# 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 –

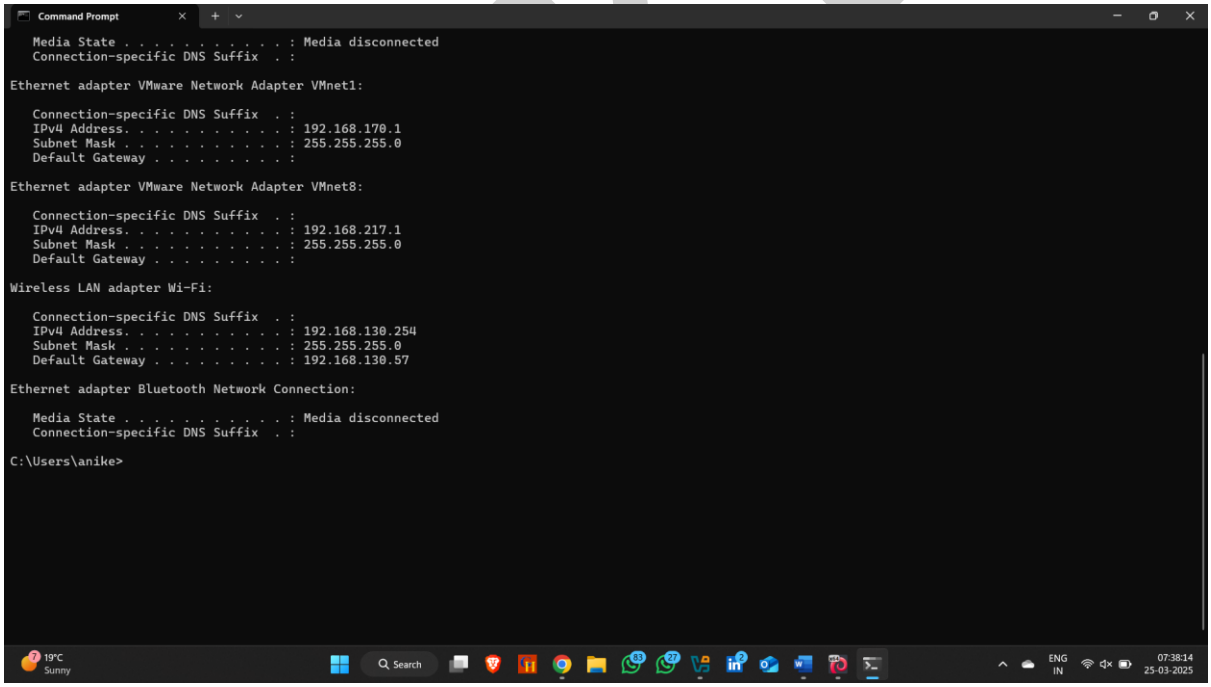
- Discovery
- Security assessment
- Vulnerability detection
- Network mapping
- Performance analysis

# Network Scaning 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 –**

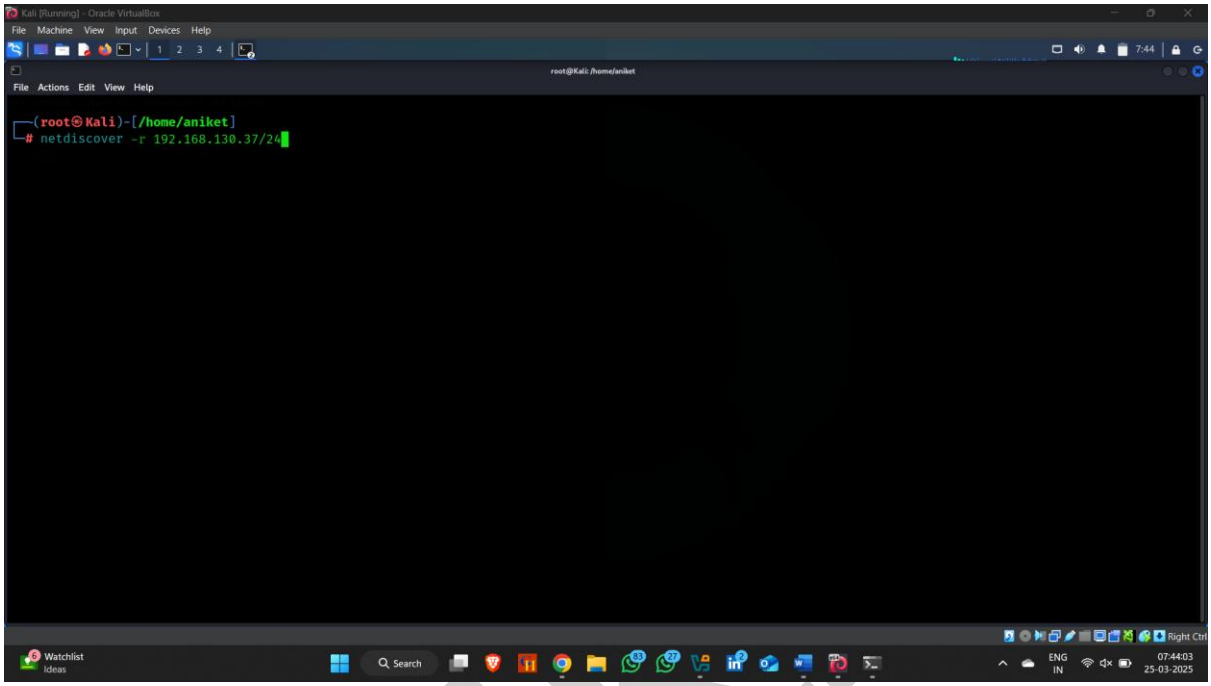
1. Open kali linux / Parrot Os
2. Type netdiscover eth0 / wlan0.
3. Netdiscover -r  < default gateway > with subnet mask.
    - **Open cmd on windows and type ipconfig , now you can see default gateway.**

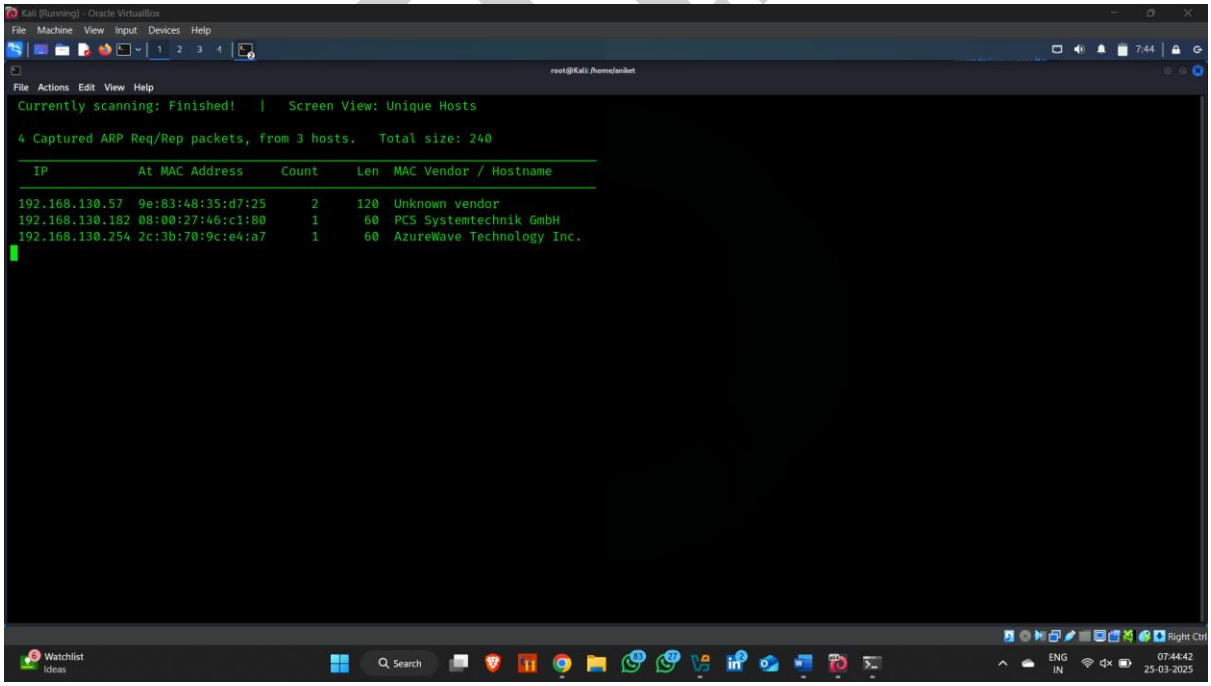



**Common Usage Commands:**

- 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.



# 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.

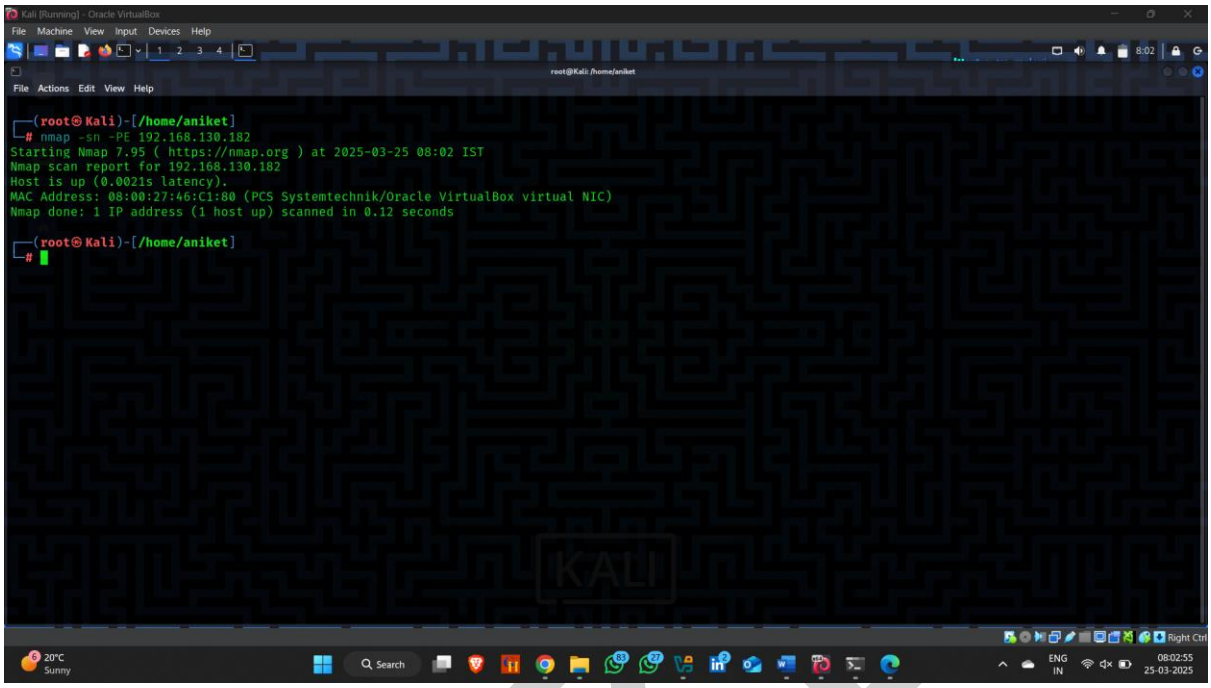
## 1.Host Discovery –

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

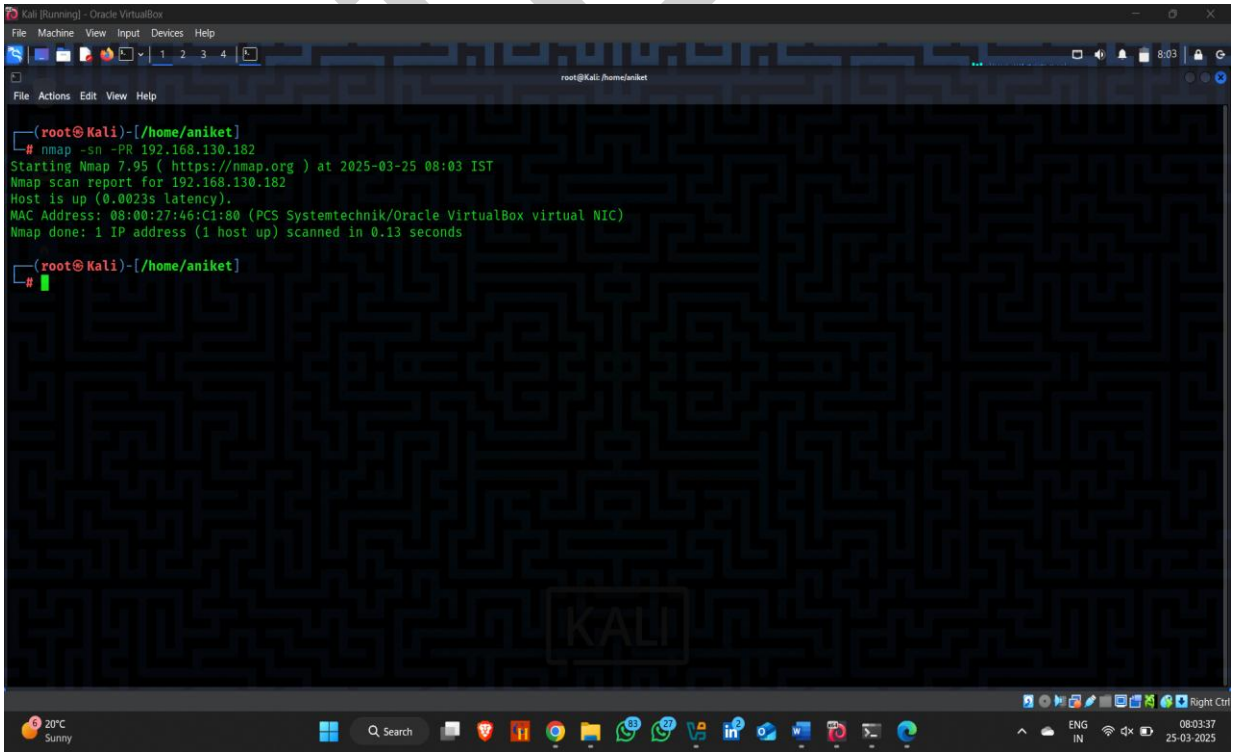
**Common Usage Command –**

- -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.

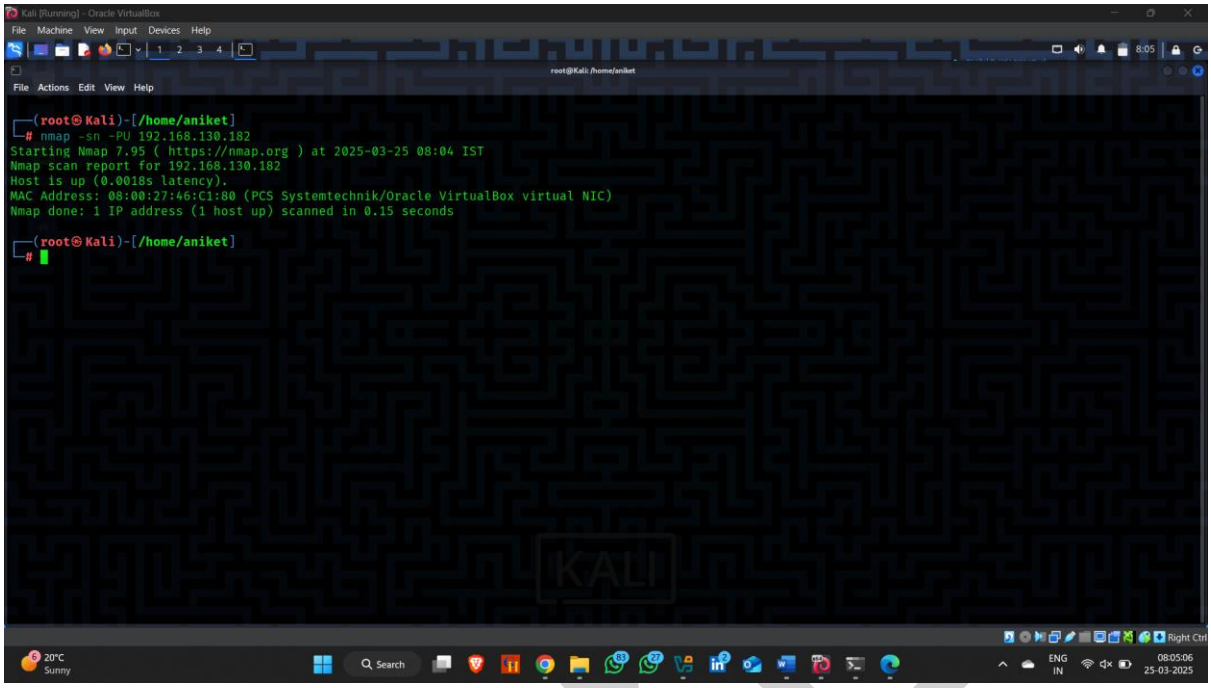
- -PE - - the -PE option is used to send **ICMP Echo Request** packets during a ping scan.



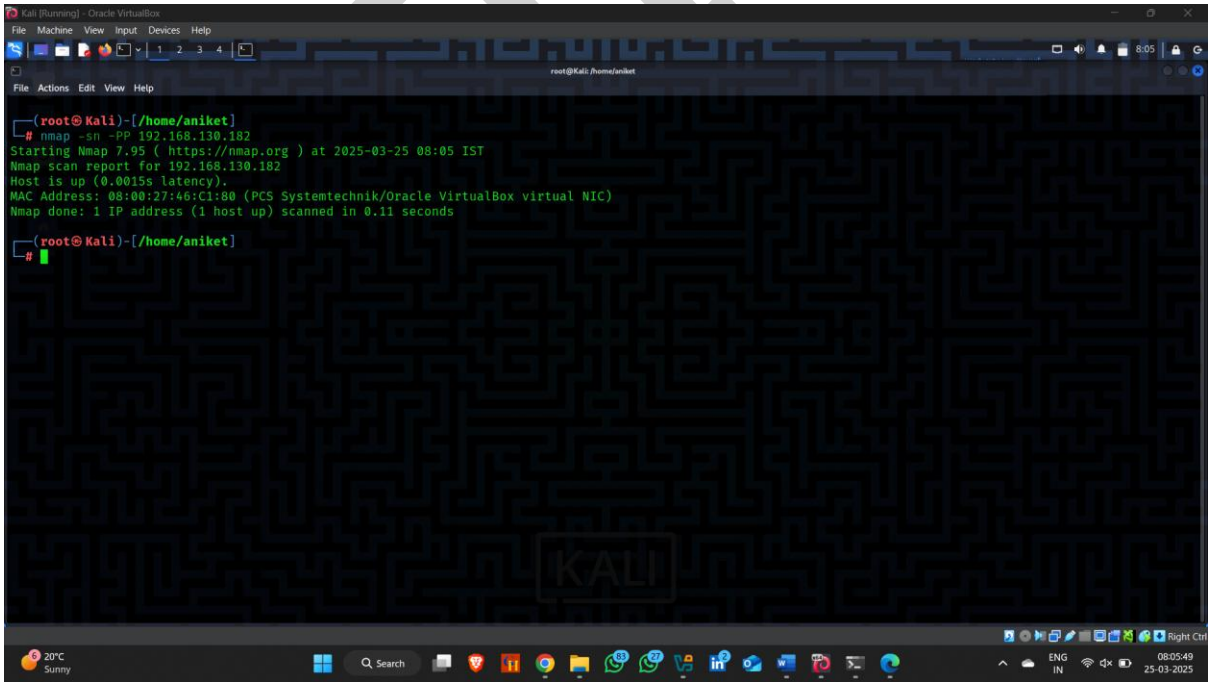

- -PR - - the -PR option is used to perform an **ARP (Address Resolution Protocol) Request Scan**.



