nmap Network scanner

Targets hosts, CIDR → `discovery` → **Live hosts** ping probes → `port scan` → **Port states** open/closed/filtered → `-sV -O -sC` → **Details** service, OS, scripts

CONCEPTS

> Only scan hosts and networks you own or are explicitly authorised to test. Unauthorised scans can be illegal and set off alarms.

> Without root, nmap falls back to a TCP connect scan (-sT); raw-packet scans like -sS, -sU and -O need privileges.

> Port states: open, closed, filtered (no reply, probably a firewall), unfiltered, plus open|filtered and closed|filtered when nmap cannot tell.

TARGETS

`nmap <host>`
Scan one host

`nmap <host1> <host2>`
Scan several hosts

`nmap <net>/24`
Scan a whole subnet (CIDR)

`nmap 192.168.0-255.1-254`
Scan with octet ranges

`nmap -iL <file>`
Read targets from a file

`nmap --exclude <hosts>`
Skip hosts or networks

TARGETS (cont.)

`nmap -6 <host>`
Scan IPv6 addresses

HOST DISCOVERY

`nmap -sn <net>/24`
Ping scan only, no port scan

`nmap -Pn <host>`
Skip discovery, assume host is up

`nmap -PS<ports> <host>`
Discover with TCP SYN probes

`nmap -n <host>`
Never resolve DNS names

PORTS

`nmap -p <port> <host>`
Scan one port

`nmap -p 22,80,443 <host>`
Scan a port list

`nmap -p 1-1023 <host>`
Scan a port range

`nmap -p- <host>`
Scan all 65535 ports

`nmap -F <host>`
Fast: top 100 ports only

`nmap --top-ports <n> <host>`
Scan the n most common ports

PORTS (cont.)

`nmap -p T:80,U:53 <host>`
Mix TCP and UDP ports

SCAN TYPES

`nmap -sS <host>`
TCP SYN (half-open) scan

`nmap -sT <host>`
TCP connect scan

`nmap -sU <host>`
UDP scan

`nmap -sN <host>`
TCP NULL scan (no flags)

DETECTION

`nmap -sV <host>`
Detect service versions

`nmap -O <host>`
Detect the operating system

`nmap -A <host>`
OS, versions, scripts, traceroute

`nmap -sV --version-intensity <0-9> <host>`
Set version probe depth

SCRIPTS (NSE)

`nmap -sC <host>`
Run default scripts

`nmap --script <name> <host>`
Run a named script

SCRIPTS (NSE) (cont.)

`nmap --script <category> <host>`
Run a category (safe, vuln...)

`nmap --script "http-*" <host>`
Run scripts by wildcard

`nmap --script-args <k>=<v> <host>`
Pass arguments to scripts

`nmap --script-help <script>`
Describe a script or category

> NSE scripts are not sandboxed and categories like intrusive, brute, exploit and dos can disrupt services. Review scripts before running them and prefer safe.

TIMING & PERFORMANCE

`nmap -T4 <host>`
Faster scan on a reliable network

OUTPUT

`nmap -v <host>`
More verbose, repeat for more

OUTPUT (cont.)

`nmap --open <host>`
Show only open ports

`nmap -oN <file> <host>`
Save normal output

`nmap -oX <file> <host>`
Save XML output

`nmap -oA <base> <host>`
Save normal, XML and grepable

`nmap -oG <file> <host>`
Save grepable output

`nmap --reason <host>`
Explain each port state

MISC

`nmap -h`
Short help screen

`nmap --version`
Print nmap version

RECIPES

Map a LAN, then dig in

```
# 1. who is up?
nmap -sn 192.168.1.0/24 -oG - | grep Up
# 2. details on one host
sudo nmap -sS -sV -O -p- 192.168.1.10
```

Thorough scan, saved

```
sudo nmap -p- -sV -sC -T4 -oA scan <host>
# review later
less scan.nmap
```