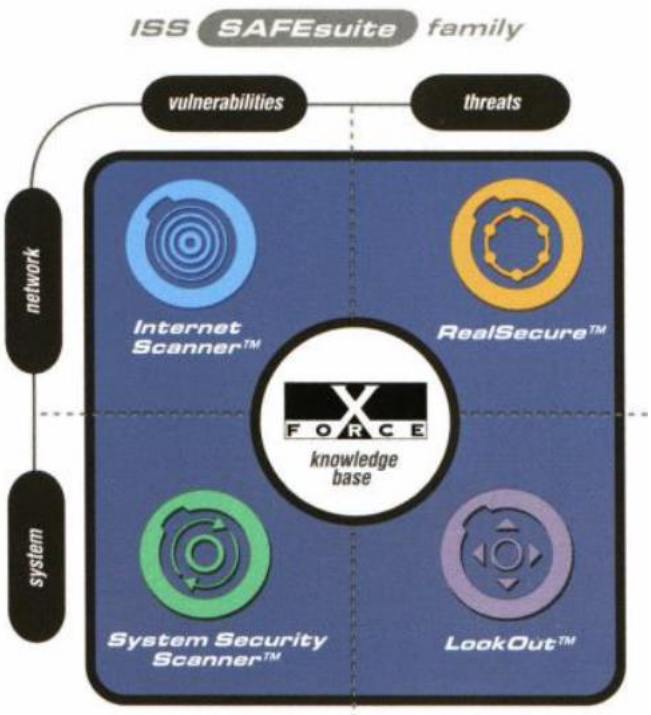
- EmTec FTP www.musthave.com/files/eftp502.zip

## eCommerce

- SecureCC: http://www.securecc.com
- siehe Hackers guide page 152

## Security Providers

***Internet Security Systems (ISS)***
Product: RealSecure www.iss.net/xforce
Description.: Automated real-time intrusion detection system.



# ALLGEMEINES

Problem: IBM360 (31.12.1969)!
siehe Hacker's Guide Seite 129.

***Imbedded Chips:***

- Alarm- und Sicherheitssysteme
- Ältere Kraftfahrzeuge
- Telefonschaltanlagen
- Safes und Tresore mit Zeitschlössern (Banken)
- Medizinische Geräte
- Luftverkehr- Kontrollsysteme
- Ältere Satelittensysteme (besonders Support Software)
- Heizungssysteme
- Aufzugssysteme
- Geldautomaten-Systeme
- Wasserversorgung

***Sicherheitszertifikate:***

- Coopers & Lybrand http://www.us.coopers.com/cas/itsswww0.html
- Intern. Computer Security ... http://www.icsa.com

***Schulung***

- LUCENT http://www.lucent.com

***WEB-HOSTING***

- Sicherheit durch betreiben der Server durch Anbieter.

***E-Mail: PWNED***

- Wurde mein E-Mail account kompromitiert?

  https://haveibeenpwned.com/

# Security Communication

## Welche potenziellen Angriffspunkte sind in der EDV und der Telekommunikation vorhanden?

- Sämtliche so genannten Dial-up oder Wählleitungen, sowohl Dial-in als auch Dial-out.
- Nicht zu vernachlässigen sind dabei die mobilen Geräte wie Funk und Telefone.
- Mietleitungen, auch leased-lines genannt; dazu gehören auch Cable-TV und Stromversorgungsnetze.
- Internet-Anschlüsse, ob als Surfer oder Anbieter einer eigenen Homepage.
- Jeder Modemanschluss.
- Datenimport mit sämtlichen Medien:
- Diskette, CD-Rom etc.
- Jedes Programm, das auf der Arbeitsplattform geladen wird.
- Das Betriebssystem selbst.

### *Risikoanalyse*

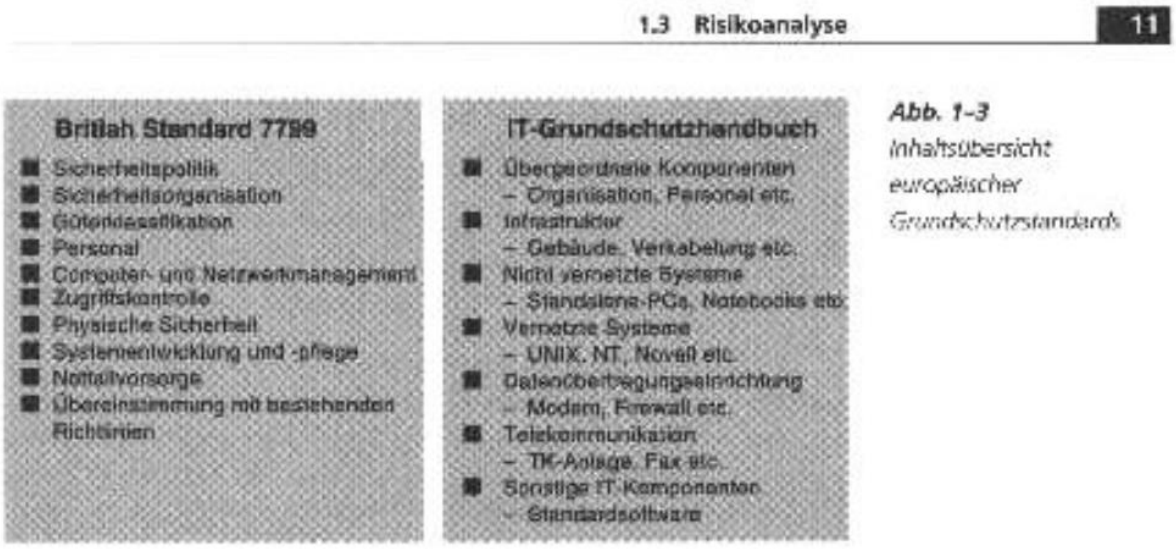



*Abb. 1-3*
*Inhaltsübersicht europäischer Grundschutzstandards*

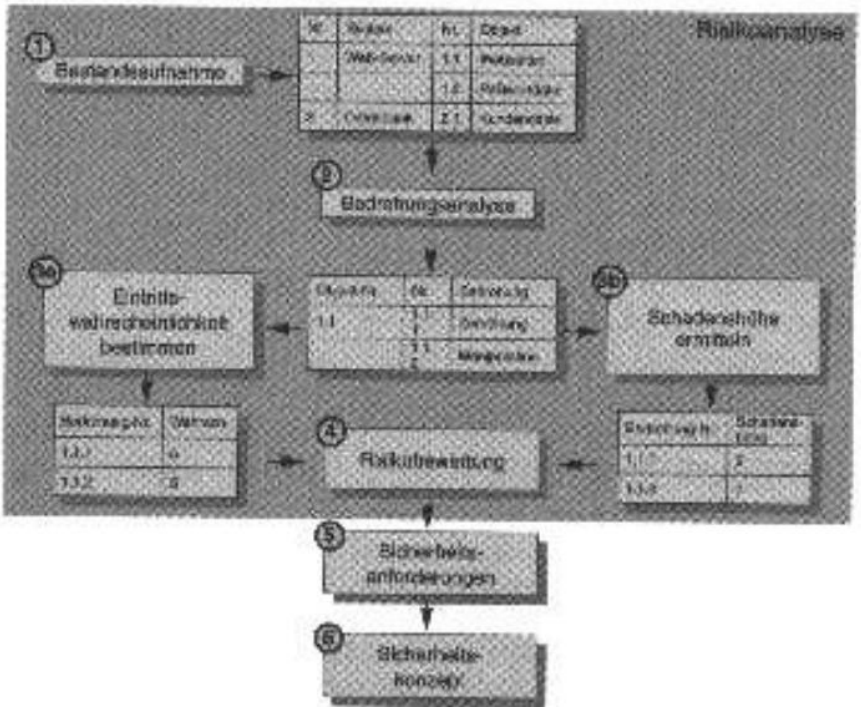



**Abb. 1-4**
*Vorgehensweise der detaillierten Risikoanalyse*

| Bewertung | Bedeutung |
|---|---|
| 0 | Denial-of-Service-Attacke (siehe 1.13.1) - es erfolgt kein unberechtigter Systemzugriff |
| 1 | Interner Eindringling kann unberechtigt Lesezugriff auf Programmdateien und Daten erlangen |
| 1 | interner Eindringling kann unberechtigten Schreibzugriff auf Programmdateien und Daten erlangen |
| 2 | interner Eindringling kann unberechtigten Schreibzugriff auf Systemdateien erlangen |
| 3 | externer Eindringling aus dem lokalen Netzwerk kann Lesezugriff auf Programmdateien und Daten erlangen |
| 4 | externer Eindringling aus dem lokalen Netzwerk kann Schreibzugriff auf Programmdateien und Daten erlangen |
| 5 | externer Eindringling aus dem lokalen Netzwerk kann Schreibzugriff auf Systemdateien erlangen |
| 6 | externer Eindringling aus dem Internet kann Lesezugriff auf Programmdateien und Daten erlangen |
| 7 | externer Eindringling aus dem Internet kann Schreibzugriff auf Programmdateien und Daten erlangen |
| 8 | externer Eindringling aus dem Internet kann Schreibzugriff auf Systemdateien erlangen |

# Artikel Cablecom

## *1. Absolute Sicherheit - die harte Tour*

- Trennen des Modems vom Rechner: Am besten das Verbindungskabel zwischen der im Computer eingebauten Ethernet-Netzwerkkarte und dem Kabelmodem am PC oder Mac herausziehen, die grüne Leuchtdiode an der Karte erlischt, der Computer ist zuverlässig vom Netzwerk und vom Internet getrennt.

- Das Herausziehen des Steckers aus der Maschine kann auch bei eingeschaltetem Computer erfolgen. Dabei ist darauf zu achten, dass der empfindliche Stecker mit zwei Fingern oben und unten angefasst wird, damit der winzige Entriegelungshebel, der die mechanische Verbindung vor unbeabsichtigtem Trennen schützt, niedergedrückt wird.

- Will man dann wieder online sein, braucht man das Kabel nur richtig herum hineinzustecken und ist sofort mit dem LAN und dem Internet verbunden; die grüne Leuchtdiode an der Netzwerkkarte glimmt auf. Das Kabelmodem selbst sollte nicht von dem Anschluss Steckdose in der Wand getrennt werden und auch nicht vom Stromnetz (Netzgerät), um Beschädigungen zu vermeiden.

## *2. Absolute (?) Sicherheit - die weiche Tour*

- Folgendes wurde unter Windows 95 (ohne zusätzliches privates LAN) getestet und gilt angeblich auch für Windows 98SE:

- "Start", "Ausführen..." anklicken. In die Zeile "Öffnen:" die Buchstaben winipcfg (Windows NT, W98 erste Ausgabe: ipconfig) eintippen und auf "OK" klicken.

- Das Tool Internet Protocol Configuration, das bei der Einrichtung der Netzwerkkarte installiert wurde, wird gestartet.

- In seinem Fenster auf "Release" ("Freigeben") klicken, damit wird die Verbindung über die im Listenfeld angegebene Ethernet-Karte gekappt; IP Configuration trennt also »softwaremässig« vom Netz und vom Internet, wenn man den Angaben des Tools trauen darf (mehrere angezeigte Werte springen auf 0.0.0.0). Die grüne LED auf der Ethernet-Karte leuchtet jedenfalls unbeeindruckt weiter; Verbindungen zu Internet-Servern können aber keine mehr aufgenommen werden, die Online-Programme reagieren mit Fehlermeldungen. Um wieder online zu gehen, im selben Fenster den "Renew" ("Aktualisieren") -Button betätigen - die Verbindung ist offensichtlich wieder aufrecht. Für diese Vorgänge können natürlich auch Shortcuts erstellt oder am Desktop oder sonstwo Verknüpfungen angelegt werden.

## *3. Windows 9x: Keine Dateifreigabe installieren*

- Gaaanz wichtig! In die "Systemsteuerung" gehen, dort auf das "Netzwerk"-Icon klicken und nachsehen, ob die "Datei- und Druckerfreigabe" aktiviert ist. In der höchsten Sicherheitsstufe (kein lokales Netzwerk angeschlossen) sollte sie nicht installiert sein und sich nicht aktivieren lassen. Ist der gleichnamige Button dort vorhanden aber nicht anklickbar (grau), dann ist alles soweit sicher. Im Zweifelsfalle kann man das mit den weiter unten angeführten Online-Sicherheitstests überprüfen.

- Ansonsten sind die Einstellungen im Windows-"Netzwerk" exakt so vorzunehmen, wie es im Internet Installationshandbuch, das jeder Kunde bekommt, steht.

- Besonders die Netzwerkkomponenten, die es zu entfernen gilt (NetBEUI), können erhebliche Sicherheitslücken auftun!

- Soll zusätzlich ein privates Local Area Network (LAN) betrieben werden, kommt man um eine sorgfältige Konfiguration dieser Windows-Netzwerkumgebung nicht herum. Dabei sollte man unbedingt wissen, was man tut, sonst kann es ganz leicht passieren, dass hundert Millionen Menschen Zugriff auf die Festplatte haben. Am besten einen Spezialisten konsultieren.

## *4. Windows: Lauscher, Wächter, Firewalls*

- Massnahmen speziell für Linux-Rechner siehe bitte die Linux-Specials. Wer als Security-Anfänger unter Windows 9x über Kabelmodem an das Internet angeschlossen ist und über eventuelle Angriffe und Schnüffeleien von »Hackern« oder »Möchtegern-Hackern« informiert sein will, der möge sich das Programm Jammer (http://www.agnitum.com/) ansehen. Es ist ein sogenannter Low-Level Network Sniffer (Port-Lauscher), läuft im Hintergrund, meldet - auf Wunsch akustisch - jeden Hack-Versuch und bietet an, dem Provider des Verursachers gleich eine entsprechend formulierte eMail zu schicken.
- Aus dem Text der Website: »Jammer erkennt NetBus 1.2, NetBus 1.53, NetBus 1.6, NetBus 1.7, NetBus 2.0 Pro Beta, NetBus 2.0 Pro, Back Orifice 1.2, Back Orifice 1.2 Modified (auch alle modifizierten Versionen von BO, zum Beispiel gepackt und komprimiert mit exe\dll Compression Tools, die von herkömmlichen Virenscannern eher nicht entdeckt werden) und BO2K (Back Orifice 2000).« Die registrierte Version kann angeblich - eventuell eingeschleuste und enttarnte - Trojanische Pferde (Trojaner, deutschsprachige Info-Site) vernichten.

- Wenn also Jammer gluckst und mit dem Auge im Systray zwinkert (Icon nahe der Windows-Uhr in der Startleiste), dann meldet es im Allgemeinen einen sogenannten Port-Scan, das heisst, ein Eindringling von aussen sieht nach, ob er Sicherheitslücken entdecken kann. Die Motive müssen nicht bösartiger Natur sein, meistens versuchen pubertierende Schüler oder Studenten in unbewachten EDV-Räumen vor ihrer Clique Eindruck zu schinden. Nicht nur, um die Meldungen Jammers verstehen und in ihrer »Brisanz« richtig einordnen zu können (es gibt keinen Grund, nervös zu werden), empfiehlt sich das Studium der englischen Hilfe-Datei von Jammer. Dort wird auch erklärt, was der Unterschied zwischen einem Scan (vorerst harmlos aber prinzipiell unerwünscht) und einem Hack (gefährlich, kriminell) ist.

- Für den Laien verständlich ist vielleicht folgender Vergleich: Jemand taucht plötzlich aus dem Nichts auf und drückt, flink wie ein Wiesel, in der Nachbarschaft oder im Stiegenhaus an allen Haus- oder Wohnungstüren die Klinken, um festzustellen, ob eine unverschlossen ist. Oder jemand schleicht behende auf einem Parkplatz herum und versucht dasselbe mit den Autotüren. Jene, die sich besonders schlau vorkommen, probieren es auf ihren Streifzügen auch über den Kamin, den Abwasserkanal und die Belüftungsschächte. Solange dieses Geschlücht nur in Erfahrung bringen will, wo es Möglichkeiten gibt hineinzukommen, handelt es sich um einen Scan. Es kann sich natürlich auch um die Vorbereitung zu einer böswilligen Aktion handeln. Und das wäredann ein Einbruch oder Hack.

- Aufgrund der IP-Adresse des »Hackers«, welche von Jammer oder ähnlichen Programmen »ersnifft« wird (eine Zahl mit mehrere Stellen und Punkten zb. 195.195.195.195), bestehen gute Chancen, dass der Schlingel festgestellt und zur Rechenschaft gezogen werden kann.

- Einer der Vorteile von Jammer ist jedenfalls, dass das Programm relativ einfach auch von Unbedarften installiert werden kann, es muss lediglich unter "Options" - "Monitor" in der Zeile "Current Adapter" die 3com EtherLink-Karte ausgewählt und unter "General" - "Launch on StartUp" angehakt werden. Die Software versieht daraufhin ihren Dienst, ohne den Internet-Betrieb zu beeinträchtigen. Soll Jammer das Versenden der eMails auf Mausklick übernehmen, sind auch noch die eMail-Parameter einzustellen. Nach diesen Konfigurationen muss das Programm neu gestartet werden. Jammer überwacht auch die Registrierungsdatei (Windows Registry), das heisst, es überprüft alle Einträge, die mit Ruhe beginnen. Wenn man also ein neues Programm installiert, das sich in die Registry entsprechend eintragen und automatisch nach dem Booten starten will (auch Trojaner arbeiten so), dann meldet sich Jammer und fragt, ob es diesen Eintrag zulassen soll. Man kann dann mit »Ja« oder »Nein« den Eintrag zulassen oder verweigern.

