**Target Specification**

| **WITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
|  | nmap 192.168.1.1 | Scan a single IP |
|  | nmap 192.168.1.1 192.168.2.1 | Scan specific IPs |
|  | nmap 192.168.1.1-254 | Scan a range |
|  | nmap scanme.nmap.org | Scan a domain |
|  | nmap 192.168.1.0/24 | Scan using CIDR notation |
| -iL | nmap -iL targets.txt | Scan targets from a file |
| -iR | nmap -iR 100 | Scan 100 random hosts |
| -exclude | nmap -exclude 192.168.1.1 | Exclude listed hosts |

**Nmap Scan Techniques**

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan (Default) |
| -sT | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
| -sA | nmap 192.168.1.1 -sA | TCP ACK port scan // If the port is filtered, the target will not send any response or drop the packet. If the port is unfiltered, the target will send back a TCP RST packet, indicating an invalid ACK. |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan // Not all ports can be tested as TCP Window Scan does not support UDP protocol |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan // sets two flags – FIN and ACK. In response, we should receive an RST packet |

## ****Host Discovery****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -sL | nmap 192.168.1.1-3 -sL | No Scan. List targets only |
| -sn | nmap 192.168.1.1/24 -sn | Disable port scanning. Host discovery only. |
| -Pn | nmap 192.168.1.1-5 -Pn | Disable host discovery. Port scan only. |
| -PS | nmap 192.168.1.1-5 -PS22-25,80 | TCP SYN discovery on port x. Port 80 by default |
| -PA | nmap 192.168.1.1-5 -PA22-25,80 | TCP ACK discovery on port x. Port 80 by default |
| -PU | nmap 192.168.1.1-5 -PU53 | UDP discovery on port x. Port 40125 by default |
| -PR | nmap 192.168.1.1-1/24 -PR | ARP discovery on local network |
| -n | nmap 192.168.1.1 -n | Never do DNS resolution |

## ****Port Specification****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -p | nmap 192.168.1.1 -p 21 | Port scan for port x |
| -p | nmap 192.168.1.1 -p 21-100 | Port range |
| -p | nmap 192.168.1.1 -p U:53,T:21-25,80 | Port scan multiple TCP and UDP ports |
| -p | nmap 192.168.1.1 -p- | Port scan all ports |
| -p | nmap 192.168.1.1 -p http,https | Port scan from service name |
| -F | nmap 192.168.1.1 -F | Fast port scan (100 ports) |
| -top-ports | nmap 192.168.1.1 -top-ports 2000 | Port scan the top x ports |
| -p-65535 | nmap 192.168.1.1 -p-65535 | Leaving off initial port in range makes the scan start at port 1 |
| -p0- | nmap 192.168.1.1 -p0- | Leaving off end port in range makes the scan go through to port 65535 |

## ****Service and Version Detection****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -sV | nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |
| -sV -version-intensity | nmap 192.168.1.1 -sV -version-intensity 8 | Intensity level 0 to 9. Higher number increases possibility of correctness |
| -sV -version-light | nmap 192.168.1.1 -sV -version-light | Enable light mode. Lower possibility of correctness. Faster |
| -sV -version-all | nmap 192.168.1.1 -sV -version-all | Enable intensity level 9. Higher possibility of correctness. Slower |
| -A | nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |

## ****OS Detection****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -O | nmap 192.168.1.1 -O | Remote OS detection using TCP/IP stack fingerprinting |
| -O -osscan-limit | nmap 192.168.1.1 -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 192.168.1.1 -O -osscan-guess | Makes Nmap guess more aggressively |
| -O -max-os-tries | nmap 192.168.1.1 -O -max-os-tries 1 | Set the maximum number x of OS detection tries against a target |
| -A | nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |

## ****Output****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -oN | nmap 192.168.1.1 -oN normal.file | Normal output to the file normal.file |
| -oX | nmap 192.168.1.1 -oX xml.file | XML output to the file xml.file |
| -oG | nmap 192.168.1.1 -oG grep.file | Grepable output to the file grep.file |
| -oA | nmap 192.168.1.1 -oA results | Output in the three major formats at once |
| -oG - | nmap 192.168.1.1 -oG - | Grepable output to screen. -oN -, -oX - also usable |
| -append-output | nmap 192.168.1.1 -oN file.file -append-output | Append a scan to a previous scan file |
| -v | nmap 192.168.1.1 -v | Increase the verbosity level (use -vv or more for greater effect) |
| -d | nmap 192.168.1.1 -d | Increase debugging level (use -dd or more for greater effect) |
| -reason | nmap 192.168.1.1 -reason | Display the reason a port is in a particular state, same output as -vv |
| -open | nmap 192.168.1.1 -open | Only show open (or possibly open) ports |
| -packet-trace | nmap 192.168.1.1 -T4 -packet-trace | Show all packets sent and received |
| -iflist | nmap -iflist | Shows the host interfaces and routes |