

Forum:[Hack Forums](#)

Thread: [Nmap Ultimate Cheat Sheet \(2025\)](#)

??????????? - July 14, 2025, 1:24 am

A concise, up-to-date reference covering all key Nmap commands and options, from target selection and scan types to scripting, evasion techniques, and output formats—for efficient network reconnaissance in 2025.

[Tool Download Link](#)

1. Target Specification & Usage

Overview: Define precisely which hosts to scan. Nmap supports single IPs, ranges, CIDR notation, domain names, file-based lists, and random hosts.

Single host

Usage: Code `nmap 192.168.1.1`

Scans a lone host. Useful for quick checks or validating a specific server.

Multiple hosts

Usage: Code `nmap 192.168.1.1 192.168.2.1`

Scan two or more non-contiguous IPs in one command.

IP range

Usage: Code `nmap 192.168.1.1-254`

Scans every address in the specified range. Handy for /24 networks.

CIDR notation

Usage: Code `nmap 192.168.1.0/24`

Equivalent to scanning 1–254, but clearer. Also works for larger networks (e.g., /16).

DNS name

Usage: Code `nmap scanme.nmap.org`

Resolves and scans the IP behind the domain. Good for external recon.

Input from file

Usage: Code `nmap -iL targets.txt`

Reads a newline-separated list of targets from targets.txt. Streamlines repeated scans.

Random hosts

Usage: Code `nmap -iR 100`

Picks 100 random IPv4 targets from the entire internet. Use Code `-Pn` to skip unreachable hosts.

Exclude hosts

Usage: Code `nmap 192.168.1.0/24 --exclude 192.168.1.5,scanme.nmap.org`

Omit specific hosts or subnets from a broader scan.

2. Scan Techniques & Descriptions

Overview: Choose your port-scan method based on stealth, speed, and privilege.

SYN scan (-sS)

Usage: Code `nmap -sS target`

A "half-open" scan: sends SYN, awaits SYN/ACK, then resets. Fast and stealthy; default with root.

TCP connect (-sT)

Usage: Code `nmap -sT target`

Uses the OS's connect syscall. No privileges needed, but easier to detect.

UDP scan (-sU)

Usage: Code `nmap -sU target`

Sends empty UDP packets. Slower—useful for DNS, SNMP.

ACK scan (-sA)

Usage: Code `nmap -sA target`

Determines firewall rules by sending ACKs. Doesn't show open ports.

Window scan (-sW)

Usage: Code `nmap -sW target`

Variation of ACK scan using TCP window size to distinguish filtered vs unfiltered.

Maimon scan (-sM)

Usage: Code `nmap -sM target`

Sends FIN/ACK packets. Works against some non-standard firewalls.

Idle (zombie) scan (-sI)

Usage: Code `nmap -sI zombie_ip target`

Uses a "zombie" host's IPID sequence for completely blind scanning.

3. Host Discovery Options

Overview: Quickly identify live hosts before port scanning.
List scan only (-sL)

Usage: Code `nmap -sL 192.168.1.0/24`
No probes sent; lists targets.

Ping scan only (-sn)

Usage: Code `nmap -sn 10.0.0.0/24`
ICMP/ARP/TCP/UDP ping to find live hosts without port scan.

No ping (-Pn)

Usage: Code `nmap -Pn target`
Skip host discovery; treats all hosts as up.

TCP ACK ping (-PA)

Usage: Code `nmap -PA22,80 target`
Send ACK to specified ports to discover hosts.

UDP ping (-PU)

Usage: Code `nmap -PU53 target`
Send UDP to specified port (default 40125).

ARP ping (-PR)

Usage: Code `nmap -PR 192.168.1.0/24`
ARP discovery on local LAN—fast and reliable.

Disable DNS resolution (-n)

Usage: Code `nmap -n target`
Skip reverse DNS to speed up scans.

4. Port Specification Techniques

Overview: Precisely define which ports to probe.
Single port (-p)

Usage: Code `nmap -p 22 target`
Scan only port 22.

Port range (-p start-end)

Usage: Code `nmap -p 1-1000 target`
Scan ports 1 through 1000.

Mixed protocols (-p U:53,T:80)

Usage: Code `nmap -p U:53,T:22,80 target`
Combine UDP and TCP in one scan.

All ports (-p-)

Usage: Code `nmap -p- target`
Scan ports 1–65535.

Fast scan (-F)

Usage: Code `nmap -F target`
Scan top 100 common ports.

Top X ports (--top-ports)

Usage: Code `nmap --top-ports 200 target`
Scan top N ports.

Service names (-p name)

Usage: Code `nmap -p http,ssh target`
Use service names from `/etc/services`.

5. Service & Version Detection

Overview: Identify services and versions.
Version probe (-sV)

Usage: Code `nmap -sV target`
Probe open ports for service/version.

Intensity (--version-intensity)

Usage: Code `nmap -sV --version-intensity 8 target`
Adjust probe aggressiveness (0–9).