### *Möglichkeiten von Firewalls*

- Ein Firewall bietet die Möglichkeit, die Kommunikation zwischen dem Internet und einem internen System einzuschränken. Man richtet ihn in der Regel dort ein, wo er seine grösste Wirkung entfalten kann, und zwar an dem Punkt, wo das interne System ans Internet angeschlossen ist. Mit einem Firewall lässt sich die Gefahr verringern, dass Angreifer von aussen in interne Systeme und Netze eindringen. Zudem kann der Firewall interne Benutzer

davon abhalten, das System zu gefährden, indem sie sicherheitsrelevante Informationen wie unverschlüsselte Passwörter oder vertrauliche Daten nach aussen geben. Ein Firewall ist also eine Art von Schutz, der es ermöglicht ein Netz an das Internet anzuschliessen und dabei ein bestimmtes Mass an Sicherheit beizubehalten. Schliesslich gilt es die Daten (gespeicherte Informationen auf den Computern) und Ressourcen (z.B. Rechenzeit oder Plattenkapazität) zu schützen und den guten Ruf der Betreiberorganisation zu wahren.

***Verschiedene Angriffsmethoden***

- Systeme werden auf verschiedenste Art und Weise angegriffen. Im folgenden Abschnitt sind die drei grundlegenden Kategorien erläutert.

***Einbrüche***

- Einbrüche sind die häufigsten Angriffe. Durch Einbrüche können Angreifer fremde Computer für sich benutzen. Die meisten Einbrecher wollen diese Computer wie legitime Benutzer verwenden.

- Eine Angriffsmethode besteht in der Manipulation von Benutzern. Dabei bringt man den Namen eines leitenden Angestellten in Erfahrung, gibt sich beim Systemverwalter als diese Person aus und bittet um die sofortige Änderung seines Passworts, um äusserst wichtige Arbeiten zu erledigen.

- Eine weitere Variante ist einfaches Raten. Um Einbrüche durch Erraten zu verhindern, werden Firewalls meist mit nicht wiederverwendbaren Passwörtern konfiguriert. Selbst wenn diese Technik nicht benutzt wird, liefert ein Firewall eine klar definierte Stelle, an der alle Zugriffsversuche protokolliert werden und somit Einbrüche durch Erraten einfach aufgedeckt werden können.

- Es gibt aber auch technisch sehr raffinierte Einbruchsmöglichkeiten, die keine Kenntnisse über Kennung und Passwörter erfordern.

***Lahmlegen eines Dienstes***

- Ein Angriff durch Lahmlegen eines Dienstes ist einzig darauf ausgerichtet, andere an der Benutzung ihres Computers zu hindern.

- Elektronische Sabotage führt in einigen Fällen zur Zerstörung von Daten oder dem Ausfall von Geräten. Meistens aber arbeitet sie mit Informationsüberflutung; ein Eindringling überlastet ein System oder Netz derart mit Nachrichten, Prozessen oder Netzanfragen, dass keine effektive Arbeit mehr möglich ist. Ein raffinierter Angreifer kann Dienste aber auch deaktivieren, sie umleiten oder ersetzen.

- Manchmal ergibt sich für die Angreifer eine Situation, in der sie kaum verlieren können. Viele Standorte richten zum Beispiel Kennungen ein, die nach einer bestimmten Anzahl gescheiterter Login-Versuche ungültig werden. Dies hindert Angreifer daran, Passwörter so lange durchzuprobieren, bis sie das richtige gefunden haben. Andererseits aber erhalten sie dadurch die Möglichkeit für eine Attacke über die Ablehnung eines Dienstes. Angreifer setzen alle Benutzerkennungen ausser Kraft, indem sie sich einfach einige Male einzuloggen versuchen.

***Informationsdiebstahl***

- Die meisten Informationsdiebe versuchen, sich Zugang zu fremden Computern zu verschaffen; sie suchen nach Benutzernamen und Passwörtern. Dummerweise sind gerade diese die an den leichtesten zugänglichen Informationen beim Abhören eines Netzes. Bei vielen Netzwerkinteraktionen befinden sich Benutzername und Passwort amAnfang und können in derselben Form auch wiederverwendet werden.

- Verschärfend kommt hinzu, dass bei den meisten gängigen Netztechnologien wie Ethernet oder Token Ring jeder Rechner im lokalen Netz den gesamten Netzverkehr abhören kann. Über das Internet gesendete Daten durchlaufen zahlreiche lokale Netze, und jedes dieser Netze kann einen Schwachpunkt darstellen. Service-Provider und allgemein zugängliche Systeme sind beliebte Angriffsziele. Informationsdiebstahl mussnicht unbedingt Spuren hinterlassen, und selbst Einbrüche werden relativ selten sofort entdeckt. Jemand, der einbricht, Daten kopiert und ohne etwas zu zerstören wieder verschwindet, hat an den meisten Standorten gute Chancen, unentdeckt zu bleiben.

- Es gibt verschiedene Möglichkeiten, sich gegen Informationsdiebstahl zu schützen. Ein gut konfigurierter Firewall schützt einen vor Benutzern, die mehr Informationen zu erlangen versuchen, als man herausgeben möchte. Hat man jedoch erst einmal beschlossen, Informationen über das Internet zu verbreiten, ist es sehr schwierig zu verhindern, dass diese Informationen in die falschen Hände gelangen. Dies kann durch Vorspiegelung falscher Tatsachen oder durch Abhören des Netzes geschehen. Vor diesen Risiken kann ein Firewall nicht schützen, da sie erst auftreten, nachdem die Informationen das eigene Netz wie beabsichtigt verlassen haben.

***LockDown 2000***

- Ausführliche Logfiles sowie Multi-Userfähigkeit zeichnen das Shareware-Programm aus.
- Wer sich in die Materie hineinarbeiten will, erhält hier eine den kompletten Überblick. Für
- Anfänger eher ungeeignet ist die detaillierte Aufschlüsselung aller verfügbaren

- Die bisherigen Beurteilungen der User sind unterschiedlich. Aus dem Text der Website: »LockDown 2000 wurde entworfen und entwickelt, um Internet User davor zu bewahren, von - sogar den ausgefuchstesten - Hackern bedrängt zu werden. LockDown 2000 sorgt für vollständige Sicherheit und eine geschützte Privatsphäre, wann immer Sie online sind.« - »LockDown 2000 was designed and developed to protect Internet users from being hacked by even the most sophisticated Hacker. LockDown 2000 provides complete security and privacy whenever you go online.« Das klingt für unseren Geschmack eindeutig übertrieben, seriöse Security-Unternehmen dürften das eigentlich nicht so formulieren. ***Complete Security gibt es einfach nicht***.

- Dieses Programm wird hier erst dann ausdrücklich empfohlen, wenn erfahrene User ihre positiven Kommentare abgegeben haben. Hier gibt es ein paar eher verhaltene Tests dazu: PCHelp Tests LockDown 2000 und Test and Review: Lockdown 2000 v2.5.4. In öffentlichen internationalen Diskussionsforen hält sich hartnäckig das Gerücht, LockDown 2000 versende heimlich Daten, und man solle besser die Finger davon lassen! Wir lassen den Hyperlink zu LockDown 2000 auf unserer Webseite vorerst nur deshalb stehen, damit die Sammlung komplett ist.

- Die Funktionen dieses Produkts sind auf Schutz vor simplen DoS-Angriffen und **NETBIOS-Zugriffen** beschränkt. Der Sinn, den Zugriff über das **NETBIOS-Protokoll** anzuzeigen, ist anfechtbar, doch funktioniert dies wenigstens ohne grössere Komplikationen: Ein schön dargestelltes Protokoll erlaubt eine detaillierte Analyse des Verhaltens eines potentiellen Eindringlings. Der Performance-Verlust, der mit Installation und Nutzen dieser Software in Kauf genommen werden muss, kann aus meiner Sicht absolut nicht gerechtfertigt werden. Komischerweise gewinnt LockDown 2000 relativ viel an Zuneigung aus den Reihen der etwas unerfahrerenen Endanwender.

Preis: 99 Dollar
Info: LockDown Corp
44P Dover
Point Office
Pk, Dover
Point
Rd.Dover, NH

03820

http://lockdown2000.com/

***eSafe Protect Desktop***

- Lokaler Schutz von Dateien und Firewall-Funktionen bilden die Basis von E-Safe Protect. Das Produkt ist die Client-Komponente eines vollständigen Firewall-Konzepts, das Elemente für die eigentliche Firewall, den Schutz von Servern und Clients, umfasst. Der Schutz umfasst drei Bereiche: Ressourcen-Schutz, Virenscanner und Schutz vor ActiveX-Controls und Java-Applets. Die Utility-Suite läuft unter Win95, 98 und NT und ist 30 Tage komplett funktionsfähig.

- Sehr üppig. Hatte ihn ein halbes Jahr laufen. Der Nachteil beim eSafe: Er ist ein mörderischer Ressourcenfresser. Wenn man mit seiner Kiste nicht hauptsächlich surft, sondern zum Beispiel öfter spielen will, ärgert man sich über den Leistungsverlust. Und noch was: Das integrierte Antivirenprog duldet - wie alle Virenscanner - kein anderes neben sich, liess aber däumchendrehend gleich 2 Viren (zum Glück nur harmlose) übers Web herein - ungeachtet der regelmässigen Signatur-Updates. Die infizierten Files lagen wochenlang auf der Festplatte. Hab' ich erst feststellen können, nachdem ich eSafe deinstalliert und McAfee in Betrieb genommen hab'.

- Alladin verlautbart, dass neue Versionen (2.2) von eSafe Desktop und Enterprise herausgekommen sind. Originalton: »Die beiden Produkte sind neu, verbessert, erweitert und bieten zusätzliche Sicherheit. Die neue Version enthält viele Verbesserungen, darunter unsere exklusiven Sandbox II und Personal-Firewall-Technologien. Surfen Sie sicher durch das Web im Wissen, dass sie von einem vollständigen und verlässlichen System vor bekannten und unbekannten Hackern, barbarischen Bedrohungen und Attacken geschützt werden. eSafe Desktop ist nun für alle Home-User inklusive aller Virus- und Vandal-Signatur-Updates gratis und kann über die Aladdin-Webseite bezogen werden.«
- Als besonderes Feature zu empfehlen ist der integrierte Viren-Scanner für eMails. Leider wurde keine passive Scan-Option für Daten eingebaut, die direkt aus dem Internet geladen werden: Werden zuvor heruntergeladene ausführbare Dateien exekutiert, wird eSafe Protect die Gewalt über deren Inhalt aus den Händen gerissen, und möglicher Schaden kann durch diese Dektop-Firewall nicht eingegrenzt oder verhindert werden. Jenem Missstand kann das Festlegen von bestimmten Sicherheitszonen Abhilfe schaffen, damit die Programme nicht einfach als ›unbekannte Anwendung‹ von Aladdins Firewall ausgeführt werden, was natürlich mit erhöhtem Aufwand verbunden ist. Die Standardkonfiguration bietet nahezu keinen Schutz vor möglichen Attacken. Dank bedienerfreundlicher Oberfläche gestaltet es sich jedoch auch für ungeübte Anwender als niedrige Hürde, das Tool den eigenen Bedürfnissen anzupassen. Neben einer kostenlosen Desktop-Version bietet Aladdin eine Enterprise-Variante mit zentraler Steuerung und Wartung an, welche mehr Features - wie das Weitergeben von verdächtigem Inhalt an eSafe - bietet.«

Aladdin Knowledge Systems GmbH
http://www.aladdin.de/

Secure4U
Kurzbeschreibung:

***ZoneAlarm***

Kurzbeschreibung:
Ein gutes Netzwerküberwachungs-Tool. Schützt vor den gefährlichen VB-Scripts wie dem Virus Loveletter und anderen mit der "MailSafe" Funktion!!! Fragt bei jedem Programm welches eine Verbindung zu ihrem Computer oder aus ihrem Computer ins Internet nach, ob diese gestattet ist. Das heisst natürlich auch, dass z.B. bei ihrem Browser nachgefragt wird. Mit ZoneAlarm2.1.25 lässt sich auch die Verbindung für verschiedene Programme ganz unterbinden!!

Detaillierte Infos:

Ein recht gutes Programm, es ist gratis. Alles läuft wie geschmiert. Bin nach der Installation zu einer Test-Site gegangen, die haben sich gewundert, dass eine Windows-Maschine so dicht sein kann; das einzige Loch fanden sie im POP, da sie aber meine Maschine nicht sehen konnten, wären sie als Hacker gar nicht dorthingegangen.

Die Installation ist extrem einfach. Danach fragt es für jedes Programm, ob man dieses
Programm ins Netz gehen lassen will. Da kann man ›Yes‹ oder ›No‹ wählen, und wenn
man vorher ein Hakerl mittels Mausklick macht, fragt es das nächste Mal nicht mehr -
ohne Anhaken fragt es jedes Mal. Man kann aber auch alles sperren, sozusagen als Notbremse; das heisst dann Emergency Lock. Wenn man das normale Schloss (Lock)
nimmt, lässt es nichts durch, was nicht vorher mit einem grünen Haken abgehakt wurde.
Mir kommt es wesentlich einfacher zu benützen vor als alle anderen Sachen, die ich vorher versuchte.

Aus der Webseite: Besorgen Sie sich den notwendigen Schutz für Ihren über DSL oder
am Kabel angeschlossenen Computer. Erfreuen Sie sich an der einfachen Installation
und den flexiblen Einsatzmöglichkeiten. Halten Sie Hacker davon ab, Ihren Computer zu finden. Entdecken und stoppen Sie Trojanische Pferde und Spyware. Schützen Sie sich gegen unbekannte Gefahren. Halten Sie Ihre Maschine und Ihre sensiblen Daten sicher. Teilen Sie sich nur Menschen mit, denen Sie vertrauen. Beachten und kontrollieren Sie alle Anwendungen, die das Internet von Ihrem Computer aus benutzen. Lernen Sie das ruhige Gewissen zu schätzen, wenn Sie Ihre Maschine in Sicherheit wiegen.

***Zone Labs,***

Inc.
530
Howard
Street
#350

San
Francisco,
CA
94105

Preis: Freeware (Gratis)

http://www.zonelabs.com/

***Black ICE Defender***

Kurzbeschreibung:

Black Ice Defender ist ein sogenanntes Intrusion-Programm(Intrusion=Einbruch), das praktisch alle eingehenden Datenpakete durchcheckt und blockt, aber den normalen Ablauf im Web nicht stört. Dies geschieht dadurch, das Black Ice passiv im Hintergrund läuft und somit auch nicht durch Hacker beispielsweise ausgeschaltet werden kann oder entdeckt werden kann. Dieses Tool eignet sich ausgezeichnet als Zusatztool zu einer Firewall. Was ausserdem positiv auffällt, ist der Umstand, das man dieses Tool auch als Anfänger nutzen kann, da es keine grossartige Konfiguration erfordert. Von der Grösse her nimmt es kaum Platz auf der Platte ein und verbraucht kaum Ressourcen !

Detaillierte Infos:

Black ICE Defender untersucht im Hintergrund sämtliche Datenströme auf Hackversuche oder zerstörerische Inhalte. Dazu dienen leistungsfähige Echtzeit-Scanner ohne merklichen Einfluss auf die Systemleistung. Besonders stark erweist sich Black ICE beim Test mit dem NAI-Cybercop-Scanner. Sogar im Betriebssystem angelegte Schwachpunkte wie mögliche Port-Scans behebt Black ICE und verhindert so Hackversuche zuverlässig. Per IP-Filter lässt sich der Zugriff auf IP-Adressen blocken. Attacken protokolliert Black ICE mit deren IP- oder DNS-Adresse. Von der Network-ICE-Website sind Details über Art und Gefahr des jeweiligen Angriffs abzurufen. Features zur Überwachung von Mails und Anhängen fehlen jedoch.
Im Test wurden ferner Skripte fälschlicherweise als unkritisch eingestuft, die den Nutzer durch eingeblendete Fenster auf dem Desktop stören. Insgesamt überzeugt Black ICE aber beim Test mit Javascript- und ActiveX-Content. Allerdings blockiert das Tool aber auch erwünschte Zugriffe auf das System, beispielsweise bei Netmeeting-Konferenzen Aufgrund fehlender Konfigurations-Optionen lässt sich das nicht ändern. Statt dieser bietet Black ICE nur mehrere Sicherheitsstufen zur Wahl. Das vereinfacht zwar das Setup, lässt dem Profi aber zu wenige Optionen. Für den Einsatz im LAN gibt es jedoch die Version Black ICE Pro, die neben mehr Konfigurations-Optionen ein zentrales Management und einen Scanner zur Prüfung der Systemsicherheit bietet.

