Nmap Cheat Sheet

Podstawowe techniki skanowania

- Skenowanie pojedynczego celu
  - `nmap [cel]`
- Skenowanie wielu celów
  - `nmap [cel1,cel2,itd.]`
- Skenowanie listy celów
  - `nmap -iL [lista.txt]`
- Skenowanie zakresu hostów
  - `nmap [zakres adresów IP]`
- Skenowanie całej podsieci
  - `nmap [adres IP/cdir]`
- Skenowanie losowych hostów
  - `nmap -iR [liczba]`
- Wykluczanie celów ze skanowania
  - `nmap [cele] -exclude [cele]`
- Wykluczanie celów za pomocą listy
  - `nmap [cele] -excludefile [lista.txt]`
- Wykonanie agresywnego skanowania
  - `nmap -A [cel]`
- Skanowanie celu IPv6
  - `nmap -6 [cel]`

Opcje wykrywania

- Wykonaj tylko skanowanie pingowe
  - `nmap -sP [cel]`
- Nie wykonuj pinga
  - `nmap -PN [cel]`
- Ping TCP SYN
  - `nmap -PS [cel]`
- Ping TCP ACK
  - `nmap -PA [cel]`
- Ping UDP
  - `nmap -PU [cel]`
- Ping SCTP Init
  - `nmap -PY [cel]`
- Ping ICMP echo
  - `nmap -PE [cel]`
- Ping ICMP Timestamp
  - `nmap -PP [cel]`
- Ping ICMP maski adresu
  - `nmap -PM [cel]`
- Ping protokołu IP
  - `nmap -PO [cel]`

- Ping ARP
  - `nmap -PR [cel]`
- Traceroute
  - `nmap -traceroute [cel]`
- Wymuś odwróconą rezerwację DNS
  - `nmap -R [cel]`
- Wyłącz odwróconą rezerwację DNS
  - `nmap -n [cel]`
- Alternatywne wyszukiwanie DNS
  - `nmap -system-dns [cel]`
- Ręcznie określ serwery DNS
  - `nmap -dns-servers [serwery] [cel]`
- Utwórz listę hostów
  - `nmap -sL [cele]`

Zaawansowane opcje skanowania

- TCP SYN Scan
  - `nmap -sS [cel]`
- TCP connect scan
  - `nmap -sT [cel]`
- Skanowanie UDP
  - `nmap -sU [cel]`
- TCP Null scan
  - `nmap -sN [cel]`
- TCP Fin scan
  - `nmap -sF [cel]`
- Xmas scan
  - `nmap -sX [cel]`
- TCP ACK scan
  - `nmap -sA [cel]`
- Skanowanie niestandardowe TCP
  - `nmap -scanflags [flagi] [cel]`
- Skanowanie protokołu IP
  - `nmap -sO [cel]`
- Wysyłanie ramek Ethernet Raw
  - `nmap -send-eth [cel]`
- Wysyłanie pakietów IP
  - `nmap -send-ip [cel]`

Opcje skanowania portów

- Szybkie skanowanie
  - `nmap -F [cel]`
- Skanowanie konkretnych portów
  - `nmap -p [porty] [cel]`

- Skanowanie portów po nazwie
  - `nmap -p [nazwa portu] [cel]`
- Skanowanie portów po protokole
  - `nmap -sU -sT -p U:[porty],T:[porty] [cel]`
- Skanowanie wszystkich portów
  - `nmap -p "*" [cel]`
- Skanowanie top portów
  - `nmap -top-ports [liczba] [cel]`
- Wykonanie sekwencyjnego skanowania portów
  - `nmap -r [cel]`

Wykrywanie wersji

- Wykrywanie systemu operacyjnego
  - `nmap -O [cel]`
- Przesyłanie odcisków TCP/IP
  - http://www.nmap.org/submit/
- Próba odgadnięcia nieznanej wersji
  - `nmap -O --osscan-guess [cel]`
- Wykrywanie wersji usługi
  - `nmap -sV [cel]`
- Rozwiązywanie problemów z wykrywaniem wersji
  - `nmap -sV --version-trace [cel]`
- Wykonywanie skanowania RPC
  - `nmap -sR [cel]`

Opcje czasowe

- Szablony czasowe
  - `nmap -T [0-5] [target]`
- Ustawienie TTL pakietu
  - `nmap -ttl [czas] [target]`
- Minimalna liczba równoległych połączeń
  - `nmap -min-parallelism [liczba] [target]`
- Maksymalna liczba równoległych połączeń
  - `nmap -max-parallelism [liczba] [target]`
- Minimalna wielkość grupy hostów
  - `nmap -min-hostgroup [liczba] [cele]`
- Maksymalna wielkość grupy hostów
  - `nmap -max-hostgroup [liczba] [cele]`
- Maksymalny czas oczekiwania na odpowiedź (RTT)
  - `nmap -initial-rtt-timeout [czas] [target]`
- Maksymalny czas oczekiwania na odpowiedź (RTT)
  - `nmap -max-rtt-timeout [TTL] [target]`
- Maksymalna liczba prób
  - `nmap -max-retries [liczba] [target]`

- Czas oczekiwania na hosta
  - `nmap -host-timeout [czas] [target]`
- Minimalne opóźnienie skanowania
  - `nmap -scan-delay [czas] [target]`
- Maksymalne opóźnienie skanowania
  - `nmap -max-scan-delay [czas] [target]`
- Minimalna liczba pakietów na sekundę
  - `nmap -min-rate [liczba] [target]`
- Maksymalna liczba pakietów na sekundę
  - `nmap -max-rate [liczba] [target]`
- Omijanie limitów szybkości resetowania
  - `nmap -defeat-rst-ratelimit [target]`

