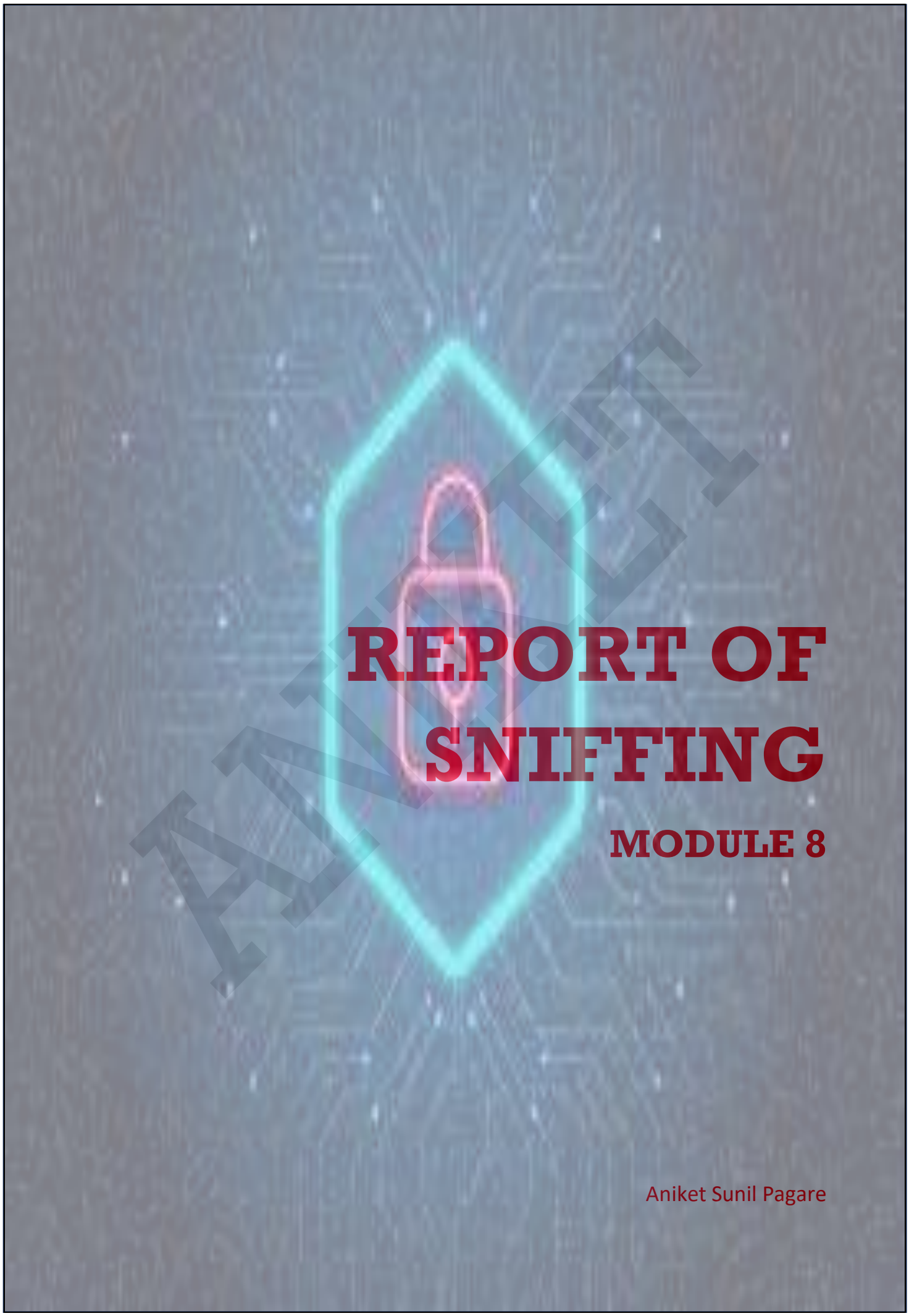


REPORT OF SNIFFING

MODULE 8

Aniket Sunil Pagare

Table of Contents

Extra Activities

6.MAC Flooding

- Perform MAC Flooding Using Scapy
- Perform MAC Flooding Using Hping3
- Perform MAC Flooding Using Ettercap
- Perform MAC Flooding Using Bettercap

7.DHCP Starvation

- Perform DHCP Starvation Using DHCPig
- Perform DHCP Starvation Using DHCPstarv

8.MAC Spoofing

- Perform MAC Spoofing Using SMAC
- Perform MAC Spoofing Using MAC Address Changer

9.ARP Poisoning

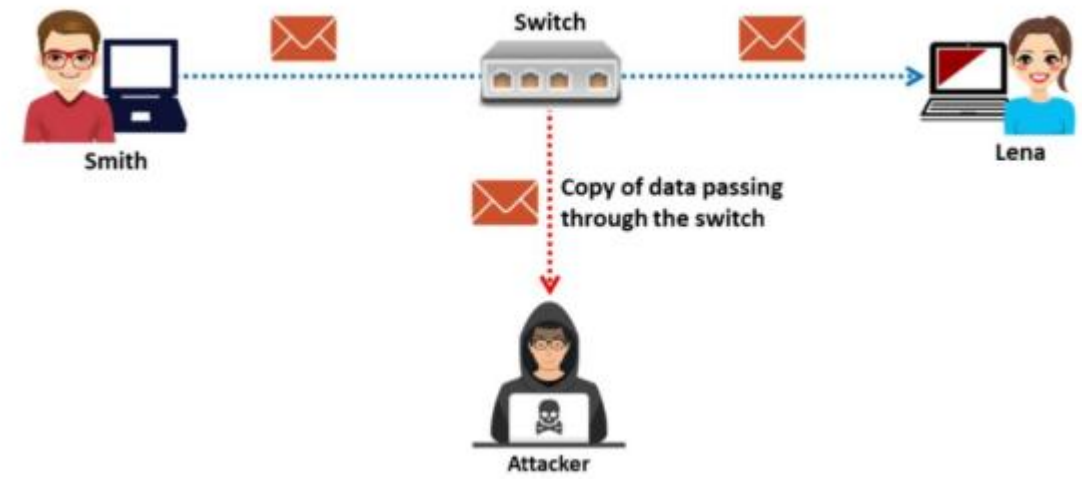
- Perform ARP Poisoning Using Ettercap
- Perform ARP Poisoning Using Bettercap
- Perform ARP Poisoning Using ARP Spoofing

10.Passive Sniffing

- Perform Passive Sniffing Using TCPDump
- Perform Passive Sniffing Using Wireshark

SNIFFING

Packet Sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware devices .



Objectives -:

- Monitor network traffic
- Detect network issues
- Capture login credentials
- Analyze data packets
- Identify unauthorized users
- Detect suspicious activities

Type of Sniffing –

1.Active Sniffing

2.Passive Sniffing

Active Sniffing

- **Definition:** Actively sends packets into the network to intercept traffic on switched networks**.**
- **Used in:** Switched LANs, where traffic is not broadcast to all devices.

- **Techniques Involved:**
- ARP Spoofing/Poisoning
- MAC Flooding
- DHCP Starvation

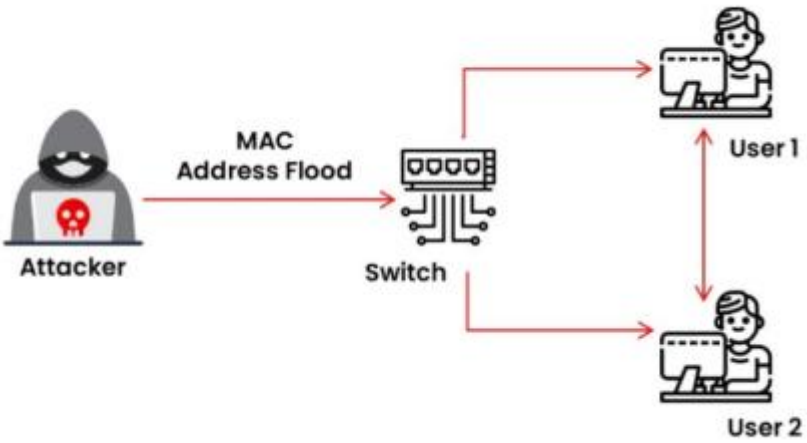
Passive Sniffing

- **Definition:** Silently listens to network traffic without interfering
- **Used in**: Hubs or broadcast networks, where all traffic is visible to all devices**.**

MAC FLOODING

MAC Flooding -:

MAC Flooding is a network attack where an attacker sends a large number of fake MAC addresses to a switch, causing it to overflow its MAC address table and start broadcasting all traffic to all ports, allowing the attacker to capture sensitive data.

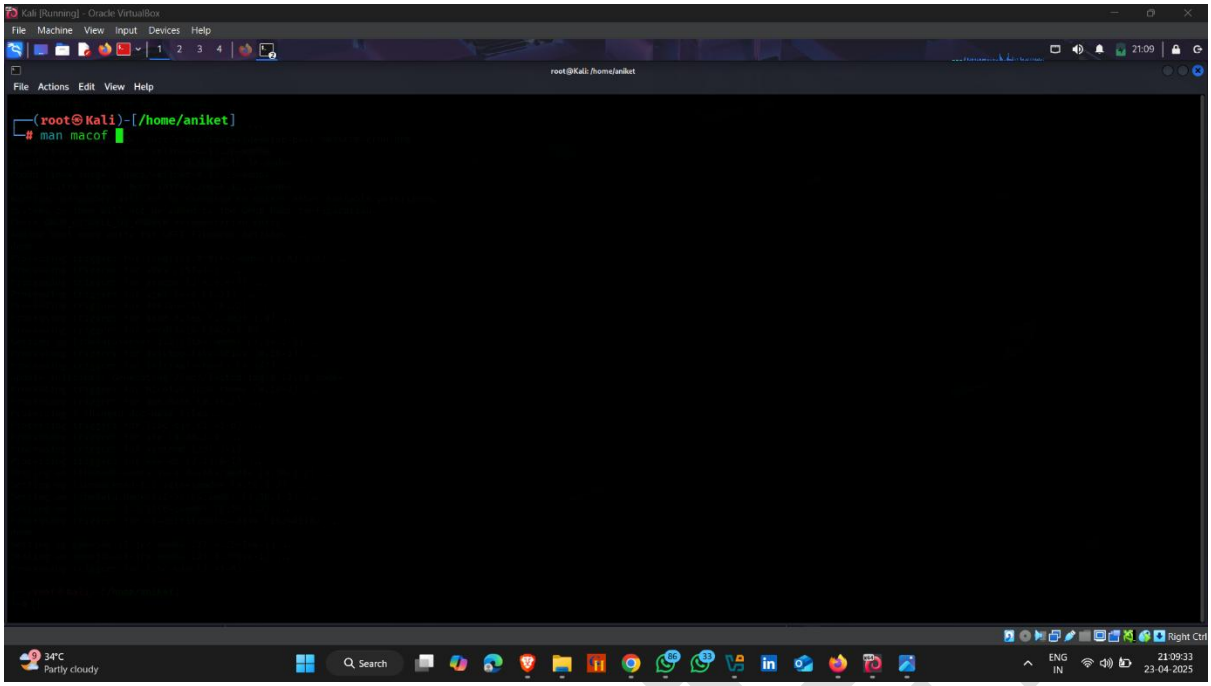


MAC Flooding Attack

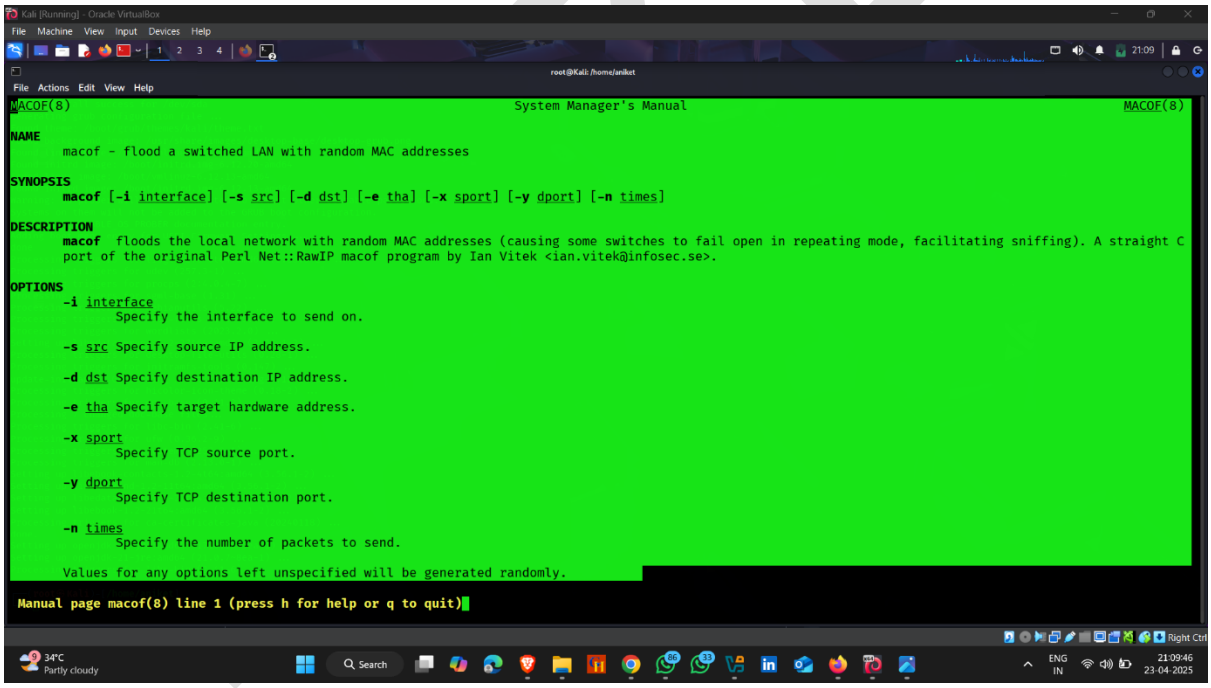
1.Mac Flooding Attack Using Macof (Linux Tool)

How to use it - :

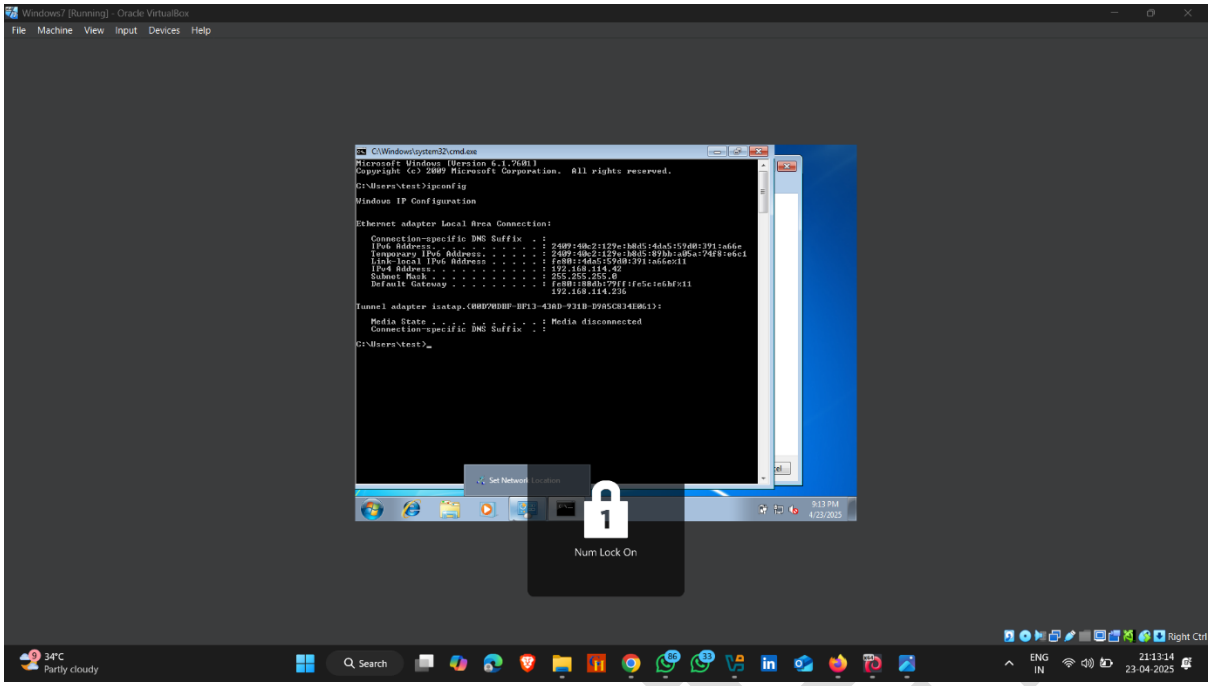
- Open kali linux / parrot os terminal
- Type sudo **apt install macof**
- Then get detailed information about macof , simply type **man macof**



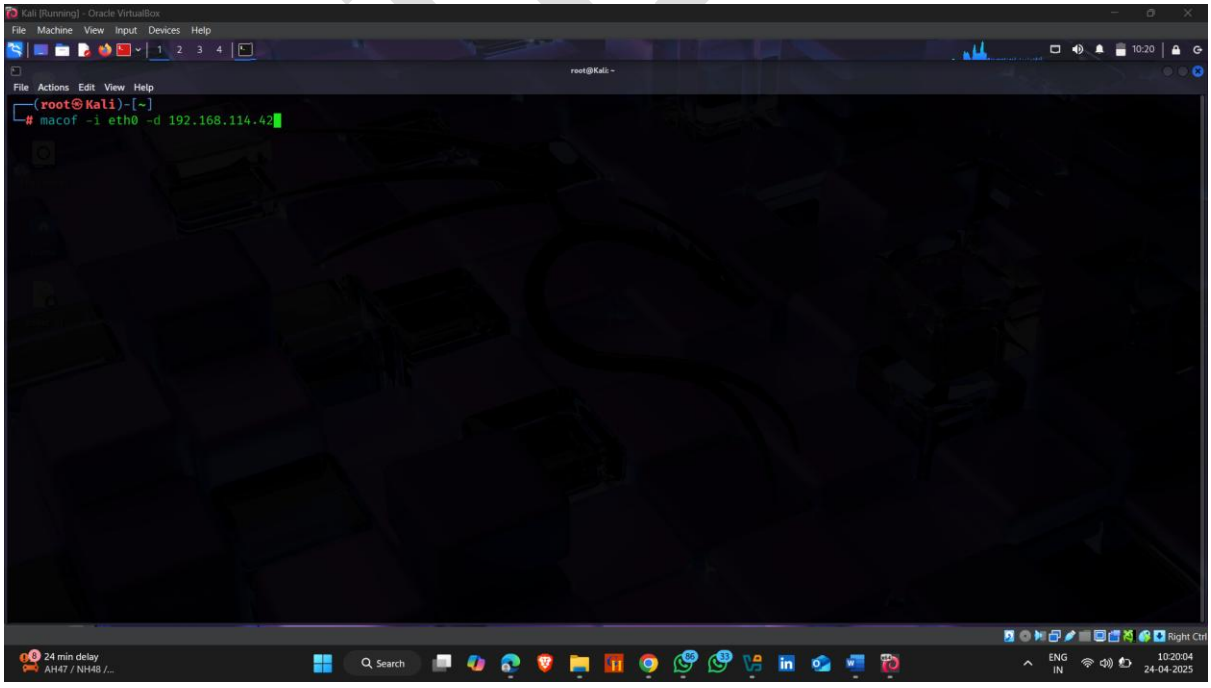
- Here you get the detailed information about macof



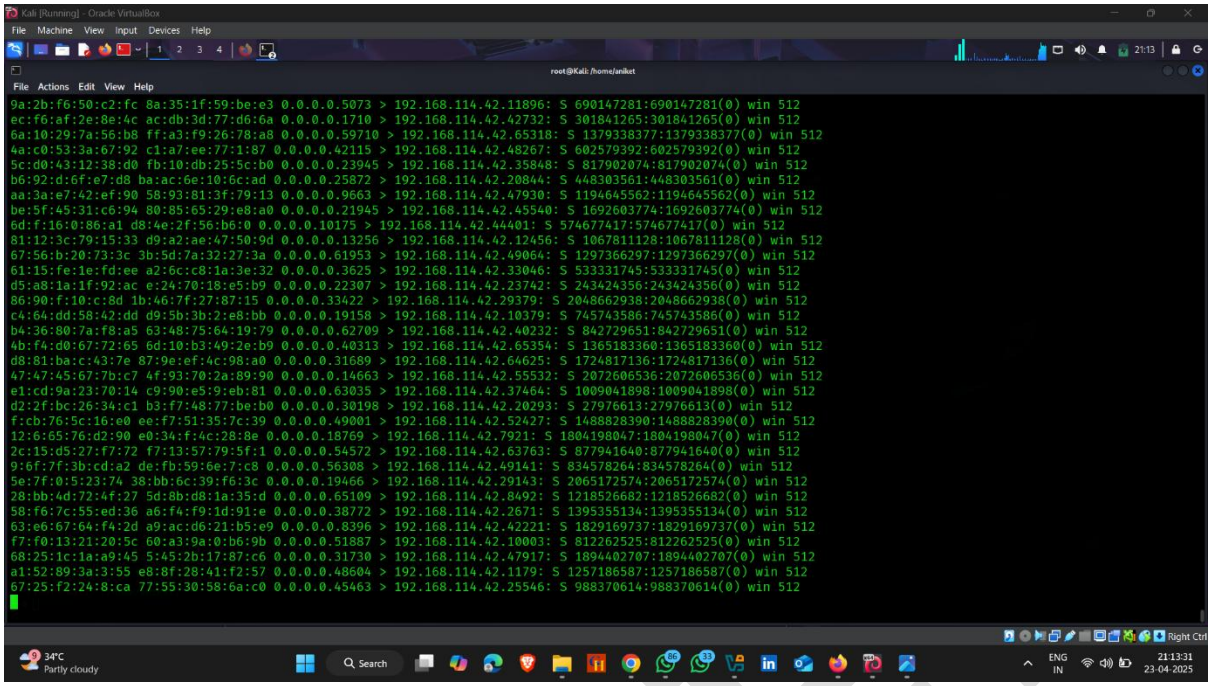
- Target machine Ip



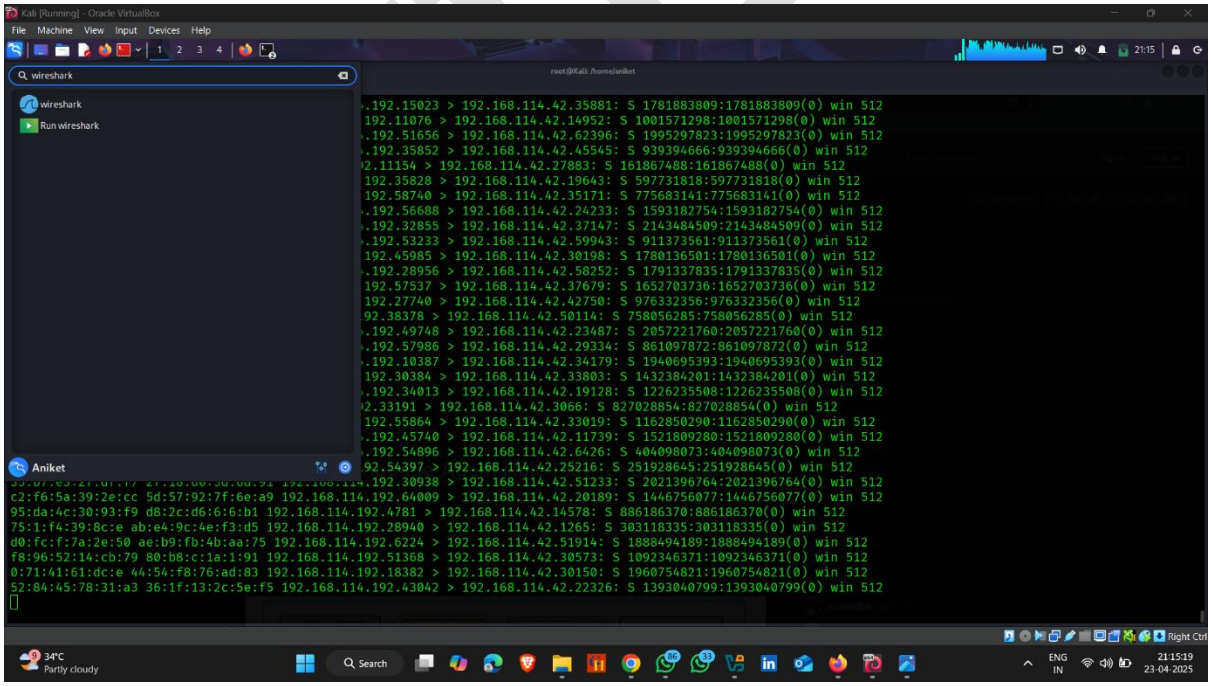
- Perform attack
- Type - : macof -I eth0 -d <target ip >
  -I → network interface
  -d → destination ip



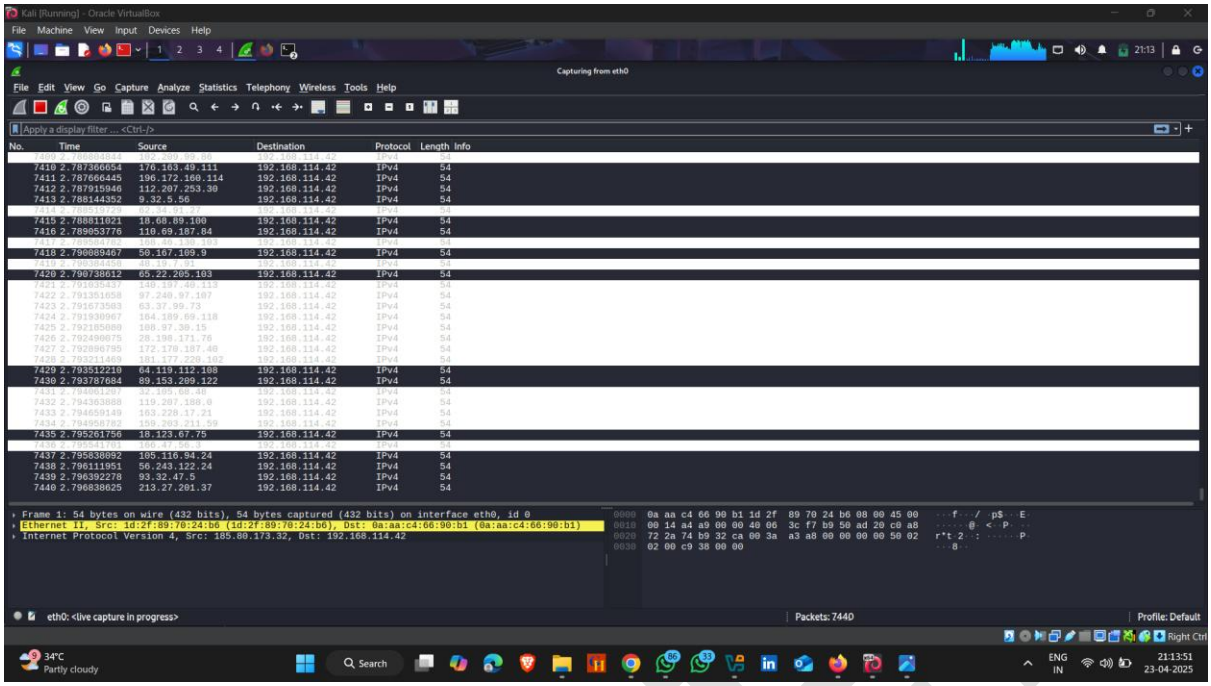
- Mac Flooding attack start



- Now monitoring the attack using Wireshark
- Open Wireshark



- Packet sending start


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
7410 2.787366654 176.163.49.111 192.168.114.42 IPv4 54
7411 2.787666445 196.172.160.114 192.168.114.42 IPv4 54
7412 2.787919946 112.207.253.30 192.168.114.42 IPv4 54
7413 2.788144352 9.32.5.56 192.168.114.42 IPv4 54
7415 2.788811021 18.68.89.100 192.168.114.42 IPv4 54
7416 2.789053776 110.69.187.84 192.168.114.42 IPv4 54
7418 2.790089467 50.167.109.9 192.168.114.42 IPv4 54
7420 2.790738612 65.22.205.103 192.168.114.42 IPv4 54
7422 2.791351658 97.240.97.107 192.168.114.42 IPv4 54
7423 2.791673503 63.37.99.73 192.168.114.42 IPv4 54
7424 2.791930967 164.189.69.118 192.168.114.42 IPv4 54
7425 2.792185080 108.97.30.15 192.168.114.42 IPv4 54
7426 2.792490875 28.198.171.76 192.168.114.42 IPv4 54
7427 2.792896795 172.170.187.46 192.168.114.42 IPv4 54
7429 2.793512210 64.119.112.108 192.168.114.42 IPv4 54
7430 2.793787684 89.153.209.122 192.168.114.42 IPv4 54
7435 2.795261756 18.123.67.75 192.168.114.42 IPv4 54
7437 2.795838092 105.116.94.24 192.168.114.42 IPv4 54
7438 2.796111951 56.243.122.24 192.168.114.42 IPv4 54
7439 2.796392278 93.32.47.5 192.168.114.42 IPv4 54
7440 2.796838625 213.27.201.37 192.168.114.42 IPv4 54
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 1d:2f:89:70:24:b6 (1d:2f:89:70:24:b6), Dst: 0a:aa:c4:66:90:b1 (0a:aa:c4:66:90:b1)
Internet Protocol Version 4, Src: 185.80.173.32, Dst: 192.168.114.42
0000 0a aa c4 66 90 b1 1d 2f 89 70 24 b6 08 00 45 00
0010 00 14 a4 a9 00 00 40 06 3c f7 b9 50 ad 20 c0 a8
0020 72 2a 74 b9 32 ca 00 3a a3 a8 00 00 00 00 50 02
0030 02 00 c9 38 00 00
eth0: <live capture in progress>
Packets: 7440
Profile: Default
Right Ctrl
34°C
Partly cloudy
Search
ENG
IN
21:13:51
23-04-2025

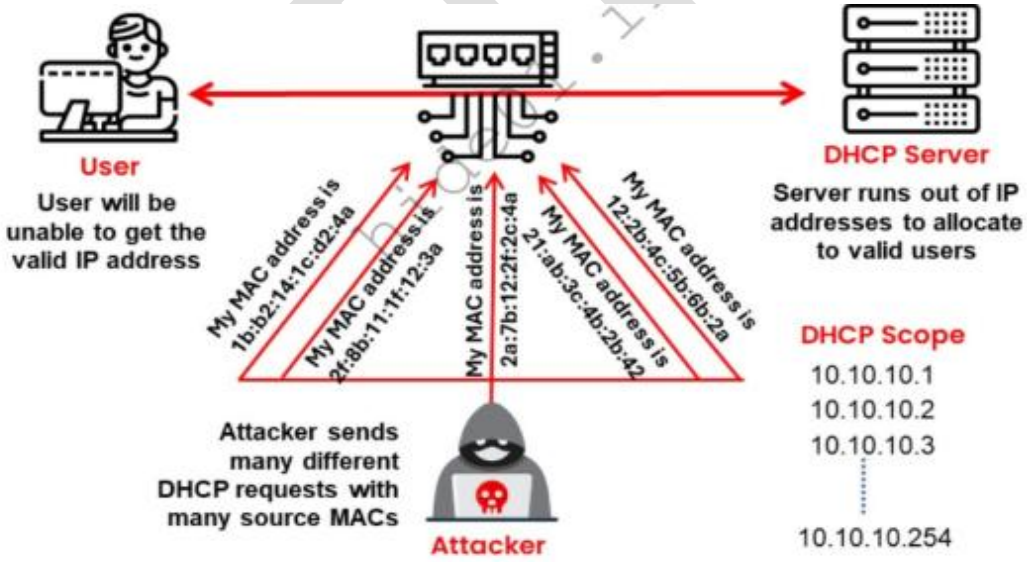
DHCP STARVATION

DHCP Starvation -:

DHCP Starvation is a type of denial-of-service attack where an attacker floods the DHCP server with numerous fake DHCP requests, exhausting the pool of available IP addresses and preventing legitimate devices from obtaining a valid IP address.

DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous DHCP requests and uses all of the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network.



DHCP Starvation Attack

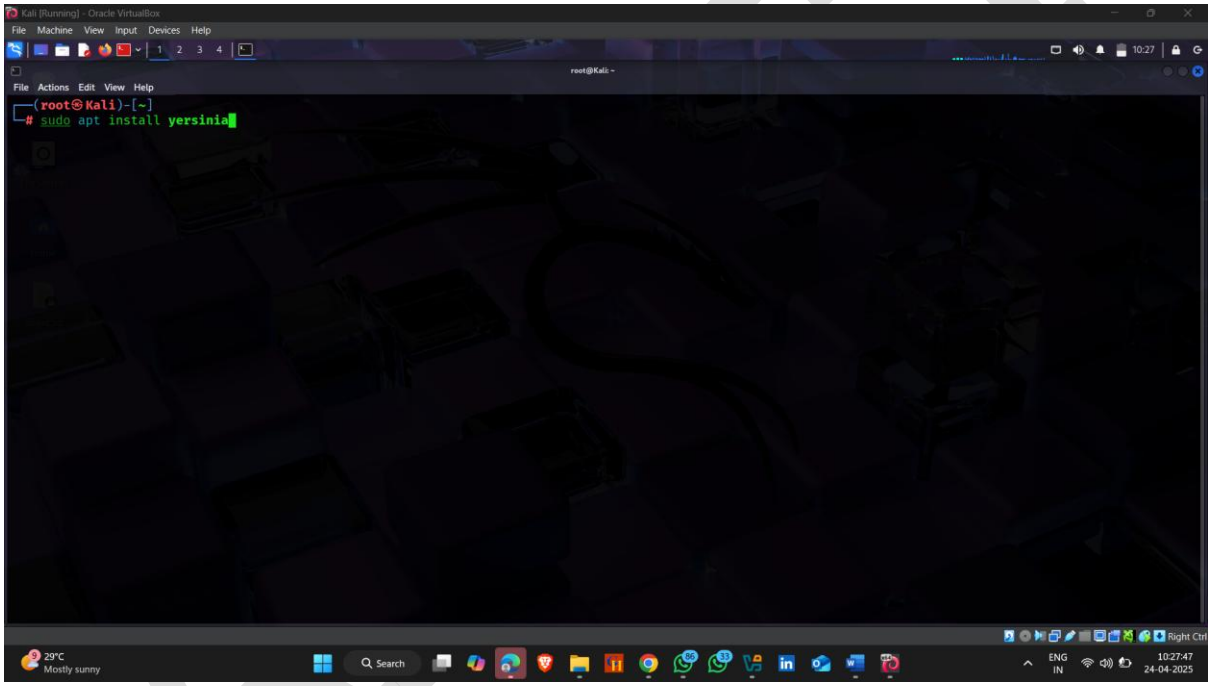
DHCP Starvation Attack Using Yersinia (Linux Tool)

Yersinia – Network Attack Tool

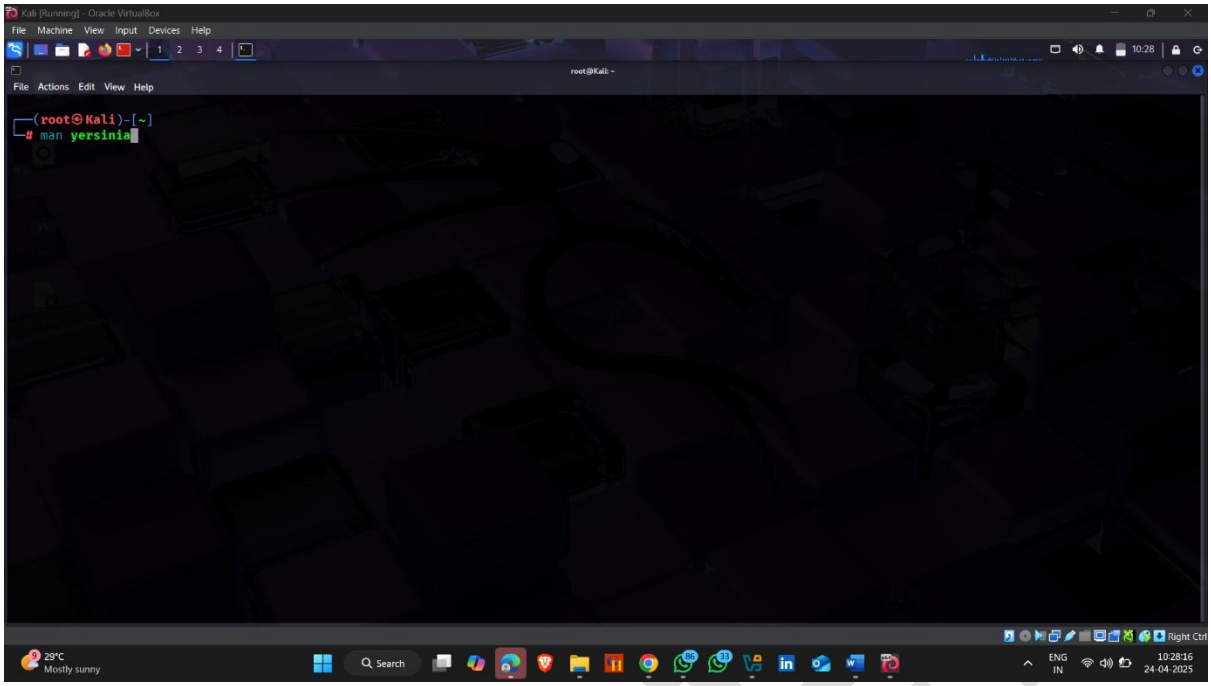
Yersinia is a **network penetration testing tool** used to exploit weaknesses in **Layer 2 (Data Link Layer)** network protocols.

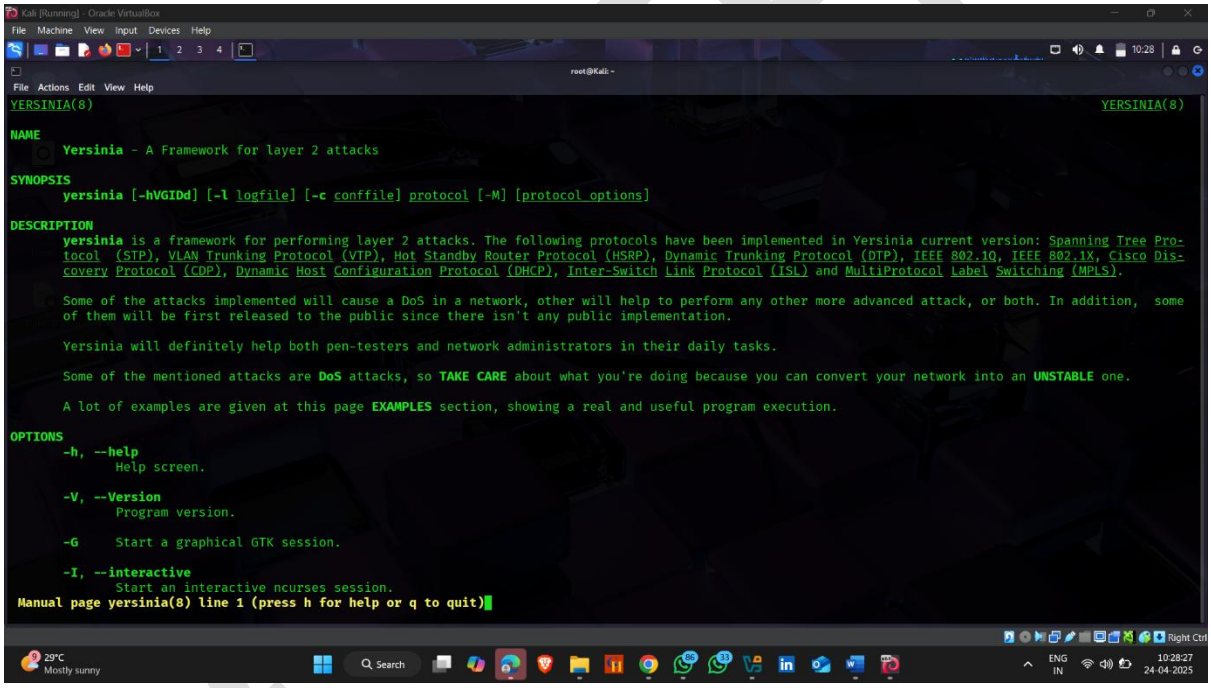
How to use it -:

- Open kali linux / parrot OS terminal
- **Type sudo apt install yersinia**

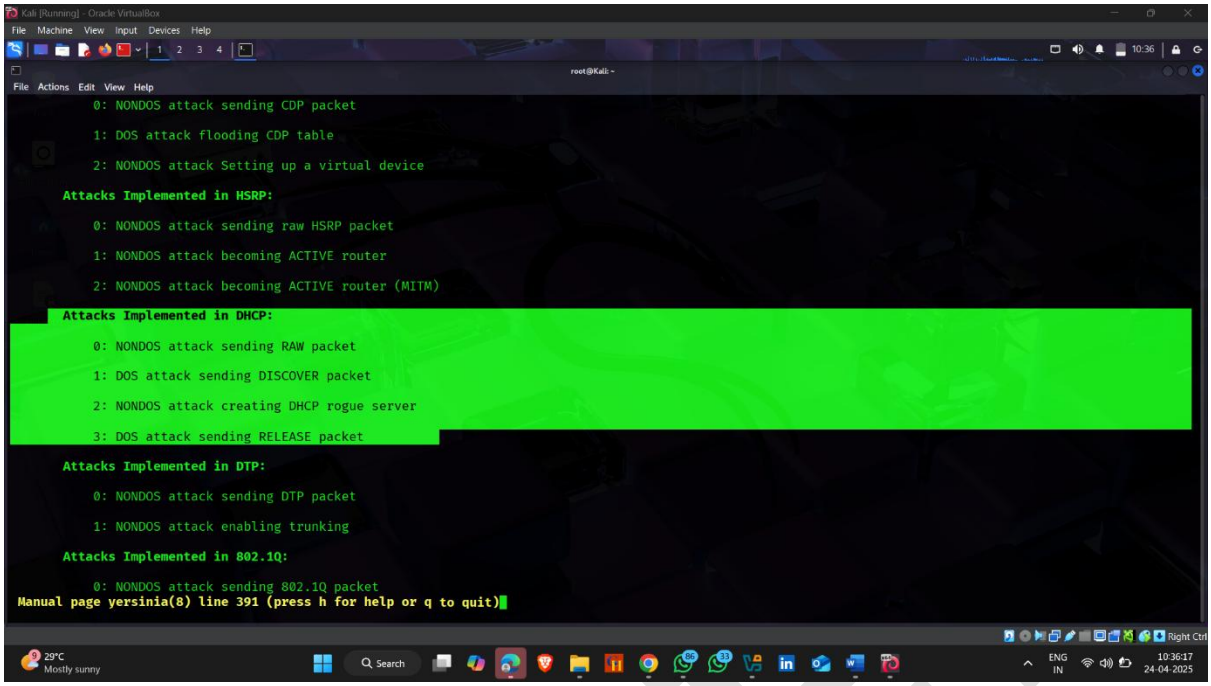


- get detailed information about macof , simply type **man yersinia**

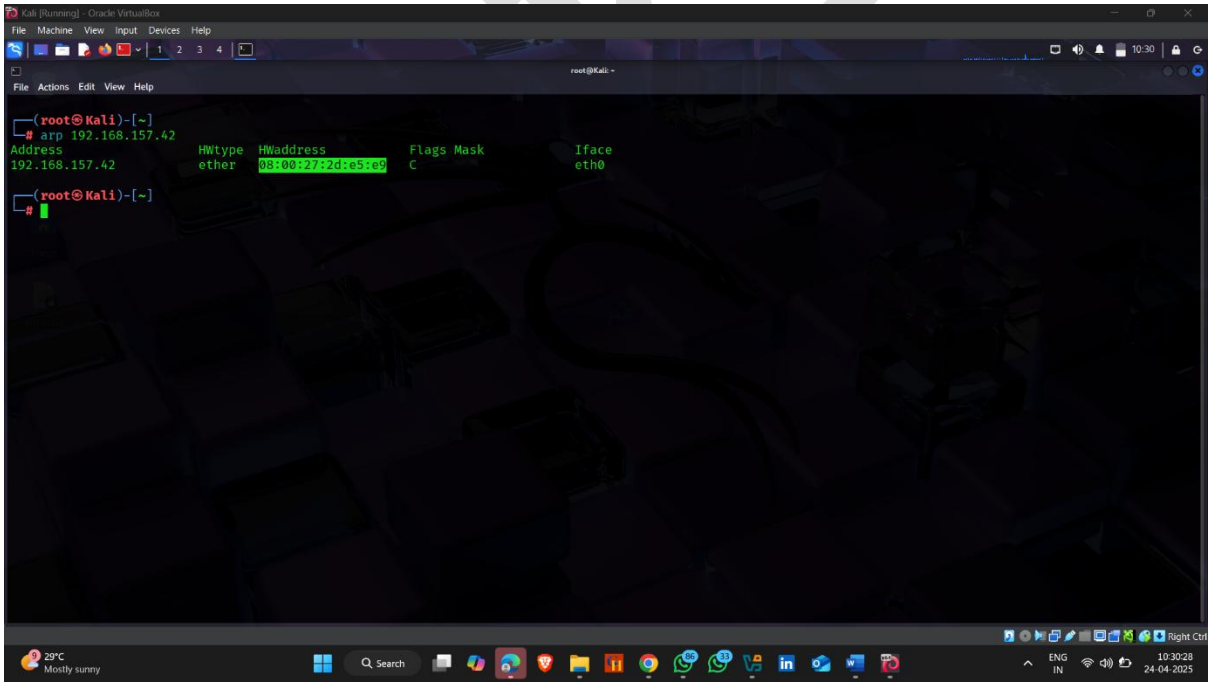




- Now find a DHCP attack commands



- Now find a target physical address/mac address
- Using → arp <target ip >



- Now perform attack

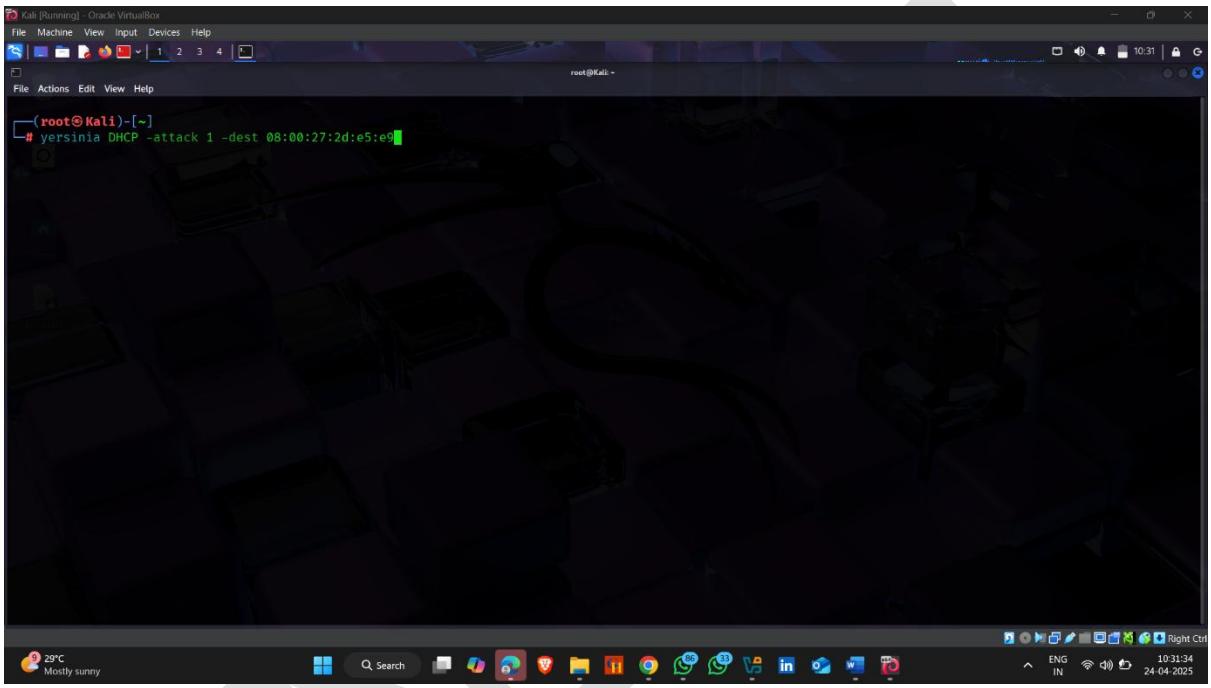
Command – yersinia DHCP -attack 1 -dest <target mac address >

