The Ultimate Nmap Cheat Sheet

Version 1.0

Prepared by
Mizanur Rahman Pranto
LinkedIn | Email

Table of Contents

General & Miscellaneous

Command	What it does	Why use it
nmap -h	Print Nmap help/usage summary.	Quick reference for options and syntax when you forget them.
nmap -6 2001:db8::1	Scan an IPv6 host/address.	Target uses IPv6 (not IPv4); required to reach IPv6-only systems.
sudo nmap -A 10.0.0.5	Enable OS detection, version detection, default NSE scripts, and traceroute.	Fast, all-in-one reconnaissance to learn services, versions, OS, and network path.
nmap -V	Print Nmap version information.	Confirm Nmap version for compatibility or debugging.
nmap --datadir /home/user/nmap-data 192.168.1.10	Use a custom Nmap data directory (scripts, signatures, etc.).	Run scans with custom scripts/signatures or alternate data files.
sudo nmap --send-eth -sS 192.168.1.0/24	Use raw Ethernet frames + TCP SYN scan across the subnet.	Needed on networks/hosts that require L2 sending or when IP-level sending is blocked.
nmap --privileged 10.0.0.1	Tell Nmap you are fully privileged (assume raw-socket capability).	Forces Nmap to use raw sockets and faster probing techniques.
nmap --unprivileged 10.0.0.1	Tell Nmap you lack raw-socket privileges.	Useful when running in restricted environments — Nmap adapts scan behavior accordingly.

Target Specification & Host Discovery

Command	What it does	Why use it
nmap -iL targets.txt	Read targets from targets.txt.	Scan many hosts from a file — automation-friendly.
nmap -iR 50	Scan 50 random hosts.	Discovery/research when you want random targets (use responsibly).
nmap --exclude 192.168.1.10,192.168.1.20 192.168.1.0/24	Exclude specified hosts from the scan.	Omit known sensitive or out-of-scope addresses.
nmap --excludefile exclude.txt 192.168.0.0/16	Exclude hosts listed in exclude.txt.	Manage large exclusion lists easily.
nmap -sL 10.0.0.0/24	List-scan — show targets/DNS names without sending probes.	Verify target list or DNS names without generating network traffic.
nmap -sn 192.168.1.0/24	Ping-scan (host discovery only, no port scan).	Quickly identify live hosts before deeper scanning.
nmap -Pn 10.0.0.1	Skip host discovery; treat hosts as up.	Use when ICMP/ping is blocked but you still want to scan ports.
nmap -PS22,80 10.10.10.0/24	TCP SYN discovery to ports 22 and 80.	Find hosts that respond to SYN on common ports when ICMP is filtered.
nmap -PA3389,443 10.10.10.0/24	TCP ACK discovery to ports 3389 and 443.	Detect hosts behind firewalls where ACK responses reveal presence.
nmap -PU53,123 10.10.10.0/24	UDP discovery to ports 53 and 123.	Discover hosts that respond only to UDP probes (DNS/NTP).
nmap -PY 10.0.0.0/24	SCTP discovery probes.	Detect SCTP-capable hosts/services (carrier/telecom equipment).
nmap -PE 10.0.0.0/24	ICMP echo request discovery (classic ping).	Use when ICMP echo is allowed — basic host discovery.
nmap -PP 10.0.0.0/24	ICMP timestamp request discovery.	Alternate ICMP method when echo is filtered.
nmap -PM 10.0.0.0/24	ICMP netmask request discovery.	Another ICMP variant to bypass simple filters.
nmap -PO 1,2,3 10.0.0.0/24	IP-protocol ping for protocols 1–3.	Check for hosts responding to specific IP-level protocols.

