NMAP QUICK REFERENCE

Port scanning, host discovery, service detection, and NSE scripts

Basic Scans

Scan Targets

```
nmap 192.168.1.1              # single host
nmap 192.168.1.0/24           # entire subnet
nmap 192.168.1.1-50           # IP range
nmap -iL targets.txt          # hosts from file
```

Target Specification

`192.168.1.1`	Single IP address
`192.168.1.0/24`	CIDR notation (256 hosts)
`192.168.1.1-254`	IP range
`example.com`	Hostname (resolved to IP)
`-iL file.txt`	Read targets from file
`--exclude 192.168.1.1`	Exclude specific hosts
`--excludefile skip.txt`	Exclude hosts from file

Port Scanning

Scan Types

`-sS`	TCP SYN scan (default, stealthy, needs root)
`-sT`	TCP connect scan (full handshake, no root)
`-sU`	UDP scan (slow, often filtered)
`-sA`	TCP ACK scan (detect firewalls)
`-sN`	TCP NULL scan (no flags set)
`-sF`	TCP FIN scan (only FIN flag)
`-sX`	Xmas scan (FIN+PSH+URG flags)

Port Selection

```
nmap -p 80,443 target         # specific ports
nmap -p 1-1000 target         # port range
nmap -p- target               # all 65535 ports
nmap --top-ports 100 target   # most common 100 ports
```

Port States

`open`	Application is accepting connections
`closed`	Port reachable but no service listening
`filtered`	Firewall blocking, can't determine state
`unfiltered`	Port accessible, open/closed unknown
`open|filtered`	Can't determine if open or filtered

Host Discovery

Discovery Methods

`-sn`	Ping scan only (no port scan)
`-Pn`	Skip host discovery (treat all as up)
`-PS 80,443`	TCP SYN discovery on ports
`-PA 80`	TCP ACK discovery
`-PU 53`	UDP discovery
`-PE`	ICMP echo request
`-PR`	ARP discovery (local network)

Network Sweep

```
nmap -sn 192.168.1.0/24       # ping sweep subnet
nmap -sn -n 10.0.0.0/24       # sweep, skip DNS
nmap -sn -PR 192.168.1.0/24   # ARP scan (fastest)
```

Service Detection

Version Detection

```
nmap -sV target               # detect service versions
nmap -sV --version-intensity 5 target  # deeper probing
nmap -sV --version-all target  # try every probe (slow)
nmap -A target                # OS + version + scripts +
traceroute
```

Service Flags

`-sV`	Probe open ports for service/version
`--version-intensity 0-9`	Probe intensity (default 7)
`--version-light`	Light probing (intensity 2)
`--version-all`	Try every probe (intensity 9)
`-A`	Aggressive: -sV -O --script=default -traceroute
`-sC`	Run default NSE scripts

OS Detection

OS Fingerprinting

```
nmap -O target                # OS detection (needs root)
nmap -O --osscan-limit target # only scan promising hosts
nmap -O --osscan-guess target # aggressive OS guessing
nmap -A target                # includes OS detection
```

OS Detection Flags

`-O`	Enable OS detection
`--osscan-limit`	Skip hosts without open+closed TCP ports
`--osscan-guess`	Guess OS more aggressively
`--max-os-tries N`	Max OS detection attempts per host

Scripts (NSE)

Script Usage

```
nmap --script=default target   # default category
nmap --script=vuln target      # vulnerability scripts
nmap --script=http-headers target
nmap --script="http-*" target  # wildcard match
```

Script Categories

`default`	Safe, useful scripts (-sC shorthand)
`vuln`	Check for known vulnerabilities
`safe`	Non-intrusive scripts
`intrusive`	May crash targets or trigger IDS
`discovery`	Network & service discovery
`auth`	Authentication-related checks
`brute`	Brute-force credential testing
`exploit`	Active exploitation attempts

Useful Scripts

`http-title`	Grab web page titles
`ssl-cert`	Show SSL certificate details
`ssh-hostkey`	Show SSH host key fingerprints
`dns-brute`	Enumerate DNS subdomains
`smb-os-discovery`	Detect Windows OS via SMB
`vuln`	Run all vulnerability checks

Output Formats

Output Options

```
nmap -oN scan.txt target      # normal text output
nmap -oX scan.xml target      # XML output
nmap -oG scan.gnmap target    # grepable output
nmap -oA scan_all target      # all formats at once
```

Output Flags

`-oN file`	Normal output to file
`-oX file`	XML output (for tools/parsing)
`-oG file`	Grepable output (one host per line)
`-oA basename`	All three formats (basename.nmap/xml/gnmap)
`-v`	Increase verbosity (-vv for more)
`-d`	Debug output (-dd for more)
`--open`	Show only open ports
`--reason`	Show reason for port state

Timing & Performance

Timing Templates

`-T0 (paranoid)`	Very slow, IDS evasion (5 min between probes)
`-T1 (sneaky)`	Slow, IDS evasion (15 sec between probes)
`-T2 (polite)`	Reduced speed, less bandwidth
`-T3 (normal)`	Default timing
`-T4 (aggressive)`	Fast, assumes reliable network
`-T5 (insane)`	Fastest, may miss results

Fine-Grained Tuning

`--min-rate 1000`	Send at least 1000 packets/sec
`--max-rate 500`	Cap at 500 packets/sec
`--max-retries 2`	Max probe retransmissions
`--host-timeout 30m`	Skip host if scan exceeds 30 min
`--scan-delay 1s`	Delay between probes
`--min-parallelism 10`	Min parallel probe groups

Firewall Evasion

Evasion Techniques

`-f`	Fragment packets (8-byte chunks)
`-D RND:5`	Decoy scan with 5 random IPs
`-S spoof_ip`	Spoof source IP (needs raw packets)
`-e eth0`	Use specific network interface
`--source-port 53`	Use specific source port (e.g. DNS)
`--data-length 25`	Append random data to packets
`--spoof-mac 0`	Randomize MAC address

Evasion Examples

```
nmap -f -D RND:3 target       # fragments + decoys
nmap --source-port 53 target  # DNS port (often allowed)
nmap -T1 --scan-delay 5s target  # slow to evade IDS
```

Common Patterns

Quick Recon

```
nmap -T4 -F target            # fast common ports
nmap -T4 -A -v target         # OS + service detection
nmap -sV --top-ports 1000 target  # top 1000 + versions
```

Comprehensive Scan

```
# Full TCP + service + OS + scripts
nmap -sS -sV -O -sC -p- -T4 -oA full target
# UDP scan on common ports
nmap -sU --top-ports 50 target
```

Web Server Audit

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Check for open proxies and vulns
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Network Inventory

```
# Discover all live hosts with OS info
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Service inventory for subnet
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```