DHCP – Perform DHCP attack

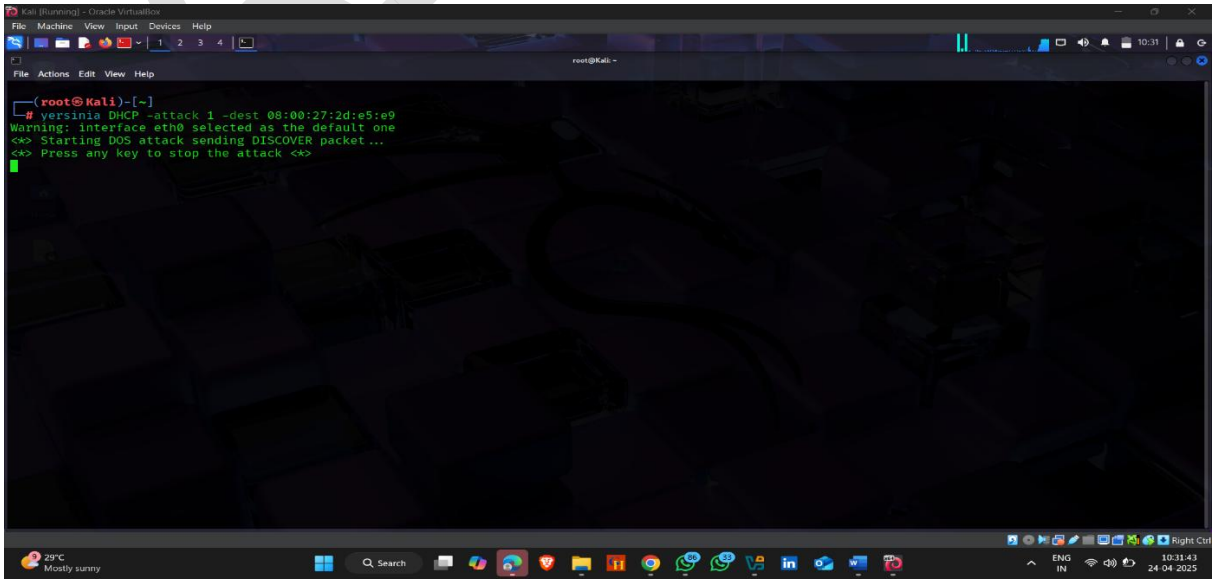
-attack – perform attack

1 – Send Raw data Packets

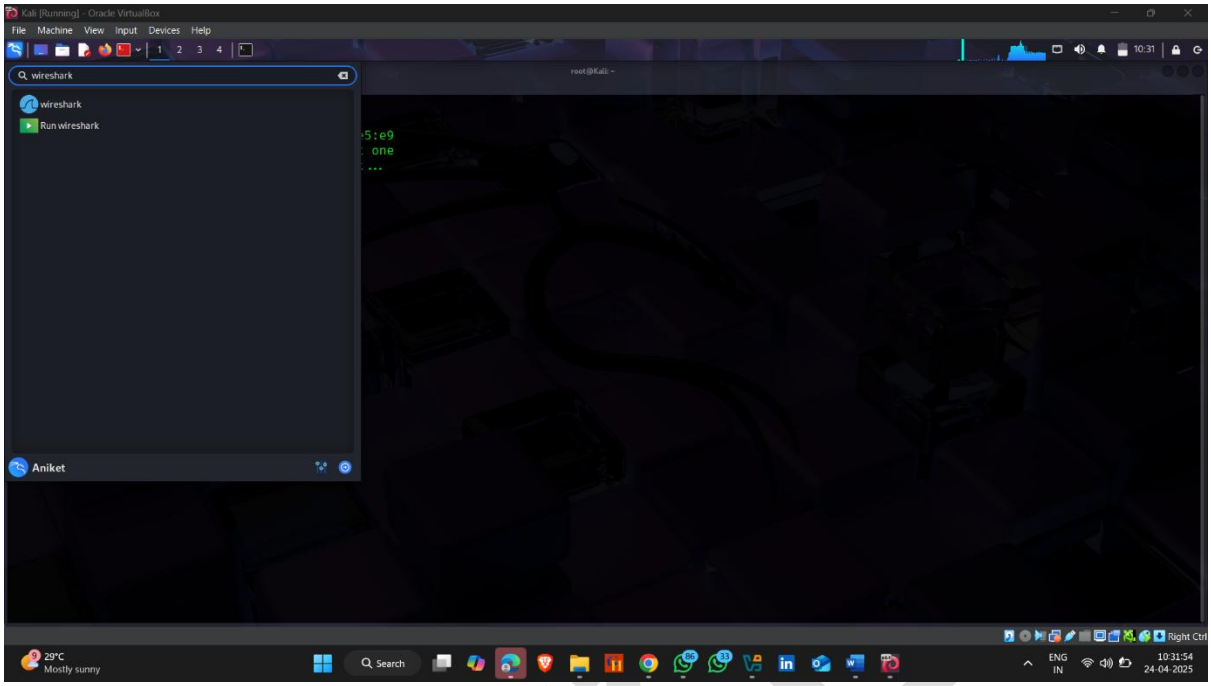
-dest – Destination



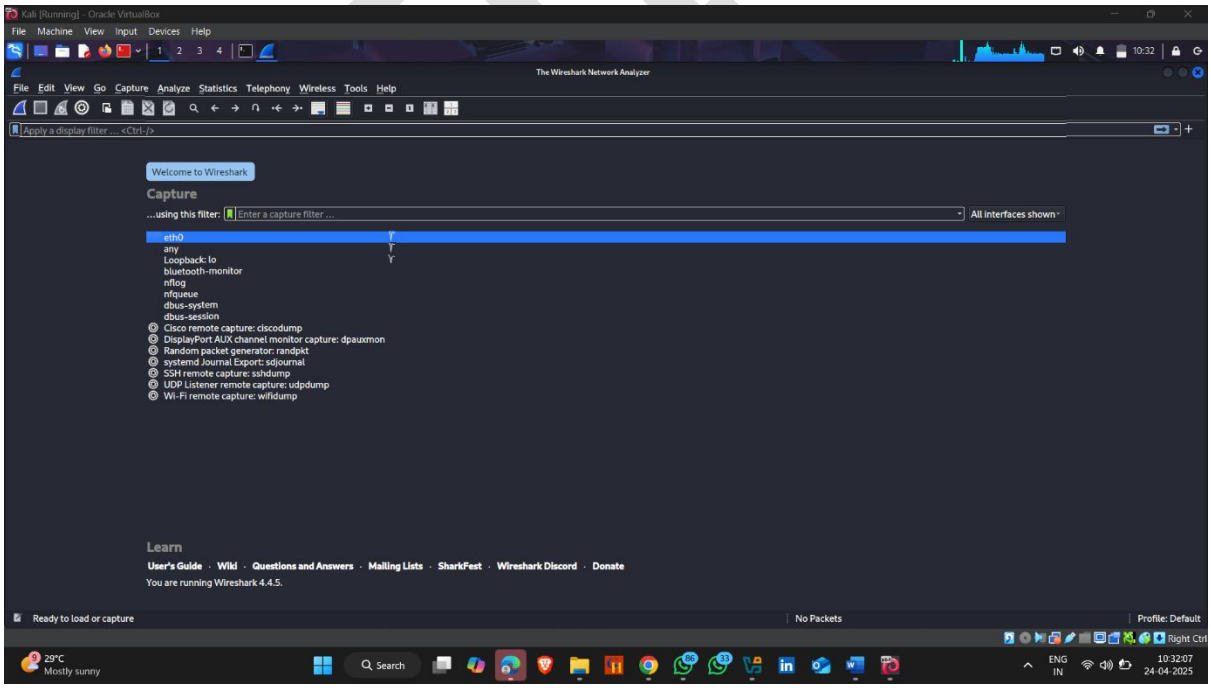
- Hare Attack Start



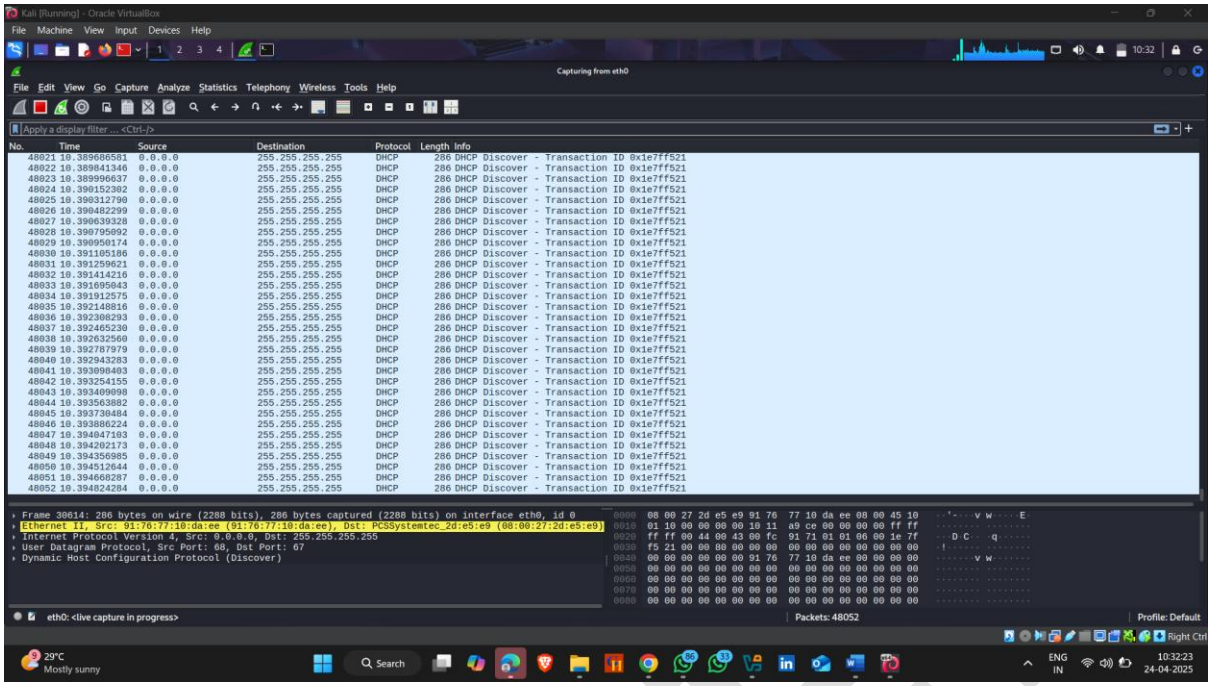
- Open Wireshark to see attack



- Click on eth0



- Here , DHCP Packets are send to the target


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
48021 10.389686581 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48022 10.389841346 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48023 10.389996637 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48024 10.390152302 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48025 10.390312790 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48026 10.390482299 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48027 10.390639328 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48028 10.390795092 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48029 10.390950174 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48030 10.391105186 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48031 10.391259621 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48032 10.391414216 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48033 10.391695043 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48034 10.391912575 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48035 10.392148816 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48036 10.392308293 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48037 10.392465230 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48038 10.392632560 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48039 10.392787979 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48040 10.392943283 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48041 10.393098403 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48042 10.393254155 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48043 10.393409098 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48044 10.393563882 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48045 10.393730484 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48046 10.393886224 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48047 10.394047103 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48048 10.394202173 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48049 10.394356985 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48050 10.394512644 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48051 10.394668287 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
48052 10.394824284 0.0.0.0 255.255.255.255 DHCP 286 DHCP Discover - Transaction ID 0x1e7ff521
Frame 30614: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0
Ethernet II, Src: 91:76:77:10:da:ee (91:76:77:10:da:ee), Dst: PCSSystemtec_2d:e5:e9 (08:00:27:2d:e5:e9)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
0000 08 00 27 2d e5 e9 91 76 77 10 da ee 08 00 45 10
0010 01 10 00 00 00 00 10 11 a9 ce 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 00 fc 91 71 01 01 06 00 1e 7f
0030 f5 21 00 00 80 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 91 76 77 10 da ee 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
eth0: <live capture in progress>
Packets: 48052
Profile: Default
Right Ctrl
29°C
Mostly sunny
Search
ENG
IN
10:32:23
24-04-2025

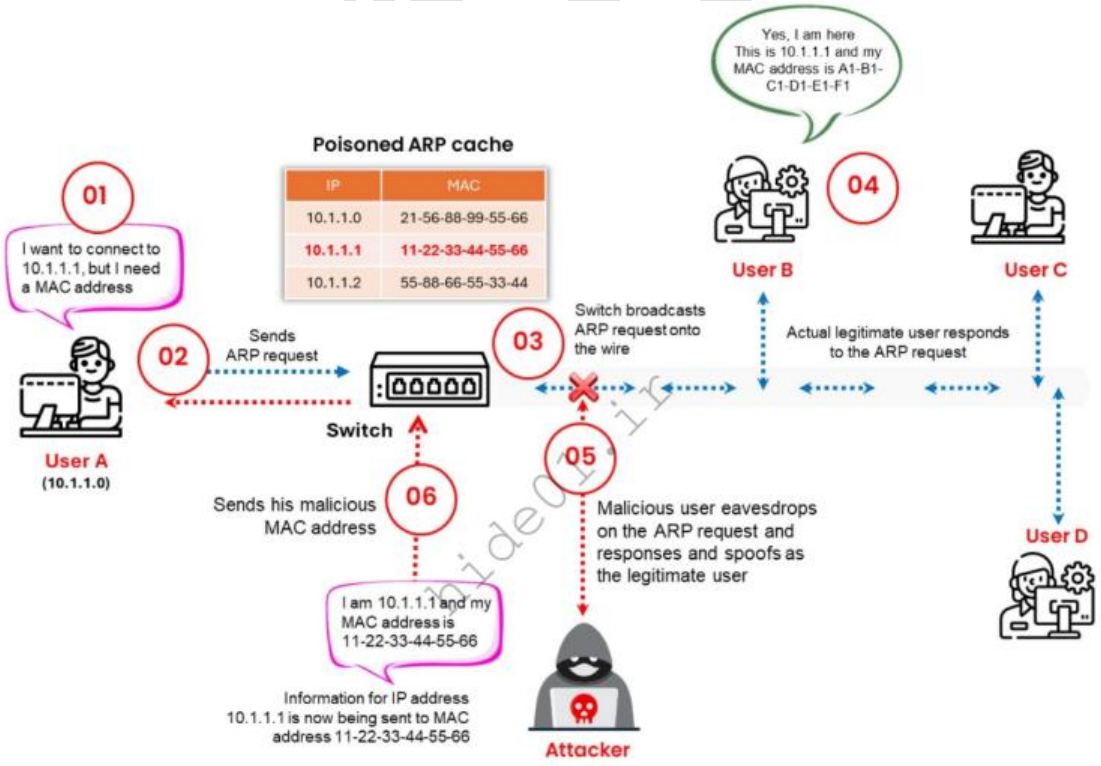
ARP POISONING

ARP spoofing / Poisoning -:

ARP Spoofing (also called ARP Poisoning) is a type of cyber attack where an attacker sends fake ARP (Address Resolution Protocol) messages on a local network to link their MAC address with the IP address of another device, like a router or victim's computer.

ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. ARP packets can be forged to send data to the attacker's machine. ARP spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. When a machine sends an ARP request, it assumes that the ARP reply will come from the right machine.



ARP Poisoning Attack

Perform Arp Poisoning Using Cain and able

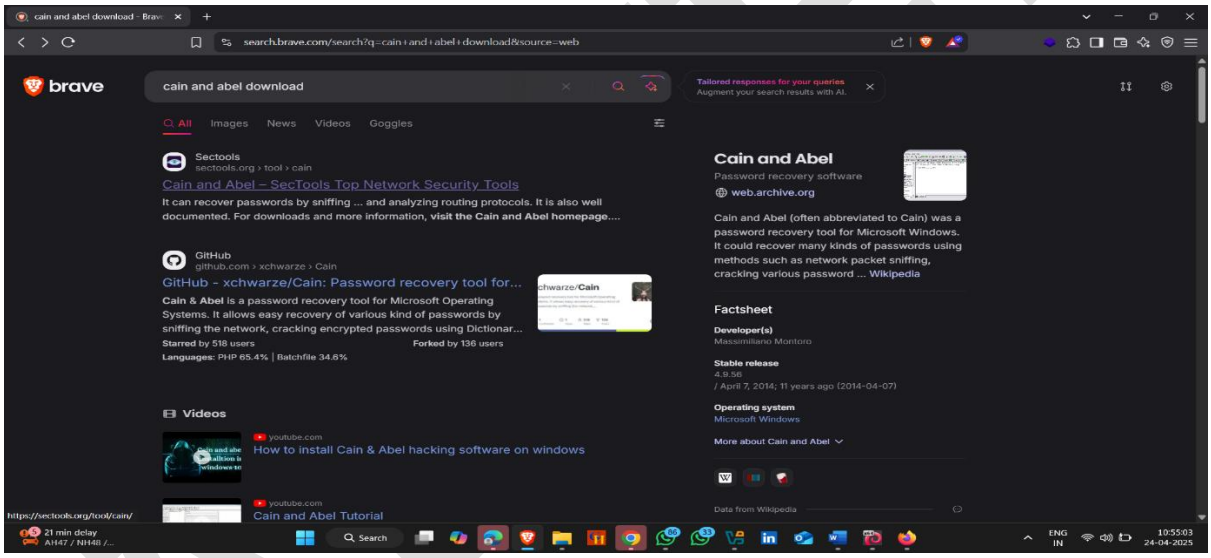
Cain & Abel is a **password recovery and network analysis tool** used by ethical hackers and penetration testers for various network security tasks.

How to install it

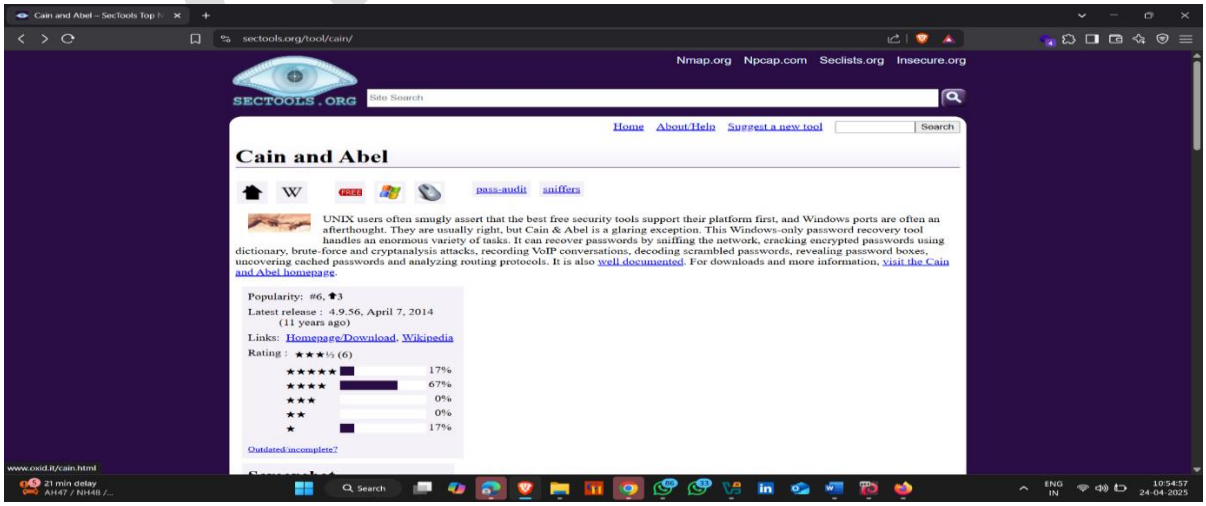
- Open a Browser and search Cain And able Download

Download Link - https://sectools.org/tool/cain/

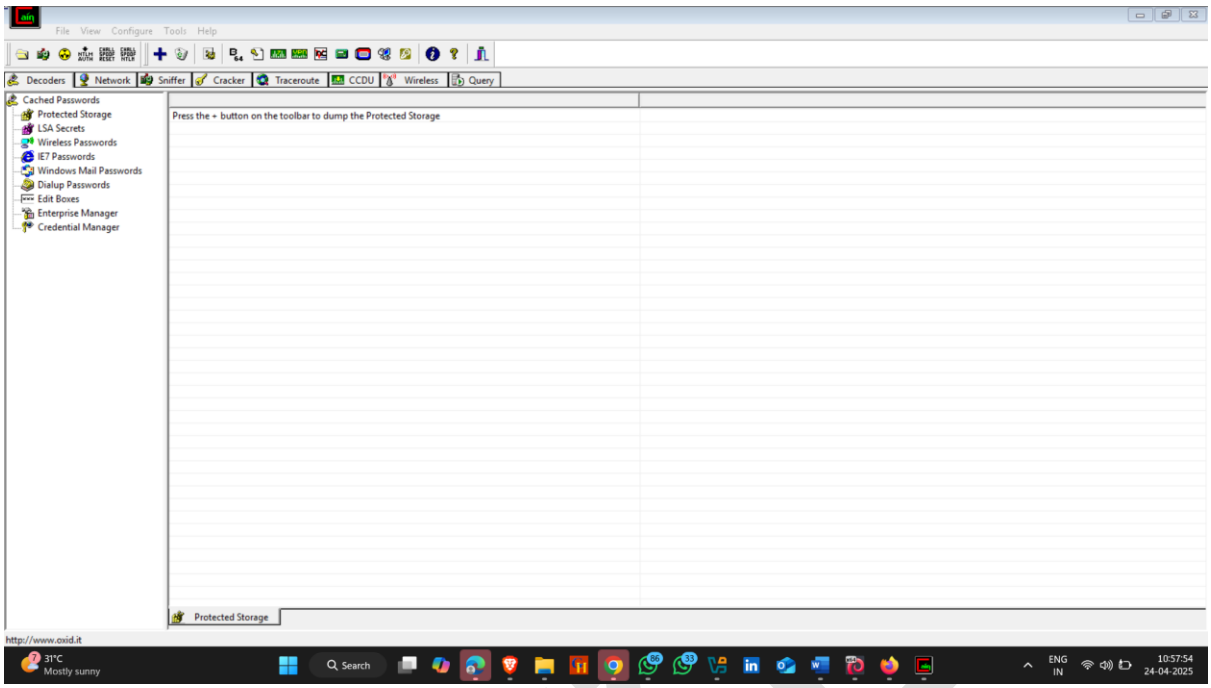
- Click on First website



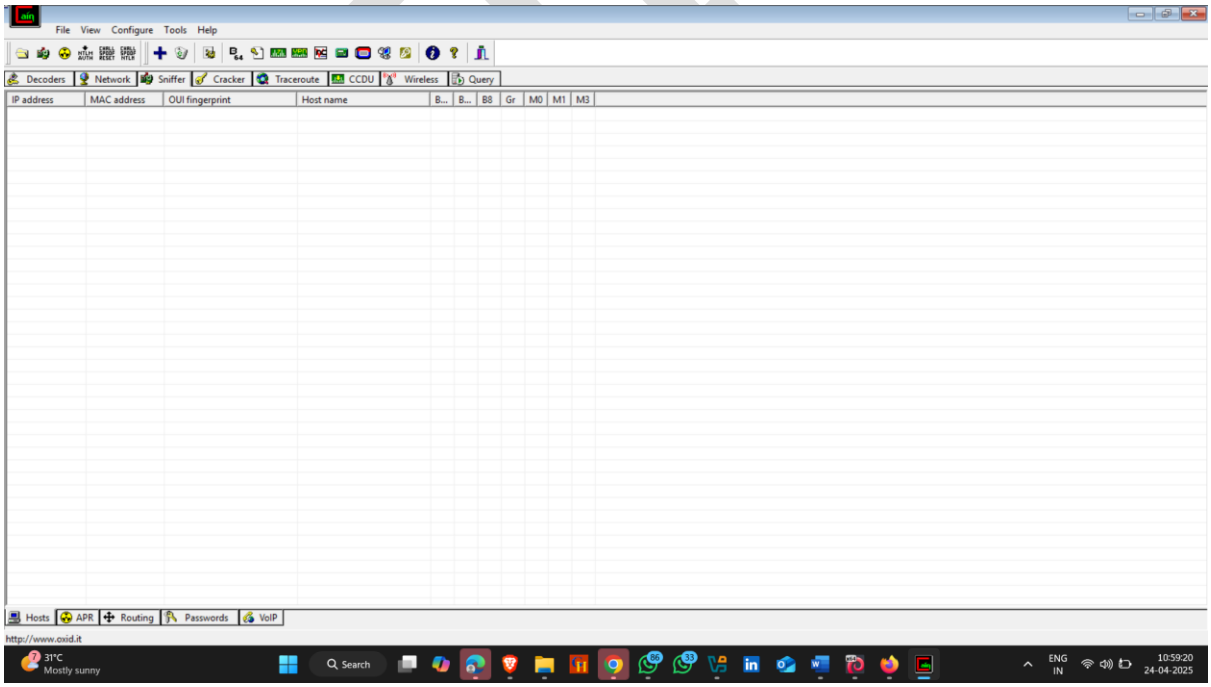
- Click on Download



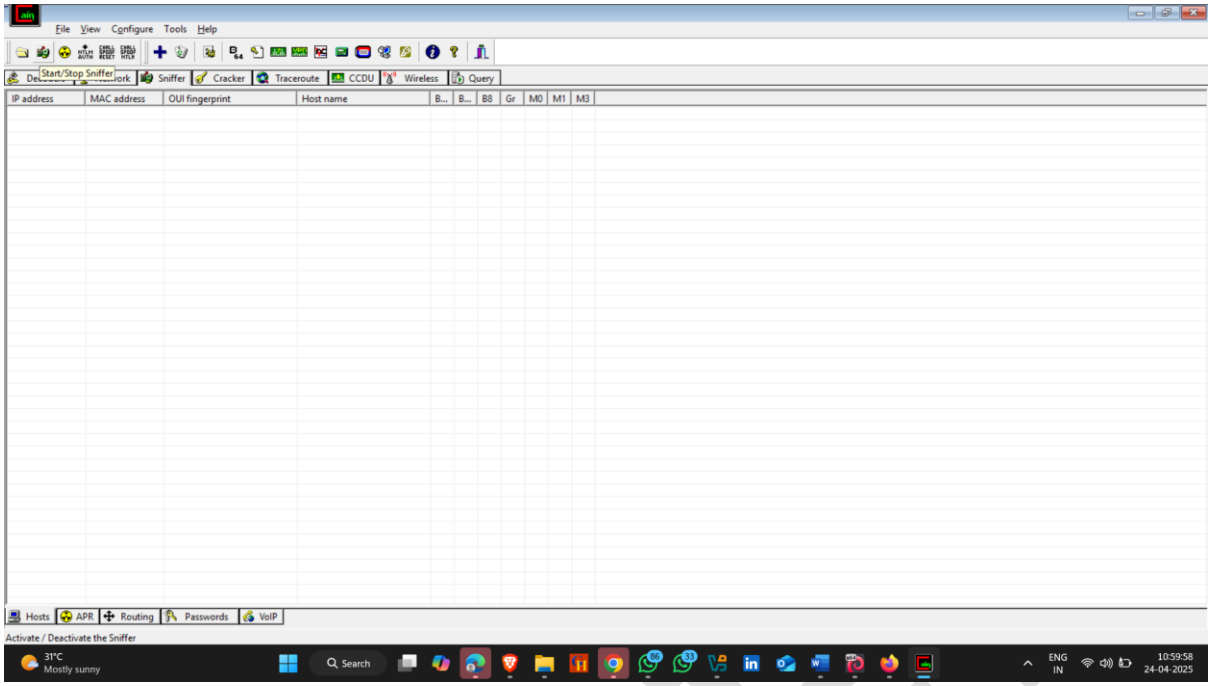
- After installation , open cain



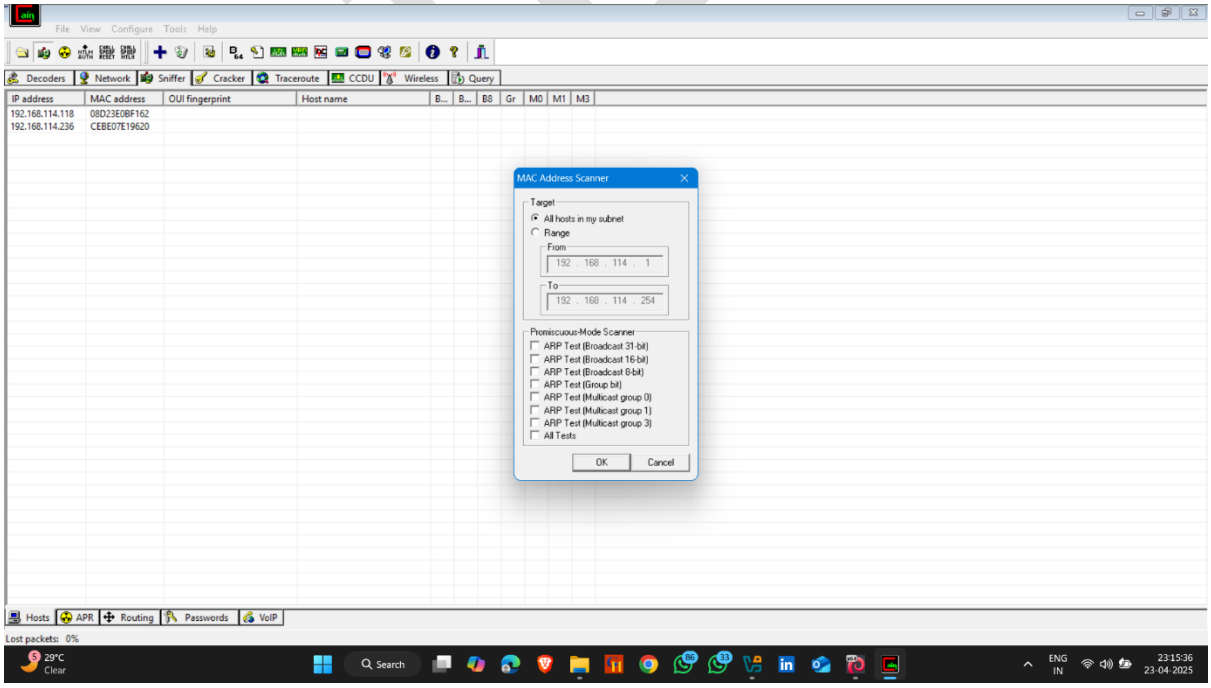
- Now click on sniffer button and then click on **Host**



- Now Start sniffer , click on sniffer ..top left side second button

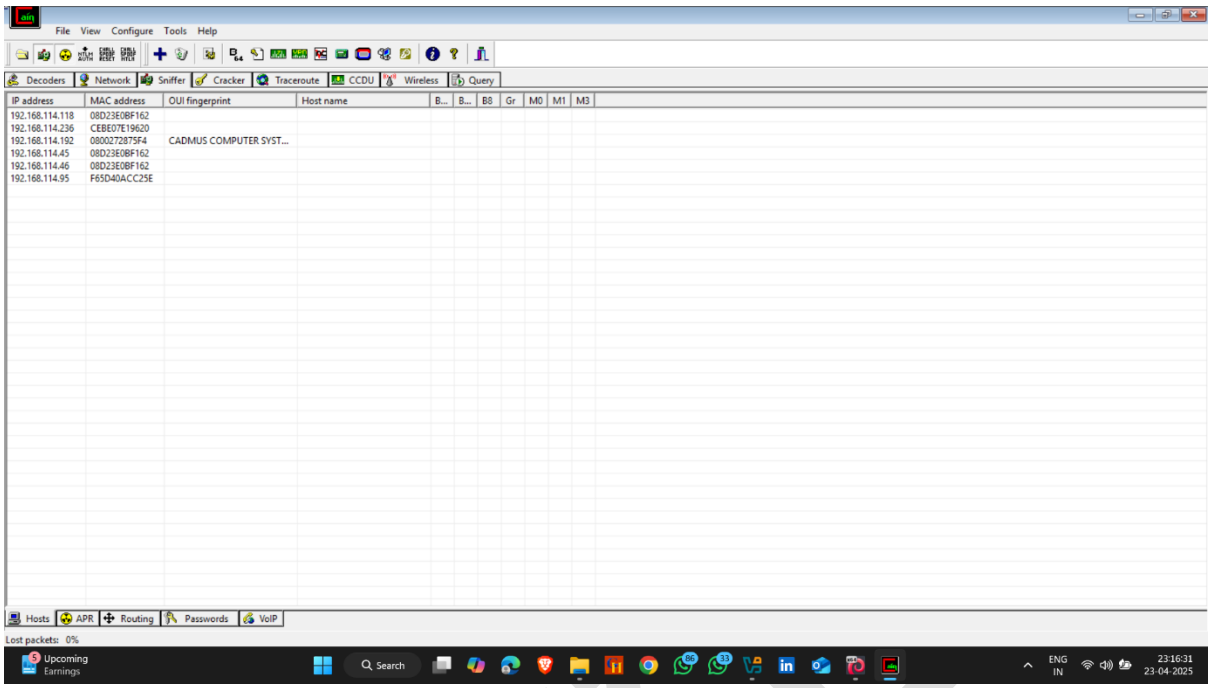


- **And then click on** + , and click on ok
- It start scanning the ip address of network

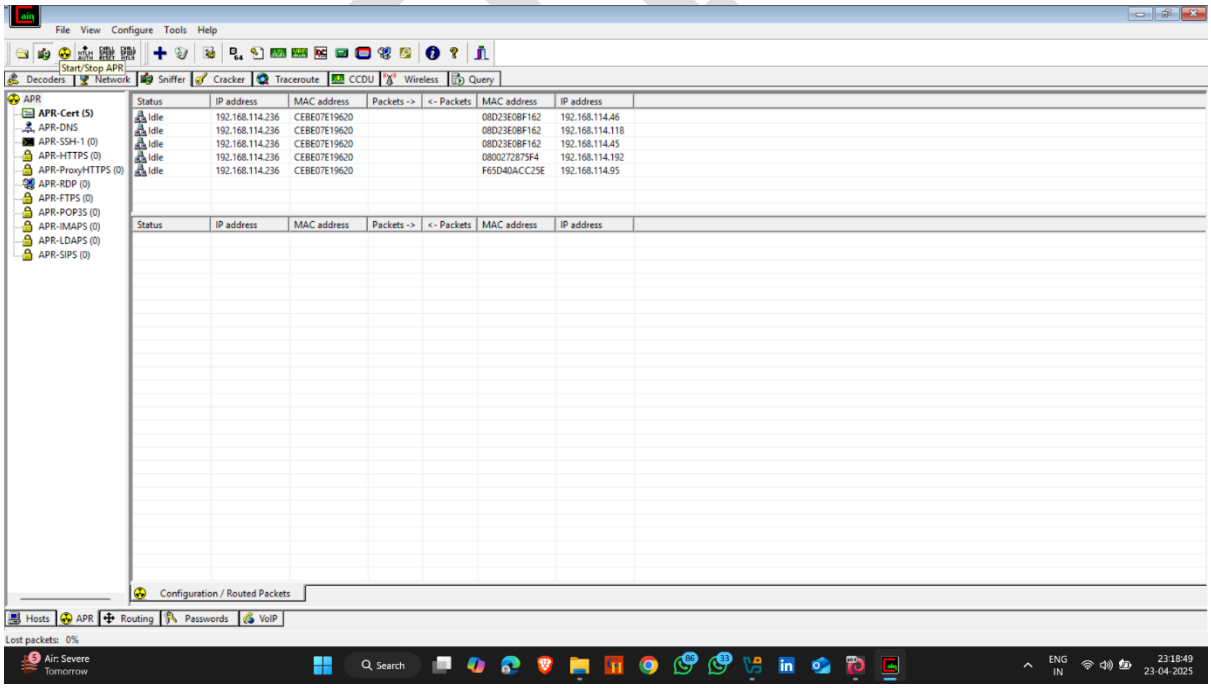


- Here it scan some ip address

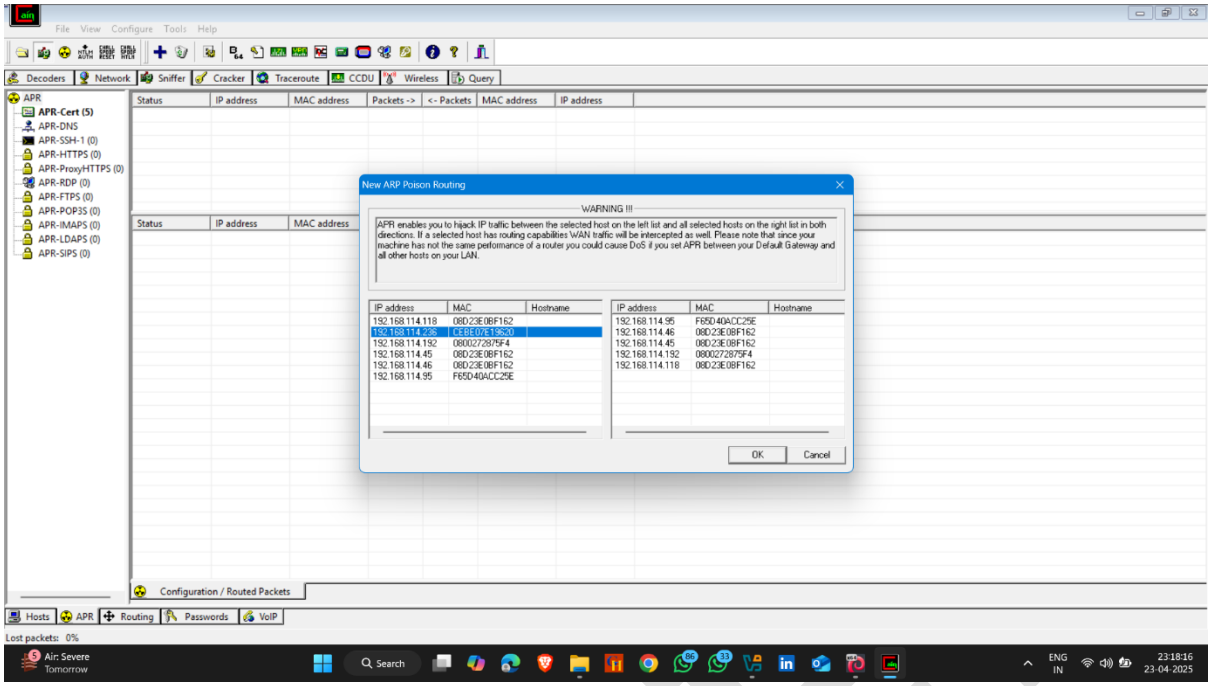
- Now click on ARP ..**bottom side**



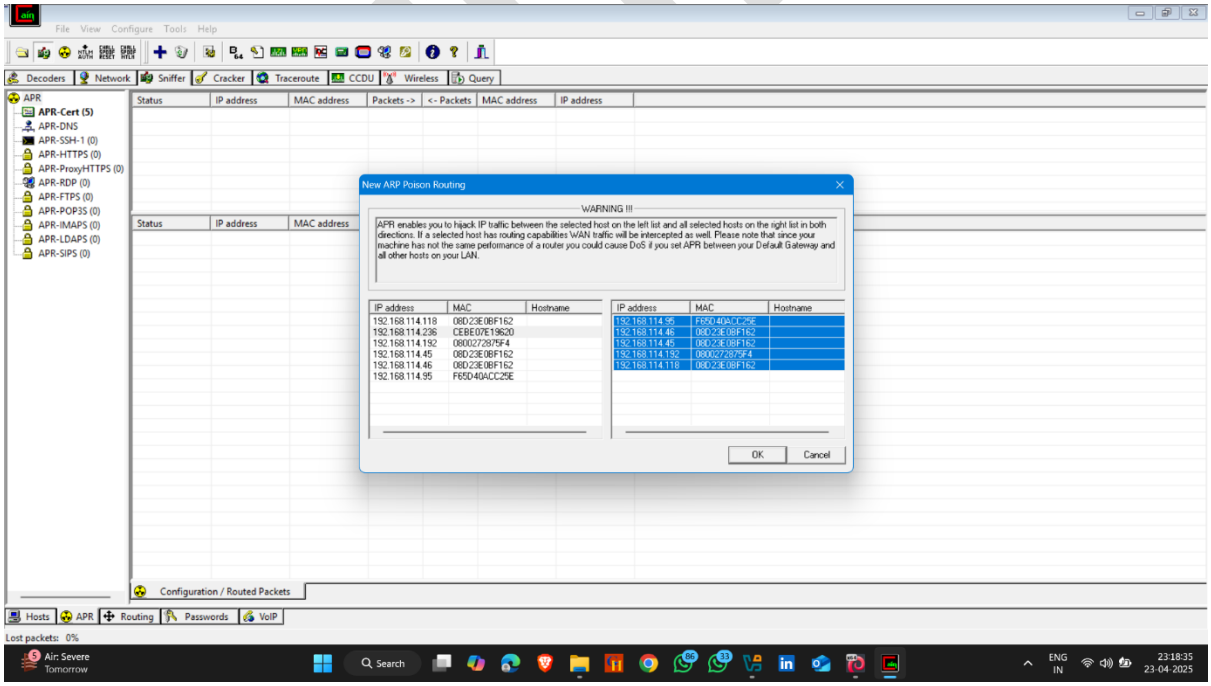
- Click on Start / Stop ARP



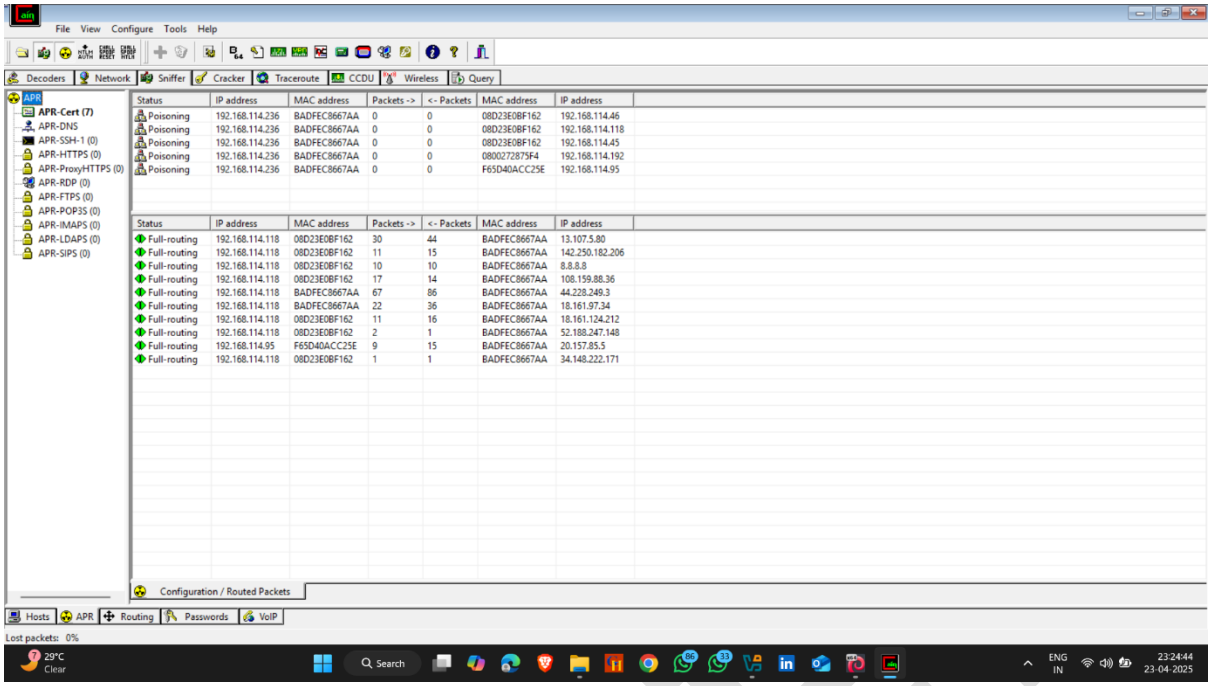
- Select Default gateway and then select ip for attack