Light scan (--version-light)

Usage: Code `nmap --version-light target`
Fewer probes—faster but less accurate.

All probes (--version-all)

Usage: Code `nmap --version-all target`
Use all probes—slowest, most thorough.

Aggressive (-A)

Usage: Code `nmap -A target`

Shortcut for -sV, -O, default scripts, and traceroute.

6. OS Detection & Fingerprinting

Overview: Fingerprint OS via TCP/IP stack.
OS scan (-O)

Usage: Code `nmap -O target`
Probe to guess OS.

Limit (--osscan-limit)

Usage: Code `nmap --osscan-limit target`
Only if open+closed port found.

Guess (--osscan-guess)

Usage: Code `nmap --osscan-guess target`
Return multiple OS matches.

Max tries (--max-os-tries)

Usage: Code `nmap --max-os-tries 1 target`
Limit attempts for speed.

7. Timing & Performance

Overview: Balance speed vs stealth.
Templates (-T0 to -T5)

Usage: Code `-T0` (Paranoid) to Code `-T5` (Insane).

Delays & rates

Usage: Code `--scan-delay 50ms --max-retries 2 --min-rate 100 --max-parallelism 10`
Control timing, retries, and parallelism.

Host timeout

Usage: Code `--host-timeout 30s`
Abort slow hosts.

8. NSE Scripting Engine

Overview: Automate with Nmap scripts.
Default (-sC)

Usage: Code nmap -sC target
Run safe default scripts.

Specific (--script)

Usage: Code nmap --script=http-title target
Run named script.

Wildcard

Usage: Code nmap --script http* target
Scripts matching pattern.

Multiple

Usage: Code nmap --script dns-brute,http-title target
Comma-separated list.

Exclude intrusive

Usage: Code nmap --script "default and not intrusive" target
Skip potentially harmful scripts.

Arguments

Usage: Code nmap --script-args snmpcommunity=public,threads=10 target
Pass parameters.

9. Evasion & Spoofing

Overview: Bypass firewalls and IDS.
Fragmentation (-f)

Usage: Code nmap -f target
Split packets.

Decoys (-D)

Usage: Code nmap -D 10.0.0.1,ME,10.0.0.2 target
Mix real and decoy IPs.

Spoofing (-S)

Usage: Code nmap -S bogus.ip.addr -e eth0 target
Spoof source IP.

Padding (--data-length)

Usage: Code nmap --data-length 50 target
Append junk data.

Proxies (--proxies)

Usage: Code `nmap --proxies http://proxy:8080,socks4://proxy2:1080 target`
Route through proxies.

Source port (-g)

Usage: Code `nmap -g 53 target`
Use specific source port.

10. Output & Reporting

Overview: Save and analyze results.
Normal (-oN)

Usage: Code `nmap -oN out.txt target`
Human-readable log.

XML (-oX)

Usage: Code `nmap -oX out.xml target`
XML output.

Grepable (-oG)

Usage: Code `nmap -oG out.gnmap target`
Easy parsing.

All (-oA)

Usage: Code `nmap -oA report target`
Produce all formats.

Append (--append-output)

Continue in same file.

Resume (--resume)

Usage: Code `nmap --resume report.nmap`
Pick up scan.

Verbose & debug

Usage: Code `-v, -vv, -d, -dd`
More detail.

Show reasons (--reason)

Usage: Code `--reason`
Explain port states.

Only open (--open)

Usage: Code --open
Filter to open ports.

Interface list (--iflist)

Usage: Code --iflist
List local interfaces.

Compare (ndiff)

Usage: Code ndiff old.xml new.xml
Highlight scan differences.

HTML report

Usage: Code xsltproc out.xml -o out.html
Convert XML to HTML.

Practical Nmap Usage Guide

1. Install Nmap

Linux (Debian/Ubuntu): Code sudo apt update && sudo apt install nmap

macOS (Homebrew): Code brew install nmap

Windows: Download the installer at nmap.org/download.html

2. Define Your Target

Single IP: Code nmap 10.0.0.5

Subnet (CIDR): Code nmap 10.0.0.0/24

IP Range: Code nmap 10.0.0.1-50

Multiple hosts: Code nmap 10.0.0.5 192.168.1.10 scanme.nmap.org

3. Quick Ping Sweep

Use a "ping" scan to list live hosts without port scans:

Code nmap -sn 10.0.0.0/24

4. Basic Port Scan

Discover open TCP ports stealthily:

Code nmap -sS 10.0.0.5

5. Service & Version Detection

Probe banners to identify services and versions:

Code nmap -sS -sV 10.0.0.5

6. Operating System Fingerprinting

Guess the target's OS from TCP/IP behavior:

Code nmap -O 10.0.0.5

7. Aggressive Scan (All-in-One)

Combine OS, version, scripts & traceroute:

Code `nmap -A 10.0.0.5`

8. NSE Scripting Examples

Run safe default scripts: Code `nmap -sC 10.0.0.5`

Run one script (http-title): Code `nmap --script=http-title 10.0.0.5`

Run vuln category: Code `nmap --script=vuln 10.0.0.5`

Pass args to a script:

