SW Nmap

Document name: SW Nmap.docx
Last update: 15.04.2020
Author: Albert Balogh

Content

NMAP

- For security auditors and system or network administrators.
- Offers excellent Application mapping capabilities.

Author: Gordon Fyodor fyodor@insecure.org

Testsite: **scanme.nmap.org** → Officially allowed to scan! (Nmap page 18)

Nmap 7.60: https://nmap.org
FOR MORE OPTIONS AND EXAMPLES: https://nmap.org/book/man.html

DOWNLOAD
http://nmap.org/book
https://nmap.org/book/man.html → FOR MORE OPTIONS AND EXAMPLES
http://seclists.org
http://sectools.org
http://www.osstmm.org

http://www.isc.org/products/BIND/bind-security.html

Recommanded subscriptions:
nmap-hackers (mailing list)
nmap-dev (mailing list)
nmap-writers

Features
- ❑ Remote OS detection
- ❑ Version/service detection
- ❑ IP ID idle scanning
- ❑ Penetration testing
- ❑ Network inventory
- ❑ Managing service upgrade schedules
- ❑ Monitoring host or service uptime

COMPLETE COMMANDS

Usage: `nmap [Scan Types] [Options] {target specification}`

TARGET SPECIFICATION:

- Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

HOST DISCOVERY:

```
-n                                  → Never do DNS resolution/Always resolve
                                      [default: sometimes]
-sL                                 → List Scan - simply list targets to scan
-sn                                 → Ping Scan - disable port scan
-Pn                                 → Treat all hosts as online -- skip host discovery
-PS                                 → TCP SYN Ping
-PA                                 → TCP ACK Ping, port list
-PU                                 → UDP ping
-PE                                 → ICMP echo, timestamp, and netmask request
                                      discovery probes
-PP                                 → ICMP timestamp request
-PM                                 → ICPM netmask request
-PO[protocol list]                  → IP Protocol Ping
-PY[portlist]                       →
-R                                  →
--dns-servers <serv1[,serv2],...>   → Specify custom DNS servers
--system-dns                        → Use OS's DNS resolver
--traceroute                        → Trace hop path to each host
```

SCAN TECHNIQUES:

```
-b <FTP relay host>             → FTP bounce scan
-sA                             → TCP ACK Scan
-sM                             → Maimon scan
-sN                             → TCP Null Scan
-sF                             → TCP FIN Scan
-hU                             → Stack fingerprinting
-sX                             → TCP Xmas Scan
-sT                             → Connect()
-sU                             → UDP Scan
-sW                             → TCP Window Scan
-sI <zombie host[:probeport]>   → Idle scan
-sY                             → SCTP INIT Scan
-sZ                             → COOKIE-ECHO Scan
-sO                             → IP protocol scan
--scanflags <flags>             → Customize TCP scan flags
```

PORT SPECIFICATION AND SCAN ORDER:

```
-F                              → Fast mode - Scan fewer ports than the default scan
-p <port ranges>                → Only scan specified ports
                                  Ex: -p22
                                      -p1-65535
                                      -p U:53,111,137,T:21-25,80,139,8080,S:9
-r                              → Scan ports consecutively - don't randomize
--exclude-ports <port ranges>   → Exclude the specified ports from scanning
--port-ratio <ratio>            → Scan ports more common than <ratio>
--top-ports <number>            → Scan <number> most common ports
```

SERVICE/VERSION DETECTION:

```
-sV                             → Probe open ports to determine service/version info
```

```
--version-all                  → Try every single probe (intensity 9)
--version-intensity <level>    → Set from 0 (light) to 9 (try all probes)
--version-light                → Limit to most likely probes (intensity 2)
--version-trace                → Show detailed version scan activity (for debugging)
```

SCRIPT SCAN:

```
-sC                                → equivalent to --script=default
--script=<Lua scripts>             → <Lua scripts> is a comma separated list of
                                     directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>  → provide arguments to scripts
--script-args-file=filename        → provide NSE script args in a file
--script-trace                     → Show all data sent and received
--script-updatedb                  → Update the script database.
--script-help=<Lua scripts>        → Show help about scripts.
                                     <Lua scripts> is a comma-separated list of
                                     script-files or script-categories.
```