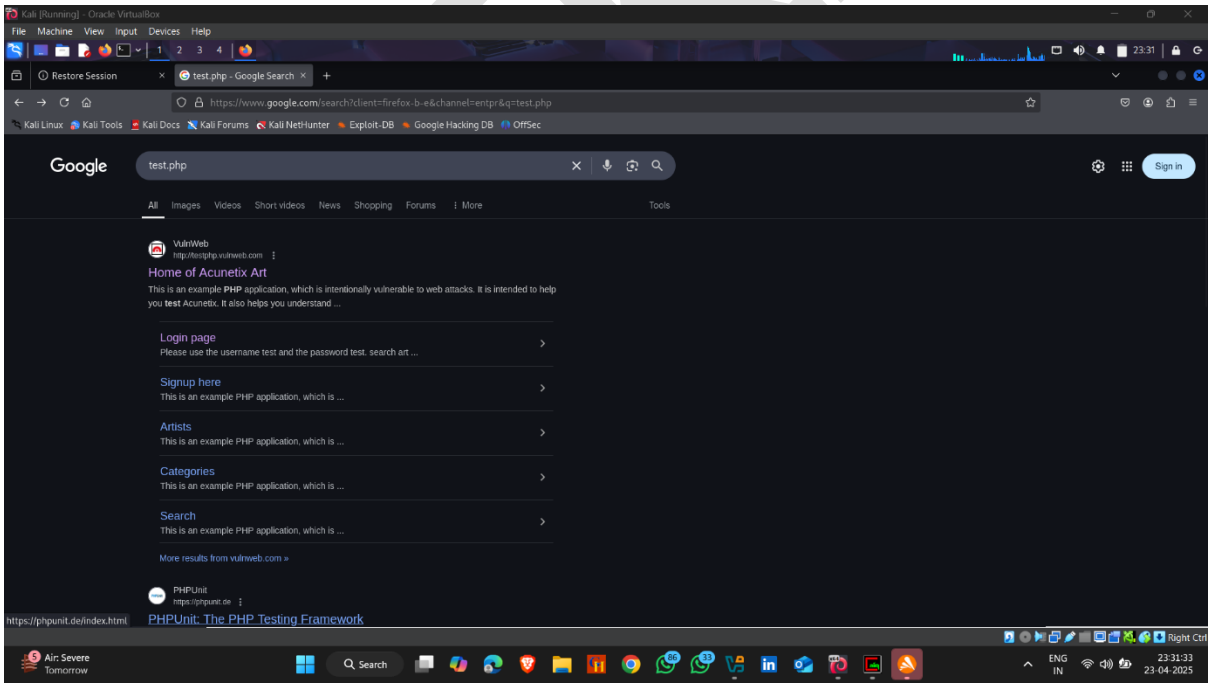
- Click on ok



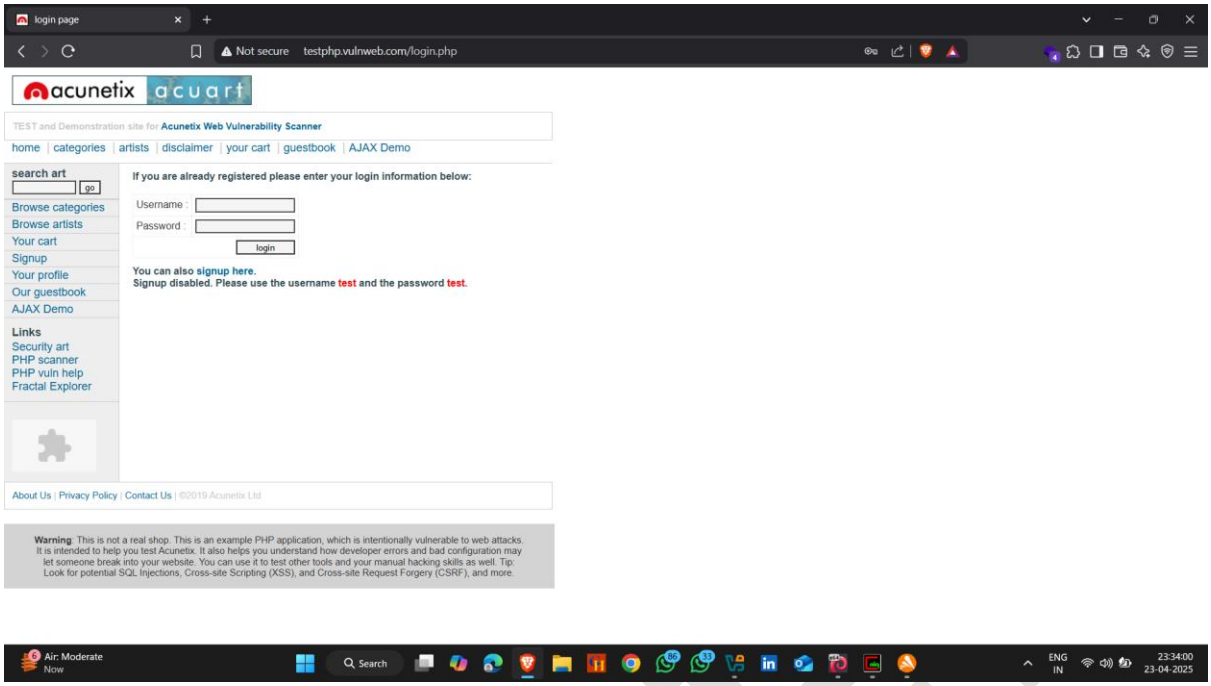
- Now Poisoning Start

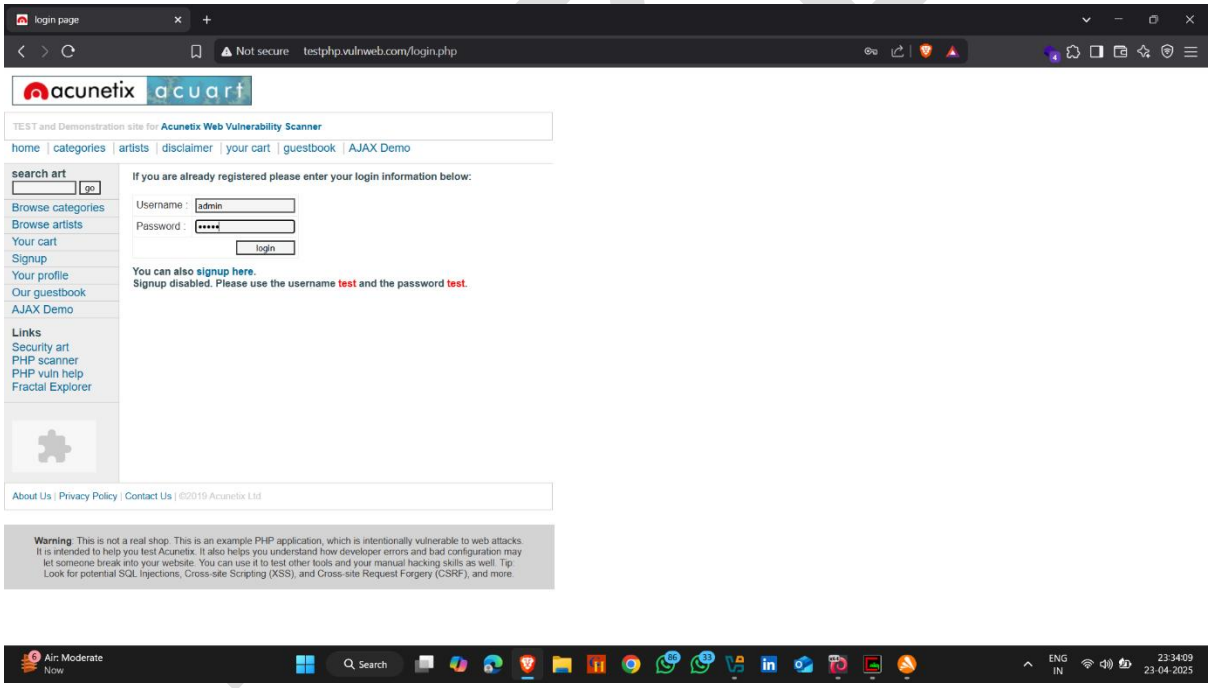


- Open the website on target Browser

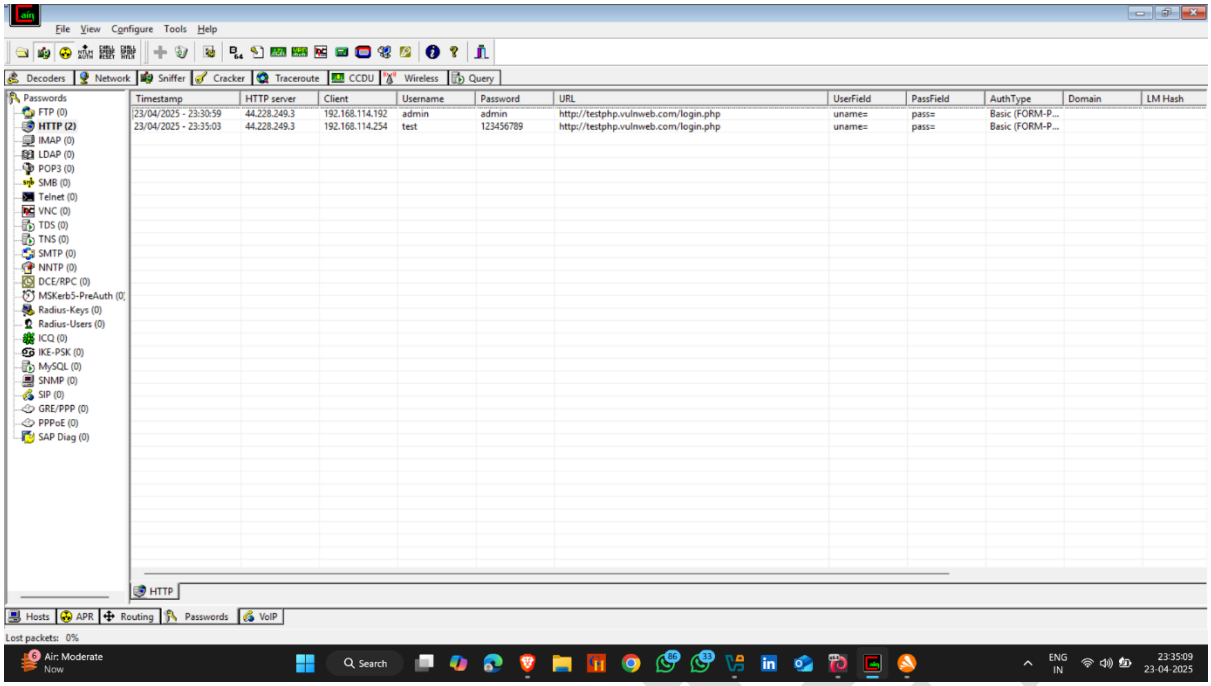


- Provide username and password





- Here , it capture the username and password



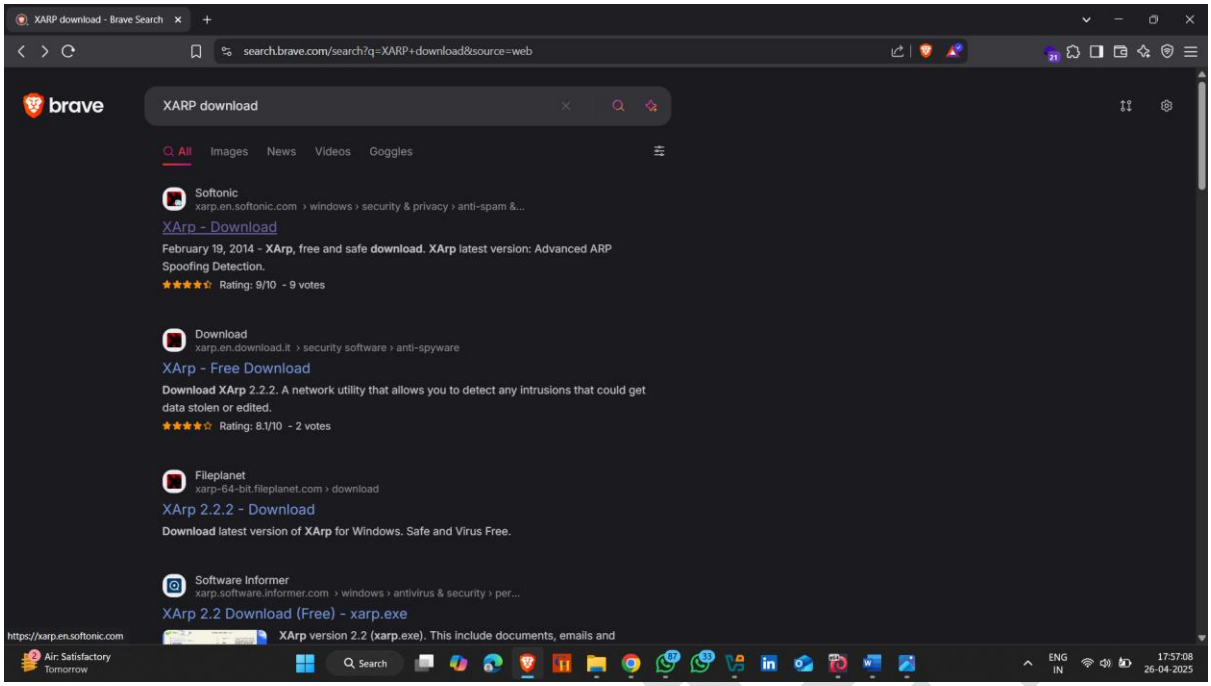
Detect Arp Poisoning Using XARP Applicartion

XARP (eXtended Address Resolution Protocol) is an advanced **security application** specifically designed to **detect and alert users to ARP spoofing attacks** within a local network. It continuously **monitors ARP traffic** and analyzes ARP packets to identify **anomalies and suspicious behavior** that indicate an attack.

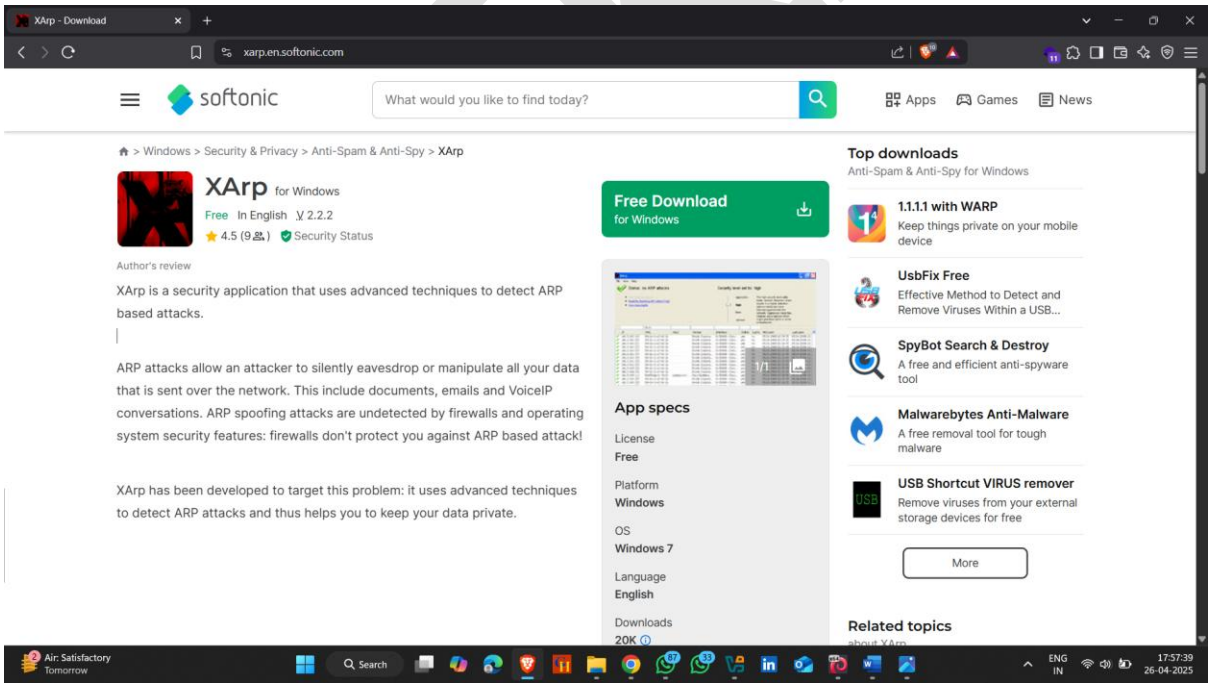
How to Download it -:

- Open Browser and Search XARP download
- Click on first Softonic Website

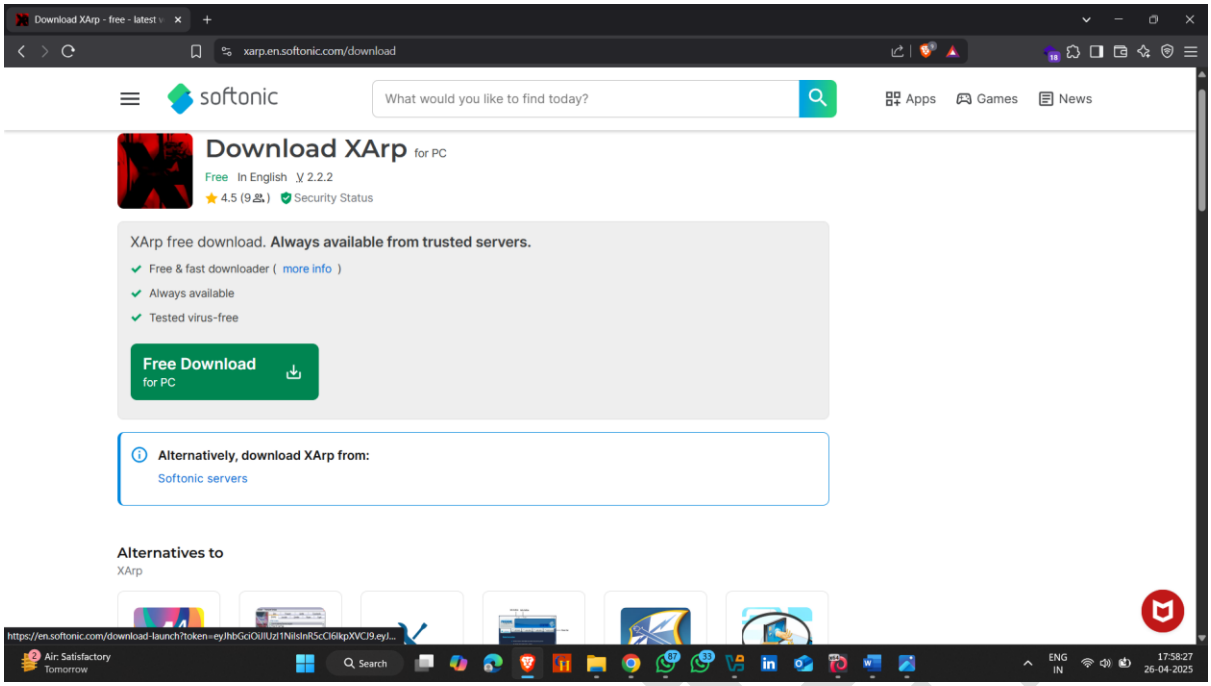
Download Link - :https://xarp.en.softonic.com/download



- Click on Free Downlaod

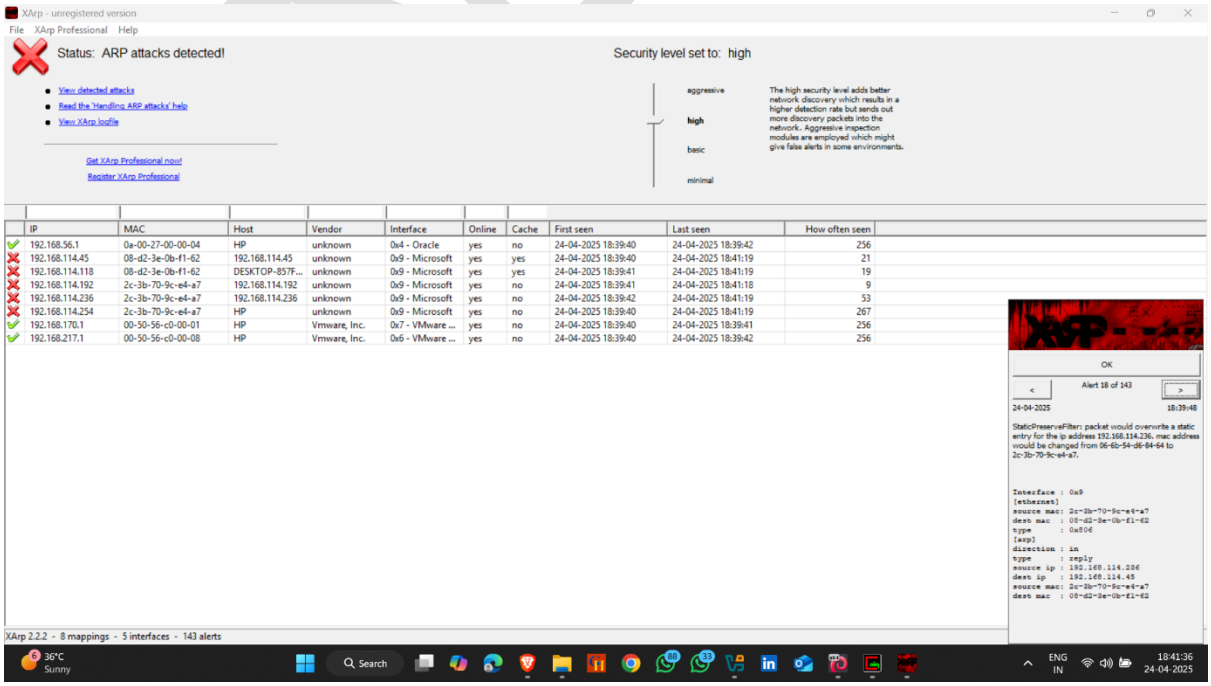


- Again click on Free Download

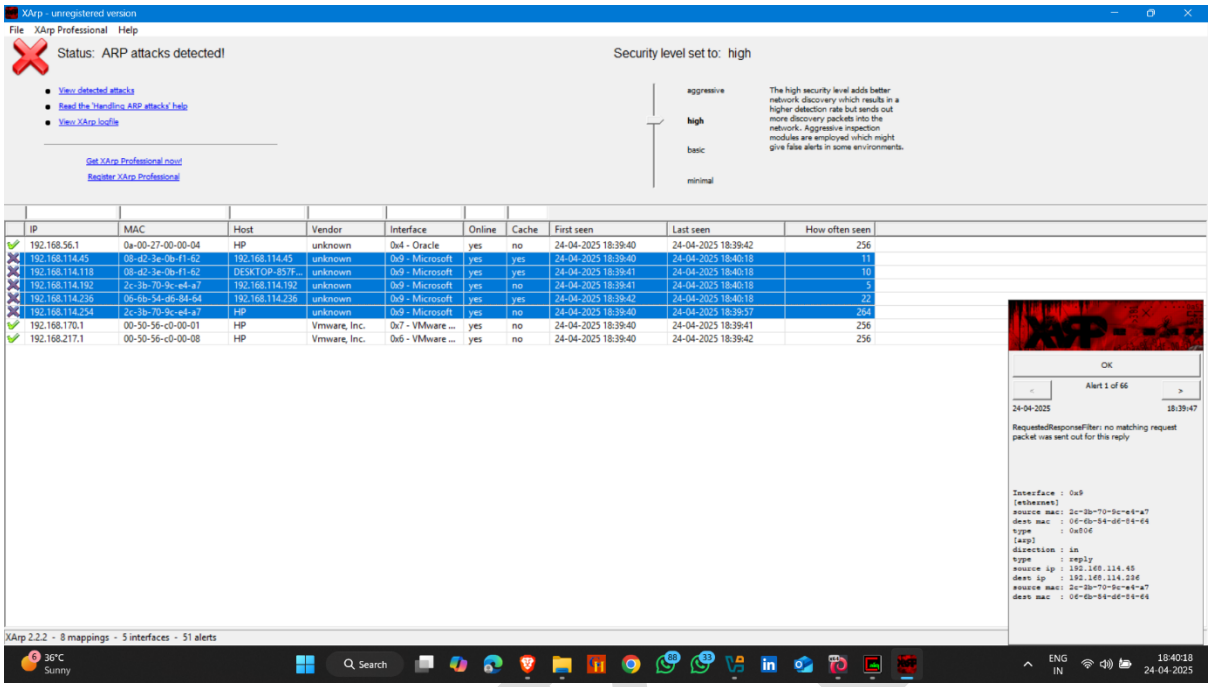


How to use it -:

- **After installation of Xarp , open it**
- **It scans the Ip address of the network**



- **It display ARP attacks ip using ❌ marks and display a alerts (Right side of the screen)**



MAC SPOOFING

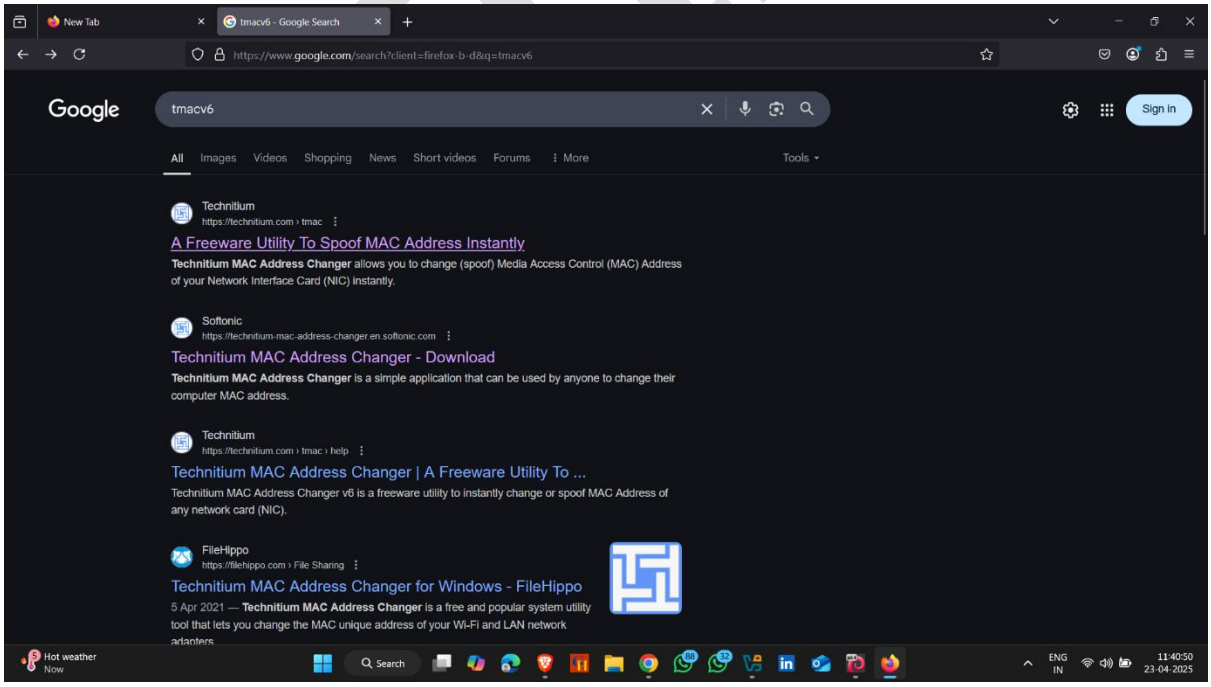
MAC Spoofing is the process of **changing the Media Access Control (MAC) address** of a device's network interface to another **fake (spoofed) MAC address**.

Perform MAC Spoofing using TMACv6

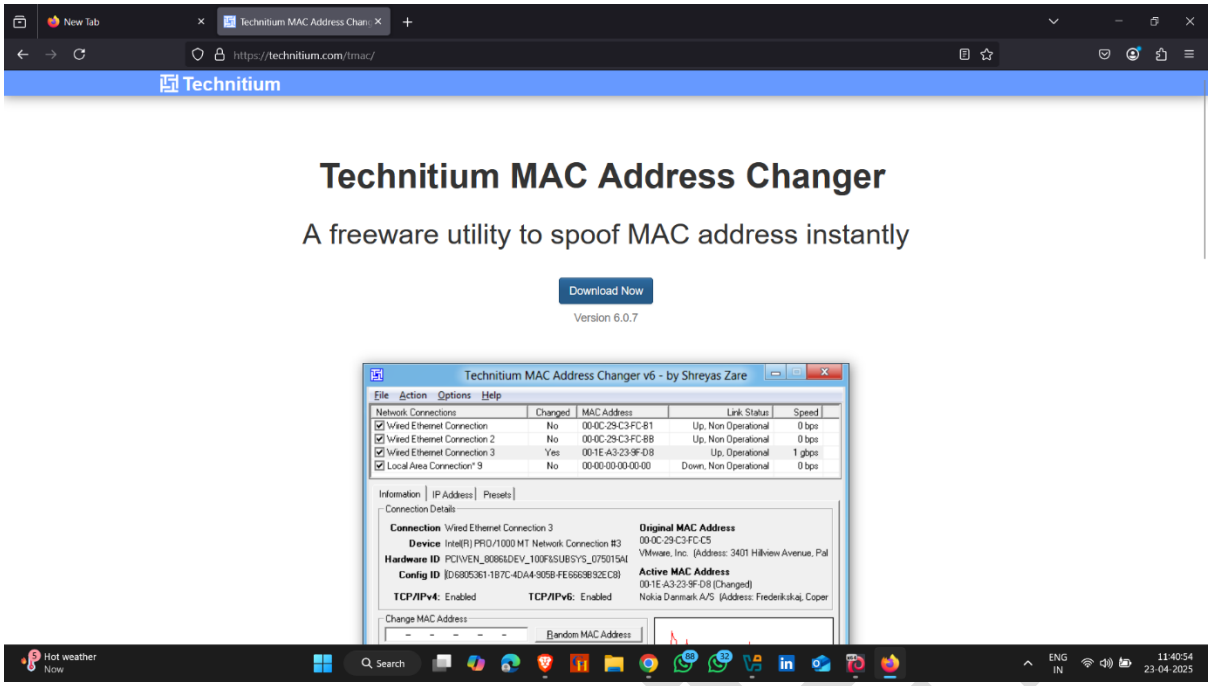
TMACv6 stands for Technitium MAC Address Changer Version 6, a free and popular tool for changing (spoofing) the MAC address of your network interface card (NIC) on Windows systems.

How to install it - :

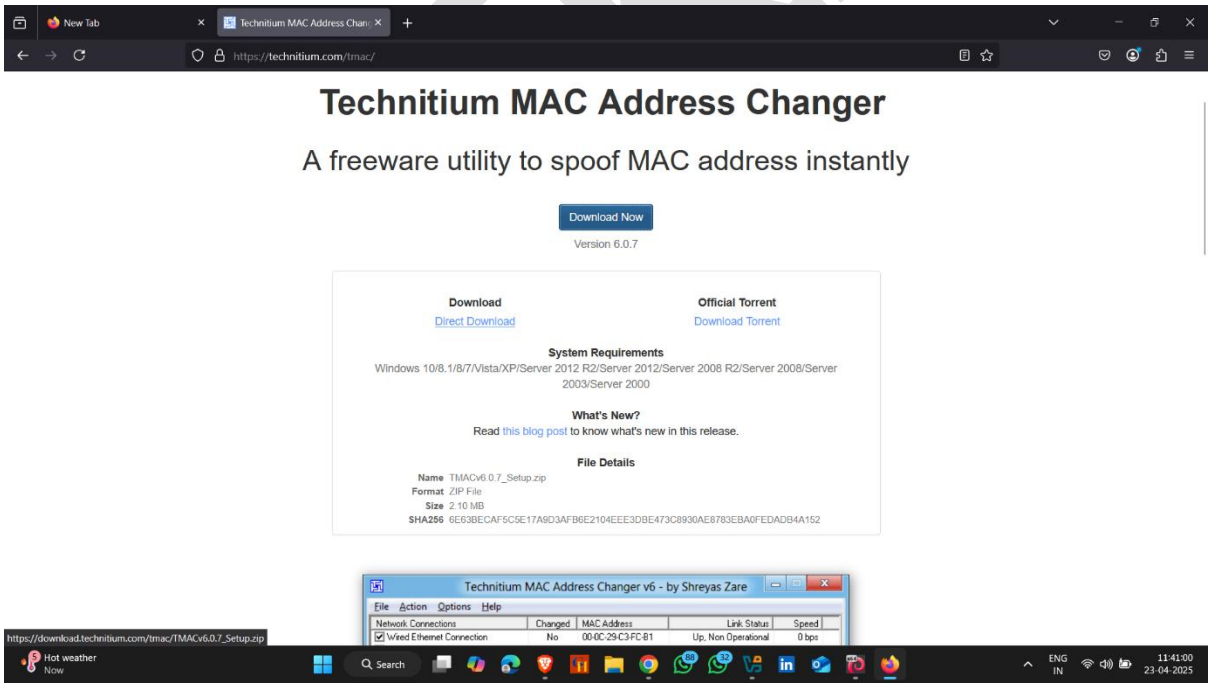
- Open Browser and search Tmacv6 Download
- Click on first website



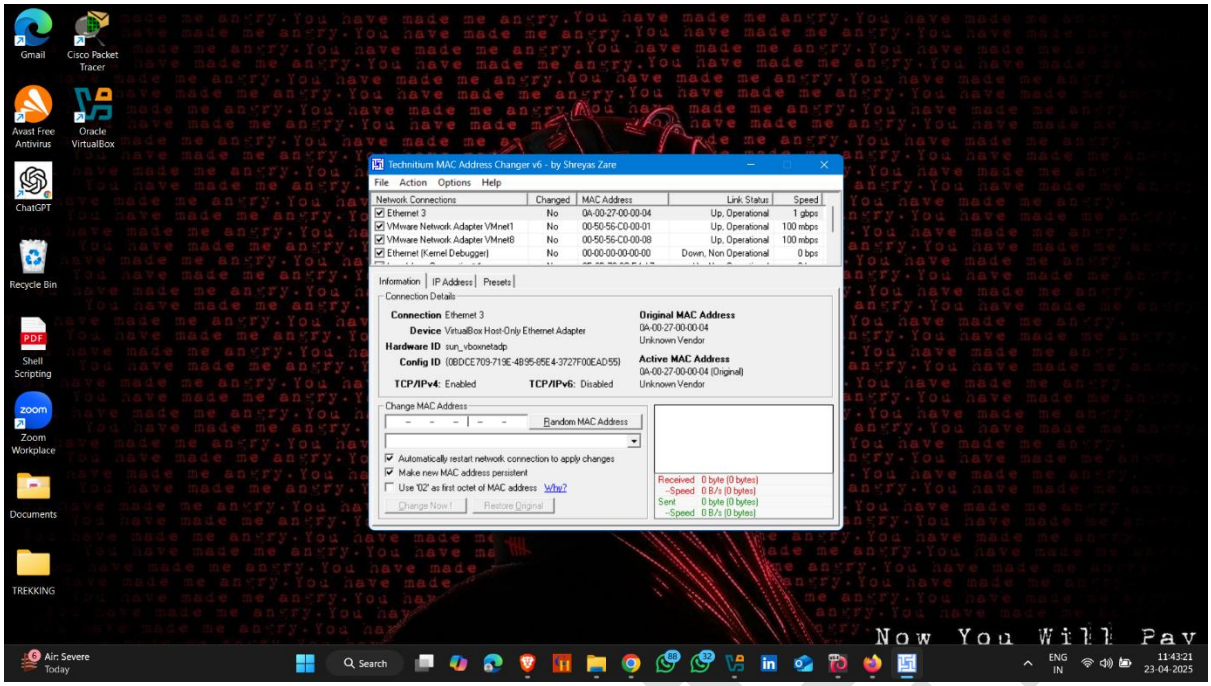
- Click on Download Now



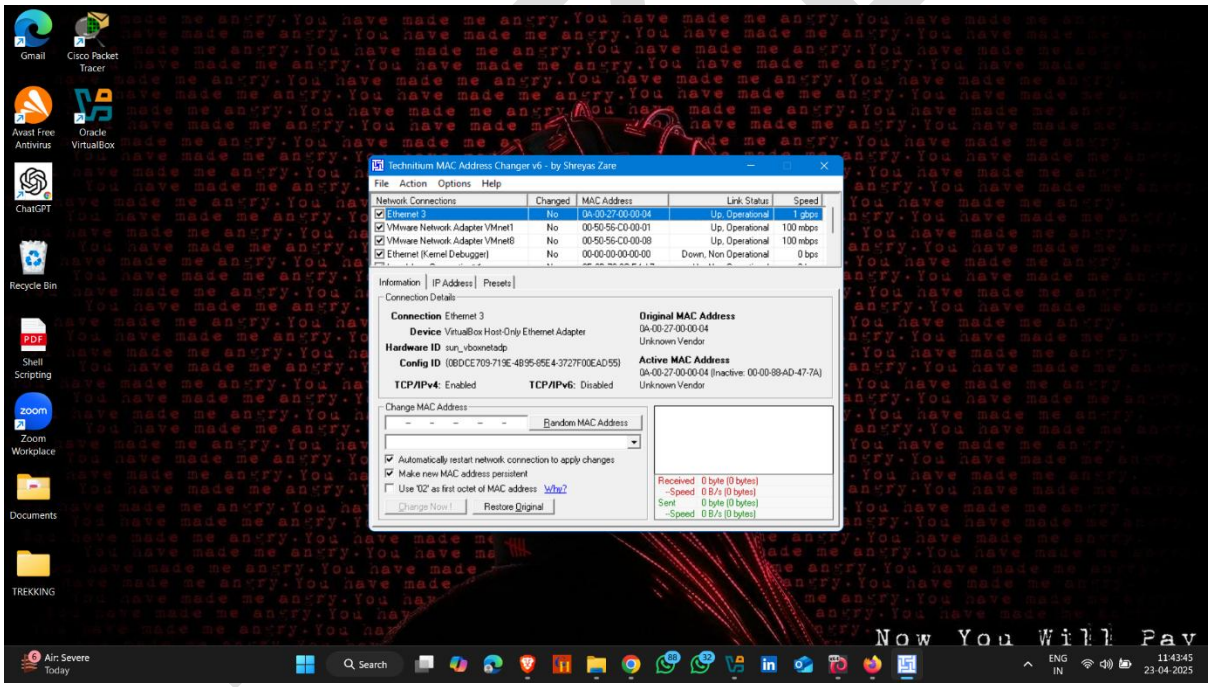
- Click on Direct Download



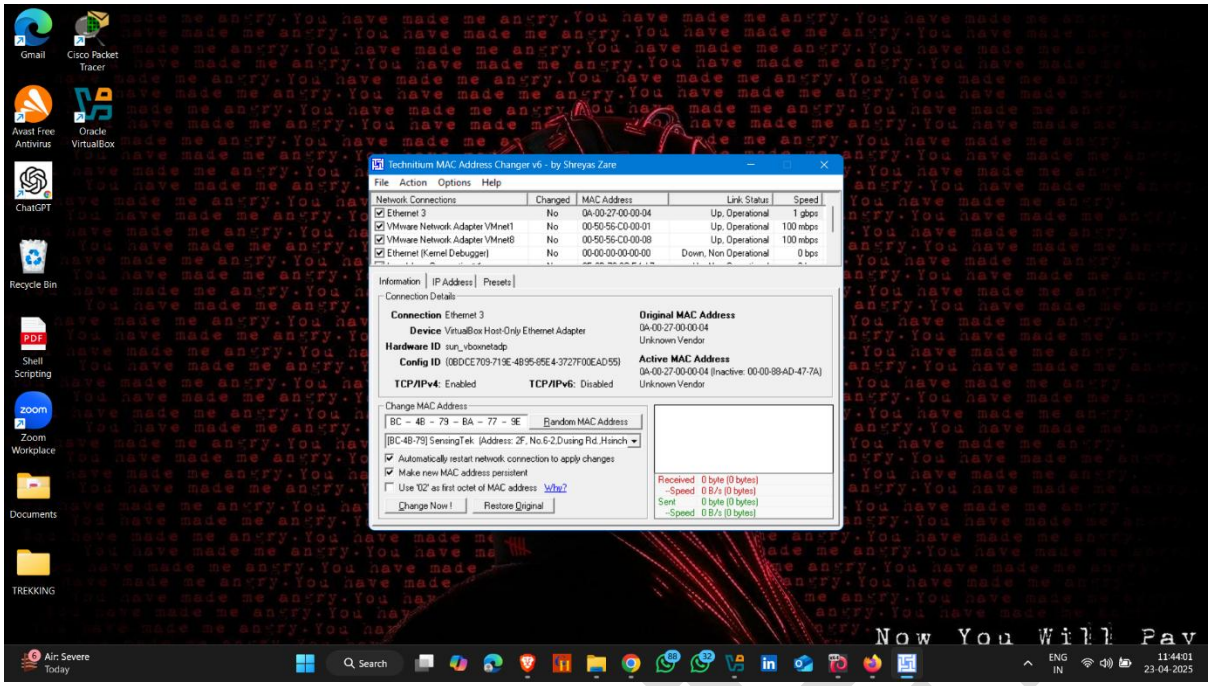
- **How to use it-**
- After installation Open it



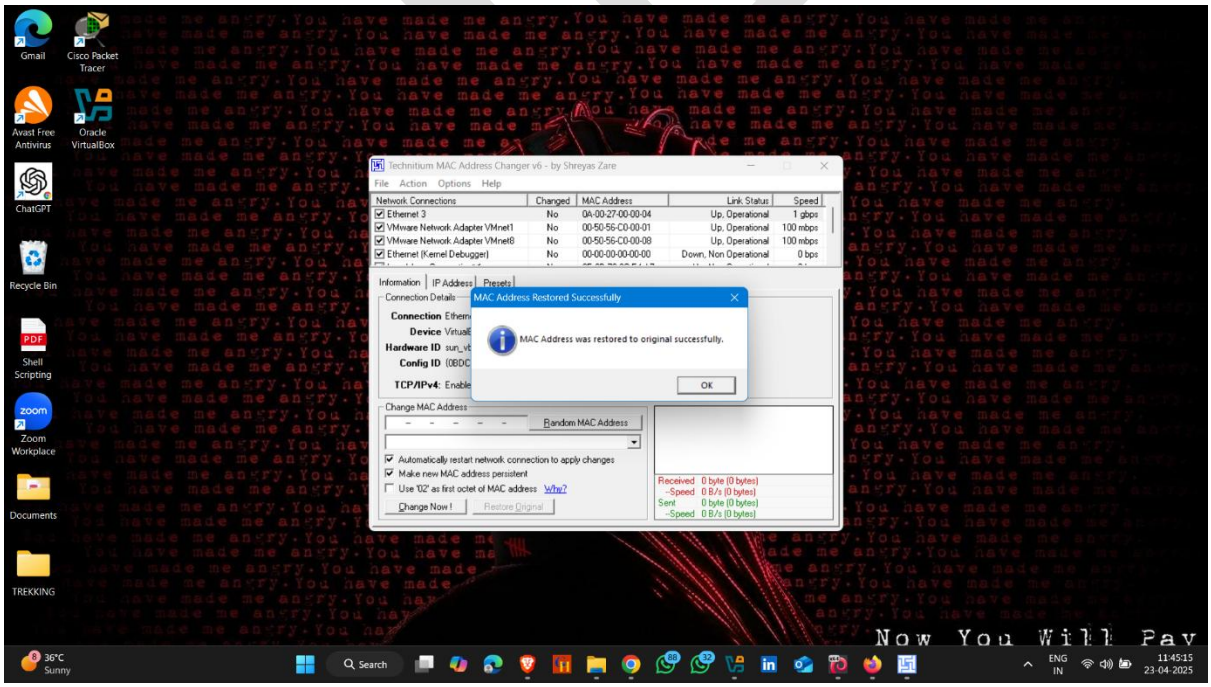
- Click on ethernet 3 and then click on **Random Mac Address**



