Nmap Cheat Sheet by

By Amit Singh

Github : Amit

Linkedin: Amit

🔍 Host Discovery

Used to determine which hosts (systems) are up and reachable on a network.
These commands use ICMP, TCP SYN, ARP, or UDP to check if a device is alive before scanning its ports.
Ideal for network reconnaissance or inventory..

- **nmap -sL <target>**: List scan - only shows what targets would be scanned. Does not send packets.
- **nmap -sn <target>**: Ping scan - checks which hosts are up without scanning ports.
- **nmap -Pn <target>**: Treat all hosts as online (skip host discovery). Useful if ping is blocked.
- **nmap -PS80,443 <target>**: TCP SYN discovery to ports 80 and 443. Any response = host is up.
- **nmap -PA21,22,23 <target>**: TCP ACK discovery to ports 21, 22, 23. Used to discover live systems through firewalls.
- **nmap -PU53 <target>**: Sends UDP probes to port 53 to check if host is up.
- **nmap -PR <target>**: ARP discovery on a local network. Most accurate for LAN scans.
- **nmap --dns-servers 1.1.1.1 <target>**: Use custom DNS server for resolution.
- **nmap -n <target>**: Never perform DNS resolution (saves time).
- **nmap -R <target>**: Force DNS resolution even for IPs.

🎯 Target Specification

Defines **which systems** to scan and how to list or exclude them.
Supports single IPs, ranges, subnets (CIDR), domains, and lists from files.

Also allows host exclusion and randomized scanning for stealth.

- **nmap 192.168.1.100**: Scan a single host.
- **nmap 192.168.1.10 192.168.1.20**: Scan multiple specific IPs.
- **nmap 192.168.1.1-50**: Scan a range of IPs.
- **nmap scanme.nmap.org**: Scan a domain.
- **nmap 192.168.1.0/24**: CIDR notation to scan a subnet.
- **nmap -iL targets.txt**: Load targets from a file (one per line).
- **nmap -iR 10**: Scan 10 random Internet hosts.
- **nmap --exclude 192.168.1.5,192.168.1.10 <target>**: Exclude specified IPs from scan.
- **nmap --randomize-hosts <target1> <target2> ...**: Randomizes the order of target scanning.

⚙️ Scan Techniques

Controls **how Nmap scans ports** (TCP, UDP, stealth, etc.).
Includes options like SYN scan (stealth), connect scan, ACK scan (firewall mapping), and null/FIN/Xmas scans for evasion.
Choice of technique affects scan speed, stealth, and privileges required.

- **nmap -sS <target>**: TCP SYN (stealth) scan. Fast, doesn't complete handshake.
- **nmap -sT <target>**: TCP Connect scan. Full connection. Used when not running as root.
- **nmap -sU <target>**: UDP scan to discover services on UDP ports.
- **nmap -sA <target>**: ACK scan. Used to map firewall rules.
- **nmap -sN <target>**: Null scan (no flags). Can bypass some firewalls.
- **nmap -sF <target>**: FIN scan. Sends TCP FIN flag to detect open ports.
- **nmap -sX <target>**: Xmas scan. FIN, URG, PSH flags — a "lit" packet.
- **nmap -sW <target>**: TCP window scan to infer port state using window size.
- **nmap -sM <target>**: Maimon scan. FIN/ACK combination.
- **nmap -sI <zombie_IP> <target>**: Idle scan using a "zombie" system to hide your identity.
- **nmap -b ftp.example.com <target>**: FTP bounce scan. Uses FTP server to scan a host (usually blocked).

📌 Port Specification

Limits or expands **which ports** are scanned on each host.
You can scan specific ports, port ranges, all ports, or even by service name (e.g., `http`).
Helps focus on known vulnerabilities or speed up the scan.

- **nmap -p 80 <target>**: Scan only port 80.
- **nmap -p 20-100 <target>**: Scan a range of ports.
- **nmap -p- <target>**: Scan all 65535 ports.
- **nmap -F <target>**: Fast mode: scan top 100 most common ports.
- **nmap --top-ports 2000 <target>**: Scan top 2000 ports based on frequency.
- **nmap -p U:53,T:21-25,80 <target>**: Scan a mix of TCP and UDP ports.
- **nmap -p http,https <target>**: Use known service names instead of numbers.

🧠 OS & Version Detection

Used to fingerprint the **operating system** and detect **service versions** on open ports.
Can guess OS types and identify outdated or vulnerable software.
Often used in vulnerability assessments and penetration testing.

- **nmap -O <target>**: OS detection using TCP/IP fingerprinting.
- **nmap --osscan-guess <target>**: Try harder to guess OS.
- **nmap -sV <target>**: Service version detection.
- **nmap -A <target>**: Aggressive: OS, version, scripts, traceroute.
- **nmap --version-intensity 5 <target>**: Adjust probing aggressiveness for version detection (0-9).
- **nmap --version-light <target>**: Light mode: faster, less accurate.
- **nmap --version-all <target>**: Use all probes.
- **nmap -O --osscan-limit <target>**: Only do OS detection if certain ports are found.
- **nmap -O --max-os-tries 1 <target>**: Limit retries for OS detection.

📜 NSE (Nmap Scripting Engine)

Extends Nmap's capabilities using powerful **Lua-based scripts**.
Supports scripts for info gathering, brute forcing, vulnerability detection, and exploitation.
You can also create or customize your own scripts.