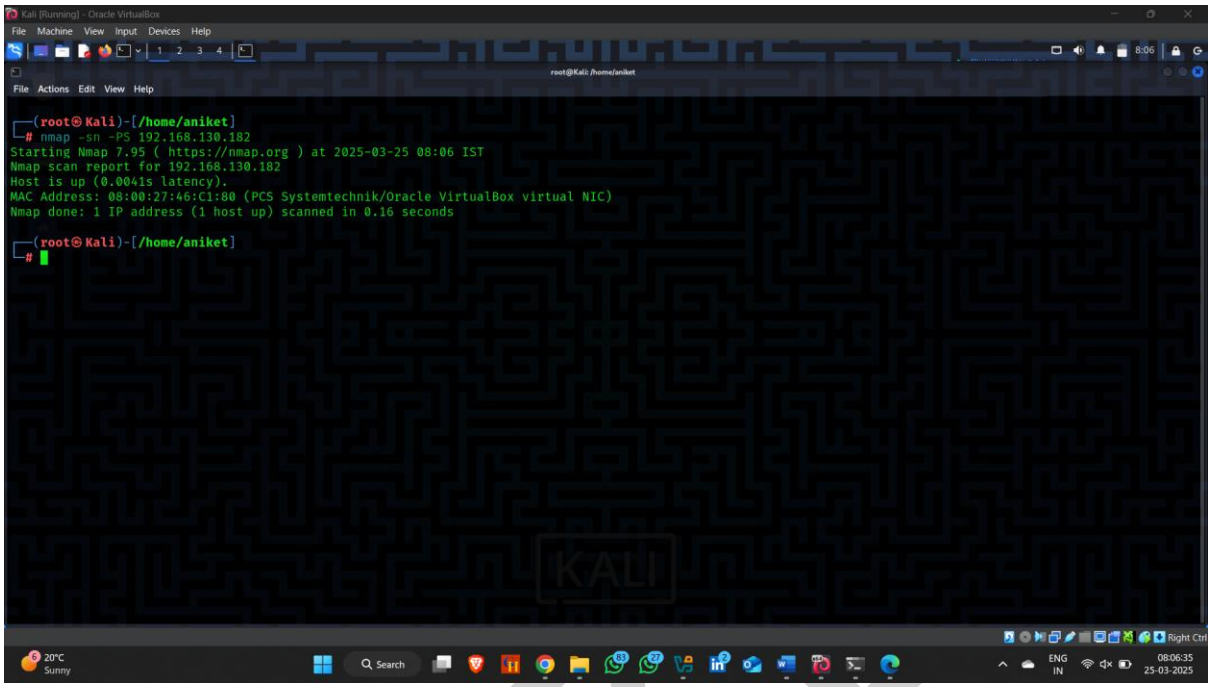
- -PU - - the -PU option is used to perform a **UDP Ping Scan.**



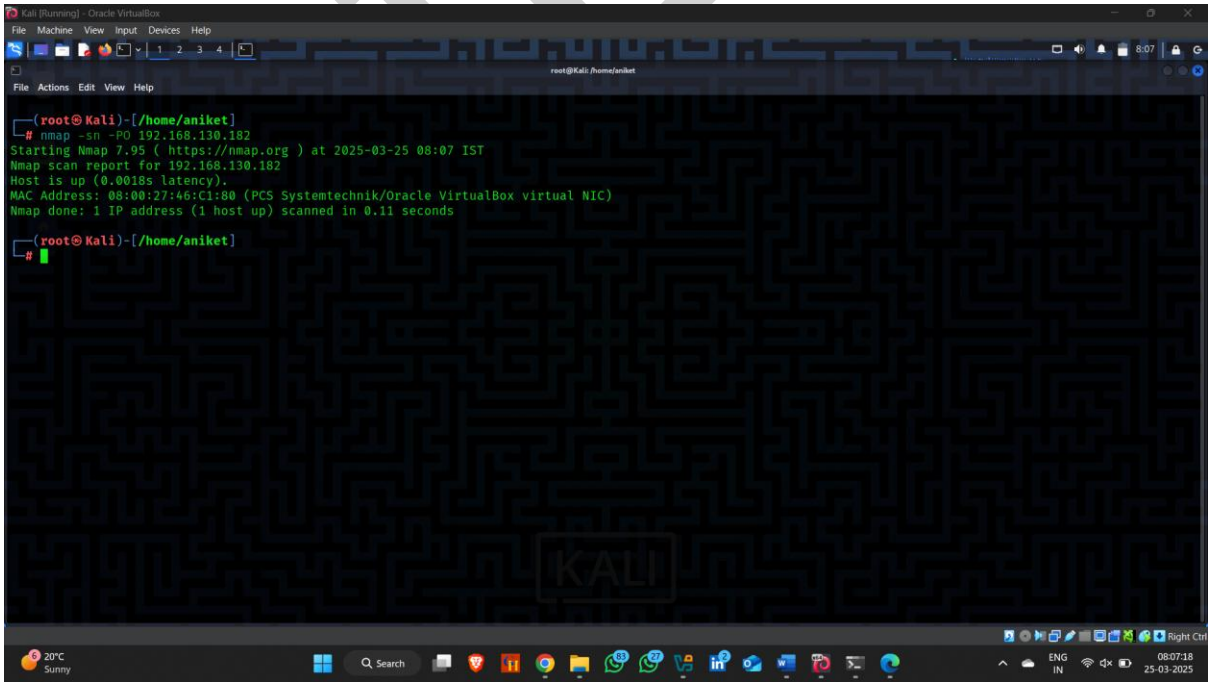

- -PP -- the -PP option is used to perform an **ICMP Timestamp Request Ping Scan**.



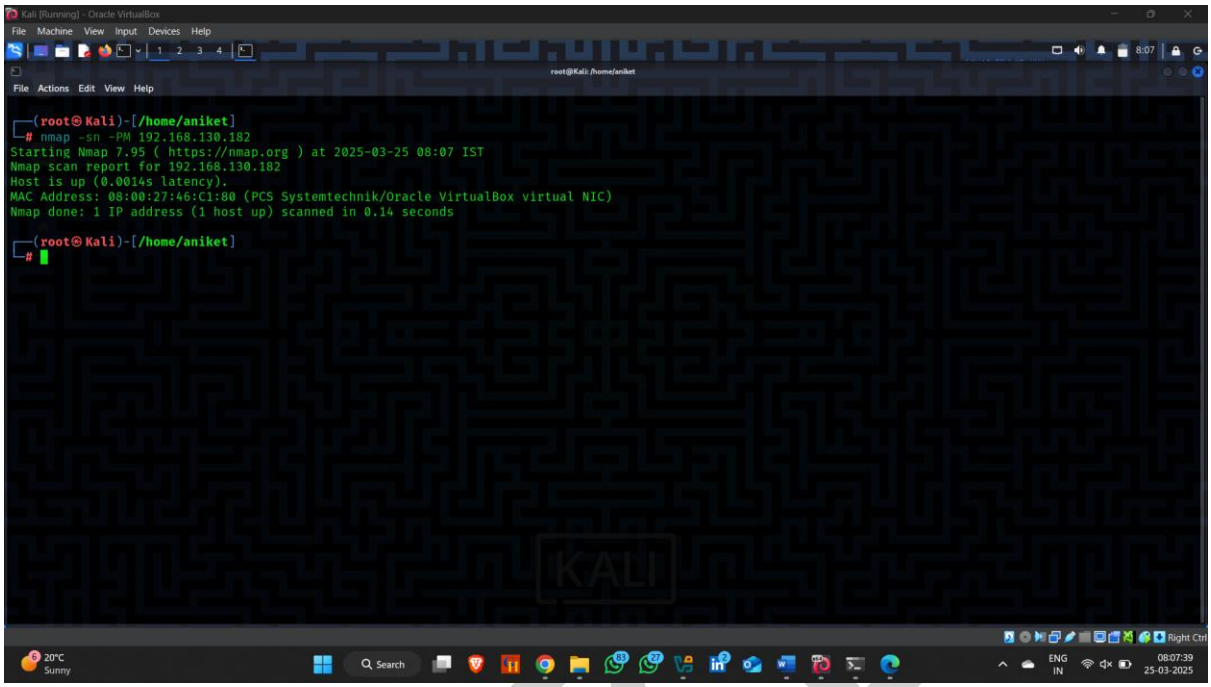
- -PS - - the -PS option is used to perform a **TCP SYN Ping Scan**.




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



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



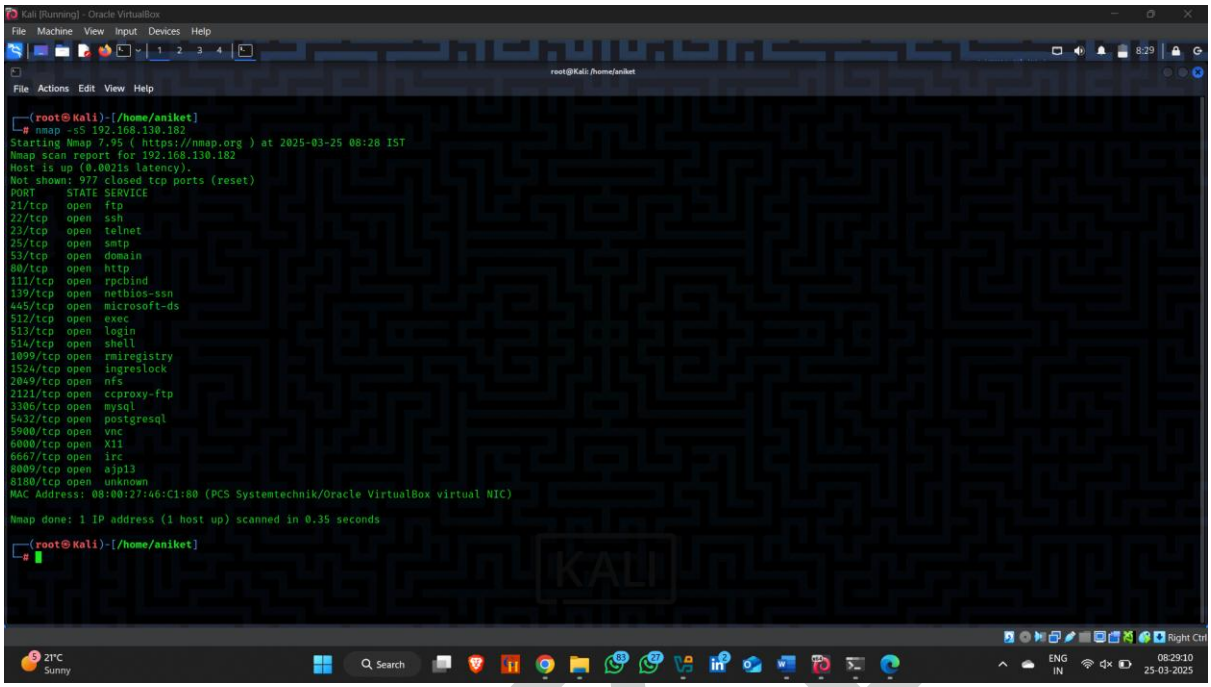
# 2. Port And Service Discovery.

**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.

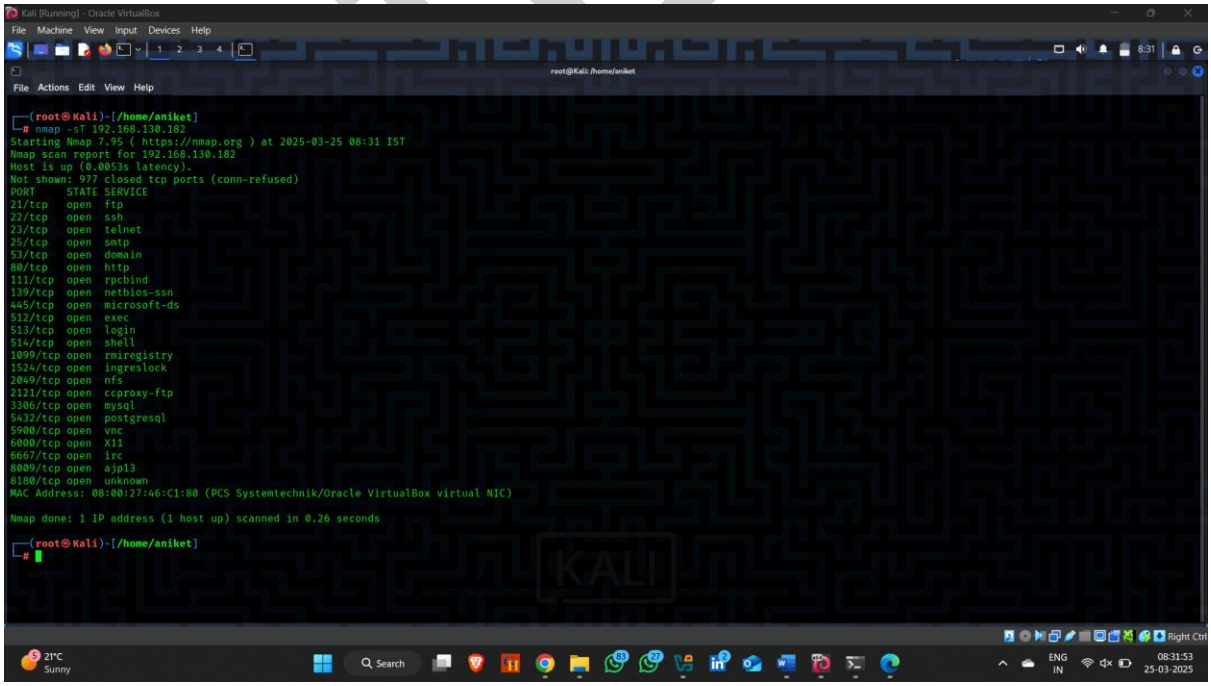
**Common Usage Command –**

- -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 = Stealtth 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.

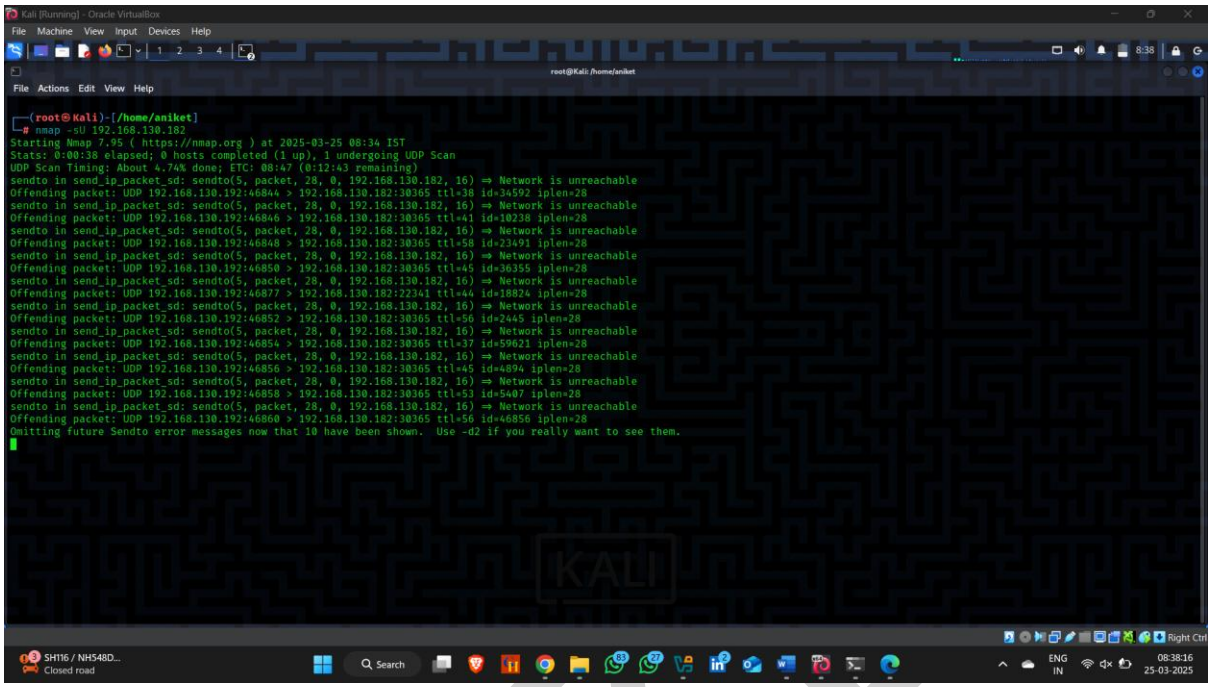
- -sS - - the -sS option specifies a **SYN scan**, often called a **stealth scan** or **half-open scan**.



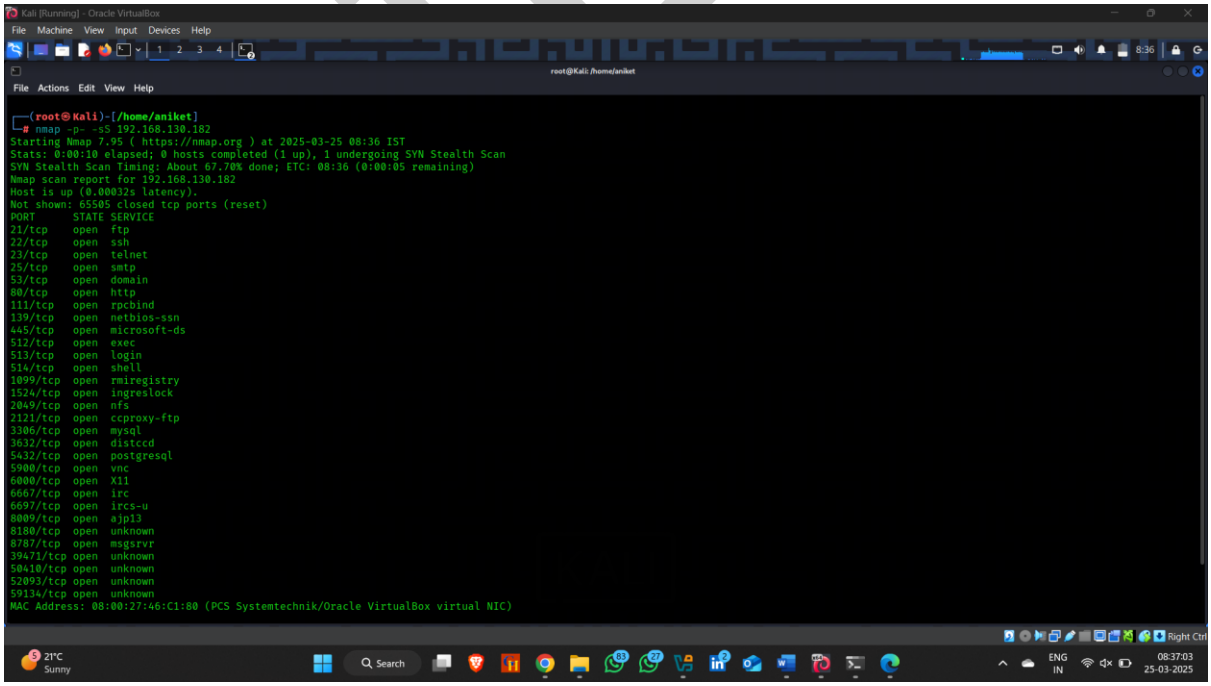

- -sT - - the -sT option specifies a **TCP Connect scan**. It's the default scan type .