- It Generate the random mac address



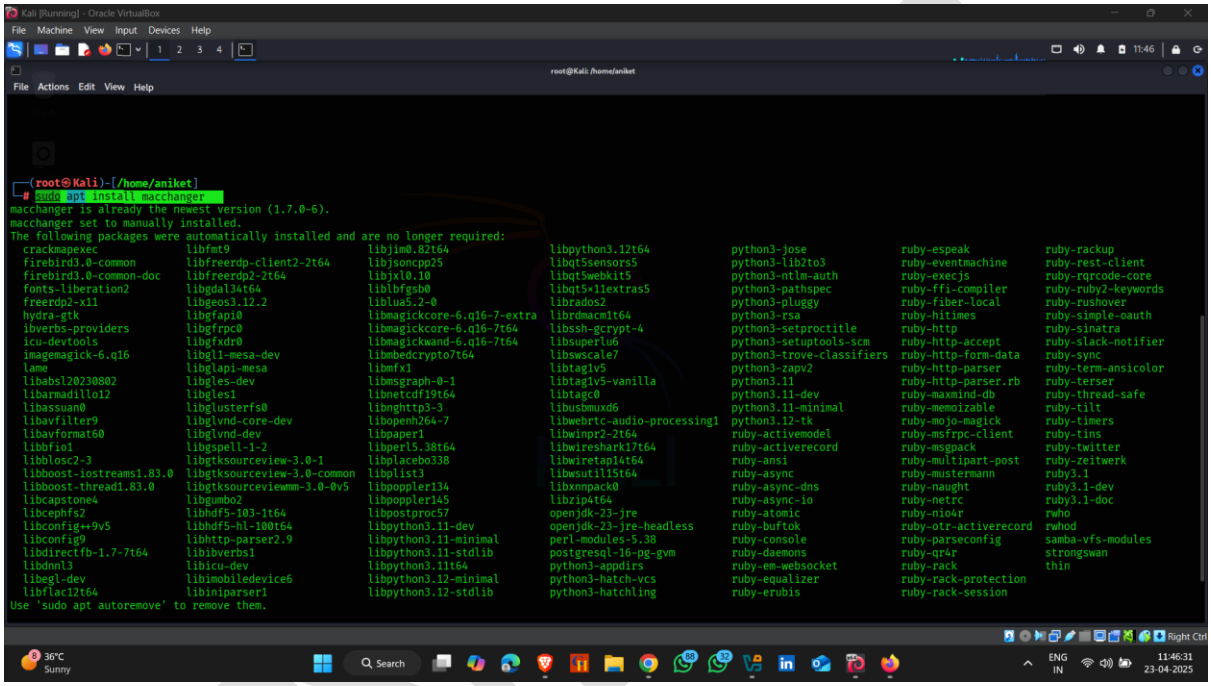
- Now click on Return Original – it back to the your real mac address



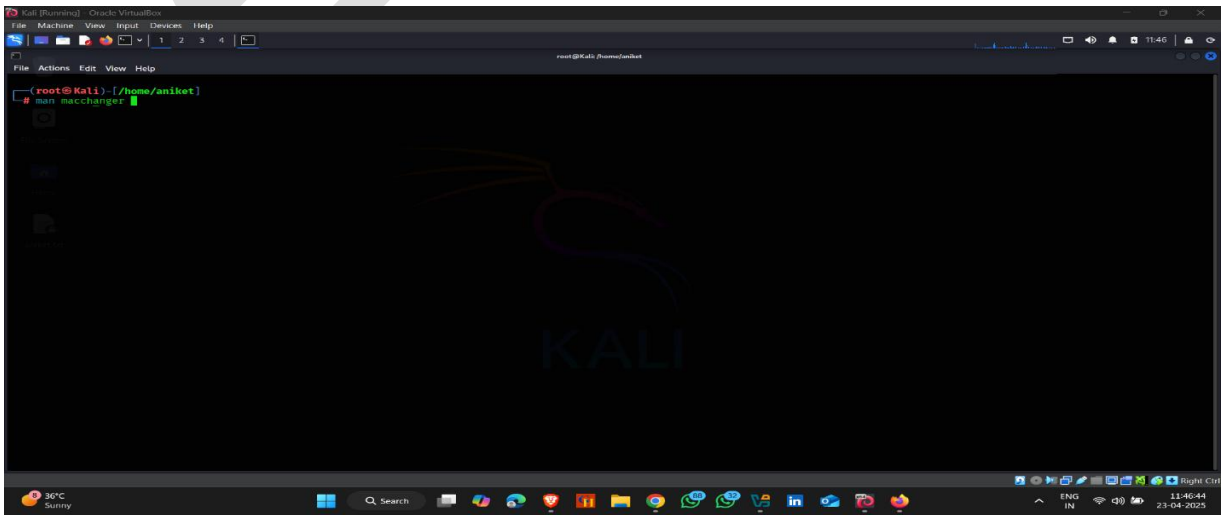
Perform MAC Spoofing using macchanger

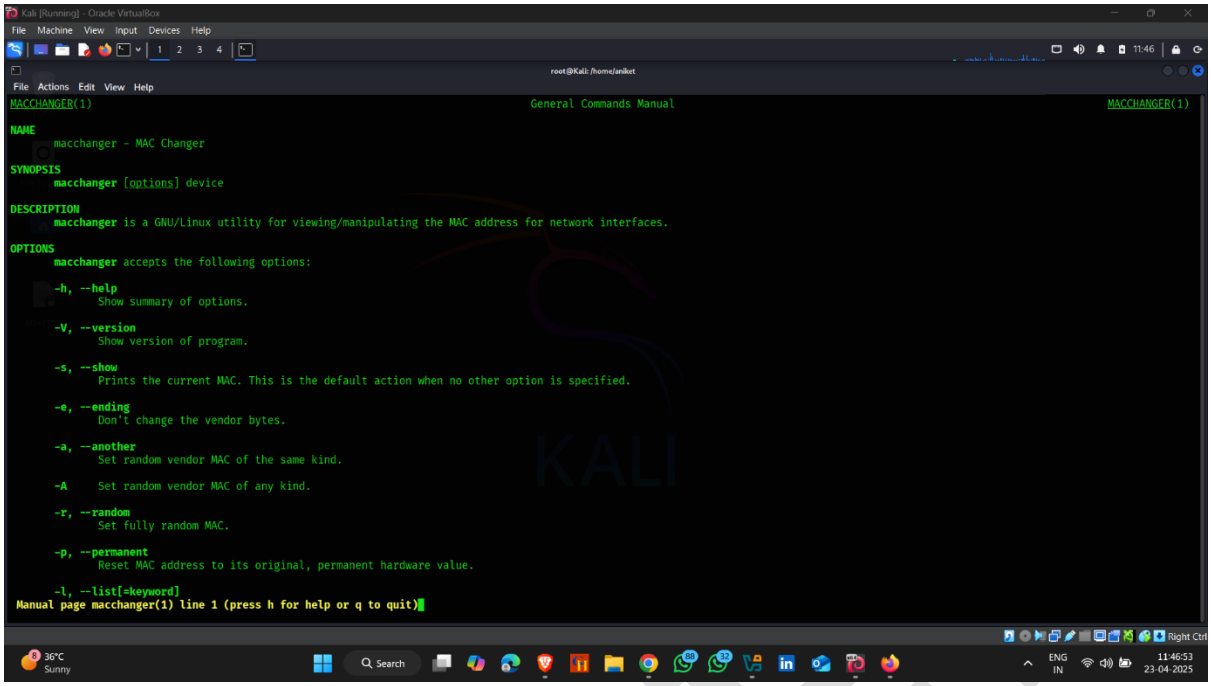
How to use it -:

- **Open kali linux /Parrot OS terminal**
- **Type** sudo apt install macchanger

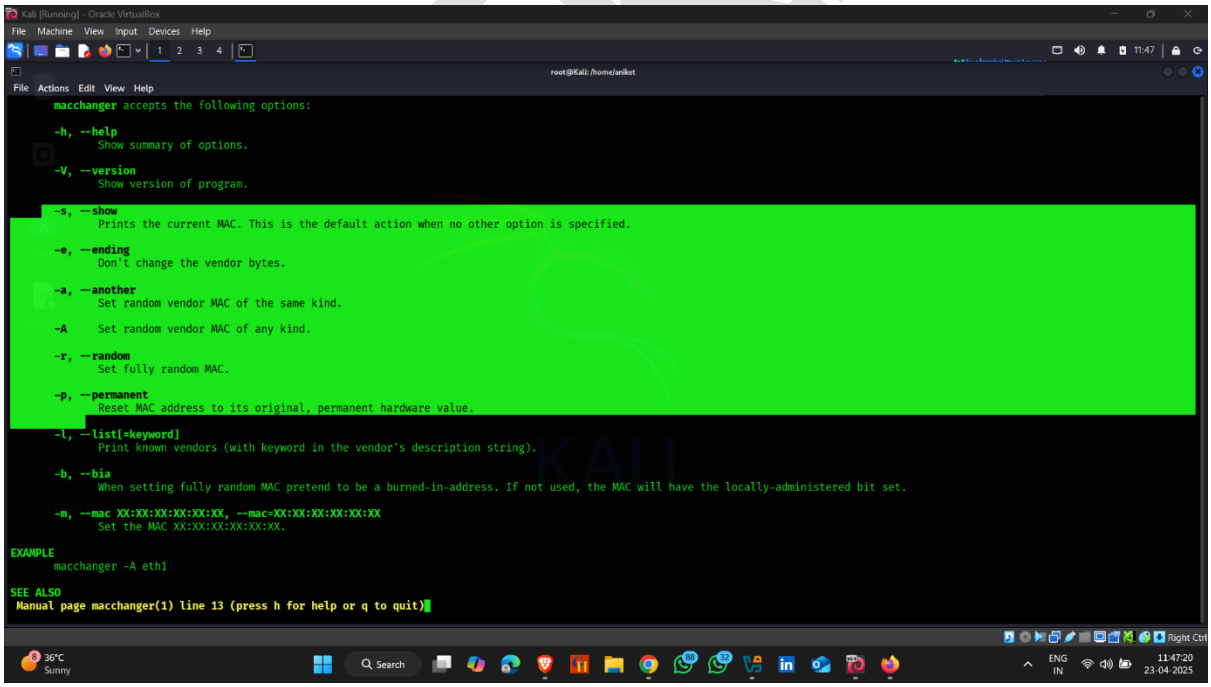


- To get detailed information about macchanger – **man macchanger**

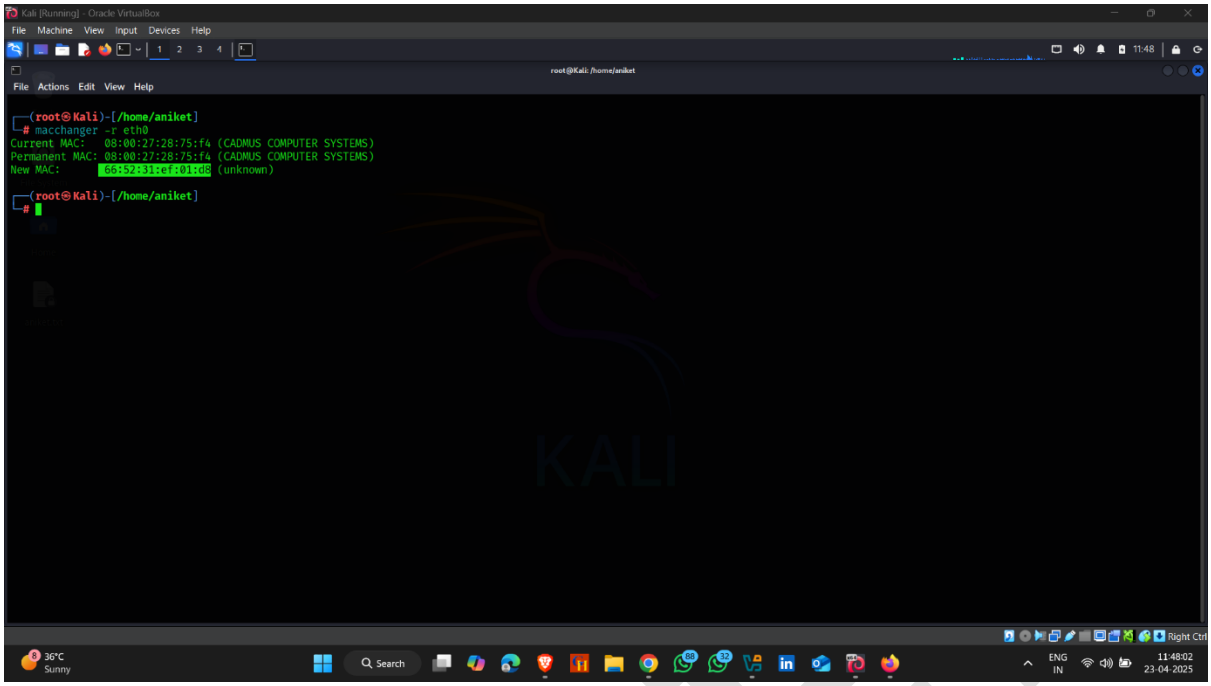




- **Here some switches to generate random mac address**

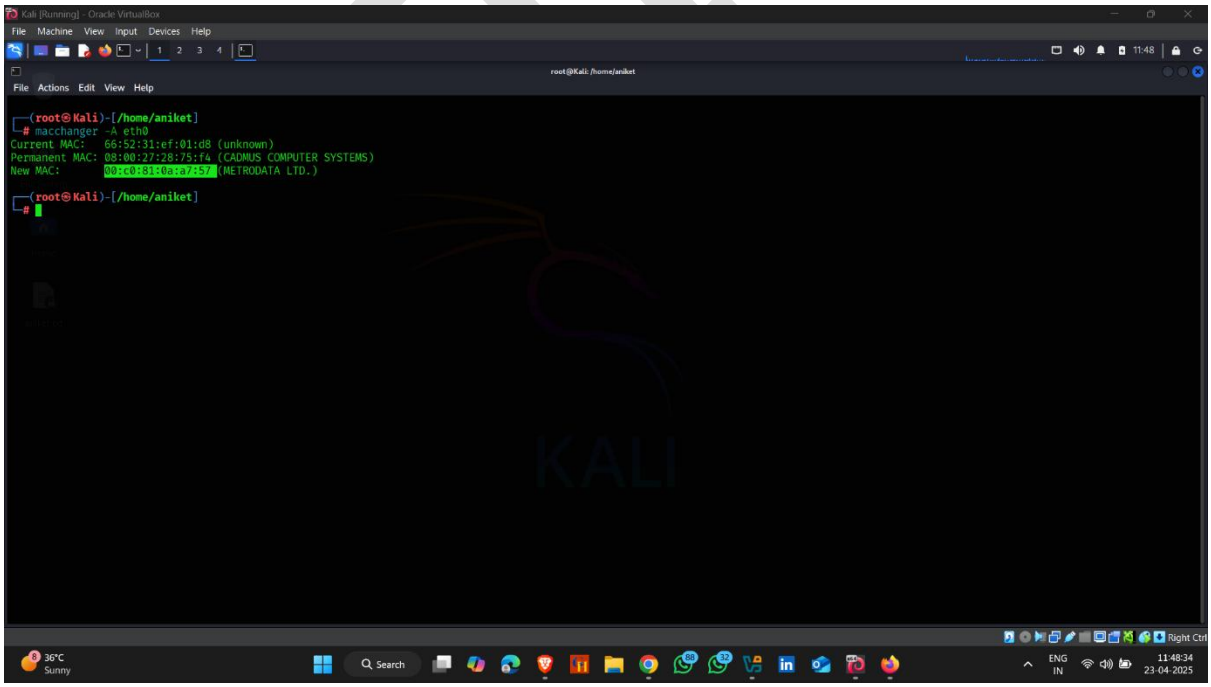


- **Macchanger -r eth0**
  -r – random
  Eth0 –network interface

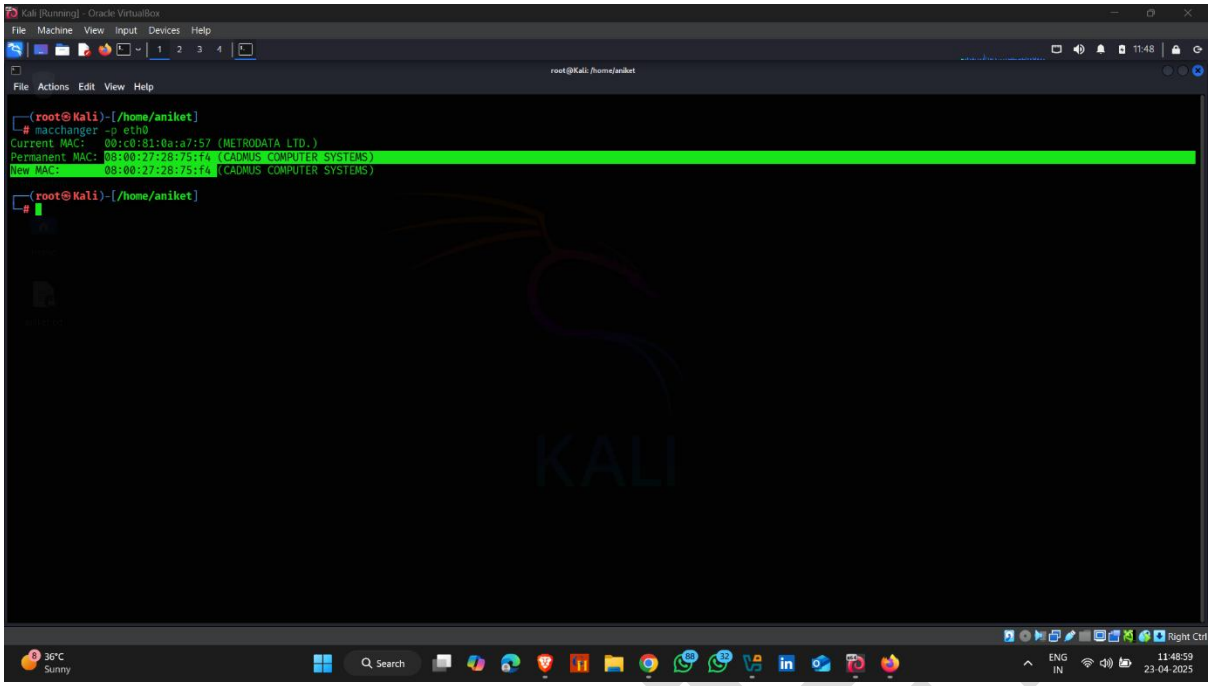


- **Macchanger -A eth0**

-A –random vendor mac of same kind



- **Macchanger -p eth0**
- **-p –permanent/original mac address**


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: /home/aniket
File Actions Edit View Help
(root㉿Kali)-[/home/aniket]
macchanger -p eth0
Current MAC: 00:c0:81:0a:a7:57 (METRODATA LTD.)
Permanent MAC: 08:00:27:28:75:f4 (CADMUS COMPUTER SYSTEMS)
New MAC: 08:00:27:28:75:f4 (CADMUS COMPUTER SYSTEMS)
(root㉿Kali)-[/home/aniket]
#
36°C
Sunny
Search
ENG
IN
11:48:59
23-04-2025
Right Ctrl

EXTRA ACTIVITY

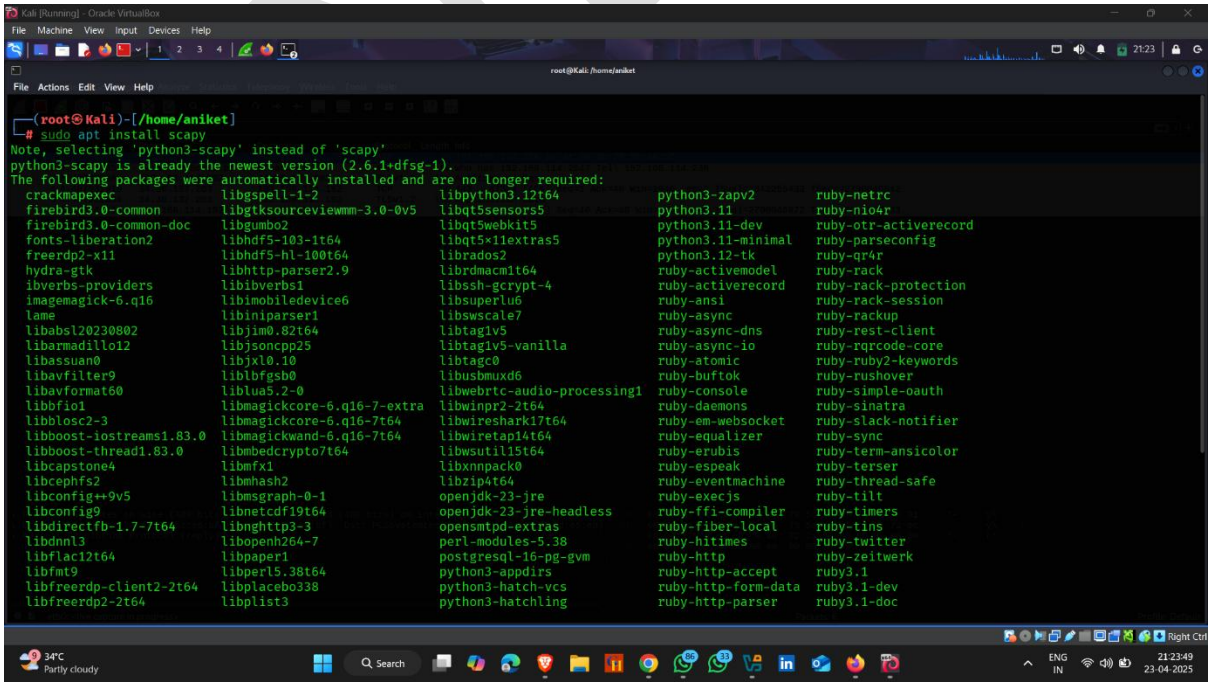
MAC FLOODING

1.Perform MAC Flooding Using Scapy (Linux Tool)

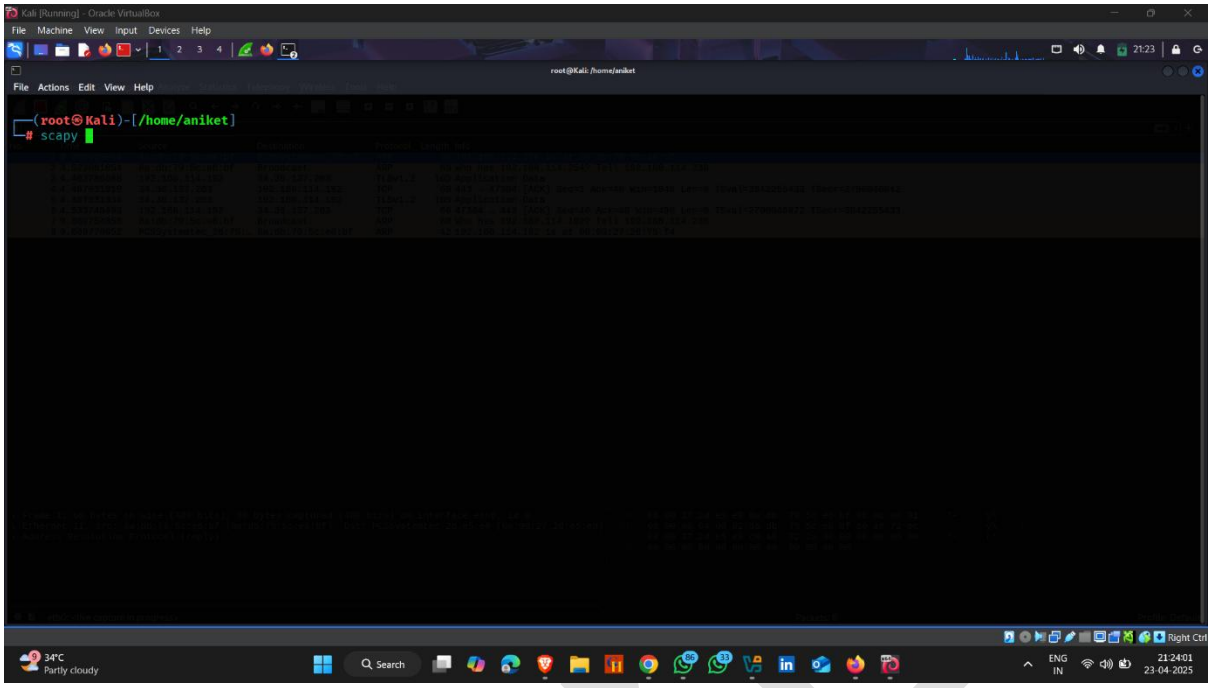
Scapy is an open-source, Python-based interactive tool used for packet crafting, sniffing, analyzing, and injecting packets into a network for the purpose of network testing, security auditing, and ethical hacking.

How to use it –

- Open kali Terminal
- Type –sudo apt install scapy

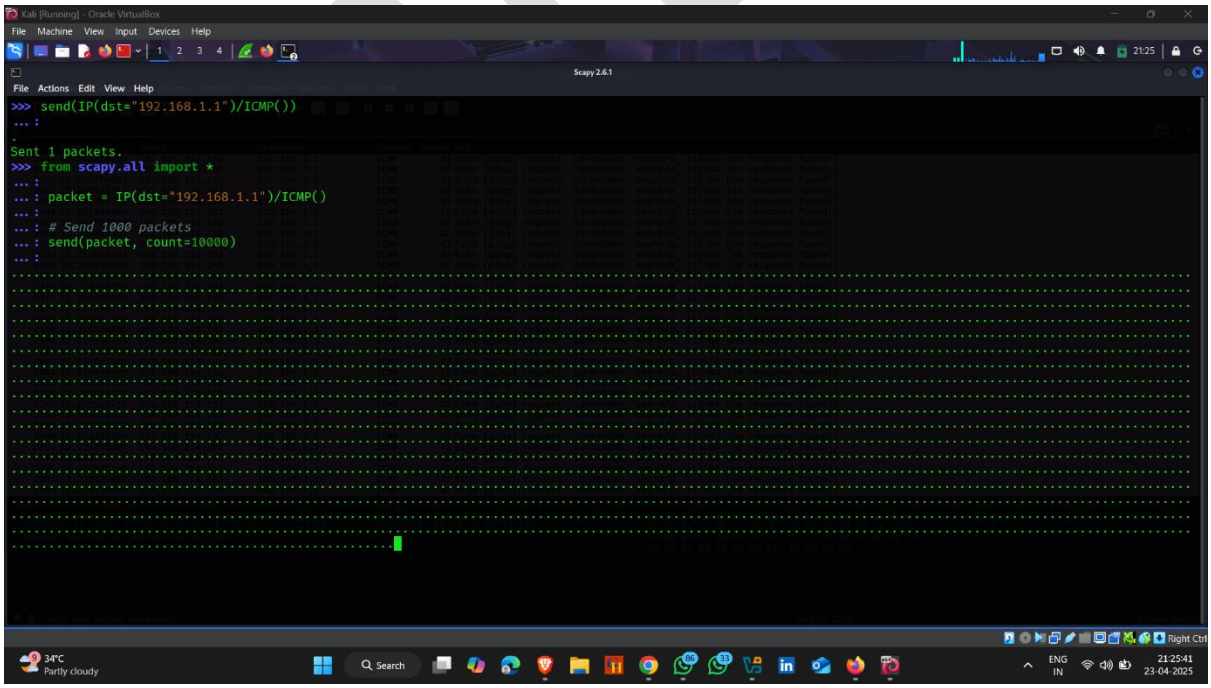


- **Run scapy**



- Sending 1 packet

Command – send(IP(dst=target ip)/ICMP())

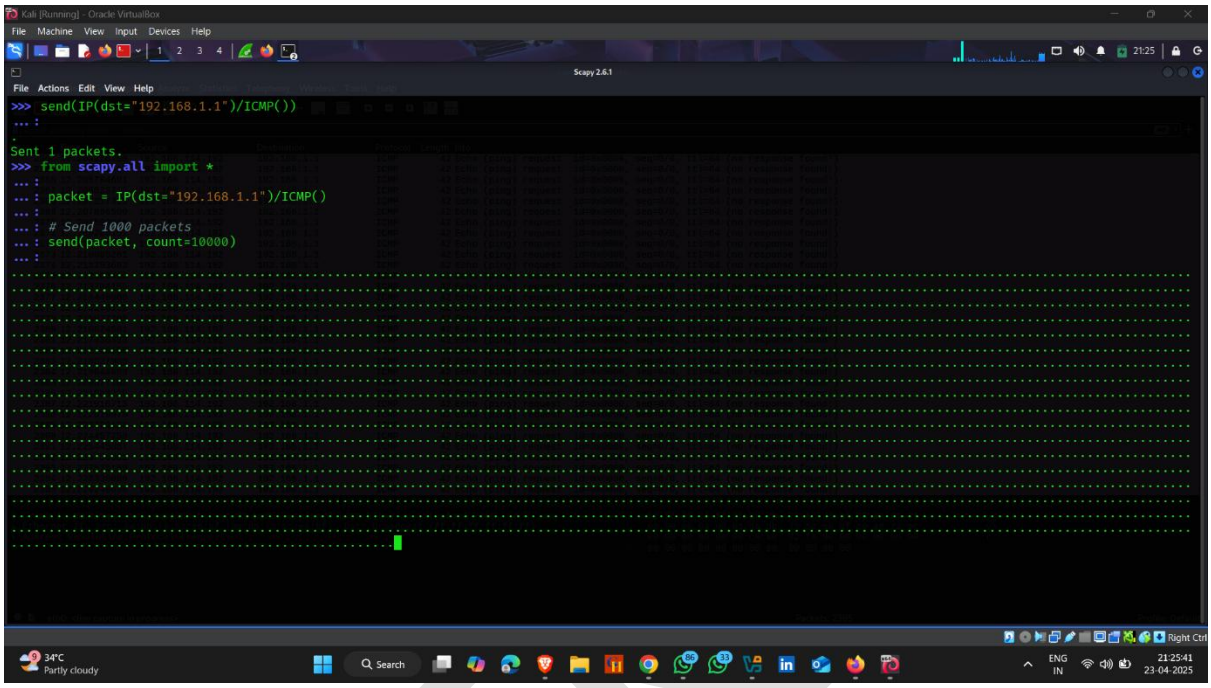


- Send Multiple packets

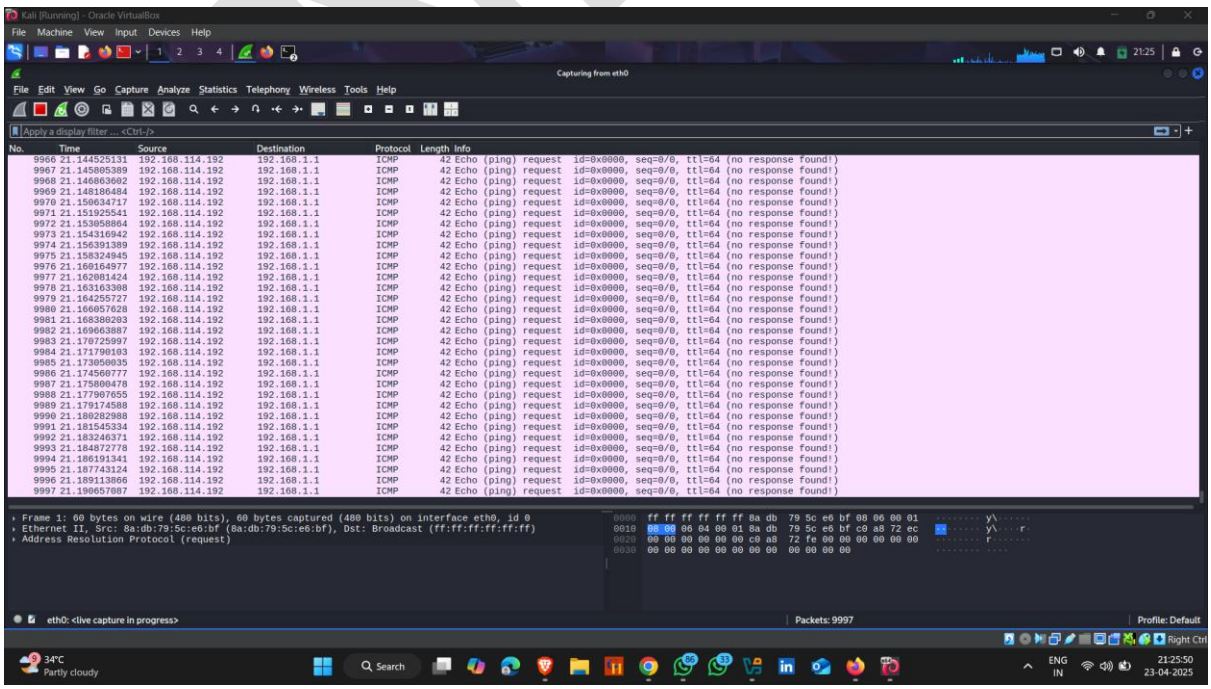
Command – packet =IP(dst=”target ip ”)/ICMP())

Send(packet,count=10000)

- 10000 packet sending started



- **Open Wireshark**
- **Here 10000 ICMP packets sending started**

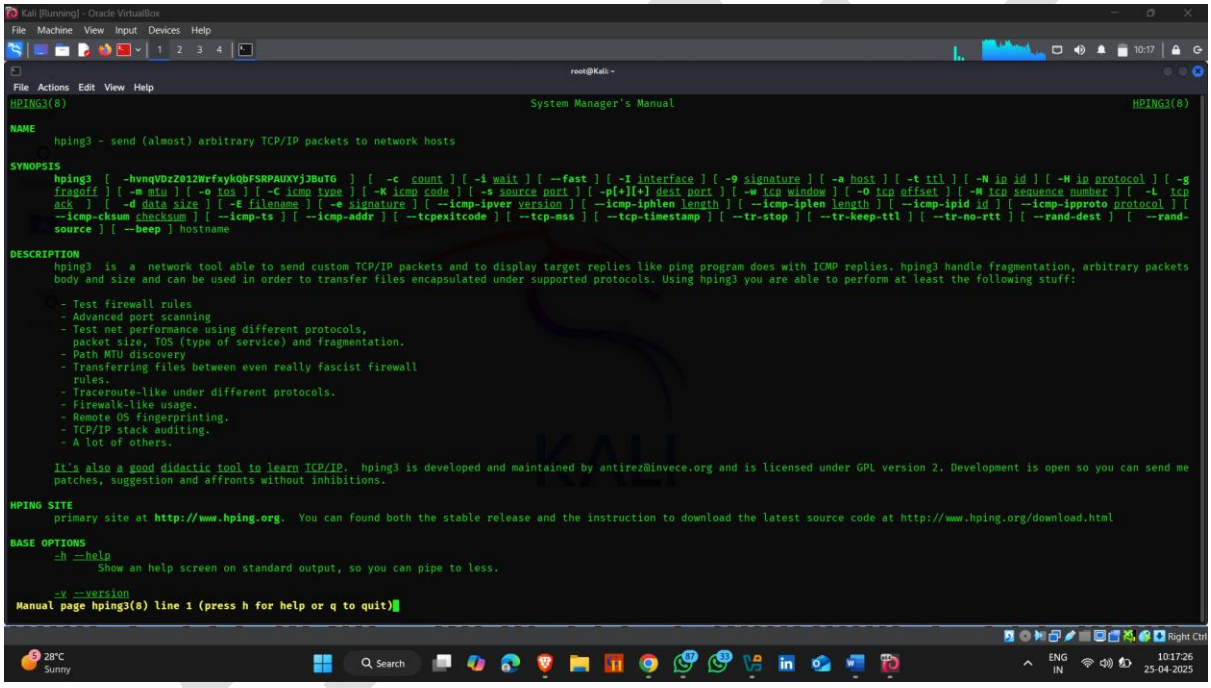


2.Perform MAC Flooding Using Hping3 (Linux Tool)

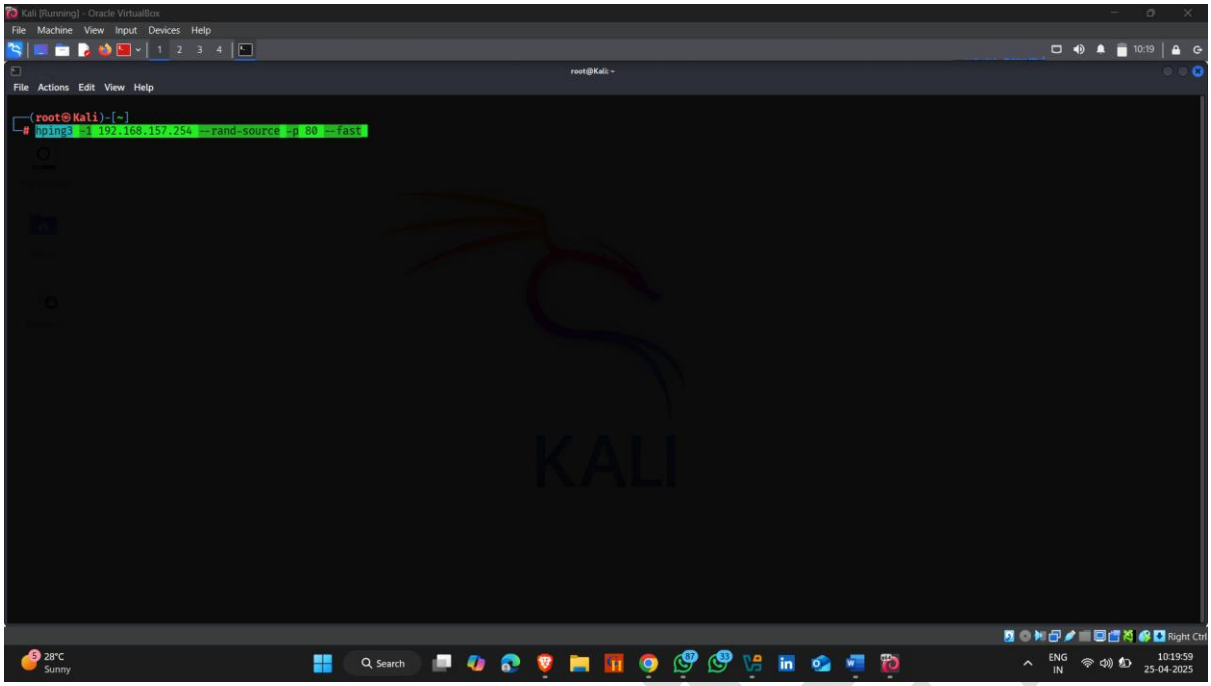
hping3 is a powerful **command-line packet crafting tool** used primarily for **network security auditing and penetration testing**. It allows you to **send custom TCP/IP packets** and analyze the responses

How to use it -:

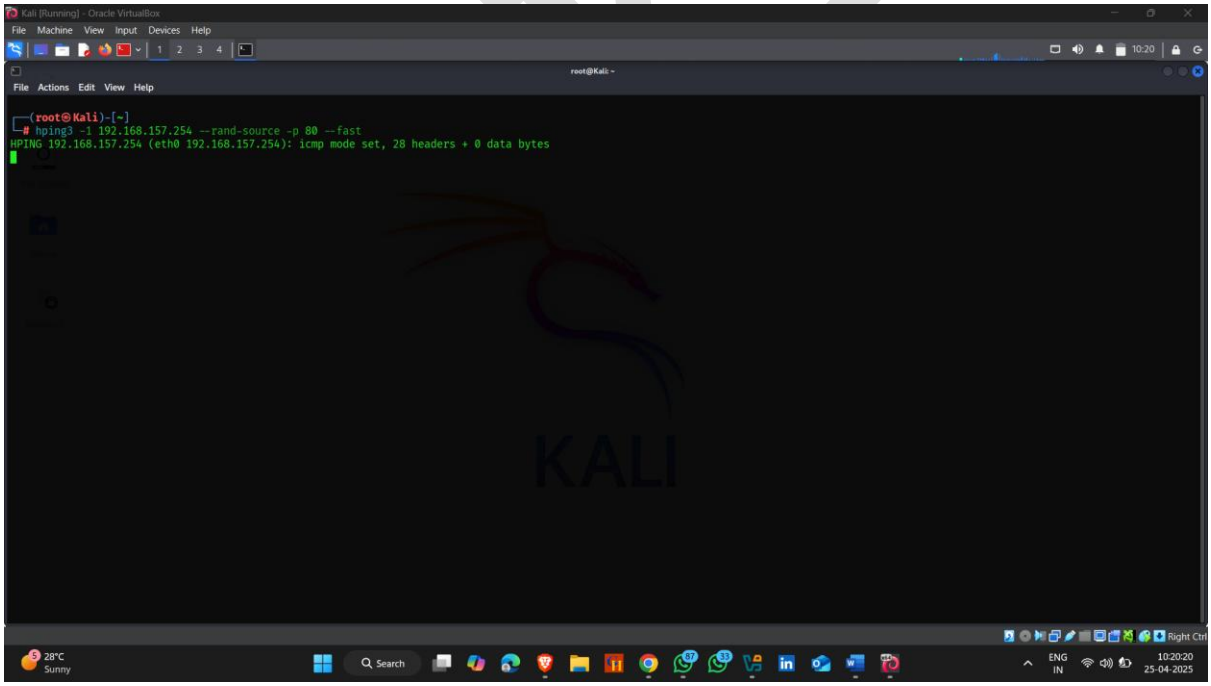
- Open kali linux Terminal and type **man hping3 –** To get Detailed information about hping3



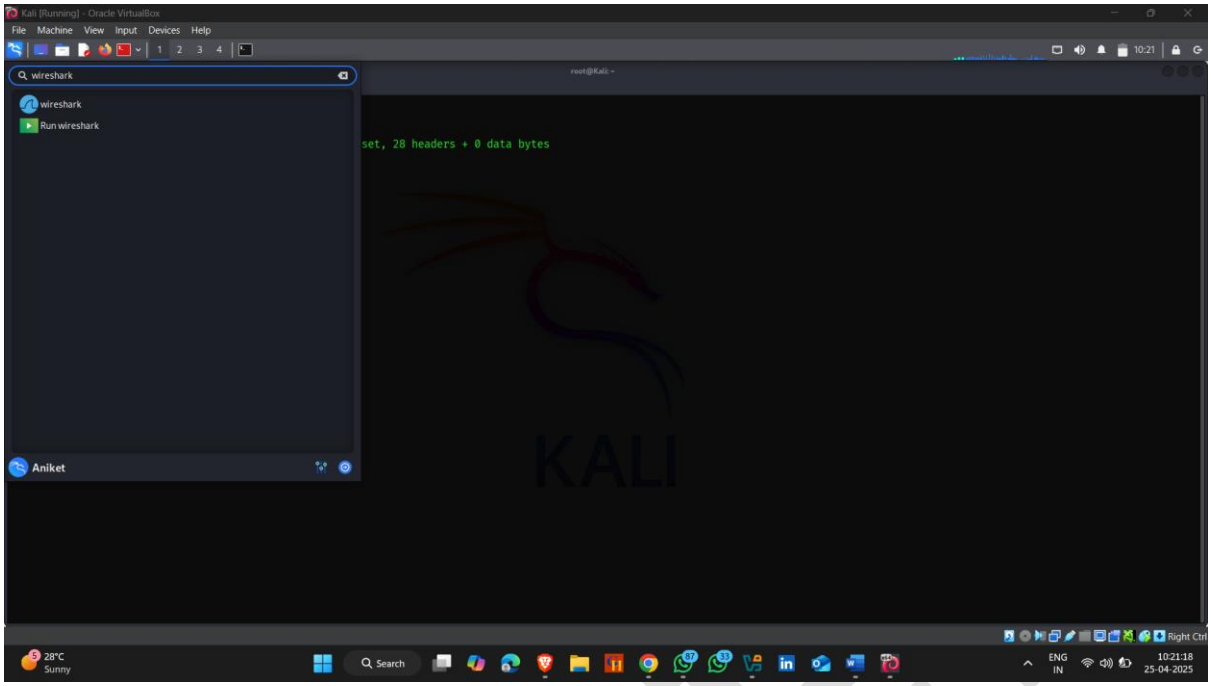
Command --:hping3 -1 192.168.157.254 --rand-source -p 80 –fast