Info:
Network ICE
International

and EMEA
Headquarters
Royal Albert
House
Sheet Street,
Windsor, Berks
SL4 1BE
United Kingdom
Phone: +44(0)
1753 705140

Preis: 39.95
Dollar

http://www.netice.com/

***Conseal PC Firewall 1.35***

Kurzbeschreibung:

Während Sie arbeiten, läuft ConSeal PC Firewall unbemerkt im Hintergrund. Das Utility blockiert unerwünschten Netzwerkverkehr, sowohl eingehenden als auch ausgehenden, und lässt nur autorisierte Daten durch. Über ein Regelset wird gesteuert, welche Datendurchgelassen und welche blockiert werden. Sie können für alle Netzwerkgeräte IhresSystems ein Regelset anwenden oder jedem Gerät separate Regeln zuordnen. ConSealPC Firewalls Basiskonfiguration liefert Schutz gegen die meisten Angriffe auf IhrNetzwerk. Das Regelset lässt sich mit Hilfe eines benutzerfreundlichen Assistenten einfach Anpassen. Die unregistrierte Version ist 15 Tage komplett funktionsfähig.

Detaillierte Infos:

Firewall-System, das selbst professionellen Anforderungen gerecht wird. Leider fehlt es an Zusatzausstattung. Das einzige Produkt im Testfeld, das bezüglich der Firewall-Funktionen an Unternehmenslösungen heranreicht, ist PC Firewall von Conseal.

Das Programm reagiert auf alle gängigen Netzwerkpaket-Typen und unterstützt eine Vielzahl von Protokollen.
Neben TCP/IP-Paketen werden auch NetBEUI und IPX unterstützt.

Im Mittelpunkt steht ein Regelset, das Filter- und Blockierfunktionen definiert, wobei für jeden Netzwerkadapter eigene Regel festgelegt werden können. PC Firewall ist mit einem vordefinierten Regelsatz ausgestattet, der laut Angaben der Entwickler für die meisten Netzwerkattacken ausreichenden Schutz bietet. Als besonders flexibel erweisen sich die vielfältigen Konfigurationseinstellungen des Regelwerks. Das Programm sieht drei Modi vor: Checked Learning Mode, Unchecked Learning Mode und Manual Mode. Im ersten Fall, dem Standardmodus, erweist sich das Programm als »lernfähig«: Ist für eine bestimmte Anforderung keine Vorgabe für Reaktionen festgelegt, kann der Anwender diese über eine Auswahlbox festlegen. Im zweiten Fall wird eine Regel zu dem Regelset hinzugefügt, wenn eine nicht vorgesehene Anfrage erfolgt. Der Modus »Manual« richtet sich an erfahrene Anwender: Hier können Aktionen von Hand definiert werden. Im Praxiseinsatz hinterlässt PC Firewall einen guten Eindruck. Sucht ein anderes System Zugang zum eigenen Rechner, kann der Anwender über das zugehörige Fenster den Zugriff erlauben, blockieren oder einfach ignorieren. Die Infobox führt die IP-Adresse des "Angreifers" und das verwendete Netzwerkprotokoll auf. Zudem kann man dem Eindringling für die aktuelle Session den Zugriff erlauben und das Regelset bearbeiten. Auch die Programmeinstellungen zeigen, dass sich PC Firewall an den ambitionierten Anwender wendet, der nicht nur mit der Terminologie, sondern auch mit den erweiterten Funktionen umzugehen versteht. Der durchschnittliche Anwender dürfte damit überfordert sein. Schwach fällt die Zusatzausstattung aus: Die PC Firewall verfügt weder über einen integrierten Virenscanner noch über andere Sicherheitsmechanismen.

Info:

Network ICE International and EMEA
Preis: 39.95 Dollar
http://www.netice.com/

5. Linux-Firewalls auf separatem Computer  Netzwerk-Spezialisten empfehlen, zum Beispiel einen alten 386er-PC, auf den nicht viel anderes als eine solche Linux-Firewall installiert ist, zwischen das Cable Modem und dem »eigentlichen« Computer über ein separates Netzwerk (Netzwerkkarten erforderlich) einzuklinken. Das erfordert allerdings einiges technisches Know-How, bietet dafür angeblich ein hohes Mass an Sicherheit.
Eine Firewall ist nur so gut wie der, der sie betreibt. Das Programm X installieren, und alles ist erledigt - so einfach spielt es sich bestimmt nicht ab. Benötigte Software gibt es bei Linux Router Project und Trinux (eine Diskette macht den PC zum Router). Es gibt auch mehrere Linux Firewall HOWTOs: Firewalls FAQ und Internet Firewalls Frequently Asked Questions. Als weitere feine Adresse wird Hali Tower (Linux Firewall and Security Site) ans Herz gelegt.

Als Anhang zu der vorliegenden Website Sicherheit im Kabelnetzwerk sind unter Linux Specials (Kapitel 9) angefügt, wo Vorkehrungen gegen Eindringlinge auf Stand-Alone-Rechnern mit Linux als Betriebssystem geschildert werden.

6. Take care! Viren, Trojaner

Als Trojaner bezeichnet man diejenigen Programme, die (als Nutzprogramm getarnt) im Verborgenen Daten ausspähen und diese an einen Angreifer übermitteln, z.B. per E-Mail, FTP, ICQ, IRC, NNTP (Newsgroups). Genaugenommen sind auch die Programme, die Backdoors einschleusen, als Trojanische Pferde anzusehen.

Folgendes gilt freilich für jeden Anschluss an ein Netzwerk und nicht nur für Cable Modem Internet, ebenfalls für jede Datei von einer Diskette oder CD oder sonst irgendeinem Datenträger, der »von draussen« kommt:
Seien Sie äusserst kritisch bei jeder Datei, die Sie vom Internet herunterladen!
Das kann gar nicht oft genug wiederholt werden. Selbst Computerprofis vergessen gelegentlich darauf.  Besonders »ausführbare« Dateien (Windows: *.exe) von unsicheren oder unseriösen Quellen können potentiell zerstörerische oder spionierende Programme enthalten! Es soll sogar schon als *.zip gekennzeichnete gepackte Dateien geben, die eigentlich getarnte *.exe-Dateien sind. Also:

Vor jedem Entpacken oder Starten einer Datei oder eines Setup-Programms unbedingt den bevorzugten Virenscanner (siehe bitte weiter unten) darüberrasseln lassen, und selbst das ist kein hundertprozentiger Schutz!

Dateien, die an eMails oder Usenet-Artikel angehängt sind, sogenannte »Attachments« (Datei-Beilagen), von denen man nichts weiss (die man also zum Beispiel nicht ausdrücklich bestellt hat) oder nicht einmal den Absender kennt, sollten sofort gelöscht und keinesfalls geöffnet, entpackt oder gestartet werden! Alle eMail-Programme und Newsreader sind so eingestellt, dass man den Text-Körper der Postings gefahrlos lesen kann - das womöglich verhängnisvolle Betrachten oder Öffnen der angehängten Dateien muss immer ausdrücklich extra befohlen und ausgeführt werden. Besonders gefährlich sind eMails oder Artikel aus Newsgroups, deren Text-Inhalt oder der Name des Attachments sympathisch und besonders harmlos klingt (happy2000, I love you)! Die weitaus meisten Computer-Viren und -Würmer werden auf diese Weise übertragen!
Microsoft-Office-Dokumente, besonders Word-Dateien *.doc, sollten prinzipiell nur ineinem Viewer und nicht in Word oder Excel selbst geöffnet werden! (Dieser Link führtdirekt zum Download des Microsoft Word Viewers für Windows, mit dem gefahrlos Word-Dokumente betrachtet - aber nicht bearbeitet - werden können.) So kann zum Beispiel aus der Preisliste eines grossen, bekannten Computerhändlers (gefälschte Angabe im Absender) mit sensationellen Angeboten rasch grösstes Ungemach entstehen.
Aber auch Java, Java-Script, ActiveX-Controls und andere HTML-Erweiterungen können solche Trojaner auf Deine Festplatte bringen, während Du ahnungslos im Internet surfst. Abhilfe bringt da nur die höchste Sicherheitsstufe bei den Browsern; der Nachteil ist dann allerdings, dass auf diese Weise ein Teil der Show im Netz nicht »empfangen« werden kann. Ein schwieriges und heikles Thema.
Die deutsche Computer-Fachzeitschrift c't bietet einen Check auf Verwundbarkeiten durch Würmer wie den »I love you«-Virus an. Von hier aus kann man sich eine eMail zuschicken lassen, welche die aktuellen Sicherheitseinstellungen des eMail-Programms überprüft. Die kritischen Einstellungen, die diese eMail kontrolliert, betreffen primär Outlook und Outlook Express von Microsoft, aber auch andere Software, die den Internet Explorer nutzt, um in HTML abgefasste eMail anzuzeigen. Die genauen Eigenschaftendieses Tests und die Beseitigung möglicher Verwundbarkeiten werden dort genau beschrieben.

Warnung bei c’t-eMail-Check

7. Virenscanner
Wichtig ist, darauf hinzuweisen, dass jeder User einen guten Virenscanner verwenden sollte, der a) was taugt?? und b) sich per Netz regelmässig aktualisiert. Gefährlich sind ja die Trojaner wie netbus, Bo etc., und ohne ordentlichen Virenscanner können Ihnen die Viren mit jedem Programm unbemerkt eingeschleust werden, - und schon sind alle Ihre Sicherheitsschlüssel entfernt worden.

Der Virenscanner von AVP Advanced Virus Protection schnitt bei mir ganz gut ab, wogegen Norton und McAffee viele der ›alten‹ Viren nicht einmal fanden, was mich eigentlich ziemlich verwunderte (marburg.a).« Aktueller (April 2000) Artikel (ProductReview) (englisch) über AntiViral Toolkit Pro von West Coast Publishing.
Es gibt Virenscanner, die auf Trojaner spezialisiert sind: The Cleaner für Windows95, 98, NT, 2000 Pro von MooSoft, nach eigenen Angaben werden damit weitaus mehr Trojaner entdeckt als mit herkömmlichen Virenscannern, und TDS - Trojan Defense Suite 2 für Windows von Diamond Computer Systems.

Mit dem Online-Virenscanner von Trend Micro, Inc. kann auf der Stelle - live sozusagen - das heimische Computersystem gratis auf Viren überprüft werden. An anderer Stelle auf unserer Webseite gibt es Ausführlicheres zu diesem Online-Virenscanner.
Das Produkt PC-cillin 2000 für Windows vom selben Hersteller muss wie üblich installiert werden. Zeitbeschränkte Evaluierungs-Version steht zum Download bereit.
Ebenfalls gratis ist InoculateIT Personal Edition für Windows 95/98/NT von Computer Associates, nur das Ausfüllen eines Registrationsformulars ist erforderlich. Die Firma bietet auch Free Unlimited Upgrades für die Software und die Virus-Definitionsdateien.
Auf der Webseite steht: »InoculateIT Personal Edition basiert auf einem der weltweit führenden Anti-Virus-Produkte, das bei unabhängigen Vergleichstest durchwegs gut abschneidet.« Das Programm entdecke automatisch herkömmliche Datei- und Boot-Sector-Viren und reinige das System davon, gleichermassen werde mit Macro-Viren verfahren, so der Hersteller. Es biete ausgezeichneten Schutz gegen Internet-Viren und solchen, die von eMails stammten, und bewahre den PC vor infizierten

Dateien, die von Webseiten aus aller Welt heruntergeladen, oder vor infizierten Datei-Beilagen, die per eMail geschickt würden.

Einen neuen Scanner gegen Trojanische Pferde gibt es von Agnitum, dem Hersteller von Jammer. Er heisst Tauscan 1.0 und läuft unter Win 95,98,NT,2000. Agnitum beschreibt das Produkt als das einzige, das für Business- und Home-User eine komplette Lösung gegen die Bedrohung durch Trojaner darstellt. »Tauscan ist ein universeller Trojaner-Scanner, der fast tausend Viren der Sorte Trojanisches Pferd entdeckt, die auf dem Computersystem eines Anwenders installiert sein könnten. Diese Zahl ist beinahe doppelt so hoch als die vieler vergleichbarer Produkte. Diese neue Software wurde auch für den Bedarf von Anfängern konzipiert, und sie enthält innovationsfreudige Ausstattungsmerkmale, die in keiner ähnlichen Anwendung gefunden werden können.
Diese Neuerungen beinhalten Drag & Drop-Scannen, Rechtsklick-Scannen und einen anwenderfreundlichen Wizard, um nur einige hervorzuheben. Falls Sie auf Ihrem System bereits unsere Anwendung Jammer installiert haben und diese mit Tauscan ergänzen, so verwandeln Sie es in eine uneinnehmbare Festung. Diese beiden Software-Produkte arbeiten hervorragend zusammen und vereiteln jeden Versuch, in Ihr System mittels bösartiger Programme einzudringen. Wir erfanden Tauscan und hatten dabei stets Jammer im Gedächtnis. Der Mechanismus, mit dem die beiden Produkte einander ergänzen, ist sehr einfach. Während Jammer sich um die Aufgabe kümmert, das Netzwerk zu beobachten, und damit viele Funktionen einer Firewall bietet, verhält sich Tauscan als eine zweite Verteidigungslinie, die alle Trojaner entdeckt und entfernt, die es geschafft haben, Ihr System über andere Wege zu infiltrieren.«Testbericht auf der deutschen Trojaner-Info-Site. Tauscan ist Shareware, es gibt eine Trial-Version zum Download (dreissig Tage, die Registrierung kostet dreissig US-Dollar, auch günstigeres Kombi-Angebot Jammer/Tauscan vorhanden), ebenso ein ausführliches Free Tauscan Tutorial in Form einer schicken Flash-Bedienungsanleitung.
Gratis Online-Viren-Check von Symantec für Windows 9x mit Internet Explorer.

Weitere Virenscanner:

# DEFINITIONS

## *ActiveX*

- Stellt eine grosse Sicherheitsbedrohung im Internet dar.
- ActiveX ermöglicht die Ausführung von beliebigem Binärcode.
- Eine bösartige ActiveX-Komponente kann geschrieben werden, um Dateien auf der lokalen Festplatte eines Benutzers zu verändern oder zu löschen, oder um eine Verbindung zu einem anderen Computer herzustellen, ohne dass der Benutzer dies merkt oder dem zustimmt.
- Ausserdem besteht immer das Risiko, dass eine an sich harmlose ActiveX-Komponente mit einem Virus behaftet sein könnte.
- Leider können Viren genauso leicht verschlüsselt werden wie gewöhnlicher Code.
- Im Grunde ist ActiveX nämlich nichts anderes als ein weiterentwickeltes OLE

## *Add-On Security*

- Security protection mechanisms that are hardware or software retrofitted to a system to increase that systems protection level.

## *Apple Pay*

- Kreditkarte direkt im ***iPhone*** (ab Generation 6) oder der ***Apple Watch*** hinterlegen.
- An der Kasse bezahlen (EFTPOS).
- Apple Pay nutzt ***Face ID*** oder ***Touch ID.***
- Mit Apple Pay wird Ihre Kartennummer nie auf Ihrem Gerät oder Apple Servern gespeichert.
- Apple Pay speichert auch keine Daten zu Ihrer Transaktion, die auf Sie zurückzuführen sind.
- Bezahlt werden kann überall wo dieses Symbol gezeigt wird:


## *Applets*

- In fact, applets are actually self-contained miniature programs that execute independently of the server that sent them.

### *Java Applets*

- Needs the Java Virtual Machine (JVM).
- Code can be shared between operatings systems without modification.
- Works as "sandboxing" system and is more secure than ActiveX.

### *ActiveX Controls*

- Uses proprietary Microsoft technology and therefore can execute only on systems running Microsoft browsers.
- Gains full access to the Windows operating environment and can perform a number of privileged actions.

## *AS400 - The AS/400 Gopher Client*

MS Windows  Hgopher, Ws_Gopher

## *Attacker*

- Malicious intruder.
- Some attackers my want to ***disable system***, whille other attackers my want to ***steal data***.

## *Authenticode*

- Sicherheit von Downloads aus dem Internet. Microsoft digitale Signaturtechnologie.

## *BGPSec*

- Prevents ***route hijacking*** but causes delayed route convergence and does not support prefix aggregation which contributes to reduce scalability.

## *Blue Coat*

- **Blue Coat Systems Inc.**, formerly **CacheFlow**, is a corporation headquartered in Sunnyvale, California and owned by Symantec.
- It provides hardware, software, and services designed for cybersecurity and network management.

## *C2*

- AS400 received the C2 rating from the "U.S. Gouvernement Department of Defense(DoD)" for all OS versions up to V4R1M0.

http://www.raium.ncsc.mil/tpep/epl/entries/CSC-EPL-95-006-C.html

## *CAP - Conditional Access Policies*

- Includes support for access policies based on group, location, or device state.
- The location feature allows to differentiate IP addresses that don't belong to your network, and satisfies their security policy to require multi-factor authentication from all such locations.

