

Scanning-with-Nmap

Nmap Scanning

Nmap (Network Mapper) is a powerful network reconnaissance tool used to discover hosts, open ports, running services, and operating systems on a network.

No scan = no awareness.

Nmap turns the *unknown* into the *known*.

What is Nmap?

Nmap is a **network scanning and mapping tool** that shows:

- Which devices are reachable
- Which ports are open
- What services are running
- How exposed a system is from the outside

Think of scanning like **walking around a building to see which doors and windows are unlocked**.

Why Nmap Is Important

For Security & Administration

- Reveals security weaknesses
- Identifies unnecessary or misconfigured services
- Helps harden systems

- Forms the foundation of security assessments

Why Hackers Use It

- Reconnaissance before an attack
- Discover open ports and services
- Understand the attack surface
- Choose the correct exploit

What Scanning Means

Scanning is:

- Checking which devices exist
- Checking which ports (doors) are open
- Identifying running services
- Observing from the outside only

Nmap Capabilities

- Network mapping
- Host discovery
- Port scanning
- Service detection
- Version detection

- OS detection
- Firewall analysis

5 Goals of Network Scanning

1. Host discovery
2. Open ports
3. Services / protocols
4. Software & versions
5. Operating system detection

Host Discovery (Is the Target Alive?)

Check a single host:

```
nmap -sn 192.168.0.105
```

Scan a local network range:

```
nmap -sn 192.168.0.1-254
```

Scan using CIDR notation:

```
nmap -sn 192.168.0.105/24
```

Flags explained

- `-sn` → Ping scan (skip port scan)

Open Ports & Services

Scan All Ports (1–65535)

```
nmap -p 1-65535 192.168.0.105
```

Verbose output:

```
nmap -p 1-65535 -v 192.168.0.105
```

Scan a limited range:

```
nmap -p 1-100 192.168.0.109
```

Scan specific services:

```
nmap -p ssh,telnet,http 192.168.0.109
```

Scan specific ports:

```
nmap -p 21,22,23,80 -v 192.168.0.109
```

Scan **all ports (fast method)**:

```
nmap -p- 192.168.0.109
```

Aggressive scan (ports + services + OS):

```
sudo nmap -A 192.168.0.109
```

TCP Scan Types

TCP Connect Scan (**-sT**)

- Completes full 3-way handshake
- Easy to detect
- Reliable

```
nmap -sT 192.168.0.109
```

SYN Scan / Half-Open (**-sS**)

- Faster and stealthier
- Does not complete full connection

```
sudo nmap -sS 192.168.0.109
```

****Results:**

**

- Open → SYN/ACK
 - Closed → RST
 - Filtered → No response
-

TCP ACK Scan (**-sA**)

Used for **firewall detection**

`nmap -sA 192.168.0.109`

- Firewall ON → No response
- Firewall OFF → RST

FIN / XMAS / NULL Scans

Used to test **firewall and IDS behavior**

FIN Scan

`nmap -sF 192.168.0.109`

XMAS Scan

`nmap -sX 192.168.0.109`

NULL Scan

`nmap -sN 192.168.0.109`

Behavior

- Open → No response
- Closed → RST

- Filtered → No response

Timing Control

Scan port 22 politely (slow):

```
sudo nmap -p 22 -sT -T2 192.168.0.109
```

- `-T2` → Polite / slow timing

NSE Scripts (Service Enumeration)

Run default Nmap scripts:

```
sudo nmap -sC 192.168.0.109
```

Turns Nmap from a **port scanner** into a **service enumerator**.

Software & Version Detection

```
sudo nmap -sV 192.168.0.109
```

Detects:

- Service name
- Software version
- Banner information

OS Detection

```
sudo nmap -O 192.168.0.109
```

Identifies the operating system using TCP/IP fingerprinting.

Disclaimer

This project is for **educational and authorized security testing only**.
Always scan systems you **own or have explicit permission** to test.

Author

SnoopySugar