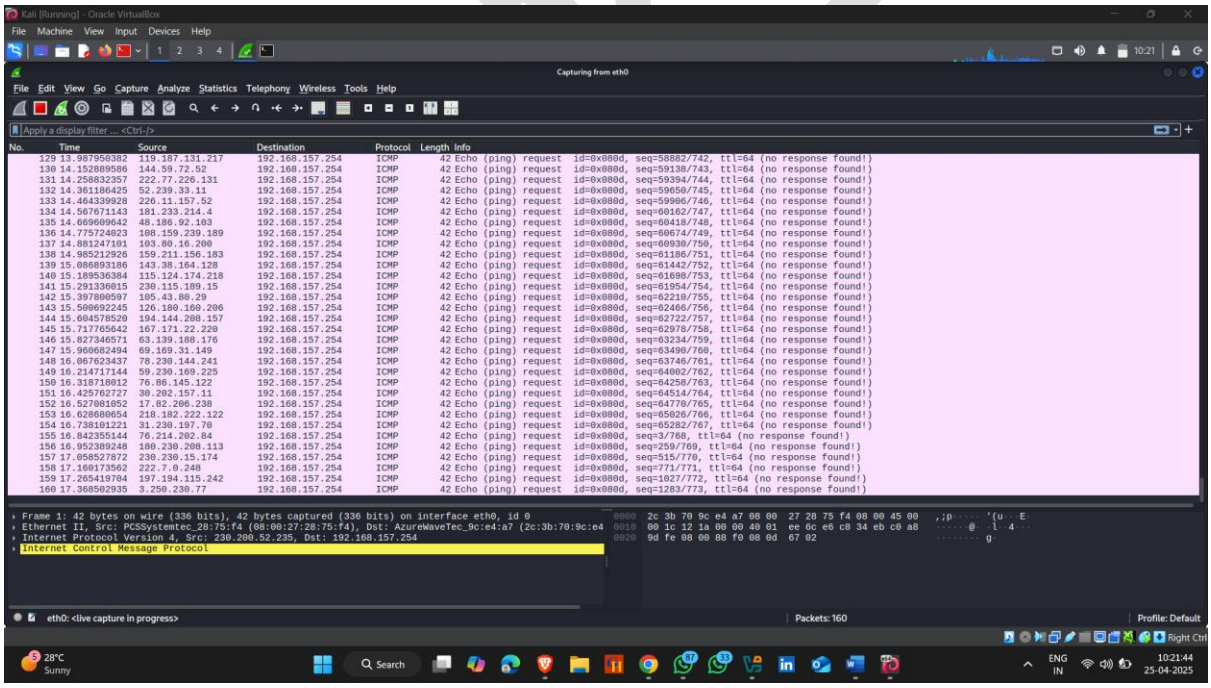
- **Attack Start**



- **Now open wireshark to analys packets**

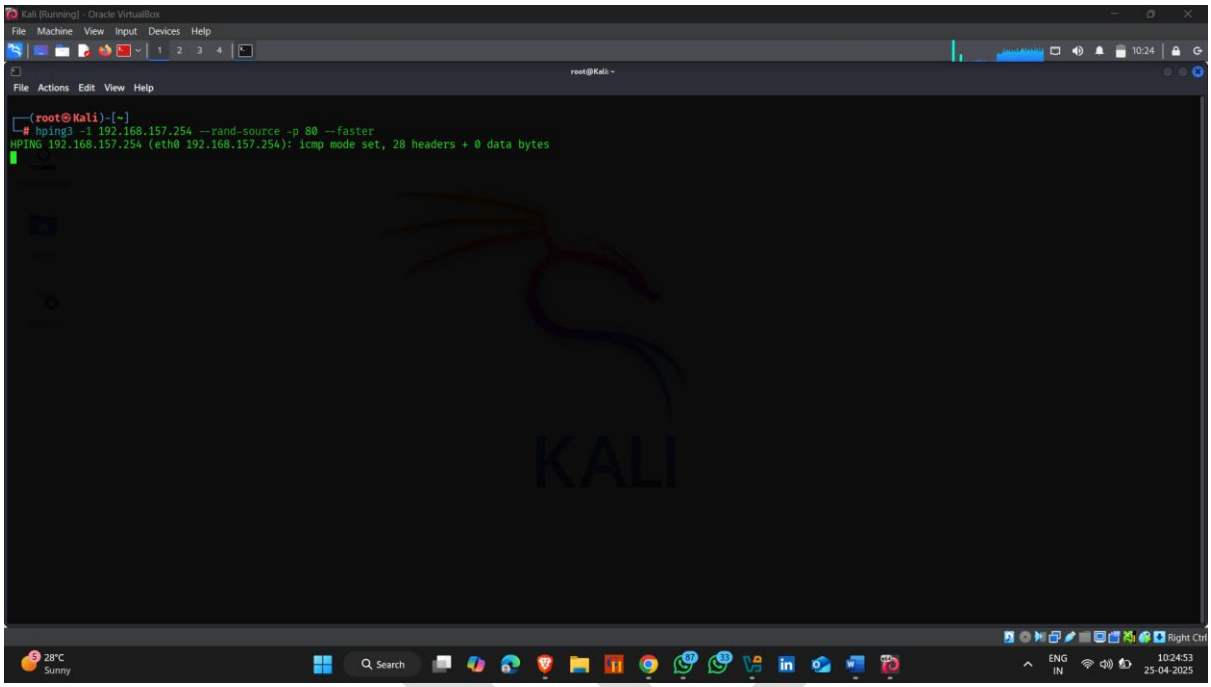


- **Packets are send to the target**

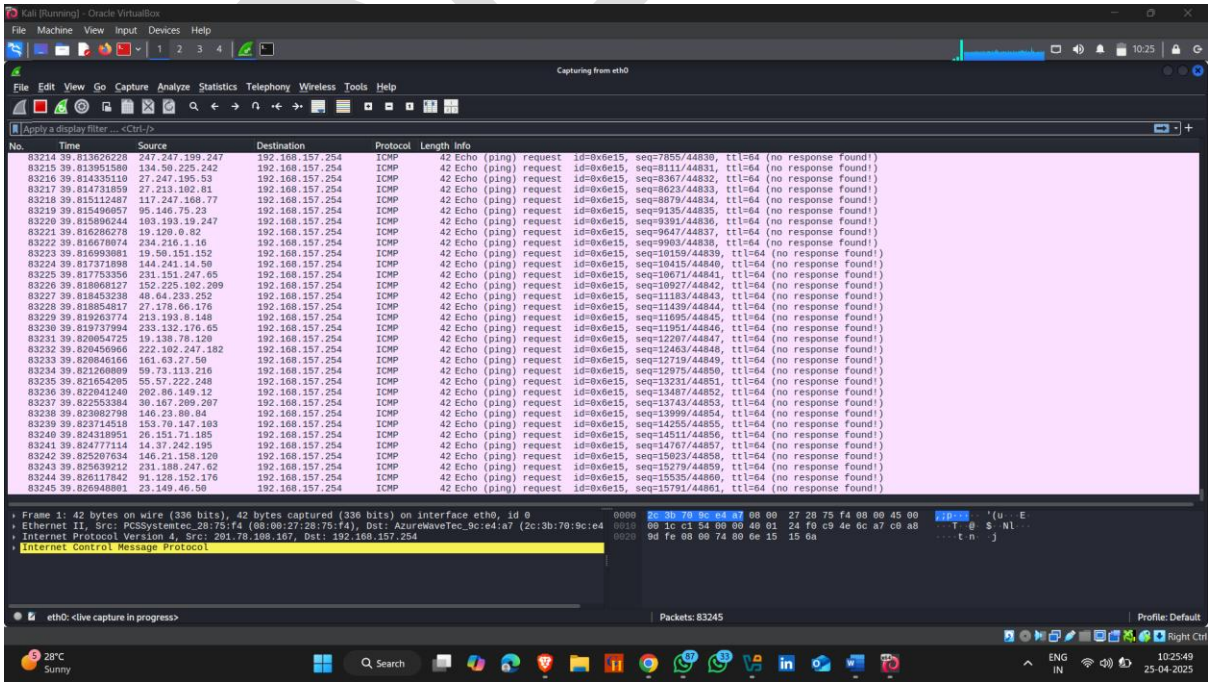


Now Send more faster

Command -- hping3 -1 192.168.157.254 --rand-source -p 80 –faster

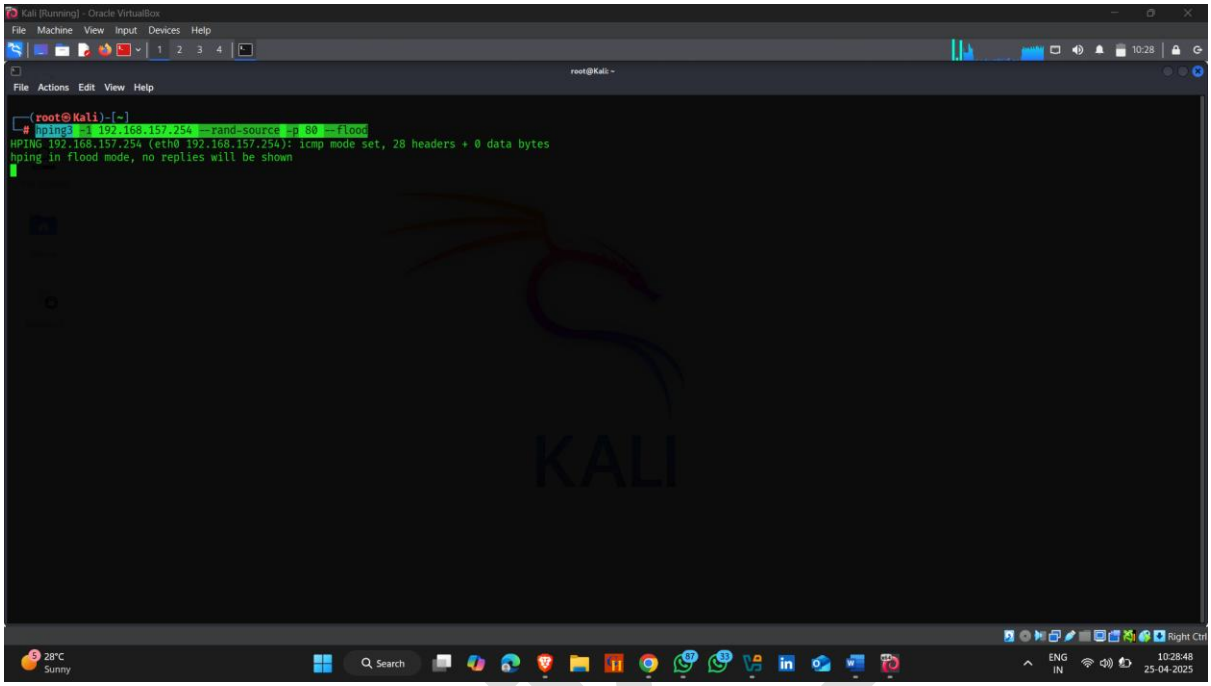


- **83000 packets are send**

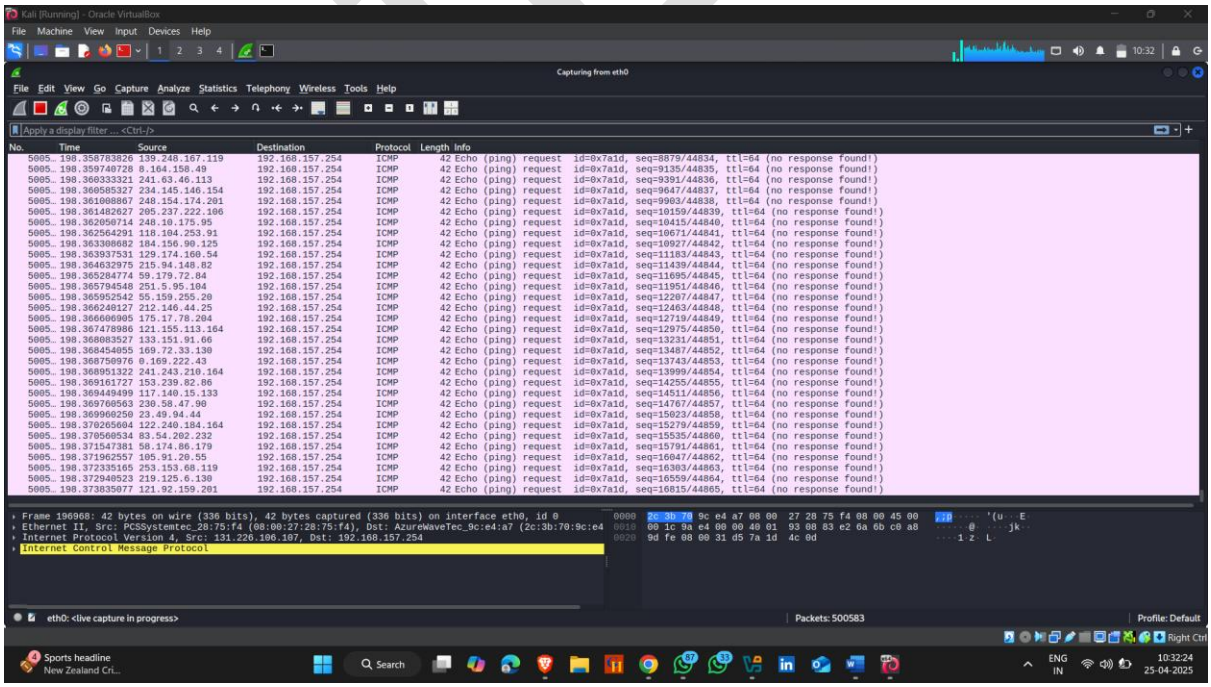


Now send Flooding of packets

Command -: hping3 -1 192.168.157.254 --rand-source -p 80 --flood



- **500000 packets are send**

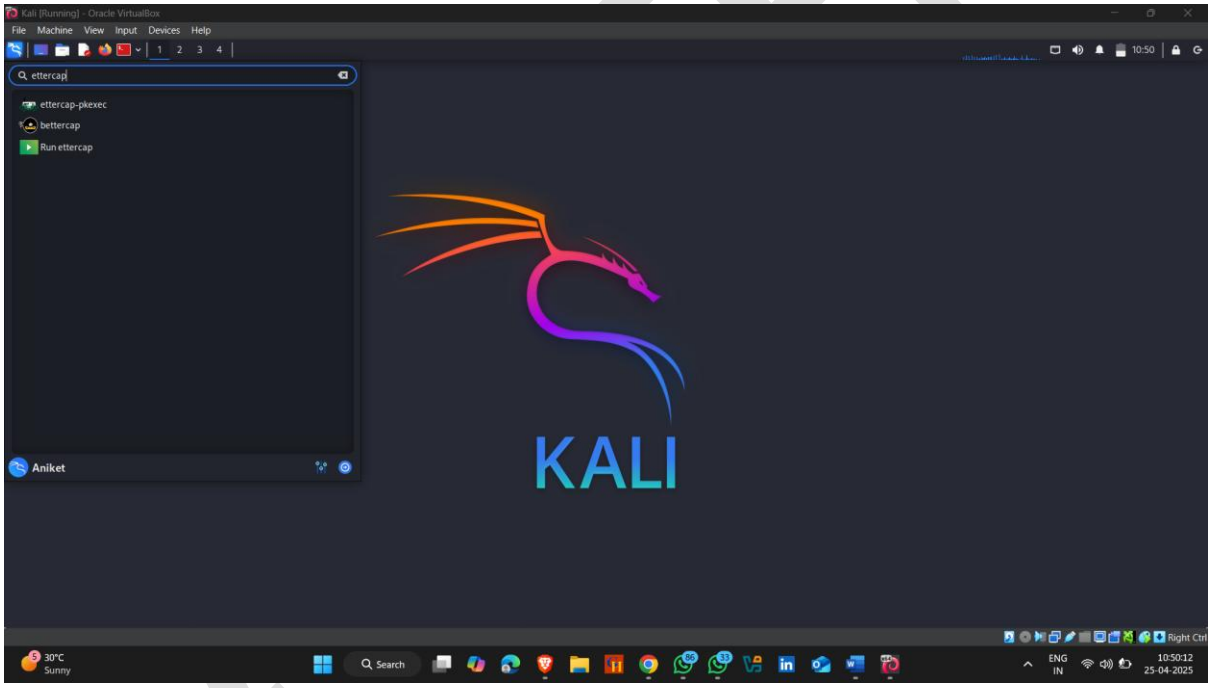


3.Perform MAC Flooding Using Ettercap (Linux Tool)

Ettercap is a powerful **network security tool** used primarily for **network protocol analysis** and **man-in-the-middle (MITM) attacks**. It's commonly used by penetration testers and cybersecurity professionals to inspect, intercept, and manipulate traffic on a local network.

How to use it -:

- Open kali linux
- Go to application Section and search Ettercap

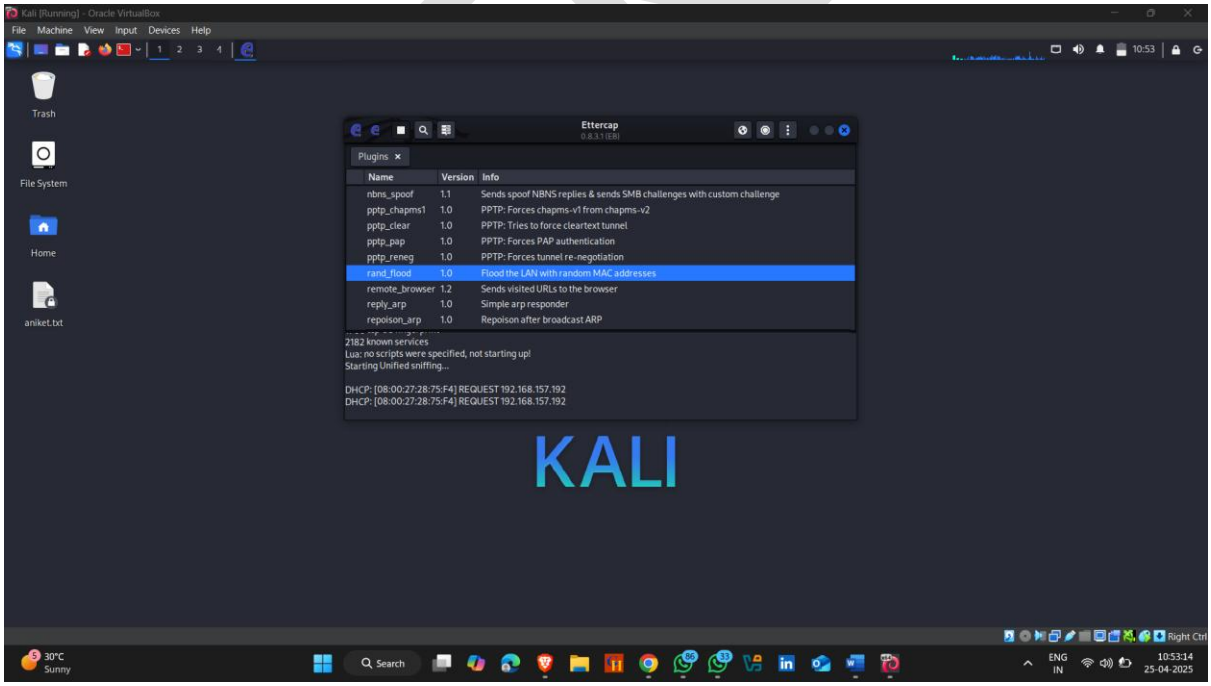


- Open it
- Click on ✅

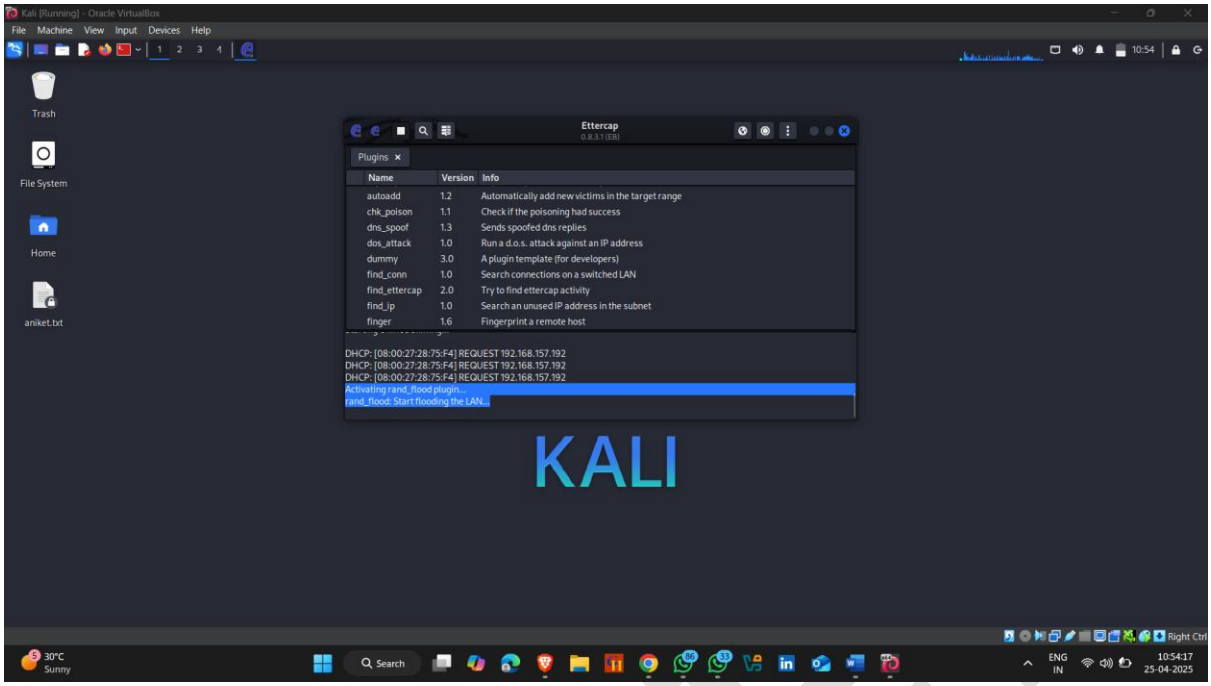
- Click on three dots and then click Plugins

- And then click on manage plugins

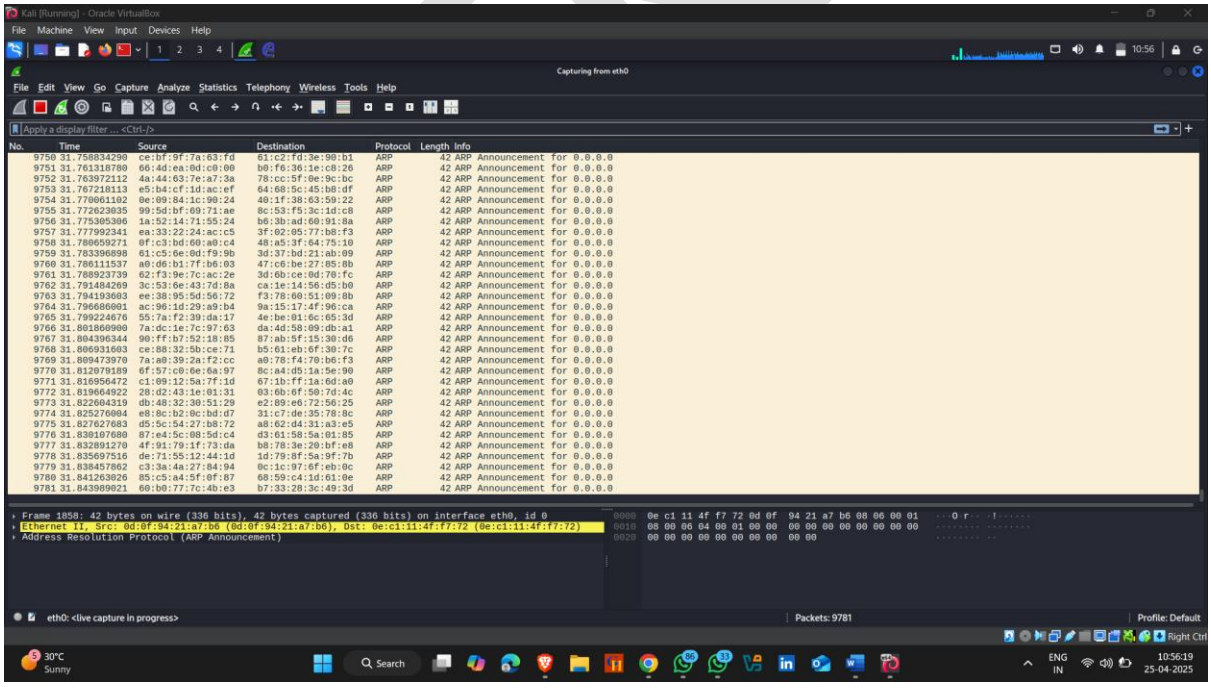
- There is a option **rand_flood**
- Double click on it



- Activating Rand_plugins



- Now go to wireshark to see our attack start or not
- Here , attack is started



4.Perform MAC Flooding Using bettercap (Linux Tool)

Bettercap is a powerful, flexible, and modern network attack and monitoring tool.

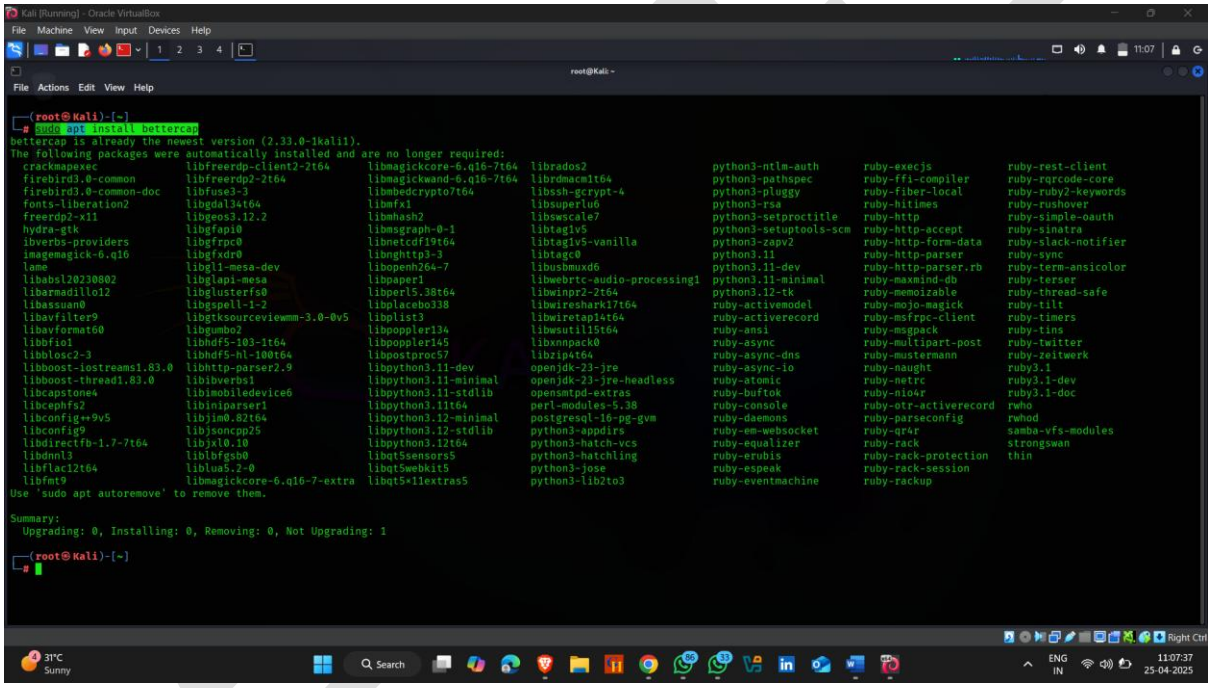
How to install it -:

- Open kali terminal and type commands

Commands -: sudo apt update

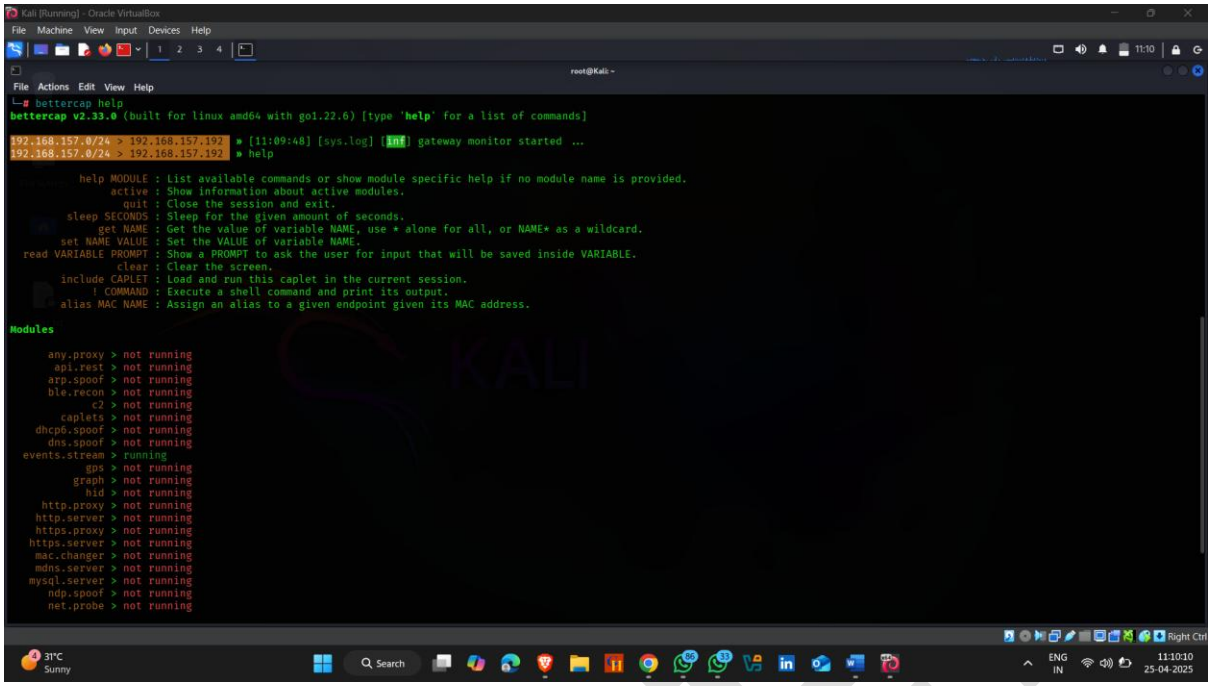
Sudo apt upgrade

Sudo apt install bettercap

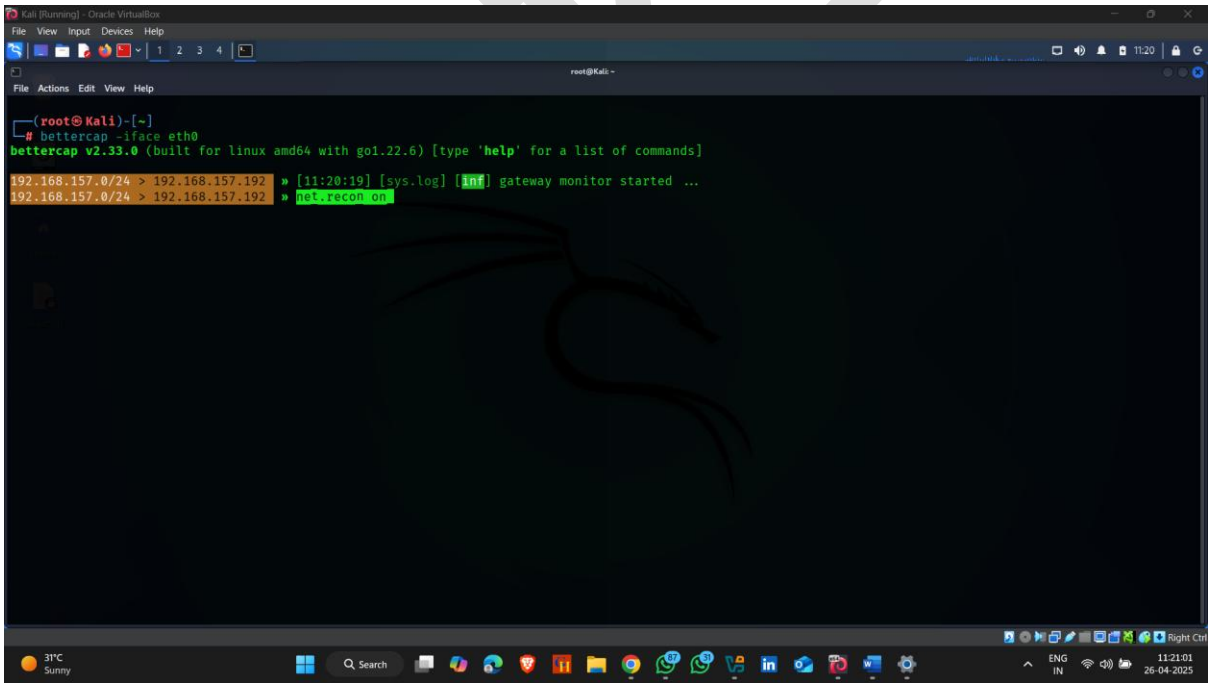


How to use it -:

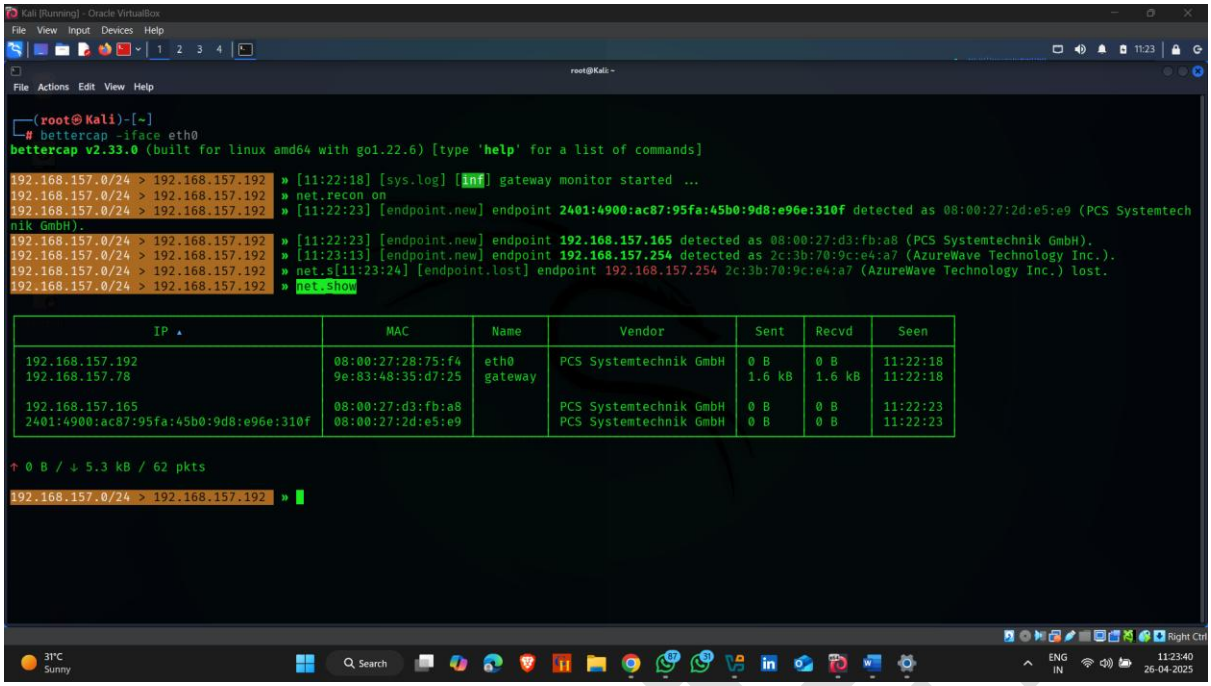
- Type command bettercap help



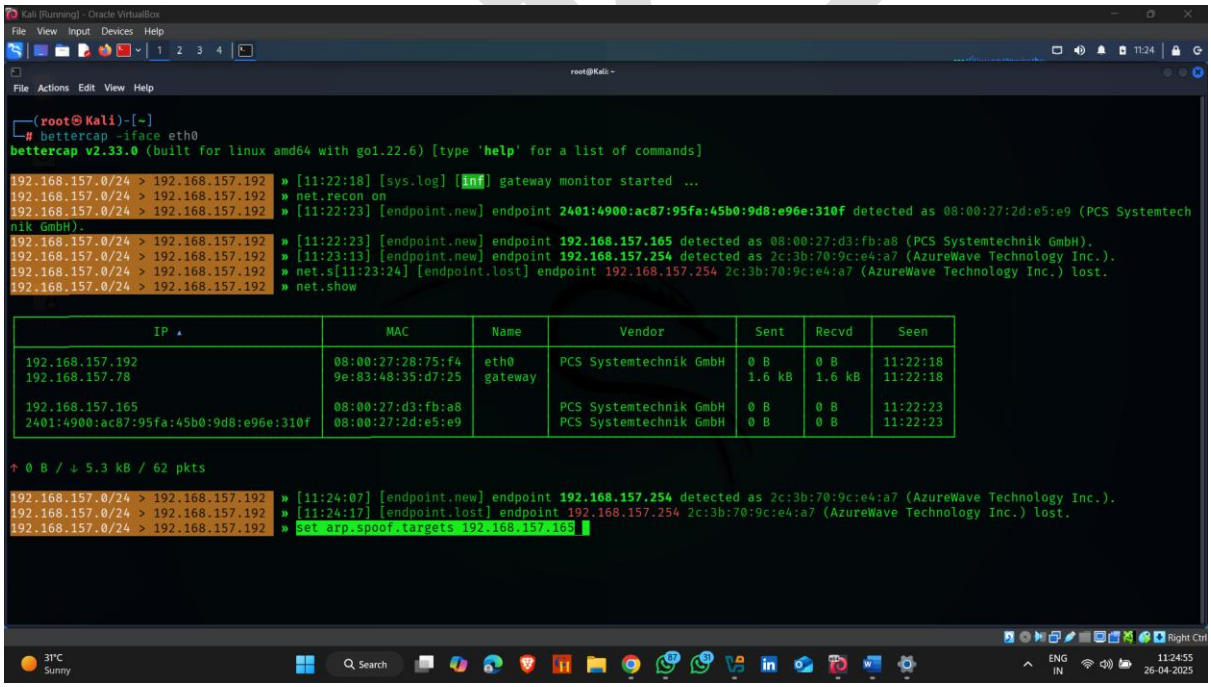
- Now use **net.recon** on – to identify devices in network



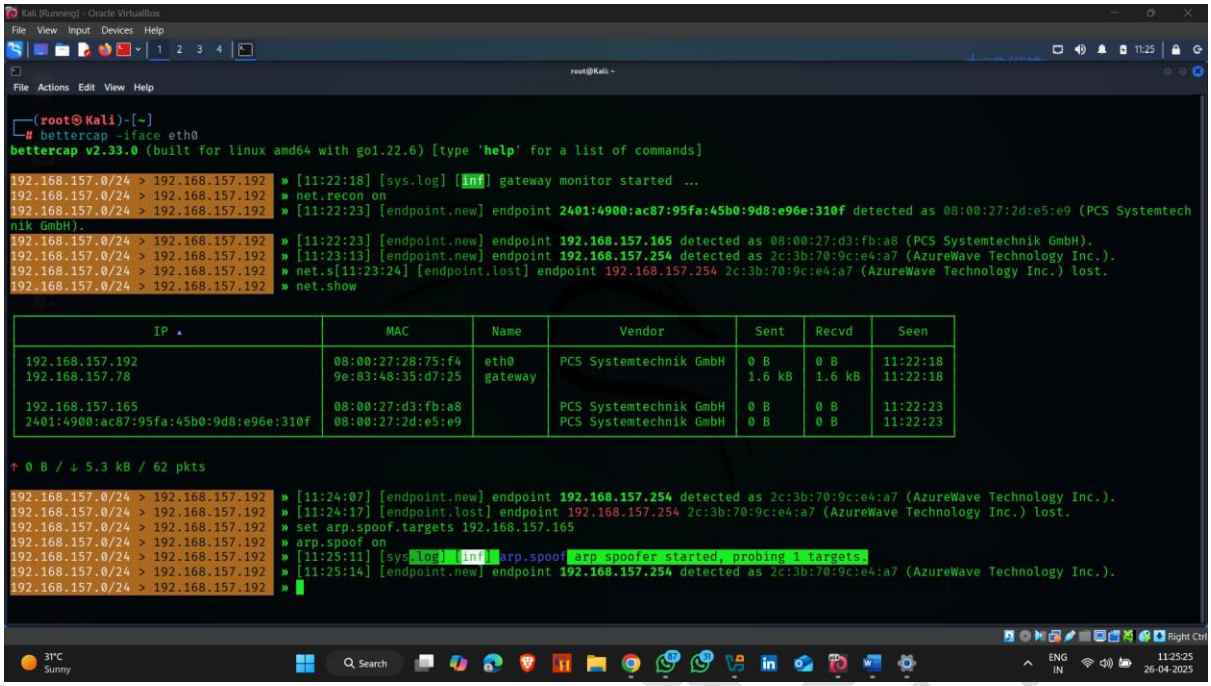
- Now use **net.show** command -- to show how many devices are connected in network



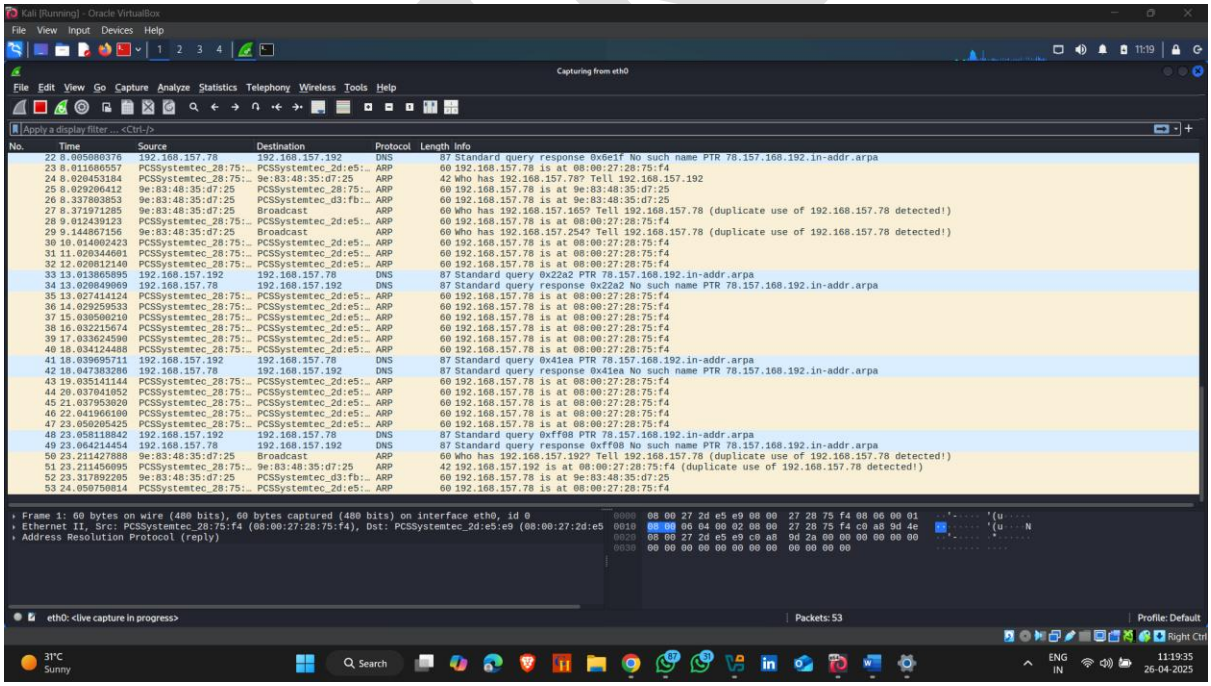
- Use arp.spoof.targets to set your target



- Arp.spoof on --- to start attack
- Attack started



- Now open wireshark to see ARP packets are send or not
- ARP packets are send 👇



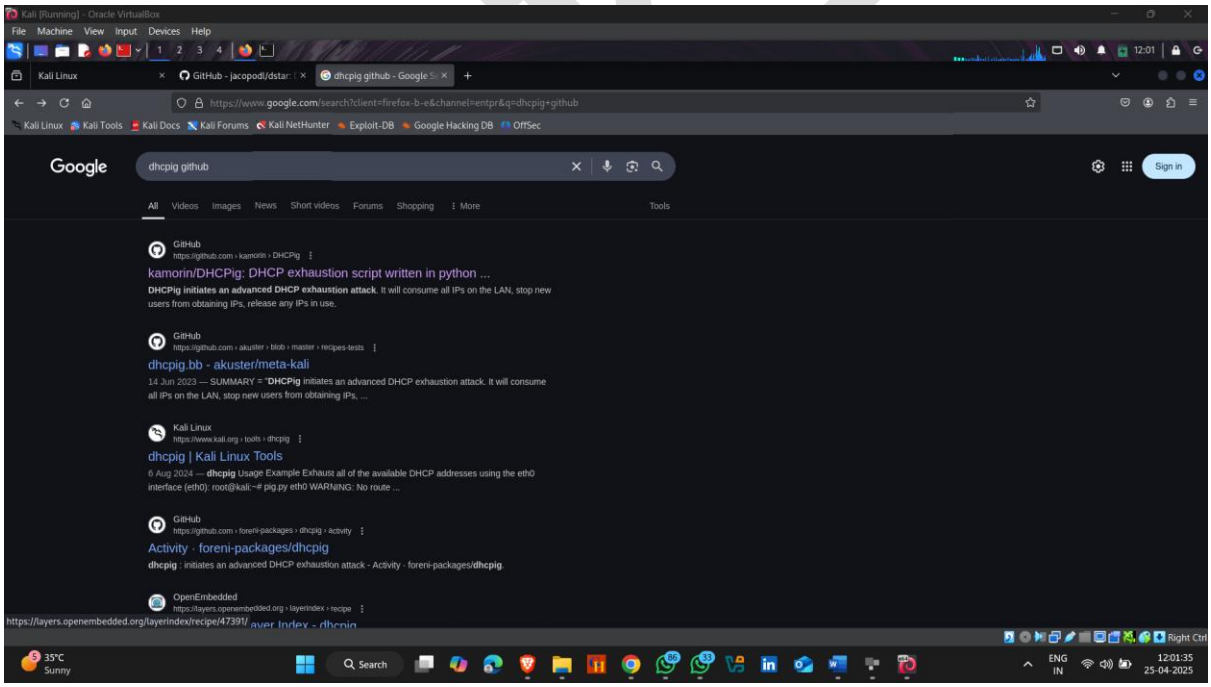
DHCP STARVATION

1.Perform DHCP Starvation using DHCPig

DHCPig is a lightweight tool specifically designed to carry out **DHCP starvation** attacks. It floods a DHCP server with **DHCP requests** from multiple spoofed MAC addresses

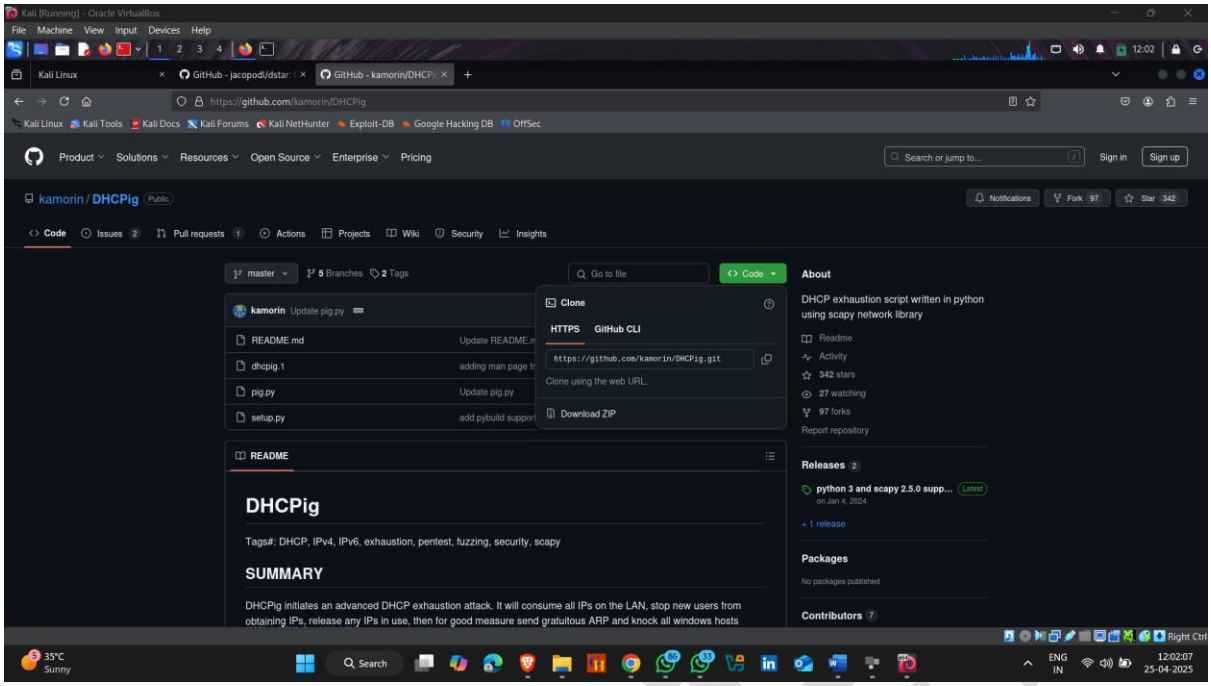
How to install it -:

- Open Browser and search DHCPig github
- Open first website

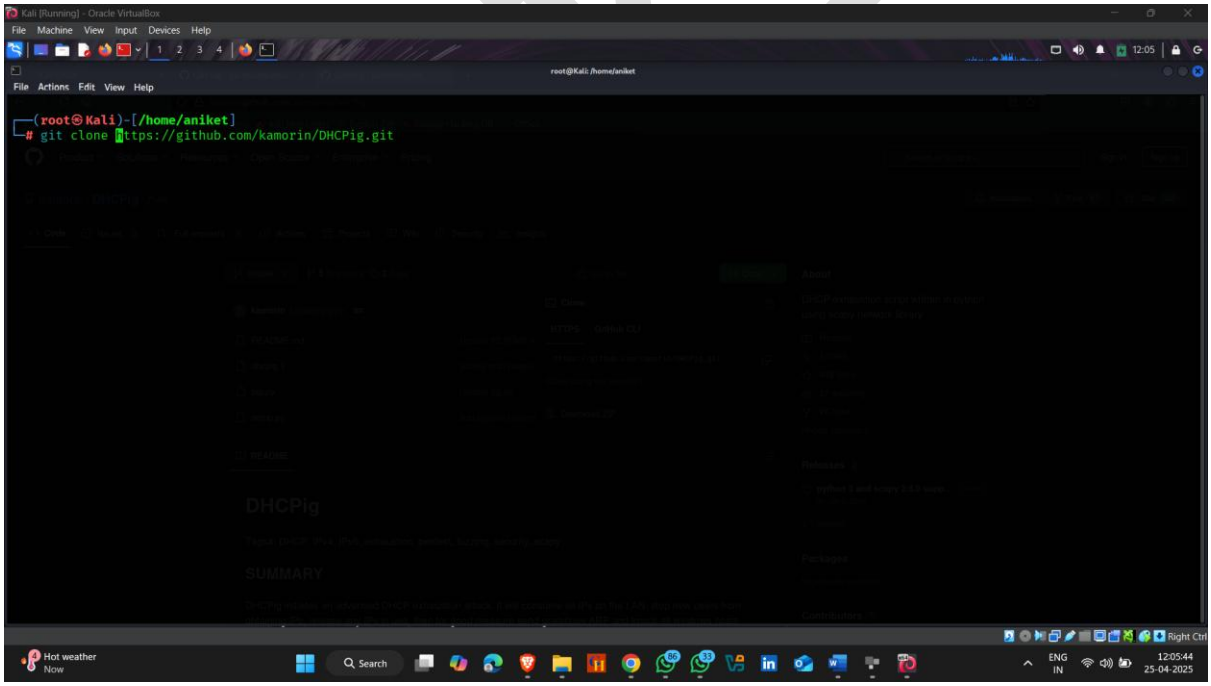


- Now click on Green <code> button and copy link

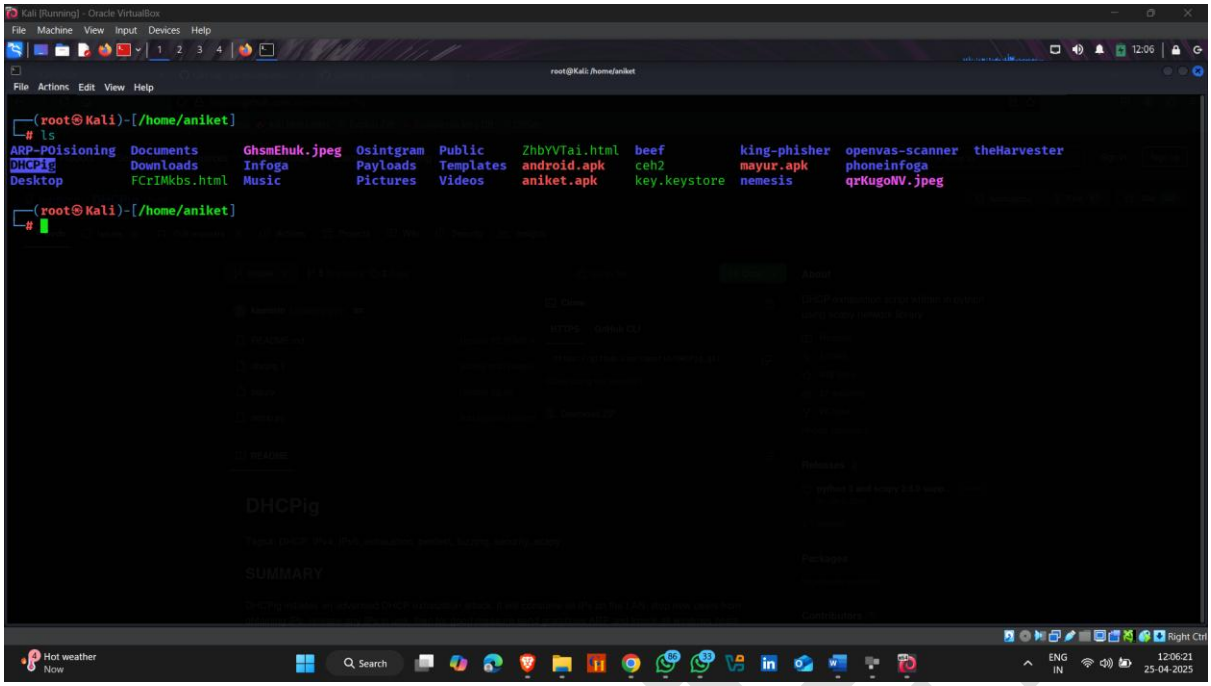
Downlaod link -: https://github.com/kamorin/DHCPig

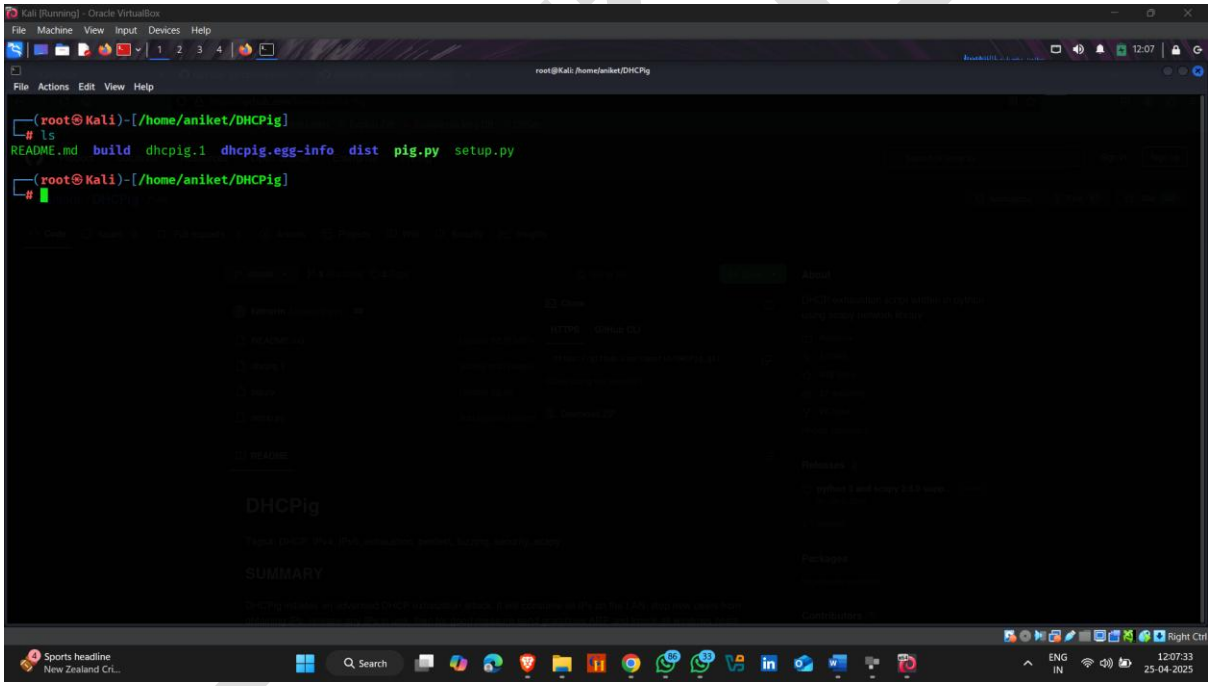


- Now open kali linux terminal and type – git clone and paste link



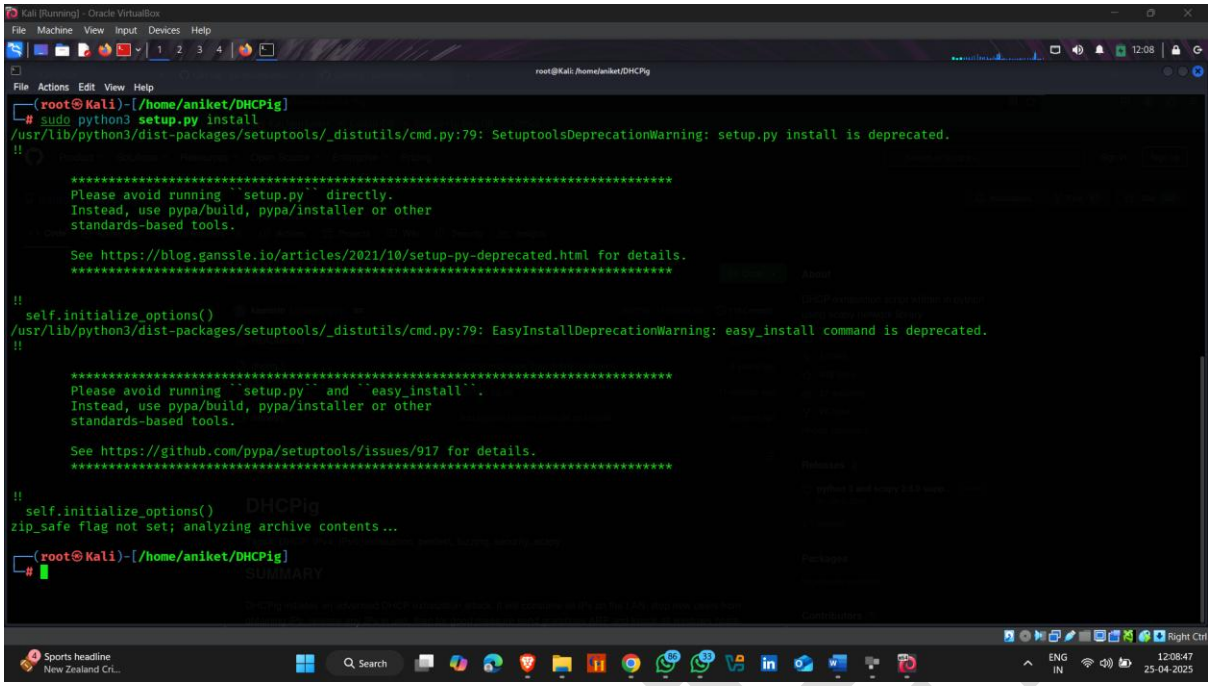
- DHCPig Install successfully
- Now go to DHCPig Directory





- Now use command to install setup file

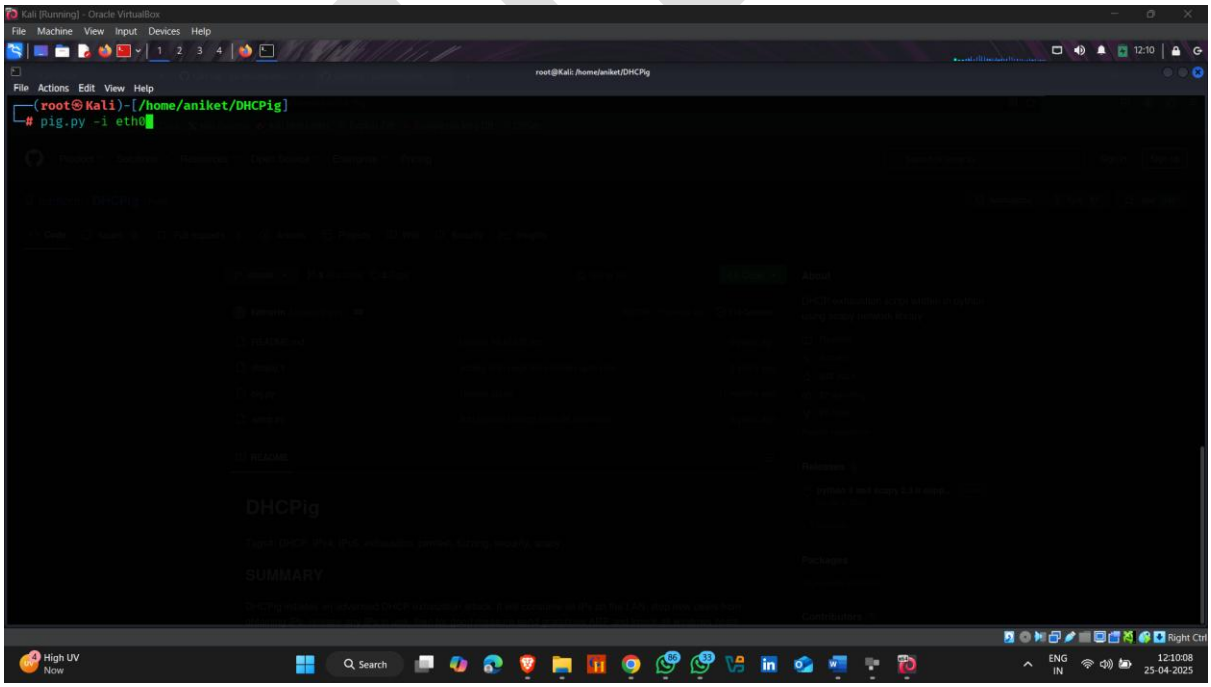
Command – **sudo python3 setup.py install**



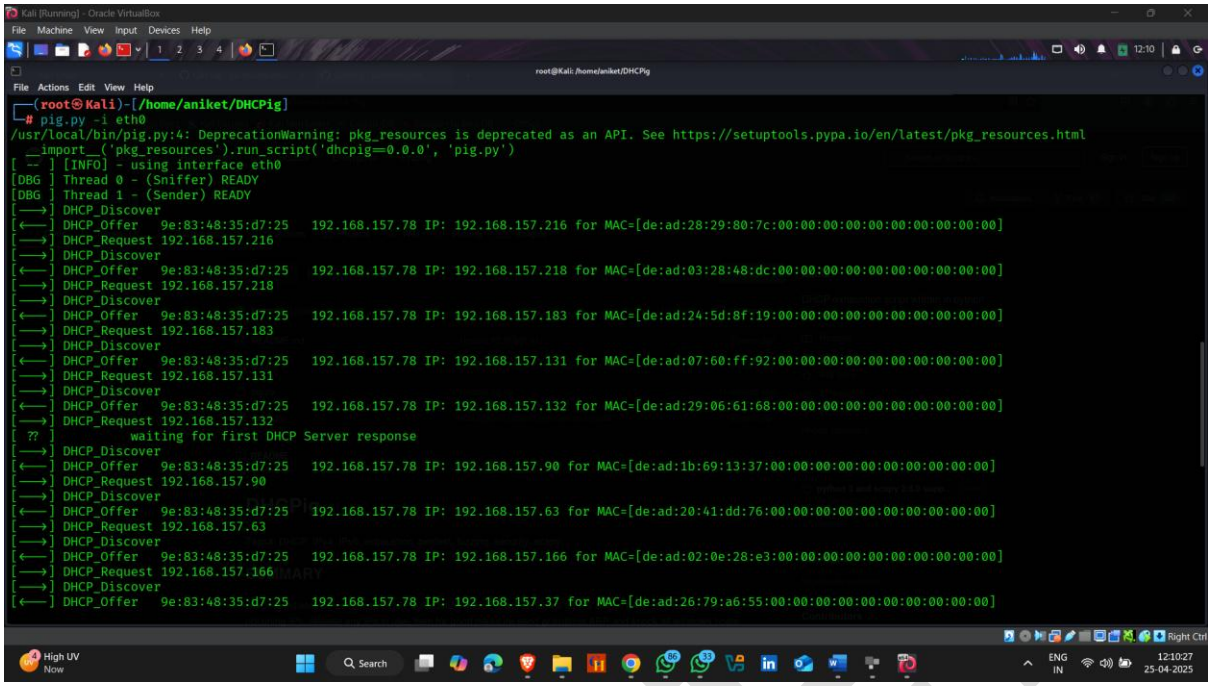
- Now run pig.py file

Command -: **pig.py -I eth0**

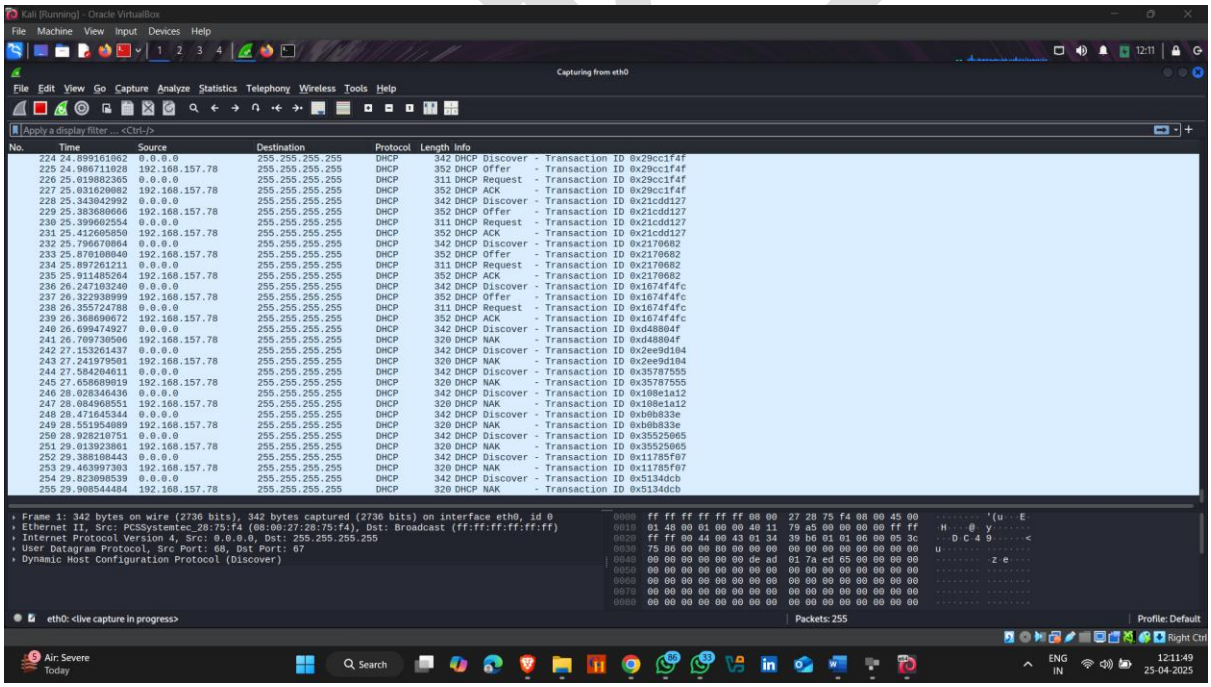
-I – network interface



- Here attack start



- Open wireshark to see DHCP attack are perform or not

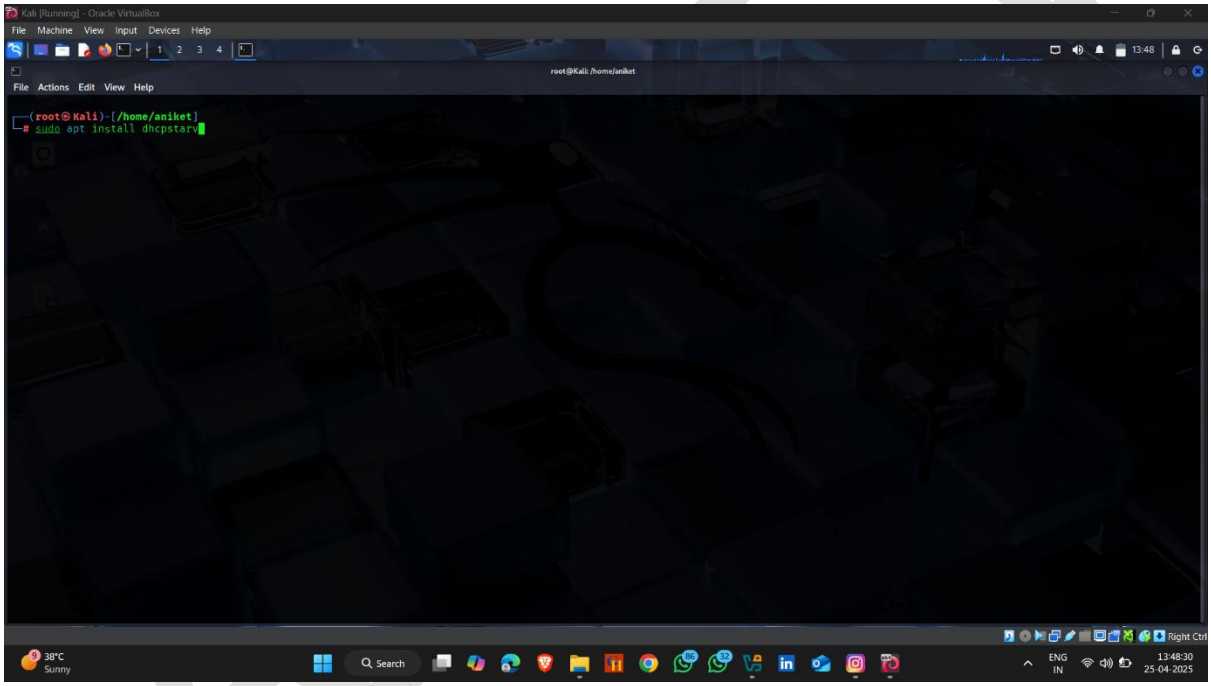


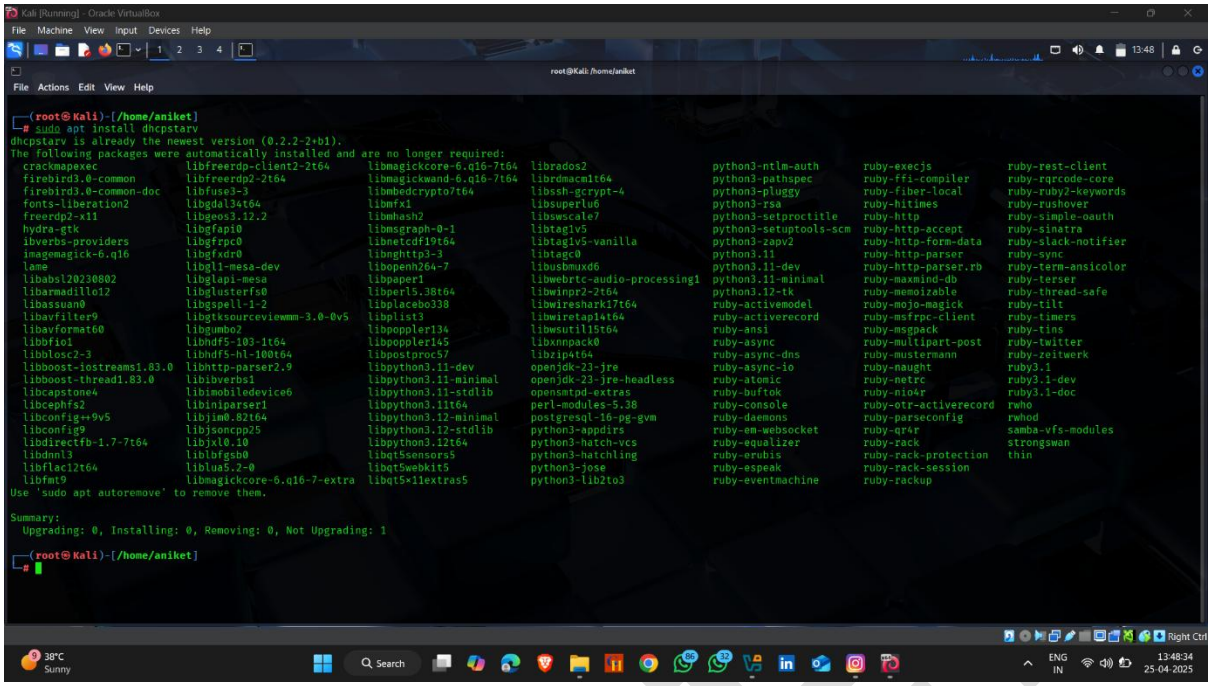
2.Perform DHCP Starvation using DHCPStarv

dhcpstarv floods a network with a large number of **fake DHCP requests**, using **spoofed MAC addresses**. This causes the DHCP server to **exhaust its IP address pool**, making it unable to assign IP addresses to legitimate devices trying to connect.

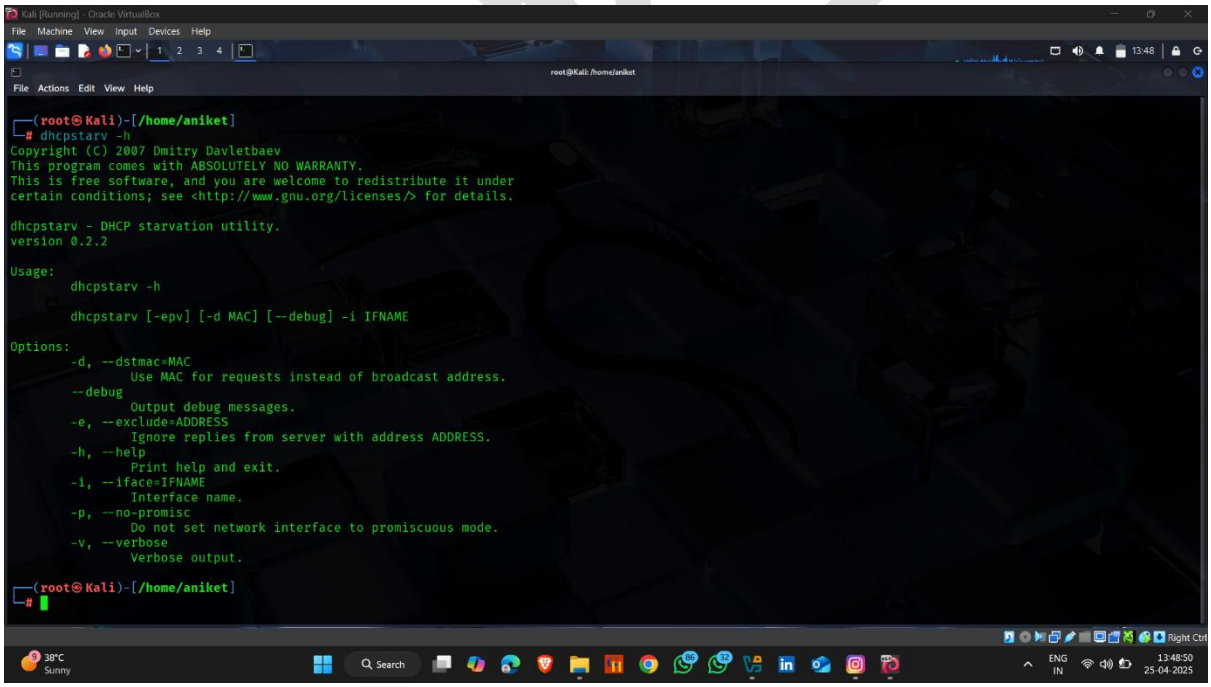
How to use it -:

- Open kali linux terminal and type **sudo apt install dhcpstarv**





- Dhcpstarv -h – getting detailed command



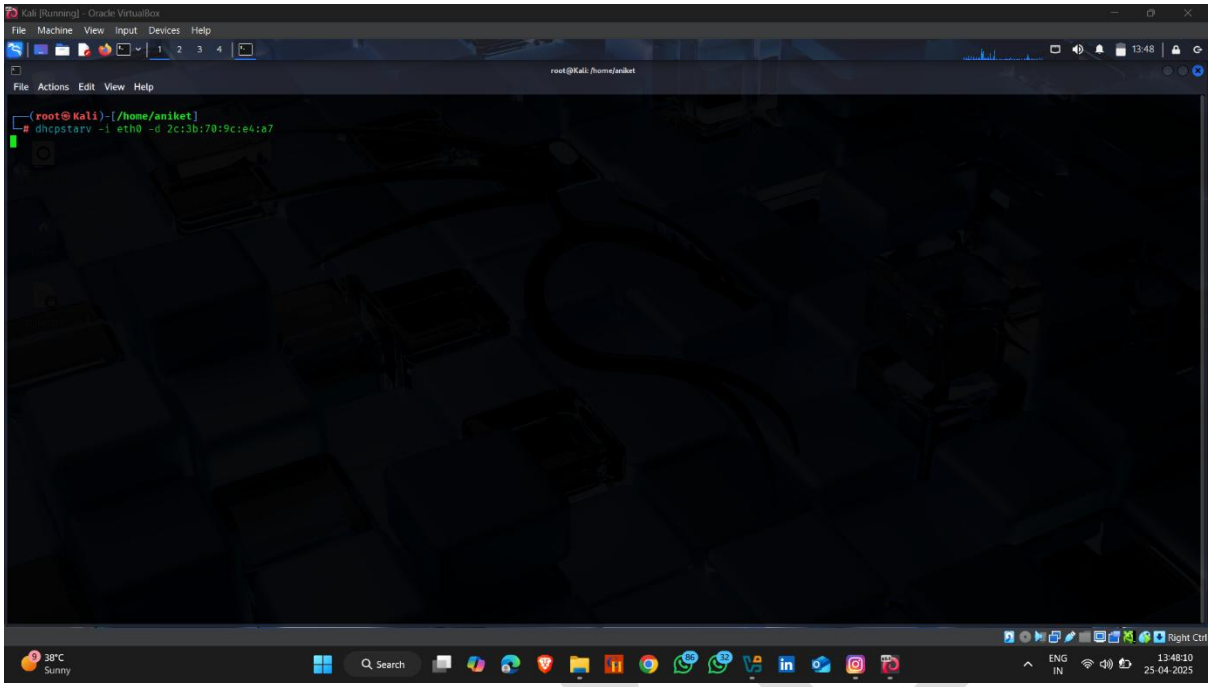
- Perform attack

Command – dhcpstarv -I eth0 -d <target mac address >

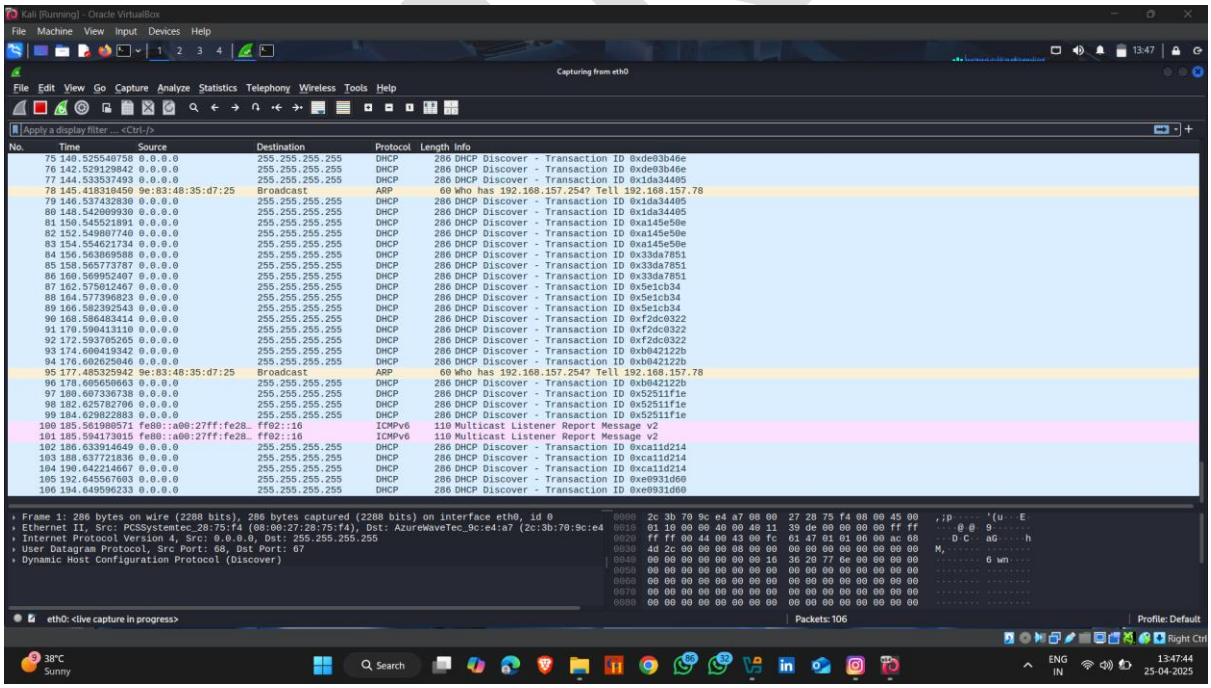
-I – network interface

-d –destination mac address

- **Attack start**



- **Now , open wireshark to see packets are send or not**



MAC SPOOFING

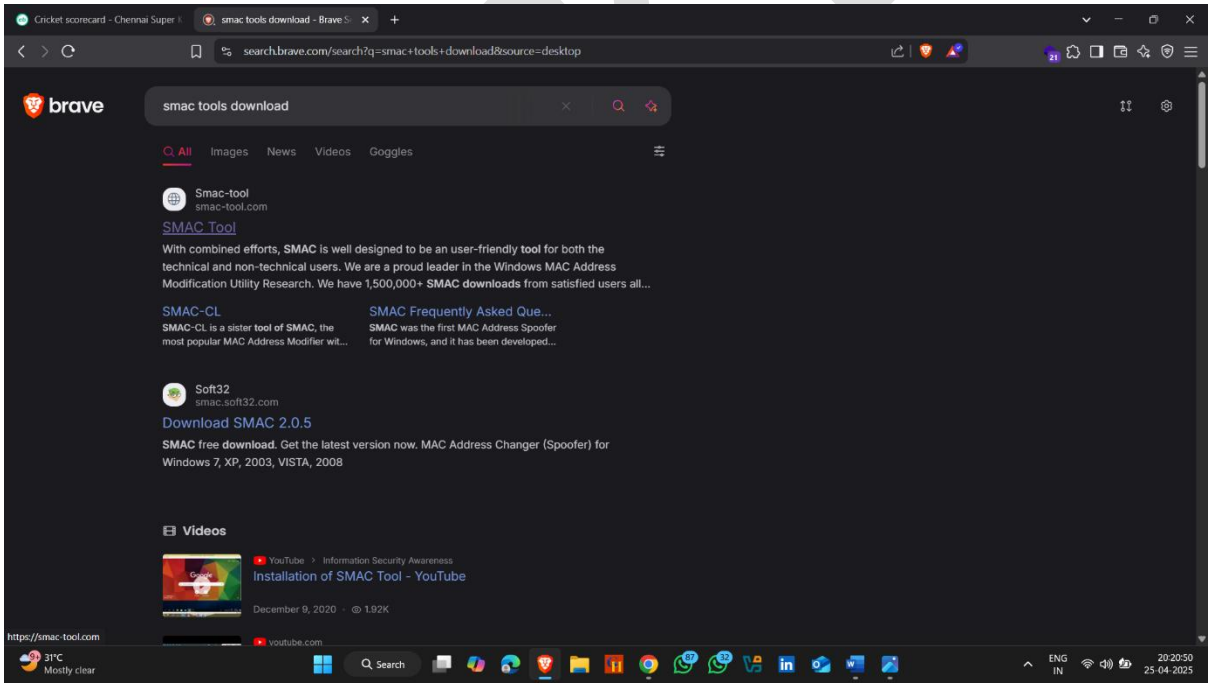
1.Perform mac spoofing using SMAC

The **SMAC MAC Address Changer** is a Windows utility developed by KLC Consulting that allows users to modify the MAC (Media Access Control) address

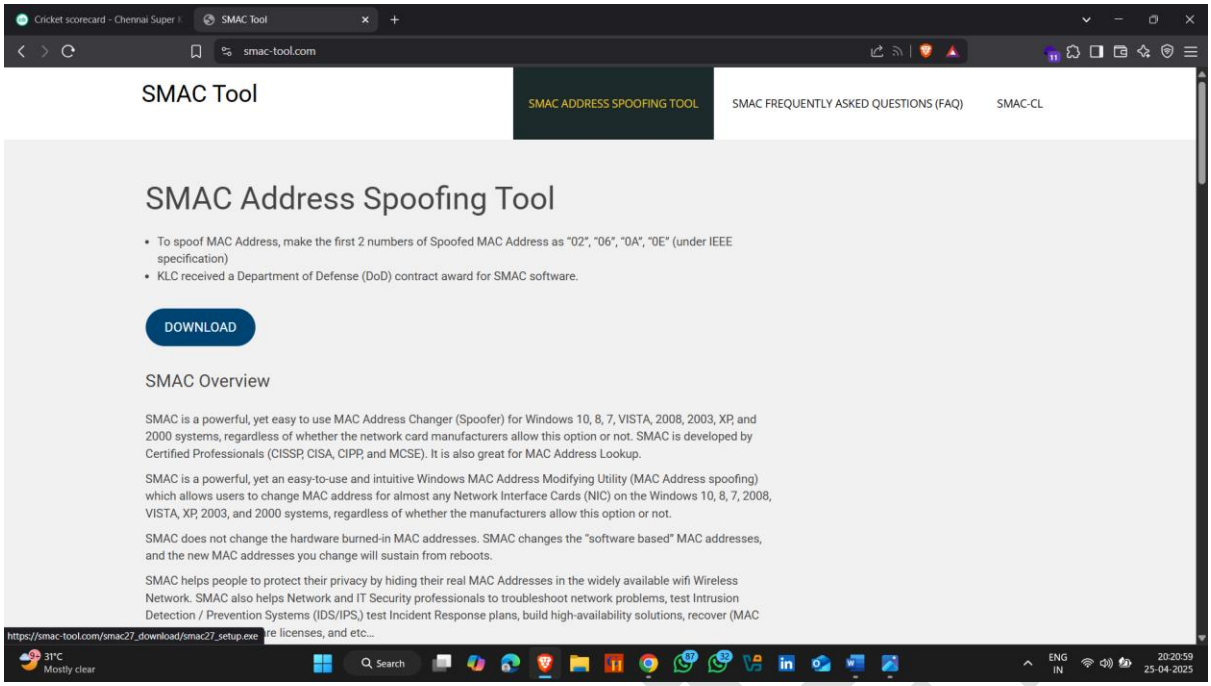
How to install it -:

- **Open a browser and search SMAC tool Download and click on first website**

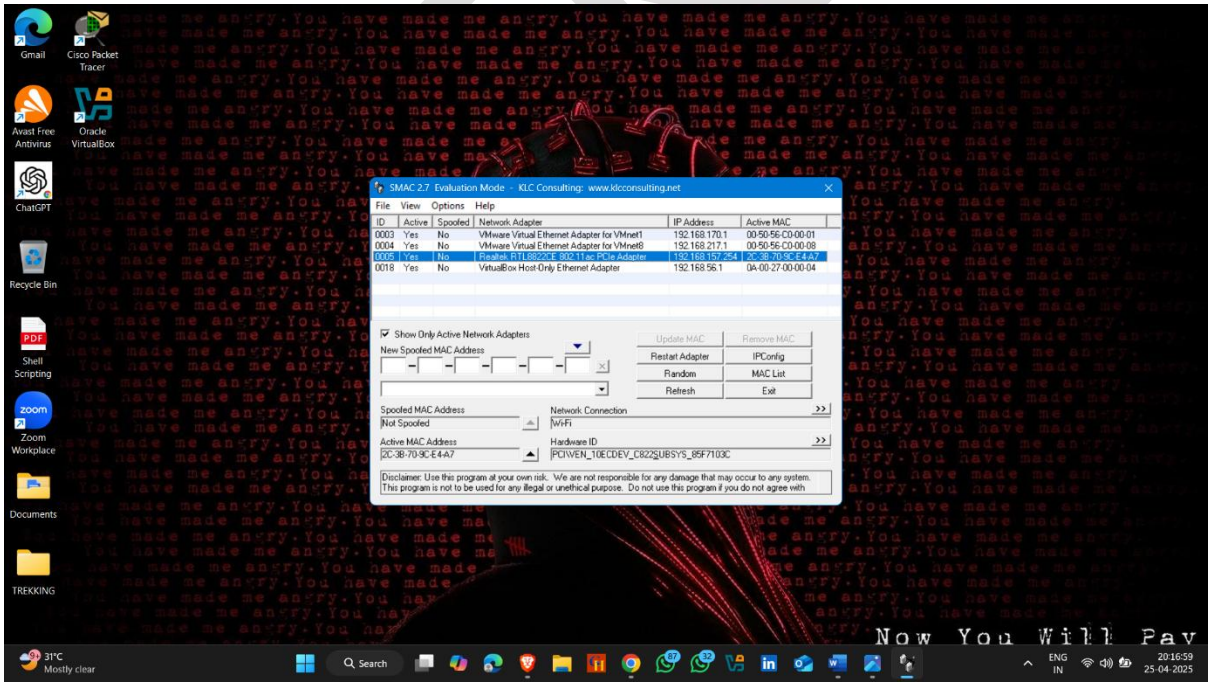
Download Link -: https://smac-tool.com/



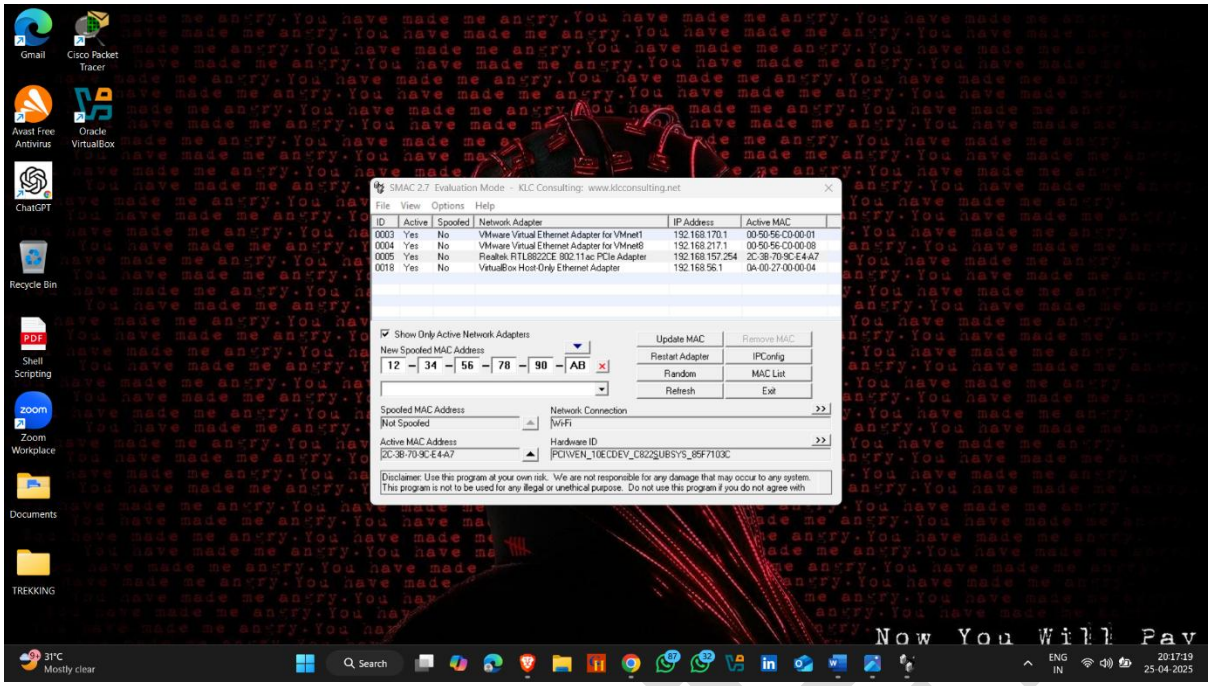
- **Click on Download**
- **Download will started**