LinkedIn | Email

nmap --traceroute 192.0.2.1	Run traceroute to the target host.	Map network path and identify intermediate devices.
nmap -n 192.168.1.0/24	Never do DNS resolution.	Speed up scans and avoid DNS queries/noise.
nmap -R example.com	Always attempt DNS resolution.	Resolve names when you require hostname mapping despite delay/noise.
nmap --dns-servers 8.8.8.8,1.1.1.1 example.com	Use specific DNS servers for resolution.	Bypass local resolver or test against public DNS servers.
nmap --system-dns example.com	Use the OS resolver for DNS.	Rely on local OS DNS logic / search domains.

Scan Techniques

Command	What it does	Why use it
sudo nmap -sS target	TCP SYN (stealth) scan — sends SYN, waits for SYN/ACK, then resets.	Fast and stealthier on many systems because it doesn't complete the TCP handshake.
nmap -sT target	TCP Connect() scan — uses the OS connect() syscall to open full TCP connections.	Use when raw sockets aren’t available (unprivileged environments).
nmap -sA target	TCP ACK scan.	Determine firewall rules and whether ports are filtered (useful for mapping stateful firewall behavior).
nmap -sW target	TCP Window scan.	Subtle technique to infer open/closed ports based on TCP window-size behavior in replies.
nmap -sM target	Maimon scan.	Corner-case scan probing specific stack behaviors — useful during research/evading naive filters.
sudo nmap -sU target	UDP scan.	Find UDP services (DNS, SNMP, etc.); typically slower, noisier, and may require retries.
sudo nmap -sN target	TCP Null scan (no TCP flags set).	Evasive method to detect responses on some OS stacks; can bypass naive filters.

LinkedIn | Email

sudo nmap -sF target	TCP FIN scan.	Send FIN to elicit different responses; can bypass some simple filters and reveal closed ports.
sudo nmap -sX target	TCP Xmas scan (FIN+PSH+URG flags).	Another evasive technique to classify port states on certain stacks.
sudo nmap -sO target	IP protocol scan.	Discover which IP protocols (ICMP, IGMP, GRE, etc.) a host supports.
sudo nmap -sI zombie.example.com:80 target	Idle (zombie) scan using zombie.example.com:80.	Spoofed scan that hides your IP by using a side-channel from a predictable “zombie” host.
sudo nmap -sY target	SCTP INIT scan.	Detect SCTP services on hosts (used in telecom/carrier equipment).
sudo nmap -sZ target	SCTP COOKIE-ECHO scan.	Alternative SCTP scanning technique to find SCTP endpoints.
nmap -b ftp.relay.example.com target	FTP bounce scan via ftp.relay.example.com.	Historical technique to scan third-party hosts through an FTP server (rarely works today).
sudo nmap --scanflags SYN,FIN,PSH target	Send custom TCP flags in probes.	Craft custom probes to research odd TCP stack or firewall behaviors.

Port Specification & Scan Order

Command	What it does	Why use it
nmap -p 22,80,443 target	Scan only ports 22, 80, and 443.	Focus on likely services (SSH, HTTP, HTTPS) and save time.
nmap -p 1-1024 target	Scan ports 1 through 1024.	Cover well-known / privileged ports where common services run.
nmap --exclude-ports 25,110 target	Skip ports 25 and 110 during the scan.	Avoid noisy/email servers or exclude services that are out-of-scope.
nmap -F target	Fast scan using a limited set of common ports.	Quick check to discover likely services with minimal time.
nmap -r -p 1-1000 target	Scan ports 1–1000 in sequential order (no randomization).	Preserve scan order (useful when IDS/defenses react differently to randomized scans).
nmap --top-ports 100 target	Scan the 100 most commonly used ports.	Efficiently find likely services across many hosts.
nmap --port-ratio 0.01 target	Scan ports that are more common than the given ratio threshold.	Target ports that are statistically more likely to be open, reducing noise/time.