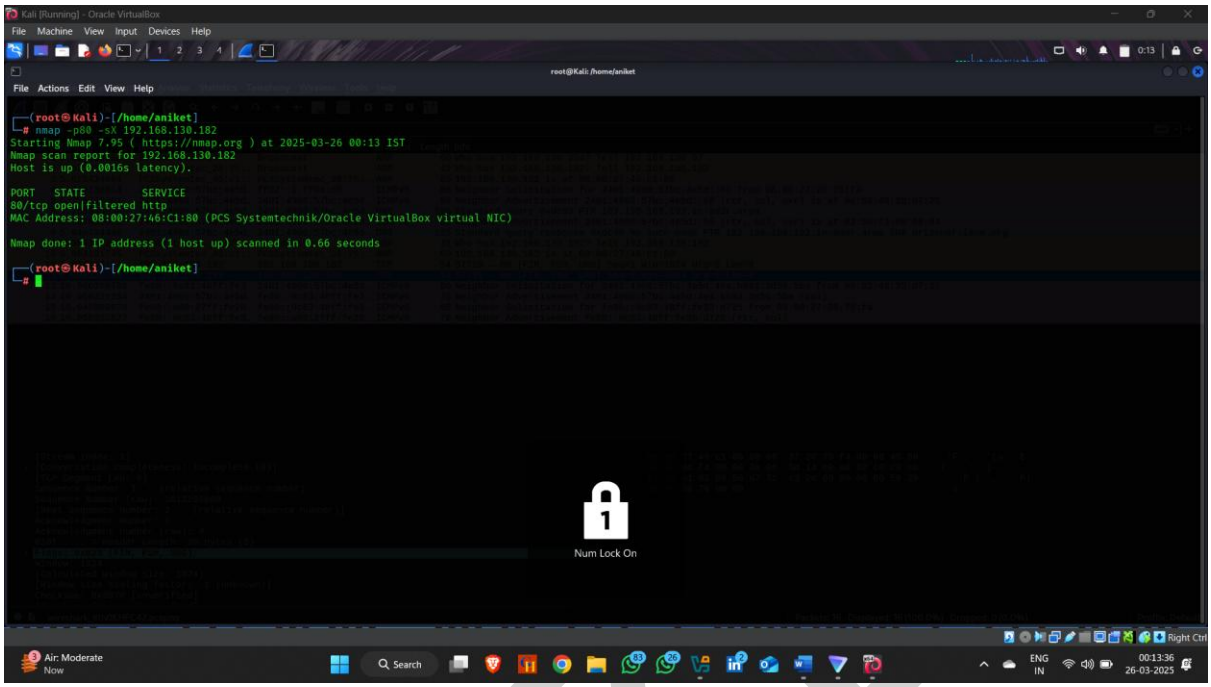
- -sU - - the -sU option specifies a **UDP scan**, which is designed to identify open **UDP ports** on a target system.

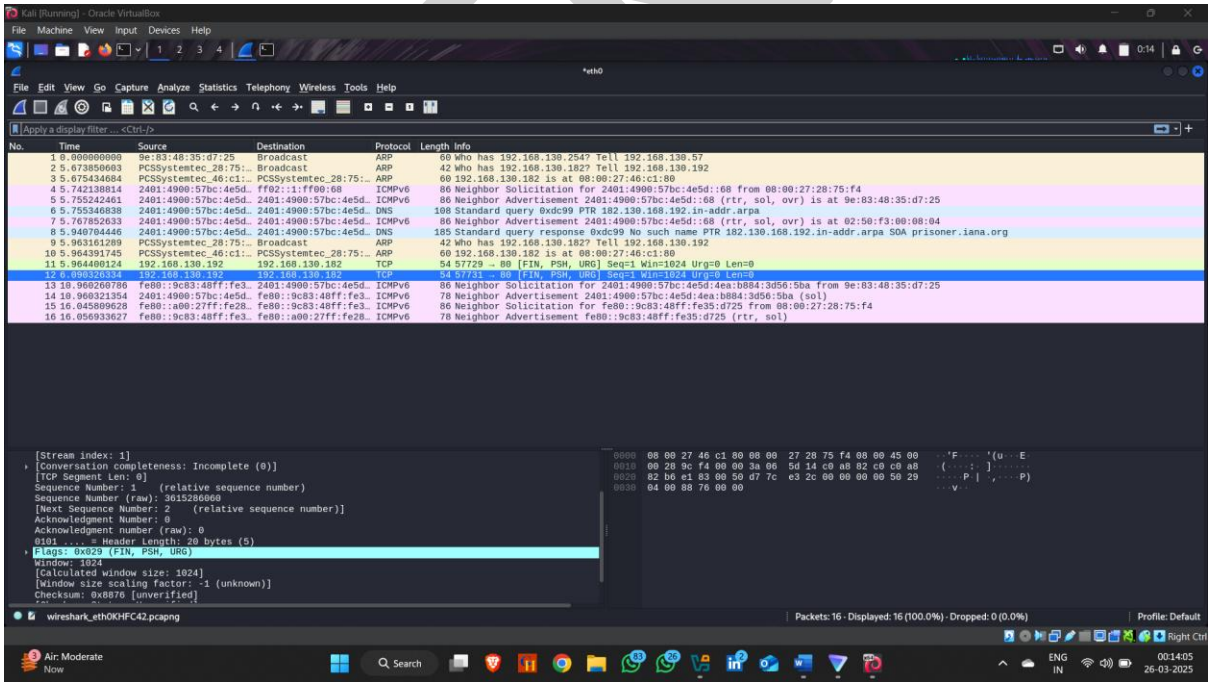



- -p- - - the -p- option is used to scan **all 65,535 TCP or UDP ports** on a target system.

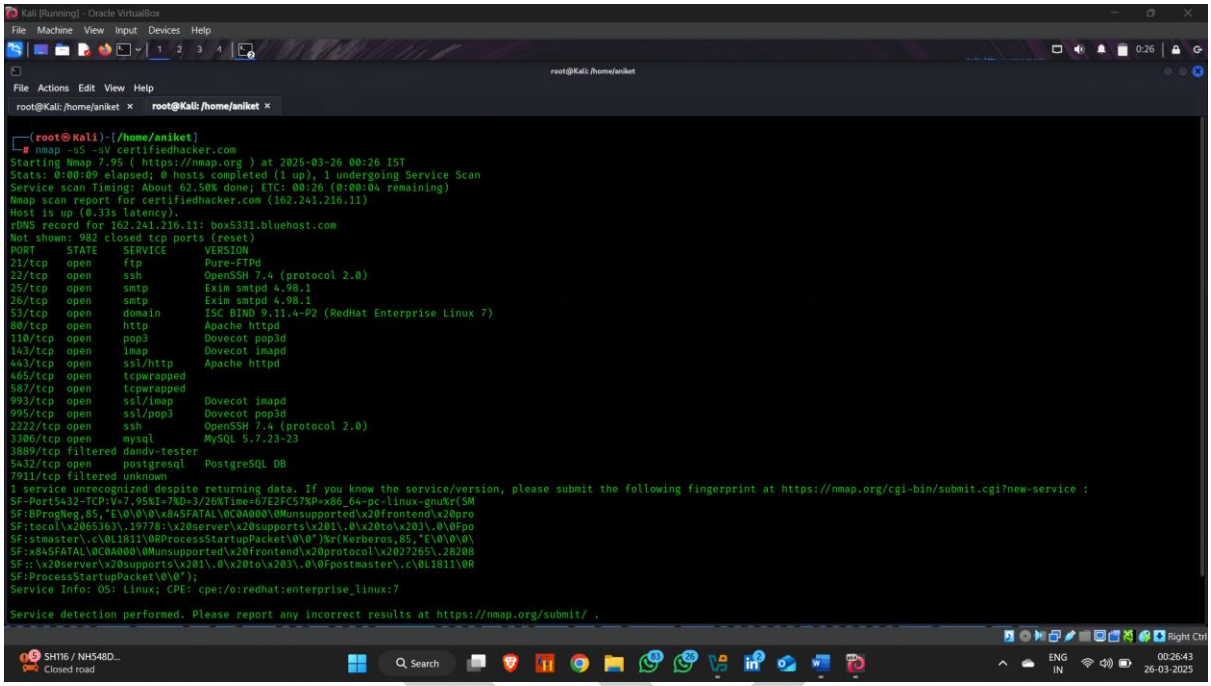


- -sX - - The **Xmas scan** sends TCP packets with the **FIN**, **PSH**, and **URG** flags set.

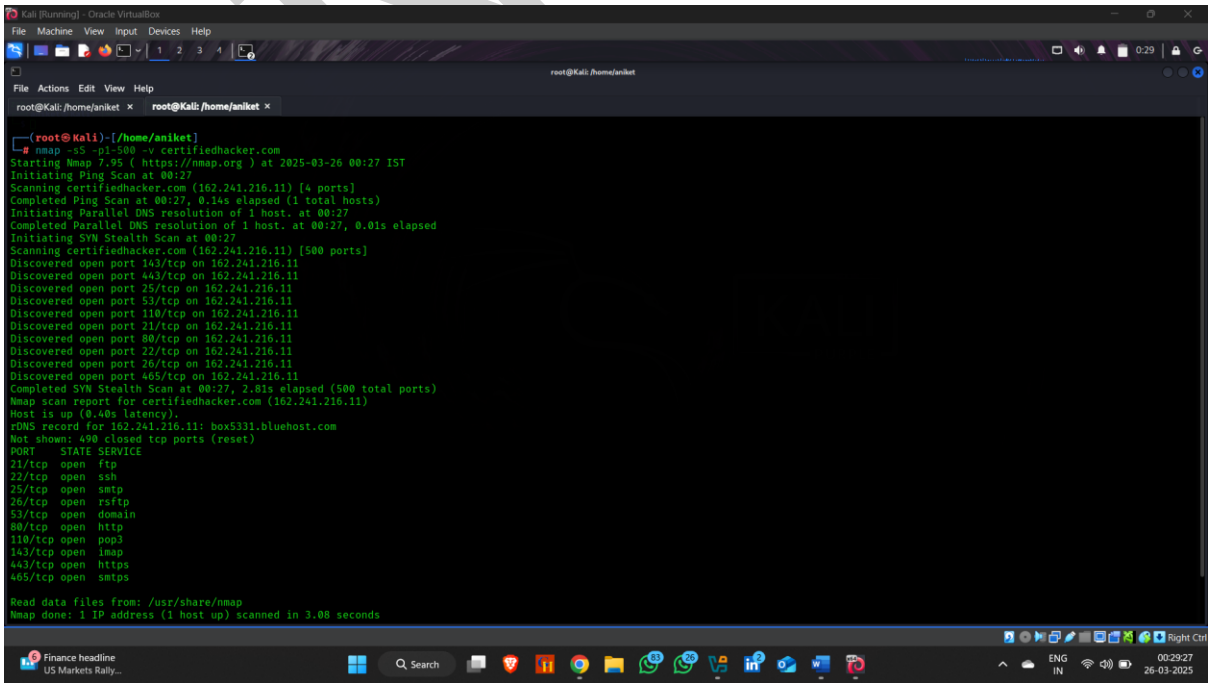


- -sV - - the -sV option is used for **service version detection**, which identifies the exact software version running on open ports.




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



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

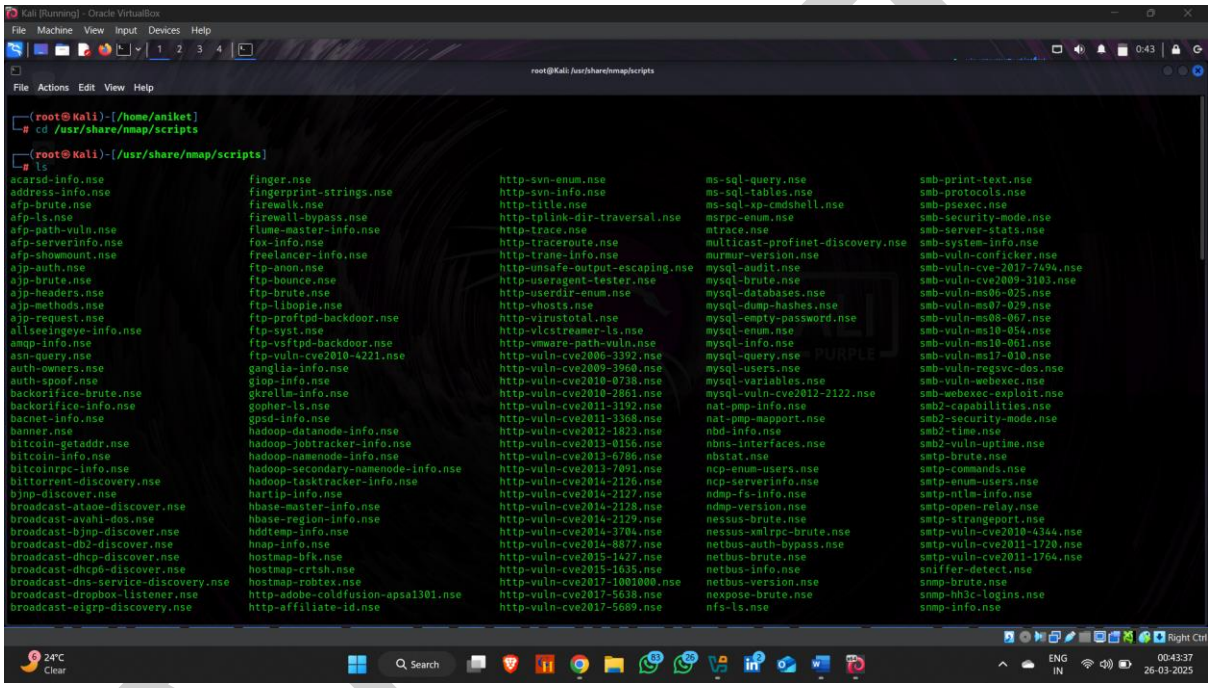
**Note** - Before performing nmap script , find all scripts locations .

Step 1: Locate the Nmap Installation Path.

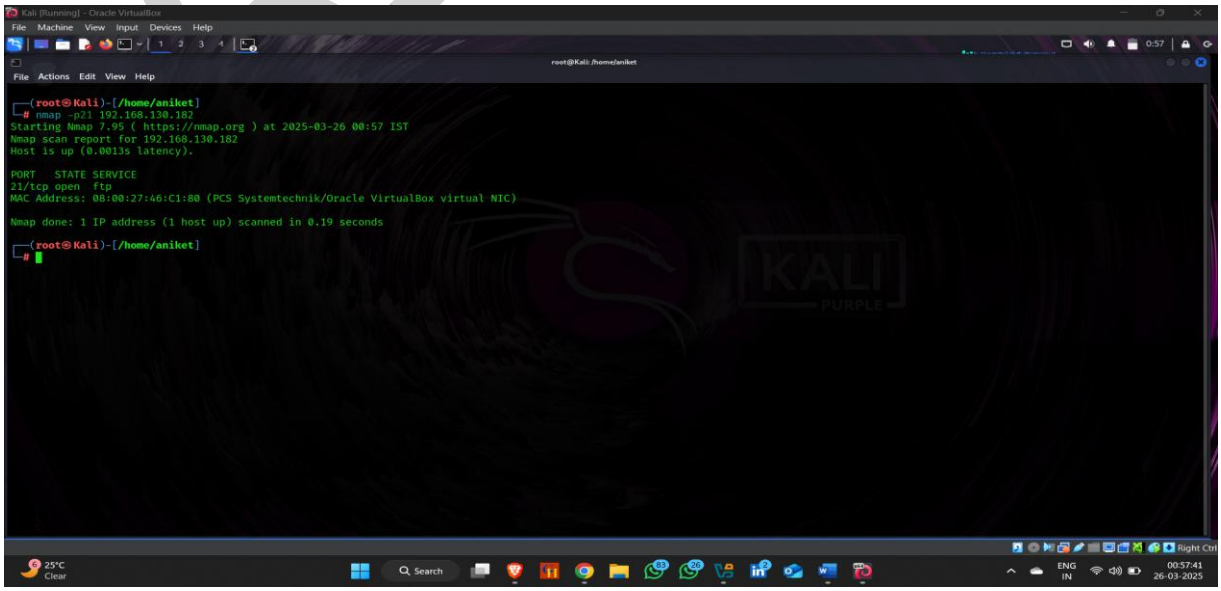
- The Nmap scripts are typically stored in the scripts folder within the Nmap installation directory.

Step 2 : The scripts are usually located in:

- /usr/share/nmap/scripts.

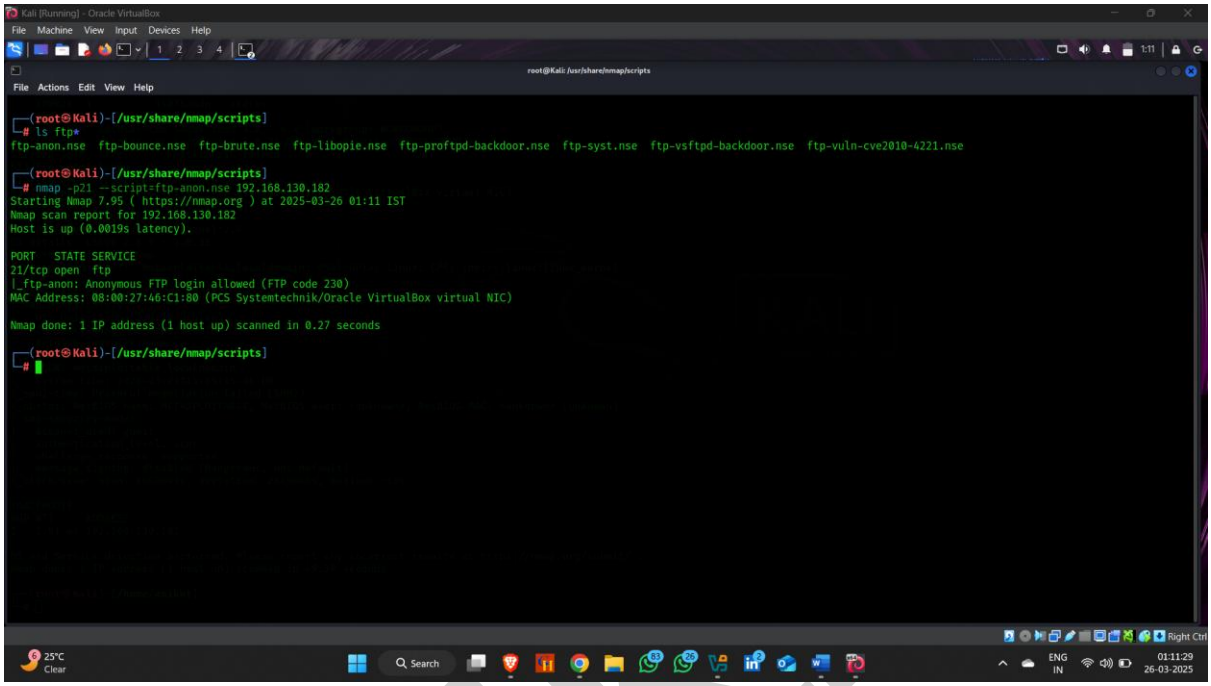



Step 3 : Kindly check the port status is open or closed .