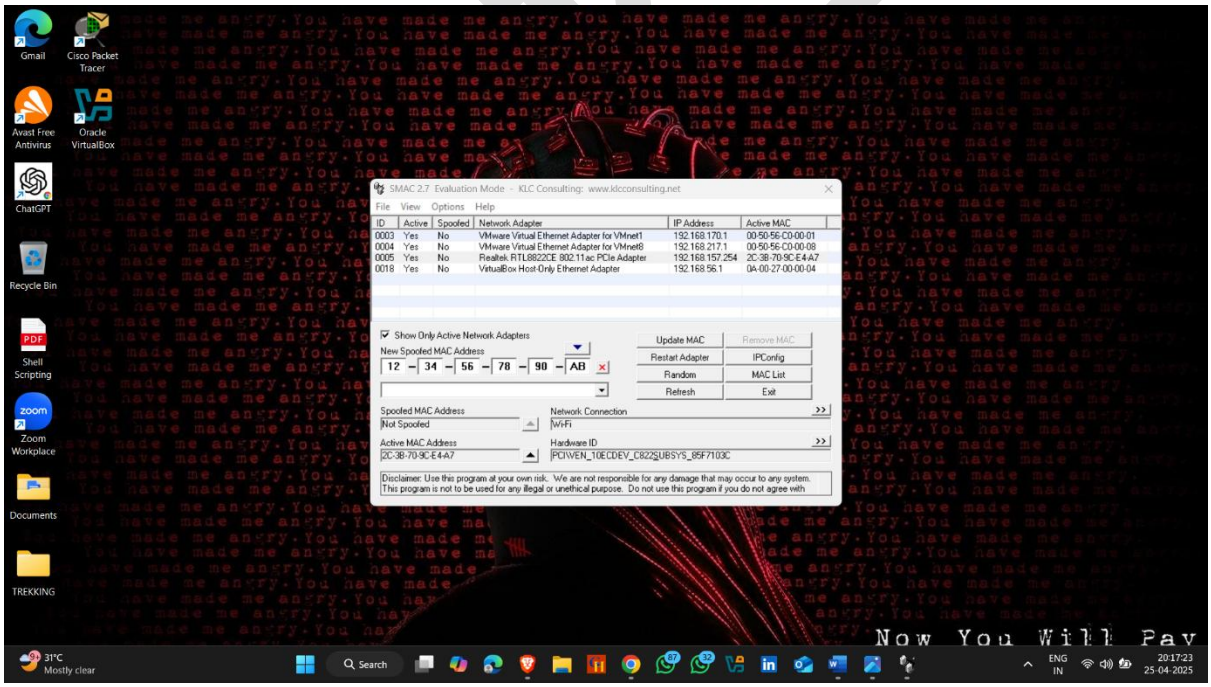
- **After installation open app**
- **Select network device**



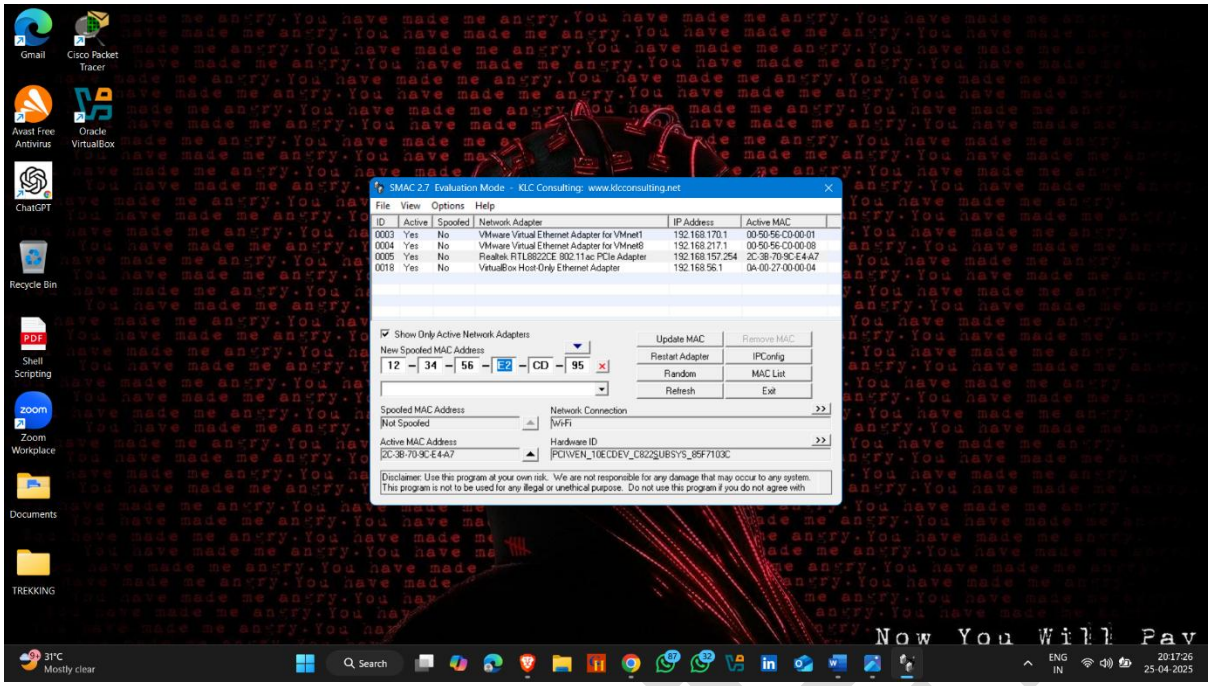
- **Enter manually MAC address**

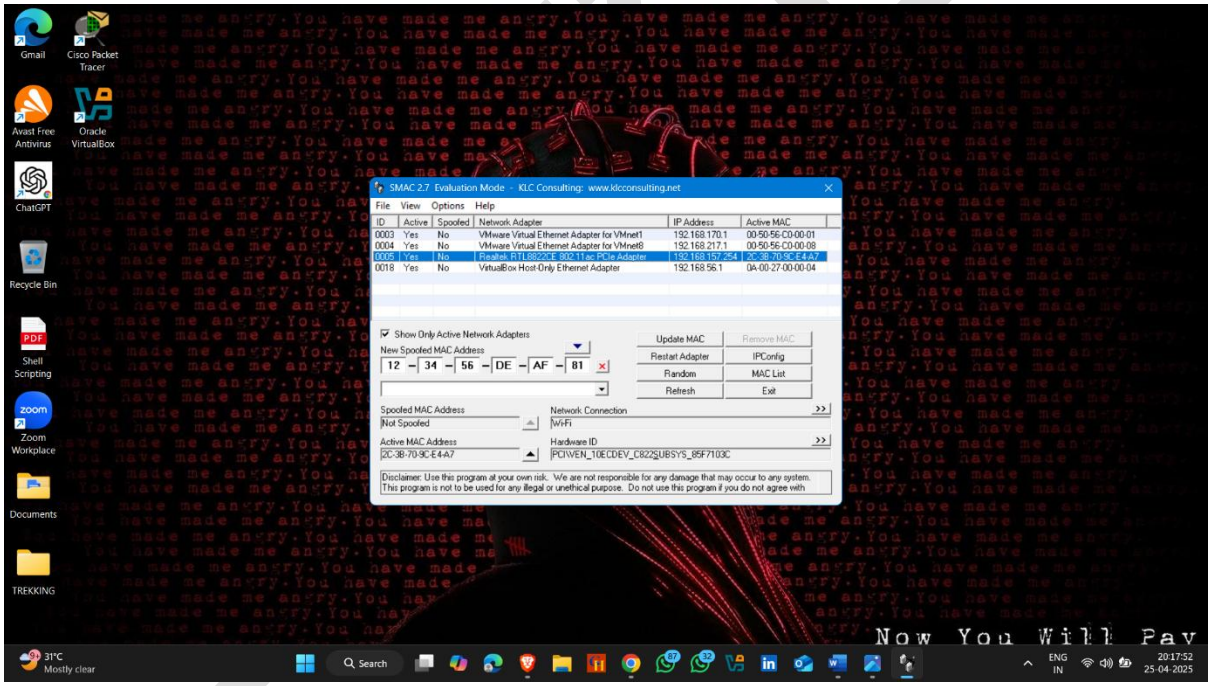


- **Now click Random to generate random**



- **Random MAC Generate successfully**


SMAC 2.7 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File View Options Help
ID Active Spoofed Network Adapter IP Address Active MAC
0003 Yes No VMware Virtual Ethernet Adapter for VMnet1 192.168.170.1 00-50-56-C0-00-01
0004 Yes No VMware Virtual Ethernet Adapter for VMnet8 192.168.217.1 00-50-56-C0-00-08
0005 Yes No Realtek RTL8822CE 802.11ac PCIe Adapter 192.168.157.254 2C-3B-70-9C-E4-A7
0018 Yes No VirtualBox Host-Only Ethernet Adapter 192.168.56.1 0A-00-27-00-00-04
Show Only Active Network Adapters
New Spoofed MAC Address
12 - 34 - 56 - E2 - CD - 95
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
Spoofed MAC Address
Not Spoofed
Network Connection
Wi-Fi
Active MAC Address
2C-3B-70-9C-E4-A7
Hardware ID
PCI\VEN_10EC&DEV_C822&SUBSYS_85F7103C
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system.
This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with
Now You Will Pay


SMAC 2.7 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File View Options Help
ID Active Spoofed Network Adapter IP Address Active MAC
0003 Yes No VMware Virtual Ethernet Adapter for VMnet1 192.168.170.1 00-50-56-C0-00-01
0004 Yes No VMware Virtual Ethernet Adapter for VMnet8 192.168.217.1 00-50-56-C0-00-08
0005 Yes No Realtek RTL8822CE 802.11ac PCIe Adapter 192.168.157.254 2C-3B-70-9C-E4-A7
0018 Yes No VirtualBox Host-Only Ethernet Adapter 192.168.56.1 0A-00-27-00-00-04
Show Only Active Network Adapters
New Spoofed MAC Address
12 - 34 - 56 - DE - AF - 81
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
Spoofed MAC Address
Not Spoofed
Network Connection
Wi-Fi
Active MAC Address
2C-3B-70-9C-E4-A7
Hardware ID
PCI\VEN_10EC&DEV_C822&SUBSYS_85F7103C
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system.
This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with
Now You Will Pay

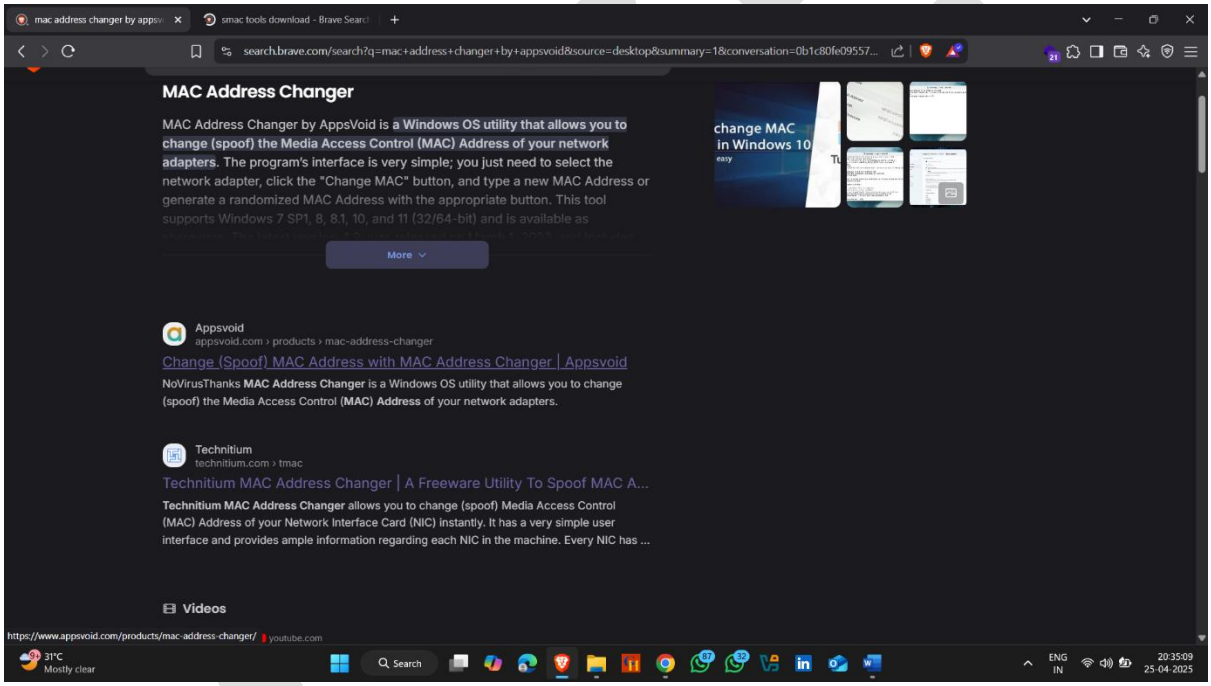
2.Perform mac spoofing using MAC Address Changer.

A **MAC address changer** application is a software tool that lets you change the **MAC (Media Access Control) address** of your computer's

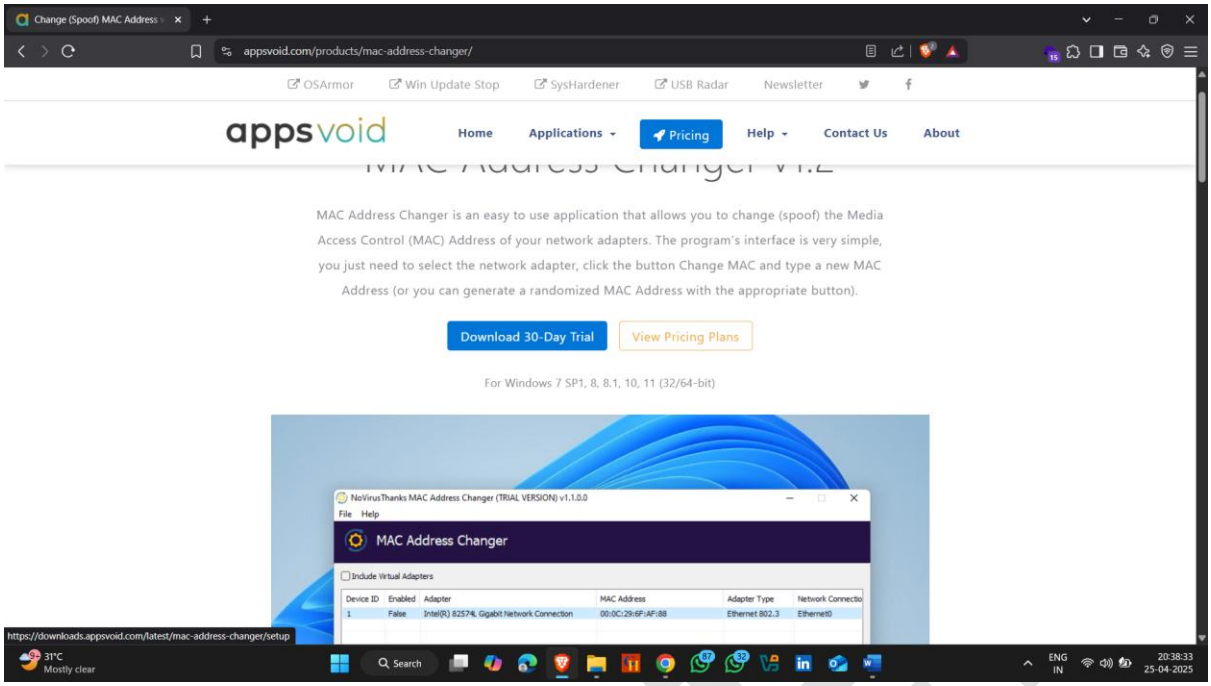
How to install it -:

- **Open browser and search mac address changer**
- **Open appvoid website**

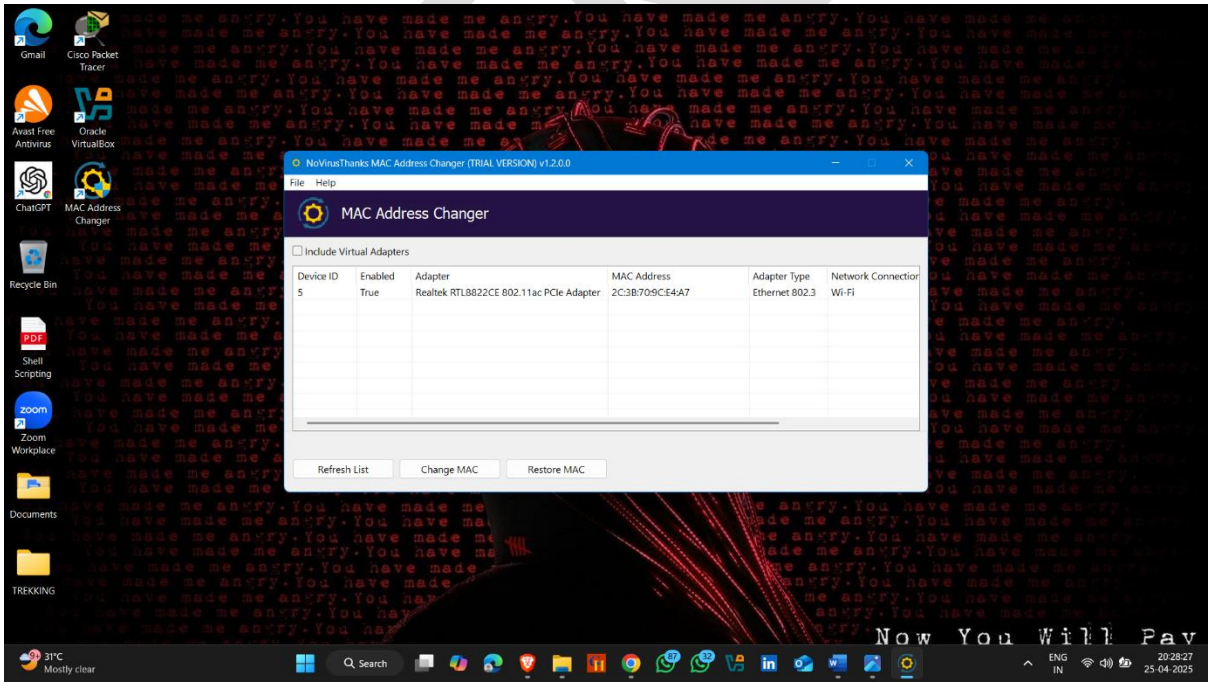
Download Link -:https://www.appsvoid.com/products/mac-address-changer/



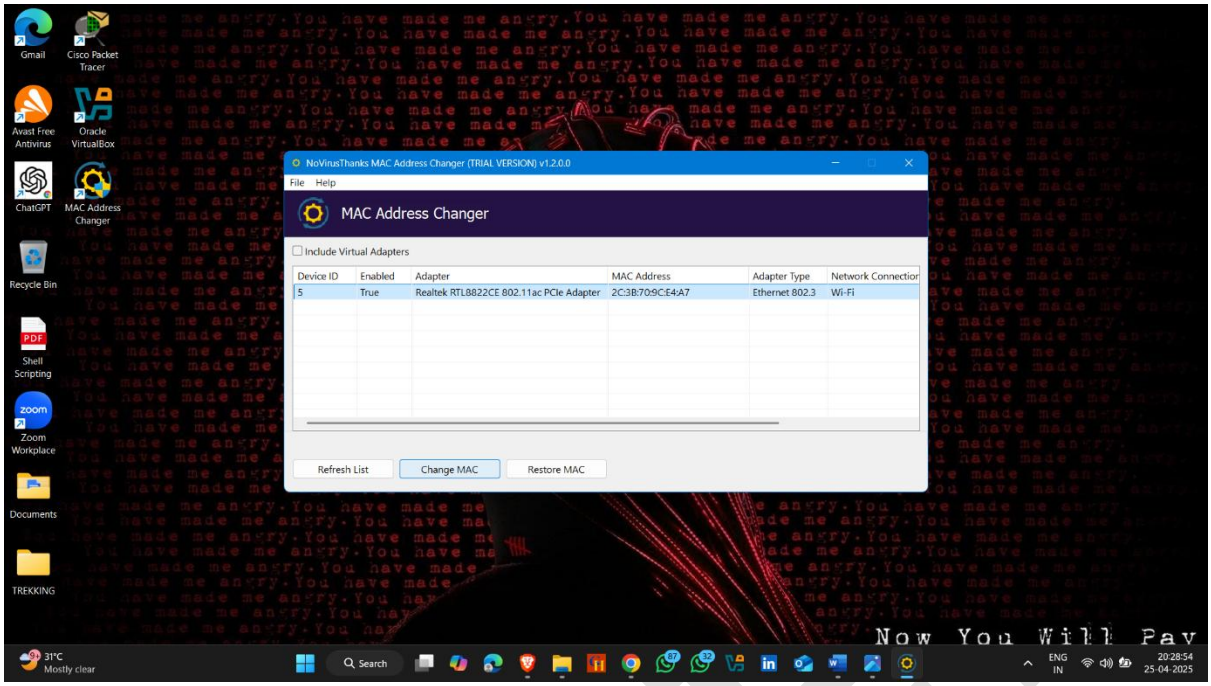
- **Click on Download 30-Day Trial**

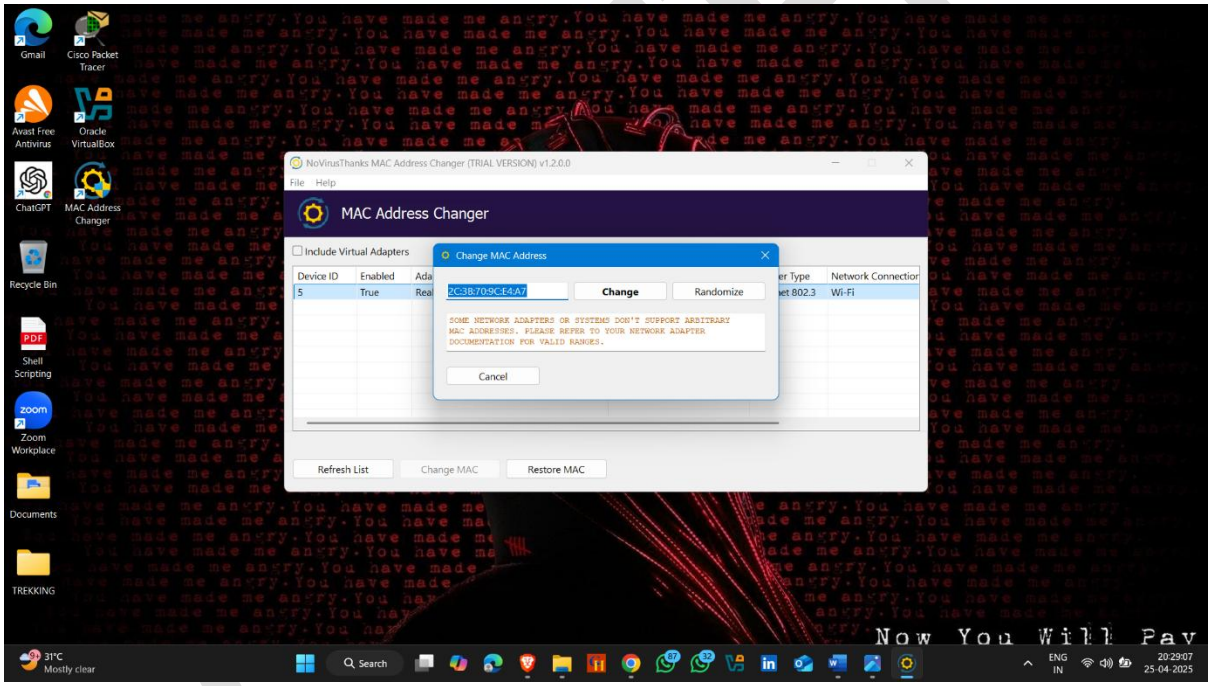


- **After installation , open application**
- **Select interface**

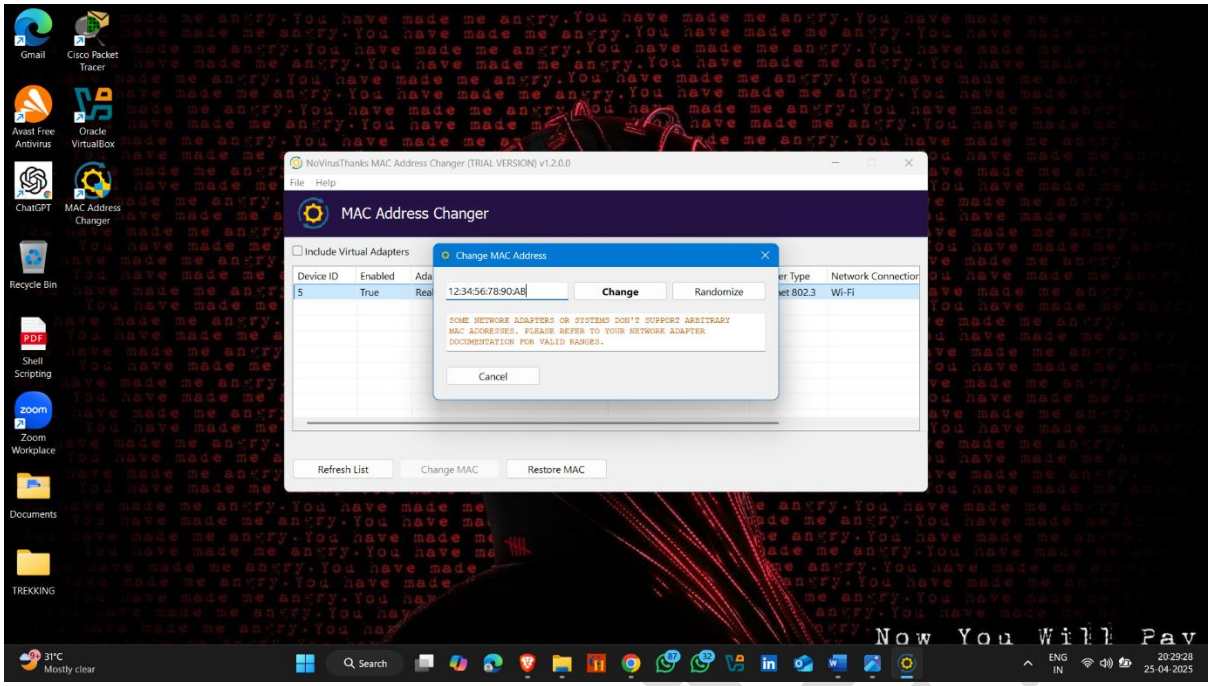


- **Click on Change MAC**

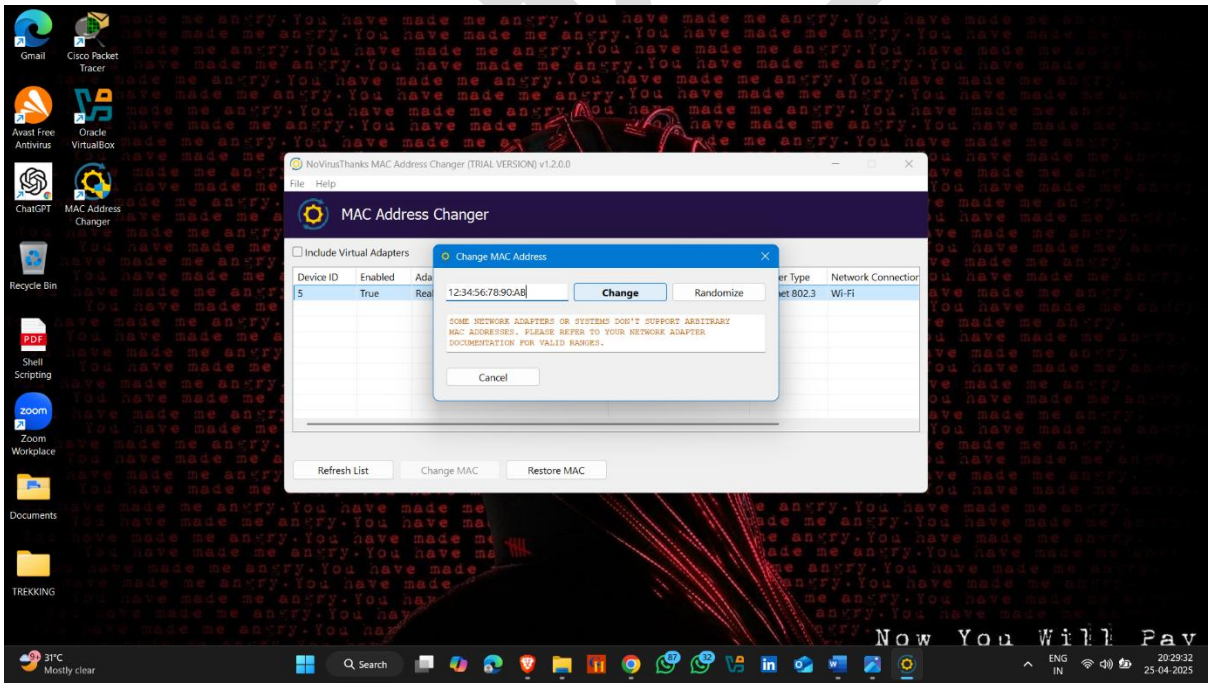




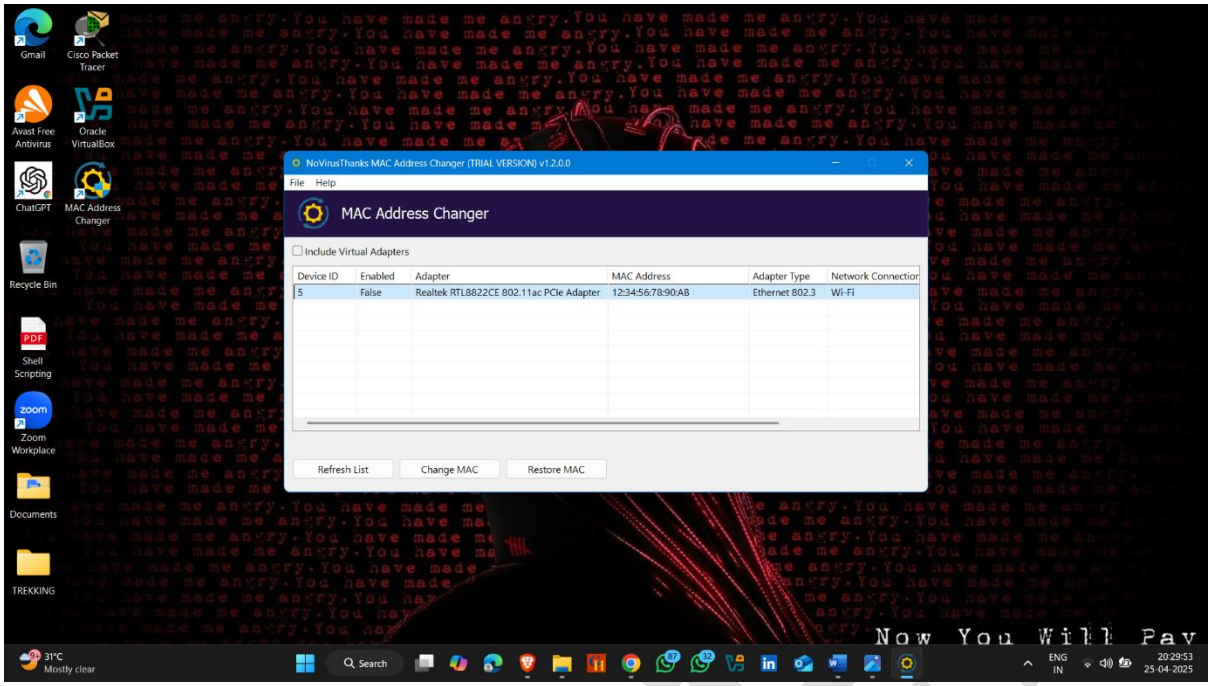
- **Create manually MAC address**



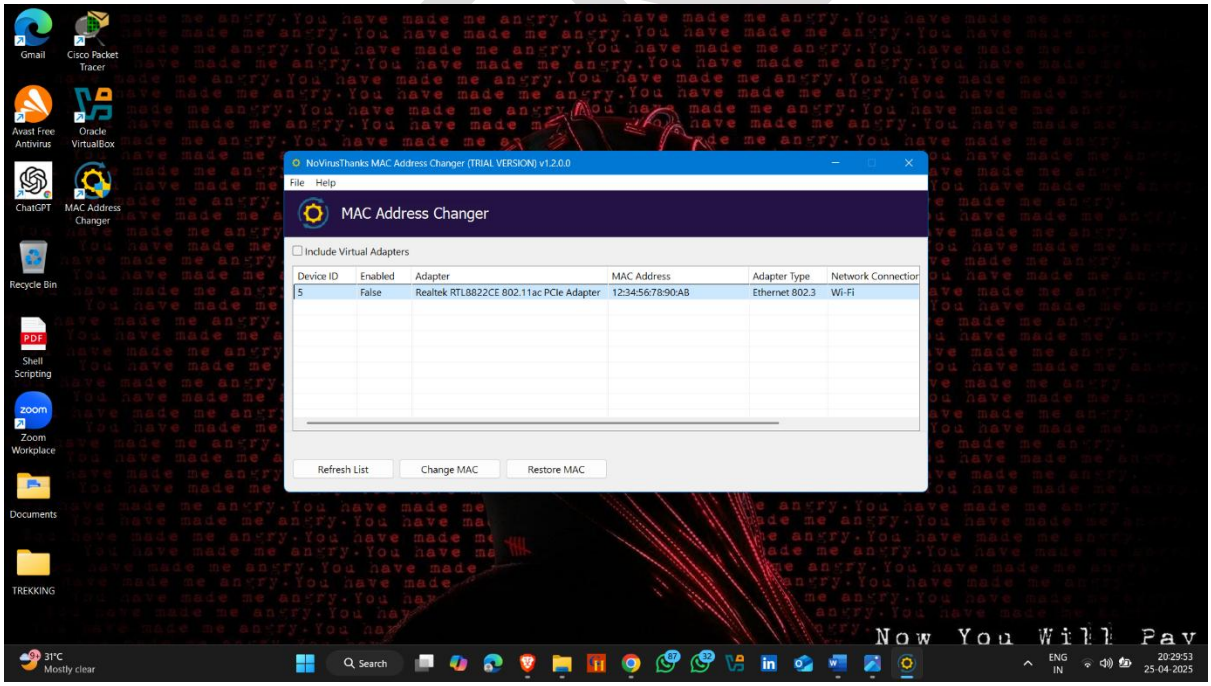
- **Click on Change**



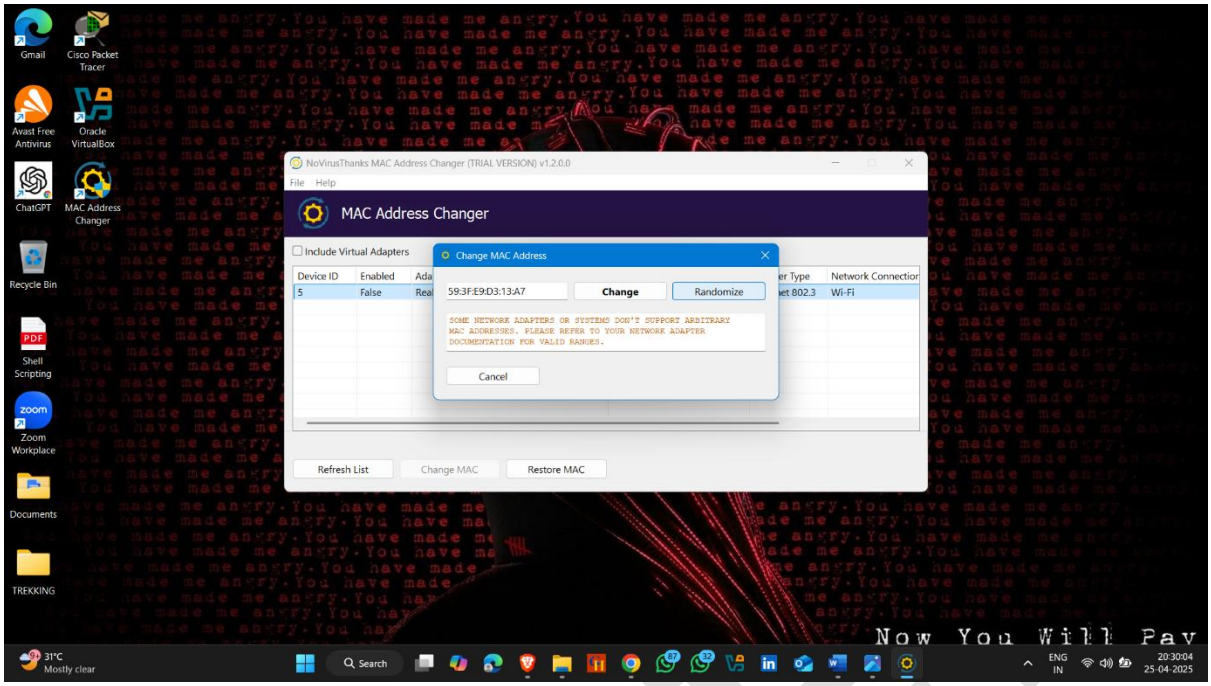
- **Random MAC Genarate successfully**



- **Generate Random MAC Address**
- **Click on Change MAC**



- **Click on Randomize**
- **Click on change**


Gmail
Cisco Packet Tracer
Avast Free Antivirus
Oracle VirtualBox
ChatGPT
MAC Address Changer
Recycle Bin
Shell Scripting
Zoom Workplace
Documents
TREKKING
NoVirusThanks MAC Address Changer (TRIAL VERSION) v1.2.0.0
File Help
MAC Address Changer
Include Virtual Adapters
Device ID
Enabled
Network Connection
5
False
Wi-Fi
Change MAC Address
59:3F:E9:D3:13:A7
Change
Randomize
SOME NETWORK ADAPTERS OR SYSTEMS DON'T SUPPORT ARBITRARY MAC ADDRESSES. PLEASE REFER TO YOUR NETWORK ADAPTER DOCUMENTATION FOR VALID RANGES.
Cancel
Refresh List
Change MAC
Restore MAC
Now You Will Pay
31°C
Mostly clear
Search
ENG
IN
20:30:04
25-04-2025

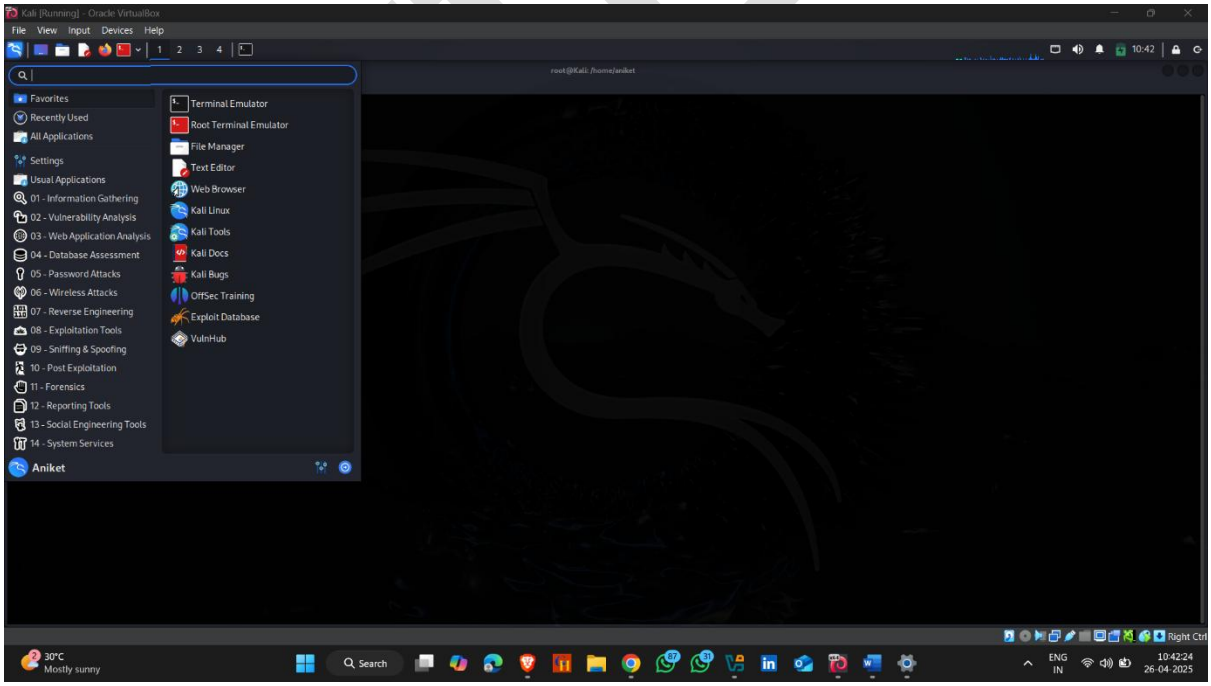
ARP POISONING

1.Perform ARP Poisoning Using Ettercap

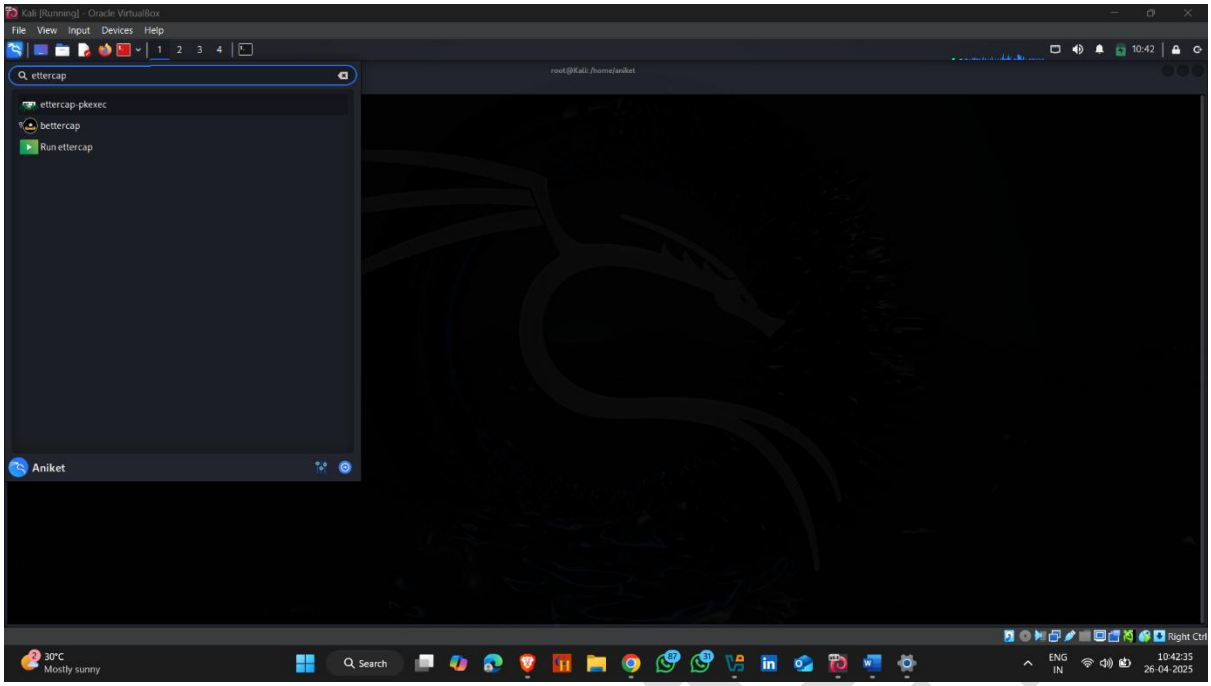
Ettercap is a powerful and classic **network security tool** used for **Man-in-the-Middle (MITM) attacks**, **packet sniffing**, and **network protocol analysis**

How to use it -:

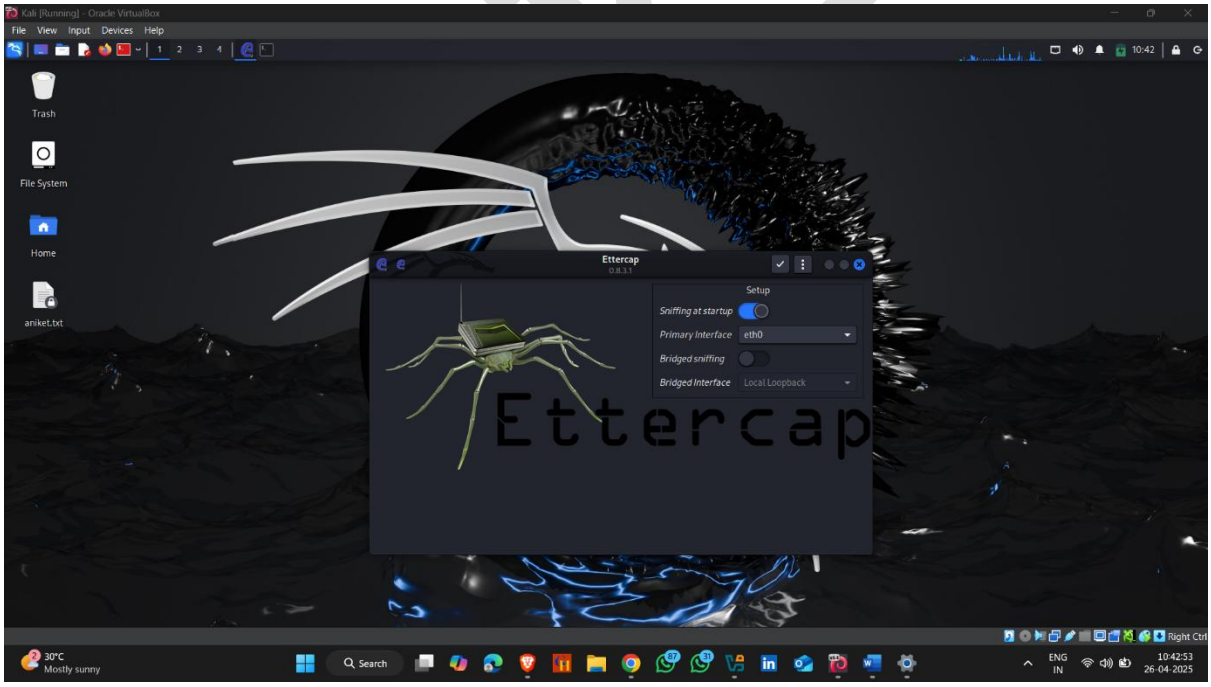
- Open Kali linux and go to Applications section



