

Nmap Cheat Sheet

Target Specification

| Switch | 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 |

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 |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan |

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 |
| -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 |