- **nmap -sC <target>**: Run the default set of safe scripts (equivalent to --script=default).
- **nmap --script=banner <target>**: Run a specific script to grab service banners.
- **nmap --script=http* <target>**: Run all scripts starting with 'http'.
- **nmap --script=http-title,dns-brute <target>**: Run multiple scripts by name.
- **nmap --script "not intrusive" <target>**: Run all default scripts except intrusive ones.
- **nmap --script-args=key=value <target>**: Pass arguments to scripts. Example: snmpcommunity=public.
- **nmap --script http-sitemap-generator <target>**: Generate a website sitemap using the script.
- **nmap --script dns-brute --script-args dns-brute.domain=example.com <target>**: Brute force DNS records for subdomains.
- **nmap --script whois* <target>**: Run all scripts related to WHOIS lookups.
- **nmap --script http-unsafe-output-escaping <target>**: Detects cross-site scripting vulnerabilities.
- **nmap --script http-sql-injection <target>**: Check for SQL injection vulnerabilities.
- **nmap --script-update-db**: Update the local NSE script database.
- **nmap --script-help=http-title**: Show description and arguments for a specific script.

🚀 Performance & Timing

Adjusts **how fast** the scan runs and how many probes Nmap sends.
Useful to reduce noise on the network, avoid detection, or speed up scans on large subnets.
Includes timing templates (`-T0` to `-T5`) and fine-tuning options.

- **nmap -T4 <target>**: Timing template (T0–T5): T0=slowest/stealthiest, T5=fastest/noisy.
- **nmap --host-timeout 30m <target>**: Stop scanning a host after 30 minutes.
- **nmap --min-rtt-timeout 100ms <target>**: Minimum probe round-trip timeout.
- **nmap --max-rtt-timeout 1s <target>**: Maximum probe timeout before giving up.
- **nmap --initial-rtt-timeout 300ms <target>**: Initial timeout used to adjust RTT dynamically.
- **nmap --min-hostgroup 64 <target>**: Minimum number of hosts to scan in a group.

- **nmap --max-hostgroup 256 <target>**: Maximum host scan group size.
- **nmap --min-parallelism 10 <target>**: Minimum concurrent probes.
- **nmap --max-parallelism 100 <target>**: Maximum concurrent probes.
- **nmap --scan-delay 1s <target>**: Delay 1 second between each probe (useful for stealth).
- **nmap --max-scan-delay 5s <target>**: Set a limit on maximum delay between probes.
- **nmap --max-retries 3 <target>**: Try scanning a port up to 3 times.
- **nmap --min-rate 100 <target>**: Send at least 100 packets per second.
- **nmap --max-rate 1000 <target>**: Limit scan speed to 1000 packets per second.

🛡️ Firewall / IDS Evasion

Helps evade **firewalls and intrusion detection systems (IDS)**.
Techniques include packet fragmentation, decoy scans, spoofing MACs/IPs, or using proxies.
Used in stealth operations or Red Team engagements.

- **nmap -f <target>**: Fragment packets into 8-byte fragments.
- **nmap --mtu 32 <target>**: Use a specific MTU size (forces packet fragmentation).
- **nmap -D 192.168.1.10,192.168.1.20,ME,192.168.1.30 <target>**: Decoy scan using fake IPs + your real one ("ME").
- **nmap -S 1.2.3.4 -e eth0 <target>**: Spoof your source IP and specify interface (root only).
- **nmap -g 53 <target>**: Use UDP port 53 as the source port (firewall evasion).
- **nmap --source-port 443 <target>**: Set TCP source port to 443 (HTTPS) for evasion.
- **nmap --proxies socks4://127.0.0.1:9050 <target>**: Use a SOCKS proxy to route scan (Tor etc.).
- **nmap --data-length 200 <target>**: Pad packets with 200 bytes of random data.
- **nmap --spoof-mac 00:11:22:33:44:55 <target>**: Spoof MAC address to hide your identity.
- **nmap --spoof-mac Apple <target>**: Spoof a vendor MAC (e.g., Apple, Cisco).
- **nmap --badsum <target>**: Send packets with incorrect checksums (to test IDS detection).

💾 Output Options

Controls **how scan results are saved or viewed**.
You can save output in normal, XML, grepable, or all formats.
Also supports resuming scans, increasing verbosity, and showing reasons behind scan results.

- **nmap -oN output.txt <target>**: Normal human-readable output saved to file.
- **nmap -oX output.xml <target>**: Save scan in XML format (for parsing or GUIs).
- **nmap -oG output.gnmap <target>**: Greppable format (used in scripts).
- **nmap -oA scan <target>**: Save output in all formats (creates scan.nmap, scan.xml, scan.gnmap).
- **nmap --append-output -oN output.txt <target>**: Append results to an existing file.
- **nmap -v <target>**: Increase verbosity (show more info in output).
- **nmap -vv <target>**: Even more verbose.
- **nmap -d <target>**: Enable debugging mode.
- **nmap -dd <target>**: Extremely verbose debug output.
- **nmap --reason <target>**: Show reason why a port is in its state.
- **nmap --open <target>**: Show only open ports.
- **nmap --packet-trace <target>**: Show raw packets sent and received.
- **nmap --resume scan.gnmap**: Resume an interrupted scan.

🔧 Miscellaneous

Additional utilities like IPv6 scanning, traceroute, help menu, interface listing, etc.
Useful for diagnostics, scripting, and integration into larger toolchains.

- **nmap -6 <target>**: Scan IPv6 target.
- **nmap -h**: Display help message.
- **nmap -V**: Display version information.
- **nmap --traceroute <target>**: Trace route to the host.
- **nmap --iflist**: List network interfaces and routes on your machine.
- **nmap --privileged**: Confirm that you're running as root.
- **nmap --unprivileged**: Treat Nmap as if run without privileges.