

**REPORT OF
NETWORK SCANNING.**

Module - 3

Aniket Sunil Pagare.

NETWORK SCANNING

Network scanning is a process used in computer networks to identify active devices, services, and potential vulnerabilities within a network. It involves sending data packets to target systems and analyzing their responses to gather information such as IP addresses, open ports, running services, and security risks.

Objectives –

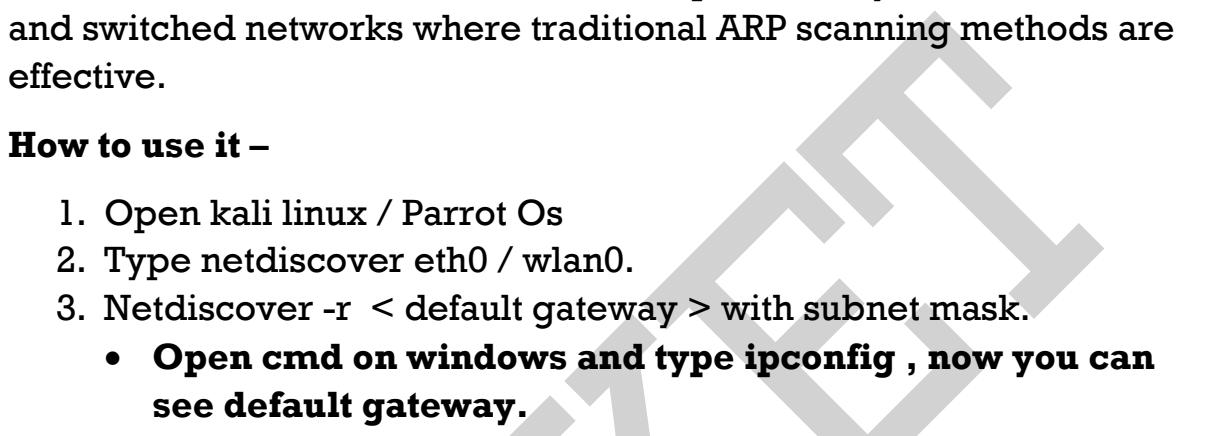
- Discovery
- Security assessment
- Vulnerability detection
- Network mapping
- Performance analysis

Network Scanning Using Netdiscover

Netdiscover is a network reconnaissance tool in Kali Linux designed to discover live hosts on a network. It is particularly useful in wireless and switched networks where traditional ARP scanning methods are effective.

How to use it –

1. Open kali linux / Parrot Os
2. Type netdiscover eth0 / wlan0.
3. Netdiscover -r < default gateway > with subnet mask.
 - **Open cmd on windows and type ipconfig , now you can see default gateway.**

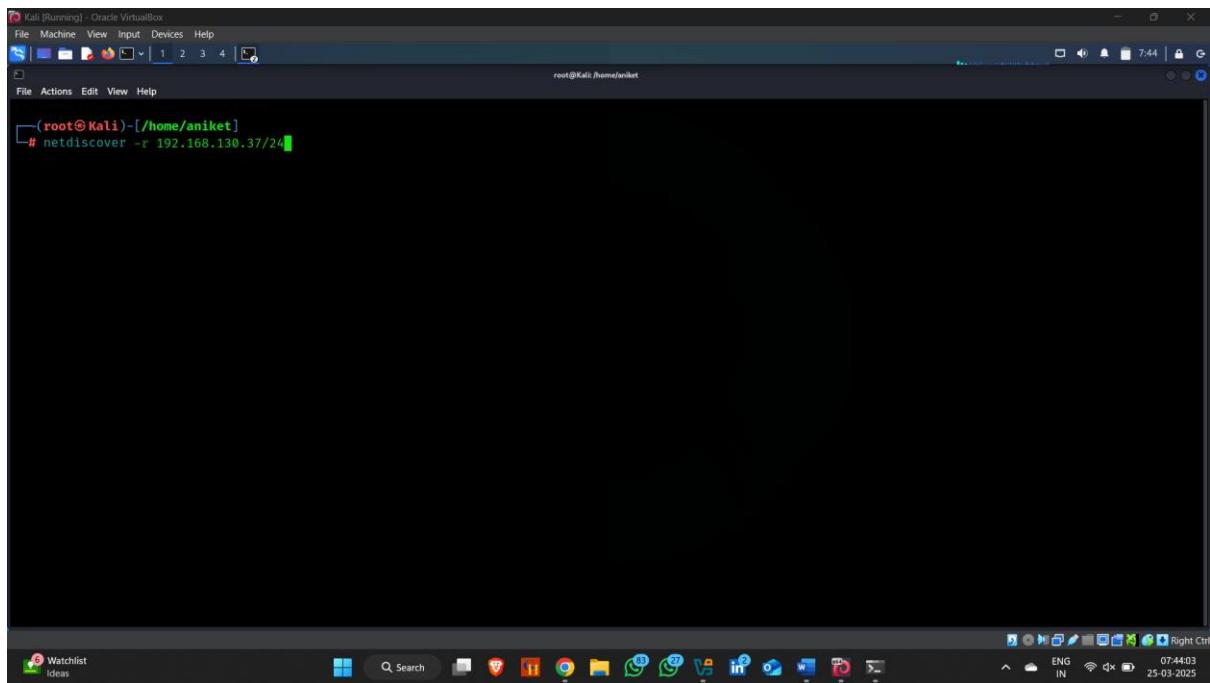


```
Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Ethernet adapter VMware Network Adapter VMnet1:
    Connection-specific DNS Suffix . . . . . :
    IPv4 Address . . . . . : 192.168.179.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
    Connection-specific DNS Suffix . . . . . :
    IPv4 Address . . . . . : 192.168.217.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . . . . . :
    IPv4 Address . . . . . : 192.168.130.254
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.130.57
Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
C:\Users\anike>
```

Common Usage Commands:

- netdiscover — Scans the local network using default settings.
- netdiscover -i eth0 — Specifies the network interface (e.g., eth0, wlan0).

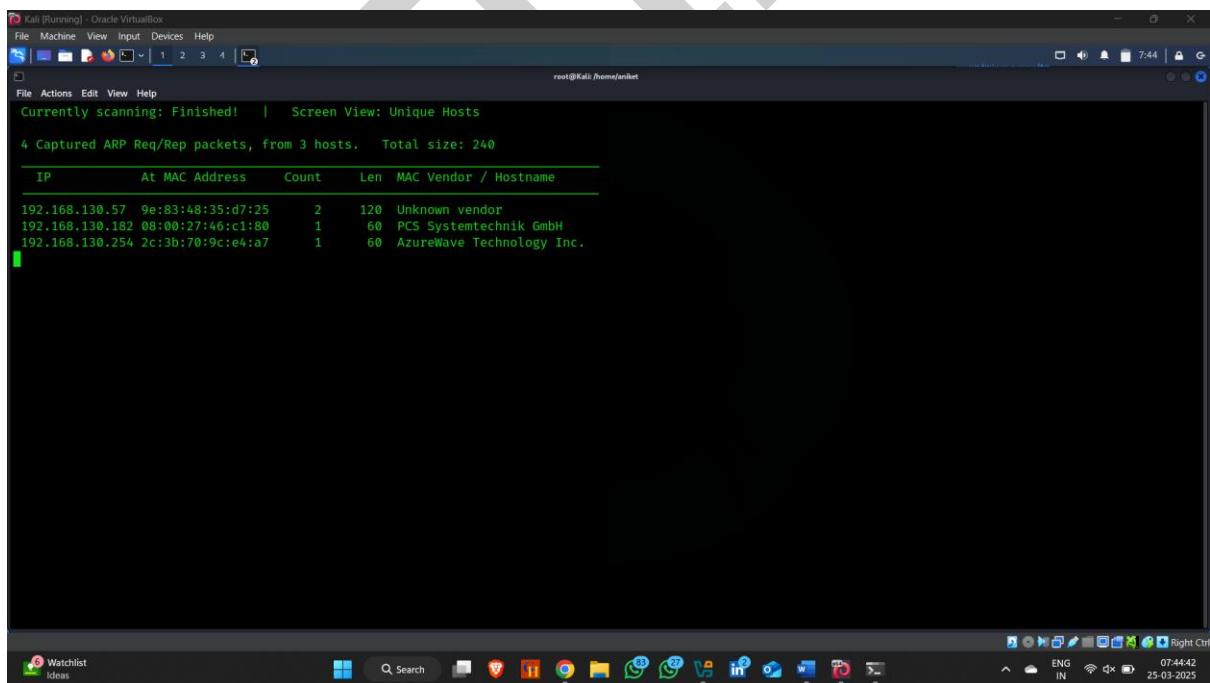
- **netdiscover -r 192.168.1.0/24** — Scans a specific IP range.
- **netdiscover -p** — Passive mode for monitoring ARP traffic without actively sending packets.



Kali [Running] - Oracle VirtualBox

```
(root@Kali:[/home/aniket]
# netdiscover -r 192.168.130.37/24
```

This screenshot shows a terminal window on a Kali Linux desktop. The terminal title is 'Kali [Running] - Oracle VirtualBox'. The command entered is 'netdiscover -r 192.168.130.37/24'. The terminal window has a dark background with white text. The desktop environment includes a dock with various icons at the bottom.



Kali [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.130.57 9e:83:48:35:d7:25 2 120 Unknown vendor
192.168.130.182 08:00:27:46:c1:80 1 60 PCS Systemtechnik GmbH
192.168.130.254 2c:3b:70:9c:e4:a7 1 60 AzureWave Technology Inc.
```

This screenshot shows the same terminal window after the scan has completed. The output shows the results of the ARP scan, indicating 4 captured ARP requests/replies from 3 hosts. The table lists the IP address, MAC address, count, length, and vendor/hostname for each host. The desktop environment is visible at the bottom.

Network Scanning using Nmap.

Nmap (Network Mapper) is a powerful open-source tool used for network discovery, security auditing, and vulnerability scanning. It's widely used by network administrators and penetration testers to map network structures and identify open ports, services, and potential security risks.

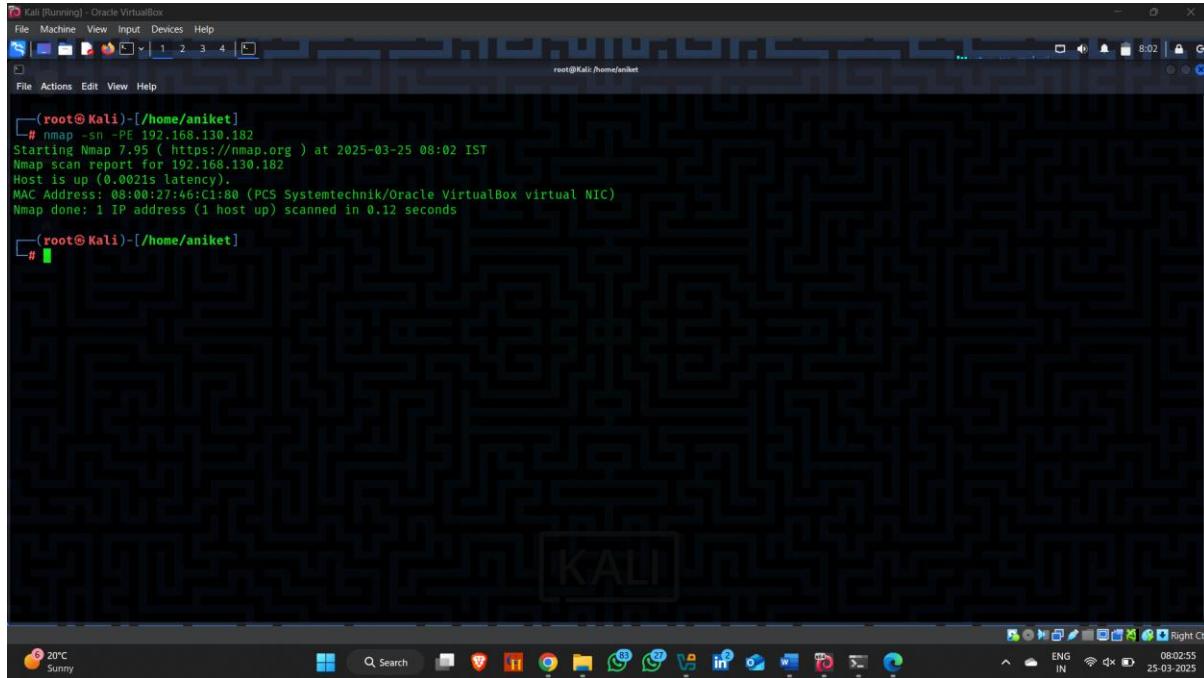
1. Host Discovery –

Host Discovery helps determine which systems are up and reachable before performing deeper scans or security assessments.

Common Usage Command –

- -PE = ICMP Echo Scan.
- -PR = ARP Ping Scan.
- -PU = UDP Ping Scan.
- -PP = ICMP Timestamp Ping Scan.
- -PS = TCP SYN Scan.
- -PO = IP Protocol Scan.
- -PM = ICMP Address Mask Scan.

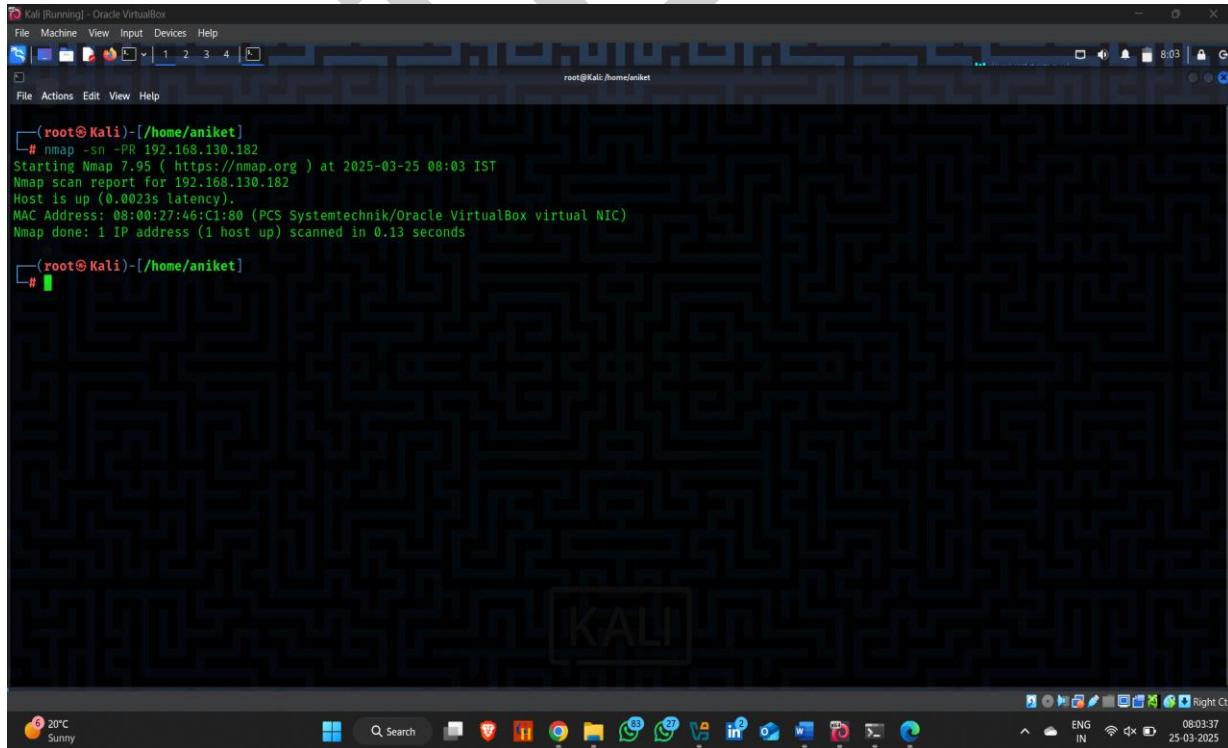
- -PE -- the -PE option is used to send **ICMP Echo Request** packets during a ping scan.



```
(root@Kali)-[~/home/aniket]
# nmap -sn -PE 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:02 IST
Nmap scan report for 192.168.130.182
Host is up (0.0021s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

The screenshot shows a terminal window on a Kali Linux desktop. The terminal output displays the results of a ping scan (-sn) with ICMP echo requests (-PE) against the IP address 192.168.130.182. The host is identified as being up with a latency of 0.0021 seconds. The MAC address of the target host is shown as 08:00:27:46:C1:80, which is associated with a PCS Systemtechnik/Oracle VirtualBox virtual NIC. The entire process took 0.12 seconds. The desktop environment includes a taskbar with various icons and a system tray at the bottom.

