nmap Cheat Sheet

Installation

```
sudo apt install nmap
```

Basic usage

Command	Description
nmap <options> <target>	Scan a target
nmap -h	Show help

Target specification

Command	Description
nmap <target>	Scan a single target
nmap <target1> <target2>	Scan multiple targets
nmap 192.168.1.0/24	Scan a network
nmap -iL <file>	Read targets from a file

Host discovery

Flag	Description
-sn	Ping scan (disable port scan)
-Pn	Treat all hosts as online (skip ICMP Echo requests)
-PE	ICMP echo request (ping)
-n	Disable DNS resolution

Scan techniques

Flag	Description
-sS	TCP SYN scan (requires root)
-sT	TCP connect scan (less invasive)
-sA	TCP ACK scan
-sU	UDP scan

Port specification

Flag	Description
-p <port>	Scan a single port
-p <port1,2>	Scan multiple ports
-p <port1-5>	Scan a range of ports
-p-	Scan all ports
-F	Fast mode (top 100 ports)
--top-ports <n>	Scan the top n common ports

OS / service / version detection

Flag	Description
-O	Enable OS detection
-sV	Probe open ports to determine service/version info
-A	Enable OS detection, version detection, and scripts

Script scanning

Flag	Description
-sC	Scan with the default set of scripts
--script=<name>	Scan with the specified script(s)

Performance

Flag	Description
--initial-rtt-timeout <time>	Set initial RTT timeout
--max-rtt-timeout <time>	Set max RTT timeout
--max-retries <tries>	Set max retries
--min-rate <number>	Set min packet rate

Timing templates

Flag	Description
-T0	Paranoid (IDS evasion)
-T1	Sneaky (IDS evasion)
-T2	Polite (slow)
-T3	Normal (default)
-T4	Aggressive (fast)
-T5	Insane (very fast)

Output

Command / flag	Description
-oN <file>	Write normal output to a file
-oG <file>	Write grepable output to a file
-oX <file>	Write XML output to a file
-oA <basename>	Write output in all 3 formats
-v	Increase verbosity
--packet-trace	Show all packets sent and received
--reason	Show the reason for the port state
--stats-every <n>	Show scan statistics every n seconds

Nmap examples

Command	Description
nmap -sn 192.168.1.1/24	Discover hosts on a network
sudo nmap -sS <target>	TCP SYN scan
sudo nmap <target> -p 80 -sV --script vuln	Scan for vulnerabilities on port 80