

Nmap (Network Mapper) is a **powerful open-source tool** used for **network scanning, security auditing, and reconnaissance**. It helps cybersecurity professionals understand what devices, services, and vulnerabilities exist on a network.

Nmap can:

## 1. Discover Hosts

Find which machines are online (host discovery).

## 2. Scan Ports

Identify which ports are open, closed, or filtered.

## 3. Detect Services & Versions

Find out what software and version is running on each port (e.g., Apache 2.4.41, SSH 7.9, MySQL 5.7).

## 4. OS Detection

Identify the operating system (Windows, Linux, etc.).

## 5. Run Vulnerability Scripts

Using NSE (Nmap Scripting Engine), Nmap can:

- Enumerate SMB shares
- Detect vulnerable services (e.g., MS17-010)
- Gather metadata from web servers
- Perform brute-force or authentication checks

## Host Discovery

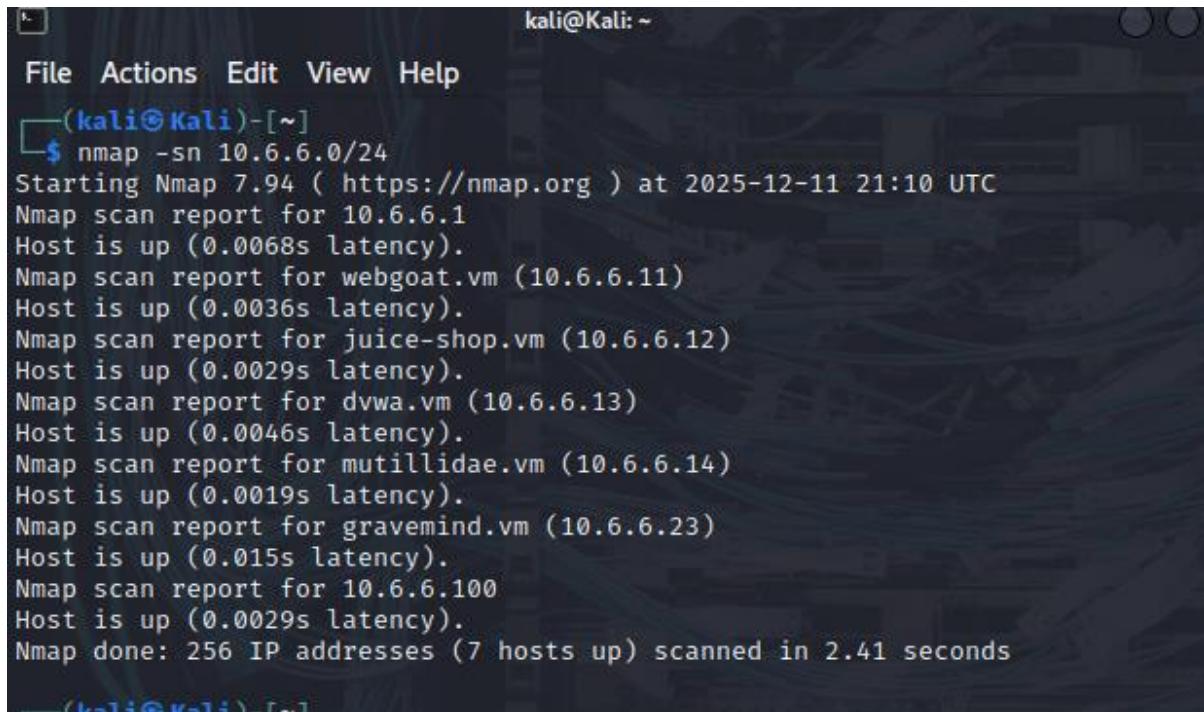
```
nmap -sn 10.6.6.0/24
```

This is used to **scan a network to find which hosts are up** (ping scan).

It does **not** scan ports — only checks if devices are alive.

- `-sn` = “ping scan”
- Scan the whole subnet 10.6.6.0 → 10.6.6.255
- Report which hosts reply (alive machines)

output



```
kali@Kali: ~
File Actions Edit View Help
└──(kali㉿Kali)-[~]
$ nmap -sn 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-11 21:10 UTC
Nmap scan report for 10.6.6.1
Host is up (0.0068s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0036s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0029s latency).
Nmap scan report for dwva.vm (10.6.6.13)
Host is up (0.0046s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0019s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.015s latency).
Nmap scan report for 10.6.6.100
Host is up (0.0029s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.41 seconds
└──(kali㉿Kali)-[~]
```

You can use `-v`, `-p`, and `-sV` to find additional information about the services running on the open ports

## Operating System discovery –

```
sudo nmap -O 10.6.6.23
```

To run this, you need root privileges

The -O option can be used to further determine information about the operating system running on the target host.

Some Nmap options require additional permissions and must be run as root or using the sudo command. To find operating system information on the target host, use the nmap -O command. Enter the password of kali when prompted.

output

```
(kali㉿kali)-[~]
$ sudo nmap -O 10.6.6.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-11 22:00 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.00037s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
8888/tcp  open  sun-answerbook
9001/tcp  open  tor-orport
MAC Address: 02:42:0A:06:06:0B (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.00015s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3000/tcp  open  ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)
```

The -A option enables aggressive scanning, which includes OS detection, version detection, script scanning (default NSE scripts), and traceroute.

You can specify multiple ports to scan by using the -p option and listing the ports separated by commas

nmap -A -p139,445 10.6.6.0/24

output

```
└─(kali㉿Kali)-[~]
$ nmap -A -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-11 22:11 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00061s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  0d00h00m01s  Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND

Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|-
|_ smb2-time:
|   date: 2025-12-11T22:11:47
|   start_date: N/A
|_ smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: gravemind
|   NetBIOS computer name: GRAVEMIND\x00
|   Domain name: \x00
|   FQDN: gravemind
|   System time: 2025-12-11T22:11:50+00:00
|_ clock-skew: mean: 0s, deviation: 1s, median: 0s
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

## SMB Services with Scripts (Nmap)

To gather detailed information about SMB (Server Message Block) services running on a target, Nmap provides specific **SMB enumeration scripts** through the Nmap Scripting Engine (NSE). These scripts help identify SMB versions, shared folders, security settings, vulnerabilities, and authentication methods.

```
nmap --script smb-enum-users.nse -p139,445 10.6.6.23
```

## output

```
(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-users.nse -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-11 22:39 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00085s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| smb-enum-users:
|   GRAVEMIND\arbiter (RID: 1001)
|     Full name:
|     Description:
|     Flags:      Account disabled, Password not required, Normal user account
|   GRAVEMIND\masterchief (RID: 1000)
|     Full name:
|     Description:
|     Flags:      Account disabled, Password not required, Normal user account
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

(kali㉿Kali)-[~]
└─$
```

You can enumerate the network shares using another NSE script, smb-enum-shares.nse. To discover shared directories on the target computer. Use the Nmap share enumeration script with the command

```
nmap --script smb-enum-shares.nse -p445 10.6.6.23
```

output

```
(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-11 22:44 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00049s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.6.6.23\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.5-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\workfiles:
|     Type: STYPE_DISKTREE
|     Comment: Confidential Workfiles
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\spool\samba
|     Anonymous access: READ/WRITE
```