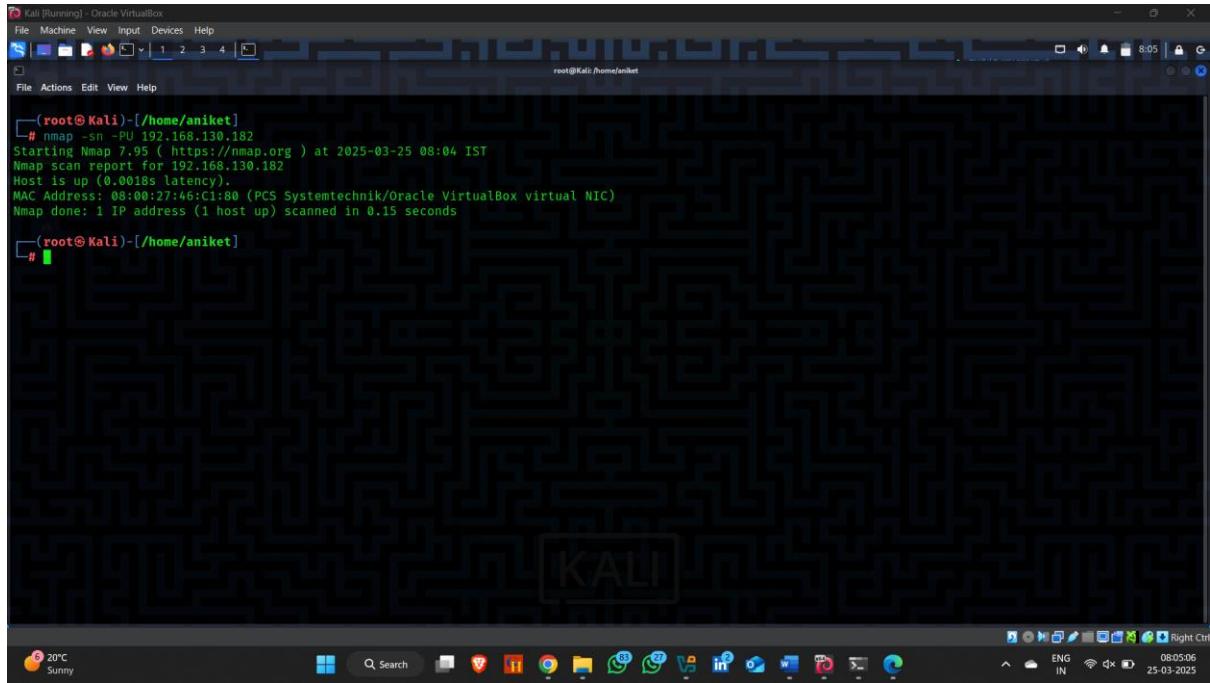
- -PR -- the -PR option is used to perform an **ARP (Address Resolution Protocol) Request Scan**.



```
(root@Kali)-[~/home/aniket]
# nmap -sn -PR 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:03 IST
Nmap scan report for 192.168.130.182
Host is up (0.0023s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

This screenshot is identical to the one above, showing the output of an nmap -sn -PR scan. It reports that the host at 192.168.130.182 is up with a latency of 0.0023 seconds. The MAC address is 08:00:27:46:C1:80, and the scan completed in 0.13 seconds. The desktop environment and terminal interface are consistent with the first screenshot.

- -PU -- the -PU option is used to perform a **UDP Ping Scan**.



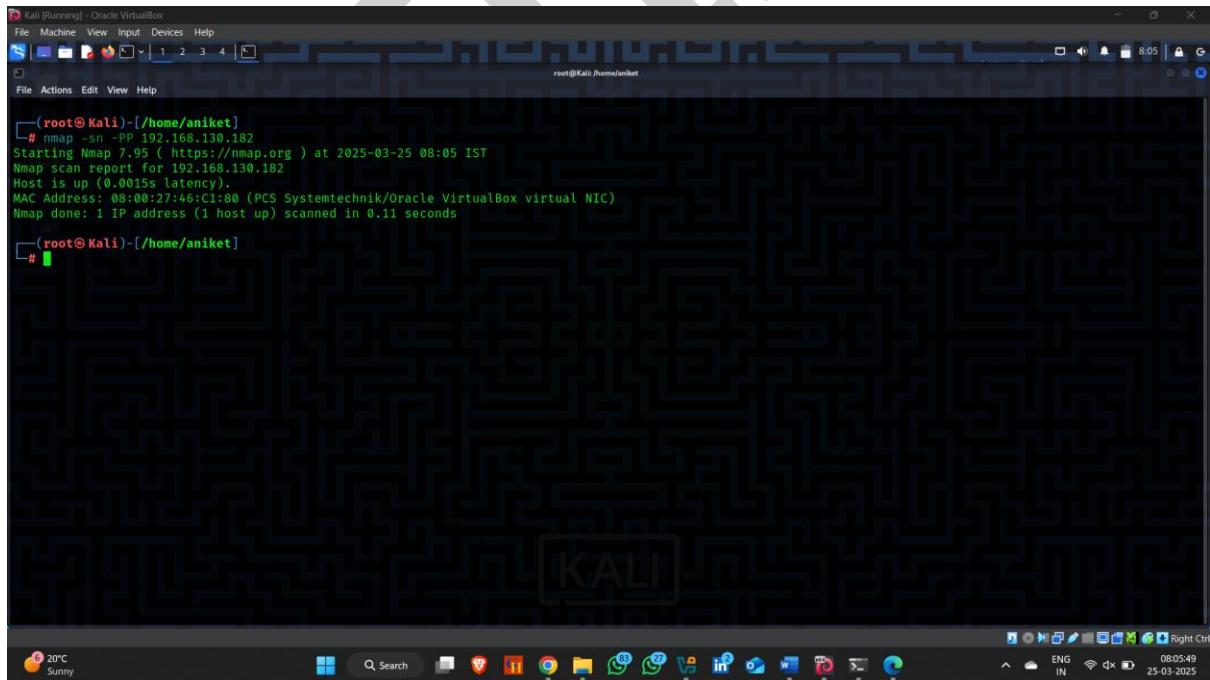
Kali [Running] - Oracle VirtualBox

```
(root@Kali)-[~/home/aniket]
# nmap -sn -PU 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:04 IST
Nmap scan report for 192.168.130.182
Host is up (0.0018s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

root@Kali:~/home/aniket#

The screenshot shows a Kali Linux desktop environment. A terminal window is open with the command `nmap -sn -PU 192.168.130.182` run by root. The output shows a single host is up with a latency of 0.0018s. The desktop background features a complex maze pattern, and the taskbar at the bottom shows various application icons.

- -PP -- the -PP option is used to perform an **ICMP Timestamp Request Ping Scan**.



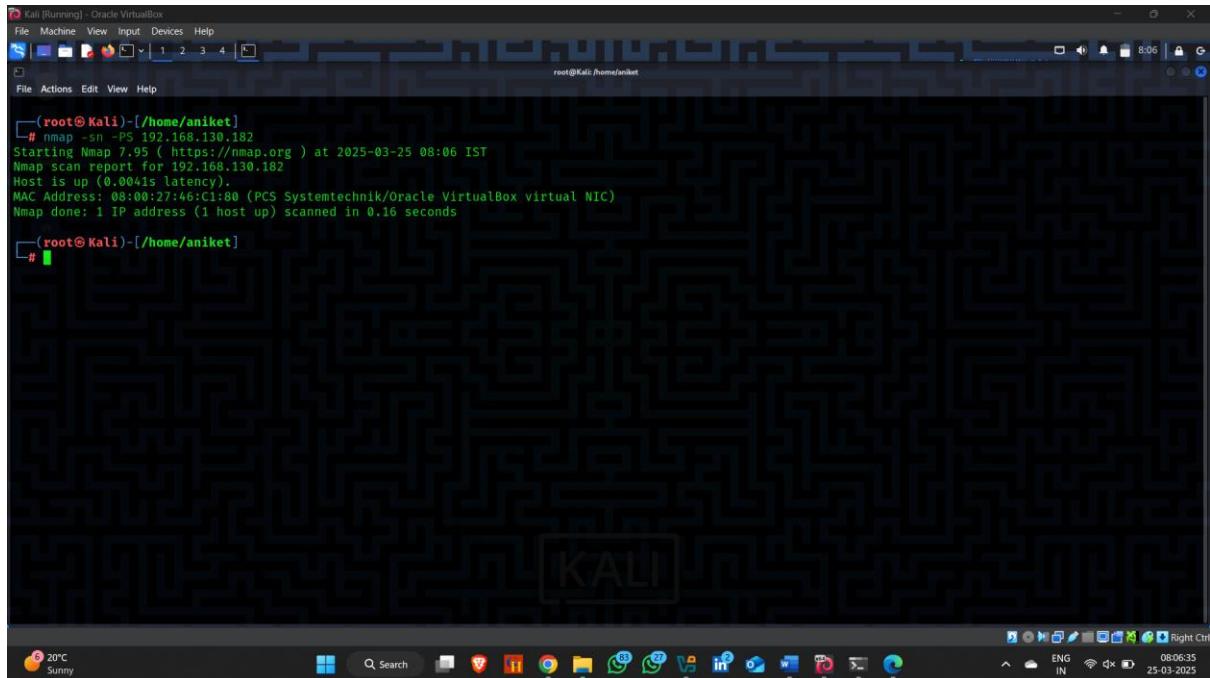
Kali [Running] - Oracle VirtualBox

```
(root@Kali)-[~/home/aniket]
# nmap -sn -PP 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:05 IST
Nmap scan report for 192.168.130.182
Host is up (0.0015s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

root@Kali:~/home/aniket#

This screenshot is identical to the one above, showing a terminal window with the same Nmap command and output. It is taken from the same Kali Linux desktop environment with the same configuration and background.

- -PS -- the -PS option is used to perform a **TCP SYN Ping Scan**.



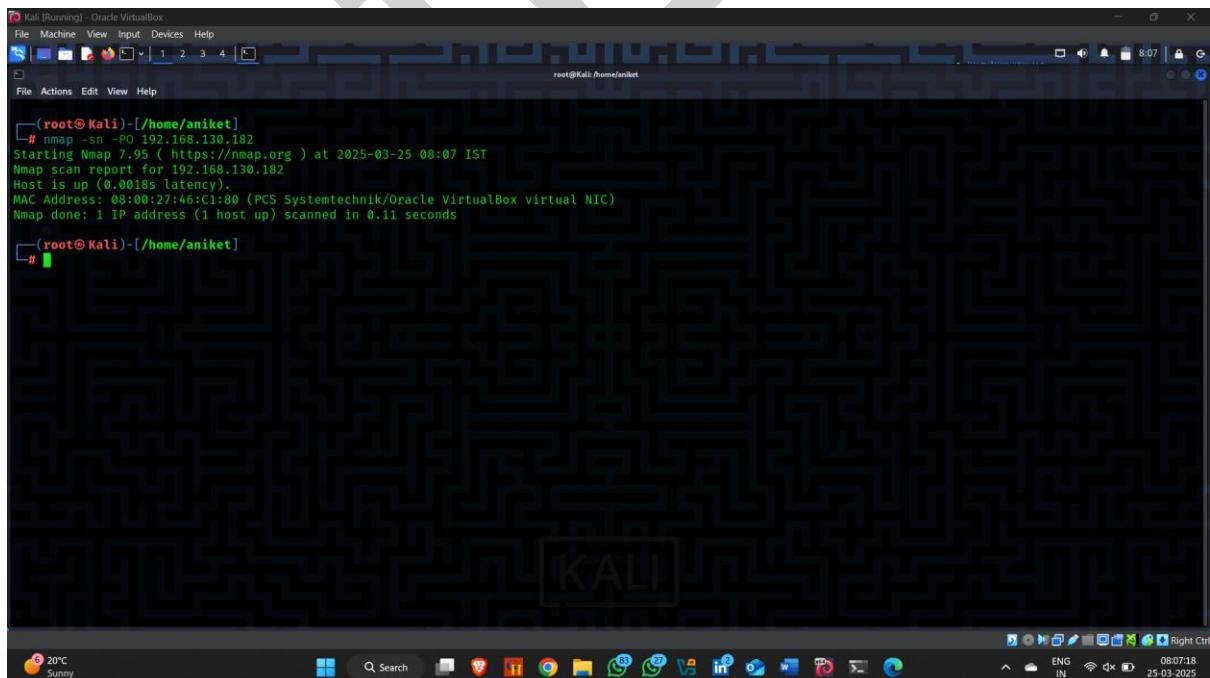
Kali [Running] - Oracle VirtualBox

```
(root@Kali)-[~/home/aniket]
# nmap -sn -PS 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:06 IST
Nmap scan report for 192.168.130.182
Host is up (0.0041s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

root@Kali:~/home/aniket#

The screenshot shows a Kali Linux desktop environment. A terminal window is open in the foreground, displaying the results of a TCP SYN ping scan using the command `nmap -sn -PS 192.168.130.182`. The output shows that the host at 192.168.130.182 is up with a latency of 0.0041s. The MAC address of the interface is 08:00:27:46:C1:80. The scan completed in 0.16 seconds. The desktop background features a complex black and white geometric pattern.

- -PO -- the -PO option is used to perform an **IP Protocol Ping Scan**.



Kali [Running] - Oracle VirtualBox

```
(root@Kali)-[~/home/aniket]
# nmap -sn -PO 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:07 IST
Nmap scan report for 192.168.130.182
Host is up (0.0018s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

root@Kali:~/home/aniket#

The screenshot shows a Kali Linux desktop environment. A terminal window is open in the foreground, displaying the results of an IP protocol ping scan using the command `nmap -sn -PO 192.168.130.182`. The output shows that the host at 192.168.130.182 is up with a latency of 0.0018s. The MAC address of the interface is 08:00:27:46:C1:80. The scan completed in 0.11 seconds. The desktop background features a complex black and white geometric pattern.

- **-PM** -- the **-PM** option is used to perform an **ICMP Address Mask Request Ping Scan**.



```
Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
[root@Kali ~]# nmap -sn -PM 192.168.130.182  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:07 IST  
Nmap scan report for 192.168.130.182  
Host is up (0.0014s latency).  
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds  
[root@Kali ~]#
```

2. Port And Service Discovery.

Port scanning is the process of probing a system's ports to identify which ones are open, closed, or filtered. It helps determine which services are running on a target system.

Common Usage Command –

- -p- = All Port Scan (65535).
- -p = Scan Specific Post (eg > -p21,80,443).
- -F = Fast Scan (Top 100 ports)
- --top-ports <number > = scan common ports
- -sS = Stealth Scan / Halft Scan / Two Way Handshake.
- -sT = TCP Scan / Full Scan / Three Way Handshake.
- -sU = UDP Scan.
- -sA = ACK Scan .
- -sM = Maimon Scan.
- -sX = Xmass Scan (send 3 flag at a time - FIN , URG , PSH)
- -sN = Tcp null scan.
- _sV = Service version Detection.
- -v = Verbosity
- -sC = Script Scan.
- -T<0-5> = Aggressive Scan.
- -A = Advance Scan.

- -sS -- the -sS option specifies a **SYN scan**, often called a **stealth scan or half-open scan**.

```

root@Kali:[/]# nmap -sS 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:28 IST
Nmap scan report for 192.168.130.182
Host is up (0.0021s 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: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

```

- -sT -- the -sT option specifies a **TCP Connect scan**. It's the default scan type .

```

root@Kali:[/]# nmap -sT 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:31 IST
Nmap scan report for 192.168.130.182
Host is up (0.0053s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

```

- **-sU** -- the **-sU** option specifies a **UDP scan**, which is designed to identify open **UDP ports** on a target system.

```

root@Kali:[~]# nmap -sU 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:34 IST
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 4.74% done; ETC: 08:47 (0:12:43 remaining)
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:4684 > 192.168.130.182:30365 ttl=3 id=34592 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:4684 > 192.168.130.182:30365 ttl=41 id=10238 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:4684 > 192.168.130.182:30365 ttl=58 id=23493 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:4684 > 192.168.130.182:30365 ttl=45 id=36355 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:46877 > 192.168.130.182:22341 ttl=44 id=18824 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:46852 > 192.168.130.182:30365 ttl=50 id=2445 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:46858 > 192.168.130.182:30365 ttl=31 id=59621 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:46858 > 192.168.130.182:30365 ttl=53 id=5407 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.168.130.182, 16) => Network is unreachable
Offending packet: UDP 192.168.130.192:46860 > 192.168.130.182:30365 ttl=56 id=46856 iplen=28
Omitting future Sendto error messages now that 10 have been shown. Use -d2 if you really want to see them.

```

- **-p-** -- the **-p-** option is used to scan **all 65,535 TCP or UDP ports** on a target system.

```

root@Kali:[~]# nmap -p- 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 08:36 IST
Stats: 0:00:00 elapsed; 1 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.78% done; ETC: 08:36 (0:00:05 remaining)
Nmap scan report for 192.168.130.182
Host is up (0.00032s latency).
Not shown: 65505 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
1080/tcp  open  registry
1324/tcp  open  mredlock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6067/tcp  open  irc
6097/tcp  open  irc-6-0
8000/tcp  open  http
8110/tcp  open  unknown
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39471/tcp open  unknown
50410/tcp open  unknown
52093/tcp open  unknown
59134/tcp open  unknown
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)


```

- **-sX** -- The **Xmas scan** sends TCP packets with the **FIN**, **PSH**, and **URG** flags set.

```
[root@Kali:~/home/aniket]
# nmap -sX 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 08:13 IST
Nmap scan report for 192.168.130.182
Host is up (0.0016s latency).

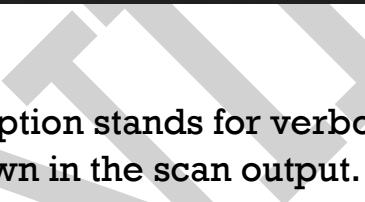
PORT      STATE     SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:46:C1:80 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
[root@Kali:~/home/aniket]
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0:00:00:00:00:00	Broadcast	Broadcast	ARP	60	Who has 192.168.130.254? Tell 192.168.138.57
2	0:00:00:00:00:03	PCSystemtec_28:75:.. Broadcast	Broadcast	ARP	42	Who has 192.168.130.182? Tell 192.168.130.192
3	0:00:00:00:00:04	PCSystemtec_28:75:..	PCSystemtec_28:75:..	ARP	60	192.168.130.182 is at 08:00:27:46:C1:80
4	0:00:00:00:00:05	PCSystemtec_28:75:..	PCSystemtec_28:75:..	ICMPv6	80	Neighbor Advertisement for fe80::9c83:48ff:fe35:d725 from 08:00:27:46:C1:80
5	0:00:00:00:00:06	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d	2401:4900:57bc:4e5d	ICMPv6	86	Neighbor Advertisement 2401:4900:57bc:4e5d::68 (rtr, sol, ovr) is at 08:00:27:46:C1:80
6	0:00:00:00:00:07	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d	2401:4900:57bc:4e5d	ICMPv6	108	Standard query 0x6cd0 PTR 192.130.168.192.in-addr.arpa
7	0:00:00:00:00:08	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d	2401:4900:57bc:4e5d	ICMPv6	86	Neighbor Advertisement 2401:4900:57bc:4e5d::68 (rtr, sol, ovr) is at 02:56:f3:08:08:04
8	0:00:00:00:00:09	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d	2401:4900:57bc:4e5d	ICMPv6	108	Standard query for the registered node name PTR 192.130.168.192.in-addr.arpa prisoner.iana.org
9	0:00:00:00:00:10	PCSystemtec_28:75:.. Broadcast	Broadcast	ARP	42	Who has 192.168.130.182? Tell 192.168.130.192
10	0:00:00:00:00:11	PCSystemtec_28:75:..	PCSystemtec_28:75:..	ARP	60	192.168.130.182 is at 08:00:27:46:C1:80
11	0:00:00:00:00:12	192.168.130.192	192.168.130.182	TCP	54	57728 - 00 [FIN, PSH, URG] Seq=1 Win=1024 Urgent Len=0
12	0:00:00:00:00:13	192.168.130.182	192.168.130.192	TCP	64	57728 - 00 [ACK] Seq=2 Win=1024
13	0:00:00:00:00:14	fe80::9c83:48ff:fe3..	2401:4900:57bc:4e5d	ICMPv6	86	Neighbor Solicitation for 2401:4900:57bc:4e5d:4e8:b984:3d56:50a from 0e:83:48:35:d7:25
14	0:00:00:00:00:15	2401:4900:57bc:4e5d:fe80::9c83:48ff:fe3..	2401:4900:57bc:4e5d:fe80::9c83:48ff:fe3..	ICMPv6	78	Neighbor Advertisement 2401:4900:57bc:4e5d:aea:b884:3d56:50a (sol)
15	0:00:00:00:00:16	fe80::0e:83:48ff:fe3..	fe80::0e:83:48ff:fe3..	ICMPv6	86	Neighbor Solicitation for fe80::9c83:48ff:fe35:d725 from 08:00:27:28:75:f4
16	0:00:00:00:00:17	fe80::0e:83:48ff:fe3..	fe80::0e:83:48ff:fe3..	ICMPv6	78	Neighbor Advertisement fe80::9c83:48ff:fe35:d725 (rtr, sol)

[Stream index: 1]
[Conversation completeness: Incomplete (0)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Next Sequence Number: 2 (relative sequence number)
Acknowledgment Number: 0
Acknowledgment number (raw): 0
Header Length: 20 bytes (5)
Flags: 0x29 (FIN, PSH, URG)
Window: 1024
[Calculated window size: 1024]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x0876 (unverified)

- **-sV** -- the **-sV** option is used for **service version detection**, which identifies the exact software version running on open ports.