Techniki omijania zapory ogniowej

- Fragmentowanie pakietów
  - `nmap -f [cel]`
- Określenie określonej MTU
  - `nmap -mtu [MTU] [cel]`
- Użyj przynęty
  - `nmap -D RND: [liczba] [cel]`
- Skanowanie zombie w stanie bezczynności
  - `nmap -sI [zombie] [cel]`
- Ręczne określenie portu źródłowego
  - `nmap -source-port [port] [cel]`
- Dołącz losowe dane
  - `nmap -data-length [rozmiar] [cel]`
- Losowe kolejność skanowania celów
  - `nmap -randomize-hosts [cel]`
- Podrobić adres MAC
  - `nmap -spoof-mac [MAC|0|vendor] [cel]`
- Wysyłaj błędne sumy kontrolne
  - `nmap -badsum [cel]`

Opcje wyjścia

- Zapisz wynik do pliku tekstowego
  - `nmap -oN [scan.txt] [target]`
- Zapisz wynik do pliku xml
  - `nmap -oX [scan.xml] [target]`
- Wynik w formacie grepable
  - `nmap -oG [scan.txt] [target]`
- Zapisz wynik w kilku formatach naraz
  - `nmap -oA [ścieżka/nazwa_pliku] [target]`
- Wyświetlaj statystyki co pewien czas
  - `nmap -stats-every [czas] [target]`

- Wynik w stylu 133t
  - `nmap -oS [scan.txt] [target]`

Rozwiązywanie problemów i debugowanie

- Pomoc
  - `nmap -h`
- Wyświetl wersję Nmap
  - `nmap -V`
- Szczegółowe wyjście
  - `nmap -v [target]`
- Debugowanie
  - `nmap -d [target]`
- Wyświetl przyczynę stanu portu
  - `nmap -reason [target]`
- Wyświetl tylko otwarte porty
  - `nmap -open [target]`
- Śledź pakiety
  - `nmap -packet-trace [target]`
- Wyświetl sieć hosta
  - `nmap -iflist`
- Określ interfejs sieciowy
  - `nmap -e [interface] [target]`

Nmap Scripting Engine

- Wykonaj pojedynczy skrypt
  - `nmap -script [script.nse] [target]`
- Wykonaj wiele skryptów
  - `nmap -script [expression] [target]`
- Kategorie skryptów
  - `all, auth, default, discovery, external, intrusive, malware, safe, vuln`
- Wykonaj skrypty według kategorii
  - `nmap -script [category] [target]`
- Wykonaj wiele kategorii skryptów
  - `nmap -script [category1,category2, etc]`
- Rozwiązywanie problemów ze skryptami
  - `nmap -script [script] -script-trace [target]`
- Aktualizacja bazy danych skryptów
  - `nmap -script-updatedb`

Ndiff

- Porównanie za pomocą Ndiff
  - `ndiff [scan1.xml] [scan2.xml]`
- Tryb szczegółowy Ndiff

  - ndiff -v [scan1.xml] [scan2.xml]
- Tryb wyjścia XML
  - ndiff -xml [scan1.xm] [scan2.xml]

```
Handy Examples:
Nmap Basics:

Scan a single target
    nmap [IP]

Scan multiple IPs
    nmap [IP1,IP2,IP3…]

Scan a list
    nmap -iL [list.txt]

Scan a range of hosts
    nmap [10.1.1.1-10.1.1.200]

Scan an entire subnet
    nmap [IP address/cdir]

Excluding targets from a scan
    nmap [IP] -exclude [IP]

Excluding targets using a list
    nmap [IPs] -excludefile [list.txt]

Create a list of hosts scanned
    nmap -sL [IPs

     Evasion
Fragment packets
    nmap -f [IP]

Specify a specific MTU
    nmap -mtu [MTU] [IP]

Append random data
    nmap -data-length [size] [IP]

Spoof MAC Address
    nmap -spoof-mac [MAC|0|vendor] [IP]

Send bad checksums
    nmap -badsum [IP]
```

```
Output
Save output to a text file
    nmap -oN [scan.txt] [IP]

Save output to a xml file
    nmap -oX [scan.xml] [IP]

Grepable output
    nmap -oG [scan.txt] [IP]

Output all supported file types
    nmap -oA [path/filename] [IP

Comparing Scan Results
Comparison using Ndiff
    ndiff [scan1.xml] [scan2.xml]

Ndiff verbose mode
    ndiff -v [scan1.xml] [scan2.xml]

XML output mode
    ndiff -xml [scan1.xm] [scan2.xml]]

Nmap Scripting Engine

Execute individual NSE scripts
    nmap -script [script.nse] [IP]

Execute multiple NSE scripts
    nmap -script [script1.nse,script2.nse…] [IP]

Execute NSE scripts by category
    nmap -script [cat] [target]

Execute multiple NSE script categories
    nmap -script [auth, default…] [IP]

NSE Script categories:
all
auth
default
discovery
external
intrusive
malware
```

```
safe

Nmap default commands:
Usage: nmap [Scan Type(s)] [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
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

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

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

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

SERVICE/VERSION DETECTION:
```

```
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --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).
  -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.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second

FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --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:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase 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)
  --log-errors: Log errors/warnings to the normal-format output file
  --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:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --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
  -V: Print version number
  -h: Print this help summary page.

EXAMPLES:
  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
```

Links

- Man Pages - http://nmap.org/book/man.html
- Nmap Scripting Engine - http://nmap.org/book/nse.html
- Nmap Scripting Engine list of current scripts - http://nmap.org/nsedoc/index.html
- Nmap Scripting Engine Documentation - http://nmap.org/book/nse.html
- Common Nmap Comman Examples - http://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

- 30 Nmap Command Examples - http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
- Fajny cheatsheet