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 )**



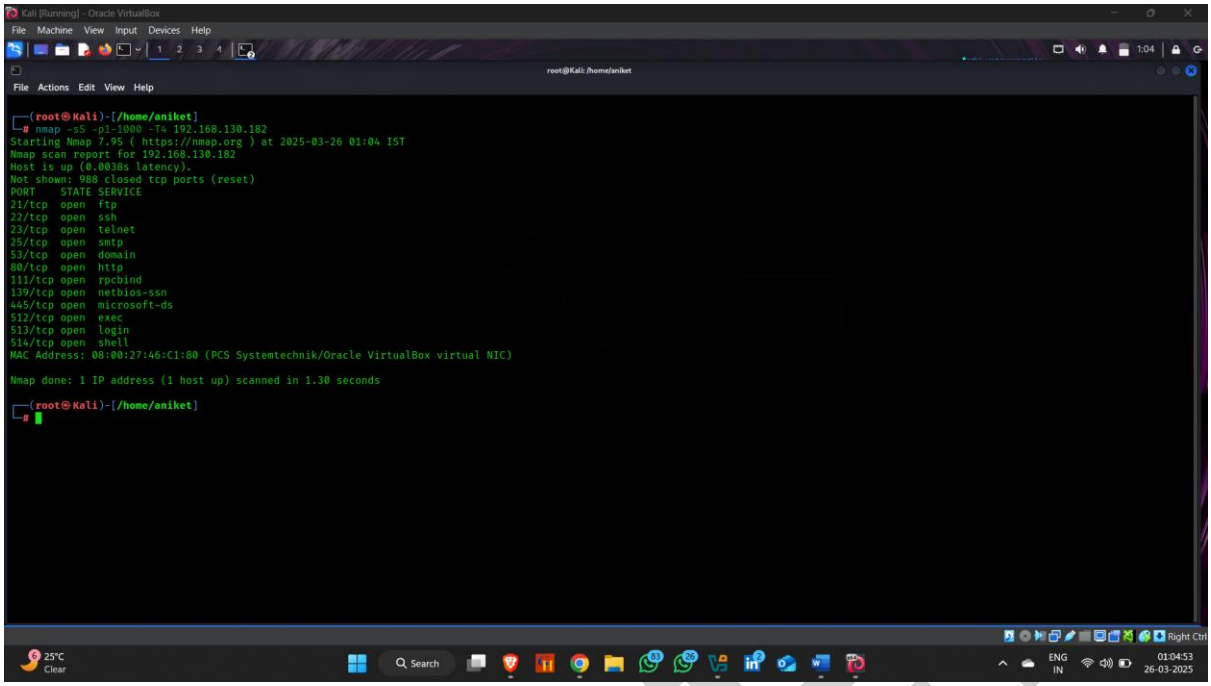

- -T < 0 – 5 > -- the -T<0-5> option controls the **timing template**, which adjusts the **speed**, **aggressiveness**, and **stealth** of your scan.

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

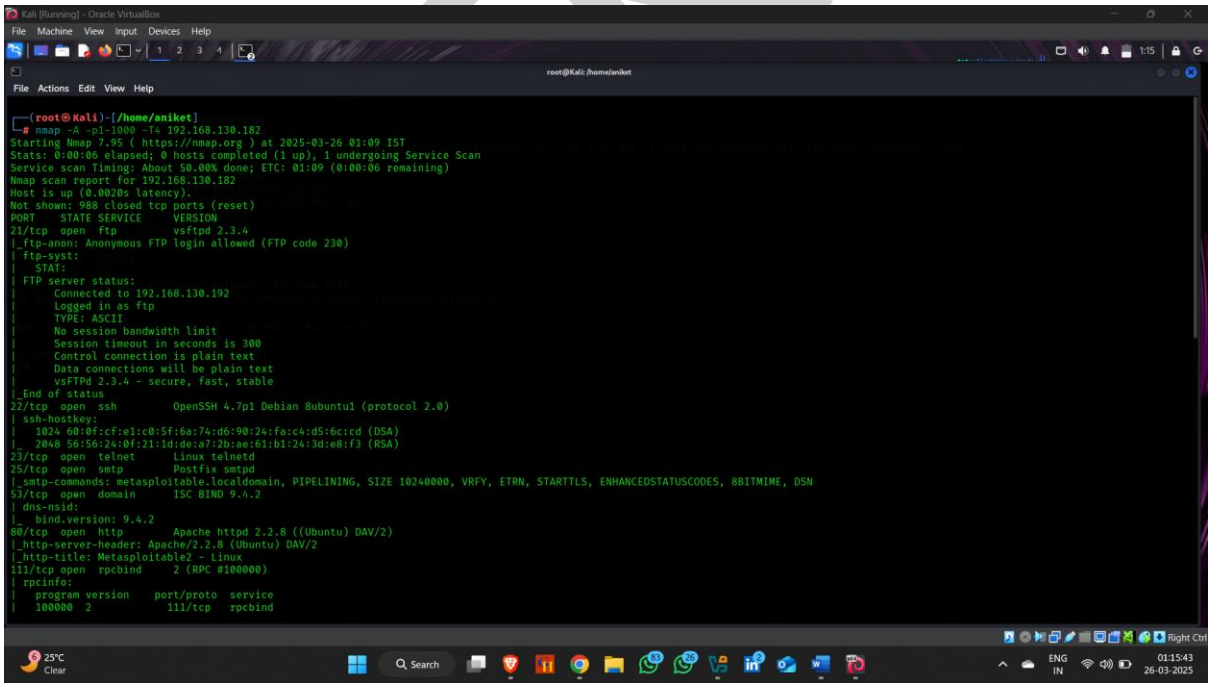
  Use -T2 or -T3 -- for **internet-facing** targets to reduce detection risk.

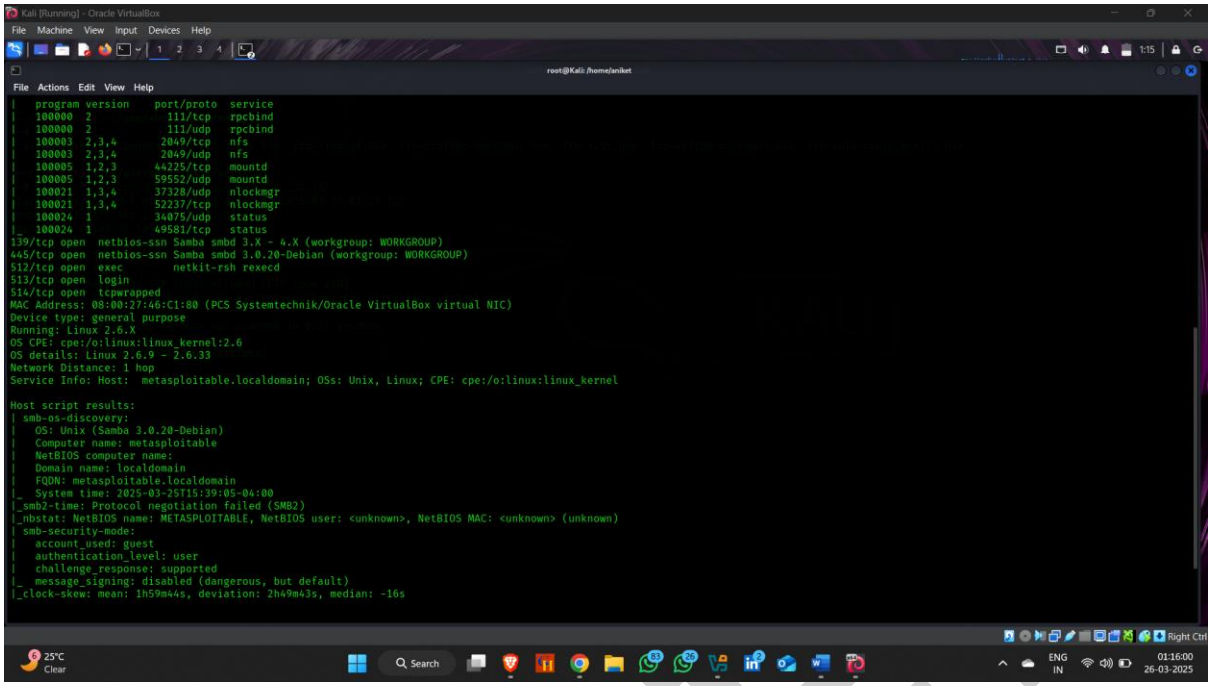
  Use -T4 -- for fast scans **local networks**.

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




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




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: /home/aniket
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 44225/tcp mountd
| 100005 1,2,3 59552/udp mountd
| 100021 1,3,4 37328/udp nlockmgr
| 100021 1,3,4 52237/tcp nlockmgr
| 100024 1 34075/udp status
|_ 100024 1 49581/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 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 tcpwrapped
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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
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_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h59m44s, deviation: 2h49m43s, median: -16s
25°C
Clear
Search
ENG
IN
01:16:00
26-03-2025

# 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.

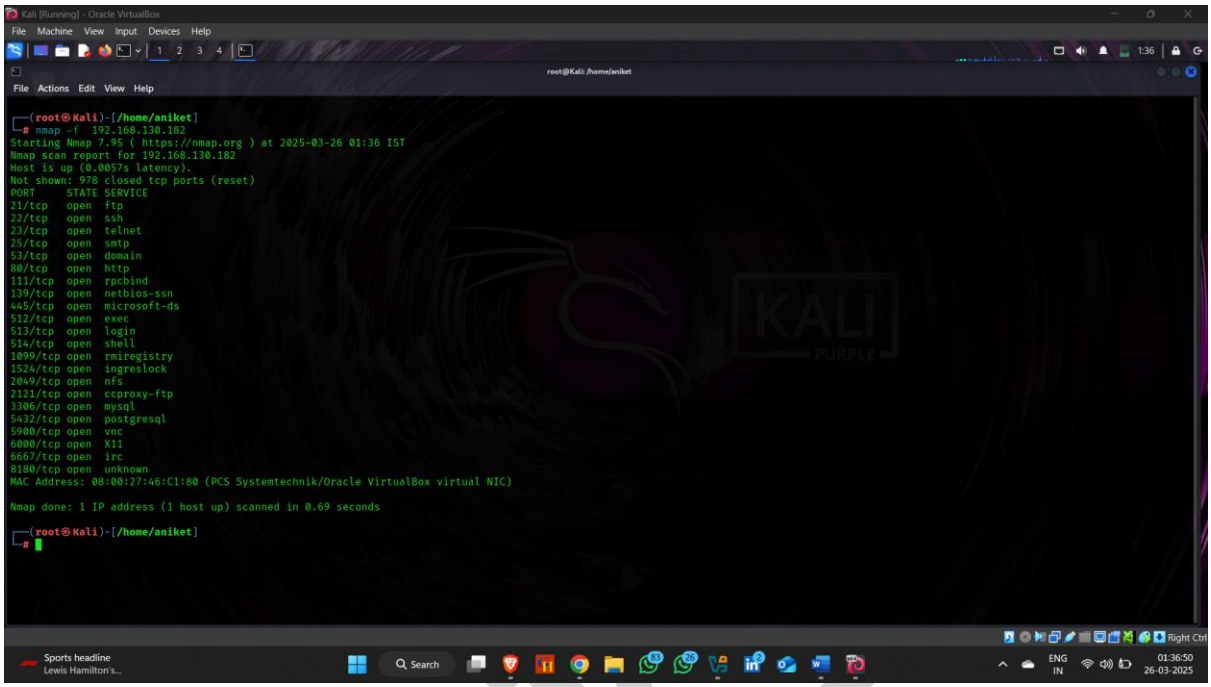
Objectives –

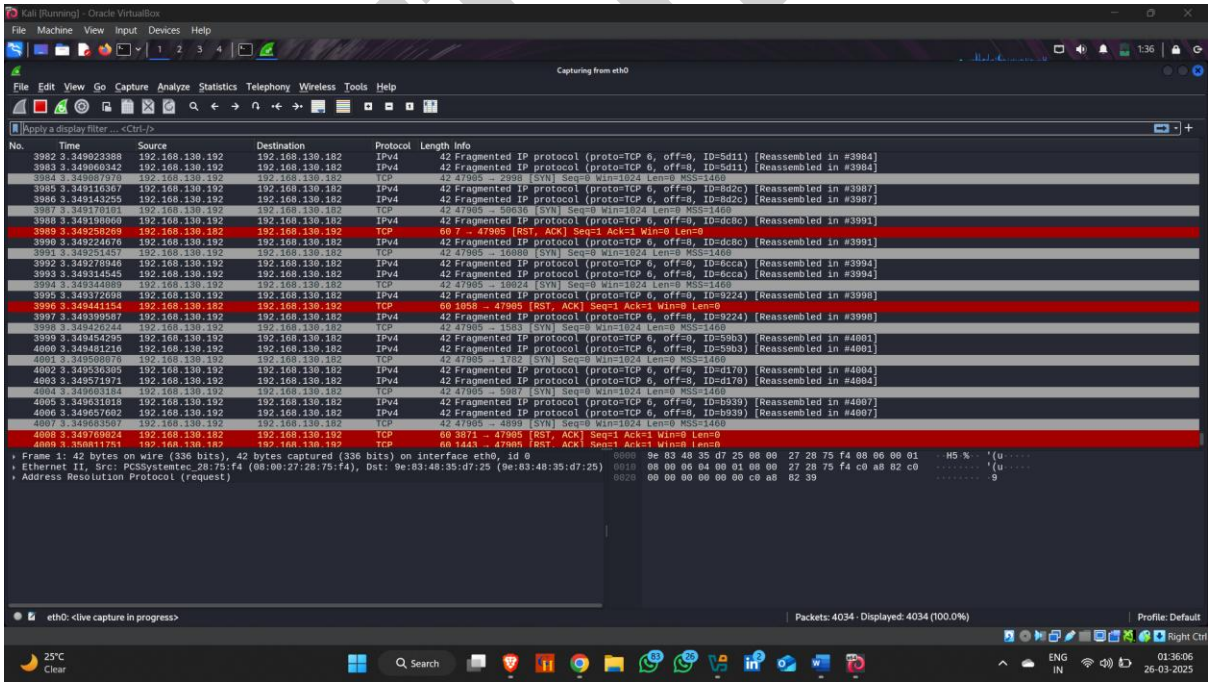
1. Network Protection and Threat Mitigation.
2. Access Control and Traffic Management.
3. Performance Optimization and Security Testing.
4. Risk Assessment and Vulnerability Testing.

**Common Usage Command –**

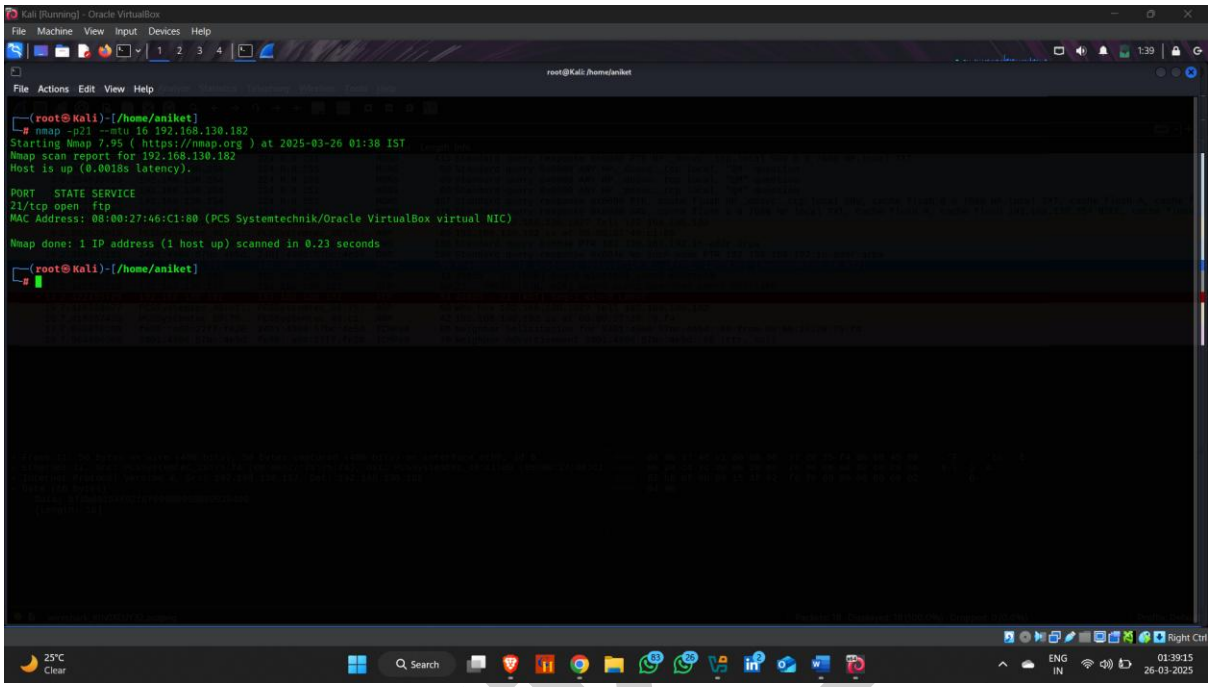
- -f - - Fragmentation
- -mtu - - maximum transmission unit.
- -g -- – Source Port Manipulation.
- --spoof-mac - - – MAC Address Spoofing.
- -D - - Decoy.

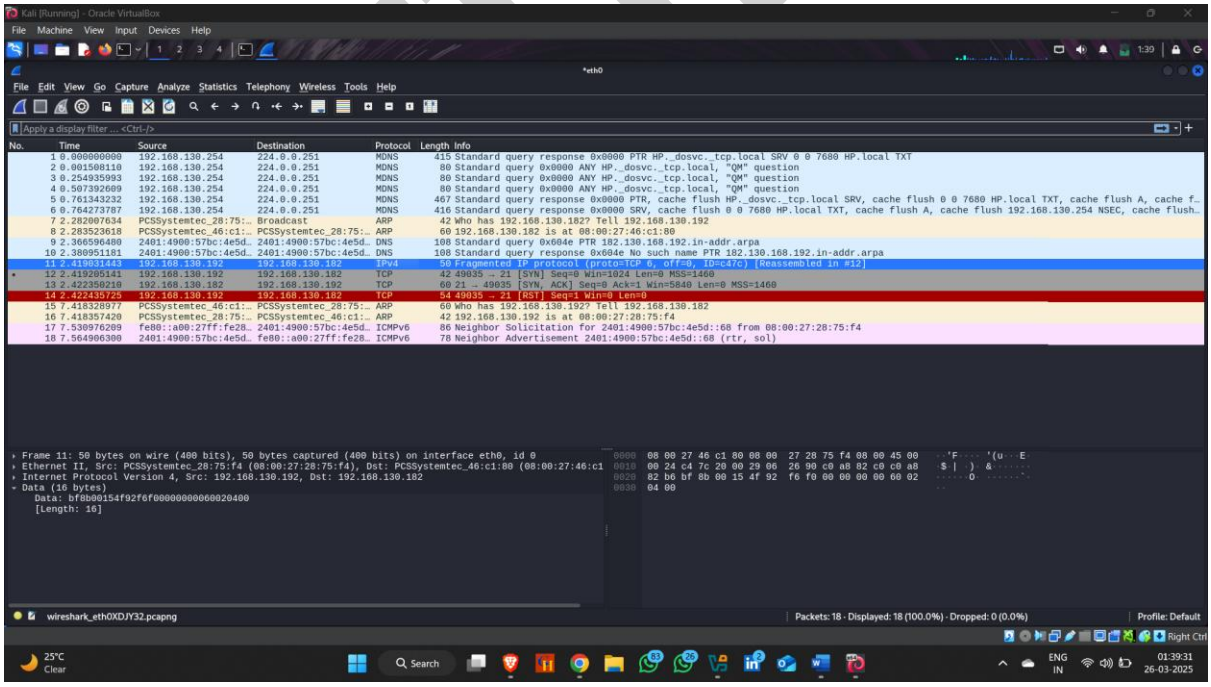
- -f - - The **-f** option in Nmap enables **packet fragmentation**, which breaks your scan packets into smaller pieces.