Kali [Running] - Oracle VirtualBox

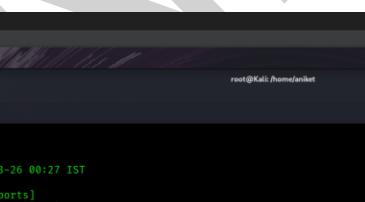
```
File Machine View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket x root@Kali:/home/aniket x

[ root@Kali ~ ]# nmap -sV certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 00:26 IST
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 62.50s done; ETC: 00:26 (0:00:04 remaining)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.33s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 989 closed tcp ports (reset)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp          Pure-FTPd
22/tcp    open      ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp    open      smtp         Exim smtpd 4.98.1
26/tcp    open      smtp         Exim smtpd 4.98.1
53/tcp    open      domain       ISC BIND 9.11.4-P2 (Redhat Enterprise Linux 7)
80/tcp    open      http         Apache httpd
110/tcp   open      pop3        Dovecot pop3d
143/tcp   open      imap        Dovecot imapsd
443/tcp   open      ssl/http    Apache httpd
465/tcp   open      tcpwrapped
587/tcp   open      tcpwrapped
993/tcp   open      ssl/imap    Dovecot imapd
995/tcp   open      ssl/pop3   Dovecot pop3d
2222/tcp  open      ssh          OpenSSH 7.4 (protocol 2.0)
3306/tcp  open      mysql       MySQL 5.7.23-23
3889/tcp  filtered  dandv-tester
5432/tcp  open      postgresql PostgreSQL DB
7379/tcp  open      redis       Redis 6.2.10
7702/tcp  open      redis       Redis 6.2.10
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:7.95X=7X0/3/26XTime=67E2FC579P*x86_64-pc-linux-gnuXrSM
SF-BProgNeg,85,"EV\0\0\0\0x&45FATAL\0C0A000\0Unsupported\x20frontend\x20proto
SF:tcp[0x20653363\,19778\,x20xServer\,x20xSupports\,x201\,0x20to\,x203\,\0xFpo
SF:sMaster\,\<x0L1811\0RProcessStartupPacket\0\0\>Xr\,Kerberos,85,"EV\0\0\0
SF:<845FATA\,0C0A000\0Unsupported\x20frontend\x20protocol\,x207265,,28208
SF::\x20xServer\,x20xSupports\,x201\,0x20to\,x203\,\0\0postmaster\,\<x0L1811\0R
SF:ProcessStartupPacket\0\0\>
Service info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

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

0:00:09.000000 SH16 / NHS48D.. Closed road
0:00:09.000000 ENG IN 00:26:43 26-03-2025
```

- **-v** -- the **-v** option stands for **verbosity**. It increases the amount of detail shown in the scan output.



Kali [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket x root@Kali:/home/aniket x

[ root@Kali ~ ]# nmap -sV -p1-500 -v certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 00:27 IST
Initiating Ping Scan at 00:27
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 00:27, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:27
Completed Parallel DNS resolution of 1 host. at 00:27, 0.01s elapsed
Initiating SYN Stealth Scan at 00:27
Scanning certifiedhacker.com (162.241.216.11) [500 ports]
DISCOVERED: certifiedhacker.com (162.241.216.11)
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 25/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Discovered open port 28/tcp on 162.241.216.11
Completed SYN Stealth Scan at 00:27, 2.01s elapsed (500 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.40s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 499 closed tcp ports (reset)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp         
22/tcp    open      ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp    open      smtp         Exim smtpd 4.98.1
53/tcp    open      domain       ISC BIND 9.11.4-P2 (Redhat Enterprise Linux 7)
80/tcp    open      http         Apache httpd
110/tcp   open      pop3        Dovecot pop3d
143/tcp   open      imap        Dovecot imapsd
443/tcp   open      https        Apache httpd
465/tcp   open      smtp         Apache httpd

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds

0:00:09.000000 Finance headline
US Markets Rally... 0:00:09.000000 ENG IN 00:27:27 26-03-2025
```

- -sC -- In **Nmap**, the -sC option stands for "**Script Scan**". It tells Nmap to run the **default scripts** during a scan.

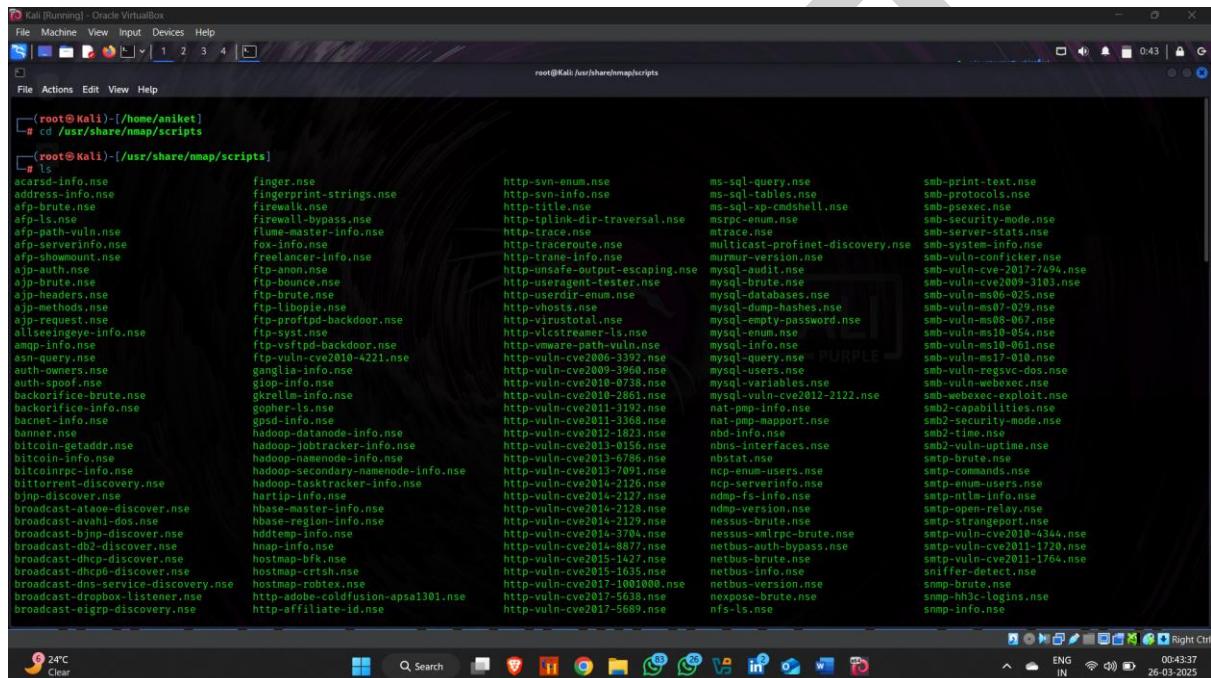
Note - Before performing nmap script , find all scripts locations .

Step 1: Locate the Nmap Installation Path.

- The Nmap scripts are typically stored in the scripts folder within the Nmap installation directory.

Step 2 : The scripts are usually located in:

- /usr/share/nmap/scripts.

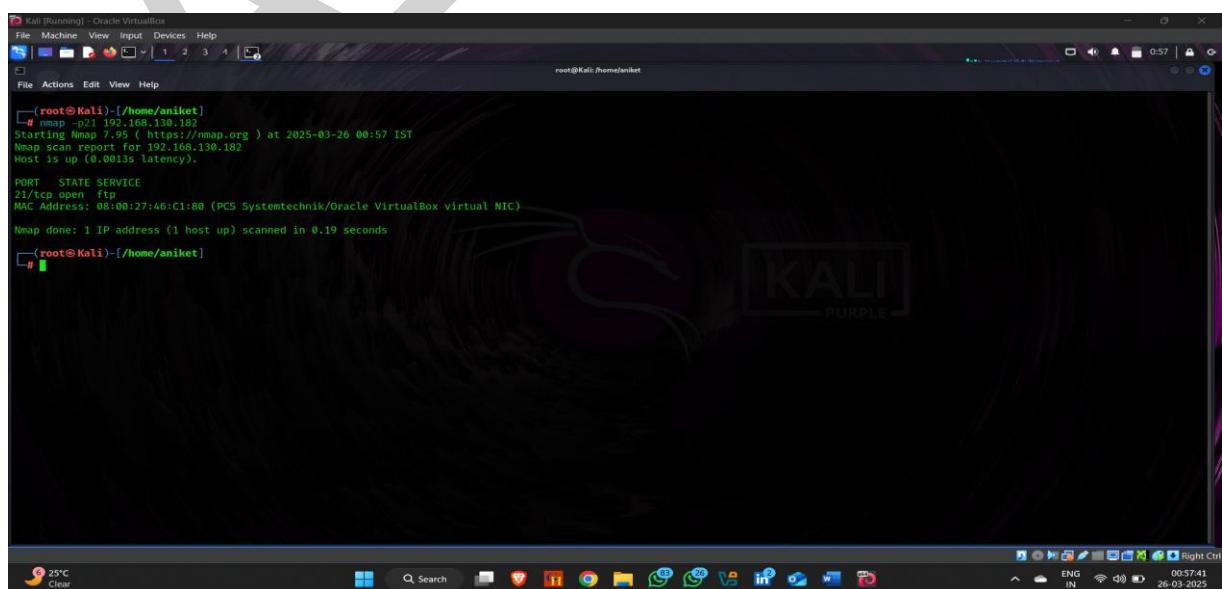


```

root@Kali:[/home/aniket]
# cd /usr/share/nmap/scripts
(root@Kali:[/usr/share/nmap/scripts]
# ls
acard-info.nse          finger.nse           http-svn-enum.nse      ms-sql-query.nse      smb-print-text.nse
address-info.nse         fingerprint-strings.nse   http-svn-info.nse       ms-sql-tables.nse    smb-pexec.nse
arp-brute.nse            firewall.nse        http-telnet-dir-traversal.nse  ms-sql-xp-cmshell.nse  smb-proto-mods.nse
arp-fuzzy.nse            firewall-cross.nse   http-trace.nse        msxgcc.nse          smb-server-stats.nse
arp-malformed-vuln.nse   firewall-master-info.nse  http-traceroute.nse   multicast-profinet-discovery.nse  smb-system-info.nse
arp-serverinfo.nse       fox-info.nse        http-unsafe-output-escaping.nse  mysql-audit.nse     smb-vuln-conficker.nse
arp-showmount.nse        freelancer-info.nse  http-trame-info.nse   mysql-brute.nse    smb-vuln-cve-2017-494.nse
ftp-auth.nse             ftp-anon.nse       http-useragent-tester.nse  mysql-databases.nse  smb-vuln-cve2009-3103.nse
ftp-brute.nse            ftp-bounce.nse     http-userdir-enum.nse   mysql-dump-hashes.nse  smb-vuln-ms06-025.nse
ftp-headers.nse          ftp-brute.nse      http-vhosts.nse       mysql-empty-password.nse  smb-vuln-ms07-029.nse
ftp-methods.nse          ftp-libopie.nse    http-virustotal.nse   mysql-info.nse      smb-vuln-ms08-007.nse
ftp-request.nse          ftp-protptd-backdoor.nse  http-wsclient.nse    mysql-injection.nse  smb-vuln-ms10-010.nse
fttseeyingyinfo.nse      ftp-syst.nse      http-wsclient-path-lm.nse  mysql-query.nse    smb-vuln-ms10-011.nse
ftpuploadinfo.nse         ftp-telepath-backdoor.nse  http-wsclient-path-lm-nse  mysql-regsvc.nse  smb-vuln-ms17-010.nse
asn-query.nse            ftp-vuln-cve2010-4221.nse  http-wsclient-path-lm-nse  mysql-users.nse   smb-vuln-webexec.nse
auth-owners.nse          ganglia-info.nse   http-wsclient-vuln-cve2009-3960.nse  mysql-variables.nse  smb-webexec-exploit.nse
auth-spoof.nse           glog-info.nse      http-wsclient-vuln-cve2010-0738.nse  mysql-vuln-cve2012-2122.nse  smb2-capabilities.nse
backorifice-brute.nse    gkrellm-info.nse   http-wsclient-vuln-cve2010-2861.nse  nat-pmp-info.nse   smb2-security-mode.nse
backorifice-info.nse     gofer.nse        http-wsclient-vuln-cve2011-3192.nse  nat-pmp-mappart.nse  smb2-time.nse
bagnet-info.nse          gosd-info.nse    http-wsclient-vuln-cve2011-3368.nse  nbd-info.nse      smb2-vuln-upnpme.nse
banner.nse               hadoop-data-node-info.nse  http-wsclient-vuln-cve2012-1823.nse  nbtstat.nse      setp-brute.nse
bitcoind-greaddr.nse    hadoop-jobtracker-info.nse  http-wsclient-vuln-cve2013-0156.nse  nbtstat-and-ipconfig.nse  setp-enum-users.nse
bitcoind-htc.nse         hadoop-mapreduce-info.nse  http-wsclient-vuln-cve2013-0620.nse  nbtstat-and-ipconfig.nse  setp-open-relay.nse
bitsnmpc-info.nse        hadoop-secondary-namenode-info.nse  http-wsclient-vuln-cve2013-0951.nse  ncp-serverinfo.nse  setp-strangeport.nse
bittorrent-discovery.nse hadoop-tasktracker-info.nse  http-wsclient-vuln-cve2014-2126.nse  ndmp-fs-info.nse   setp-vuln-cve2010-4344.nse
Dimp-discover.nse       harpoon-info.nse   http-wsclient-vuln-cve2014-2127.nse  ndmp-version.nse  smtp-vuln-cve2011-1720.nse
broadcast-ataoe-discover.nse hbase-master-info.nse  http-wsclient-vuln-cve2014-2128.nse  nessus-brute.nse  smtp-vuln-cve2011-1764.nse
broadcast-avahi-dos.nse  hbase-region-info.nse  http-wsclient-vuln-cve2014-3704.nse  nessus-xmlrpc-brute.nse  sniffer-detect.nse
broadcast-bjnp-discover.nse hdtemp-info.nse    http-wsclient-vuln-cve2014-8877.nse  netbus-auth-bypass.nse  smmp-brute.nse
broadcast-dhcp-discover.nse hostmap-afp.nse     http-wsclient-vuln-cve2015-1427.nse  netbus-brute.nse   smmp-hhdc-logins.nse
broadcast-dhcpo-discover.nse hostmap-bfk.nse    http-wsclient-vuln-cve2015-1635.nse  netbus-info.nse   smmp-info.nse
broadcast-dns-service-discovery.nse hostmap-crtsh.nse  http-wsclient-vuln-cve2017-1004000.nse  netbus-version.nse  00:43:37
broadcast-dropbox-listener.nse hostmap-rotbox.nse  http-wsclient-vuln-cve2017-5638.nse  nospose-brute.nse  26-03-2025
broadcast-eigrp-discovery.nse http-affiliate-id.nse  http-wsclient-vuln-cve2017-5689.nse  nbtstat.nse

```

Step 3 : Kindly check the port status is open or closed .



```

root@Kali:[/home/aniket]
# nmap -p21 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 00:57 IST
Nmap scan report for 192.168.130.182
Host is up (0.0013s latency).

