# Nmap Basics - One Page Cheat Sheet

**Nmap Command Format:** nmap [Scan Type(s)] [Options] {target}
**Nmap Script Scan Format:** nmap --script [Script(s) Name] {target}

**Help**

All OS

| | |
|---|---|
| nmap | Help |
| nmap -h | Same as above |
| nmap -V | Version information |
| nmap --script-help <script name> | |

Linux/Unix

| | |
|---|---|
| man nmap | nmap Man Page |
| man zenmap | Zenmap Man Page |

**Scan Techniques**

| | |
|---|---|
| nmap -sS | TCP SYN port scan (Default) |
| nmap -sT | TCP Full-connect port scan |
| nmap -sU | UDP port scan |
| nmap -sO | IP Protocol scan |

**Host Discovery**

| | |
|---|---|
| nmap - sL | List scan. Reverse DNS lookup. |
| nmap -sn | Ping scan/sweep. Doesn't scan ports. |
| nmap -Pn | No ping scan. Only scans ports. |

**OS Discovery**

| | |
|---|---|
| nmap -O | Basic operating system discovery |
| nmap -O --osscan-guess | Will guess, Gives % certainty |
| nmap --script smb-host-discovery | |

**NSE Script Scans (located in Nmap directory \scripts)**

| | |
|---|---|
| nmap -sC | Scans with all scripts labeled default |
| nmap --script <category> | |
| nmap --script <script name> | |

**Timing and Performance (time in ms, s, h)**

| | |
|---|---|
| nmap -T0 | Paranoid. IDS evasion, very slow. |
| nmap -T1 | Sneaky. IDS evasion, slow. |
| nmap -T2 | Polite. Use if machines or network slow |
| nmap -T3 | Default. If using, just leave off. |
| nmap -T4 | Aggressive. Fast, assumes fast network |
| nmap -T5 | Insane. Very fast, less accurate results |
| nmap --host-timeout <time> | Give up on target after this amount of time |
| nmap --scan-delay <time> | Adjust delay between probes |
| nmap --min-rate <# packets> | Send packets no slower than this per second |

**Target** nmap *{target}*

Host name - FILESERVER
FQDN - scanme.nmap.org
IP - 192.168.1.1
IPs - 192.168.1.1 192.168.1.2
Range - 192.168.1.1-50
CIDR - 192.168.1.1/24
DNS CIDR - nmap.org/24

**Ports** nmap -p

nmap -p 80
nmap -p 21-3389
nmap -sU -p 1-1000
nmap -sS -sU -p T:21-25,80,U:53-389
nmap -F

**Service/Version Detection**

| | |
|---|---|
| nmap -sV | App & Service Versions |
| nmap -A | Aggressive / Advanced |
| nmap --version-intensity <level> | |

**Output (e.g. nmap -oN <filename>)**

| | |
|---|---|
| nmap -oN | Normal output to file |
| nmap -oX | XML output to file |
| nmap -oG | Grepable output to file |
| nmap -oA | Three output formats |
| nmap -v | More detail |
| nmap -d | Debugging information |

**Misc. Options & IDS/Firewall Evasion**

| | |
|---|---|
| -6 | IPv6 scanning (put first) |
| -D <decoy> | Decoy cloaking |
| -f <val> | Fragment packets |
| -S <ip> | Spoof source |
| -g <#> | Use source port |