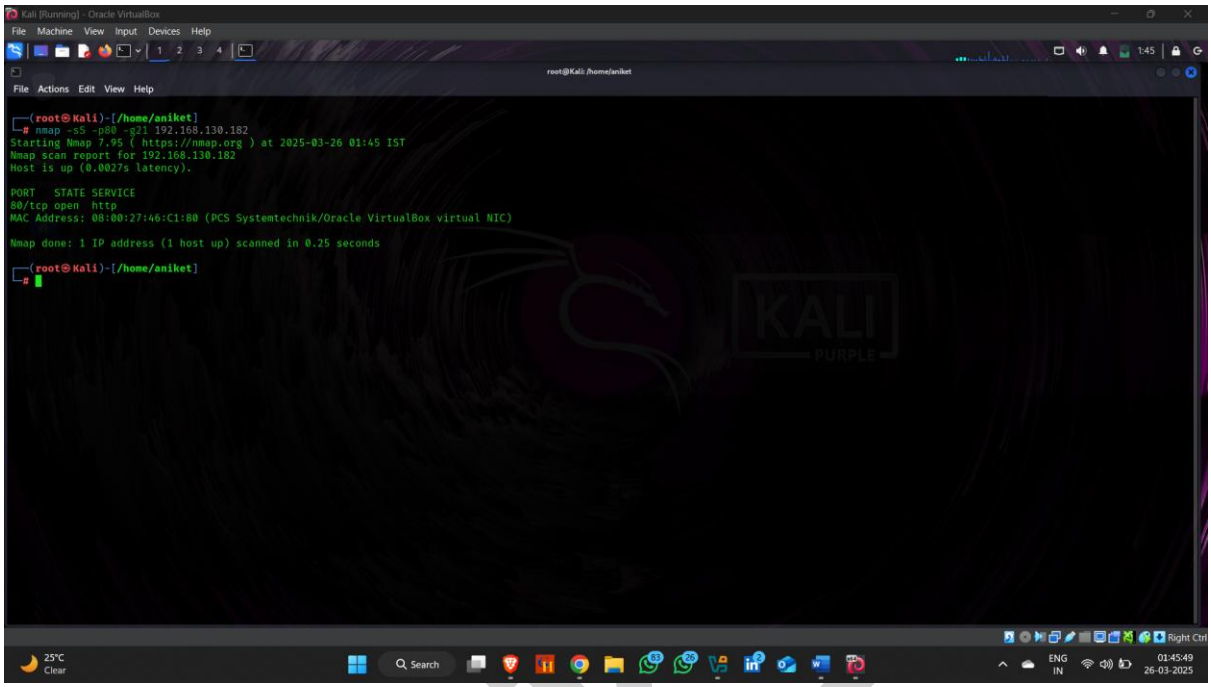



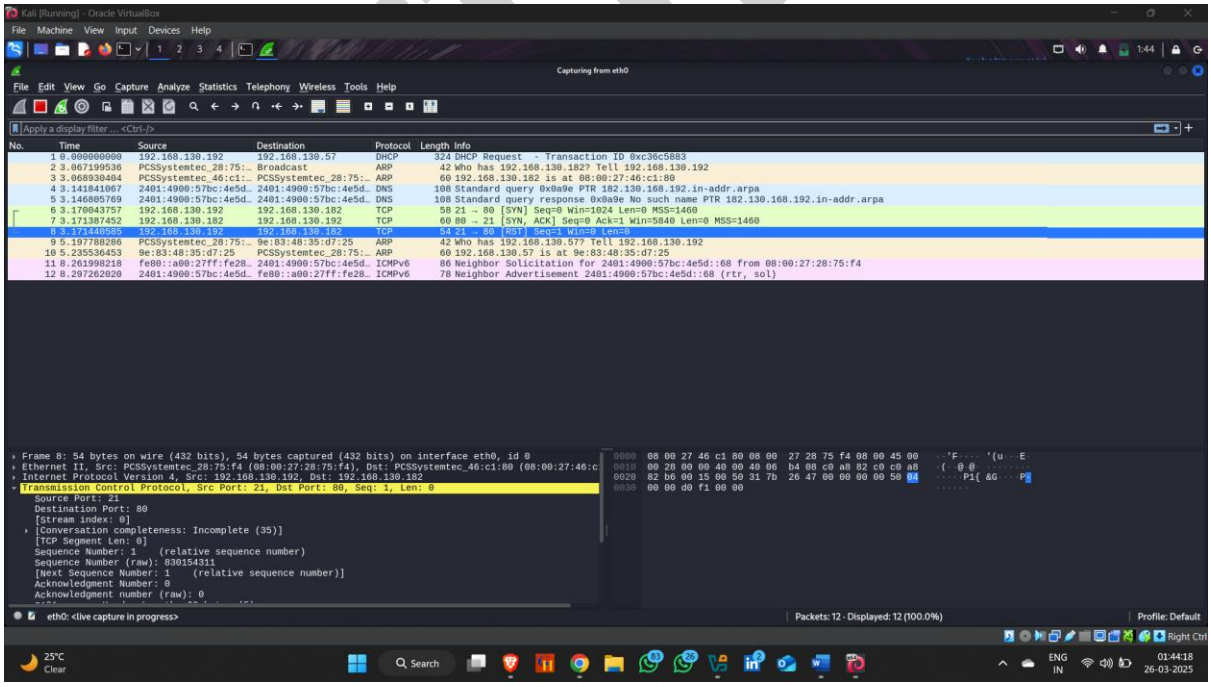
- --mtu -- The **--mtu** option in Nmap allows you to specify a custom **MTU (Maximum Transmission Unit)** value for your scan packets.



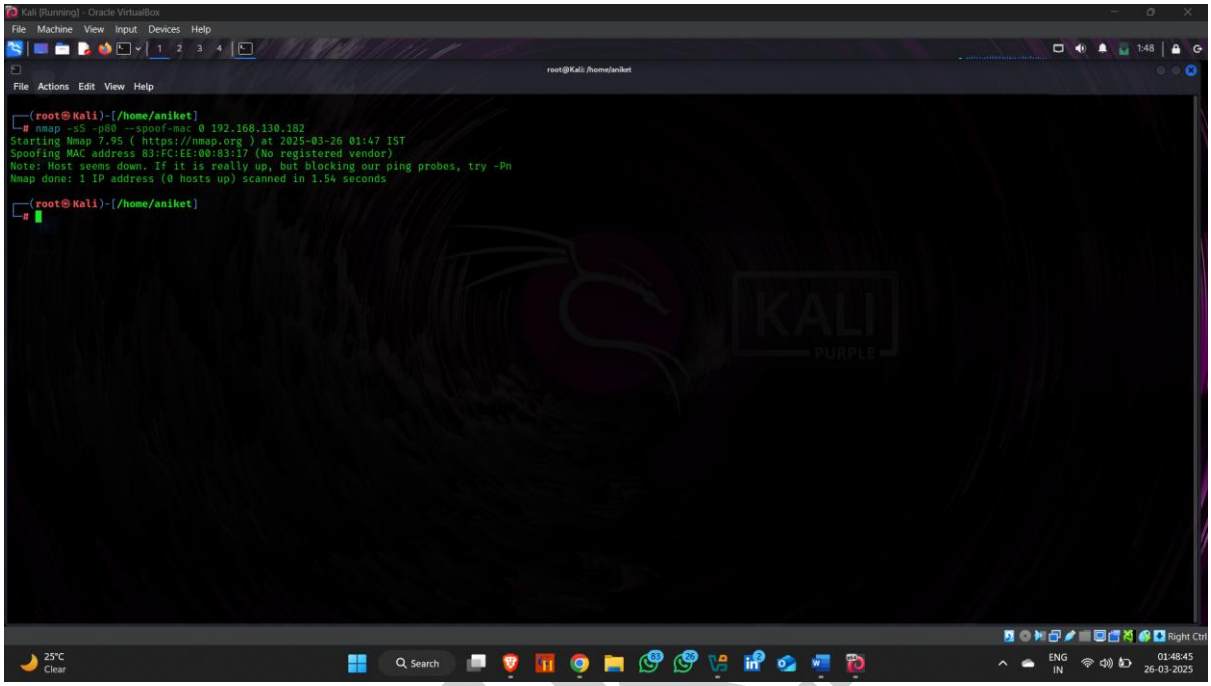



- -g - - The **-g** option in Nmap allows you to specify a **source port** for your outgoing packets.

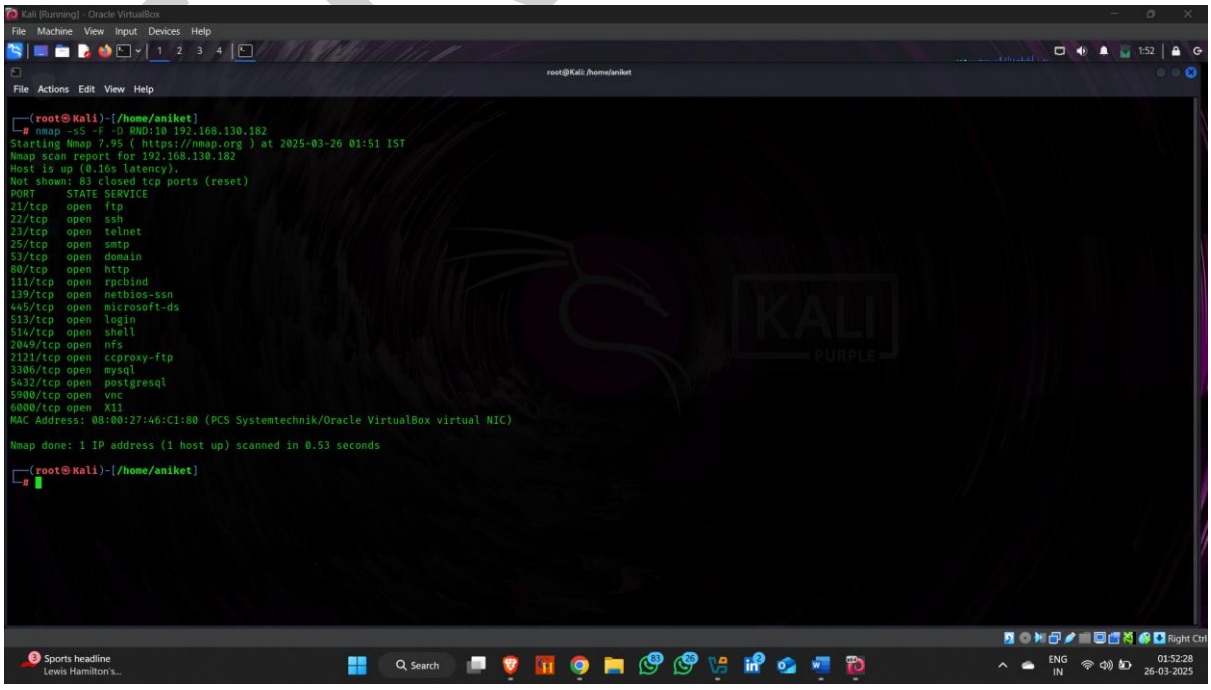


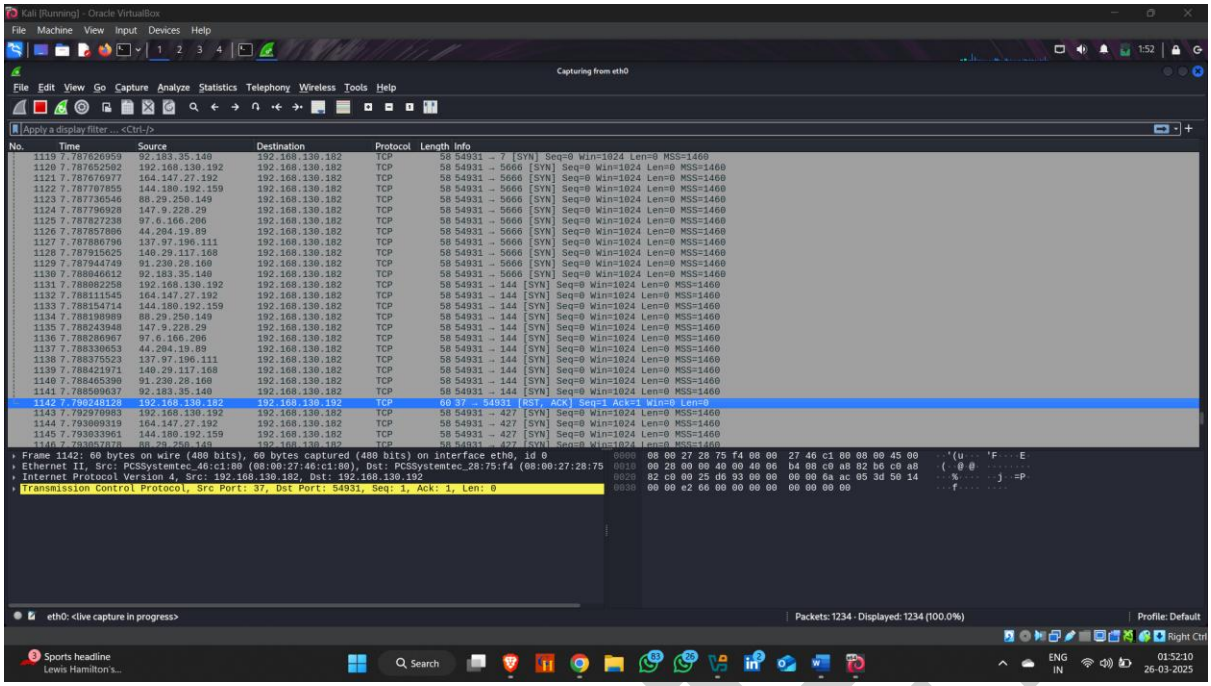



- --spoof-mac -- The **--spoof-mac** option in Nmap allows you to **fake** (spoof) your **MAC address** during a scan.




- -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
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1119 7.787626959 92.183.35.140 192.168.130.182 TCP 58 54931 → 7 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1120 7.787652502 192.168.130.192 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1121 7.787676977 164.147.27.192 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1122 7.787707855 144.180.192.159 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1123 7.787736546 88.29.250.149 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1124 7.787796928 147.9.228.29 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1125 7.787827238 97.6.166.206 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1126 7.787857806 44.204.19.89 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1127 7.787886796 137.97.196.111 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1128 7.787915625 140.29.117.168 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1129 7.787944749 91.230.28.160 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1130 7.788046612 92.183.35.140 192.168.130.182 TCP 58 54931 → 5666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1131 7.788082258 192.168.130.192 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1132 7.788111545 164.147.27.192 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1133 7.788154714 144.180.192.159 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1134 7.788198989 88.29.250.149 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1135 7.788243948 147.9.228.29 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1136 7.788286967 97.6.166.206 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1137 7.788330653 44.204.19.89 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1138 7.788375523 137.97.196.111 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1139 7.788421971 140.29.117.168 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1140 7.788465390 91.230.28.160 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1141 7.788509637 92.183.35.140 192.168.130.182 TCP 58 54931 → 144 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1142 7.790248128 192.168.130.182 192.168.130.192 TCP 60 37 → 54931 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1143 7.792570083 192.168.130.192 192.168.130.182 TCP 58 54931 → 427 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1144 7.793009319 164.147.27.192 192.168.130.182 TCP 58 54931 → 427 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1145 7.793033961 144.180.192.159 192.168.130.182 TCP 58 54931 → 427 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
Frame 1142: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_46:c1:80 (08:00:27:46:c1:80), Dst: PCSSystemtec_28:75:f4 (08:00:27:28:75
Internet Protocol Version 4, Src: 192.168.130.182, Dst: 192.168.130.192
Transmission Control Protocol, Src Port: 37, Dst Port: 54931, Seq: 1, Ack: 1, Len: 0
0000 08 00 27 28 75 f4 08 00 27 46 c1 80 08 00 45 00
0010 00 28 00 00 40 00 40 06 b4 08 c0 a8 82 b6 c0 a8
0020 82 c0 00 25 d6 93 00 00 00 00 6a ac 05 3d 50 14
0030 00 00 e2 66 00 00 00 00
eth0: <live capture in progress>
Packets: 1234 · Displayed: 1234 (100.0%)
Profile: Default
Right Ctrl
Sports headline
Lewis Hamilton's...
Search
ENG
IN
01:52:10
26-03-2025

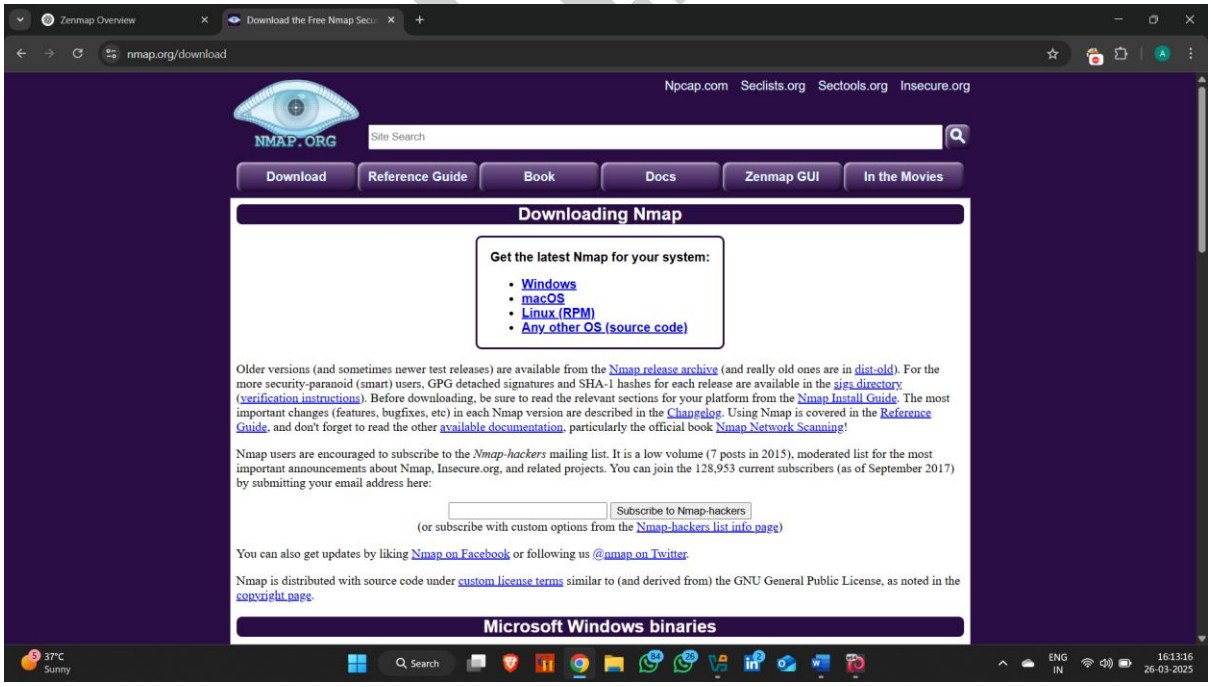
# Network Scanning Using Zenmap.