## *Captcha*

- Distinguishes humans from computers.
- Completely Automated Public Turing test to tell Computers and Humans Apart.
- Machine Learning makes some types of **captcha** useless.
- Criminals xould sometimes have 1000 different Captchas solved for about a dollar, this enables DDoS attacks and sending of spam E-Mails

## *CASB - Cloud Access Security Broker*

- Der Cloud Access Security Broker (CASB) ist ein Service oder eine Anwendung, die ***Cloud-Applikationen absichert***.
- Der Cloud Access Security Broker soll die in die Cloud verlagerten Anwendungen eines Unternehmens oder einer Organisation schützen.
- Der Cloud Access Security Broker (CASB) steht als Wächter zwischen Anwender und Cloud überwacht die Kommunikation und kann so feststellen, ob ein Anwender berechtigt ist auf die Anwendung zuzugreifen, bei verdächtigen Aktionen, kann CASB ***alarmieren***.
- Dank der Verwendung eines CASB lassen sich die intern einzuhaltenden ***Sicherheitsrichtlinien*** auf externe Services ausweiten und durchsetzen.
- Dies kann beispielsweise notwendig werden, um die ***Compliance Richtlinien*** einer Organisation oder eines regulierten Wirtschaftsbereichs zu erfüllen.
- Unerwünschte Nutzung von Cloud-Services, wie sie durch eine ***Schatten-IT*** entstehen kann, wird durch den CASB verhindert.
- Der CASB ermöglicht es darüber hinaus, sichere Zugangsvoraussetzungen zu schaffen, indem User sich authentifizieren und sämtlichen Verkehr verschlüsseln.
- Die ***Security-Policies*** werden im Vorfeld definiert und anschliessend vom Cloud Access Security Broker überwacht.
- Weitere Anwendungsbereiche sind das ***Logging*** sämtlicher Aktionen in der Cloud und die Überprüfung der Cloud-Nutzung zu Abrechnungszwecken mit dem Provider.

## *CDOC - Cyber Defense Operations Center*

- See Microsoft

## *CCTV - Closed-Circuit Television*

- CCTV enables you to compare the audit trails and access logs with a visual recording of the events.

## *CKIP - Cisco Key Integrity Protocol*

- Layer 2 - Security Feature

## *Clipper Chip*

- The Clipper Chip was a chipset that was developed and promoted by the ***NSA*** as an encryption device, with a ***built-in backdoor***, intended to be adopted by telecommunications companies for ***voicetransmission***.
- It was announced in ***1993*** and by ***1996*** was entirely defunct.
- The Clipper Chip made use of the ***Skipjack*** algorithm, which is a symmetric ciper that uses an ***80-bit key***.

## *Compound Authentication*

- Any method that uses a ***series of authentication methods***, possibly with different credentials at different stages, is a compound authentication method.
- The most notable examples are the TLS tunneling methods used on wireless networks (***TTLS*** and ***PEAP***), as well as the eXtended Authentication (***XAUTH***) comonly used with IPSec.

## *Concealment Cipher*

- Is a symmtric key, transposition cipher where the words or characters oft he plaintext message are embedded in a page of words or characters at a consistent interval.

## *CONTROLS*

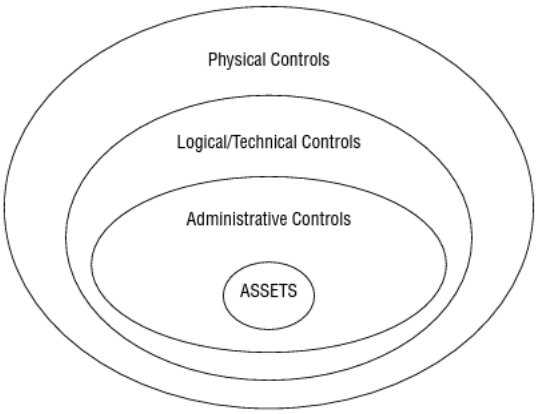



**Abbildung 2: The categories of security controls in a defense-in-depth implementation**

***Procedural Controls (Administrative Controls)***

- Procedural controls codify how people should conduct themselves and their activities within the organization. Procedural controls most often exist as official policies, standards, procedures, and guidelines that formally define behavior within the organization.

***Logical Controls / Technical Controls***

- Logical controls are technology solutions that manage risks in the digital world.
- Logical controls include many familiar security technology solutions like firewalls, intrusion detection system (IDS), data loss prevention (DLP) systems, network access control (NAC), and other solutions.

***Examples***

- Authentication methods, such as usernames, passwords, smartcards and biometrics, encryption, constrained interfaces, access control lists, protocols, firewalls, routers, IDS and clipping levels.

***Physical Controls***

- Physical controls manage risks in the physical world.
- Physical security solutions, for example, prevent inappropriate physical access to offices, data centers, and other facilities.
- Other physical controls include environmental detection and remediation solutions such as smoke detectors, motion sensors, sprinklers, and generators.

***Access Control Readers***

- System sensing access control readers, also called ***transponders***, recognize the presence of an approaching object within a specific are.
- This type of system does not require the user to swipe the card through the reader.
- The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

***Vibration Control Devices***

- They are vulnerable to non-adversarial disturbances

***Heat-Activated Detectors***

- For earliest possible warning, place them below the raised floor and suspended ceilings.

***Preventive Controls***

- Preventive controls protect the organization by precluding a threat from exploiting a vulnerability.
- This type of control proactively prevents a risk from being manifested.
- Preventive controls are optimal because they actively work to prevent exploitation of a vulnerability.
- ***Preventive/physical controls*** are meant to discourage a potential attacker using items put into place to protect facility, personall, and resources.

***Examples:***

- Password Management
- Passwords, biometrics, smart cards
- Encryption, secure protocols, call-back systems, database views, constrained user interfaces
- Antimalware software, access control lists, firewalls, intrusion prevention systems

***Detective Controls***

- Detective controls identify the existence of anomalous or improper activity.
- Although detective controls identify potential threats, they take ***no action*** to prevent or address the threat.
- Solutions designed to reveal bad behavior for follow-up by security operations personnel are detective controls.
- Detective controls are important, especially when preventive or corrective controls are difficult to implement.
- In addition, detective controls provide an important service in a layered defense approach because they can identify control failures in preventative and corrective controls.
- ***Detective/physical controls*** helps to identify an incidents activities and potentially an intruder using items put into places to protect facility, personell, and resources. This items include motion detectors and CCTVs.
- ***Detective/technical controls*** helps to identify an incidents activities and potentially an intruden using softtware or hardware components, which include Audit logs and ids.
- ***Detective/administrative controls*** helps to identify activities and potentially an intruder using management-oriented controls, which include monitoring and supervising, job rotation, and investigations.

***Corrective Controls***

- Corrective controls modify an environment and take action to restore the environment to its normal operating state.
- An intrusion detection system (IDS) functions as a detective control because it identifies the existence of improper activity.
- An intrusion prevention system (IPS) functions as a corrective control because it can terminate unauthorized sessions or take other action to stop an attack and restore services.

***Deterrent Controls***

- Deterrent controls discourage the exploitation of a vulnerability or system.
- For example, a warning banner that provides system-use notification acts as a deterrent to discourage unauthorized access to a system.

- This type of control does not prevent unauthorized access, but helps deter this unauthorized access.

***Compensating Controls***

- A compensating control exists when the recommended approach to implement a control is too expensive, too impractical, or too difficult.
- The compensating control provides an alternative approach to achieve the intended outcome.

## *Cookies*

- Sind so etwas Ähnliches wie der Stempel, den Sie auf die Hand bekommen, wenn Sie eine Disco besuchen.

cookies.txt
c:\windows\cookies

***Google Chrome***
Stores the cookies in a SQLite database file.
Use: SQLite Database Browser
C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Cookies

Cookie-cutter programm zum cookie management.

| ***Programm*** | ***URL*** |
|---|---|
| Cookie Pal | http://www.kburra.com/cp1setup.exe |
| CookieCutterPC | http://ayecor.com/software/cc32/ccpc32.zip |
| Anti-Cookie | http://users.derbytech.com/~gregeng/cookie10.zip |
| Cookie? NOT! | http://www.geocities.com/SiliconValley/Vista/2665/bake.zip |

## *Covert Channels*

- A ***covert channel*** is a method that is used to pass information over a path that is ***not normally used*** for communication.
- Covert channels are one of the ***important examples of vulnerabilities of security architectures***.
- ***Shared resource matrix*** is a technique commonly used to locate covert channels.
- A covert channel is an intentional communications path that is ***hidden***, using a technique like ***steganography***.

## *Cracker*

- Are malicious individual's intent on waging an attack against a person or system.
- Crackers are simply ***criminal***.

Ein **Cracker** ist jemand, der böswillig in die Systemintegrität eines entfernten Rechners einbricht bzw. sie auf andere Weise schädigt. Nachdem Cracker unautorisiert Zugang erhalten haben, zerstören sie wichtige Daten, verweigern Dienste für legitime Benutzer oder verursachen grundsätzlich Probleme im Arbeitsablauf des angegriffenen Rechners. Cracker können sehr leicht identifiziert werden: ihre Absichten sind böswillig.

## *Cryptographic Hash*

- Provides Integrity and computational in-feasibility

## *CSIRT - Computer Security Incident Response Team*

- ???

## *CSMS - Cyber Security Management Systems*

- These management systems provide an organization with a well established method for protecting its assets from ***cyber attacks***.

## *Cyber Kill Chain*

- Die Cyber Kill Chain wurde von Lockheed Martin entwickelt, um Cyberangriffe zu beschreiben.
- Sie besteht aus mehreren Stufen, die ein immer tieferes Vordringen des Angreifers beschreiben.

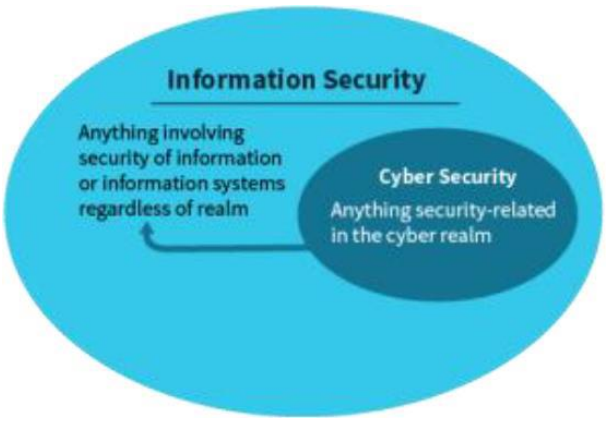
**PHASEN:**
Phase 1: Erkundung
Phase 2: Passende Angriffsmethode finden
Phase 3: Gezielter Angriff
Phase 4: Brückenkopf
Phase 5: Übernahme

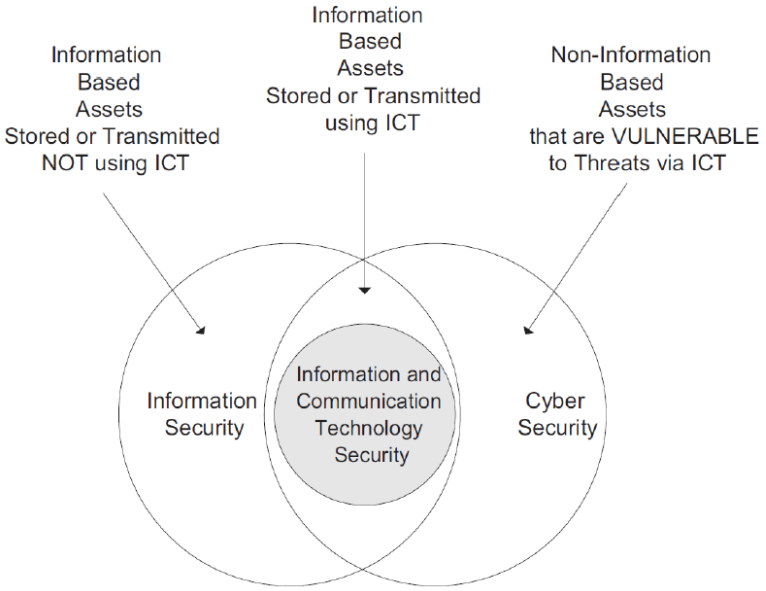
## *Cyber Security*

- Requires the coordination of efforts throughout an information system.
- One of the most problematic elements of cybersecurity is the constantly evolving nature of security risks.
- The traditional approach has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks.

***AREAS:***

- Application security
- Information security
- Network security
- Disaster recovery/business continuity planning
- Operational security
- End-user education






## *DCE - Distributed Computing Environment*

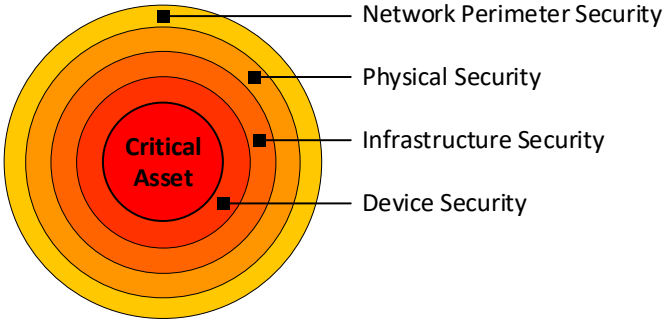
- Is a standard developed by the "Open Software Foundation (OSF)".
- A client/server framework that is available to many vendors to use within their products.
- Provides an RPC service.

## *DCOM - Distributed Component Object Model*

- Ist ein objektorientiertes Remote Procedure Call-System, das auf dem Distributed Computing Environment-Standard basiert.
- Es wurde von Microsoft definiert, um die Technologie Component Object Model über ein Rechnernetz kommunizieren zu lassen.

## *Defense-In-Depth*

- Unter „Defense in Depth“ versteht man einen koordinierten Einsatz mehrerer Sicherheitsmassnahmen, um die Datenbestände in einem Unternehmen zu schützen.
- Die Strategie basiert auf dem ***militärischen Prinzip***, dass es für einen Feind schwieriger ist, ein komplexes und vielschichtiges Abwehrsystem zu überwinden als eine einzige Barriere.



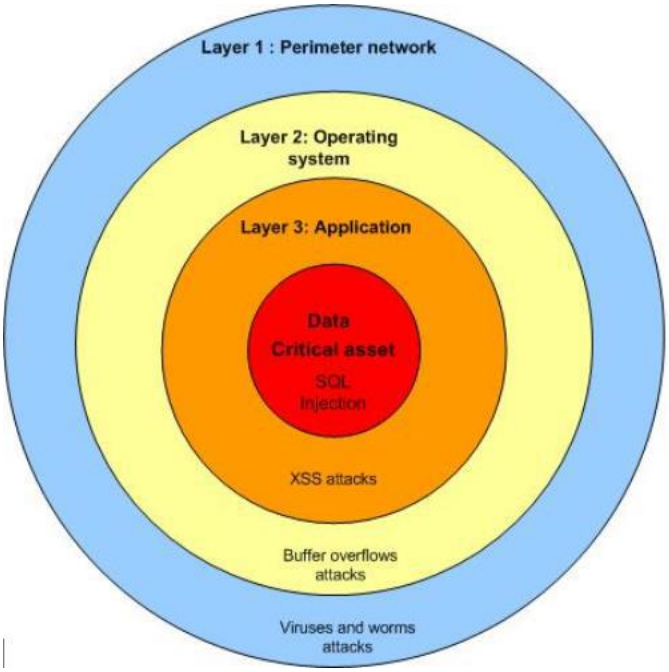
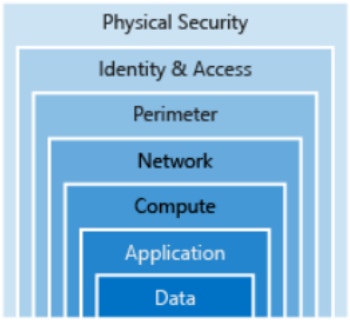




**Abbildung 3: Defense-in-depth architecture**



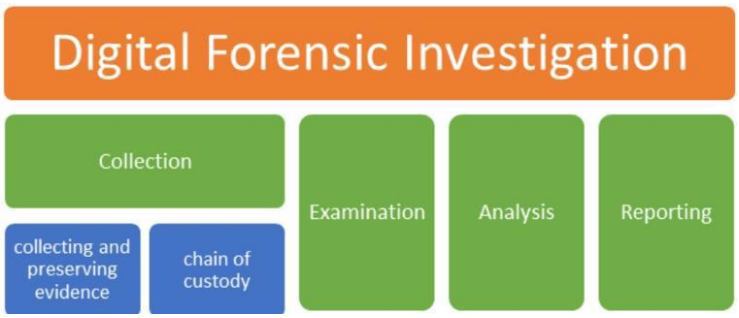
| # | Ring | Example | Principle |
|---|---|---|---|
| 1 | Data | Data encryption at rest in Azure blob storage | Integrity |
| 2 | Application | SSL/TLS encrypted sessions | Integrity |
| 3 | Compute | Regularly apply OS and layered software patches | Availability |
| 4 | Network | Network security rules | Confidentiality |
| 5 | Perimeter | DDoS protection | Availability |
| 6 | Identity & Access | Azure Active Directory user authentication | Integrity |
| 7 | Physical Security | Azure data center biometric access controls | Confidentiality |

## *Digital Forensic Investigation*

- Digital forensic investigation is a skill that requires extensive training and specialized software.
- The cost to support an internal digital forensics team leads some organizations to obtain support from third-party specialists when an investigation is necessary to support root-cause analysis or legal action.
- Contracts for forensic services can provide significant cost savings if this type of service is rarely required.
- This model also provides the advantage of access to impartial expert witnesses if evidence from a forensic investigation is used in legal proceedings.