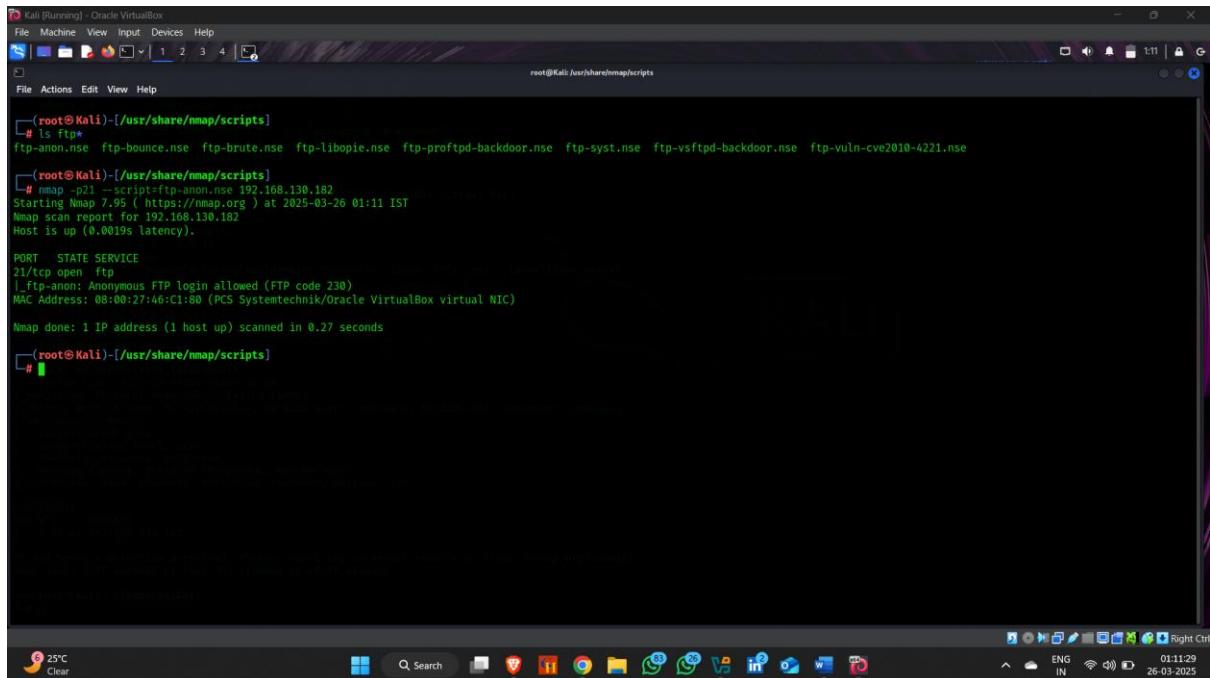
PORT      STATE SERVICE
21/tcp    open  ftplib
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

```

Step 4 : after going to the nmap directory , type ls and service name that you want a script

Example – ls ftp* (* for all ftp scripts)



```
(root@Kali:[/usr/share/nmap/scripts]
# ls 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
# nmap -p21 --script=ftp-anon.nse 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:11 IST
Nmap scan report for 192.168.130.182
Host is up (0.0019s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

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

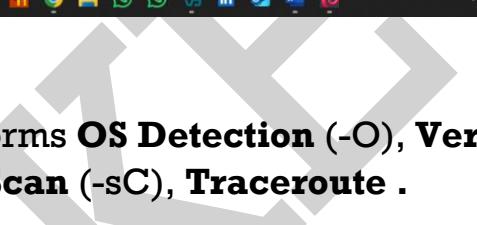
- **-T < 0 – 5 >** -- the **-T<0-5>** option controls the **timing template**, which adjusts the **speed, aggressiveness, and stealth** of your scan.

Use **-T0 or -T1** -- for **maximum stealth** in security assessments.

Use **-T2 or -T3** -- for **internet-facing** targets to reduce detection risk.

Use **-T4** -- for fast scans **local networks**.

Avoid **-T5** -- unless you're scanning a **test environment or trusted network**.



Kali [Running] - Oracle VirtualBox

```
(root@Kali:[/home/aniket]
# nmap -sS -p1-1000 -T4 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:04 IST
Nmap scan report for 192.168.130.182
Host is up (0.0038s latency).
Not shown: 988 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
513/tcp   open  login
514/tcp   open  shell
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

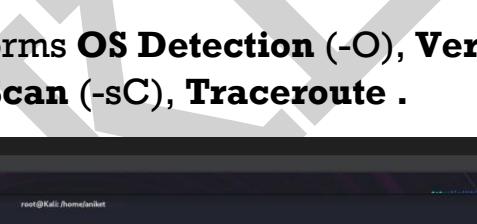
```

(root@Kali:[/home/aniket]

25°C Clear

ENG IN 01:04:53 26-03-2025

- **-A -- The -A option performs OS Detection (-O), Version Detection (-sV), Script Scan (-sC), Traceroute .**



Kali [Running] - Oracle VirtualBox

```
(root@Kali:[/home/aniket]
# nmap -A -p1-1000 -T4 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:09 IST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 01:09 (0:00:06 remaining)
Nmap scan report for 192.168.130.182
Host is up (0.0020s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsFTpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.130.192
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfc:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 5e:56:24:0f:11:id:de:a7:20:ae:61:b1:24:d3:e8:f3 (RSA)
23/tcp    open  telnet
35/tcp    open  domain
53/tcp    open  domain      ISC BIND 9.7.2
| dns-nsid:
| bind-version: 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp  rpcbind

```

25°C Clear

ENG IN 01:15:43 26-03-2025

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 4425/tcp mountd
| 100006 1,2,3 59552/udp mountd
| 100021 1,3,4 513/udp nmbnrg
| 100021 1,3,4 52237/tcp nlocknrg
| 100024 1 34075/udp status
| 100024 1 49581/tcp status
139/tcp open netbios-ssn Samba smbd 3.0 - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open tcprwapped
MAC Address: 0B:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
OS Details: 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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery
|   | OS: Unix (Samba 3.0.20-Debian)
|   | Computer name: metasploitable
|   | NetBIOS computer name:
|   | Domain name: localdomain
|   | FQDN: metasploitable.localdomain
|   | System time: 2025-03-25T15:39:05-04:00
|   | smb2-time: Protocol negotiation failed (SMB2)
|   | nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|   | smb-security-mode:
|   |   account_name: guest
|   |   authentication_level: user
|   |   challenge_response: supported
|   |   message_signing: disabled (dangerous, but default)
|   | clock-skew: mean: 1h59m44s, deviation: 2h49m43s, median: -10s
```

HANTALY

3. Firewall / IDS And Spoofing Using Nmap.

A **firewall** is a security system that monitors and controls incoming and outgoing network traffic based on predefined rules. It acts as a **barrier** between a trusted internal network and untrusted external networks.

An **IDS** is a system that monitors network traffic for suspicious activity and alerts administrators. It doesn't block traffic but detects threats.

Spoofing tricks the target system by forging source information (like IP addresses or MAC addresses) to disguise your true identity.

Objectives –

1. Network Protection and Threat Mitigation.
2. Access Control and Traffic Management.
3. Performance Optimization and Security Testing.
4. Risk Assessment and Vulnerability Testing.

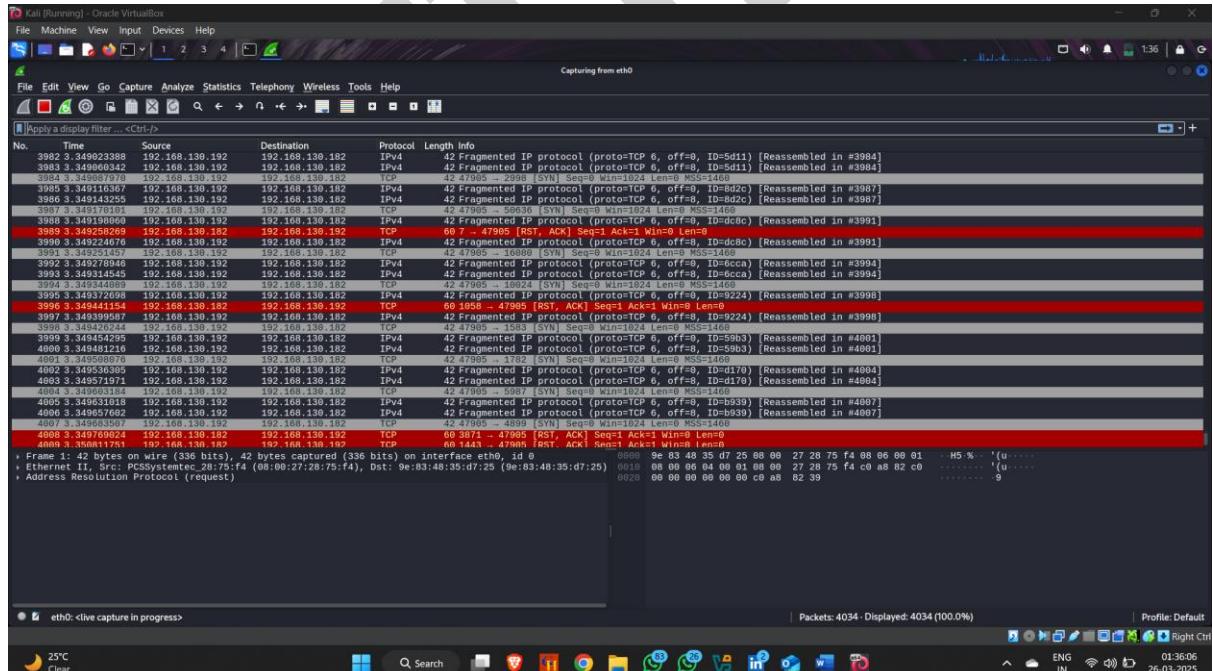
Common Usage Command –

- -f -- Fragmentation
- -mtu -- maximum transmission unit.
- -g --- Source Port Manipulation.
- --spoof-mac --- MAC Address Spoofing.
- -D -- Decoy.

- **-f** -- The **-f** option in Nmap enables **packet fragmentation**, which breaks your scan packets into smaller pieces.

Kali (Running) - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap -f 192.168.130.182
Starting Nmap 7.91 (https://nmap.org) at 2025-03-26 01:36 IST
Nmap scan report for 192.168.130.182
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
PORT STATE SERVICE
21/tcp open ftplib
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
113/tcp open rpdbind
330/tcp open memcached-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
109/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
321/tcp open cproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8180/tcp open unknown
MAC Address: 08:00:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds

#



- **--mtu** -- The **--mtu** option in Nmap allows you to specify a custom **MTU (Maximum Transmission Unit)** value for your scan packets.

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@Kali:[/home/aniket]
# nmap -p21 --mtu 16 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:38 IST
Nmap scan report for 192.168.130.182
Host is up (0.0018s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

```

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.130.254	224.0.0.251	IGMP	415 Standard query response 0x0000 PTR HP._dnsvc._tcp.local SRV 0 0 7680 HP.local TXT
2	0.001589110	192.168.130.254	224.0.0.251	MDNS	80 Standard query 0x0000 ANY HP._dnsvc._tcp.local "QM" question
3	0.254539593	192.168.130.254	224.0.0.251	MDNS	80 Standard query 0x0000 ANY HP._dnsvc._tcp.local "QM" question
4	0.507392091	192.168.130.254	224.0.0.251	MDNS	80 Standard query 0x0000 ANY HP._dnsvc._tcp.local "QM" question
5	0.760244591	192.168.130.254	224.0.0.251	MDNS	80 Standard query 0x0000 ANY HP._dnsvc._tcp.local "QM" question
6	0.764273787	192.168.130.254	224.0.0.251	MDNS	416 Standard query response 0x0000 SRV cache flush HP._dnsvc._tcp.local SRV, cache flush 0 0 7680 HP.local TXT, cache flush A, cache flush f...
7	2.282097634	PCSSystemtec_28:75:.. Broadcast	ARP	42 Who has 192.168.130.182? Tell 192.168.130.192	
8	2.283523616	PCSSystemtec_46:c1:.. PCSSystemtec_28:75:.. ARP	ARP	60 192.168.130.182 is at 08:00:27:46:c1:80	
9	2.3665596489	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d:.. DRX	DRX	108 Standard query 0x0000 PTR 192.168.169.192.in-addr.arpa	
10	3.000000000	2401:4900:57bc:4e5d:2401:4900:57bc:4e5d:.. DRX	DRX	108 Standard query 0x0000 response for name server PTR 192.168.169.192.in-addr.arpa	
11	3.101031443	192.168.130.172	192.168.130.192	TCP	50 Fragments (IP protocol 1, offset 0x10, id=47c), (Reassembled in #4)
12	2.419285141	192.168.130.192	192.168.130.182	TCP	42 49835 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	2.419285141	192.168.130.192	192.168.130.182	TCP	68 21 49835 ACK=1 Win=1024 Len=0 MSS=1460
14	2.422337293	192.168.130.192	192.168.130.182	TCP	14 49835 - 23 [RST] Seq=1 Win=0 Len=0
15	7.418328977	PCSSystemtec_46:c1:.. PCSSystemtec_28:75:.. ARP	ARP	69 Who has 192.168.130.192? Tell 192.168.130.182	
16	7.418357428	PCSSystemtec_28:75:.. PCSSystemtec_46:c1:.. ARP	ARP	42 192.168.130.192 is at 08:00:27:28:75:f4	
17	7.5309376209	Fee0:a0:27ff:fe20:2401:4900:57bc:4e5d:.. ICMPv6	ICMPv6	86 Neighbor Solicitation for 2401:4900:57bc:4e5d:68 from 08:00:27:28:75:f4	
18	7.5945996309	2401:4900:57bc:4e5d:.. fe00:0:0:0:0:0:0:68	ICMPv6	78 Neighbor Advertisement 2401:4900:57bc:4e5d:68 (rtr, sol)	

> Frame 11: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface eth0, id 0
 Ethernet II, Src: PCSSystemtec_28:75:f4 (08:00:27:28:75:f4), Dst: PCSSystemtec_46:c1:80 (08:00:27:46:c1:80)
 Internet Protocol Version 4, Src: 192.168.130.182, Dst: 192.168.130.102
 Data (36 bytes)
 Data: 0x0000154f92ff0f00000000000000004000
 [length: 16]

- **-g** -- The **-g** option in Nmap allows you to specify a **source port** for your outgoing packets.

```
(root@Kali:[/home/aniket]
# nmap -sS -p80 -g23 192.168.130.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 01:45 IST
Nmap scan report for 192.168.130.182
Host is up (0.0027s latency).

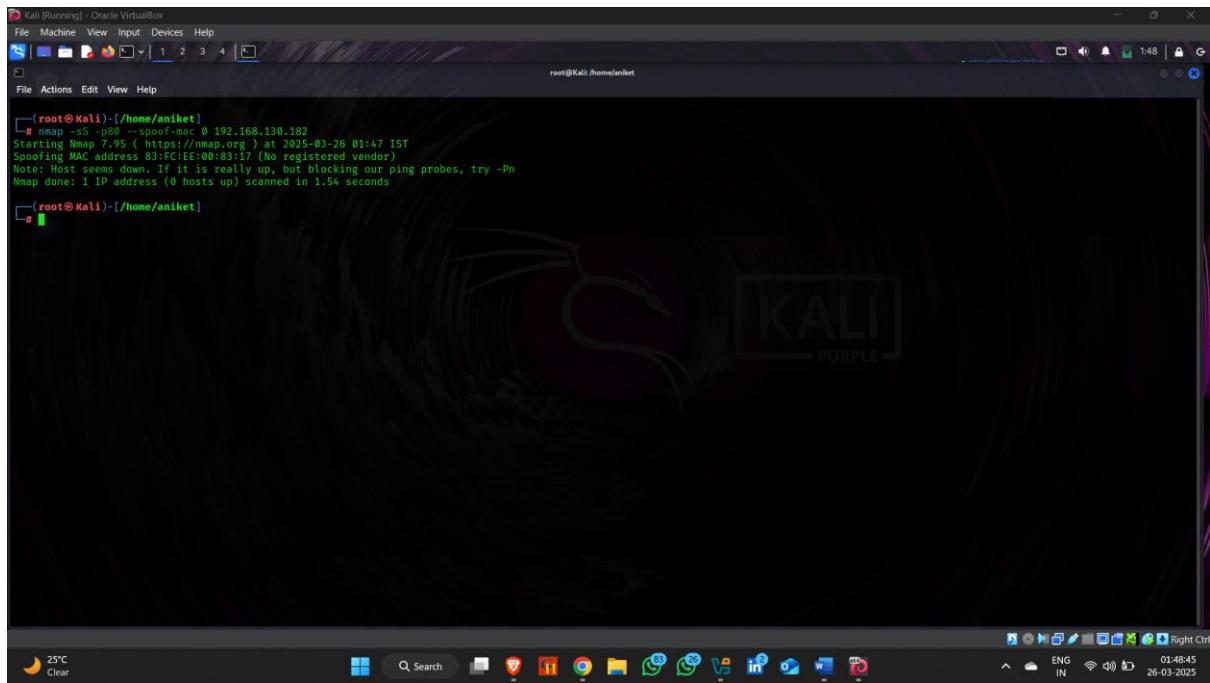
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
(root@Kali:[/home/aniket]
```

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.130.192	192.168.130.182	HTTP	334 bytes on wire (267 bits), 334 bytes captured (267 bits) on interface eth0, id 0x0000000000000000
2	0.067199536	PCSSystemtec_28:75:.. Broadcast		ARP	64 who has 192.168.130.182? Tell 192.168.130.192
3	0.068938484	PCSSystemtec_46:c1:.. PCSSystemtec_28:75:.. ARP		ARP	42 who has 192.168.130.182? Is at 08:00:27:46:c1:180
4	1.14841067	2401:4900:57bc:4e5d.. 2401:4900:57bc:4e5d.. DNS		DNS	108 Standard query 0x009e PTR 192.130.168.192.in-addr.arpa
5	1.14841067	2401:4900:57bc:4e5d.. 2401:4900:57bc:4e5d.. DNS		DNS	108 Standard query 0x009e PTR 192.130.168.192.in-addr.arpa
6	0.170843757	192.168.130.192	192.168.130.182	TCP	58 21 - 80 SYN ACK Seq=0 ACK=1 Win=1024 Len=0 MSS=1460
7	0.171387452	192.168.130.192	192.168.130.182	TCP	60 80 - 21 [SYN, ACK] Seq=0 ACK=1 Win=5840 Len=0 MSS=1460
8	0.171440585	192.168.130.192	192.168.130.182	TCP	54 21 - 80 [SST] Seq=1 Win=3 Len=0
9	0.171440585	PCSSystemtec_28:75:.. 0e:83:40:35:02:28		ARP	42 who has 192.168.130.182? Tell 192.168.130.192
10	0.1735536453	192.168.130.192	192.168.130.182	ARP	60 192.168.130.182 57 - at 0e:83:40:35:02:28
11	0.201998218	fe80::a06:27ff:fe28.. 2401:4900:57bc:4e5d.. ICMPv6		ICMPv6	86 Neighbor Solicitation for 2401:4900:57bc:4e5d::68 from 00:00:27:28:75:f4
12	0.297262020	2401:4900:57bc:4e5d.. fe80::a06:27ff:fe28.. ICMPv6		ICMPv6	78 Neighbor Advertisement 2401:4900:57bc:4e5d::68 (rtr, sol)