**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:

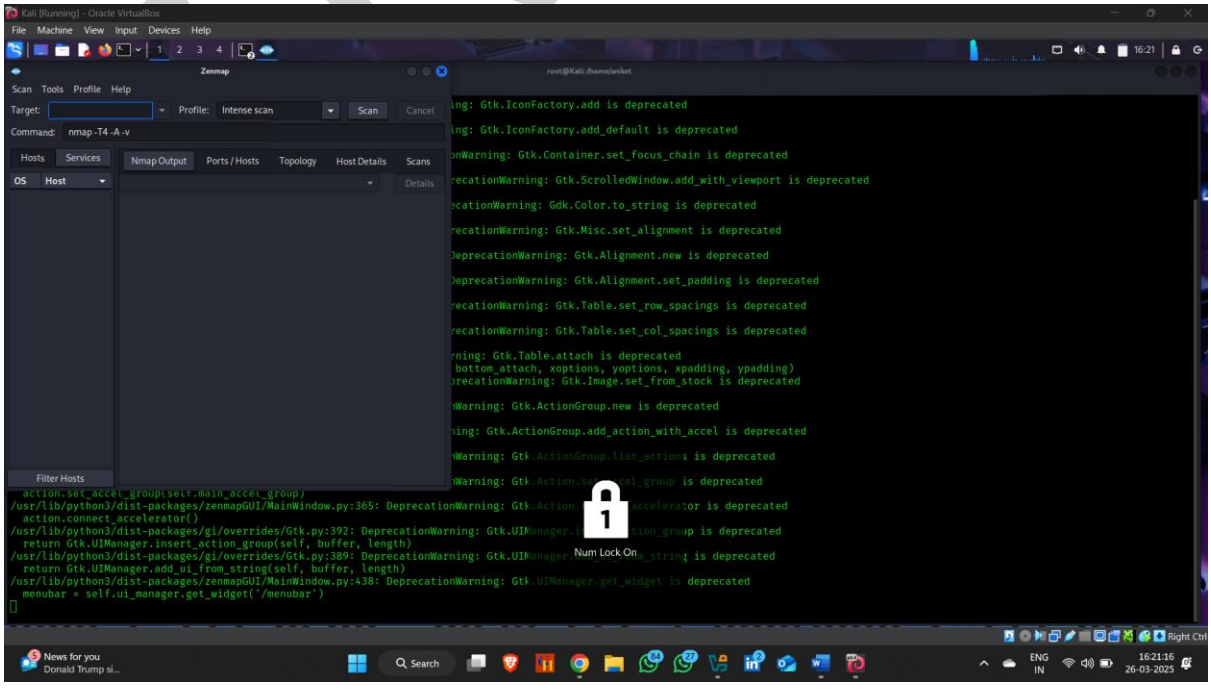
  wget https://old.kali.org/kali/pool/main/n/nmap/zenmap_7.80-1_all.deb

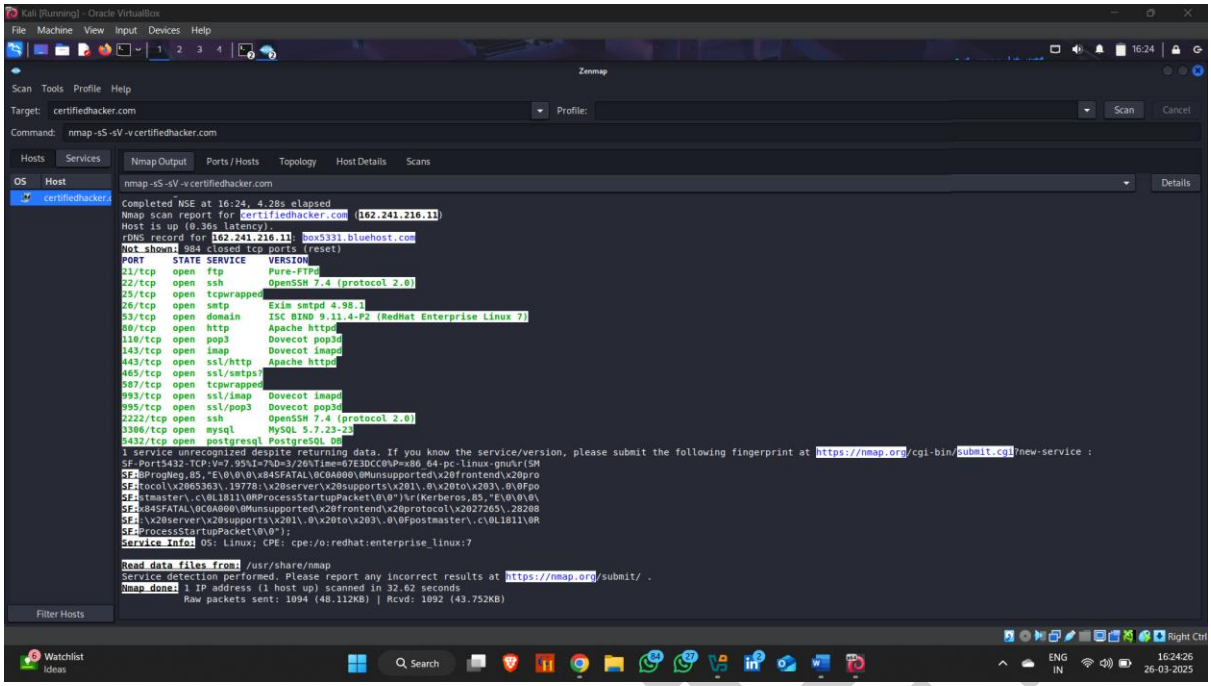
- Step 4 : install the downloaded package:

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

- Step 5 : **Run Zenmap**

  sudo zenmap






**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.**

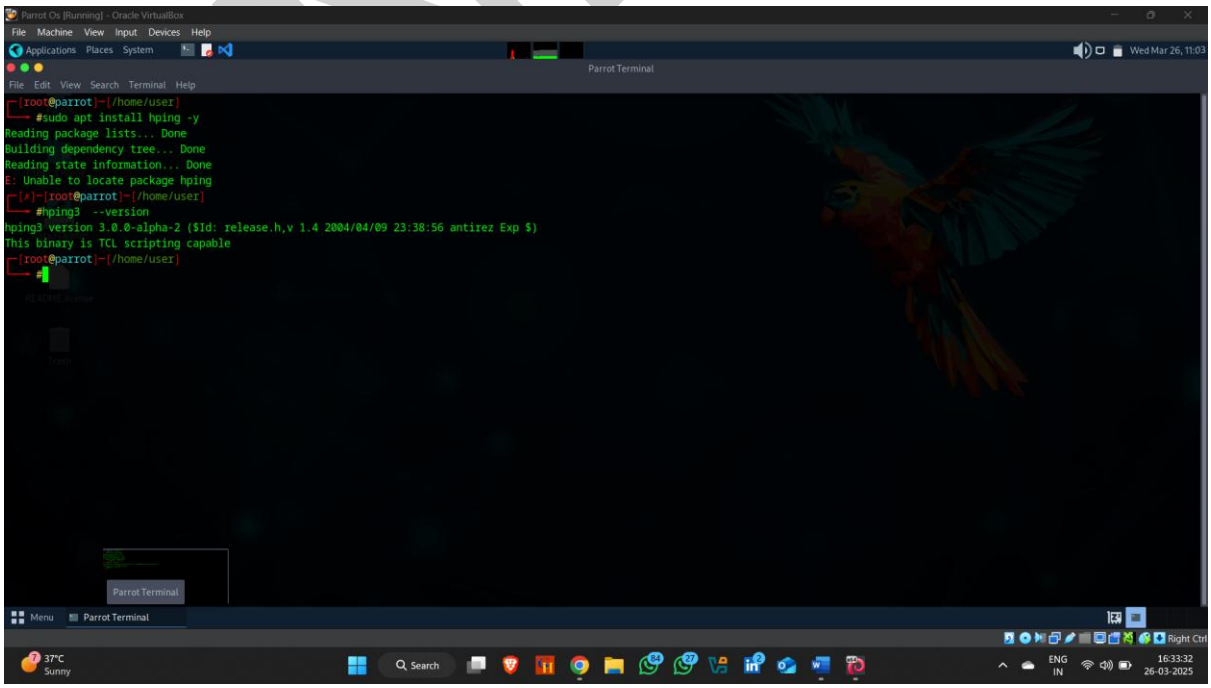
  sudo apt update && sudo apt upgrade -y.

- **Step 2: Install Hping3**

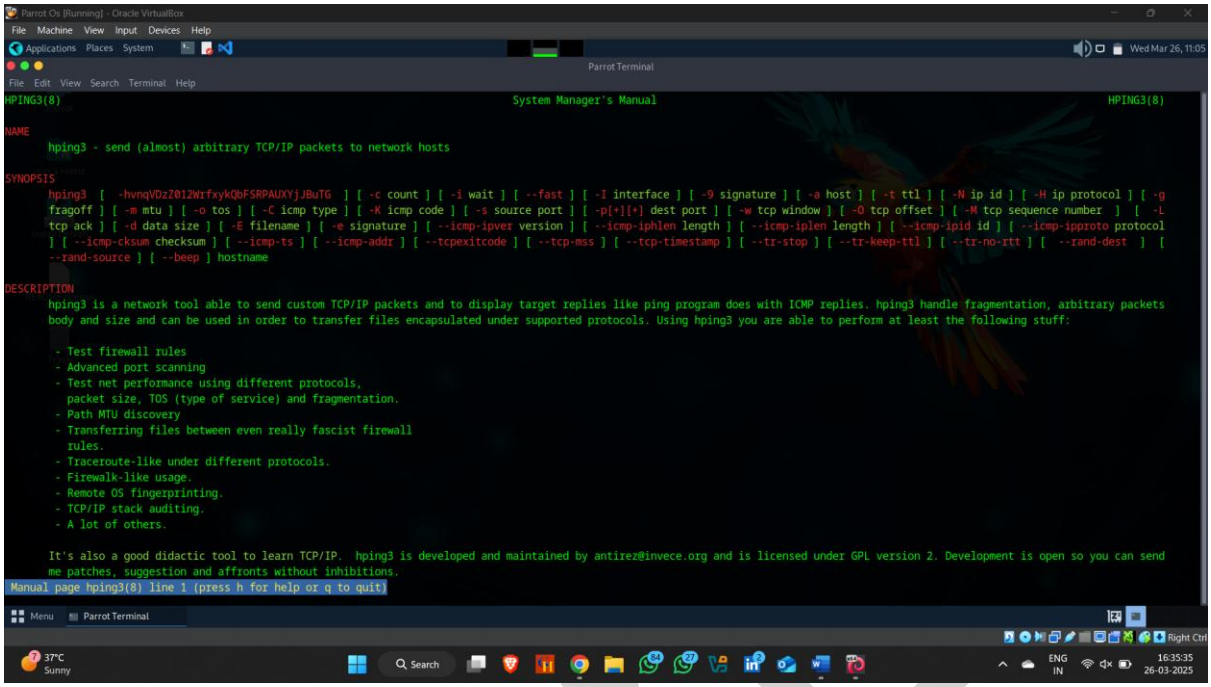
  sudo apt install hping3 -y

- **Step 3: Verify the Installation**

  hping3 --version



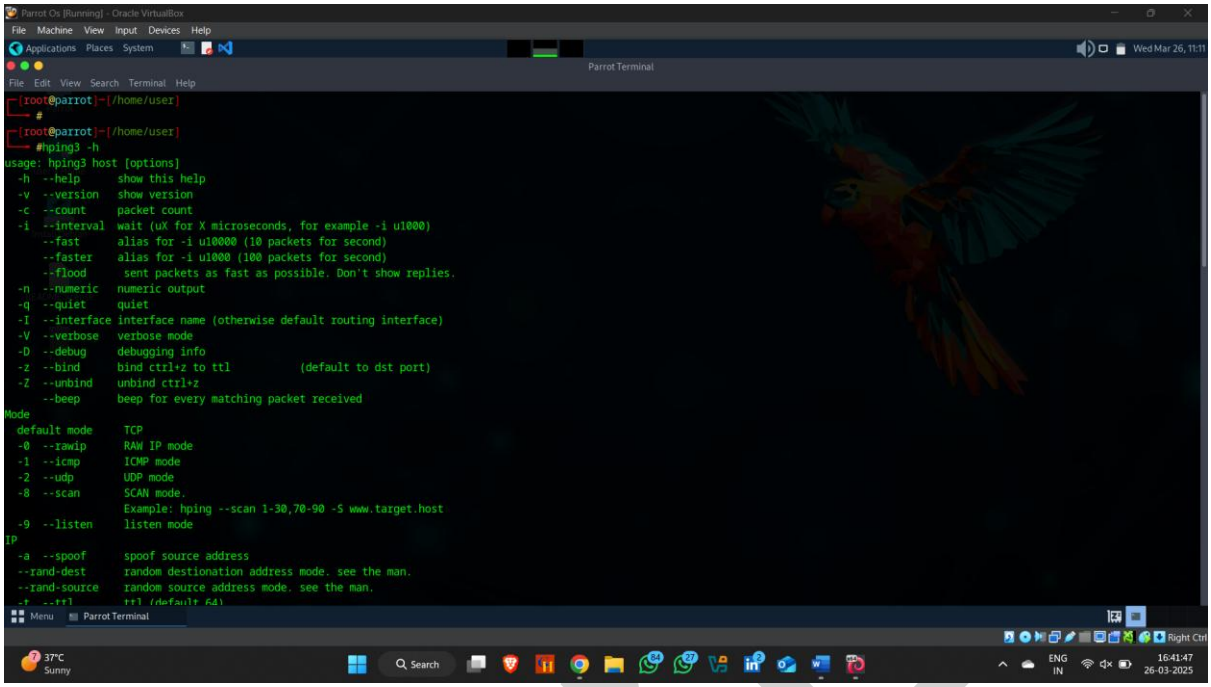
- Use Man hping3 - - To show detail about hping3 .



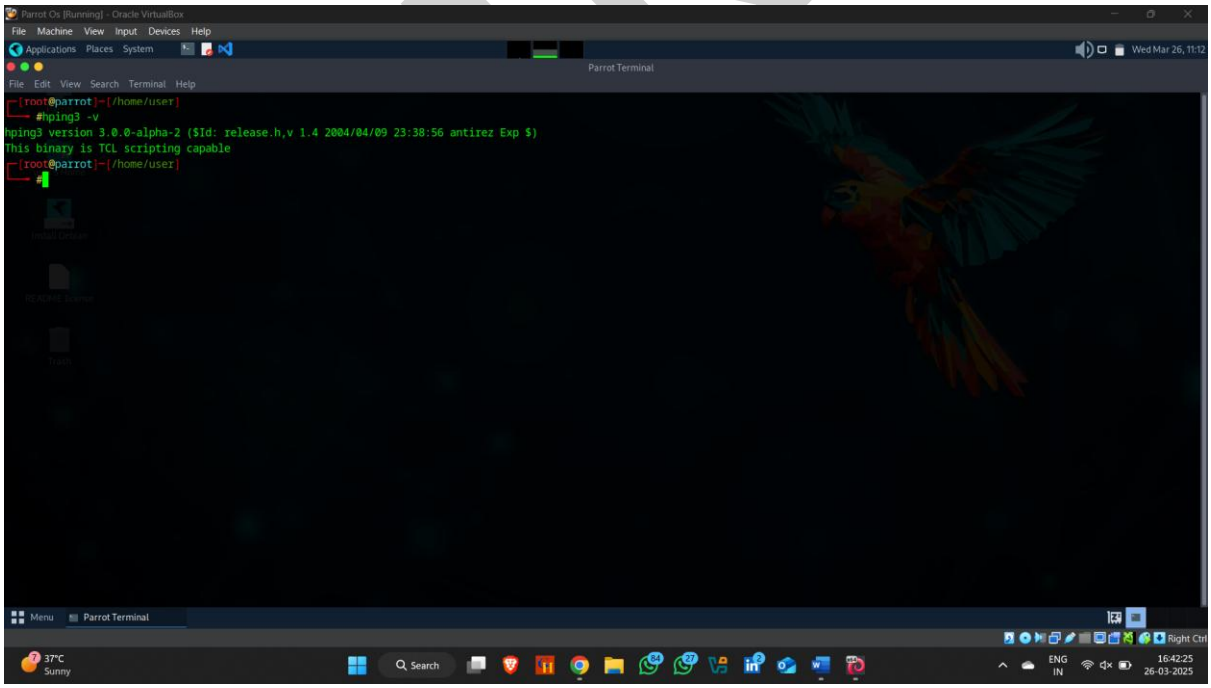

## Common Usage Commands –

- -h – help .
- -v – version .
- --fast .
- --faster.
- --flood.
- -V –verbose.
- -1 –ICMP.
- -2 –UDP .
- -8 –Scan .
- -f –fragments.
- -S - -SYN Flag
- -A - - ACK Flag
- -U - - URG Flag
- -R - - RST Flag
- -P - - PUSH Flag
- -X – Xmass