***NIST process for Forensic Investigation phases***

- ❑ collection
- ❑ examination
- ❑ analysis
- ❑ reporting




***Corroborative Evidence***
Is supporting evidence used to help prove an idea or point. It cannot stand its own.

***Opinion Evidence***
Would be the opinion of a witness, but the opinion rule dictates that the witness must testify to only facts of the issue and not her opinion of the facts.

***Circumstantial Evidence***
Can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact. This type of fact is used so the judge or jury will logically assume the existence of a ***primary fact***.

***Secondary Evidence***
Is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence. Oral evidence, such as a ***witnesse's testimony***, ***copies of original documents*** and ***Computer-generated*** evidence are placed in the secondary evidence category.

## *DRM - Digital Rights Management*

Products:

- https://www.fileopen.com
  PDFs sichern

## *Due Diligence*

- Due diligence is performing reasonable examination and research before committing to a course of action.
- Basically, "look before you leap". In law, you would perform due diligence by researching the terms of a contract before signing it.
- The opposite of due diligence might be "haphazard" or "not doing your homework".

## *Due Care*

- Is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation.
- This is especially important if the due care situation exists because of a contract, regulation, or law.
- The opposite of due care is "negligence".

## *EMI - Electromagnetic Interference*

***Common-mode noise***
Noise from the radiation generated by the difference between the hot and ground wires.

***Traverse-mode noise***
Noise from the radiation generated by the difference between the hot and neutral wires.

## *Endpoint Security*

***Bromium***
bromium.com

- Nutzt den Micro Virtualisierungs Ansatz µVM.

***Tanium***
Tanium.com

- Tanium is a privately held endpoint security and systems management company based in Emeryville, California. Founded in 2007 by David Hindawi and Orion Hindawi, the company's platform employs a novel technology that enables visibility and control across enterprise-wide network endpoints within 15 seconds.

***Exclusionary Rule***

- In the United States, the exclusionary rule is a legal rule, based on constitutional law, that prevents evidence collected or analyzed in violation of the defendant's constitutional rights from being used in a court of law.
- This may be considered an example of a prophylactic rule formulated by the judiciary in order to protect a constitutional right.
- The exclusionary rule may also, in some circumstances at least, be considered to follow directly from the constitutional language, such as the Fifth Amendment's command that no person "shall be compelled in any criminal case to be a witness against himself" and that no person "shall be deprived of life, liberty or property without due process of law".

## *Enumeration*

- Is a process of retrieving information like ***usernames***, ***default credentials***, ***host names***, ***network shares***, and ***services*** from the target system.

## *Exploit*

- A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in ordert o cause unintended or unanticipated behavior to occur on computer software.

## *Hacker*

- Ein **Hacker** ist eine Person, die sich für die geheimnisvollen und verborgenen Arbeitsweisen eines jeglichen Betriebssystems interessiert.
- Hacker sind meistens Programmierer. Als solche erhalten Hacker ein fortgeschrittenes Wissen über Betriebssysteme und Programmiersprachen. Sie können Sicherheitslöcher in Systemen und die Gründe dafür entdecken.
- Hacker sind ständig auf der Suche nach weiterem Wissen, teilen freimütig ihre Entdeckungen mit und würden niemals absichtlich Daten zerstören.

### *Script-Kiddies*

- In programming and hacking culture, a script kiddie, skiddie, or ***skid*** is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites.
- It is generally assumed that most script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. However, the term does not relate to the actual age of the participant.

### *White Hat*

- White Hat ist der Ausdruck für einen Hacker oder Cracker, der eine Security-Schwachstelle in einem Computersystem oder einem Netzwerk identifiziert.
- Er nutzt dieses Wissen aber nicht, um Schaden zu verursachen.
- Stattdessen teilt er seine Erkenntnisse auf irgendeine Art und Weise mit dem Betroffenen.
- Nun hat der Besitzer des Systems die Chance, das Problem zu beheben, bevor jemand die Lücke ausnutzen kann

### *Grey Hat*

- Grey-Hats (Grau-Hüte) verstossen möglicherweise gegen Gesetze oder restriktive Auslegungen der Hackerethik, allerdings zum Erreichen eines höheren Ziels.
- Beispielsweise durch die Veröffentlichung von Sicherheitslücken, um ein Leugnen unmöglich zu machen und die Verantwortlichen dazu zu zwingen, diese zu beheben.
- Grey-Hats zeichnen sich dadurch aus, dass sie nicht eindeutig als gut oder böse einzustufen sind.

### *Black Hat*

- Ein Black Hat Hacker, nutzt die Schwachstelle für eigenen Zwecke.

### *Packet Monkey*

- Although the term packet monkey can be used in a more general sense, it is often used to talk about malicious hackers sending large numbers of packets in order to disrupt system traffic.
- These relatively ***inexperienced hackers*** are contrasted to other professional hackers who use their own code, and infiltrate systems for more sophisticated purposes than denial of service attacks, for instance, where they do not leave a trace of their intrusion, or steal valuable data.
- In addition, someone may use the term “packet monkey” to talk about analysts who are observing packet traffic and packet contents

## *Honepot*

- Detective/technical control.

## *Ethical Hacker*

- ***Ethical hacking*** is often used as another name for ***penetration testing***.
- An ethical hacker is someone that understands network security and methds to breach security but does not use that knowledge fpr personal gain.

## *Galois Field*

- A Galois field is a finite field.
- In der Algebra, einem Teilgebiet der Mathematik, ist ein endlicher Körper oder Galoiskörper (nach Évariste Galois) ein Körper mit einer endlichen Anzahl von Elementen, d. h. eine endliche Menge, auf der zwei als Addition und Multiplikation verstandene Grundoperationen definiert sind, sodass die Menge zusammen mit diesen Operationen alle Anforderungen eines Körpers erfüllt.
- Endliche Körper spielen eine wichtige Rolle in der ***Kryptographie*** und der Codierungstheorie (Vorwärtsfehlerkorrektur, zum Beispiel beim ***Reed-Solomon-Code***).
- Daneben sind sie grundlegend für das Studium der Primideale im Ring der ganzen Zahlen einer endlichen Körpererweiterung von **Q** im Rahmen der algebraischen Zahlentheorie.
- Man vergleiche hierzu auch Verzweigung im Kontext von Erweiterungen von ***Dedekindringen***.

## *Homebanking Computer Interface( HBCI )*

- Ist ein offener Standard für den Bereich Electronic Banking und Kundenselbstbedienung.
- Er wurde von verschiedenen Bankengruppen in Deutschland entwickelt und vom Zentralen Kreditausschuss (ZKA; heute Die Deutsche Kreditwirtschaft) beschlossen.
- HBCI ist eine ***standardisierte Schnittstelle*** für das Homebanking.
- Dabei werden ***Übertragungsprotokolle***, ***Nachrichtenformate*** und ***Sicherheitsverfahren*** definiert.

## *Fail Safe versus Fail Secure*

- All electrified locking devices fall into one of two categories.
- They either need power to lock, or they need power to unlock. The original terms for these conditions were ***fail safe*** and ***fail secure***.

***Fail Safe***

- Fail safe deals directly with ***protecting people***.
- Fail safe means, if power fails, the door is ***unlocked***.
- In the event of a specific type of failure, inherently responds in a way that will cause ***no*** or ***minimal harm*** to other equipment, the environment or to people.

***Fail Secure***

- Fail secure means that if the power fails, the door ***remains secure/locked***.

## *FAIR - Factor Analysis of Information Risk*

- See: Risk Management
- FAIR is a tool that complements existing risk management frameworks by providing a model to understand, analyze, and quantify information risk in financial terms.

## *False Positive*

False Positive

- Type I error
- Ein «False Positive» ist ein Fehler bei einer Überprüfung, bei der ein Zustand fälschlicherweise als solcher erkannt wurde.

False Negative

- Type II error
- Ein «False Negativ» ist ein Fehler bei einer Überprüfung, bei der ein Zustand nicht erkannt wurde, obwohl vorhanden.

True Positive

True Negative

| Kondition | Test Resultat | Effektiv | Definition | Tip |
|---|---|---|---|---|
|  | Ist Spam | Nicht korrekt | **False Positive** | **NOK** |
|  | Ist kein Spam | Nicht korrekt | **False Negative** | **NOK** |
|  | Ist Spam | Korrekt identifiziert | **True Positive** | **OK** |
|  | Ist kein Spam | Korrekt identifiziert | **True Negative** | **OK** |

## *Finger*

- Finger (fingerd) dient dazu, entfernten hosts Benutzerinformationen zur Verfügung zu stellen.

| *Client* | *URL* |
|---|---|
| InkFinger | ftp://ftp.demon.co.uk/pub/ibmc/win95/apps/finger/inkf100.zip |
| QuikFinger | http://fuzz.stanford.edu/QuikFinger/quikfinger.exe |
| Total Finger | http://ahab.nantucket.net/files/tfinger.exe |
| Nfinger | ftp://papa.indstate.edu/winsock-1/Windows95/Finger/NFinger.zip |

target@host.com

finger @mein_zielhost.com
grep Ihr_Benutzername /etc/passwd

oder
Telnet <Host> 25
expn benutzername
vrfy

## *FIREWALL*

- Eine Firewall ist jedes Gerät, das dazu entwickelt wurde, Aussenseiter davon abzuhalten, Zugang zu Ihrem Netzwerk Zu erhalten. Eine Firewall besteht aus Software und Hardware.

z.B. Rechner, Router, Firewall proprietär.

Firewalls können eingehende Datenpakete von verschiedenen Protokollen analysieren. Basierend auf dieser Analyse (Regeln) kann eine Firewall verschieden Aktionen durchführen.

- Zugangsprüfung
- Überprüfung des Inhaltes (Java-, Java-Script, VBScript- und ActiveX-Scripts sowie Cookies zu blockieren)
- Erkennen von Angriffssignaturen
- No. 1 reason for hacked firewalls is incorrect configured firewalls.

*Regeln*
Ansatz 1: **Was nicht ausdrücklich erlaubt ist, wird abgelehnt.**
Ansatz 2: Was nicht ausdrüklich verboten ist, wird angenommen.

*Variablen:*
- Ursprungsadresse
- Protokoll
- Port-Nummer
- Inhalt

**Firewall-Arten:**

- Application-Level Firewall
- Netzwerkschicht-Firewall
- Circuit-Level Firewall
- Packet Filtering Firewalls
- Stateful Inspection Firewall
- Multilayer Inspection Firewall

**Proxy-Based Firewall**

- A proxy firewall is a network security system that protects network resources by filtering messages at the application layer.
- A proxy firewall may also be called an application firewall or gateway firewall

**Dynamic-Packet-Filtering Firewall**

- When an outgoing request is made on a port greater than 1023, this typw of firewall creates ans ACL to allow the incoming reply on that port to pass.

***Application-Level Firewall***

- See: Communication Cisco CCxx.docx

- Sind weniger geeignet für Unternehmen, Universitäten, Internet Service Provider oder andere Umgebungen, für die eine flüssigere Kommunikation (und mehrere Kontakte mit der Öffentlichkeit) notwendig sind.
- Sicherer als Paketfilter!
- (Proxies) combine some of the attributes of packet-filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended (as specified by the destination port), but also by certain other characteristics such as HTTP request string. While application-level gateways provide considerable data security, they can ***dramatically impact network performance***.

***Packet-Filtering Firewall***

- ***First-generation*** FWs.
- ***Layer 3*** Based
- Also called: ***Netzwerkschicht-Firewall***, ***Router-Firewall***
- The ***simplest*** kind of Firwall.
- Appropriate for ***medium-risk environments***.
- Operate at the router and compare each packet received to a set of established criteria (such as allowed IP addresses, packet type, port number, etc.) before being either dropped or forwarded.

  Pros:
  Easy to connect.
  Dual Interfaces possible

  Cons:
  Prone to "Spoofing Attacks"
  Limited logging functionality
  No support for advanced user authentication schemas
  Insufficient for medium-risk envrvironments

***Circuit-Level Firewall***

- See: Communication Cisco CCxx.docx

***Stateful Inspection Firewall***

- See: Communication Cisco CCxx.docx

***Multilayer Inspection Firewall***

- Combine packet filtering with circuit monitoring, while still enabling direct connections between the local and remote hosts, which are transparent to the network.

- They accomplish this by relying on algorithms to recognize which service is being requested, rather than by simply providing a proxy for each protected service.
- Multilayer firewalls work by retaining the status (state) assigned to a packet by each firewall component through which it passes on the way up the protocol stack.
- This gives the user maximum control over which packets are allowed to reach their final destination, but again affects network performance, although generally not so dramatically as proxies do.

***IPTables***

- See: Communication Cisco CCxx.docx

***TIS Firewall Toolkit (WAF)***

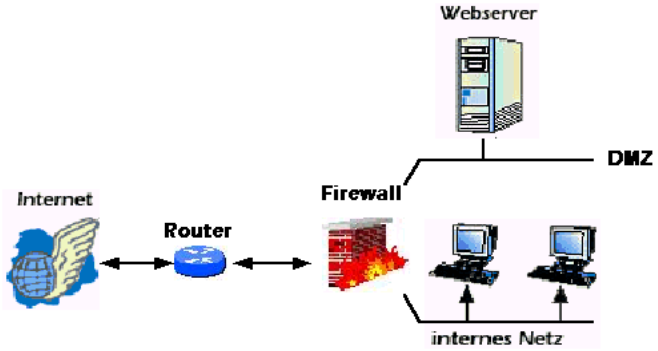
- See: Communication Cisco CCxx.docx

***DMZ - Demilitarisierte Zone***

- Auch: **Screened Subnet** genannt.
- Gruppe von Rechnern in einem Sicherheitssystem, die sowohl vom sicheren (trusted) als auch vom unsicheren (untrusted) Netz durch > Firewalls geschützt sind. > Security

**Variante 1**


**Variante 2**



***DROP versus REJECT***

- ***REJECT:*** TCP aborts the connection andthe application gets to know that the connection has failed after just one round-trip time. This allows the application attempting the connection to notify the user straight away.
  ***connection rejected***

- ***DROP:*** Will just cause TCP to retry the connection until the threshold for retranmission is exceeded. This should be at least 100 seconds.
  ***Connection timed out***

- An experiment on Linux gives 0.01 seconds for a REJECT to give an application error from a TCP connection, but 189 seconds for DROP.

***Result:***
- Preferred way should be REJECT.

## *GNSS - Global Navigation Satellite System*

- Ist ein System zur Positionsbestimmung und Navigation auf der Erde und in der Luft durch den Empfang der Signale von Navigationssatelliten und Pseudoliten.
- GNSS ist ein Sammelbegriff für die Verwendung bestehender und künftiger globaler Satellitensysteme wie: NAVSTAR GPS (USA), GLONASS (RU), Galileo (EU), Beidou CN)

## *Gopher*

- Ist ein Netzwerkprotokoll zum Abrufen von Dokumenten über das Internet.
- Ähnelt dem World Wide Web (WWW) in einem frühen Zustand.

## *Hamming Code*

- Der Hamming-Code ist ein von Richard Wesley Hamming entwickelter linearer fehlerkorrigierender Blockcode, der in der digitalen Signalverarbeitung und der Nachrichtentechnik zur gesicherten Datenübertragung oder Datenspeicherung verwendet wird.

## *IAM - Identity Access Management*

- IAM-Systeme erteilen den Benutzern schnell und sicher Zugänge und Berechtigungen zu unterschiedlichsten Applikationen und Systemen (Provisioning) und entziehen ihnen diese rechtzeitig wieder (De-Provisioning).
- Dies erfolgt über einen rollen- und regelbasierten Ansatz.
- In vielen Unternehmen können Nutzer über Self-Service-Portale selbst entscheiden, welche Zugänge oder Zugriffsberechtigungen sie benötigen.
- Durchgängig automatisierte Antrags- und Freigabeprozeduren binden die jeweiligen Verantwortlichen mit ein.

***Products:***
- CoreOne Suite (CH)
- Ergon Argon Airlock IAM (Integrated Access Management)

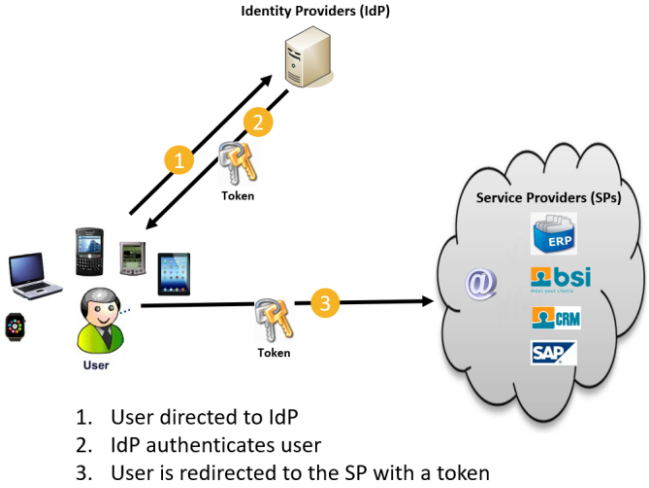
## *IAVA - Information Assurance Vulnerability Management*

- An information assurance vulnerability alert (IAVA) is an announcement of a computer application software or operating system vulnerability notification in the form of alerts, bulletins, and technical advisories identified by DoD-CERT, a division of the United States Cyber Command.
- These selected vulnerabilities are the mandated baseline, or minimum configuration of all hosts residing on the GIG.
- USCYBERCOM analyzes each vulnerability and determines if it is necessary or beneficial to the Department of Defense to release it as an IAVA. Implementation of IAVA policy will help ensure that DoD Components take appropriate mitigating actions against vulnerabilities to

avoid serious compromises to DoD computer system assets that would potentially degrade mission performance.