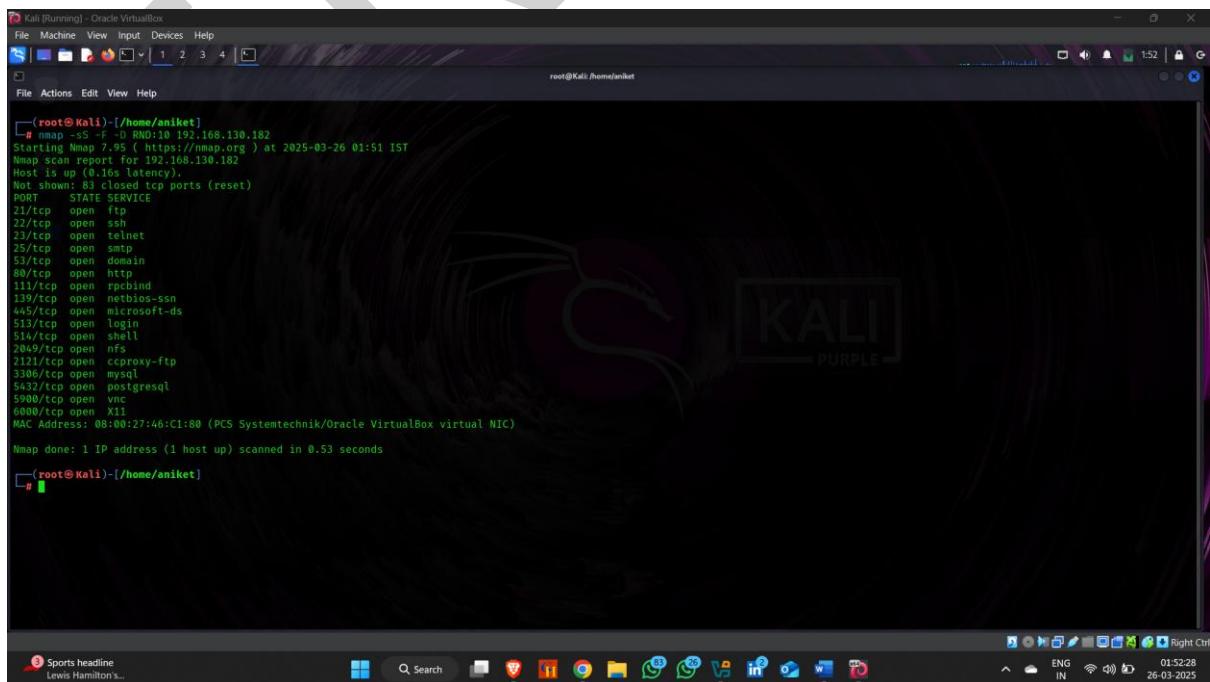
Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_28:75:f4 (08:00:27:28:75:f4), Dst: PCSSystemtec_46:c1:80 (08:00:27:46:c1:80)
Transmission Control Protocol, Src Port: 21, Dst Port: 80, Seq: 1, Len: 0
Source Port: 21
Destination Port: 80
[...]
Conversation completeness: Incomplete (35)
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (Raw): 000154211
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (Raw): 0
[...]
eth0 <live capture in progress>

- **--spoof-mac** -- The **--spoof-mac** option in Nmap allows you to **fake** (spoof) your **MAC address** during a scan.

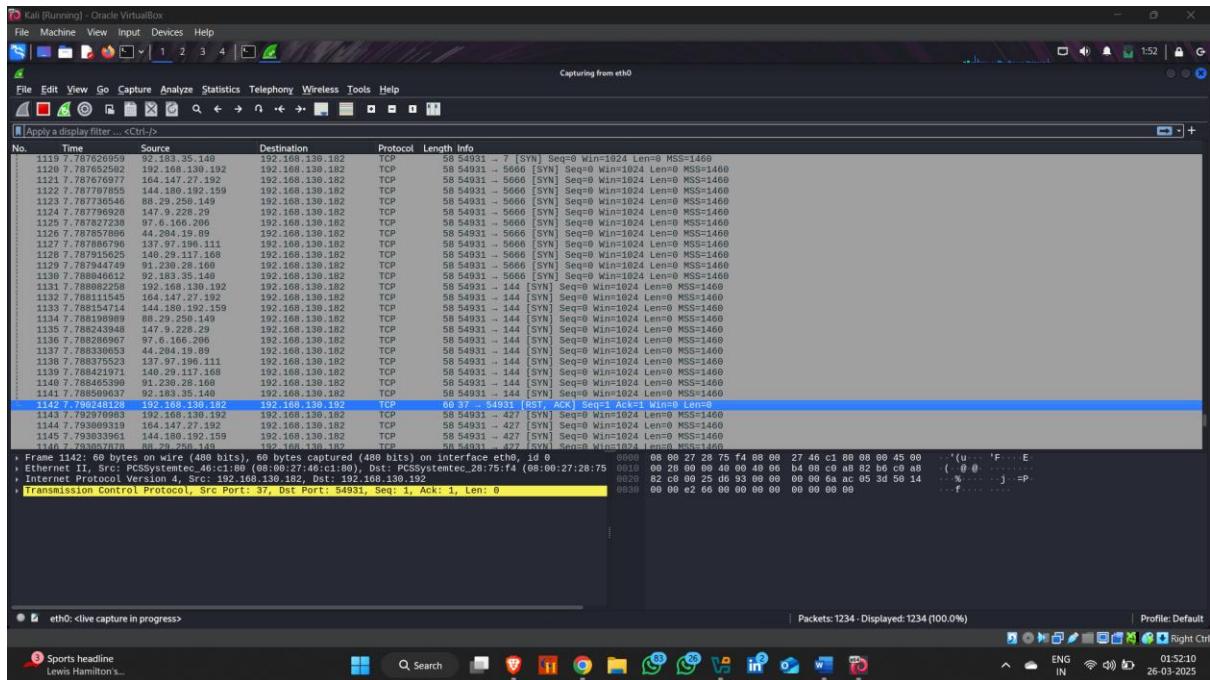


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali:~# nmap -S -p80 --spoof-mac 0 192.168.130.182
Starting Nmap 7.95 (https://nmap.org) at 2025-03-26 01:47 IST
Spoofing MAC address 83:FC:EE:00:83:17 (No registered vendor)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.54 seconds

- **-D** -- The **-D** option in Nmap is used to perform a **decoy scan**, where multiple **fake IP addresses** (decoys) are added to mask the real source of the scan.



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali:~# nmap -S -f -D RND:10 192.168.130.182
Starting Nmap 7.95 (https://nmap.org) at 2025-03-26 01:51 IST
Nmap scan report for 192.168.130.182
Host is up (0.16s latency).
Not shown: 83 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
513/tcp open login
514/tcp open shell
2000/tcp open nfs
3121/tcp open cprox-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
MAC Address: 08:00:27:46:CI:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds



HANITY

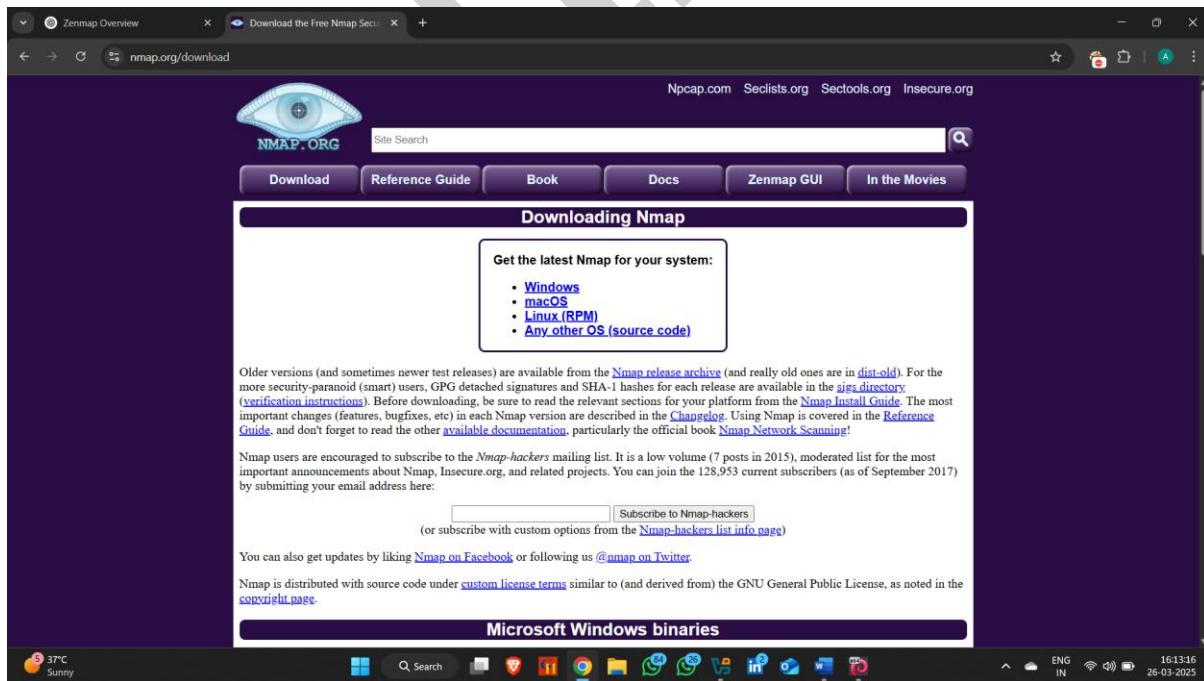
Network Scanning Using Zenmap.

Zenmap is the official graphical user interface (GUI) for **Nmap** (Network Mapper), a powerful open-source tool used for network discovery and security auditing.

How to use it - -

Step 1: Download Zenmap in Windows .

- Visit the official Nmap website :
<https://nmap.org/download.html>
- Scroll down to the Windows Binaries section.
- Download the Nmap-<version>-setup.exe installer (this includes Zenmap in the package).



Download Zenmap in Kali Linux .

- Step 1: Update Your System.

```
sudo apt update && sudo apt upgrade -y
```

- Step 2: Install Zenmap.

```
sudo apt install zenmap -y
```

- Step 3 : Download the .deb package for Zenmap:

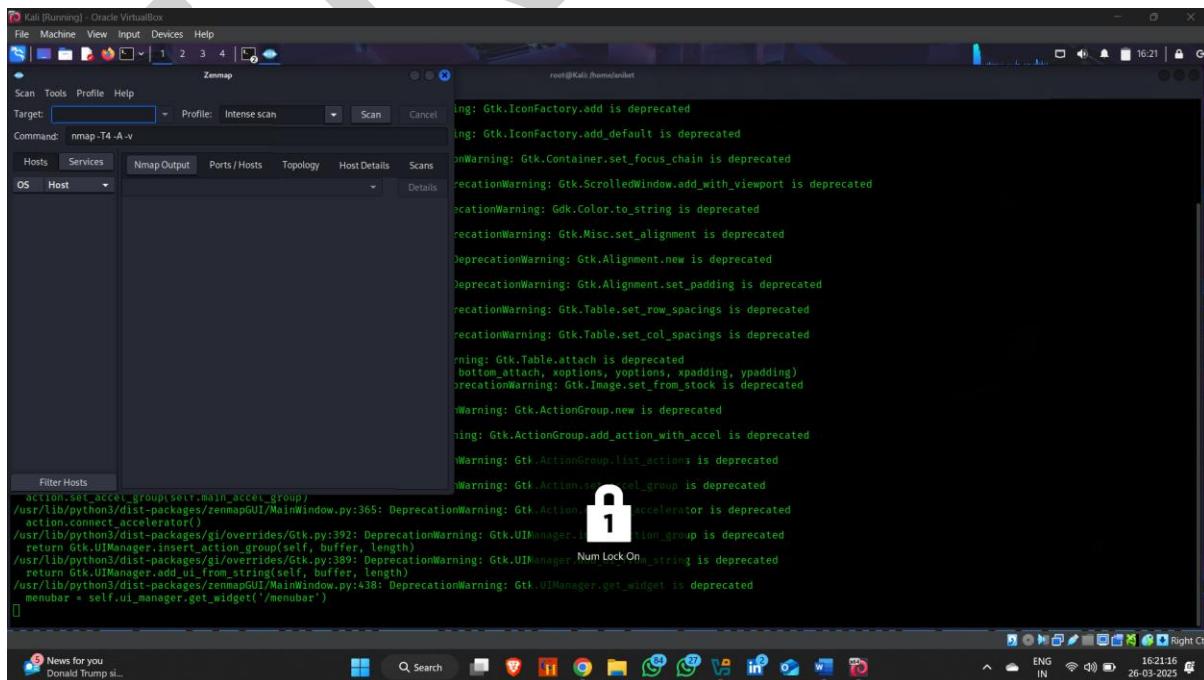
```
wget https://old.kali.org/kali/pool/main/n/nmap/zenmap\_7.80-1\_all.deb
```

- Step 4 : install the downloaded package:

```
sudo dpkg -i zenmap_7.80-1_all.deb
```

- Step 5 : Run Zenmap

```
sudo zenmap
```



The screenshot shows the Kali Linux desktop environment with the Zenmap interface open. The target host is set to 'certifiedhacker.com'. The scan command used is 'nmap -sS -sV -v certifiedhacker.com'. The results pane displays a detailed list of open ports, their states, services, and versions. Key findings include:

- Port 21/tcp: Open, Service is Pure-FTPd
- Port 22/tcp: Open, Service is OpenSSH 7.4 (protocol 2.0)
- Port 25/tcp: Open, Service is Exim smtpd 4.90-1
- Port 70/tcp: Open, Service is ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
- Port 80/tcp: Open, Service is Apache httpd
- Port 110/tcp: Open, Service is Dovecot pop3d
- Port 143/tcp: Open, Service is Dovecot imapd
- Port 443/tcp: Open, Service is Apache httpd
- Port 465/tcp: Open, Service is SSL/TLS
- Port 587/tcp: Open, Service is TCPWRAPPED
- Port 993/tcp: Open, Service is Dovecot imapd
- Port 995/tcp: Open, Service is Dovecot pop3d
- Port 2222/tcp: Open, Service is OpenSSH 7.4 (protocol 2.0)
- Port 3306/tcp: Open, Service is MySQL 5.7.23-01
- Port 5432/tcp: Open, Service is PostgreSQL DB

The output also includes service fingerprints and a note about Kerberos support.

Note :- Zenmap, on the other hand, is simply the graphical user interface (GUI) for Nmap. While Zenmap offers the same scanning capabilities as Nmap,

it provides a user-friendly interface that makes it easier for less experienced users to run scans, visualize results, and compare scan outputs.

Network Scanning Using Hping3.

Hping3 is a powerful command-line network tool used for security auditing, network testing, and troubleshooting. It is particularly effective for crafting and sending custom TCP/IP packets, making it a versatile choice for both attackers.

Installation - :

- **Step 1: Update the System.**

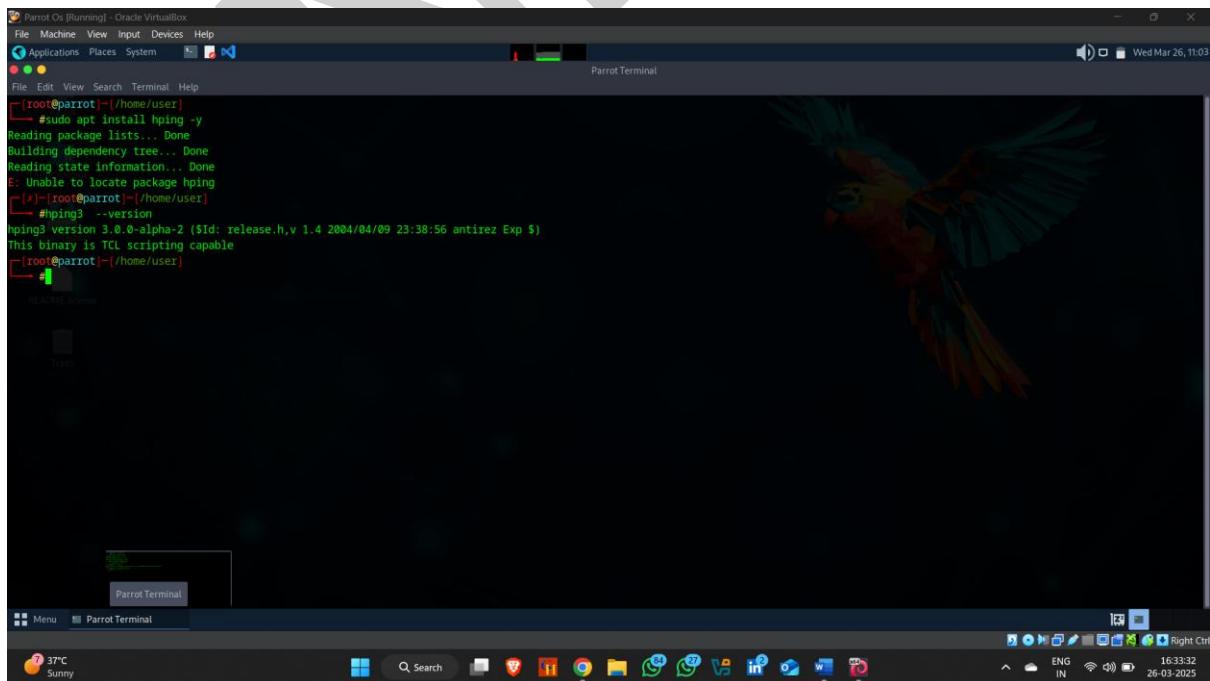
```
sudo apt update && sudo apt upgrade -y.
```

- **Step 2: Install Hping3**

```
sudo apt install hping3 -y
```

- **Step 3: Verify the Installation**

```
hping3 --version
```

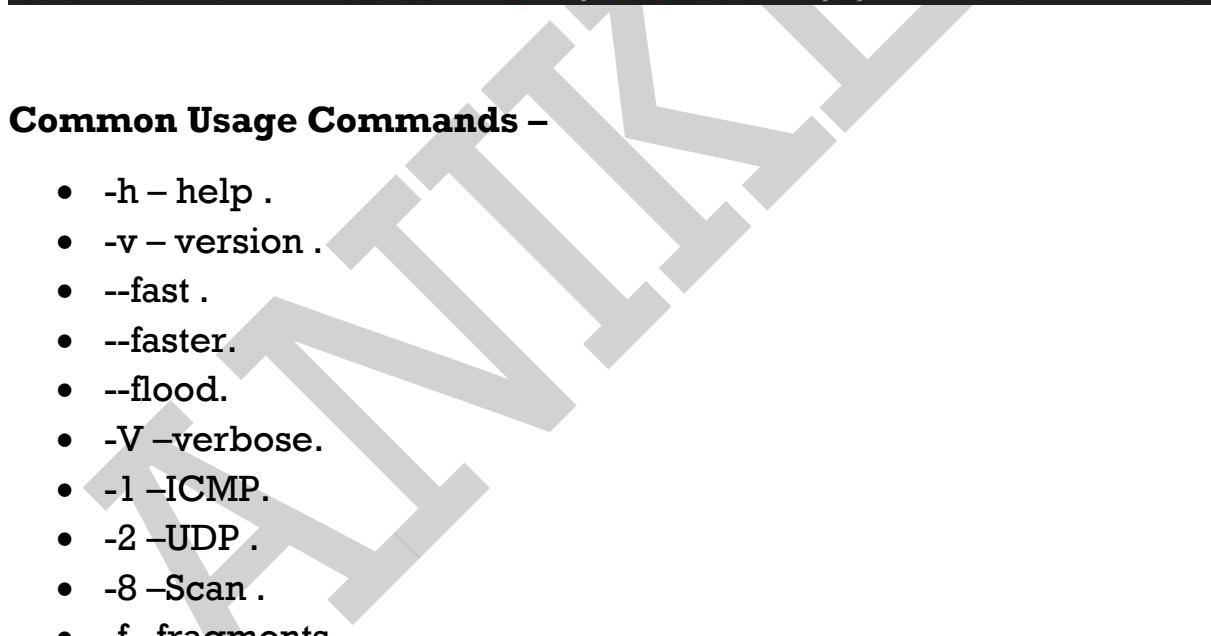


The screenshot shows a terminal window titled "ParrotTerminal" running on Parrot OS. The terminal displays the following command and its output:

```
#sudo apt install hping -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package hping
#hping3 --version
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
#
```

The terminal window is located on a desktop environment with a parrot logo wallpaper. The desktop bar at the bottom shows various icons and system status.