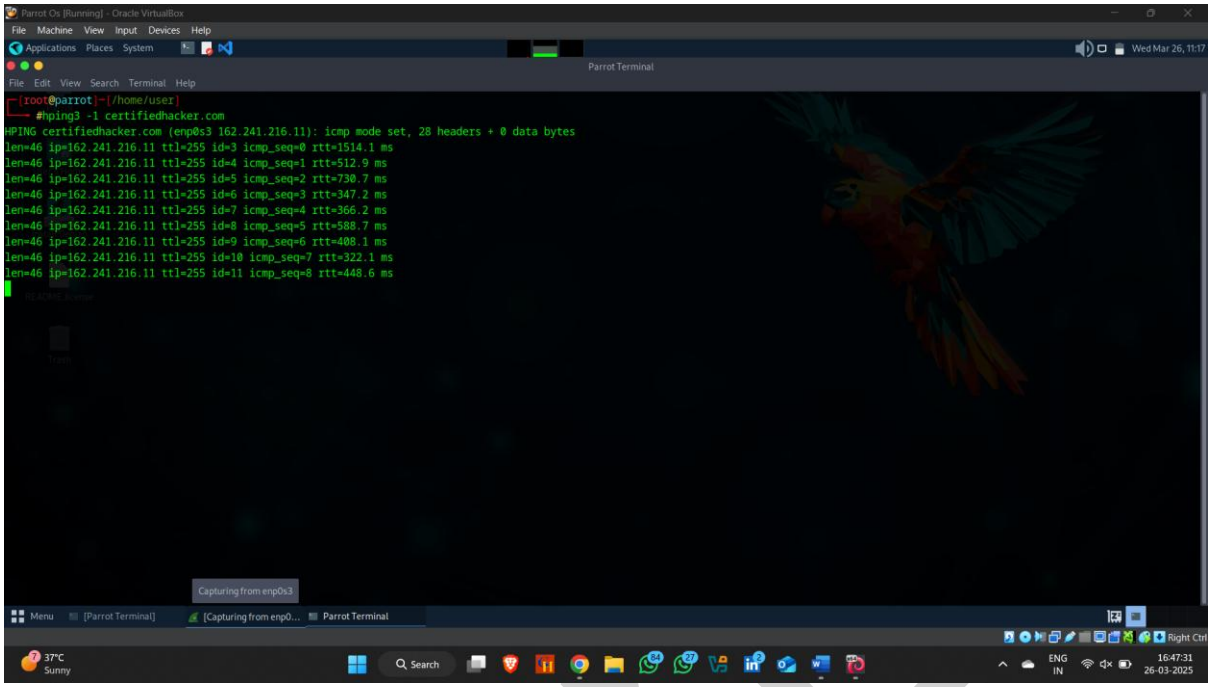
- -h – help

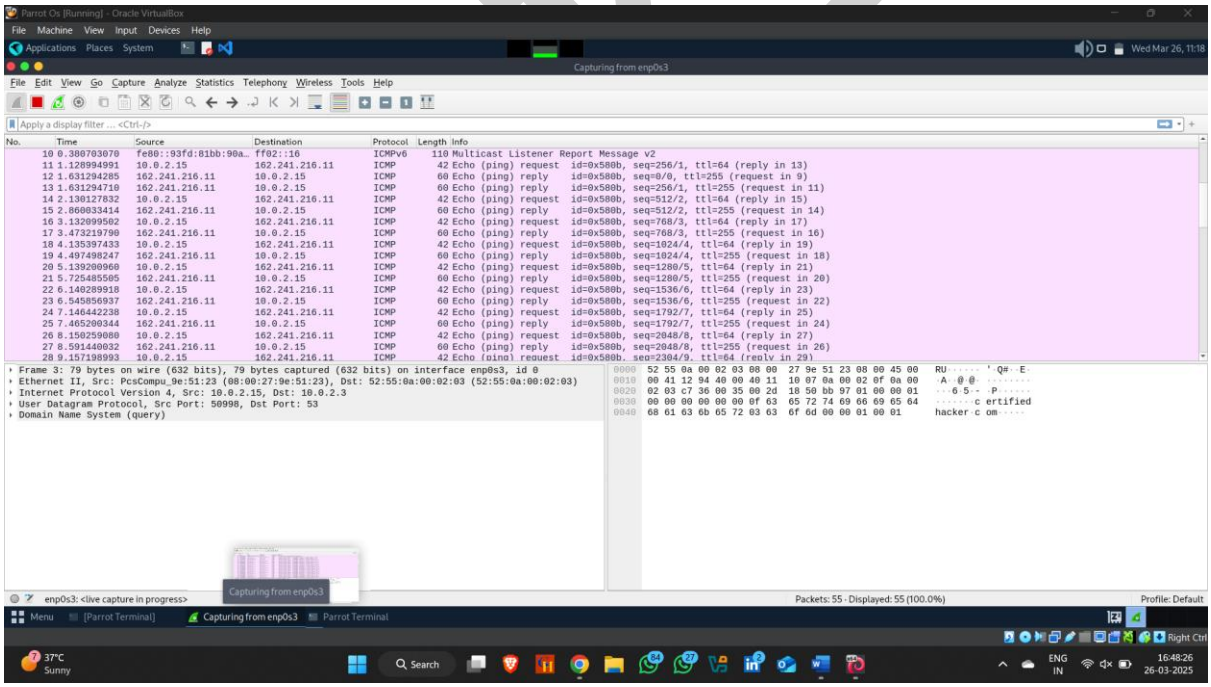



- -v - - Version

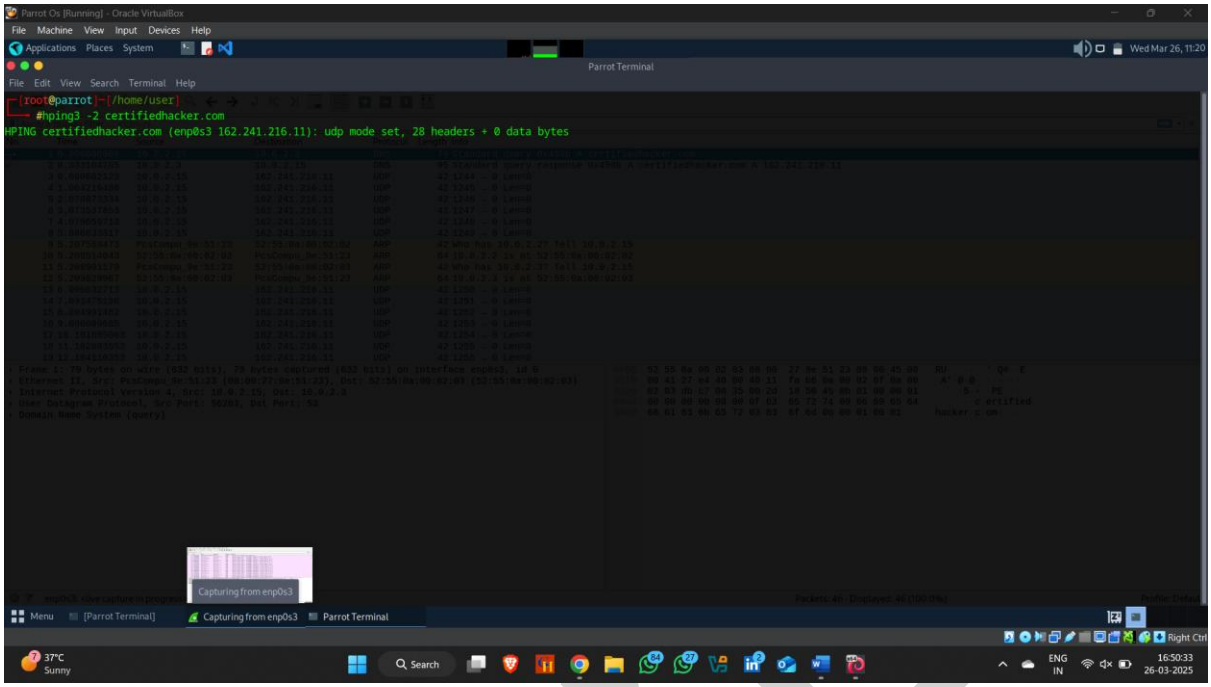


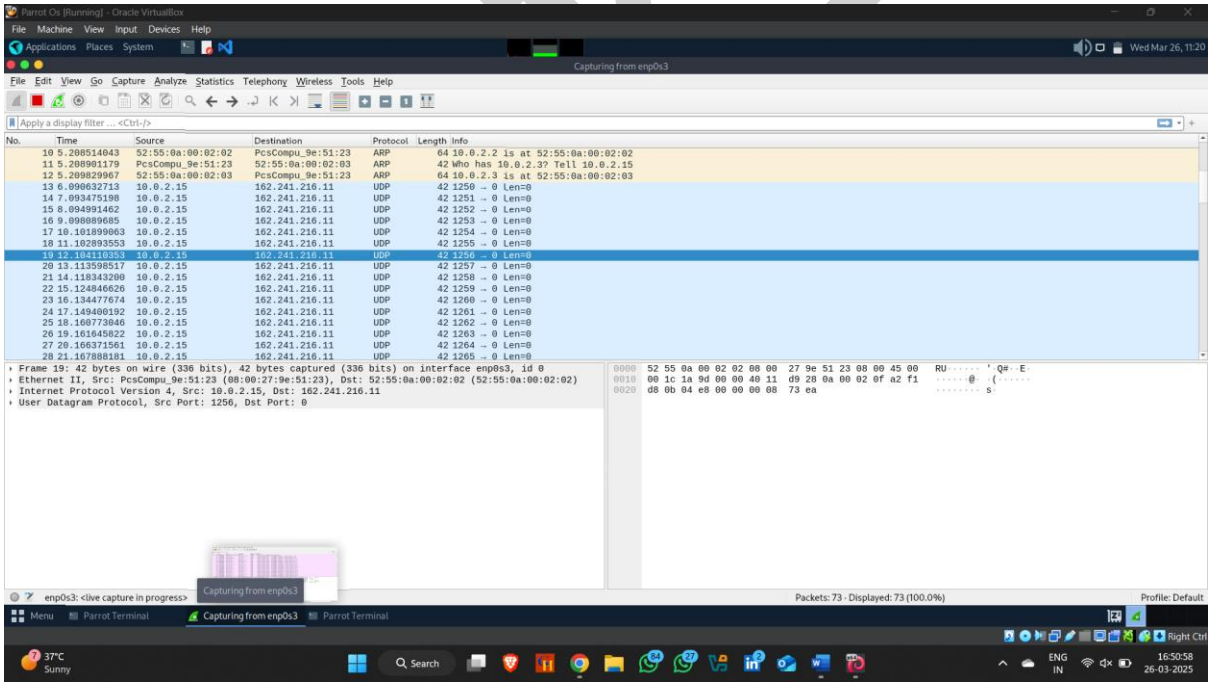
- -1 - - Sends ICMP Packets



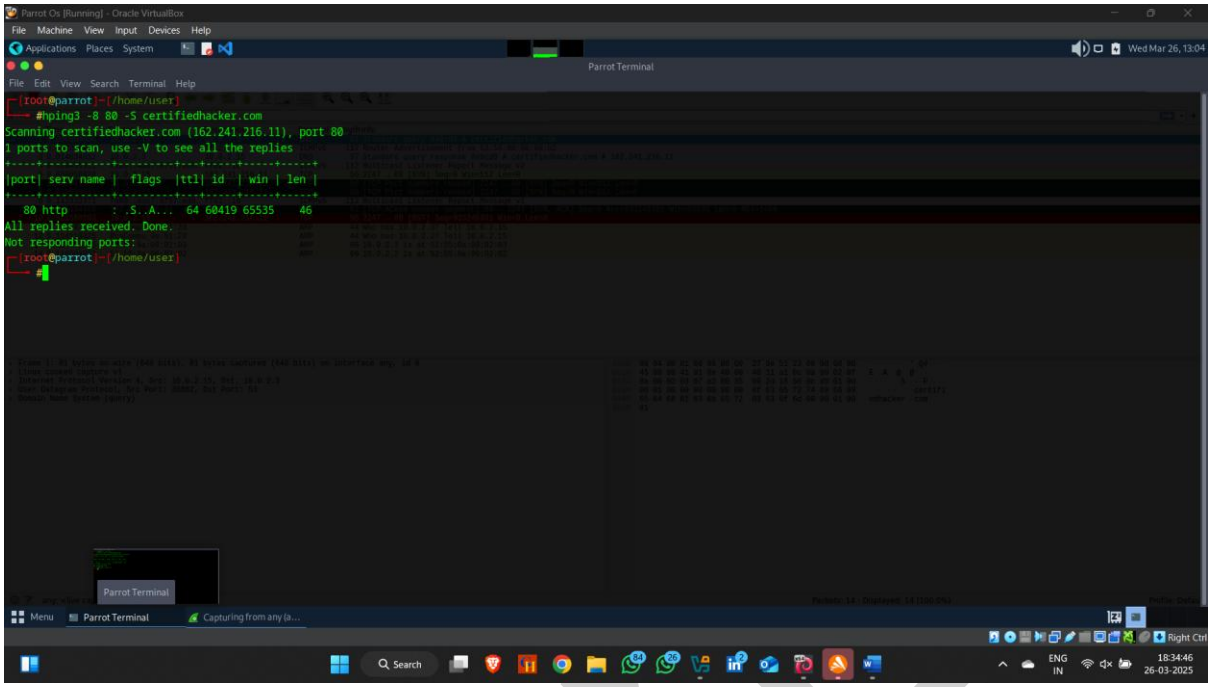



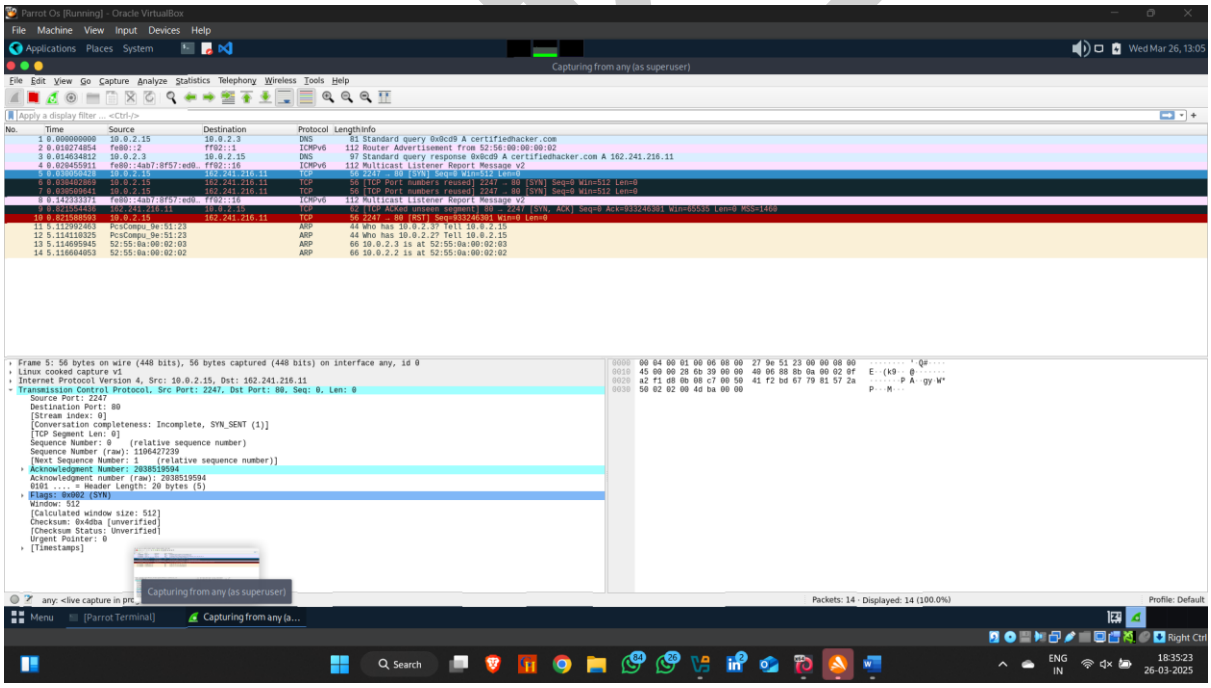
- -2 - - UDP packets send



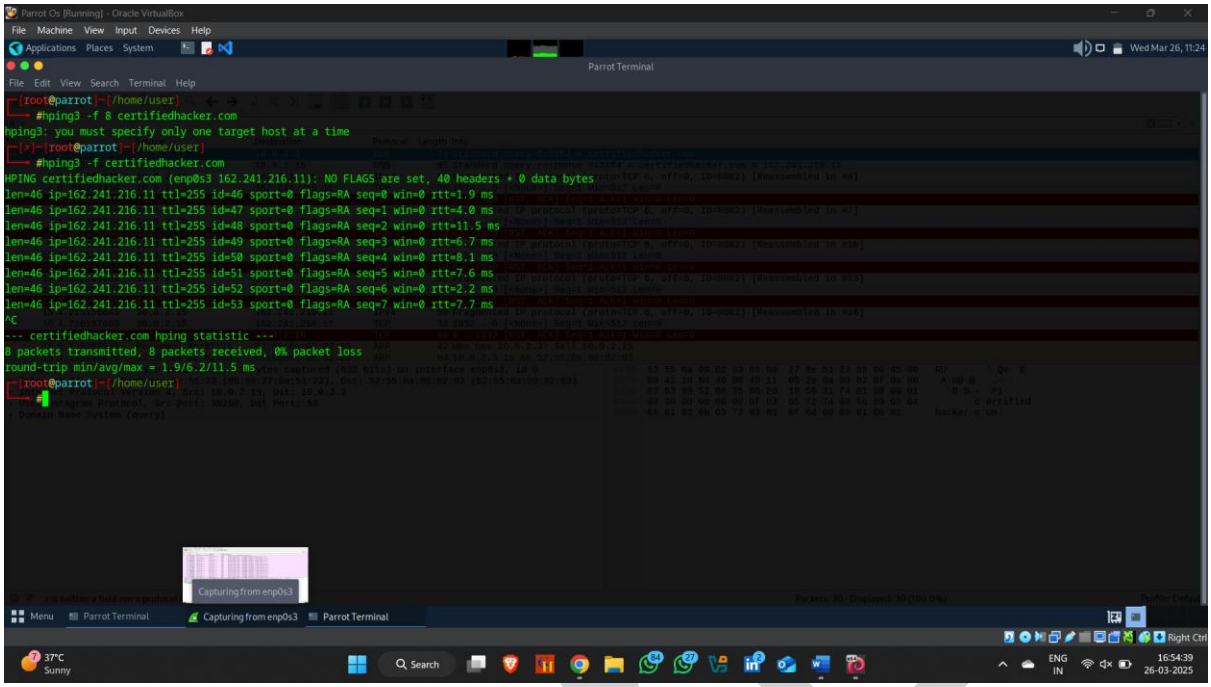



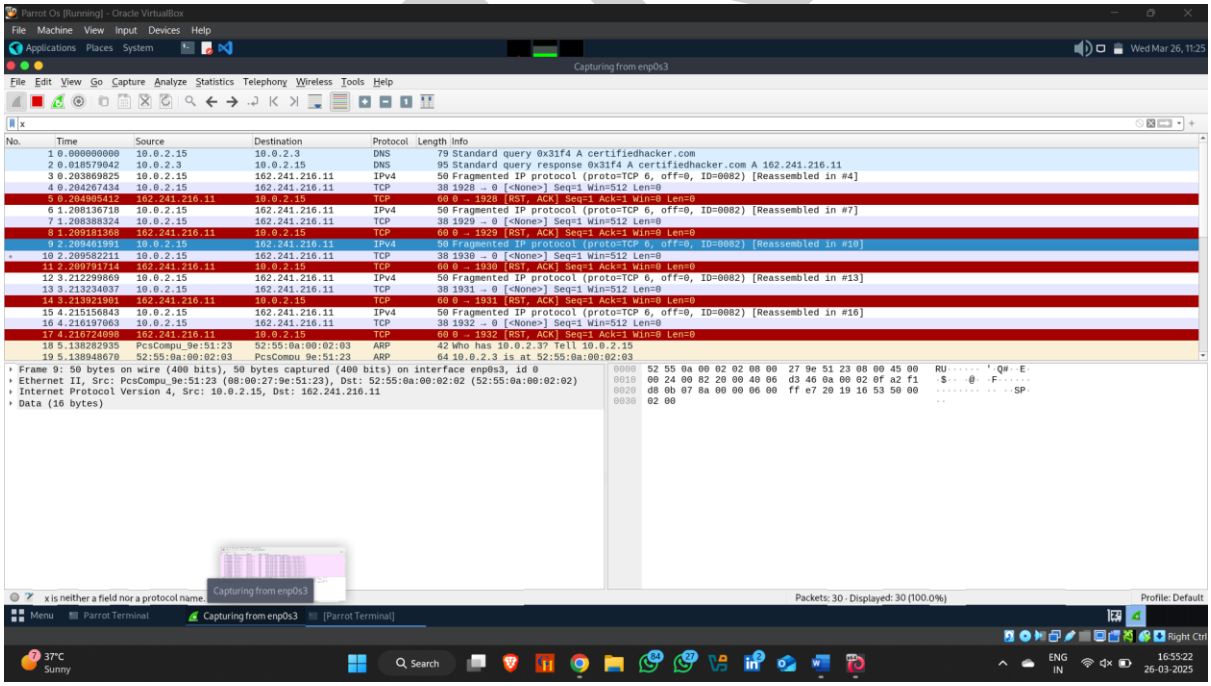
- -S – SYN Flag


Parrot Terminal
#hping3 -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:
#


Capturing from any (as superuser)
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
Flags: 0x002 (SYN)
Window: 512

- -f – fragmentation.