## *IDP - Identity Provider*

- See also: ***SSO/IAM***
- Target is to use the company's ***policies***, ***procedures*** and ***profiles*** to access cloud based applications with different devices such as PC's Laptops, Mobiles and so on.




***Products see:***

- Ergon Airlock Suite
- Identity Federation Hub
- Imprivata OneSign
- PKI
- SafeNet — Gemalto
- SecureAuth
- SES IDENTITY — United-Security-Providers
- WIB Solutions
- 10Duke Identity Provider

***SafeNet Trusted Access (Gemalto)***

- An ***access management service*** that centrally manages and secures access to web and cloud-based applications.
- Supports PKI SmartCards/USB-Tokens
- GDPR Approved

***Features***

- Validates the user's identity
- Assesses which access policy should be applied
- Applies the appropriate level of authentication with Smart Single Sign-On (SSO)

***Authentication Methods***

- OTP Push
- OTP App
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- Resource Access Control Facility (RACF, IBM, Mainframes)
- Kerberos
- PKI credentials
- Google Authenticator
- Passwordless authentication
- Biometric

- Voice
- 3rd party

***SecureAuth (SecureAuth)***

- Source:***secureauth.com***
- SecureAuth IdP is an identity management solution that ***uses two-factor authentication*** and ***SSO for mobile***, the cloud, web, and virtual private networks (VPN).

## *inetd*

- http://www.trumpton.demon.co.uk/index.html
- On Unix: /etc/inetd.conf
- Die Dienste von inted: FTP, Telnet, SMTP, TFTP, Finger, Systat, Netstat.

## *IPSec - Internet Protocol Security*

RFC 4301

- Defined by ***IETF***
- For setting up a ***secure channel*** to exchange information between two entities.
- Uses ***public key cryptography***.
- Primary use for ***VPNs***.
- ***IPSec*** is an industry-wide standard framework of protocols and algorithms that allow for secure data transmission over an ***IP-based network*** and functions at the ***layer 3*** of the OSI model.
- ***IPSec*** can't be used to encrypt ***non-IP traffic***.
- The two primary security protocols used by IPSec are ***Authentication Header (AH)*** and ***Encapsulating Security Payload (ESP)***.
- ***AH and ESP*** can be used in ***tunnel mode*** or ***transport mode***.
- Data will be sent ***encrypted***.
- Data Encryption Standard (***DES***).
- Triple DES (***3DES***).
- Advanced Encryption Standard (***AES***).

IPSec ist im Wesentlichen ein Mechanismus, um Sicherheit für die Daten zu gewährleisten, die zwischen zwei Computern in einem IP-Netzwerk ausgetauscht werden. Weil IPSec ein Standard ist, der Interoperabilität bietet, kann IPSec verwendet werden, um die Kommunikation zwischen Windows und Nicht-Windows-Computern zu schützen.

Datenauthentifizierung, Datenintegrität, Verschlüsselung.

Filteraktionen: Blocken, zulassen oder "Sicherheit aushandeln".

***Kerberos*** ist das Standardauthentifizierungsprotokoll in einer Active Directory-Umgebung.
***Zertifikate***: Empfohlen wenn keine Kerberos-Authentifizierung verfügbar ist.
***Vorinstallierte Schlüssel***: Nicht empfohlen!

***Security Association(SA).***

- Authentication Header(AH)
  Bietet Authentifizierung
- Encapsulating Security Payload(ESP)
  Bietet: Authentifizierung und Datenverschlüsselung.

Um SA's dynamisch zwischen IPSec-Partnern aufzubauen, wird das ***IKE-Protokoll*** (Internet Key Exchange) benutzt.

***IKE*** wird in zwei Phasen aufgebaut:

- Phase 1: main mode
- Phase 2: quick mode

**IPSec features:**

- ***Confidentiality***
  Encrypting data using the following methods:
  RSA, Diffie-Hellmann, AES, 3DES (symmetric)

- ***Integrity***
  Ensures that data is not modified in transit using checksum using:
  HMAC-SHA-1, HMAC-SHA-2, HMAC-md5

- ***Authentication***
  Allows to verify, the that the other parties involved is the party it claims to be.
  Signatures: RSA, Preshared Keys

- ***Antireplay***
  IPSec uses ***sequence numbers*** to check the packet is not a duplicate.

***ESP - Encapsulating Security Payload***
Transport: IP protocol number ***50.***

- ESP ***encrypts*** the original packet (Payload).
- ESP provides ***confidentiality, encryption***, ***authentication*** and ***integrity***.
- Default algorithm for ***IPv6 ESP*** extension header = ***Cipher Block Chaining (CBC)***

**ESP transport mode**

- Frequently used for ***client-to-site*** VPNs.
- ***Authenticates*** the ESP header.
- Uses the ***original IP header***, thus less overhead.
- Transport mode ***encrypts the data payload***.


**Figure 25: Transport Mode**

**ESP tunnel mode**

- Frequently used in ***site-to-site*** VPNs.
- Encapsulate the entire packet, thus ***hides internal addressing***.
- ***Highest level*** of protection


**Figure 26: Tunnel Mode**

***AH - Authentication Header***
Transport: IP protocol number ***51.***

- Does ***not offer any encryption***.

***ISAKMP - Internet Security Association and Key Management Protocol***
RFC 2408

- Provides background security support services for IPSec by negotiating, establishing, modifying, and deleting security associations (SAs).

***IPSec VPN Steps***

The IPSec VPN process of establishing a session consists of ***5 steps***.

**Step 1** Data classification "***Interesting Traffic***"

**Step 2** Build ***IKE Phase 1 tunnel***.
Security Association (***SA***) negotiation and building ***ISAKMP tunnel***.
See also ***ISAKMP/Oakley***.
Transform sets, hash methods, and other parameters are determined.
Policy negotiation can include different lifetimes and policy numbers.

**Step 3** Build ***IKE Phase 2 tunnel***. Building ***IPSec tunnel***.
IPSec policy will be determined and applied.

**Step 4** Data exchange of ***interesting traffic*** through the tunnel.
***Noninteresting traffic*** is transmitted outside of the tunnel.

**Step 5** Torn down IPSec tunnel.

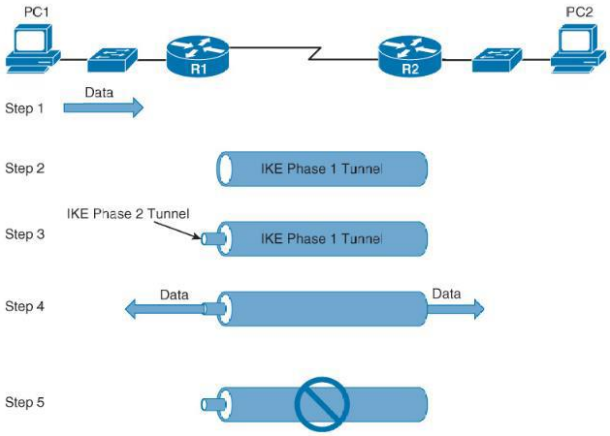



**Figure 27: IPSec VPN Steps**

***IPSec Phases***

| | | | |
|---|---|---|---|
| ***Phase 1:*** | Encryption | ( ) | 3DES (symmetric) |
| | | ( ) | AES-128 |
| | | ( ) | AES-256 |
| | Hash | ( ) | MD5 |
| | | ( ) | SHA-1 |
| | | ( ) | SHA-2 (Includes SHA-224, SHA-256 and SHA-512) |
| | Diffie-Hellman | ( ) | Group 2 (1024-bit) |
| | | ( ) | Group 5 (1536-bit) |
| | Lifetime IKE | ( ) | 86400 seconds (default) |
| ***Phase 2:*** | Encryption | ( ) | 3DES (symmetric) |
| | | ( ) | AES-128 |
| | | ( ) | AES-256 |
| | Hash | ( ) | MD5 |
| | | ( ) | SHA-1 |
| | PFS | ( ) | Y/N |

***Crypto Map Defines***

- SA lifetimes
- Key management method
- Remote VPN peers
- Cipher policy
- Interesting traffic

## *JAVA*

- JAVA hat eine höhere Sicherheit als Perl und ein viel Höhere als ActiveX.
- JAVA ist schwieriger zu erlernen als C oder Perl.

## *KDD - Knowledge Discovery in Databases*

- Also known as data mining

***Approaches:***

- Classification
- Probabilistic
- Statistical

## *Key Encapsulation*

- See ***RFC 4949***
- Is a ***key recovery technique*** for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key.
- Key encapsulation typically permits direct retrieval of a secret key used to provide data confidentiality.

## *Key Escrow*

- ***"fair"*** cryptosystem
- Is an arrangement in which the keys needed to decrypt encrypted data are ***held in escrow*** so that, under certain circumstances, an authorized third party may gain access to those keys.
- These third parties may include businesses, who may want access to employees' ***private communications***, or ***governments***, who may wish to be able to view the contents of encrypted communications.
- See also ***Clipper Chip***.

## *LM Hashes*

***Windows LAN Manager (LM)*** hashes are known to be weak.

- Converts passwords to uppercase
- Hashes are sent in ***clear text*** over the network
- Effective length is ***7 characters***
- Max. password length is ***14 characters***
- Simple algorithm, so 10'000'000 hashes can be generated per second
- Encryption algorythm: ***DES***

## *MACSec - 802.1ae*

- Is the IEEE MAC Security standard (also known as MACsec) which defines ***connectionless data confidentiality and integrity for media access independent protocols***.
- It is standardized by the ***IEEE 802.1*** working group.
- Verschlüsselung auf ***Layer 2*** und kann damit verkabelte LANs auf der Anbindung zwischen Endgerät und Switch sowie zwischen Switches und Routern absichern.
- Ein ***Session Spoofing*** und ***Replay-Angriffe*** sind mit MACsec nicht mehr möglich.

## *Man Trap*

- A man trap is nothing more than a locked space you can hold someone in while verifying their right to proceed into the secured area.
- It's usually a glass walled room that lockst he exterior door as soon as you enter.
- Then there is a sort of authentication mechanism, such as a smartcard with a PIN or a biometric system. Assuming the authentication is succesful, the second door leading tod the interior oft he building will unlock, and the person is allowed to proceed.
- If it's not successful, the door will remain locked until the guard can check things out.
- As an aside, in addition to authentication, some man traps add a sort of extra fun, such as checking your weight to see if you've mysteriously gained or lost 20 pounds since Friday.

## *MD - Message Digest*

- Mit Message Digest (MD, auf Deutsch in etwa: ***Nachrichten-Kurzfassung***) wird eine Gruppe kryptografischer Protokolle bezeichnet.
- Es handelt sich um ***Einweg-Hash-Funktionen***.
- Diese Funktionen treten mit dem Anspruch auf, dass sie - bei vertretbarem Aufwand - nicht umkehrbar seien und auch keine Kollision berechenbar sei.
- Das bedeutet, dass es nicht möglich sein soll, zu einem Chiffrat den Originaltext wiederherzustellen (***unumkehrbar***).
- Es soll auch nicht möglich sein, einen Text zu berechnen, der das gleiche Chiffrat wie der Originaltext erzeugt (***kollisionsfrei***).

## *MD5 - Message Digest Algorithm 5*

Link: md5-generator.de

- A widely used ***hash function*** producing a ***128-bit hash value***.
- MD5 is ***neither encryption nor encoding***.
- Provides ***data integrity***.
- It can be ***cracked by brute-force attack***.

## *MQV - Menezes-Qu-Vanstone*

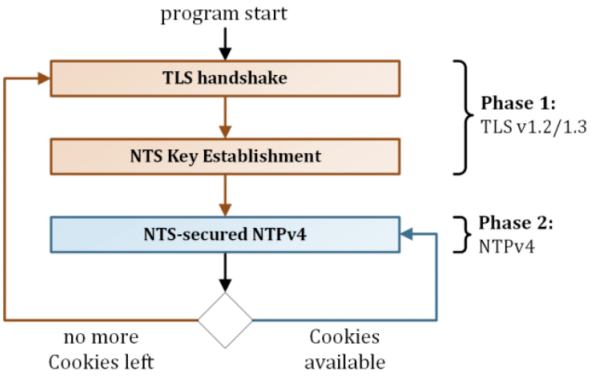
- Is an authenticated protocol for key agreement based on the ***Diffie-Hellman*** scheme.
- Like other authenticated Diffie-Hellman schemes, MQV provides ***protection against an active attacker***.
- ***Implicit signature***.
- Some weaknesses of MQV has fixed in ***HMQV***.

## *NPMD - Network Performance Monitoring and Diagnostics*

- See ARX 4300

## *NTS -*

- The NTS protocol is a security extension for time protocols and currently focuses on NTP in unicast mode.
- It provides strong cryptographic protection against packet manipulation, prevents tracking, scales, is robust against packet loss, and minimizes the loss of accuracy due to the securing process.
- To protect the time information, NTS uses the NTP Extension Fields (EF), in which parameter and status information are also transferred between the client and time server.




## *Oakley*

- Superseded by the ***IKE*** protocol.
- **Oakley - RFC2412,** is the key exchange protocol.
- One difference to the IKE worth mentioning is that Oakley provides something called ***Perfect Forward Secrecy (PFS)***.

- ***PFS*** is a security property of the Oakley protocol that ensures that a session key (in the PKI's deployment) will not be compromised if one of the private keys is compromised in the future.

**Features:**
- It uses ***Diffie-Hellman*** algorithm.
- It uses ***PFS***.

## *OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation*

- See: Risk Management
- OCTAVE Allegro is a lean risk assessment method and does not provide guidance in selecting security controls.
- The framework supports a simple qualitative risk assessment and structured threat analysis, which is primarily suitable for ***smaller organizations.***

## *OpenID Connect 1.0*

- Is a simple identity layer on top of the ***OAuth 2.0*** protocol.
- It allows Clients to verify the ***identity*** of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.
- OpenID Connect allows clients of all types, including ***Web-based***, ***mobile***, and ***JavaScript clients***, to request and receive information about authenticated sessions and end-users.
- The specification suite is extensible, allowing participants to use optional features such as ***encryption of identity data***, ***discovery of OpenID Providers***, and ***session management***, when it makes sense for them.

***Videos:*** https://youtu.be/Kb56GzQ2pSk

## *OPSEC - Operations security*

- OPSEC is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.
- In a more general sense, OPSEC is the process of protecting individual pieces of data that could be grouped together to give the bigger picture (called aggregation).
- OPSEC is the protection of critical information deemed mission essential from military commanders, senior leaders, management or other decision-making bodies.
- The process results in the development of countermeasures, which include technical and non-technical measures such as the use of email encryption software, taking precautions against eavesdropping, paying close attention to a picture you have taken (such as items in the background), or not talking openly on social media sites about information on the unit, activity or organization's Critical Information List.

## *OTP - One Time Pad*

- Is an ***encryption technique*** that ***cannot be cracked***.
- Also known as ***Vernam ciphers***.

## *Overt Channel*

- Is a communications path that is not hidden.
- Overt channels are legitimate communication channels

## *PAM - Privileged Account Management*

- ***SW:*** Avantec / BeyondTrust
  https://www.cyberark.com
- ***Service:*** www.smarttech247.com
- See also: ***TPAM - Total Privileged Access Management***

### *Passwort-Knacker*

- Ein Passwortknacker ist ein Programm, das Passwort-Sicherheitsmassnahmen umgeht, indem es Passwörter aufdeckt, die vorher verschlüsselt wurden.
- In der Regel können Passwörter, die mit starken Algorithmen verschlüsselt wurden, nicht entschlüsselt werden.

/usr/dict/words

**Zitat "Yaman Akdeniz"**
Kryptographie, definiert als ***"Die Wissenschaft und Lehre der Geheimschrift"***, umfasst die Art und Weise, in der Kommunikation und Daten durch Codes, Chiffren und andere Methoden verschlüsselt werden können, um eine Offenlegung ihrer Inhalte durch Abhören oder Abfangen zu verhindern, so dass nur bestimmte Leute die richtige Nachricht sehen können.

Codes:

| | |
|---|---|
| ROT-13 | A +13 = N |
| crypt(3) | Praktisch unknackbar(von IBM)! |

*Cracker:*

| | |
|---|---|
| 10phtCrack 2.0 | http://www.10pht.com/10phtcrack/ |
| ScanNT | http://www.ntsecurity.com/Products/ScanNT/index.html |
| NTCrack | http://www.somarsoft.com/ftp/NTCRACK.ZIP |
| PasswordNT | http://www.ntsecurity.com/Servvices/Recovery/index.html |
| samdump | |
| NTFSDOS | |
| PaceCrack95 | http://tms.netrom.com/~cassidy/utils/pace.zip |

| | |
|---|---|
| Hades | |
| Star Cracker | http:/massacre.wizardtech.net/Misc/scrk03.zip |
| Hellfire Cracker | lcl130.zip |
| XIT | xit20.zip |
| Claymore | claym10.zip |
| Guess | |
| Merlin | |
| ZipCrack | zipcrk10.zip |
| Fast Zip 2.0 | fzc101.zip |
| Glide | Knacken von PWL-Dateien.<br>http://www.iaehv.nl/users/rvdpeet/unrelate/glide.zip |
| PGPCrack | |
| CP.EXE | Für Compuserve (cis_pw.zip) |
| md5cracker | http://md5cracker.org |

## *PEN - Penetration*

- PEN-Test have always a scope

### *3 PEN-Test Phases*

- Pre-Attack
- Attack
- Post-Attack

## *PERL (Practical Extraction and Report Language)*

www.perl.com/latest.html.