Service/Version & OS Detection

Command	What it does	Why use it
nmap -sV target	Service/version detection.	Identify application types and versions for vulnerability mapping.
nmap --version-intensity 2 -sV target	Version detection with intensity level 2.	Balance speed vs accuracy by limiting probes.
nmap --version-light -sV target	Light version scan.	Faster, less intrusive version checks.
nmap --version-all -sV target	Try all version probes.	Maximize chance to identify obscure services.
nmap --version-trace -sV target	Show detailed version-scan activity.	Debug why a probe succeeded or failed.
sudo nmap -O target	OS detection (fingerprinting).	Fingerprint target OS to guide follow-up testing or tooling.
sudo nmap --osscan-limit 10.0.0.0/24	Limit OS detection to promising hosts.	Save time by OS-scanning only likely targets.
sudo nmap --osscan-guess -O target	Aggressive OS guessing when exact match absent.	Get a probable OS when an exact fingerprint isn't found.

LinkedIn | Email

Script Scan (NSE)

Command	What it does	Why use it
nmap -sC target	Run the default set of NSE scripts.	Quick baseline checks for common misconfigurations and known low-hanging vulnerabilities.
nmap --script "http-*,auth" target	Run NSE scripts matching the http-* and auth categories.	Focused web/auth checks without running unrelated scripts.
nmap --script /path/to/script.nse target	Run a specific local or custom NSE script.	Test a newly written or local script against a target.
nmap --script-args user=admin,pass=1234 --script http-brute target	Pass key/value arguments to a script (example: credentials).	Supply credentials or options required by some scripts (interactive & automated testing).
nmap --script-args-file script-args.txt --script http-brute target	Read script arguments from a file.	Keep secrets out of shell history and make automation cleaner.
nmap --script-help http-headers	Show help and available arguments for the http-headers script.	Understand script options, required args, and expected outputs before running.
nmap --script-updatedb	Update the local NSE script database/cache.	Refresh script metadata after adding/removing scripts so Nmap recognizes changes.
nmap --script-trace --script http-some-script target	Enable detailed tracing of script I/O for the specified script.	Debug script data exchanges and behavior to diagnose failures or unexpected outputs.

Timing & Performance

Command	What it does	Why use it
nmap -T4 target	Use timing template 4 (faster, more aggressive).	Speed up scans on stable/reliable networks where higher aggression is safe.
nmap --min-rate 100 --max-rate 500 -p 1-65535 target	Set minimum and maximum probe rate while scanning all ports.	Throttle scanning speed to avoid flooding networks or getting blocked.
nmap --min-hostgroup 16 --max-hostgroup 64 192.168.0.0/16	Control how many hosts are grouped for parallel scanning.	Tune parallelism for large network scans to balance speed and network/host load.
nmap --min-parallelism 10 --max-parallelism 50 target	Set min/max simultaneous probes across targets.	Control concurrency to improve reliability on sensitive or slow networks.
nmap --initial-rtt-timeout 100ms --max-rtt-timeout 2s target	Configure RTT timeouts (initial and maximum).	Adapt to slow or fast networks and reduce false timeouts.
nmap --max-retries 2 target	Limit number of retransmissions per probe.	Reduce time spent retrying on unreliable networks (faster scans with risk of missed ports).
nmap --host-timeout 5m target	Abort scanning a host after 5 minutes.	Prevent scans from hanging indefinitely on very slow or unresponsive hosts.
nmap --scan-delay 50ms target	Add fixed delay between probes.	Slow down scans to be stealthier or to reduce load on target/network.
nmap --max-scan-delay 200ms target	Cap the maximum inter-probe backoff delay.	Prevent exponential backoff from making scans extremely slow in flaky networks.