- Use Man hping3 -- To show detail about hping3 .

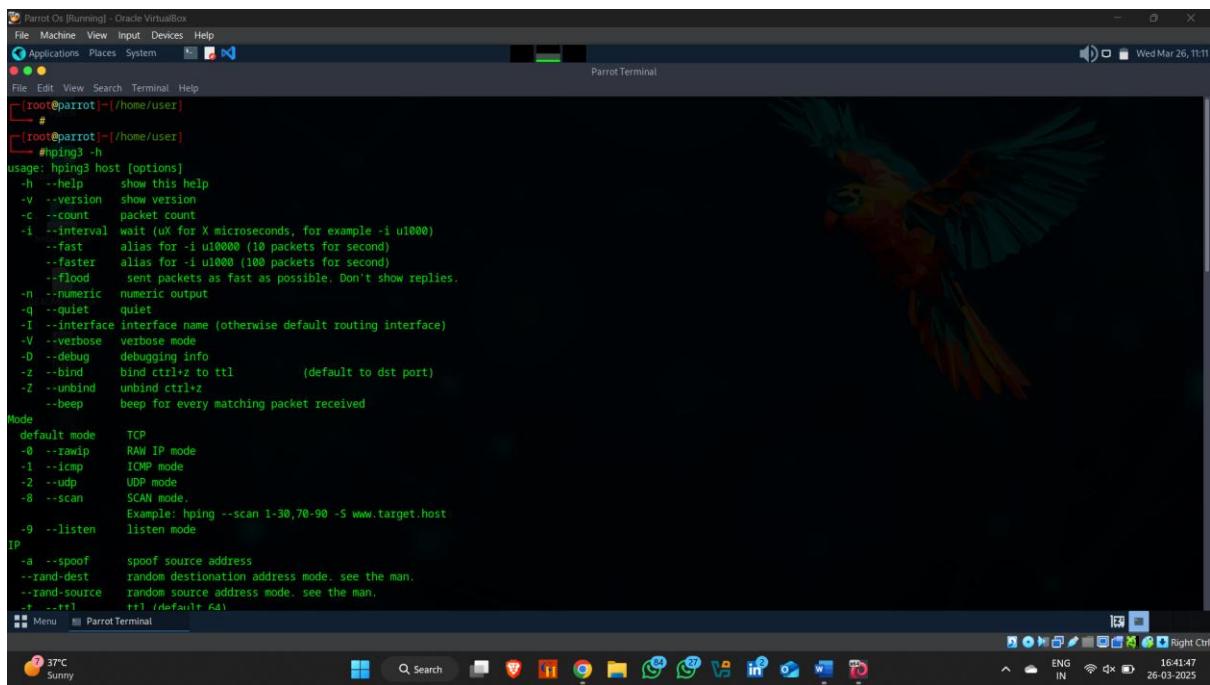


Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
HPING3(8) System Manager's Manual HPING3(8)
NAME
hping3 - send (almost) arbitrary TCP/IP packets to network hosts
SYNOPSIS
hping3 [-hvnqV0z01ZWRfxyKQPSRPAUXyJBuTG] [-c count] [-i wait] [-f fast] [-I interface] [-g signature] [-a host] [-t ttl] [-N ip id] [-M ip protocol] [-g flagoff] [-m mtu] [-o tos] [-C icmp type] [-K icmp code] [-s source port] [-p[+] dest port] [-w tcp window] [-O tcp offset] [-M tcp sequence number] [-L tcp ack] [-d data size] [-E filename] [-e signature] [-i icmp-ipver version] [--icmp-iphlen length] [--icmp-iplen length] [--icmp-ipid id] [--icmp-ipproto protocol] [--icmp-csum checksum] [--icmp-ts] [--icmp-addr] [--tcpexitcode] [--tcp-mss] [--tcp-timestamp] [--tr-stop] [--tr-keep-ttl] [--tr-no-rtt] [--rand-dest] [--rand-source] [--beep] hostname
DESCRIPTION
hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff:
- Test firewall rules
- Advanced port scanning
- Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
- Path MTU discovery
- Transferring files between even really fascist firewall rules.
- Traceroute-like under different protocols.
- Firewall-like usage.
- Remote OS fingerprinting.
- TCP/IP stack auditing.
- A lot of others.
It's also a good didactic tool to learn TCP/IP. hping3 is developed and maintained by antirez@invece.org and is licensed under GPL version 2. Development is open so you can send me patches, suggestion and affronts without inhibitions.
Manual page hping3(8) line 1 (press h for help or q to quit)

Common Usage Commands –

- **-h – help .**
- **-v – version .**
- **--fast .**
- **--faster.**
- **--flood.**
- **-V –verbose.**
- **-l –ICMP.**
- **-2 –UDP .**
- **-8 –Scan .**
- **-f –fragments.**
- **-S – SYN Flag**
- **-A – ACK Flag**
- **-U – URG Flag**
- **-R – RST Flag**
- **-P – PUSH Flag**
- **-X – Xmass**

- **-h – help**

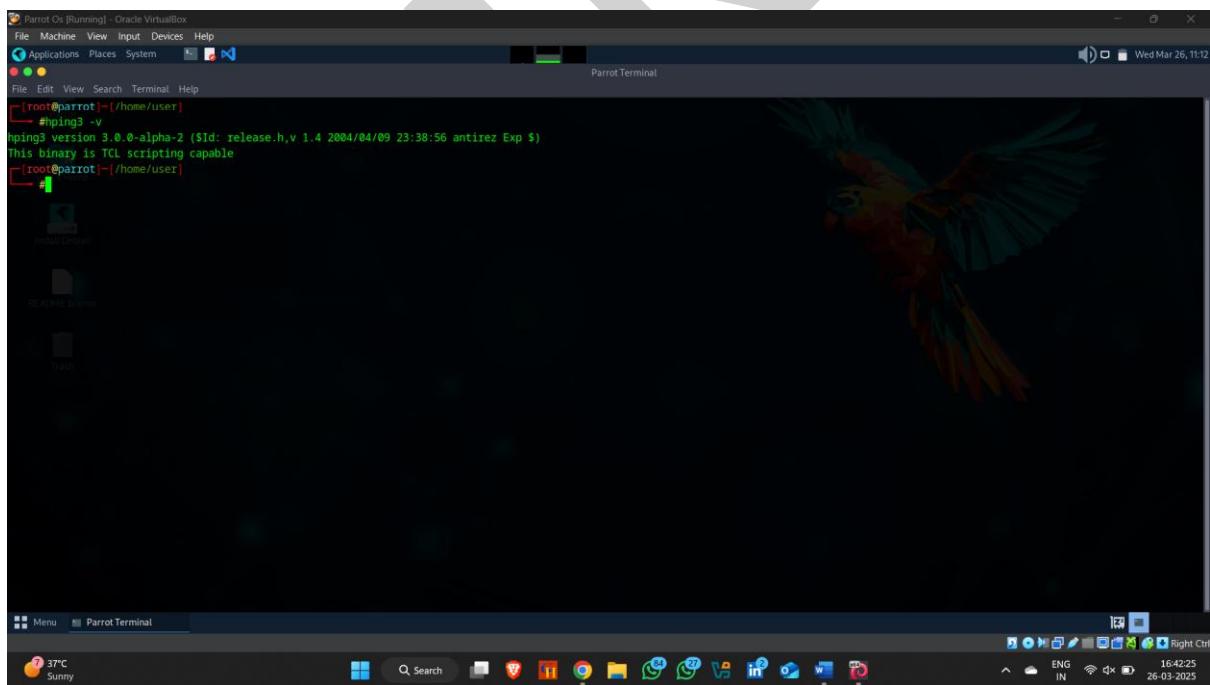


```
[root@parrot]~[~/home/user]
└── #
[root@parrot]~[~/home/user]
└── #hping3 -h
usage: hping3 host [options]
  -h --help      show this help
  -v --version   show version
  -c --count     packet count
  -i --interval  wait (uX for X microseconds, for example -i u1000)
  --fast         alias for -i u10000 (10 packets for second)
  --faster       alias for -i u1000 (100 packets for second)
  --flood        sent packets as fast as possible. Don't show replies.
  -n --numeric   numeric output
  -q --quiet     quiet
  -I --interface interface name (otherwise default routing interface)
  -V --verbose    verbose mode
  -D --debug     debugging info
  -z --bind      bind ctrl+z to ttl          (default to dst port)
  -Z --unbind    unbind ctrl+z
  --beep        beep for every matching packet received

Mode
  default mode  TCP
  -0 --rawip    RAW IP mode
  -1 --icmp    ICMP mode
  -2 --udp     UDP mode
  -8 --scan    SCAN mode.
  Example: hping --scan 1-30,70-90 -S www.target.host
  -9 --listen   listen mode

IP
  -a --spoof    spoof source address
  --rand-dest   random destination address mode, see the man.
  --rand-source  random source address mode, see the man.
  -r --ttl     ttl (default 64)
```

- **-v -- Version**



```
[root@parrot]~[~/home/user]
└── #
[root@parrot]~[~/home/user]
└── #hping3 -v
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
[root@parrot]~[~/home/user]
└── #
```

• -l -- Sends ICMP Packets

```
#ping3 -l certifiedhacker.com
PING certifiedhacker.com (eng0s3) 162.241.216.11: icmp mode set, 28 headers + 0 data bytes
len=46 ip=162.241.216.11 ttl=255 id=3 icmp_seq=0 rtt=1514.1 ms
len=46 ip=162.241.216.11 ttl=255 id=4 icmp_seq=1 rtt=512.9 ms
len=46 ip=162.241.216.11 ttl=255 id=5 icmp_seq=2 rtt=730.7 ms
len=46 ip=162.241.216.11 ttl=255 id=6 icmp_seq=3 rtt=347.2 ms
len=46 ip=162.241.216.11 ttl=255 id=7 icmp_seq=4 rtt=366.2 ms
len=46 ip=162.241.216.11 ttl=255 id=8 icmp_seq=5 rtt=588.7 ms
len=46 ip=162.241.216.11 ttl=255 id=9 icmp_seq=6 rtt=408.1 ms
len=46 ip=162.241.216.11 ttl=255 id=10 icmp_seq=7 rtt=322.1 ms
len=46 ip=162.241.216.11 ttl=255 id=11 icmp_seq=8 rtt=448.6 ms
```

Capturing from eng0s3

No.	Time	Source	Destination	Protocol	Length	Info
10	0:398783078	fe80::93fd:81bb:90a...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
11	1.128994991	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=256/1, ttl=64 (reply in 13)
12	1.631294285	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=0/0, ttl=255 (request in 9)
13	1.631294710	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=256/1, ttl=255 (request in 11)
14	2.138127832	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=512/2, ttl=64 (reply in 15)
15	2.138127841	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=256/1, ttl=255 (request in 14)
16	2.132699999	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=768/3, ttl=64 (reply in 16)
17	3.473219798	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=768/3, ttl=255 (request in 18)
18	4.135397433	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=1024/4, ttl=64 (reply in 19)
19	4.497498247	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=1024/4, ttl=255 (request in 18)
20	5.139224960	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=1024/5, ttl=64 (reply in 21)
21	5.172885665	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=1024/5, ttl=255 (request in 20)
22	6.148289918	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=1536/6, ttl=64 (reply in 23)
23	6.545856937	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=1536/6, ttl=255 (request in 22)
24	7.146442238	10.0.2.15	162.241.216.11	ICMP	42	Echo (ping) request id=0x580b, seq=1792/7, ttl=64 (reply in 25)
25	7.146442344	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=1792/7, ttl=255 (request in 24)
26	8.158025990	162.241.216.11	10.0.2.15	ICMP	42	Echo (ping) request id=0x580b, seq=2348/8, ttl=64 (reply in 27)
27	8.591440832	162.241.216.11	10.0.2.15	ICMP	60	Echo (ping) reply id=0x580b, seq=2348/8, ttl=255 (request in 26)
28	9.197138993	162.241.216.11	10.0.2.15	ICMP	42	Echo (ping) request id=0x580b, seq=2304/9, ttl=64 (reply in 29)

Frame 3: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eng0s3, id 0

Ethernet II, Src: PosCompu_0e:51:23 (08:00:27:9e:51:23), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3

User Datagram Protocol, Src Port: 50998, Dst Port: 53

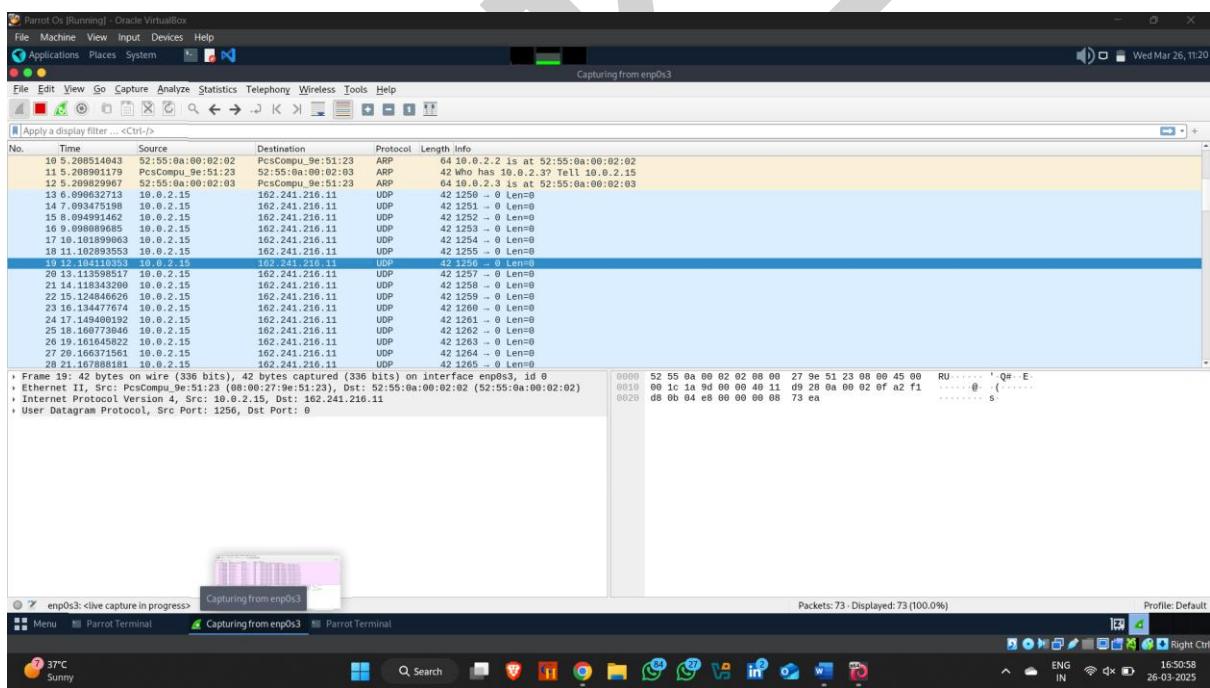
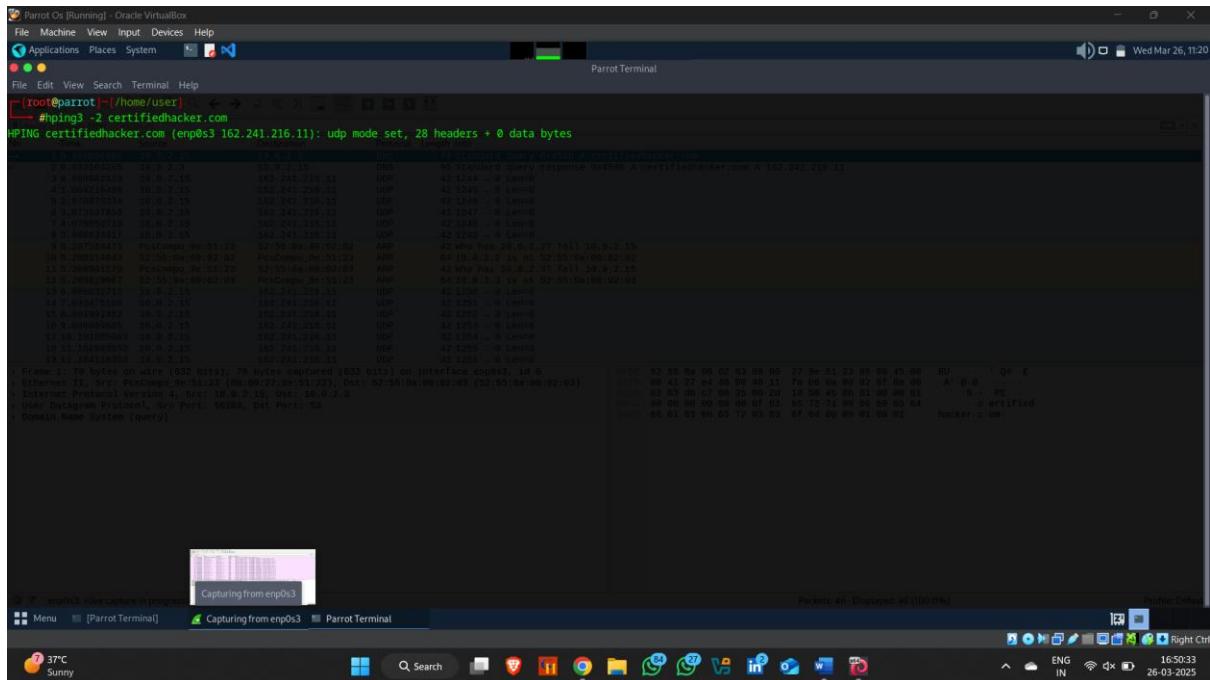
Domain Name System (query)