OS DETECTION:

```
-O                             → Enable OS detection
--osscan-limit                 → Limit OS detection to promising targets
--osscan-guess                 → Guess OS more aggressively
```

TIMING AND PERFORMANCE:

Options which take <time> are in seconds, or append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

```
--host-timeout <time>          → Give up on target after this long
-T<0-5>                        → Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>    → Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>    → Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>   → Specifies probe
                                                                 round trip time.
--max-retries <tries>          → Caps number of port scan probe retransmissions.
--scan-delay/--max-scan-delay <time>    → Adjust delay between probes
--max-rate <number>            → Send packets no faster than <number> per second
--min-rate <number>            → Send packets no slower than <number> per second
```

TIMING AND PERFORMANCE OPTIONS:

```
--host-timeout                 → Max timeout to scan a target
--initial-rtt-timeout          → Initial probe timeout
--max-rtt-timeout              → Max probe timeout
--min-rtt-timeout              → Min probe timeout
--max-hostgroup                → Max hosts in parallel
--min-hostgroup                → Min hosts in parallel
--max-parallelism              → Max outstanding probes
--min-parallelism              → Min outstanding probes
--max-scan-delay               → Max scan delay
--sca-delay                    → Min delay between probes
```

FIREWALL/IDS EVASION AND SPOOFING:

```
-D                             → Use decoys to hide identity
-D <decoy1,decoy2[,ME],...>    → Cloak a scan with decoys
-e <iface>                     → Use specified interface
-f; --mtu <val>                → fragment packets (optionally w/given MTU)
-g/--source-port <portnum>     → Use given port number
-S <IP_Address>                → Spoof source address
--proxies <url1,[url2],...>    → Relay connections through HTTP/SOCKS4 proxies
--data <hex string>            → Append a custom payload to sent packets
--data-string <string>         → Append a custom ASCII string to sent packets
--data-length <num>            → Append random data to sent packets
--ip-options <options>         → Send packets with specified ip options
--ttl <val>                    → Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>  → Spoof your MAC address
--badsum                       → Send packets with a bogus TCP/UDP/SCTP checksum
```

OUTPUT:

-oA <basename> → Output in the three major formats at once
-oN/-oX/-oS/-oG <file> → Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.
-v → Incr. verbosity level (use -vv or more for greater effect)
-d → Incr. debugging level (use -dd or more for greater effect)
--reason → Display the reason a port is in a particular state
--open → Only show open (or possibly open) ports
--packet-trace → Show all packets sent and received
--iflist → Print host interfaces and routes (for debugging)
--append-output → Append to rather than clobber specified output files
--resume <filename> → Resume an aborted scan
--stylesheet <path/URL> → XSL stylesheet to transform XML output to HTML
--webxml → Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet → Prevent associating of XSL stylesheet w/XML output

MISC:

--datadir <dirname> Specify custom Nmap data file location
--send-eth/--send-ip Send using raw ethernet frames or IP packets
--privileged Assume that the user is fully privileged
--unprivileged Assume the user lacks raw socket privileges

Scan Options

-6 → Enable IPv6 scanning
Fastest way to scan ports (Stealth)
-A → Enable all advanced/aggressive options
OS detection, version detection, script scanning, and traceroute
-b → FTP bounce attack
-h → Print this help summary page.
-n → Disable reverse DNS resolution
-O → **Operating system detection** (Fingerprinting)
-oX → Output the result in XML format to a file
-sA → **TCP ACK scan**
Map out firewall rulesets
Returns no response on a closed port
-sF → **FIN scan** (Sets just the TCP FIN bit)
-si → **Stealth scan**
-sl → **Idle Scan** (Zombie)
-sn → **Ping Scan**
-sN → **NULL scan** (Does not set any bits (TCP flag header is 0)
if the port is **open = No response**
if the port is **closed = RST**
-sP → **IPScan**, active IP Addresses active on a network

-sS → **Stealth scan**, TCP port scan, SYN scan,
-sT → **TCP Connect** / Most reliable and most visible
-sV → Version detection
-sU → UDP
-sO → IP Protocol, shows open ports
-sX → **Xmas scan** (Sets the FIN, PSH, and URG flags)
if the port is **open = no response**
if the port is **closed = RST**
-p- → Scan all ports from 1-65535
-p 22 → Scan a single port (22)
-V → Print version number
--spoof-mac → MAC address spoofing
--packet-trace