Firewall/IDS Evasion & Spoofing (use only with permission)

Command	What it does	Why use it
sudo nmap -f target	Fragment packets into smaller IP fragments.	Attempt to evade simple IDS/IPS that do not reassemble fragments.
sudo nmap --mtu 24 target	Set explicit MTU (forces fragmentation).	Control fragment size for evasion or special routing scenarios.
sudo nmap -D decoy1,decoy2,ME target	Use decoy IPs along with your scan.	Obfuscate the true scanner IP in target logs (has legal/ethical implications).
sudo nmap -S 1.2.3.4 target	Spoof the source IP address.	Test target behavior for spoofed traffic (requires permission and routing control).
sudo nmap --spoof-mac 00:11:22:33:44:55 target	Spoof the MAC address to an explicit value.	Match an allowed vendor MAC or bypass MAC-based filtering.
sudo nmap --spoof-mac 0:vendor target	Spoof MAC using a vendor prefix.	Emulate a device from a specific vendor.
nmap -g 53 target	Use source port 53 for outgoing probes.	Exploit permissive firewall rules that allow DNS-source traffic.
nmap --proxies http://proxy:8080,socks4://proxy2:1080 target	Route scans through listed proxies.	Route scan via proxies for research or to test proxy behavior.
sudo nmap --data 0x414141 --data-length 64 target	Append raw hex data plus padding to probes.	Investigate how services handle unusual payloads or try to bypass simple filters.
sudo nmap --data-string "HELLO" target	Append ASCII string payload to probe packets.	Test protocol handlers that echo or expect certain payloads.
sudo nmap --ip-options "RR,LS" target	Include IP options (e.g., Record Route, Loose Source).	Probe how routers/hosts handle unusual IP header options.
sudo nmap --ttl 5 target	Set IP TTL (time-to-live) for outgoing packets.	Manipulate packet lifetime to influence path or avoid local capture.
sudo nmap -e eth0 target	Use specified network interface (eth0).	Choose interface when multiple NICs/VLANs exist or for targeted testing.

LinkedIn | Email

sudo nmap --badsum target	Send packets with incorrect checksums.	Test TCP/IP stack robustness or detect middleboxes that drop malformed checksums.

Safety / legality note: many of these options are evasive and can be illegal or disruptive on networks you don't own. Use them only with explicit authorization and within your scope..

Output & Debugging

Command	What it does	Why use it
nmap -oN output.txt target	Normal (human-readable) output saved to output.txt.	Save readable results for later review.
nmap -oX output.xml target	XML formatted output.	Structured format for parsing or integrating with other tools.
nmap -oG grepable.txt target	Grepable output format.	Quickly filter results using grep/awk.
nmap -oS scriptkiddie.txt target	"Script-kiddie" output format.	Historical / novelty format; rarely used today.
nmap -oA scanbase 10.0.0.0/24	Save normal, XML, and grepable outputs with basename scanbase.	Store scan outputs in multiple formats for different tools/uses.
nmap -v target	Increase verbosity level (one v).	Show more progress and basic details.
nmap -vv target	Extra verbosity (two v).	More detail about Nmap actions and progress.
nmap -d target	Enable debug output (level 1).	Troubleshoot scanning issues or Nmap behavior.
nmap -dd target	Very high debug output (level 2).	Deep debugging with lots of internal info.
nmap --append-output -oN out.txt target	Append results to existing out.txt.	Keep cumulative logs across multiple runs.
nmap --resume scan-results.xml	Resume an aborted scan from saved results.	Avoid re-scanning completed work; save time.
nmap --reason target	Show reasons Nmap used to classify port states.	Understand why a port was marked open/closed/filtered.

LinkedIn | Email

nmap --open target	Show only open (or possibly open) ports in output.	Focus on actionable findings.
nmap --packet-trace target	Print all packets sent and received.	Low-level troubleshooting of probes and replies.
nmap --iflist	Print local interfaces, routing, and other network info.	Check which NIC/routing Nmap will use before scanning.
nmap --noninteractive target	Disable interactive prompts.	Safe for automated scripts or CI environments.
nmap --stylesheet /path/to/style.xsl -oX out.xml target	Add a custom XSL stylesheet reference to XML output.	Produce prettier HTML from Nmap XML using a custom stylesheet.
nmap --webxml -oX out.xml target	Reference the official Nmap.org stylesheet in XML.	Portable XML that references an official stylesheet for viewing.
nmap --no-stylesheet -oX out.xml target	Produce XML without any stylesheet reference.	Avoid adding external references to XML output.