Packets: 55 : Displayed: 55 (100.0%)

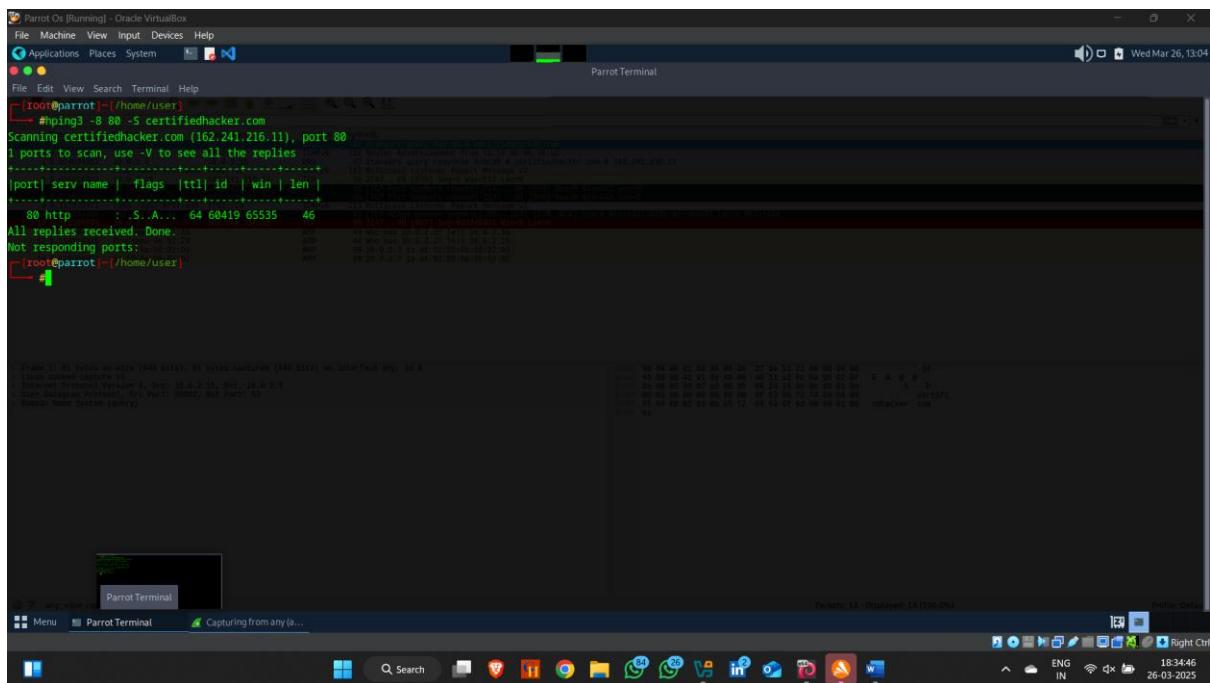
Profile: Default

37°C Sunny

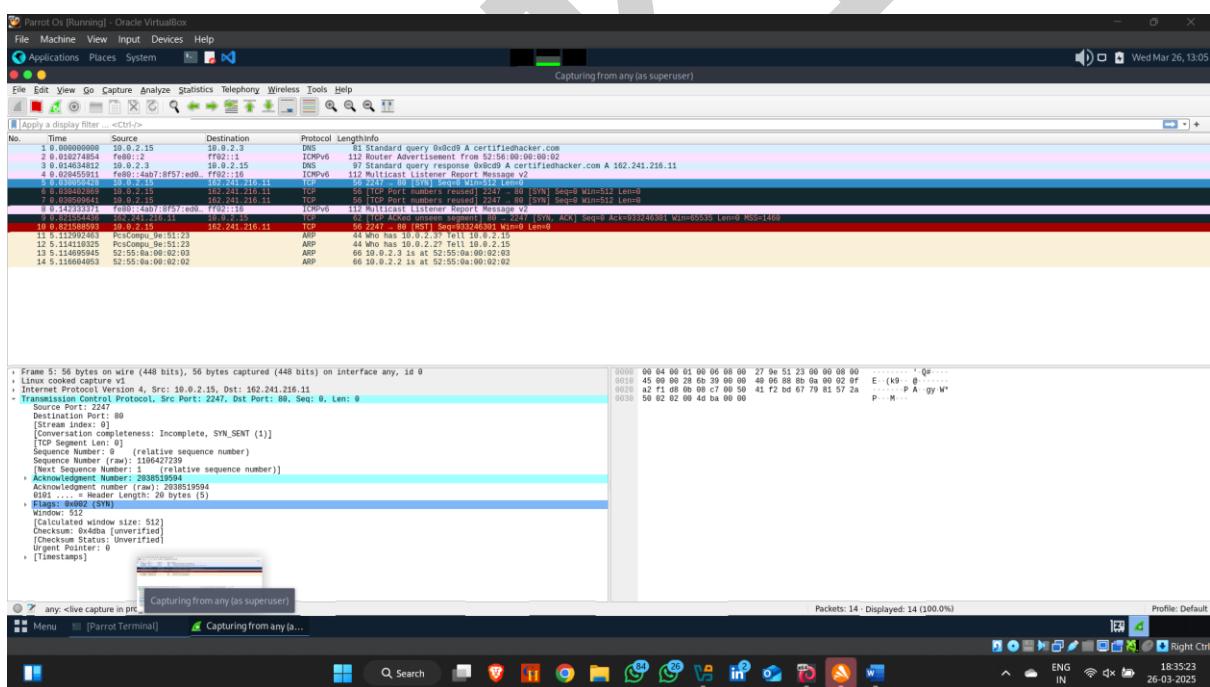
- 2 - UDP packets send



- -S – SYN Flag



```
# ping3 -8 80 -S certifiedhacker.com
Scanning certifiedhacker.com (162.241.216.11), port 80
1 ports to scan, use -V to see all the replies
[port] serv name | flags [ttl] id | win | len |
80 http : S.A. 64 60419 65535 46
All replies received. Done.
Not responding ports:
[root@parrot]~[/home/user]
```



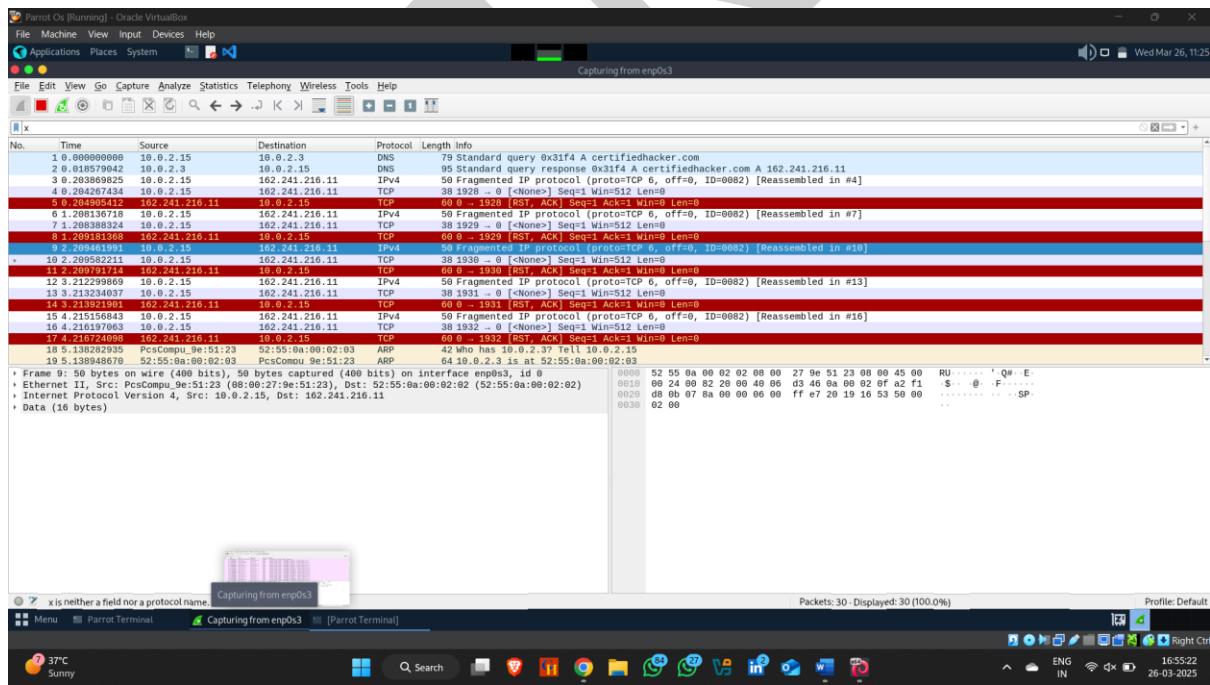
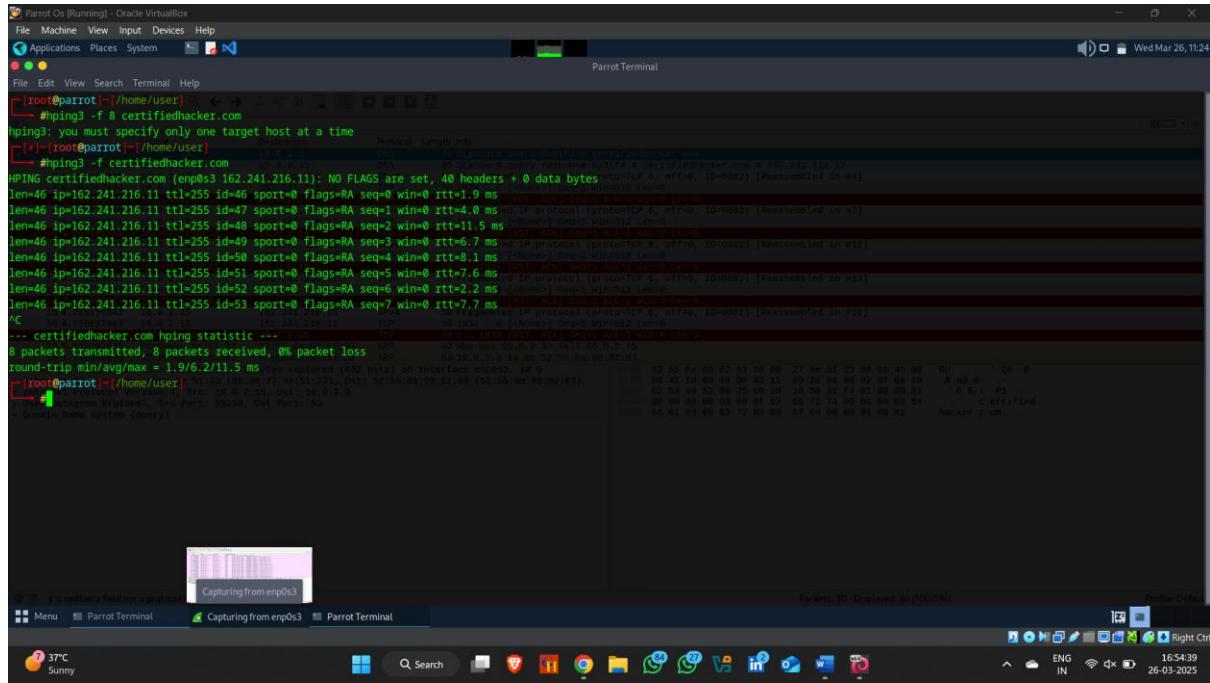
Capturing from any (as superuser)

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	10.0.2.25	10.0.2.3	DNS	64 Standard query 0x0cd9 A certifiedhacker.com
2	0.018274854	fe80::2	ff02::1	ICMPv6	12 Router Advertisement from 52:56:99:00:00:02
3	0.014634812	10.0.2.3	10.0.2.15	DNS	97 Standard query response 0x0cd9 A certifiedhacker.com A 162.241.216.11
4	0.014634821	fe80::2	ff02::1	ICMPv6	12 Multicast Listener Report Message v2
5	0.014634821	10.0.2.15	10.0.2.16:11	TCP	56 TCP Port numbers reused 2241-80 [Syn] seq=54525 len=64
6	0.014634821	10.0.2.15	10.0.2.16:11	TCP	56 TCP Port numbers reused 2241-80 [Syn] seq=54525 len=64
7	0.014634821	10.0.2.15	10.0.2.16:11	TCP	56 TCP Port numbers reused 2241-80 [Syn] seq=54525 len=64
8	0.142333771	fe80::4bb:/em0	ff02::16	ICMPv6	112 Multicast Listener Report Message v2
9	0.821598893	10.0.2.15	162.241.216.11	TCP	56 2247 > 80 [RST] Seq=53246301 Win=55535 Len=140
10	5.112992463	Pc3Compu_9e:51:23	ARP	64 Who has 10.0.2.3? Tell 10.0.2.15	
11	5.112992463	10.0.2.15	ARP	44 10.0.2.3 is at 52:55:0a:00:02:03	
12	5.114669945	52:55:0a:00:02:03	ARP	66 10.0.2.3 is at 52:55:0a:00:02:03	
13	5.114669945	52:55:0a:00:02:03	ARP	66 10.0.2.2 is at 52:55:0a:00:02:02	
14	5.116604053	52:55:0a:00:02:02	ARP	66 10.0.2.2 is at 52:55:0a:00:02:02	

Frame 5: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
 Linux cooked capture v1
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.241.216.11
 Transmission Control Protocol, Src Port: 2247, Dst Port: 80, Seq: 0, Len: 0

Source Port: 2247
 Destination Port: 80
 [String length: 0]
 [Conversation completeness: Incomplete, SYN_SENT (1)]
 [Sequence Number: 0 (relative sequence number)]
 Sequence Number (raw): 110427239
 [Acknowledge Number: 0 (relative sequence number)]
 Acknowledgment Number (raw): 203851954
 Acknowledgment Number (raw): 203851954
 Flags: 0x0002 (SYN)
 Window: 55535
 [Calculated window size: 512]
 Checksum: 0x4dba [unverified]
 [Checksum: 0x4dba unverified]
 Urgent Pointer: 0
 [Timestamps]

- **-f – fragmentation.**



Port Scanning Using Hping3

Command –

- hping3 -S -8 1-1000 <target ip or domain name>
 - ❖ -S -- Send SYN packet
 - ❖ -8 -- Scan
 - ❖ 1-1000 -- port scan 1 to 1000