Ping Options

-PV → SCTP INIT ping probes

Target Options

-iL → Target list file
-iR → Scan random hosts
-e → Set network interface

```
-F                              → Fast scan
-p                              → Ports to be scanned
-PR                             → ARP Scan
-S                              → Set source IP address
--source-port                   → Set source port
--exclude                       → Exclude hosts/networks
--exclude <host1[,host2],...>   → Exclude hosts/networks
--excludefile                   → Exclusion file
--excludefile <exclude_file>    → Exclude list from file
```

Other Options

```
-d                              → Debugging level
-f                              → Fragment OP packets
-r                              → Disable randomizing scanned ports
-v                              → Verbosity level
--ttl                           → Set IPv4 time to live
--packet-trace                  → Packet trace
--traceroute                    → Trace routes to targets
--max-retries                   → Max retries
```

EXAMPLES

```
nmap
nmap –version
nmap <target>
nmap -6 -sV <target>                → Simple IPv6 Scan
nmap -A -T4 -v
nmap -A -T4 -f <target>             → Simple version detection
nmap -A -T4 <target>                → Complex version detection
nmap -A -F -Ssu <target>            → RPC Scan
nmap -f <target>                    → ???
nmap -hU -Q<host(s.>                → Stack fingerprinting
nmap -iL <inputfilename>            → Input from list of hosts/networks
nmap -iR <num hosts>                → Choose random targets
nmap -n -sS -P0 -p 80 ***.***.**.** → Stealth Scan
nmap -O -v <target>                 → OS detection with verbosity
nmap -p 21 [IP]                     → Display open ports
nmap -p 1-65535 -T4 -A -v           → Intense Scan all TCP Ports
nmap -SC -sV -O <target>            →
nmap -sL <IP | Network>
nmap -sn                            → Ping Scan
nmap -sn --traceroute               → Quick Traceroute
nmap -sO -T <target>                → Show open ports
nmap –sP x.x.x.x/24                 → Ping Sweep
nmap -sS -sU -T4 -A -v              → Intense Scan plus UDP, half-open scan,
                                      Stealth scan
nmap -sS -D <SrcIP1>,<SrcIp2> <target>

nmap -sT -O -T0                     → Least amount of noise
nmap -sU -v <target>                → UDP Scan
nmap -sV -T4 -O -F --version-light  → Quick Scan plus
nmap -T4                            → Agressive Scan, fast and parallel
nmap -T4 -A -v                      → Intense Scan
nmap -T4 -A -v <IP>                 → Intense Scan single IP
nmap -T4 -A -v -Pn                  → Intens Scan no Ping
nmap -T4 -F                         → Quick Scan
nmap -T4 -F x.x.x.x/24              → Enumerating a network
nmap -T5                            → Very Fast test
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
nmap --mtu 8 <target>               → Use a multiple of 8
nmap -vv <target>                   → Verbose mode reporting details.
```

SCRIPTS

- http-git
- http-methods
  Detect HTTP Methods such as CONNECT, GET, POST, HEAD, PUT, DELTE, TRACE
- Cmd: for /L %V in (1 1 254) do PING -n 1 192.168.2%V | FIND /I "Reply"
  Enumeration of alive systems in a Class C network
- ssl-heartbleed

EXAMPLES

```
nmap --script http-methods <target>
```

DEFINITIONS

Maimon Scan

-sM

- The Maimon scan is named after its discoverer, Uriel Maimon.
- He described the technique in *Phrack* Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later.
- This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK.

Abbreviations

ANCP	Access Node Control Protocol (Port: 6068)
BACnet	Building Automation and Control Network
BRAS	Broadband Remote Access Servers
EPAN	Ethernet Protocol Analyzer
MIB	Management Information Base (ASN 1)
MSDU	MAC Service Data Unit (max. 2304 bytes)
NSE	Nmap Scripting Engine
OID	Object IDs
ONC	Open Network Computing (var of RPC)
PPI	Per-Packet Information (WLAN)
RTP	Real-time Transport Protocol
RTO	TCP Retransmission Timeout
SIP	Session Initiation Protocol
SOC	Security Operation Center
SRT	Service Response Time
TSO	TCP Segmentation Offload

Table of Figures

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Tables

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Index