

### Target Specification

| <u>Switch</u> | <u>Example</u>                | <u>Description</u>       |
|---------------|-------------------------------|--------------------------|
|               | nmap 192.168.50.1             | Scan a single IP         |
|               | nmap 192.168.50.1 192.168.2.1 | Scan specific IPs        |
|               | nmap 192.168.50.1-254         | Scan a range             |
|               | nmap scanme.nmap.org          | Scan a domain            |
|               | nmap 192.168.50.0/24          | Scan using CIDR notation |
| -iL           | nmap -iL targets.txt          | Scan targets from a file |
| --exclude     | nmap --exclude 192.168.50.1   | Exclude listed hosts     |

### Scan Techniques

| <u>Switch</u> | <u>Example</u>        | <u>Description</u>                                     |
|---------------|-----------------------|--|
| -sS           | nmap 192.168.50.1 -sS | TCP SYN port scan (Default)                            |
| -sT           | nmap 192.168.50.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU           | nmap 192.168.50.1 -sU | UDP port scan  |
| -sA           | nmap 192.168.50.1 -sA | TCP ACK port scan                                      |
| -sW           | nmap 192.168.50.1 -sW | TCP Window port scan                                   |

### OS Detection

| <u>Switch</u>     | <u>Example</u>                        | <u>Description</u>   |
|-------------------|---------------------------------------|--|
| -O                | nmap 192.168.50.1 -O                  | Remote OS detection using TCP/IP stack fingerprinting  |
| -O --osscan-limit | nmap 192.168.50.1 -O --osscan-limit   | If at least one open and one closed TCP port are not found it will not try OS detection against host |
| -O --osscan-guess | nmap 192.168.50.1 -O --osscan-guess   | Makes Nmap guess more aggressively   |
| -O --max-os-tries | nmap 192.168.50.1 -O --max-os-tries 1 | Set the maximum number x of OS detection tries against a target                                      |
| -A                | nmap 192.168.50.1 -A                  | Enables OS detection, version detection, script scanning, and traceroute                             |

### Host Discovery

| <u>Switch</u> | <u>Example</u>                  | <u>Description</u>                                 |
|---------------|---------------------------------|--|
| -sL           | nmap 192.168.50.1-3 -sL         | No Scan. List targets only                         |
| -sn           | nmap 192.168.50.1/24 -sn        | Disable port scanning. Host discovery only.        |
| -Pn           | nmap 192.168.50.1-5 -Pn         | Disable host discovery. Port scan only.            |
| -PS           | nmap 192.168.50.1-5 -PS22-25,80 | TCP SYN discovery on port x. Port 80 by default    |
| -PA           | nmap 192.168.50.1-5 -PA22-25,80 | TCP ACK discovery on port x.<br>Port 80 by default |
| -PU           | nmap 192.168.50.1-5 -PU53       | UDP discovery on port x.<br>Port 40125 by default  |
| -PR           | nmap 192.168.50.1-1/24 -PR      | ARP discovery on local network                     |
| -n            | nmap 192.168.50.1 -n            | Never do DNS resolution                            |

### Port Specification

| <u>Switch</u> | <u>Example</u>                       | <u>Description</u>   |
|---------------|--------------------------------------|--|
| -p            | nmap 192.168.50.1 -p 21              | Port scan for port x   |
| -p            | nmap 192.168.50.1 -p 21-100          | Port range   |
| -p            | nmap 192.168.50.1 -p U:53,T:21-25,80 | Port scan multiple TCP and UDP ports                                     |
| -p-           | nmap 192.168.50.1 -p-                | Port scan all ports  |
| -p            | nmap 192.168.50.1 -p http,https      | Port scan from service name  |
| -F            | nmap 192.168.50.1 -F                 | Fast port scan (100 ports)   |
| --top-ports   | nmap 192.168.50.1 --top-ports 2000   | Port scan the top x ports  |
| -p-65535      | nmap 192.168.50.1 -p-65535           | Leaving off initial port in range<br>makes the scan start at port 1      |
| -p0-          | nmap 192.168.50.1 -p0-               | Leaving off end port in range<br>makes the scan go through to port 65535 |

### Service and Version Detection

| <u>Switch</u>           | <u>Example</u>                              | <u>Description</u>   |
|-------------------------|---|--|
| -sV                     | nmap 192.168.50.1 -sV                       | Attempts to determine the version of the service running on port           |
| -sV --version-intensity | nmap 192.168.50.1 -sV --version-intensity 8 | Intensity level 0 to 9. Higher number increases possibility of correctness |
| -sV --version-light     | nmap 192.168.50.1 -sV --version-light       | Enable light mode. Lower possibility of correctness. Faster                |
| -sV --version-all       | nmap 192.168.50.1 -sV --version-all         | Enable intensity level 9. Higher possibility of correctness. Slower        |
| -A                      | nmap 192.168.50.1 -A                        | Enables OS detection, version detection, script scanning, and traceroute   |

### Timing and Performance

| <u>Switch</u> | <u>Example</u>        | <u>Description</u>   |
|---------------|-----------------------|--|
| -T0           | nmap 192.168.50.1 -T0 | Paranoid (0) Intrusion Detection System evasion  |
| -T1           | nmap 192.168.50.1 -T1 | Sneaky (1) Intrusion Detection System evasion  |
| -T2           | nmap 192.168.50.1 -T2 | Polite (2) slows down the scan to use less bandwidth and use less target machine resources |
| -T3           | nmap 192.168.50.1 -T3 | Normal (3) which is default speed  |
| -T4           | nmap 192.168.50.1 -T4 | Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network     |
| -T5           | nmap 192.168.50.1 -T5 | Insane (5) speeds scan; assumes you are on an extraordinarily fast network                 |