Nmap Commands

https://www.stationx.net/nmap-cheat-sheet/ : NMAP Commands
https://www.geeksforgeeks.org/nmap-cheat-sheet/ : NMAP Commands

Command	Short Description
nmap <IP>	Basic port scan to check open ports.
nmap -sP <IP>/24	Ping scan across subnet for live hosts.
nmap -p <port> <IP>	Scan specific port(s) on target.
nmap -p- <IP>	Scan all 65535 TCP ports.
nmap -sS <IP>	Stealthy SYN scan using half-open connections.
nmap -sT <IP>	Full TCP connect scan using system stack.
nmap -sU <IP>	Scan for open UDP ports.
nmap -sN <IP>	NULL scan to bypass firewalls.
nmap -sF <IP>	FIN scan to detect open ports.
nmap -sX <IP>	Xmas scan using FIN, PSH, URG flags.
nmap -A <IP>	Aggressive scan: OS, version, scripts, traceroute.
nmap -O <IP>	Attempt to detect operating system.
nmap -sV <IP>	Service version detection for open ports.
nmap -Pn <IP>	Skip ping, directly scan target.
nmap -T4 <IP>	Faster scan timing for stable networks.
nmap -T0 <IP>	Slow scan for stealth and IDS evasion.
nmap -F <IP>	Fast scan, top 100 ports only.
nmap -v <IP>	Verbose mode to show detailed progress.
nmap -vv <IP>	Extra verbose output per-port.
nmap -iL targets.txt	Scan multiple IPs from file.
nmap -oN output.txt	Save output in human-readable format.
nmap -oX output.xml	Save output in XML format.
nmap --script=<script> <IP>	Run specific NSE script on target.

Command	Short Description
nmap --script vuln <IP>	**Run vulnerability detection scripts.**
nmap --top-ports 100 <IP>	**Scan top 100 commonly used ports.**
nmap --reason <IP>	**Show reasons behind port state decisions.**
nmap --open <IP>	**Show only open ports in scan output.**
nmap -6 <IP>	**Scan using IPv6 addressing.**
nmap -n <IP>	**Disable DNS resolution for faster scanning.**
nmap --traceroute <IP>	**Show network path to the target host.**
nmap -sC <IP>	**Run default detection scripts.**

Detailed explanation

✅ **nmap <IP>**

- nmap is the command-line utility used for scanning.
- <IP> represents the target host or IP address you want to scan.
- Without additional options, this runs a **default scan**, which includes host discovery and scanning the **top 1000 TCP ports**.
- It performs a ping to check if the host is up and scans open ports using a TCP connect.
- This is the simplest and most commonly used scan.

✅ **nmap -sP <IP>/24** ***(Note: -sP is deprecated; modern flag is -sn)***

- -sP tells Nmap to perform a **ping scan**, which identifies live hosts in a network without scanning ports.
- <IP>/24 defines the subnet range (e.g., 192.168.1.0/24 scans all 256 IPs in that subnet).
- Nmap sends ICMP echo requests and ARP or TCP pings to check if hosts are alive.
- This is useful for quickly mapping active systems on a network.
- Modern Nmap uses -sn instead of -sP.

✅ **nmap -p <port> <IP>**

- -p specifies which port(s) to scan.
- You can input a single port (e.g., -p 22) or a list/range (e.g., -p 22,80,443 or -p 1-1000).
- <IP> is the target system.
- This focuses the scan on specified ports rather than all 1000 default ports.
- It's useful when you know which services may be running or want to reduce scan time.

✅ **nmap -p- <IP>**

- -p- instructs Nmap to scan **all 65535 TCP ports**.
- <IP> is the target host.
- This is useful to discover services running on non-standard ports.

- It’s slower than scanning only the top ports, but more thorough.
- Often combined with service detection or stealth scanning.

✅ **nmap -sS <IP>**

- -sS performs a **SYN scan**, also called a **stealth scan**.
- It sends only a TCP SYN packet and waits for a SYN-ACK (open) or RST (closed).
- The TCP handshake is never completed, making it less likely to be logged by the system.
- <IP> is the target being scanned.
- It is one of the fastest and most commonly used Nmap scan types.

✅ **nmap -sT <IP>**

- -sT is a **TCP Connect scan**.
- It completes the entire 3-way TCP handshake (SYN, SYN-ACK, ACK).
- This scan is used when SYN scan isn’t possible (e.g., not run as root/admin).
- <IP> is the address of the target system.
- It is more detectable but works reliably across most environments.

✅ **nmap -sU <IP>**

- -sU enables **UDP scanning**.
- UDP scans are useful for detecting services like DNS, SNMP, and TFTP.
- <IP> is the target host to be scanned.
- UDP scanning is **slower** and often inconclusive without version detection.
- It is recommended to combine with -sS for full TCP+UDP visibility.

✅ **nmap -sN <IP>**

- -sN executes a **NULL scan**, sending packets with **no TCP flags set**.
- It attempts to evade firewalls and intrusion detection systems.
- Some operating systems respond differently to such packets, helping identify port states.
- <IP> is the destination host.
- This technique works best on older UNIX-like systems.

✅ **nmap -sF <IP>**

- -sF performs a **FIN scan**, sending TCP packets with only the FIN flag set.
- It attempts to bypass firewalls that do not properly inspect FIN packets.
- <IP> is the system being scanned.
- Responses (or lack thereof) are interpreted to identify open or closed ports.
- It is stealthy but not universally reliable.