Parrot OS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~ /home/user]
→ hping3 -S -8 1-1000 certifiedhacker.com
Scanning certifiedhacker.com (162.241.216.11), port 1-1000
1000 ports to scan, use -V to see all the replies
[port] serv name | flags | ttl | id | win | len |
21 ftp : .S.A... 64 768 65535 46
53 domain : .S.A... 64 1024 65535 46
143 imap2 : .S.A... 64 1280 65535 46
22 ssh : .S.A... 64 1536 65535 46
110 pop3 : .S.A... 64 1792 65535 46
443 https : .S.A... 64 2048 65535 46
465 submissions: .S.A... 64 2304 65535 46
587 submission : .S.A... 64 2560 65535 46
995 pop3s : .S.A... 64 2816 65535 46
80 http : .S.A... 64 3072 65535 46
26 telnet : .S.A... 64 3328 65535 46
993 imaps : .S.A... 64 3584 65535 46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nntp) (3) (4 echo) (5) (6 zip) (7 echo) (8) (9 discard) (10) (11 systat) (12) (13 daytime) (14) (15 netstat) (16) (17 qotd) (18) (19 chargen) (20 ftp-data) (23 telnet) (24) (25 smtp) (27) (28) (29) (30) (31) (32) (33) (34) (35) (36) (37 time) (38) (39) (40) (41) (42) (43 whois) (44) (45) (46) (47) (48) (49 tacacs) (50) (51) (52) (54) (55) (56) (57) (58) (59) (60) (61) (62) (63) (64) (65) (66) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (71) (72) (73) (74) (75) (76) (77) (78) (79 finger) (80) (82) (83) (84) (85) (86) (87) (88 kerberos) (89) (90) (91) (92) (93) (94) (95) (96) (97) (98) (99) (100) (101) (102 iso-tsap) (103) (104 acr-nema) (105) (106) (107) (108) (109) (111 sunrpc) (112) (113 auth) (114) (115) (116) (117) (118) (119 nntp) (120) (121) (122) (123 ntp) (124) (125) (126) (127) (128) (129) (130) (131) (132) (133) (134) (135 imap) (136) (137 netbios-ns) (138 netbios-dgm) (139 netbios-ssn) (140) (141) (142) (144) (145) (146) (147) (148) (149) (150) (151) (152) (153) (154) (155) (156) (157) (158) (159) (160) (161 snmp) (162 snmp-trap) (163 cisp) (164) (165) (166) (167) (168) (169) (170) (171) (172) (173) (174 mailq) (175) (176) (177 xdmcp) (178) (179 bgp) (180) (181) (182) (183) (184) (185) (186) (187) (188) (189) (190) (191) (192) (193) (194) (195) (196) (197) (198) (199 smux) (200) (201) (202) (203) (204) (205) (206) (207) (208) (209 gmp) (210 2390) (211) (212) (213) (214) (215) (216) (217) (218) (219) (220) (221) (222) (223) (224) (225) (226) (227) (228) (229) (230) (231) (232) (233) (234) (235) (236) (237) (238) (Num Lock Off) (241) (242) (243) (244) (245) (246) (247) (248) (249) (250) (251) (252) (253) (254) (255) (256) (257) (258) (259) (260) (261) (262) (263) (264) (265) (266) (267) (268) (269) (270) (271) (272) (273) (274) (275) (276) (277) (278) (279) (280) (281) (282) (283) (284) (285) (286) (287) (288) (289) (290) (291) (292) (293) (294) (295) (296) (297) (298) (299) (300) (301) (302) (303) (304) (305) (306) (307) (308) (309) (310) (311) (312) (313) (314) (315) (316) (317) (318) (319 ntn-event) (320 ntn-general) (321) (322) (323) (324) (325) (326) (327) (328) (329) (330) (331)
File Menu ParrotTerminal
File Search Applications Home Help ENG IN 18:27:29 26-03-2025

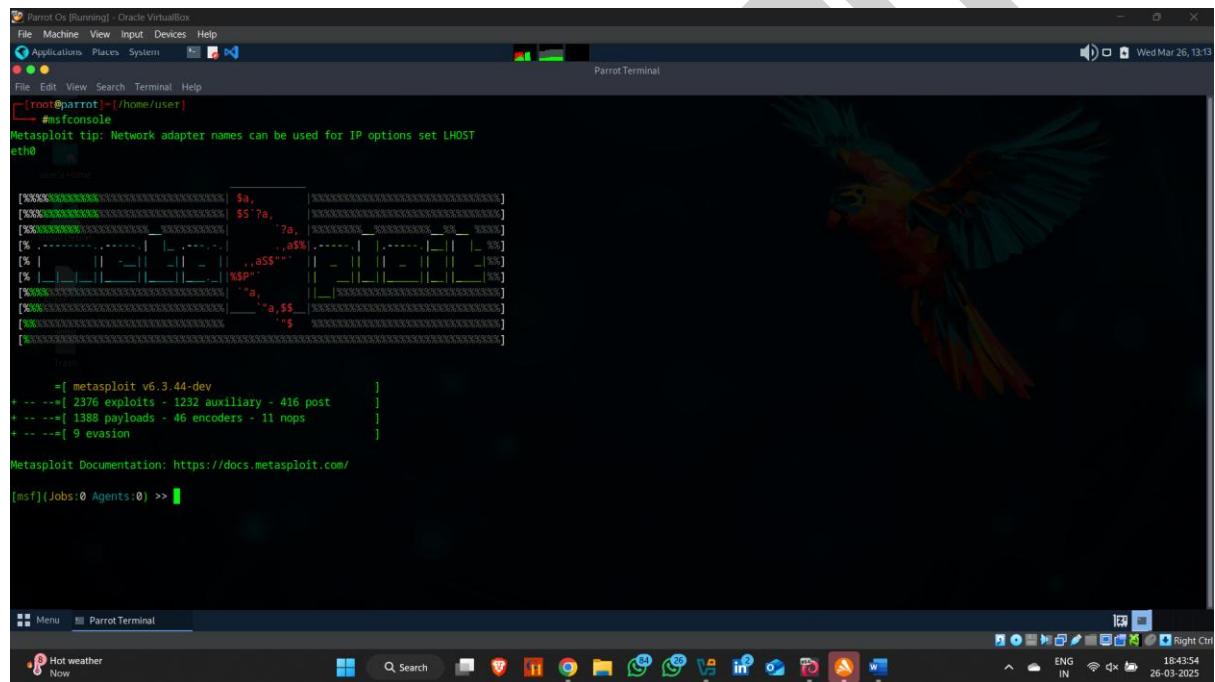
Parrot OS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System Capturing from any (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Apply a display filter: <<Ctrl>>]
No. Time Source Destination Protocol Length Info
2011 25.728525 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 9 [SYN] Seq=0 Win=512 Len=0
2012 25.728526 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 10 [SYN] Seq=1 Win=512 Len=0
2013 25.728527 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 11 [SYN] Seq=0 Win=512 Len=0
2014 25.728528 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 12 [SYN] Seq=0 Win=512 Len=0
2015 25.728529 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 13 [SYN] Seq=0 Win=512 Len=0
2016 25.728530 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 14 [SYN] Seq=0 Win=512 Len=0
2017 25.728531 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 15 [SYN] Seq=0 Win=512 Len=0
2018 25.728532 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 16 [SYN] Seq=0 Win=512 Len=0
2019 25.728533 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 17 [SYN] Seq=0 Win=512 Len=0
2020 25.728534 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 18 [SYN] Seq=0 Win=512 Len=0
2021 25.728535 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 19 [SYN] Seq=0 Win=512 Len=0
2022 25.728536 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 20 [SYN] Seq=0 Win=512 Len=0
2023 25.728537 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 21 [SYN] Seq=0 Win=512 Len=0
2024 25.728538 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 22 [SYN] Seq=0 Win=512 Len=0
2025 25.728539 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 23 [SYN] Seq=0 Win=512 Len=0
2026 25.728540 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 24 [SYN] Seq=0 Win=512 Len=0
2027 25.728541 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 25 [SYN] Seq=0 Win=512 Len=0
2028 25.728542 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 26 [SYN] Seq=0 Win=512 Len=0
2029 25.728543 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 27 [SYN] Seq=0 Win=512 Len=0
2030 25.728544 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 28 [SYN] Seq=0 Win=512 Len=0
2031 25.728545 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 29 [SYN] Seq=0 Win=512 Len=0
2032 25.728546 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 30 [SYN] Seq=0 Win=512 Len=0
2033 25.728547 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 31 [SYN] Seq=0 Win=512 Len=0
2034 25.728548 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 32 [SYN] Seq=0 Win=512 Len=0
2035 25.728549 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 33 [SYN] Seq=0 Win=512 Len=0
2036 25.728550 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 34 [SYN] Seq=0 Win=512 Len=0
2037 25.728551 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 35 [SYN] Seq=0 Win=512 Len=0
2038 25.728552 10.0.2.15 102.241.216.11 TCP 56 [TCP Port numbers reused] 2576 - 36 [SYN] Seq=0 Win=512 Len=0
Frame 2044: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
Linux cooked capture v1
Internet Control Message Protocol, Version 4, Src: 10.0.2.15, Dst: 102.241.216.11
Transmission Control Protocol, Src Port: 2576, Dst Port: 42, Seq: 8, Len: 8
Source Port: 2576
Destination Port: 42
[Stream index: 2041]
[TCP Sequence Number: 8]
Sequence Number: 0 (relative sequence number)
Next Sequence Number: 1 (relative sequence number)
Acknowledge Number: 273992599
Checksum: 0x00000000 (0)
Checksum Status: Verified
Urgent Pointer: 0
Flags: S (SYN)
Window Size: 512
[Calculated window size: 512]
Options: (none)
[Checksummed]
[Checksum Status: Unverified]
Urgent Pointer: 0
Flags: S, E (SYN, ACK)
[SEQ/ACK analysis]
any. <live capture in progress> Capturing from any (a...
Packets: 8952 - Displayed: 8952 (100.0%) Profile: Default
File Menu ParrotTerminal Capturing from any (a...
File Search Applications Home Help ENG IN 18:39:24 26-03-2025

Port Scanning Using Metasploit.

Metasploit offers powerful tools to identify open ports, services, and potential vulnerabilities on a target system.

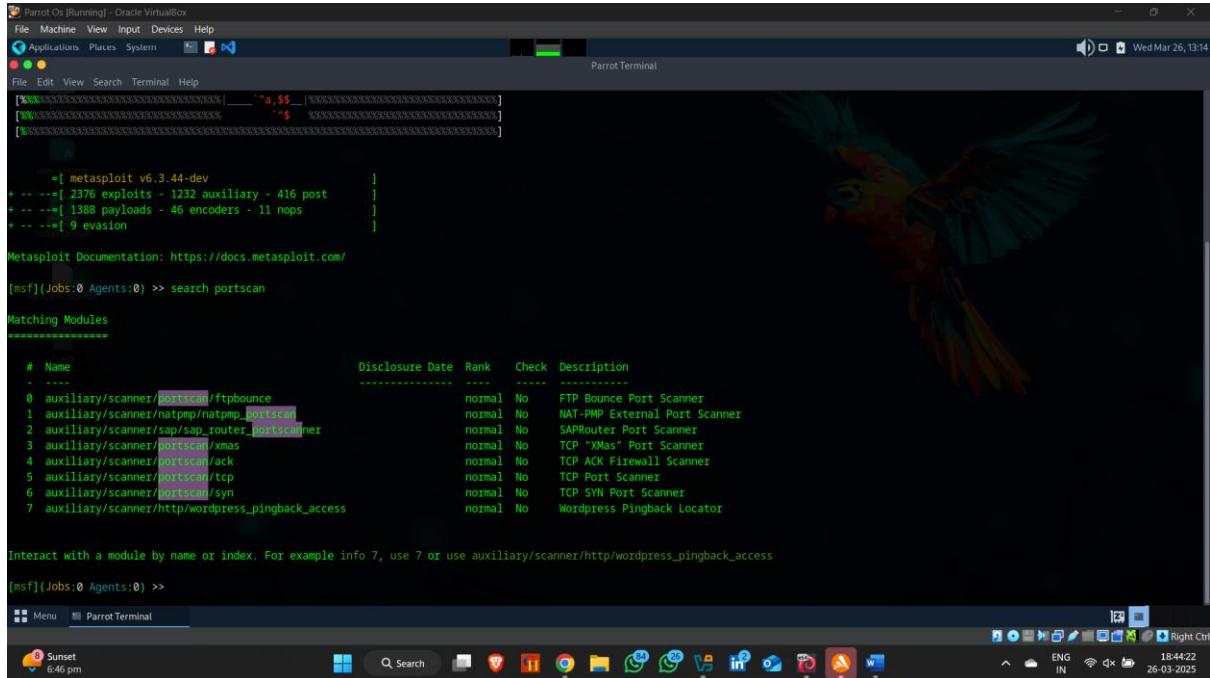
How to use it :-

Step 1 : Open terminal and type **msfconsole**



The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The window title bar includes the text "Parrot Os [Running] - Oracle VirtualBox". The terminal prompt is "[root@parrot]~(/home/user)". The user has typed "#msfconsole" and is now in the Metasploit framework. The screen displays the Metasploit banner, which is a colorful parrot logo, followed by the version information: "Metasploit v6.3.44-dev", "2376 exploits", "1232 auxiliary", "416 post", "1388 payloads", "46 encoders", "11 nops", and "9 evasion". Below this, a link to the documentation is shown: "Metasploit Documentation: <https://docs.metasploit.com/>". The bottom of the terminal shows the command "[msf] (Jobs:0 Agents:0) >>". The desktop environment behind the terminal window includes a taskbar with various icons and a system tray showing network status and battery level.

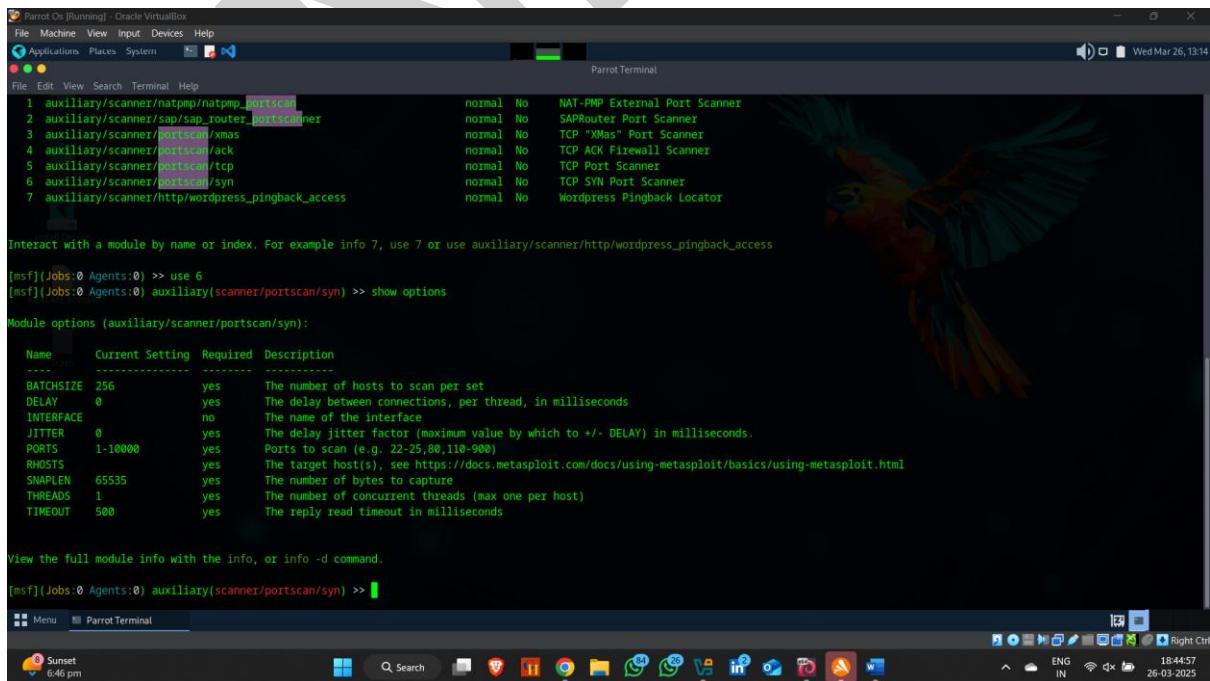
Step 2 : type search portscan



The screenshot shows a terminal window titled "ParrotTerminal" on a Parrot OS desktop. The terminal displays the Metasploit framework documentation and search results for "portscan". The search command was "search portscan", and the results show various auxiliary/scanner modules related to port scanning, such as "auxiliary/scanner/natpmp/natpmp_portscanner", "auxiliary/scanner/sap/sap_router_portscanner", and "auxiliary/scanner/portscan/xmas". The terminal also includes a "Matching Modules" section and a note about interacting with modules by name or index.

Step 3 : type **use <number of port scan >** to set which port scan are you want and press enter and then type **show option** to check , selected port scan number is set or not

- Example - : use 6



The screenshot shows a terminal window titled "ParrotTerminal" on a Parrot OS desktop. The terminal displays the Metasploit framework documentation and search results for "portscan". The search command was "use 6", followed by "auxiliary(scanner/portscan/syn) >> show options". The output shows the module options for "auxiliary(scanner/portscan/syn)", including "BATCHSIZE", "DELAY", "INTERFACE", "JITTER", "PORTS", "RHOSTS", "SNAPLEN", "THREADS", and "TIMEOUT". The "show options" command provides detailed descriptions for each option.

Step 4 : Then type set RHOST to set target ip .

The screenshot shows a terminal window titled "Parrot Os [Running] - Oracle VirtualBox". The terminal displays the following Metasploit module configuration:

```
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set RHOST 192.168.81.182
RHOST => 192.168.81.182
[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> show options

Module options (auxiliary/scanner/portscan/syn):

Name Current Setting Required Description
-----
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 192.168.81.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >>
```

The terminal window is part of the Parrot OS desktop environment, with a colorful parrot icon in the background. The taskbar at the bottom shows various application icons.

Step 5 : type show options to check target ip are set or not

The screenshot shows a terminal window titled "Parrot Os [Running] - Oracle VirtualBox". The terminal displays the following Metasploit module configuration, identical to the previous step but with the RHOST option explicitly set:

```
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 192.168.81.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set PORTS 1-1000
PORTS => 1-1000
[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> show options

Module options (auxiliary/scanner/portscan/syn):

Name Current Setting Required Description
-----
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-1000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 192.168.81.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds

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

[msf] (Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >>
```

The terminal window is part of the Parrot OS desktop environment, with a colorful parrot icon in the background. The taskbar at the bottom shows various application icons.

Step 6 : type run .



```
Parrot Os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[msf] (Jobs:0) Agents:0) auxiliary(scanner/portscan/syn) >> show options

Module options (auxiliary/scanner/portscan/syn):

Name      Current Setting  Required  Description
-----  =  -----  =  -----
BATCHSIZE  256           yes        The number of hosts to scan per set
DELAY      0              yes        The delay between connections, per thread, in milliseconds
INTERFACE   no            no        The name of the interface
JITTER     0              yes        The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS      1-1000         yes        Ports to scan (e.g. 22-25,80,110-900)
RHOSTS    192.168.81.182  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN   65535          yes        The number of bytes to capture
THREADS   1              yes        The number of concurrent threads (max one per host)
TIMEOUT   500            yes        The reply read timeout in milliseconds

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

[msf] (Jobs:0) Agents:0) auxiliary(scanner/portscan/syn) >> run

[*] TCP OPEN 192.168.81.182:23
[*] TCP OPEN 192.168.81.182:80
[*] TCP OPEN 192.168.81.182:111
[*] TCP OPEN 192.168.81.182:139
[*] TCP OPEN 192.168.81.182:445
[*] TCP OPEN 192.168.81.182:512
[*] TCP OPEN 192.168.81.182:513
[*] TCP OPEN 192.168.81.182:514
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf] (Jobs:0) Agents:0) auxiliary(scanner/portscan/syn) >>
```