Nmap Command with Examples

Nmap is a Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts, and even by network and system administrators. It is used for the following purposes:

- Real-time information of a network
- Detailed information of all the IPs activated on your network
- Number of ports open in a network
- Provide the list of live hosts
- Port, OS and Host scanning

Installing Nmap Command

- sudo apt-get install nmap

Target Specification

- Target specification controls the scope of your scan, so you scan only the systems you intend to test.
- Define exactly which IPs, ranges, or subnets Nmap should scan during your network reconnaissance.

SWITCH	EXAMPLE	DESCRIPTION
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts

-exclude	nmap -exclude 192.168.1.1	Exclude listed hosts

nmap Scan Techniques:

Choose the type of scan to run, from stealthy SYN scans to full TCP and UDP scans.

SWITCH	EXAMPLE	DESCRIPTION
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery:

Identify which hosts are online before running a full scan or when skipping port scans entirely.

SWITCH	EXAMPLE	DESCRIPTION

-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Port Specification:

Target specific ports, ranges, or combinations of TCP and UDP ports for more precise scans.

SWITCH	EXAMPLE	DESCRIPTION
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range

-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
-top-ports	nmap 192.168.1.1 -top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

Service and Version Detection:

Detect which services are running and attempt to identify their software versions and configurations.

SWITCH	EXAMPLE	DESCRIPTION
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port

-sV -version-intensity	nmap 192.168.1.1 -sV -version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV -version-light	nmap 192.168.1.1 -sV -version-light	Enable light mode. Lower possibility of correctness. Faster
-sV -version-all	nmap 192.168.1.1 -sV -version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

OS Detection:

Use TCP/IP fingerprinting to guess the operating system of target hosts.

SWITCH	EXAMPLE	DESCRIPTION
-O	nmap 192.168.1.1 -O	**Remote OS detection** using TCP/IP stack fingerprinting
-O -osscan-limit	nmap 192.168.1.1 -O -osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O -osscan-guess	nmap 192.168.1.1 -O -osscan-guess	Makes Nmap guess more aggressively

-O -max-os-tries	nmap 192.168.1.1 -O -max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Timing and Performance:
Adjust scan speed and stealth based on your target environment and detection risk.

SWITCH	EXAMPLE	DESCRIPTION
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

NSE Scripts:

Enhance your scans with Nmap’s scripting engine for automation and deeper inspection.

SWITCH	EXAMPLE	DESCRIPTION
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe
-script default	nmap 192.168.1.1 -script default	Scan with default NSE scripts. Considered useful for discovery and safe
-script	nmap 192.168.1.1 -script=banner	Scan with a single script. Example banner
-script	nmap 192.168.1.1 -script=http*	Scan with a wildcard. Example http
-script	nmap 192.168.1.1 -script=http,banner	Scan with two scripts. Example http and banner
-script	nmap 192.168.1.1 -script "not intrusive"	Scan default, but remove intrusive scripts
-script-args	nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.1	NSE script with arguments

Firewall / IDS Evasion and Spoofing:
Bypass security measures using packet fragmentation, spoofed IPs, and stealthy scan methods.

SWITCH	EXAMPLE	DESCRIPTION
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
-mtu	nmap 192.168.1.1 -mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number

-proxies	nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
-data-length	nmap -data-length 200 192.168.1.1	Appends random data to sent packets