## *Piggybacking*

***Remember***: Pigs would never wear a badge, they don't have any clothes to attach it to.

## *Rijndael*

- Advanced Ecryption Standard (***AES***)
- ***Block Cipher***
- ***Symmetric*** encryption algorithm
- Maximum key size is ***256 bits***.
- It uses a ***128-bit block size*** and various key lenghts (128.192, 256).
- The block size must be a multiple of ***32 bits***.
- Substitution linear transformation cipher that uses ***triple discreet*** invertible uniform transformations.

## *PKCS - Public Key Cryptography Standards*

### *PKCS #10 - Certification Request Standard*

- See RFC 2986.
- Format of messages sent to a certification authority to request certification of a public key.

- See certificate signing request.

***PKCS #11 - Cryptographic Token Interface***

- Also known as "***Cryptoki***".
- An API defining a generic interface to cryptographic tokens (see also hardware security module).
- Often used in single sign-on, public-key cryptography and disk encryption systems.
- RSA Security has turned over further development of the PKCS #11 standard to the OASIS PKCS 11 Technical Committee.

***PKCS #12 - Personal Information Exchange Syntax Standard***

- See ***RFC 7292***.
- Describes a ***transfer syntax*** for personal identity information.
- Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.
- ***PFX*** is a predecessor to PKCS #12.
- This container format can contain multiple embedded objects, such as multiple certificates.
- Usually protected/encrypted with a password.
- Usable as a format for the Java key store and to establish client authentication certificates in Mozilla Firefox.
- Usable by Apache Tomcat.

## *Protokollierungstools*

- Log-Dateien sind ein wichtiges Beweismittel, wenn Sie einen Angreifer anzeigen wollen!
- Cracker ändern Log-Dateien!

***Tools zur Änderung von Log-Dateien:***

- cooke (WNT)

Tools wie ***SATAN*** (Port Scanner) öffnen viele Socket-Verbindungen innerhalb kurzer Zeit. Dieses Verhalten ist sehr ungewöhnlich und kann leicht von Aktivitäten legitimer Benutzer unterschieden werden.
Tools wie ***Courtney*** verlassen sich mehr auf das Verhalten eingehender Hosts (und ihren Regelkreis) als auf die Art der Daten, die übertragen werden.

## *PSIRT - Product Security Incident Response Team*

- ???

## *Public Key Certificate*

- In cryptography, a public key certificate (or identity certificate) is an electronical document which incorporates a ***digital signature*** to ***bind together a public key with an identity***.
- Information such as the name of a person or an organization, their address, and so forth.
- The certificate can be used to verify that a public key belongs to an ***individual***.

## *Rootkits*

- Are one of the anti-forensic techniques that attackers use to hide data, malicious files, and processes.
- This software is intended to hide processes that could reveal an attack from the OS itself.
- Rootkits allow viruses and malware to “hide in plain sight” by concealing files in ways that antivirus software might overlook them, disguising files as legitimate system files, through unlinking processes, and even hiding from detection by the OS.
- Can hide processes from the process list, can hide files, registry entries and intercept keystrokes.
- It replaces legitimate programs
- Attaches itself to the master boot record in a hard drive and changing the machines boot sequence/options

Some of the commonly used rootkits: ***Avatar, Necurs, Azazel, ZeroAccess***

**Symptoms:**
- Core operating system files are hidden
- Backdoor access for attackers to return
- Permissions changing on key files
- asuspicious device driver
- Encryption applied to certain files without explanation
- Logfiles being wiped

## *RPO - Recovery Point Objective*

- The maximum duration of acceptable data loss.
- Ist he maximum period of time in which data might be lost if a disaster strike.
- It ist he most recent point in time to which data must be synchronized to avoid major impact on the organization.
- RPO is measured in units of time, not volume: "30 minutes of data", "four hours of data", and so on.
- RPO is about limiting and recovering from data loss, not data theft.

## *RTO - Recovery Time Objective*

- Ist he duration of time and a service level within which a business process must be restored after a disaster in ordert to avoid unacceptable consequences associated with a break in continuity.
- The maximum duration of acceptable downtime, where "downtime" needs to be defined by your specification.
- For example, if the acceptable downtime duration is eight hours in the event of a disaster, then your RTO is eight hours.

## *SCANNER*

- Scanner sind Programme, mit deren Hilfe ein Angreifer seinen Ziel Host nach vermeintlichen fehlerhaften Diensten abtasten kann.

*Informationen:*
- Welche Dienste laufen derzeit
- Unter welcher User-ID diese Dienste laufen
- Ob anonymes Login unterstützt wird.
- Ob gewisse Netzwerkdienste eine Authentifizierung erfordern.

*Network Toolbox:*
*SiteScan:* http://www.antionline.com/archives/windows/scan/sites-can.exe
*Chesapeake* http://www.ccci.com/tools/portscan/faq.htm
*YAPS:* http://www.tni.net/~ted/Yaps/Yaps.html
*PortScanner:* http://sunsite.cnlab-switch.ch/javafaq/course/week12/13.html
*PortFlash:* http://www.webroot.com/pflash.htm
*Ostronet:* http://www.antionline.com/archives/windows/scan/ostronet.zip
*NESSUS* (Linux)
http://www.nessus.org
ftp://ftp.gimp.org/pub/gtk
Can be used for ***session splicing***.

*SATAN*(Security Administrator's Tool for Analyzing Networks)
*Ballista*
*Ogre* Autor: Chameleon, Humble, NeonSurge, Rhino9
*WebTrends:* http://www.webtrends.com/wss
*SAFESuite:*
*CONNECT*: http://www.giga.or.at/pub/hakker/unix
*FSPScan*: http://www.giga.or.at/pub/hacker/unix
*XSCAN*: http://www.giga.or.at/pub/hakker/unix

***Adress- und Portscanner***

Um aus einem unbekannten Netzwerk eine möglichst vollzählige Liste aller Knoten zu gewinnen, muss jede potenzielle Netzwerkadresse mit einem Paket angesprochen werden. Kommt ein solches Datenpaket zurück, kann mit hoher Wahrscheinlichkeit auf die "Anwesenheit" eines Gerätes geschlossen werden. Diese Aufgabe wird von Adressscannern wahrgenommen. Im IP - Bereich senden diese z. B. einen ***ICMP Echo*** - Request (Ping - Paket) an alle möglichen Adressen eines Subnetzes und warten auf die Antwortpakete vom Typ ICMP Echo - Reply.

Da viele Firewalls einen ICMP - Verkehr abblocken, versuchen gute Adressscanner auf mehreren Wegen an die gewünschten Informationen zu kommen. Alle denkbaren Protokolltypen werden ausprobiert, um schliesssslich doch eine Antwort und damit die Information zu bekommen. Auch die Wahl einer falschen Absenderadresse (aus dem Adressbereich des Opfers) hilft manchmal weiter. Der Angreifer muss allerdings sicherstellen, dass die Antwortpakete bei ihm vorbeikommen.

Wenn dann eine Liste der aktiven Netzwerkknoten erstellt ist, ist die Suche nach wartenden Serverprozessen die nächste Aufgabe. Diese wird von den Portscannern erledigt, die meist als kombinierte Adress- / Portscanner auch die Suche nach den Knoten durchführen. Beim Portscan werden Wünsche nach TCP - Verbindungsaufnahmen oder UDP - Pakete an alle oder einen Teil der Ports gesendet und aus den Antworten Rückschlüsse auf aktive Dienste geschlossen.

Auch hier besteht bei Zugriffen vom Internet aus die Möglichkeit, dass Firewallsysteme die Pakete überwachen und es ggf. nicht weiterleiten. Bei UDP - Paketen sind die Möglichkeiten eine Firewall zu überlisten gering; aber beim TCP - Portscan gibt es eine Reihe von Varianten, die eine nähere Betrachtung wert ist. Die einfachst Variante des Scans empfindet eine gewöhnliche TCP - Verbindungsaufnahme nach. Dabei spielen die TCP - Flagge, die sog. Code - Bits SYN und ACK, die entscheidende Rolle. Diese Art der Kontaktaufnahme ist allerdings von Firewalls leicht festzustellen du zu blockieren.

Der ***TCP SYN - Scan***, auch *half open Scan* genannt, verzichtet auf den kompletten Dreiphasen - Handshake.

Es sendet ein SYN - Paket und wartet auf die Antwort. Kommt eine SYN / ACK - Antwort, ist ein Dienst gefunden. Das folgende Reset - Paket RST beendet diese Verbindung gleich wieder. Kommt allerdings keine Antwort oder ein RST - Paket, ist an dem angesprochenen Port kein Dienst aktiv oder eine Firewall blockt den Port ab.

Der ***TCP FIN - Scan*** nutzt eine Menge weitere TCP - Flagge, mit der das Ende einer bestehenden TCP - Verbindung angezeigt wird. Wartet am betreffenden Port kein Serverprozess, wird ein RST - Paket gesendet. Kommt hingegen keine Antwort, kann auf die Existenz eines Dienstes geschlossen werden, da in den TCP - Spezifikationen auf ein FIN - Paket bei nicht zuvor geöffneter Verbindung keine Antwort erfolgen darf. Firewalls lassen FIN - Pakete häufig passieren, so dass mit dieser Technik ein Blick hinter die Kulissen geworfen werden kann.

Die bisher angesprochenen Scan - Verfahren können bei Bedarf mit einer zusätzlichen Fragmentierung auf IP - Ebene durchgeführt werden. Fragmente sind von Paketfiltern nur schwer zu durchschauen weil die Pakete am Zielsystem zusammengebaut werden, und dann dort zu den oben beschriebenen Antworten führen.

Ein ***UDP - Scan*** ist bedeutend schwieriger durchzuführen als ein TCP - Scan, da ein aktiver Serverprozess nicht verpflichtet ist, ein Antwortpaket zu senden. Ebenso müssen inaktive Ports keine Fehlermeldung senden, doch in der Praxis kann aus dem Empfang eines ICMP Port unreachable - Paketes auf einen inaktiven Port geschlossen werden.

Die Ergebnisse eines Portscans können wichtige Aufschlüsse über das eingesetzte Betriessystem und die darauf laufenden Applikationen geben. So sind die Ports 135 - 139 wichtige Indizien auf Microsoftsysteme, wohingegen Portnummern ab 512 die unter Unix verbreiteten r - Dienst bedeuten. Auch Firewalls und sogar Intrusion - Detection - Systeme verraten sich durch ihre Administrations- und Kommunikationsports, wenn der Scan aus dem Intranet ausgeführt wird. Verantwortungsvolle

Administratoren ändern deshalb grundsätzlich die Nummern dieser Ports, sofern die Konfiguration der Systeme das erlaubt.

***Integrity checking***

- Can also be used to scan for viruses.
- Integrity checkers work by building a database of checksums or hashed values.
- Periodically, new scans are performed and the results are compared to the stored results.
- Although not always effective for data files, this technique is useful for executables because their contents rarely change.

## *SCAP - Security Content Automation Protocol*

- See also: National Vulnerability Database (***NVD***)
- Automated ***vulnerability management***
- ***Measure- and Policy-Compliance reporting***
- SCAP is a method for using specific standards to help organizations automate vulnerability management and policy compliance evaluation.
- SCAP comprises numerous open security standards, as well as applications which use these standards to check systems for vulnerabilities and misconfigurations.

## *SCRIPT*

- JavaScript (Netscape-Communicator)
- VBScript (Internet Explorer)

**Countermeasure:**
JavaScript wie auch VBScript am Router filtern, oder im Browser deaktivieren.

Metazeichen

| | |
|---|---|
| ; | Durch dieses Metazeichen getrennte Befehle werden der Reihe nach ausgeführt. |
| ¦ | Spezifiziert, dass die Ausgabe des ersten Befehls zur Eingabe des zweiten werden soll. |
| && | Spezifiziert, dass der zweite Befehl ausgeführt werden soll, wenn der erste Befehl erfolgreich ist. |
| ¦¦ | Spezifiziert, dass der zweite Befehl ausgeführt werden soll, wenn der erste Befehl scheitert. |
| () | Spezifiziert, dass alle angegebenen Befehle zu einer Gruppe zusammengefasst und in einer Subshell ausgeführt werden sollen. |

## *SD3+C*

- See Microsoft.
- Threat modeling.

## *Secure Socket Layer (SSL)*

**Versions:**

- SSL v2 insecure
- SSL v3 POODLE
- SSL v4
- TLS 1.0 BEAST
- TLS 1.1
- TLS 1.2
- TLS 1.3

**Encryption Algorithm:**

| | | |
|---|---|---|
| RC2 | 40 Bit | Symmetric |
| RC3 | | |
| RC4 | 128 Bit | Symmetric / Stream Cipher |
| RC5 | 0-2040 Bit | Symmetric Encryption Algorithm (32, 64 or 128-bit blocks) |
| RC6 | 128-2040 Bit | Symmetric Key Block Cipher (128-bit blocks) |
| DES | 56 Bit | Symmetric |
| 3DES | 112 Bit | Symmetric Cryptographic Standard |

AES Symmetric / Bulk Data Encryption

***Kryptografische Verfahren***

**Symmetrische Verfahren**

- Ein Schlüssel für Ver- und Entschlüsselung
- Fast and works great with bulk encryption
- For 7 people, 21 keys are necessary **7 * (7-1) / 2 = 21**

**Asymmetrische Verfahren**

- Öffentlicher Schlüssel für den Sender / privater Schlüssel für den Empfänger

Der Empfänger muss über einen Mechanismus verfügen, um zu gewährleisten, dass das Schlüsselpaar zum beabsichtigten Sender gehört. und nicht zu jemandem der sich als Sender ausgibt. Dies geschieht durch das Zertifikat einer vertrauenswürdigen Drittpartei. Dabei handelt es sich um eine Zertifizierungsstelle (Certificate Authority, CA).

Der öffentliche Schlüssel wird auf eine der folgenden Verfahren erworben:

- Der Besitzer des privaten Schlüssels sendet dem Empfänger den passenden öffentlichen Schlüssel
- Der Empfänger erhält den Schlüssel von einem Verzeichnisdienst wie Z.B. ADS oder DNS.

## *SELinux - Security-Enhanced Linux*

- SELinux ist eine Erweiterung des Linux-Kernels, die den ersten Versuch darstellt, das FLASK-Konzept des US-amerikanischen Geheimdienstes NSA umzusetzen.
- Es implementiert die Zugriffskontrollen auf Ressourcen im Sinne von ***Mandatory Access Control***.
- SELinux wird massgeblich von der ***NSA*** und von dem Linux-Distributor ***Red Hat*** entwickelt. Unternehmen wie Network Associates, Secure Computing Corporation, und Tresys sind bzw. waren ebenfalls an der Arbeit an SELinux beteiligt, besonders Tresys übernimmt vermehrt Aufgaben am Projekt.
- SELinux ist Open-Source-Software und setzt sich aus einem Kernel-Patch und aus zahlreichen Erweiterungen für Systemprogramme zusammen.
- Für das Festlegen der Regeln gibt es eine sogenannte Policy, die momentan von Tresys herausgegeben wird.
- Die meisten Distributionen bieten spezielle SELinux-Policy-Pakete für ihre Programme an, die die Policy um das jeweilige Programm erweitern.

*Source: Wikipedia*

## *SEM - Security Event Management*

- Provides real-time analysis of events occurring on systems throughout an organization.

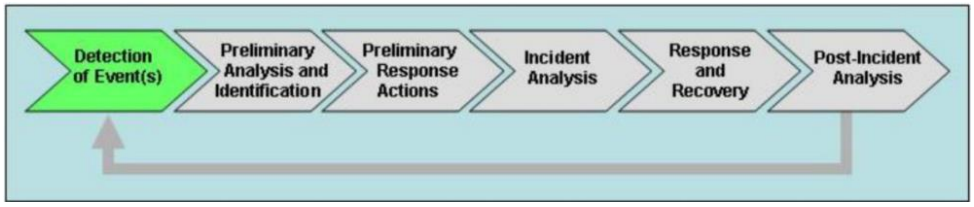



**Figure 28: DoD Cyber Incident Handling Process**

***Processes to implement:***

- ❑ Security logs must be consolidated and maintained.
- ❑ A strategy for storage and maintenance of log files must be defined and implemented.
- ❑ Events must be aggregated, normalized, and analyzed on a consistent basis to provide a baseline for normal activities within the enterprise.
- ❑ Alerts must be generated and routed to appropriate individuals when suspicious or anomalous activity has been identified.
- ❑ If the event represents an imminent security threat, the incident management process must be activated.

| | Incident | Event |
|---|---|---|
| Training and Exercise | | |
| Root-Level Intrusion | 1 | |
| User-Level Intrusion | 2 | |
| Unsuccessful Activity Attempt | | 3 |
| Denial of Service | 4 | |
| Non-Compliance Activity | 5 | |
| Reconnaissance | | 6 |
| Malicious Logic | 7 | |
| Investigating | | 8 |
| Explained Anomaly | | 9 |

***e.g. Incident and Cyber Event Categories***

## *SHA - Secure Hash Algorithm*

- Developed by the NSA
- ***Cryptographic hash function***.

