🔎 What is Nmap?

Nmap (Network Mapper) is a powerful open-source tool for network discovery and security auditing. It can discover hosts, list open ports & services, detect service versions, run lightweight scripts, and try to identify the operating system. Nmap has many options; you'll find the most common ones below.

Command explanations & examples

1 `nmap <ip>`

Scan default top ports and detect what's open.

```
nmap 192.168.1.10
```

Output:

```
22/tcp open ssh
80/tcp open http
```

---

2 `nmap -p20-5000 <ip>`

Scan a **specific port range** (20 to 5000).

```
nmap -p20-5000 192.168.1.10
```

Output:

```
21/tcp open ftp
443/tcp open https
```

---

3 `nmap -p22,32,23,8080 <ip>`

Scan **selected ports** (comma separated).

```
nmap -p22,32,23,8080 192.168.1.10
```

Output:

```
22/tcp open ssh
23/tcp open telnet
8080/tcp open http-proxy
```

---

4 `nmap -sV <ip>`

Version detection. Shows software running on open ports.

```
nmap -sV 192.168.1.10
```

Output:

```
22/tcp open ssh OpenSSH 7.6p1
80/tcp open http Apache 2.4.29
```

---

5 `nmap -sC <ip>`

Run **default scripts** for extra info like vulnerabilities.

```
nmap -sC 192.168.1.10
```

Output:

```
| http-title: Example webpage
| smb-os-discovery: Windows Server detected
```

---

6 `nmap -O <ip>`

Detect Operating System (needs root privileges).

```
sudo nmap -O 192.168.1.10
```

Output:

```
OS details: Linux Kernel 4.x
```

---

7 `nmap` (just typing nmap)

Shows **help menu** and usage instructions.

```
nmap
```

---

8 `nmap -sV <ip> -oN filename`

Save results in **normal text** format.

```
nmap -sV 192.168.1.10 -oN scan.txt
```

Creates:

```
scan.txt
```

---

9 `nmap -sV <ip> -oA myfile`

Save results in **all 3 formats**:

- `.nmap` (normal)
- `.gnmap` (grepable)
- `.xml` (for tools)

```
nmap -sV 192.168.1.10 -oA myscan
```

Creates:

```
myscan.nmap
myscan.gnmap
myscan.xml
```

---

10 `nmap -A <ip>`

Aggressive scan: version detection + OS detection + scripts + traceroute
(Noise + easily detected)

```
nmap -A 192.168.1.10
```

Output:

```
22/tcp ssh OpenSSH 7.6p1
OS: Linux 4.x
Traceroute: 2 hops
```

✓ Quick Summary Table

Command	Purpose
nmap ip	Basic scan
-p20-5000	Scan port range
-p22,32,23,8080	Specific ports
-sV	Version detection
-sC	Default scripts
-O	OS detection
-oN	Save normal output
-oA	Save all formats
-A	Full aggressive scan

---

11 nmap -sn <ip-address>

What: Ping scan only. Discovers which hosts are up without doing port scans.
Example:

```
nmap -sn 192.0.2.0/24
```

Sample output:

```
Nmap scan report for 192.0.2.10
Host is up (0.012s latency).
```

```
Nmap done: 256 IPs (3 hosts up) scanned in 2.45 seconds
```

---

12 nmap -Pn <ip-address>

What: Skip host discovery (treat targets as up). Useful when ICMP or ping is blocked.
Example:

```
nmap -Pn 198.51.100.5
```

Sample output (starts port scan immediately):

```
Nmap scan report for 198.51.100.5
Host is up (0.05s latency).
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

---

13 nmap -v <ip-address>

What: Verbose mode. Shows more progress/detail while the scan runs. Can be combined with other options.
Example:

```
nmap -v 203.0.113.7
```

Sample (verbose lines intermixed):

```
Initiating Ping Scan at 19:00
Scanning 203.0.113.7 [4 ports]
Completed SYN Stealth Scan at 19:00, 0.20s elapsed
```

---

14 nmap --source-mac <mac> -sV <ip-address>

What: Force the Ethernet source MAC address for sent probes and run version detection. Useful in lab tests or when spoofing is required. Requires privileged access and same L2 network.
Example:

```
sudo nmap --source-mac 00:11:22:33:44:55 -sV 192.0.2.10
```

Sample output:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4
```

---

15 ls /usr/share/nmap/scripts | grep http

What: Shell command to list NSE (Nmap Scripting Engine) scripts and filter those with "http" in the name. Good to discover relevant scripts.
Example:

```
ls /usr/share/nmap/scripts | grep http
```

Sample output lines:

```
http-title.nse
http-enum.nse
http-vuln-cve2017-5638.nse
http-robots.txt.nse
```

---

16 nmap --script=ftp-brute.nse <ip-address>

What: Run a single NSE script (ftp-brute) that attempts FTP credential brute force using bundled username/password lists. This is intrusive and noisy. Only run against systems you own or have explicit permission to test.
Example:

```
sudo nmap --script=ftp-brute.nse 198.51.100.20
```

Sample script output:

```
| ftp-brute:
|   Accounts
|     anonymous:anonymous  Login Successful
|     admin:admin          Login Failed
|_  Statistics: Performed 20 guesses in 3s
```