✅ **nmap -sX <IP>**

- -sX initiates a **Xmas scan**, setting the FIN, PSH, and URG TCP flags.
- Like -sF and -sN, it’s a **stealth scan** attempting to bypass packet filters.
- <IP> is the target to be analyzed.
- This scan mimics a malformed packet that might slip through simple firewalls.
- May not work against modern operating systems with hardened stacks

✅ **nmap -A <IP>**

- -A enables **aggressive mode**, combining multiple features.
- It includes **OS detection**, **version detection**, **script scanning**, and **traceroute**.
- <IP> is the target host to scan deeply.
- It provides a lot of information but is noisier and more intrusive.
- Often used during full assessments or deep analysis of a system.

✅ **nmap -O <IP>**

- -O triggers **OS fingerprinting**.
- It examines TCP/IP stack responses to guess the target's operating system.
- <IP> is the system to be fingerprinted.
- Accuracy depends on open ports and firewall settings.
- May fail or produce unreliable results on filtered/modern systems.

✅ **nmap -sV <IP>**

- -sV enables **service/version detection** on open ports.
- It sends probes to ports and analyzes responses to identify applications.
- <IP> is the target for service analysis.
- Results include version numbers and sometimes OS type.
- Good for identifying vulnerable software versions.

✅ **nmap -Pn <IP>**

- -Pn disables host discovery (ping).
- It assumes the host is up and proceeds with scanning.
- <IP> is the address to be scanned.
- Useful when ICMP is blocked or host discovery fails.
- Can increase false positives if host is truly offline.

✅ **nmap -T4 <IP>**

- -T4 sets the scan timing template to "Aggressive".
- It reduces delays between packets and speeds up the scan.
- <IP> is the target to be scanned quickly.
- Ideal for scanning fast and stable networks (e.g., LANs).
- Can be detected more easily by IDS/IPS systems.

✅ **nmap -T0 <IP>**

- -T0 sets the scan to **"Paranoid"** mode (ultra-slow).
- Delays are maximized to avoid detection by intrusion detection systems.
- <IP> is the system to be scanned slowly and stealthily.
- Useful for red teaming or highly monitored networks.
- Significantly increases total scan time.

✅ **nmap -F <IP>**

- -F enables a **fast scan**.
- It scans only the top 100 most common ports.

- <IP> is the host to be quickly assessed.
- Ideal for fast enumeration or wide-range scanning.
- Saves time during early recon phases.

✅ **nmap -v <IP>**

- -v increases **verbosity**.
- You get real-time updates and progress during scanning.
- <IP> is the scan target.
- Shows more scan phases and findings as they happen.
- Good for monitoring during long scans.

✅ **nmap -vv <IP>**

- -vv is **very verbose** output.
- Displays detailed per-port information as Nmap progresses.
- <IP> is the scanned host.
- Helps during debugging or fine-tuning.
- Often used in scripting and automation for log clarity.

✅ **nmap -iL targets.txt**

- -iL tells Nmap to read targets from a file.
- targets.txt is a file with multiple IPs/domains listed line by line.
- Useful for scanning multiple systems in one go.
- Avoids manual input for bulk scans.
- Works well in enterprise or large-scale assessments.

✅ **nmap -oN output.txt**

- -oN outputs scan results in a **normal, human-readable format**.
- output.txt is the file where results are saved.
- Good for reports or quick reference.
- Content is easy to parse manually.
- Suitable for documentation.

✅ **nmap -oX output.xml**

- -oX writes scan results in **XML format**.
- output.xml is the destination file.
- Useful for automation, reporting tools, or dashboards.
- Can be converted to HTML using XSLT.
- Required by some third-party tools for parsing.

✅ **nmap --script=<script> <IP>**

- --script= loads a specific Nmap Scripting Engine (NSE) script.
- <script> can be anything like http-title, ftp-anon, etc.
- <IP> is the host where the script is executed.
- Used for custom tasks like brute-forcing, info gathering.
- Offers modular scanning for various protocols.

✅ **nmap --script vuln <IP>**

- --script vuln runs a category of **vulnerability-detection scripts**.
- These scripts look for known CVEs, misconfigs, and weaknesses.
- <IP> is the scan target.
- Fast way to identify low-hanging security issues.
- Often used for quick vulnerability assessment.

✅ **nmap --top-ports 100 <IP>**

- --top-ports lets you specify how many common ports to scan.
- 100 means Nmap scans the 100 most used ports (based on frequency data).
- <IP> is the destination system.
- Useful for performance tuning and faster coverage.
- Combines speed with effectiveness.

✅ **nmap --reason <IP>**

- --reason forces Nmap to explain **why** it classified a port as open/closed/filtered.
- Shows reasoning like TCP flags received or ICMP responses.
- <IP> is the scan target.
- Good for learning or auditing.
- Increases transparency of scanning logic.

✅ **nmap --open <IP>**

- --open filters output to show **only open ports**.
- Removes clutter from closed/filtered ones.
- <IP> is the scanned host.
- Useful for cleaner reports and faster parsing.
- Does not change scanning behavior, only display.

✅ **nmap -6 <IP>**

- -6 forces Nmap to use **IPv6 scanning**.
- <IP> must be a valid IPv6 address.
- Required in IPv6-only networks.
- Works with other flags like -sS, -sV, etc.
- Same behavior as IPv4 scanning otherwise.

✅ **nmap -n <IP>**

- -n disables DNS resolution.
- <IP> is scanned directly without converting to hostname.
- Speeds up scans when reverse DNS is not needed.
- Avoids leaking queries to external DNS servers.
- Useful for anonymous or high-speed scanning.

✅ **nmap --traceroute <IP>**

- --traceroute maps the **network path** to a host.
- Reveals intermediate routers and hops.
- <IP> is the end target.
- Helps understand network topology and latency.
- Useful for discovering firewalls or chokepoints.

✅ **nmap -sC <IP>**

- -sC runs a set of **default scripts**.
- These scripts check for common issues and service information.
- <IP> is the target host.
- Equivalent to --script=default.
- Great for general service discovery.