***SHA-1***

- SHA-1 produces a ***160-bit (20-byte) hash value*** known as a ***message digest***.
- SHA-1 is ***no longer considered secure***.

***SHA-2***

- SHA-2 produces a ***224-, 256-, 384- and 512-bits outputs***

***SHA-3***

- SHA-3 produces a ***…. -bits outputs***
- Uses the Keccak algorithm, a sponge construction in which message blocks are XORed into a subset of the state, which is then transformed as a whole.
- In the version used in SHA-3, the state consists of a 5×5 array of 64-bit words, 1600 bits total.

## *SIM - Security Information Management*

- Provides real-time analysis of events occurring on systems throughout an organization.

## *SIEM - Security Incident and Event Management*

- SIEM combines ***SIM*** (security information management) and ***SEM*** (security event management) functions into one security management system.
- Provides ***real-time analysis of events*** occurring on systems throughout an organization.
- ***Log Aggregation*** System
- Automated cross correlation and analysis of all event logs.
- Detect suspicious behavior
- Detect probems before thy become breaches
- Monitor and enforce corporate policies
- Identify systems with ***missing patches***.
- Identify systems with ***unauthorized software installed.***.
- Regulatory compliances require you to have a SIEM. PCI, HIPAA and FFIEC.

***Define Usecases:***

- ❑ Define the requirements for the use case and identify the intended outcome
- ❑ Define the scope of the requirement
- ❑ Validate event sources that support the expected use case function
- ❑ Define the logic of the alert and the associated attack vector
- ❑ Conduct implementation and testing to confirm the SIEM produces the intended result

- ❑ Define use case response procedures
- ❑ Conduct maintenance to support continuous improvement and tuning.

***RULES***

- ❑ Define ***filters*** for new data sources
- ❑ Get rid of ***unnecessary logs***
- ❑ Have ***naming conventions*** for your fields (see Elasticsearch)


***ArcSight***

***Elasticsearch***

Video: https://www.youtube.com/watch?v=C3tlMqaNSaI

- More ***Search Engine*** than a SIEM
- Elasticsearch handles the JSON requests.
- ***Kibana*** is the Web GUI
- ***Logstash & Beats*** are feeding the data into Elasticsearch
- ***X-Pack*** AddOn from third party (Cost) to Alert, Monitor and reporting

***FortiSIEM***

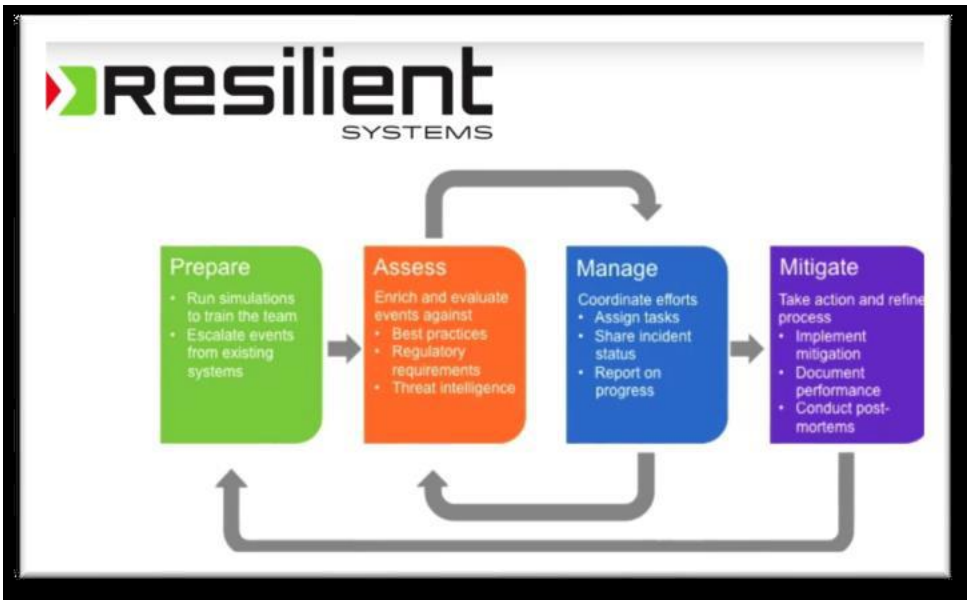
- See: **SIEM**
- Source: https://www.fortinet.com
- It is a Security Information and Event Management (SIEM) used for the detection and remediation of security events.
- It offers security, performance, and compliance management.
- Based on unified data collection and analytics from diverse information sources such as: ***logs***, ***performance metrics***, ***SNMP Traps***, ***security alerts*** and ***configuration changes***

**Video:**

- https://www.youtube.com/watch?v=_oLZJZWlRE8&feature=youtu.be

***IBM QRADAR***

- Leader in Gartner SIEM Magic Quadrant for 2008 - 2012
- Integration into "Resilient" www.resilientsystems.com




***Juniper (See: InfoGuard)***

***Logrythm***

***Splunk***

splunk.com

Splunk Enterprise
Splunk Enterprise Security
Splunk Cloud
Splunk IT Service Intelligence

***Solarwinds***

- Solarwinds Security Event Manager (SEM)

***Vectra***

## *SmartCards*

- Are credit-card sized IDs, badges or security passes with an embedded magnetic strip, bar code or integrated circuit chip.
- Some smartcards can even ***process information*** or ***store reasonable amounts of data*** in a memory chip.

- Haben die Grösse einer Kreditkarte und können zum speichern der öffentlichen und privaten Schlüssel sowie der Zertifikate von Benutzern verwendet werden.

Systemvoraussetzungen

- Lesegerät für SmartCards

## *SMTPS - Simple Mail Transfer Protocol Secure*

- Port: ***465***
- It is intended to provide authentication of the communication partners, as well as data integrity and confidentiality.
- SMTPS is not a proprietary protocol and not an extension of SMTP.
- Is a method for securing the SMTP using ***transport layer security (TLS)***.
- Conceptually, it is similar to how HTTPS wraps HTTP inside TLS.
- This means that the client and server speak normal SMTP at the application layer, but the connection is secured by SSL or TLS.

- This happens when the TCP connection is established, before any mail data has been exchanged.
- Since whether or not to use SSL or TLS is not explicitly negotiated by the peers, services that speak SMTPS are usually reachable on a dedicated port of their own.

## *SOAR - Security Orchestration, Automation and Response*

- SOAR-Systeme sammeln Bedrohungsdaten, erkennen Angriffe und ergreifen automatisch Gegenmassnahmen.

## *Split Knowledge*

- See PCI DSS
- "***Split knowledge***" is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key.

## *SSD - Solid-State Drives*

- It is good security practice to ***encrypt SSDs*** prior to storing any data.

## *SSH - Secure Shell*

- ***End-to-end encryption*** technique.
- Network protocol which allows to exchange data between two networks using a secure channel.

Versions:

- SSH1 Insecure
- SSH2

**Encryption algorithms:**

- ***AES*** also called Rijndael ***Symmetric***
- Blowfish 64 Bit Block Cipher
- DES (56 bits) ***Symmetric***
- IDEA (128 bits)
- Triple DES
- Twofish ***Symmetric***
    - Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish.
    - Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.
    - Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments.
    - Like Blowfish, Twofish is freely available to anyone who wants to use it.
    - As a result, you'll find it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software ***TrueCrypt***.
- Skipjack ***Symmetric*** Key Block Cipher

## *Stride*

- Is a ***threat classification model*** developed by Microsoft for thinking about computer security threats.
- It provides a mnemonic for security threats in six categories.

**The threat categories are:**

1. Spoofing of user identity
2. Tampering
3. Repudiation
4. Information disclosure (privacy breach or data leak)
5. Denial of service (DoS)
6. Elevation of privilege

## *SUDO*

- Ist ein Befehl unter Unix und unixartigen Betriebssystemen wie Linux oder macOS, der dazu benutzt wird, Prozesse mit den Rechten eines anderen Benutzers (z. B. des Superusers root) zu starten, ohne dessen Passwort kennen zu müssen.
- Im Gegensatz zu dem nicht zu sudo gehörenden su ist einstellbar, welche Befehle ausgeführt werden dürfen. Der dauerhafte Wechsel der Identität ist ebenfalls möglich durch sudo -s und sudo -i.

## *Tailgating*

- Tailgating involves following someone through an open door or gate just like piggybacking does.
- However, in tailgating, a ***fake identification badge*** of some sort is used.

## *TARA - Threat Agent Risk Assessment*

- Part of Risk Management.
- The TARA methodology identifies which threat agents pose the greatest risk, what they want to accomplish, and the likely methods they will employ.

## *TCB - Trusted Computing Base*

- ***Trusted Distribution*** is to ensure that the trusted computing base is not tampered with during shipment or installation.

## *TELNET*

Der Zweck des Telnet-Protokolls ist die Bereitstellung einer recht allgemeinen, bidirektionalen Kommunikationsmöglichkeit. Das Besondere an Telnet ist, dass es eine ASCII-Terminalverbindung zwischen zwei Rechnern simuliert, die weit voneinander entfernt sind.

Telnet wie auch ***rlogin*** funktioniert so, als würden Sie persönlich vor der Konsole sitzen.
Vergleich: **PcAnywhere, CloseUp**

Telnet kann auf alle ports versucht werden.

```
telnet [dst] 21 (FTP)
```

| | |
|---|---|
| 21 | FTP |
| 23 | TELNET |
| 25 | MAIL |
| 70 | GOPHER |
| 80 | HTTP |
| 6000 | High Port |

Telnet kann auch dazu benutzt werden, um festzustellen ob ein bestimmter Port offen ist.

Telnet <Zielrechner> 135 Kann das System zu aufhängen/abstürzen bringen.

SSH alternative zu Telnet.

Telnet ist eine sogenannte rudimentäre Verbindung(serielle).

Als Codesatz wird 7-Bit US-ASCII in einem 8-Bit-Feld verwendet.

***ACHTUNG!***
Bei mehreren Unix-Rechnern wurden die Telnet-Programme von unberechtigten Personen durch Telnet-Programme ersetzt, die externe Login-Sitzungen protokollieren (einschliesslich der Benutzernamen und Passwörter entfernter Systeme).

Telnet Clients mit Script funktionalität: http://www2.tinet-1.or.jp/cybird-f/windows/comm/ttermv13.zip

### *Threat Detection*

- Bedrohungserkennung
- Produkte: WatchGuard, …

### *Transaction Monitoring*

- See also: AML, KYC
- Target is to detect unusual customer transactions.

### *Trojan Horse*

RFC 1244
Bericht: http://www.drsolmon.com/vircen/vanalyse/va002.html
http://www.ciac.org/ciac/bulletins/a-10.shtml
http://www.emergency.com/aolgold.htm
http://www.pcworld.com/news/daily/data/0697/970627trojan.html
ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire
ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/preneel/mdxmac_crypto95.ps
ftp://ftp.rocksoft.com/clients/rocksoft/papers/digest10.ps
ftp://ftp.rocksoft.com/clients/rocksoft/papers/verty10.ps
ftp://ftp.cert.dfn.de/pub/docs/betsi/Betsi.ps

Ein Trojanisches Pferd ist:

- Unautorisierter Code innerhalb eines legitimen Programmes.
- Trojaner sind schwer zu entdecken
- In den meisten Fällen in Binärdateien

e.g. Passwörter stehlen oder Dateien kopieren.

Sabotage-Variante: PC-CYBORG
AOLGOLD
AOL4FREE.com

### *Trusted Shell*

- Means, that someone who is working in that shell cannot "bust out of it", and other processes cannot "bust into it".

### *Visa DUKPT - Derived Unique Key Per Transaction*

- In cryptography, "***DUKPT***" is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key.
- Therefore, if a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be determined easily.
- DUKPT is specified in ANSI X9.24 part 1.

### *Vigenere Cipher*

- Based on the Caesar cipher.

### *VLIW - Very Long Instruction Word Processor*

- Very long instruction word (VLIW) refers to instruction set architectures designed to exploit instruction level parallelism (ILP).
- Whereas conventional central processing units (CPU, processor) mostly allow programs to specify instructions to execute in sequence only, a VLIW processor allows programs to explicitly specify instructions to execute in parallel.
- This design is intended to allow higher performance without the complexity inherent in some other designs.

### *VOMIT - Voice Over Misconfigured Internet Telephones*

- See: VoIP

- The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.
- The phone conversation can either be played directly from the network or from a tcpdump output file.
- Vomit is also capable of inserting wavefiles into ongoing telephone conversations.
- Vomit can be used as a network debugging tool, a speaker phone, etc ...

## *Vulnerability*

- Ein Sicherheitsloch (Vulnerability) is jeder Fehler in Hardware, Software oder Richtlinien, der es einem Angreifer ermöglicht, ***unauthorized accesss*** zu Ihrem System zu bekommen.

***Neuralgische Punkte:***

- Router
- Client- und Server-Software
- Betriebssysteme
- Firewalls

***Aufdecken:***

- Hacker
- Cracker
- Sicherheitsteams des Herstellers

- Ein Netzwerk mit Internet-Anbindung zu verwalten, unterscheidet sich von der Verwaltung eines geschlossenen LAN's.
- In einem geschlossenen Netzwerk können Sie sich Zeit lassen, abtrünnige Benutzer aufzuspüren.
- Die Anzahl der potentiellen Angreifer ist limitiert und diese Leute müssen ihre Aktivitäten meist auf die Geschäftszeiten beschränken.
- Wenn Sie dagegen ein Netzwerk mit Internet-Anbindung verwalten, können Sie jederzeit von jedermann von jedem beliebigen Ort angegriffen werden.

***SOA-Vulnerability***

- XML denial of service issues

## *Wrapper*

- The legitimate file the Trojan is attached to.

## *X.509*

- Bezieht sich auf den Internationale Telecommunication Union-Telecommunication-Standard (ITU-T) für Zertifikatssyntax.

**Registrieren von Zertifikaten**

1. Zertifikat anfordern
2. Zertifikat auf Client installieren

## *Zero Trust Model*

- Introduced by the analyst firm «***Forrester Research»***.
- Beim Zero-Trust-Modell handelt es sich um ein Sicherheitskonzept, das ***grundsätzlich allen Diensten, Anwendern und Geräten misstraut***.
- Es wird kein Unterschied zwischen Diensten, Anwendern und Geräten innerhalb oder ausserhalb des eigenen Netzwerks gemacht.
- Sämtlicher Verkehr muss geprüft werden und alle Anwender oder Dienste müssen sich authentifizieren.
- Ziel des Modells ist es, das Risiko für Firmennetze und -anwendungen zu minimieren und neben externen Bedrohungen auch interne Gefahrenpotentiale auszuschliessen.
- Herkömmliche Sicherheitskonzepte stuften lediglich externen Datenverkehr als gefährlich ein und vertrauten sämtlichen internen Anwendern und Services.

# Abbreviations

| | |
|---|---|
| ACS | Annualized Cost of Safeguard |
| ARO | Annualized rate of occurrence |
| ATO | Authorization To Operate |
| AUP | Acceptable Use Policy |
| AV | Asset Value |
| CBK | Common Body of Knowledge |
| CCC | Chaos Computer Club |
| CERT | Computer Emergency Response Team |
| CGI | Common Gateway Interface |
| CIB | Candidate Information Bulletin |
| CIAC | Computer Incident Advisory Capability |
| CPTED | Crime Prevention Through Environmental Design |
| CSOR | Computer Security Objects Register |
| CSP | Cloud Service Provider |
| DES | Data Encryption Standard |
| DFIR | Digital Forensics and Incident Response |
| EF | Exposure Factor |
| HVAC | Heating, Ventilation and Air Conditioning |
| ISMS | Information Security Management System |
| IRC | Internet Relay Chat (Via seriellem Terminal) |
| IRM | Information Risk Management |
| Lynx | Terminal basierter HTML-Browser |
| MIM | Major Incident Management Team |
| MSSP | Managed Security Services Provider |
| MTD | Maximum Tolerable Downtime |
| MTO | Maximum Tolerable Outage |
| NAT | Network Address Translation |
| NCA | Noncompete Agreement |
| NIC | Network Information Center |
| NVT | Network Virtual Terminal |
| OLTP | Online transaction Processing System |
| PED | Portable Electronic Device |
| Perl | Practical Extraction and Report Language |
| PHI | Protected Health Information |
| Quotas | Sind Limitierungen des Festplattenspeichers auf dem E-Mail Server. |
| RFI | Radio Frequency Interference |
| RMF | Risk Management Framework |
| SAML | Security Association Markup Language |
| SOC | Service Organization Control |
| TATO | Temporary Authorization To Operate |
| URL | Universal Resource Locator |
| UTM | Unified Threat Management |
| X-Terminals | Plattenlose Clients |

# Table of Figures

# Index