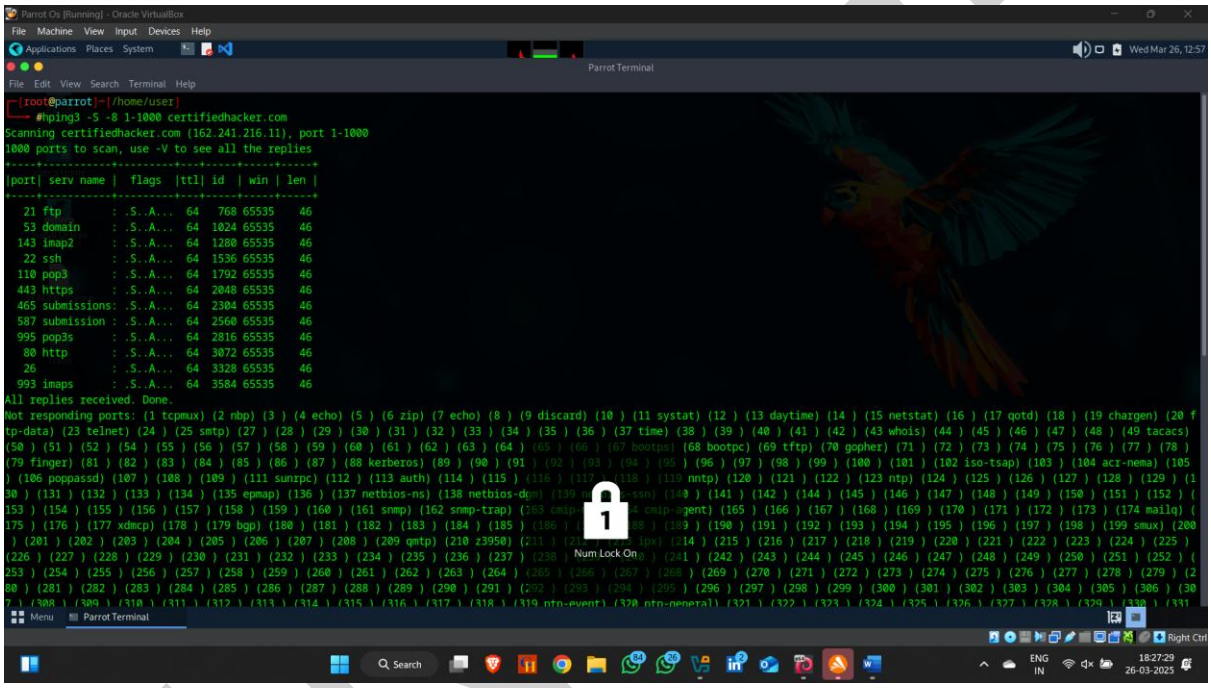


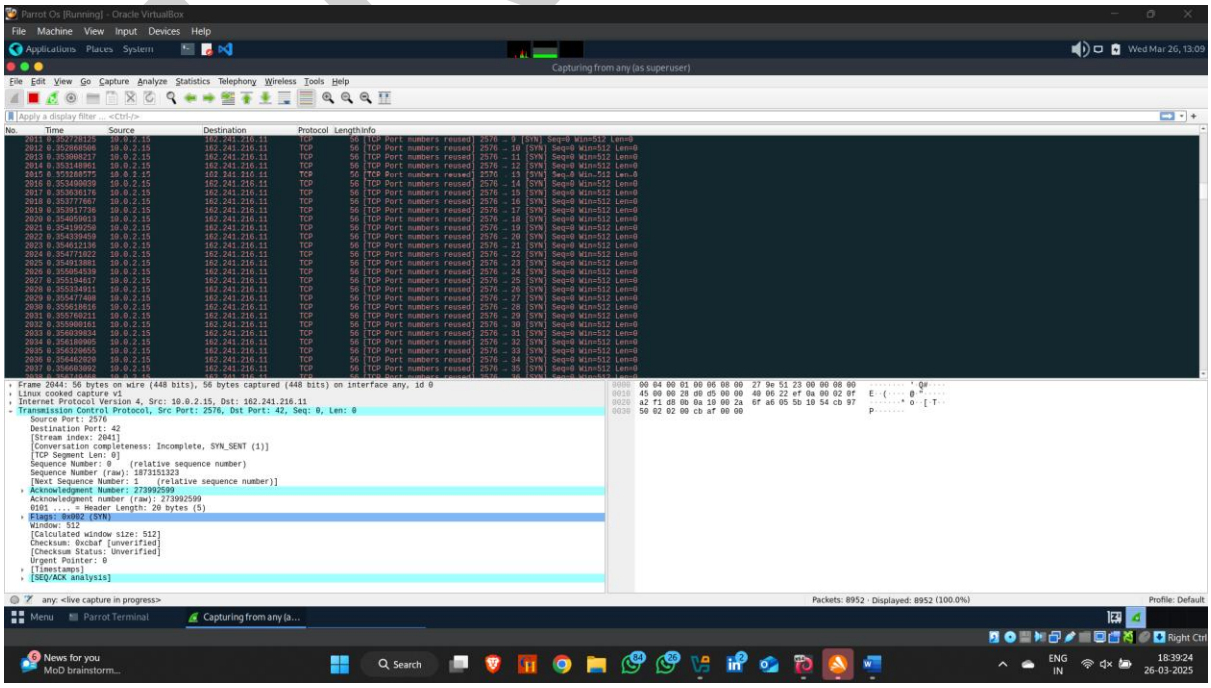



# Port Scanning Using Hping3

**Command –**

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



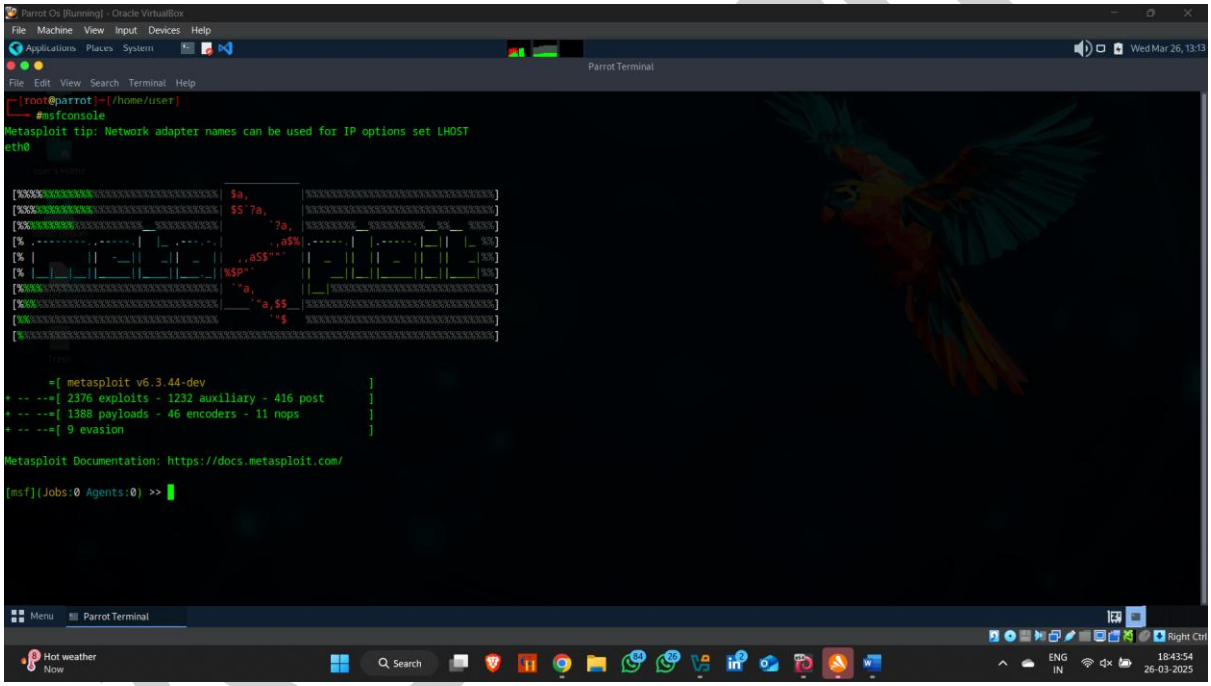



# Port Scanning Using Metasploit.

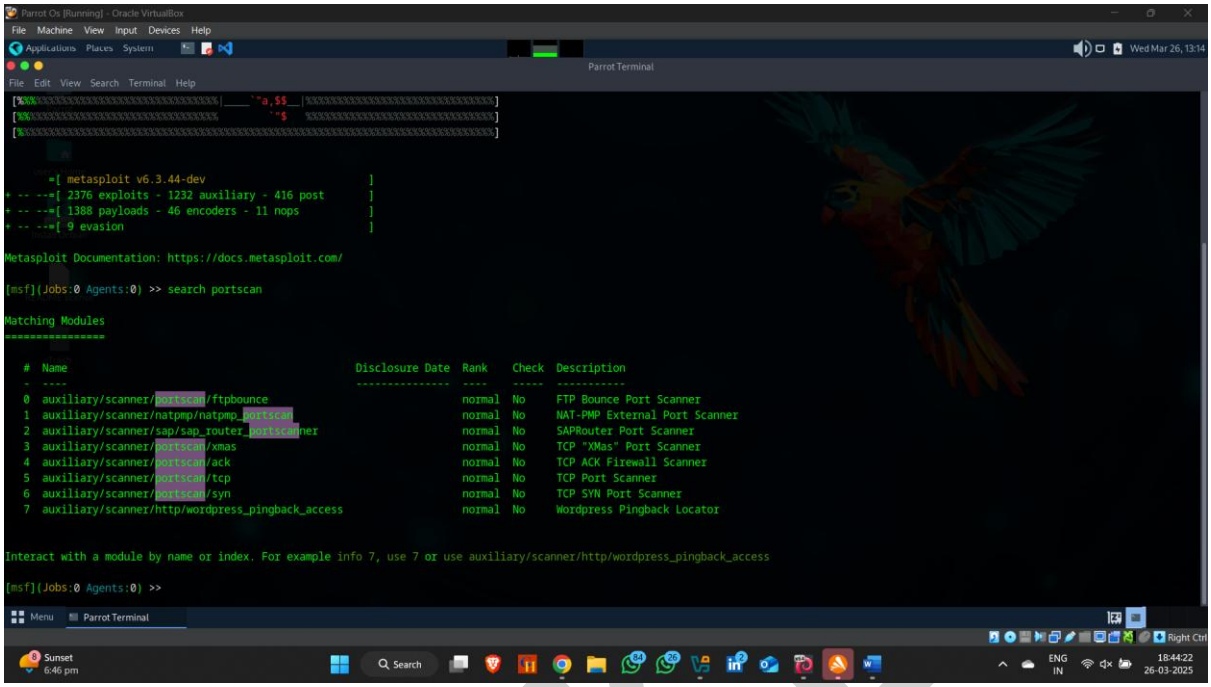
Metasploit offers powerful tools to identify open ports, services, and potential vulnerabilities on a target system.

**How to use it -:**

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

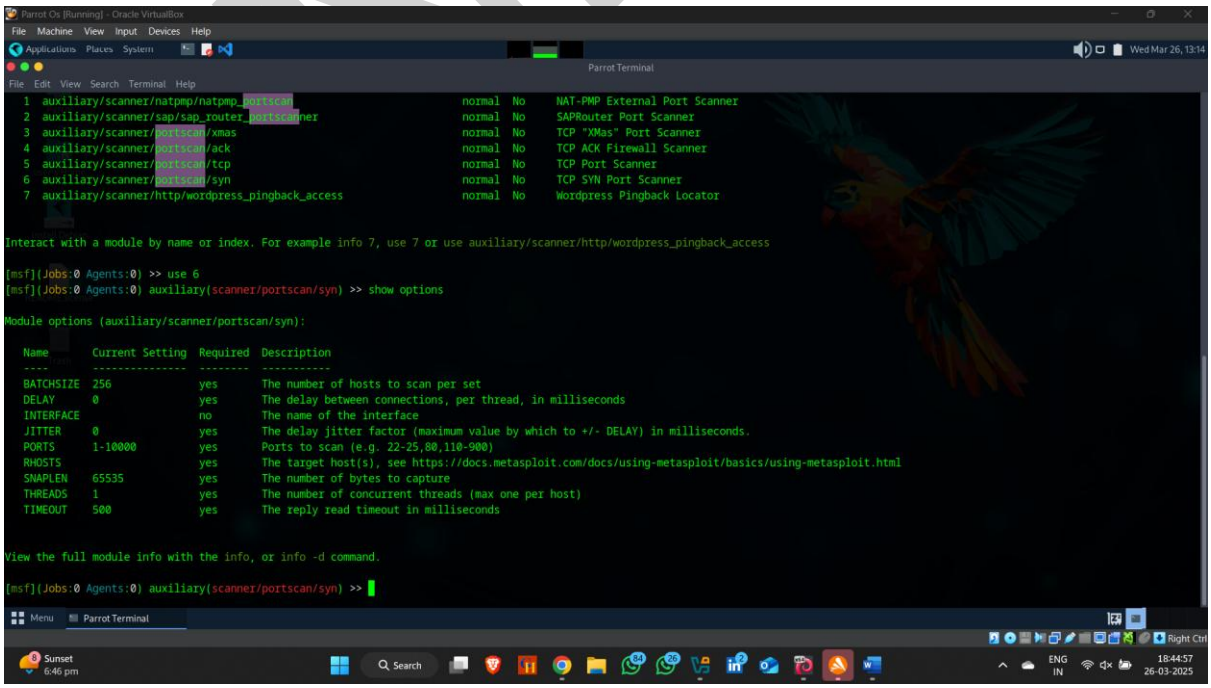


Step 2 : type **search portscan**

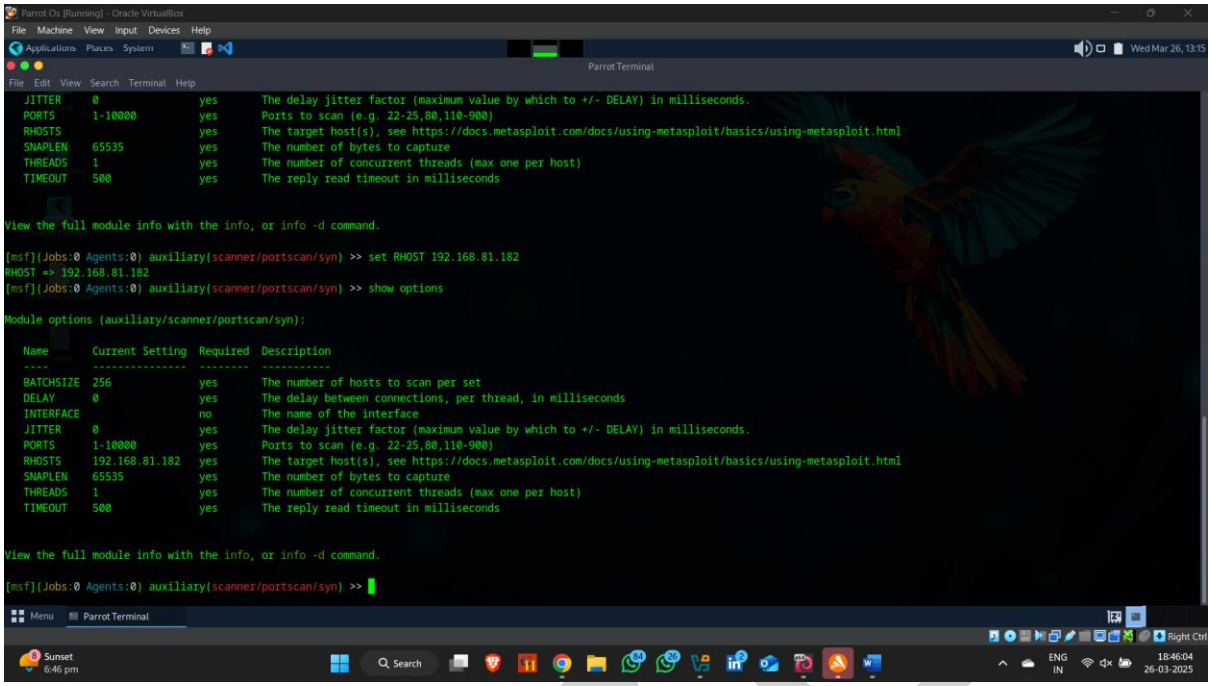



Step 3 : type **use <number of port scan >** to set which port scan are you want and press enter and then type **show option** to check , selected port scan number is set or not

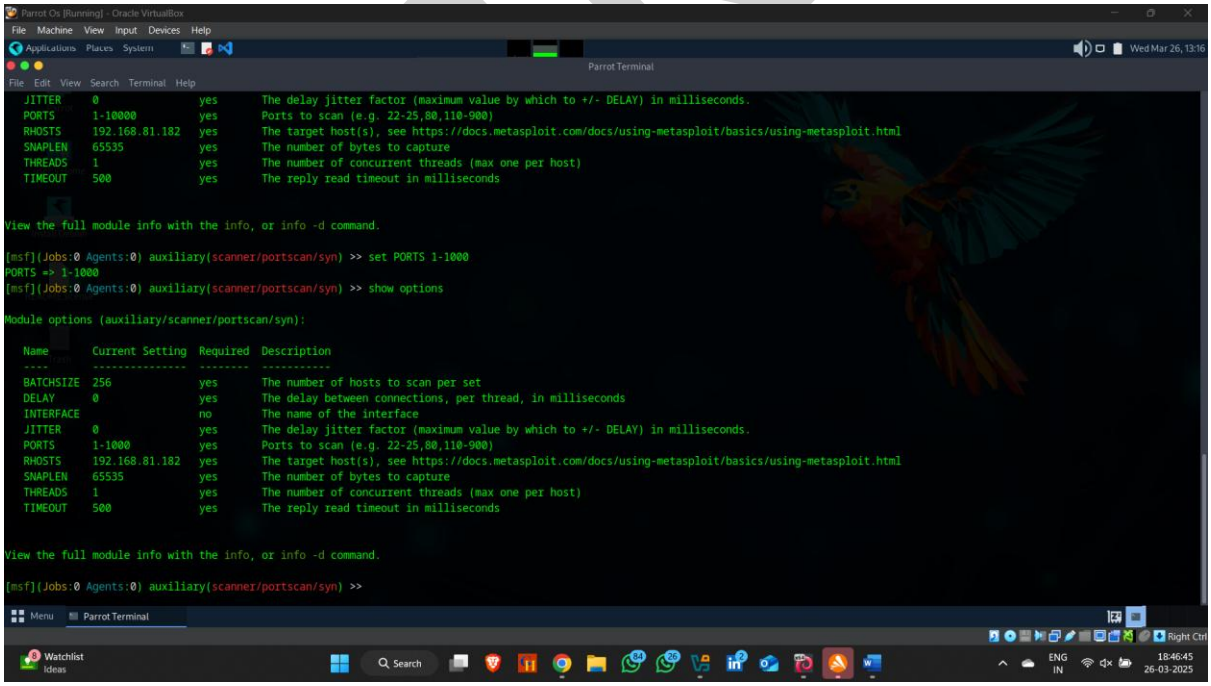
- Example - : use 6



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




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



Step 6 : type **run .**