Code `nmap --script=http-brute --script-args userdb=users.txt,passdb=passes.txt 10.0.0.5`

9. Timing & Stealth Controls

Slower & stealthy (Paranoid): Code `nmap -sS -T1 10.0.0.5`

Faster & obvious (Aggressive): Code `nmap -sS -T4 10.0.0.5`

Skip discovery (no ping): Code `nmap -Pn 10.0.0.5`

10. Save & Export Results

Normal text: Code `nmap -oN myscan.txt 10.0.0.5`

XML format: Code `nmap -oX myscan.xml 10.0.0.5`

Grepable output: Code `nmap -oG myscan.gnmap 10.0.0.5`

All formats at once: Code `nmap -oA report 10.0.0.5`

Red Team Nmap Workflow (Authorized Engagement Strictly)

1. Initial Recon & Network Mapping

Stealthy Ping Sweep

Code `nmap -sn -T2 10.10.0.0/24`

Identify live hosts without noisy port scans.

Topology & OS Fingerprinting

Code `nmap -O --osscan-guess 10.10.0.5`

Gather OS details to tailor your exploit selection.

2. Service Enumeration

SYN Scan of Common Ports

Code `nmap -sS --top-ports 1000 10.10.0.5`

Fast discovery of the most likely open services.

Full TCP/UDP Sweep

Code `nmap -sS -sU -p- 10.10.0.5`

Find oddball UDP services and high-numbered TCP ports.

Version & Script Enumeration

Code `nmap -sV --version-intensity 9 --script=banner,default,vuln 10.10.0.5`

Fingerprint versions and run vulnerability checks.

3. Credential & Brute-Force Checks

SMB Login Brute-Force

Code `nmap --script smb-brute --script-args userdb=users.txt,passdb=passes.txt 10.10.0.5`
Test for weak Windows credentials.

HTTP Form Brute-Force

Code `nmap --script http-form-brute --script-args userdb=users.txt,passdb=passes.txt 10.10.0.5`
Automate login attempts against web applications.

4. Evasion & Stealth Techniques

Fragmentation & Slow Timing

Code `nmap -f -T1 --scan-delay 500ms 10.10.0.5`
Break packets and slow probes to slip past IDS.

Proxy Chains

Code `proxychains nmap -sT 10.10.0.5`
Route scans through TOR or SOCKS proxies.

5. Pivoting & Internal Recon

Scan Through a Tunnel Interface

Code `nmap -Pn -sS -e tun0 192.168.1.0/24`
Use a compromised host's tunnel/VPN interface.

Service Tunnel with Ncat

Code # On compromised host:
`ncat -l -p 4444 --sh-exec "nmap -sS -p22,80 10.10.1.0/24"`

[h1]On your machine:[/h1]

`ncat victim-ip 4444`

Leverage Ncat to run Nmap from inside the target network.

6. Results & Exploitation Integration

Export to XML

Code `nmap -oX redteam-scan.xml 10.10.0.0/24`
Save structured output for tool ingestion.

Import into Metasploit

Code # In msfconsole:

`db_import redteam-scan.xml`

Automatically populate the database with discovered hosts/services.

Graph with BloodHound/Cobalt Strike

Use the XML/CSV data to map privileges and plan lateral movement.

? Disclaimer: Ensure you have explicit, written authorization before running any scans, unauthorized testing is illegal. This workflow is provided strictly for educational and training purposes.

Additional Red Team Nmap Suggestions

Logging & Verbosity

Use ``-v``, ``--reason`` or ``-d`` to capture why ports are marked open/filtered and to aid debugging.

Impact Assessment

Throttle with ``--min-rate``/``--max-rate`` or schedule scans during agreed "test windows" to avoid service disruption.

IPv6 Scanning

Include `-6`` to discover hosts and services on IPv6 networks when applicable.

Certificate Inspection

Chain NSE scripts like `--script ssl-cert`` for HTTPS services to extract certificate details.

Post-Scan Cleanup

Terminate any proxy/Ncat listeners and remove temporary files or logs from pivot hosts.

Report Generation

Convert XML output to HTML with `xsltproc``, or to CSV/PDF via tools like `nmaptocsv`` -> Excel -> PDF for deliverables.

Integration Hooks

Automate notifications (e.g., Slack, email, webhooks) when high-severity findings appear via custom scripts.

Scan Documentation

Record target ranges, timestamps, and all Nmap options in your engagement notes or ticketing system for audit and reproducibility.

HerrWinston - July 14, 2025, 2:32 am

thanks man, nice thread, i will take a closer look tonight, much information well presented! ?

???????????? - October 18, 2025, 2:08 pm

(Jul 14, 2025 02:32 AM)HerrWinston Wrote: [\[CITE\]](#) thanks man, nice thread, i will take a closer look tonight, much information well presented! ?

Did you check and had a closer look into this? Make sure to provide any suggestions if you have any.

Stanley - September 12, 2026, 6:21 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley