

## Scanning

**Scanning** is the second phase of the hacking methodology and comes right after reconnaissance (or footprinting). While reconnaissance gathers passive and active information about a target, scanning focuses on actively identifying open ports, services, and potential vulnerabilities in systems.

What is Scanning?

Scanning involves using tools and techniques to **probe a target system/network** for open ports, live hosts, services, and vulnerabilities. This helps the attacker (or ethical hacker) understand how to exploit the system.

### Types of Scanning

#### 1. Port Scanning

- Identifies open ports on a target system.
- Helps determine which services are running.
- Common tools: Nmap, Netcat, Angry IP Scanner.
- Example types:
  - TCP Connect Scan
  - SYN Scan (Half-open)
  - UDP Scan
  - Stealth Scan

#### 2. Network Scanning

- Identifies active devices on a network and maps the topology.
- Helps detect live hosts, IP addresses, and shared resources.
- Tools: Nmap, Angry IP Scanner, Advanced IP Scanner.

#### 3. Vulnerability Scanning

- Scans systems for known vulnerabilities (missing patches, misconfigurations).
- Helps in finding exploits.
- Tools: Nessus, OpenVAS, Nikto, Qualys.

#### 4. Banner Grabbing

- Retrieves information about the software version running on open ports.
- Helps identify outdated or vulnerable services.

#### **Common Tools:**

- Nmap – Port and network scanning.
- **Netcat** – Port scanning and banner grabbing.
- **Nessus/OpenVAS** – Vulnerability assessment.
- **Nikto** – Web server vulnerability scanning.
- **Wireshark** – Packet capture and analysis.

#### **Purpose of Scanning:**

- Identify entry points for attack (open ports, services).
- Assess the security posture of the target.
- Map the target network structure.
- Prepare for the next phase: **Gaining Access**.

# Nmap

Nmap is a network scanning and security auditing tool used to discover devices, identify open ports, detect services and their versions, and determine operating systems on a network.

## Some commands I practice in class while leaning the nmap tool...

I. `nmap 192.168.1.9`

It shows all the open ports present in targeted machine.

```
(kali㉿kali)-[~]
$ nmap 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 01:56 EDT
Nmap scan report for 192.168.1.9
Host is up (0.027s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.50 seconds
```

II. `nmap -p22 192.168.1.9`

It shows specific port in this example namp is only checking for port 22.

```
(kali㉿kali)-[~]
$ nmap -p22 198.162.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:02 EDT
Nmap scan report for 198.162.1.9
Host is up (0.00066s latency).

PORT      STATE SERVICE
22/tcp    filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
```

### III. nmap -p22-1000 192.168.1.9

In this command we give the range of ports we want to check.

```
(kali㉿kali)-[~]
$ nmap -p22-1000 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:08 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.50% done; ETC: 02:18 (0:08:33 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.54% done; ETC: 02:17 (0:06:57 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:05:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.55% done; ETC: 02:14 (0:00:55 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:07:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 02:15 (0:00:00 remaining)
Stats: 0:07:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 02:16 (0:00:00 remaining)
Nmap scan report for 192.168.1.9
Host is up (2.6s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
514/tcp   filtered shell
Nmap done: 1 IP address (1 host up) scanned in 468.48 seconds
```

### IV. nmap -p22,80,8080,443

This command is use to scan given specific ports.

```
(kali㉿kali)-[~]
$ nmap -p22,80,8080,443 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:21 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0037s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

## V. nmap -p- 192.168.1.9

This command scans all the port of targeted machine.

```
(kali@kali)-[~]
$ nmap -p- 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:07 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0093s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 165.84 seconds
```

## VI. nmap -sV 192.168.1.9

This command shows the service versions of ports of targeted machine.

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 01:54 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0043s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.13 seconds
```

## VII. nmap -O 192.168.1.9

This command is for scanning and it shows the operating system of targeted machine.

```
(kali@kali)-[~]
$ nmap -O 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:21 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0078s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
514/tcp   filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (93%), Actiontec MI424WR-GEN3I MAP (90%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 SP2 (88%), HP Officejet Pro 8500 printer (87%), Linux 3.2 (87%), Linux 4.4 (87%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (87%), ReactOS 0.3.7 (87%), D-Link DFL-700 firewall (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds
```

## VIII. nmap -A 192.168.1.9

This Command shows the Operating System, Service version and Trace route of targeted machine.

```
(kali@kali)-[~]
$ nmap -A 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:20 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
514/tcp    filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DO-WRT v24-sp2 (Linux 2.4.37) (93%), Actiontec MI424NR-GEN3I NAD (90%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 SP2 (88%), HP Officejet Pro 8500 printer (87%), Linux 3.2 (87%), Linux 4.4 (87%), Microsoft Windows XP SP3 or Windows 7 on Windows Server 2012 (87%), ReactOS 0.3.7 (87%), D-Link GPL-780 Firewall (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.63 ms 192.168.8.2
2 0.68 ms 192.168.1.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.63 seconds
```

## IX. nmap -Pn 192.168.1.9

This command is for checking the ping block or any of the option is block.

```
(kali@kali)-[~]
$ nmap -Pn 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:23 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.47% done; ETC: 02:27 (0:01:25 remaining)
Stats: 0:03:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.67% done; ETC: 02:29 (0:02:06 remaining)
Stats: 0:03:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.90% done; ETC: 02:29 (0:02:14 remaining)
Stats: 0:04:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.31% done; ETC: 02:30 (0:02:19 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.1.9
Host is up (2.4s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
143/tcp    open  imap
443/tcp    open  https
445/tcp    open  microsoft-ds
514/tcp    filtered shell
1022/tcp   filtered exp2
5001/tcp   open  complex-link
5911/tcp   filtered cpdlc
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1233.62 seconds
```

## X. nmap -Sn 192.168.1.9

For checking the Ping

```
(kali@kali)-[~]
$ nmap -sn 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:53 EDT
Nmap scan report for 192.168.1.9
Host is up (0.00065s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

## XI. nmap -sC 192.168.1.9

For finding a basic vulnerability it scans a machine.

```
(kali㉿kali)-[~]
$ nmap -sC 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:51 EDT
Nmap scan report for 192.168.1.9
Host is up (0.044s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp   open  netbios-ssn
143/tcp   open  imap
|_imap-capabilities: SORT CHILDREN OK IMAP4rev1 THREAD-REFERENCES CAPABILITY completed ACL2=UNIONA0001 UIDPLUS ACL QUOTA IDLE THREAD=ORDEREDSUBJECT NAMESPACE
443/tcp   open  https
|_http-methods:
|_ Potentially risky methods: TRACE
|_ssl-cert: Subject: commonName=owaspbwa
|_Not valid before: 2013-01-02T21:12:38
|_Not valid after: 2022-12-31T21:12:38
|_ssl-date: 2025-05-09T06:52:08+00:00; +7s from scanner time.
|_http-title: owaspbwa OWASP Broken Web Applications
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
|_http-title: Site doesn't have a title.
8081/tcp  open  blackice-icecap

Host script results:
|_smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 6s, deviation: 0s, median: 6s
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 68.51 seconds
```

## XII. nmap -v 192.168.1.9

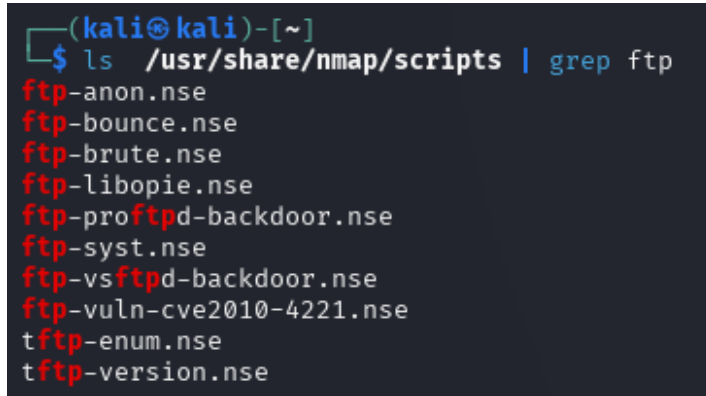
Verbosity for viewing a proper running command.

```
(kali㉿kali)-[~]
$ nmap -v 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:54 EDT
Initiating Ping Scan at 02:54
Scanning 192.168.1.9 [4 ports]
Completed Ping Scan at 02:54, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:54
Completed Parallel DNS resolution of 1 host. at 02:54, 0.04s elapsed
Initiating SYN Stealth Scan at 02:54
Scanning 192.168.1.9 [1000 ports]
Discovered open port 8080/tcp on 192.168.1.9
Discovered open port 143/tcp on 192.168.1.9
Discovered open port 443/tcp on 192.168.1.9
Discovered open port 80/tcp on 192.168.1.9
Discovered open port 445/tcp on 192.168.1.9
Discovered open port 139/tcp on 192.168.1.9
Completed SYN Stealth Scan at 02:54, 21.75s elapsed (1000 total ports)
Nmap scan report for 192.168.1.9
Host is up (0.0020s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
Raw packets sent: 3008 (132.268KB) | Rcvd: 203 (8.144KB)
```

XIII. `ls/usr/share/nmap/script | grep "ftp"`

This command is for accessing the inbuild Script of nmap we can use for hacking any machine. In this example (Command) we are specifically finding the exploit for ftp service.



```
(kali㉿kali)-[~]  
$ ls /usr/share/nmap/scripts | grep ftp  
ftp-anon.nse  
ftp-bounce.nse  
ftp-brute.nse  
ftp-libopie.nse  
ftp-proftpd-backdoor.nse  
ftp-syst.nse  
ftp-vsftpd-backdoor.nse  
ftp-vuln-cve2010-4221.nse  
tftp-enum.nse  
tftp-version.nse
```

XIV. `nmap -script =__address_of_script__ 192.168.1.9`

In this command we are running script that we take from inbuild nmap scripts for targeted machine.