- Search Ettercap and open it



- Click on ✅ this icon

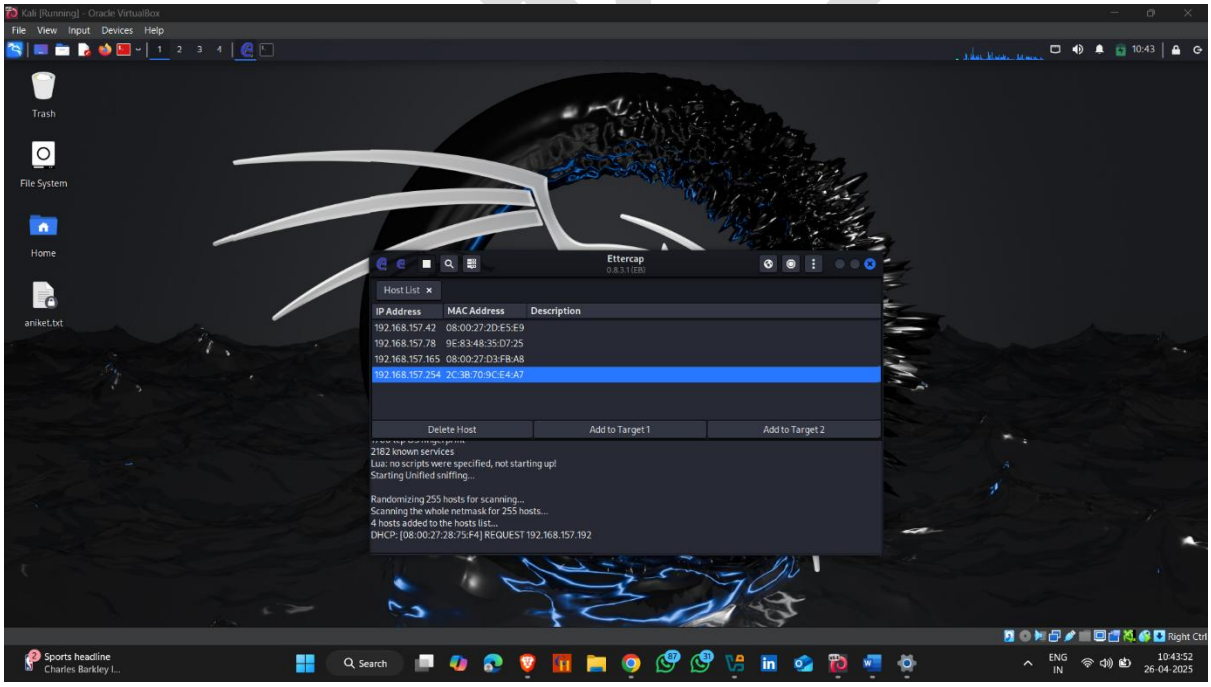


- Now click on Tree dots “ :” and click on Hosts

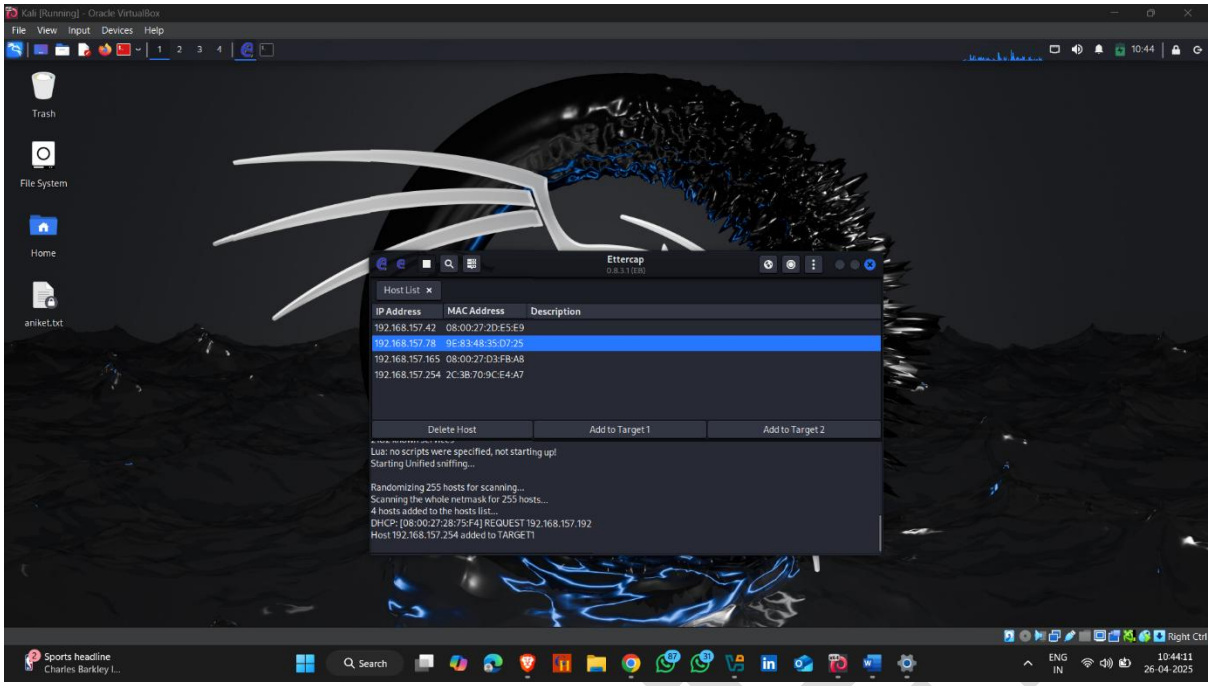
- Click on **Scan for Hosts**

- After Scan completed click on **Host List**

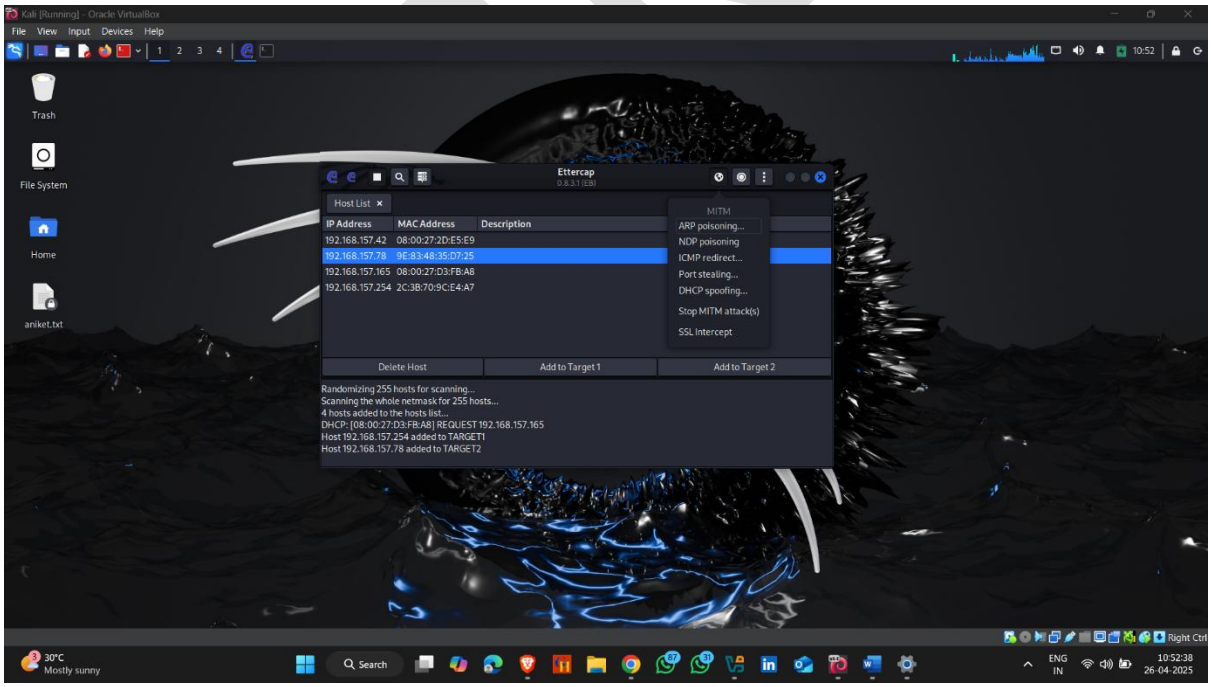
- Now click on your target ip and add it on **"Add to Target 1"**



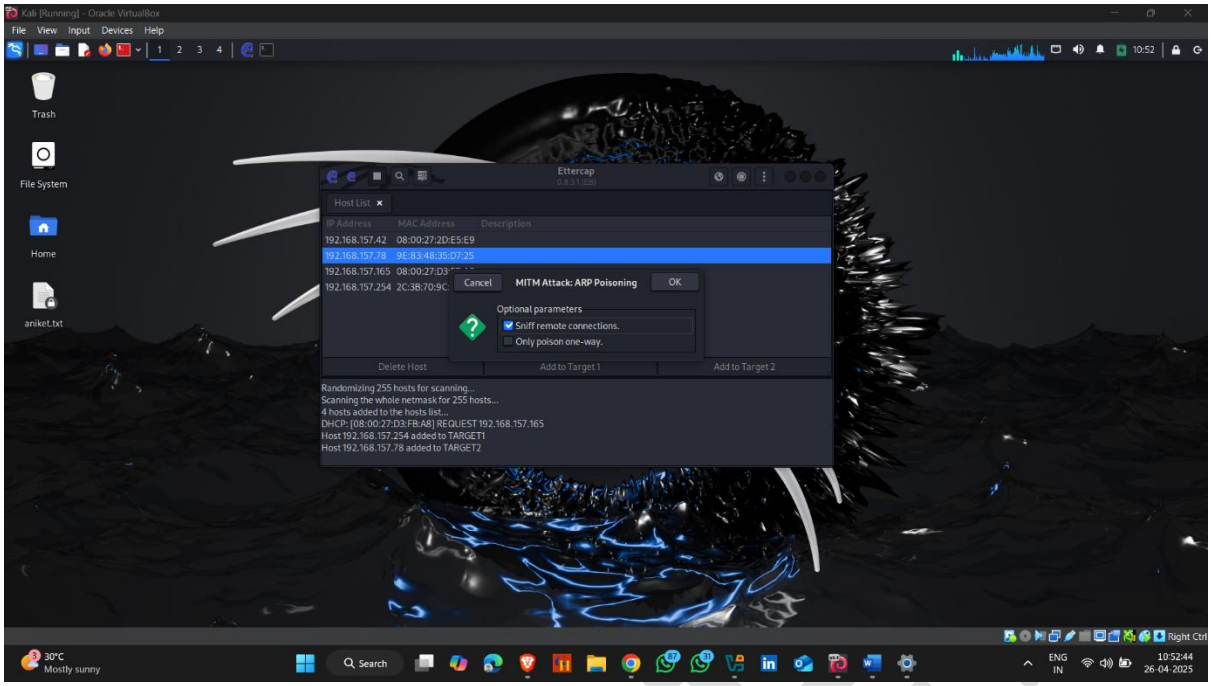
- Select your gateway ip address and add it on **"Add on Target 2"**



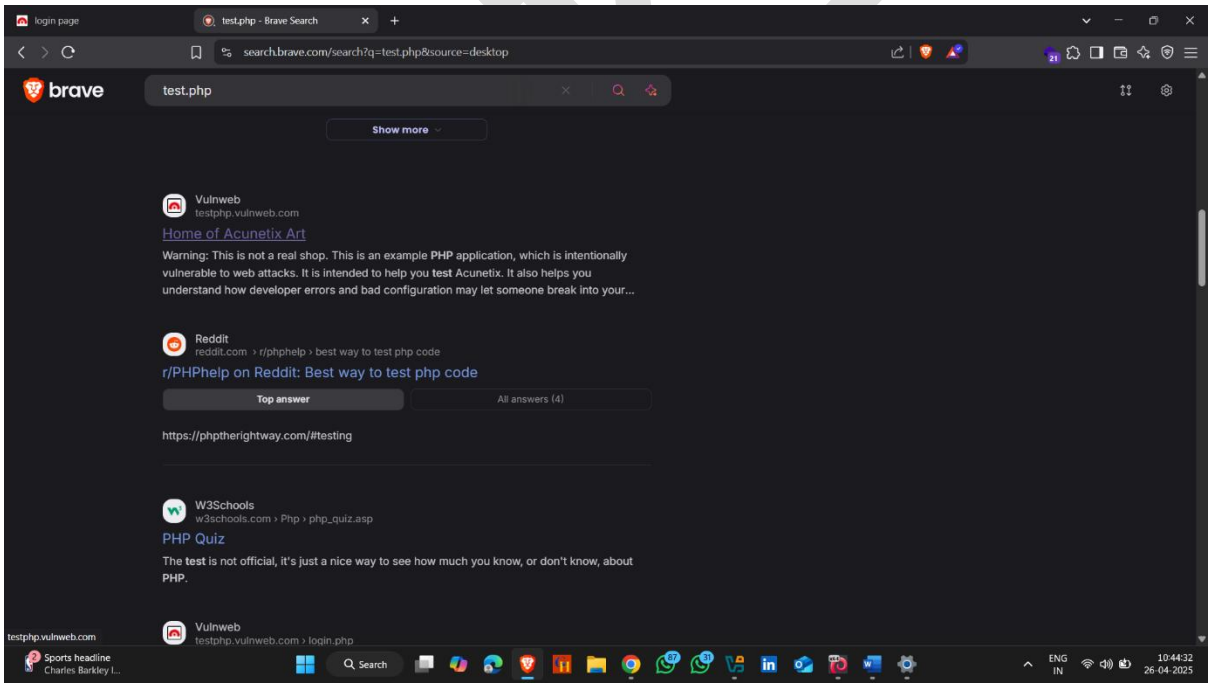
- Now click on **MITM menu** and then click on **ARP Poisoning**

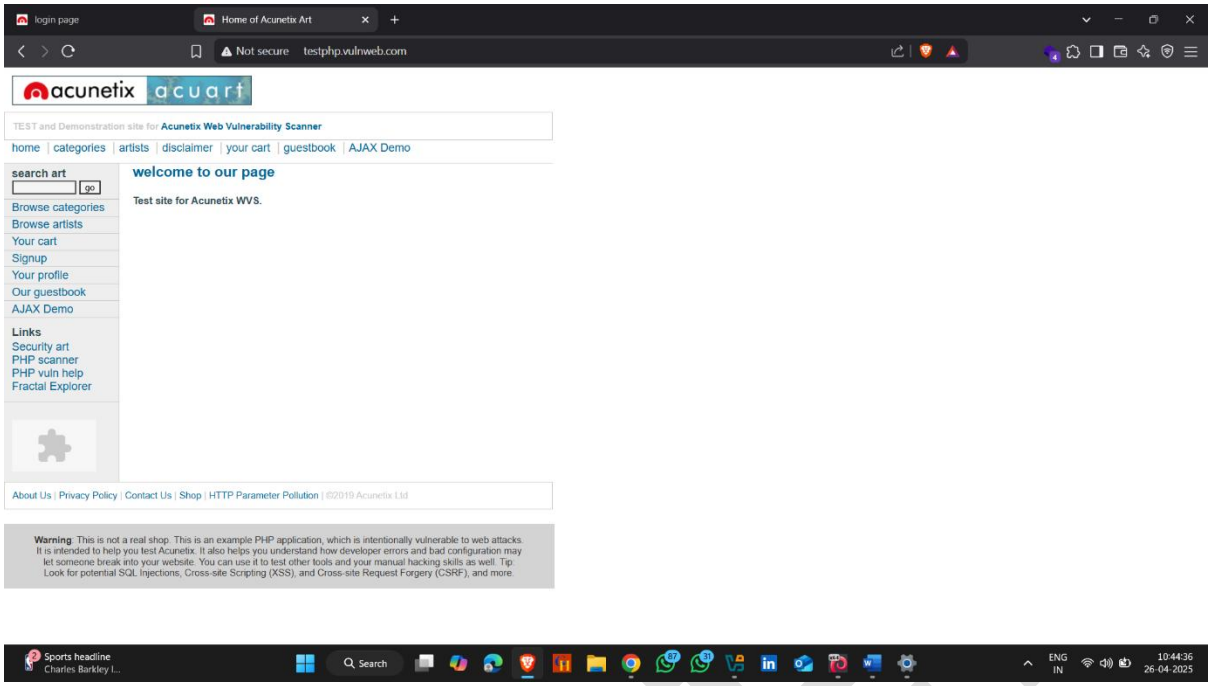


- Click on ok

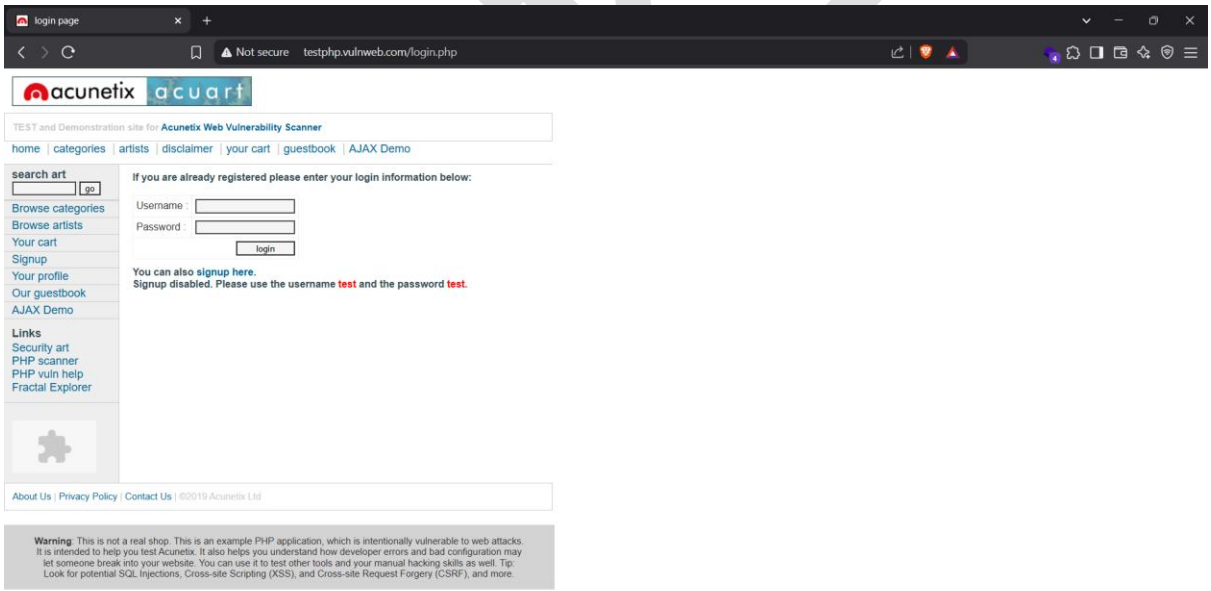


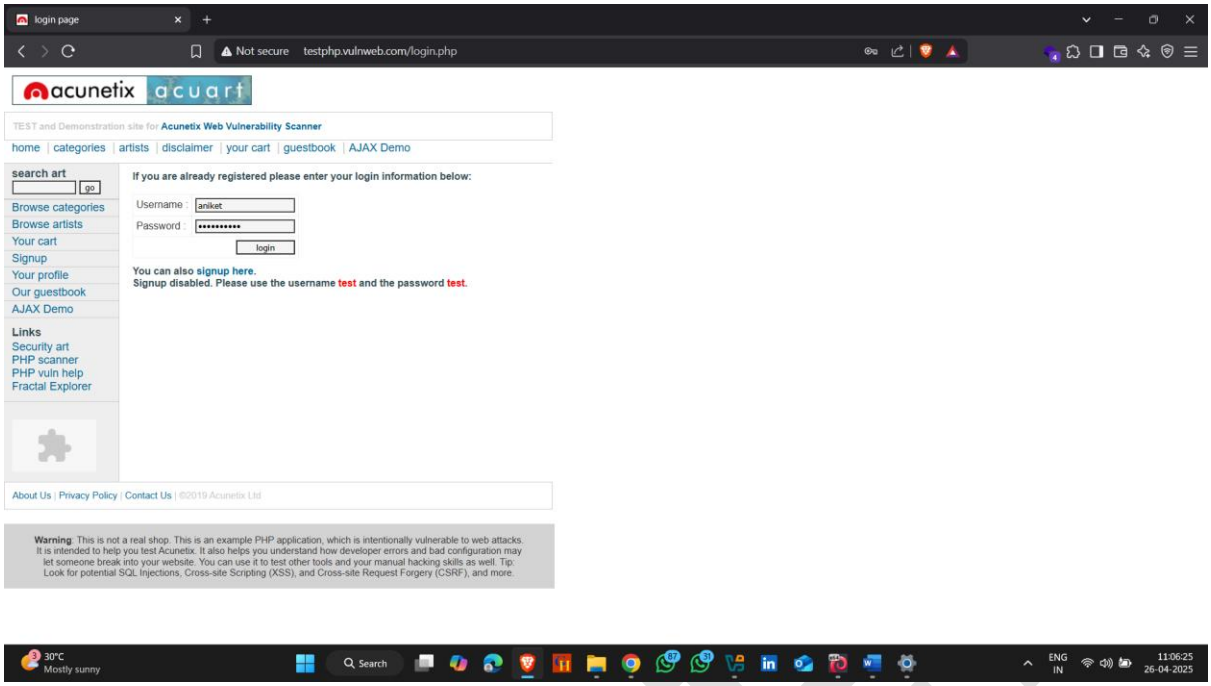
- Now go to target machine and open browser



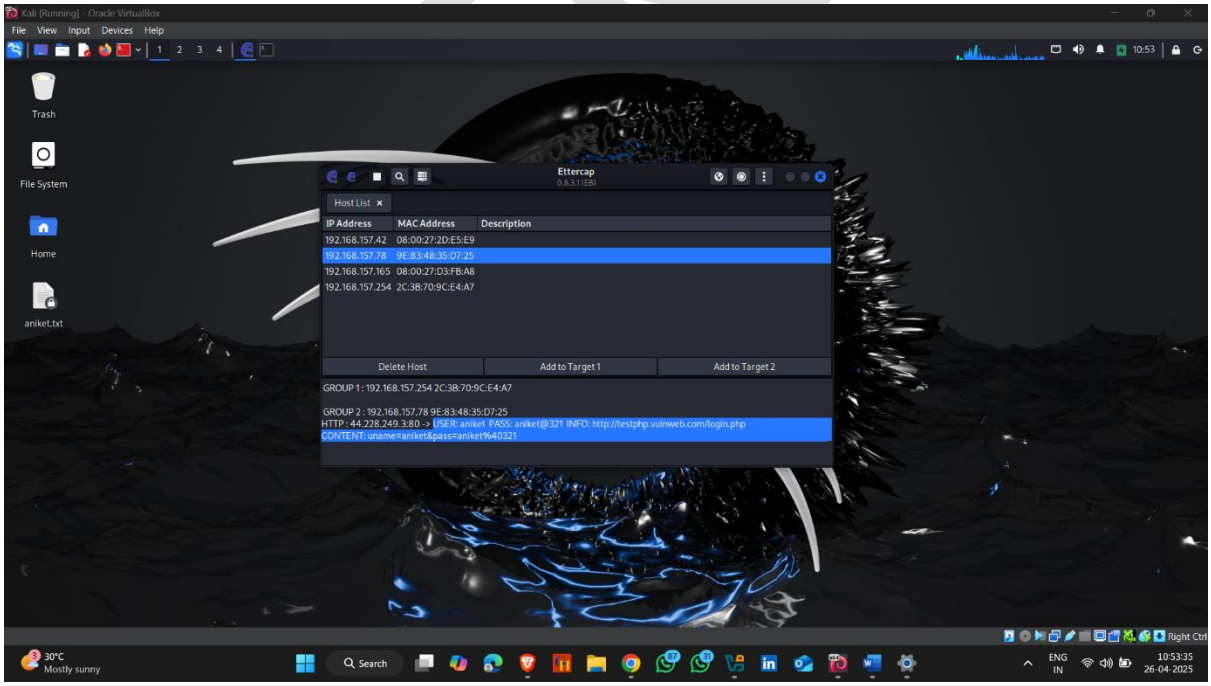


- Enter Credentials here





- Back to the Ettercap
- Here , Ettercap capture the username and password

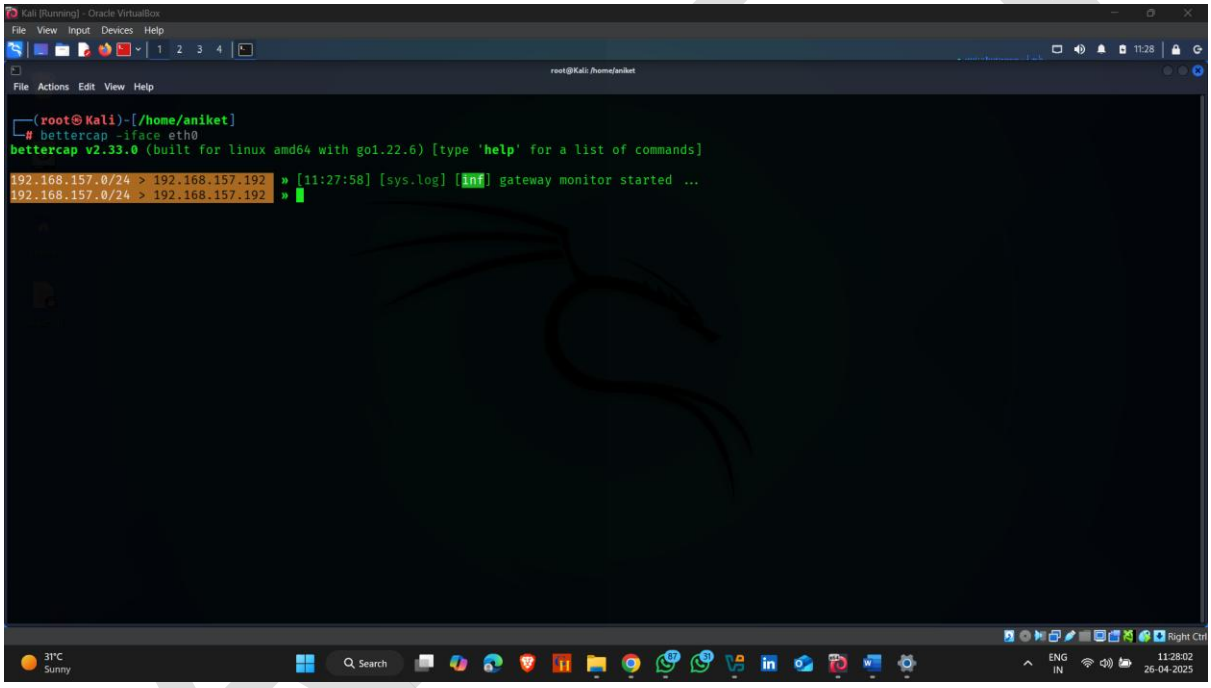


2.Perform ARP Poisoning Using Bettercap

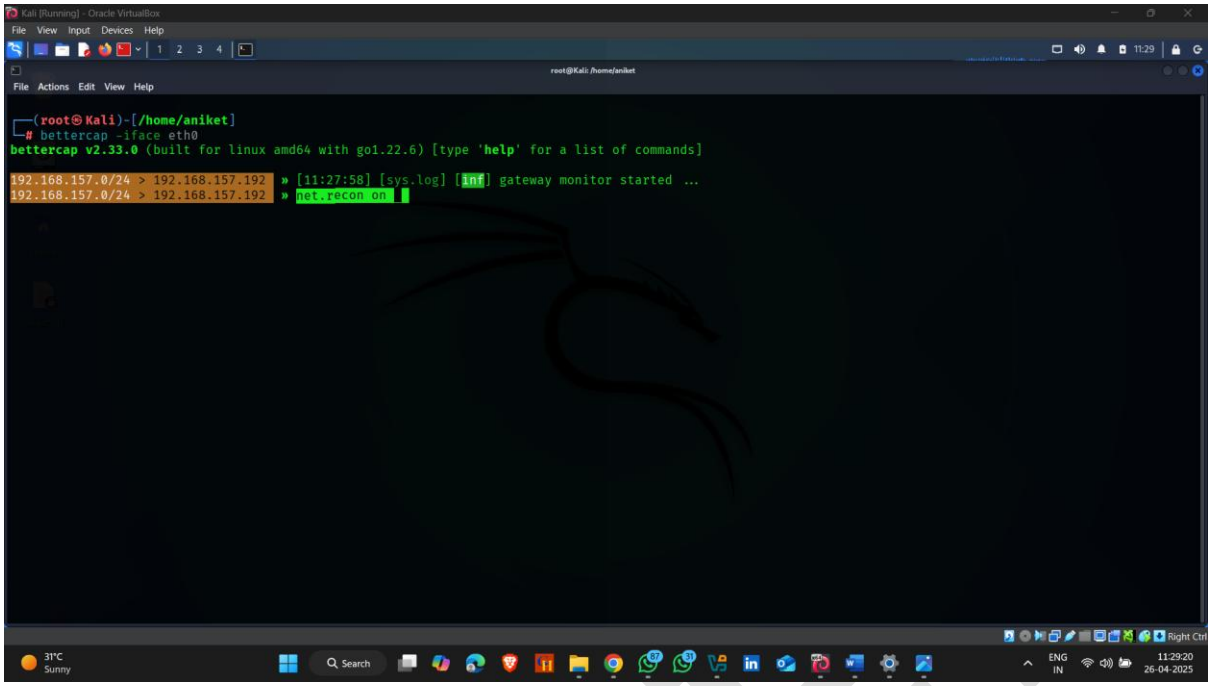
Bettercap is a **modern, powerful, and flexible tool** designed for **MITM attacks**, **network sniffing**, **traffic manipulation**, **credential harvesting**, and **network protocol analysis**.

How to use it - :

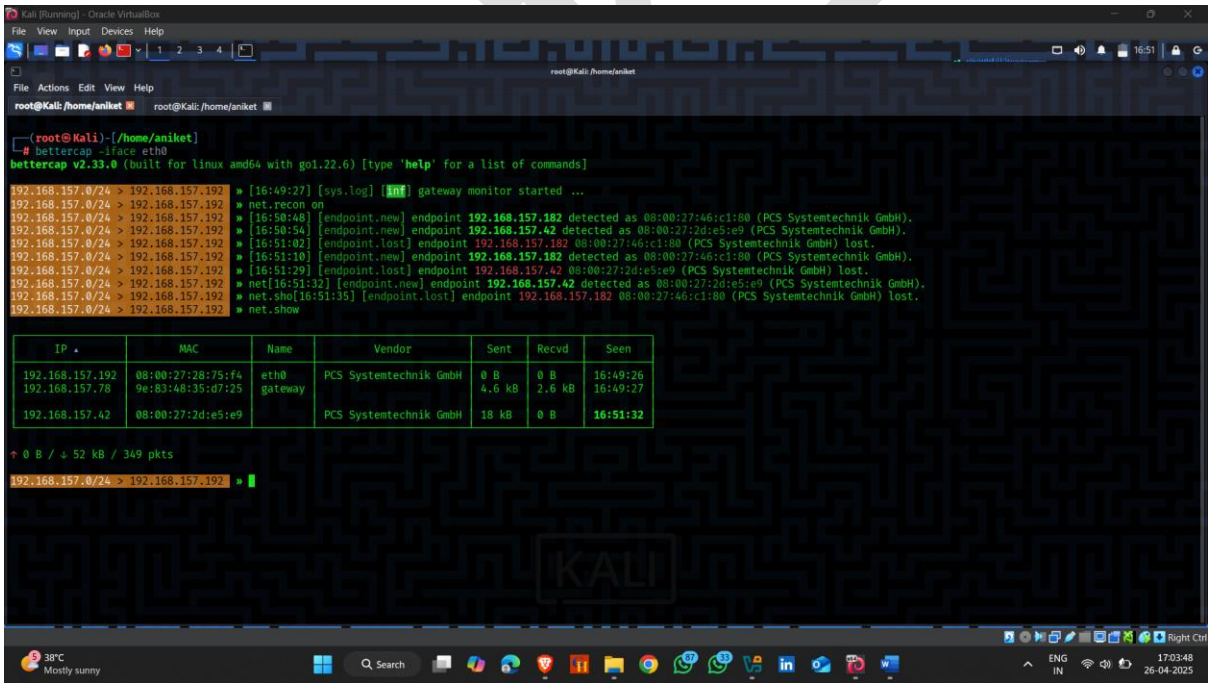
- Open Kali linux and open terminal
- And type bettercap



- Type **net.recon on** – to scan devices in network

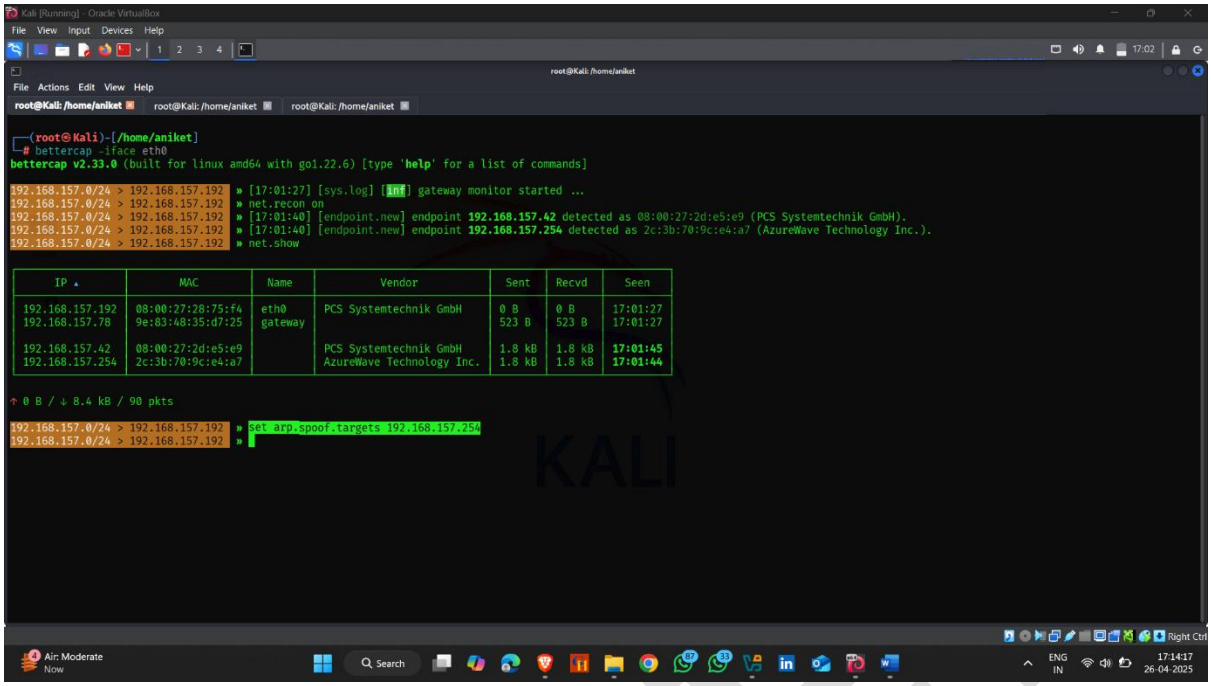


- **Used net.show** -- to display devices in network

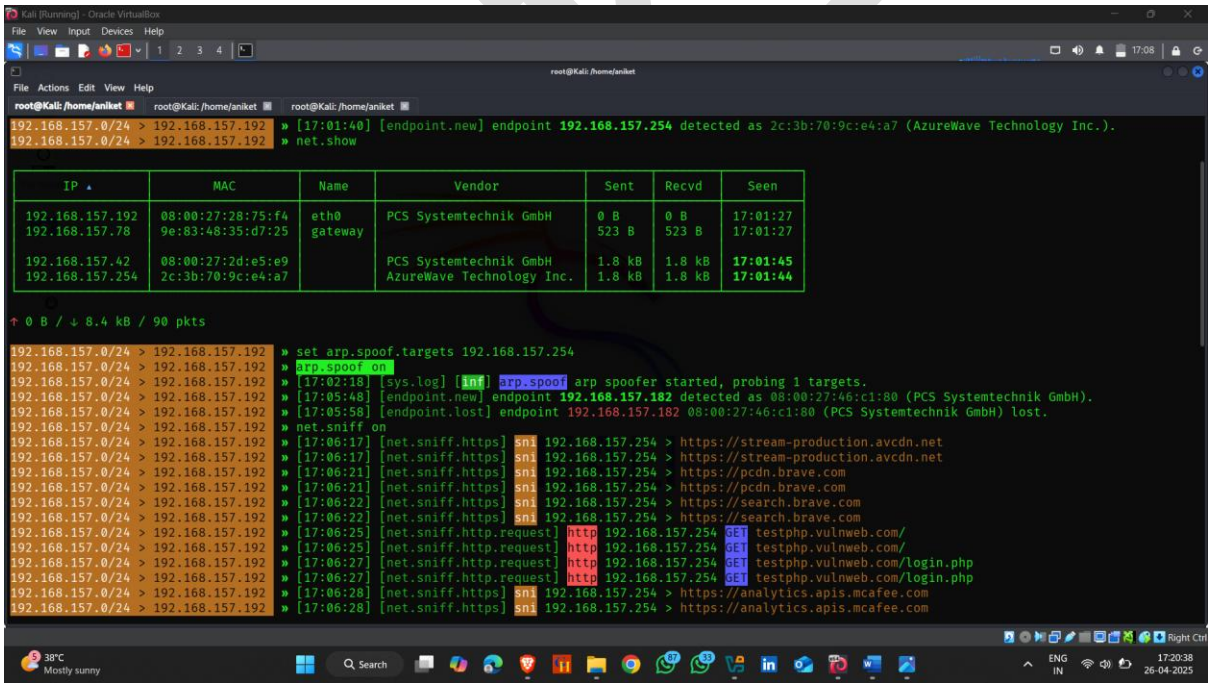


- **Now set a target**

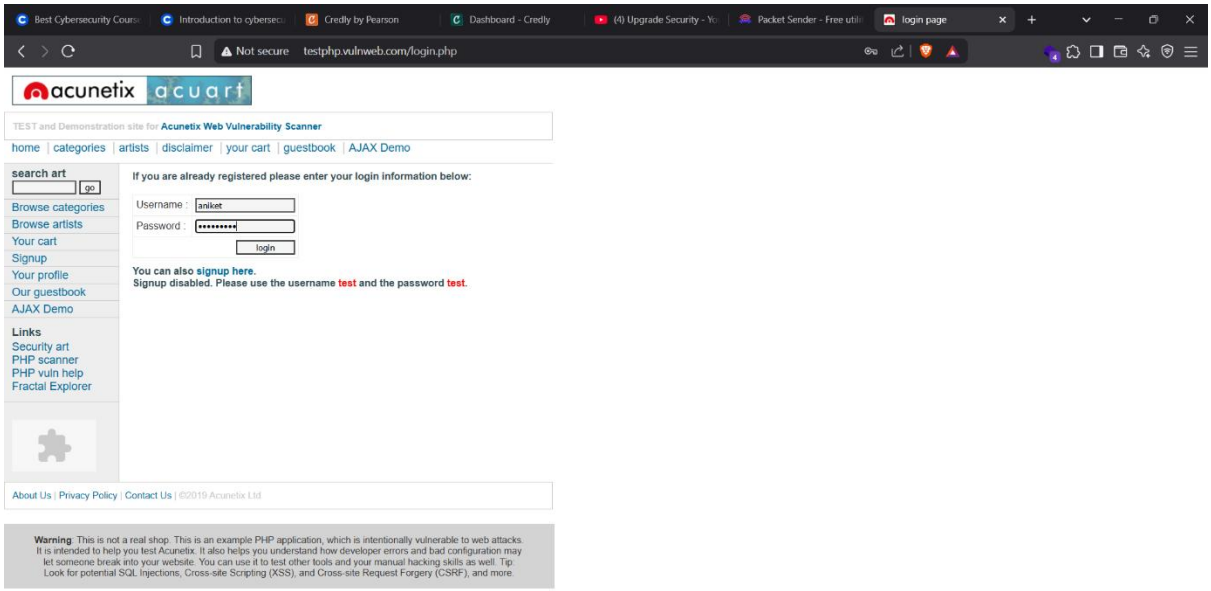
Command -: set arp.spoof.targets <target ip >



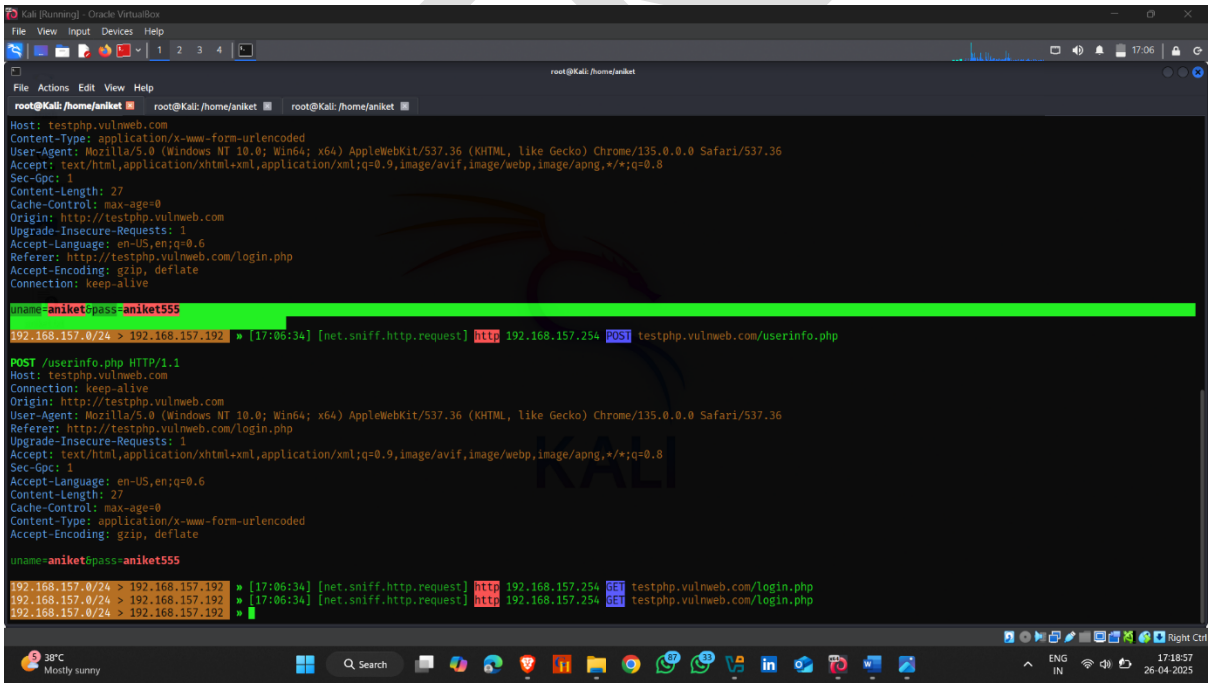
- Then **start arp.spoof on**



- Now go to target machine and used browser
- Add username and password



- Back to the kali linux
- Here, it capture the username and passwords

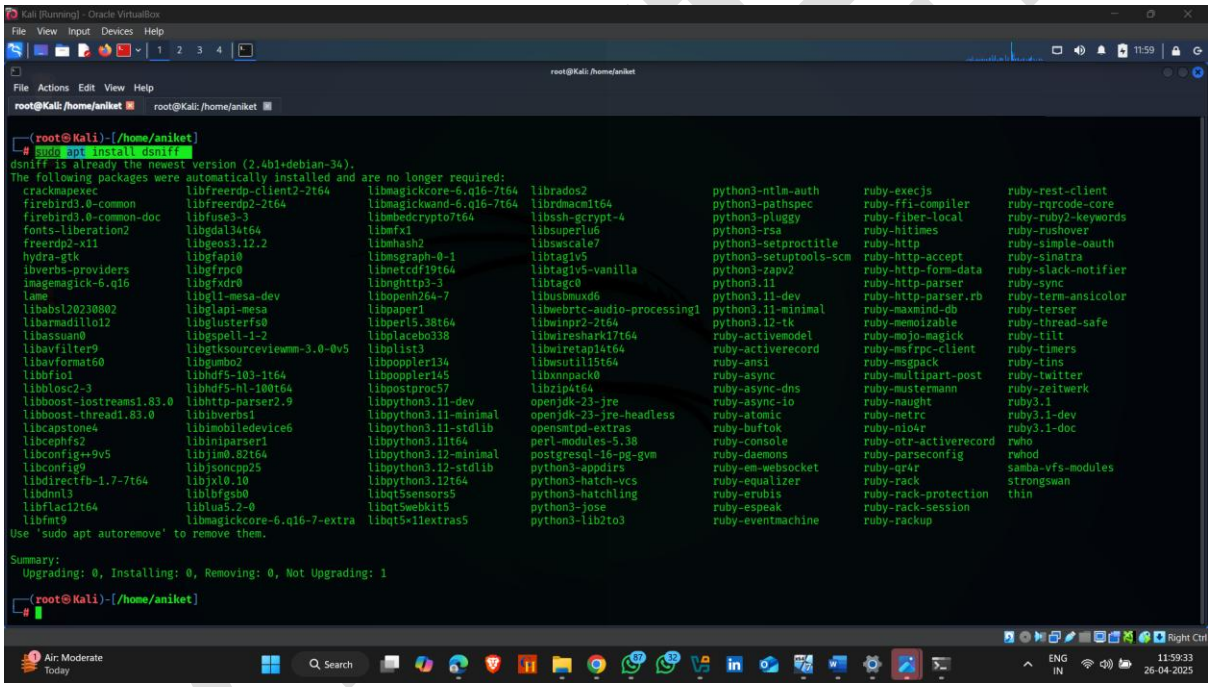


3.Perform ARP Poisoning Using Arp Spoofing

ARP spoofing (also called **ARP poisoning**) is a technique used in **Man-in-the-Middle (MITM) attacks** where the attacker tricks devices on a local network into thinking that their device (attacker's device) is the trusted one (like the router or another device).

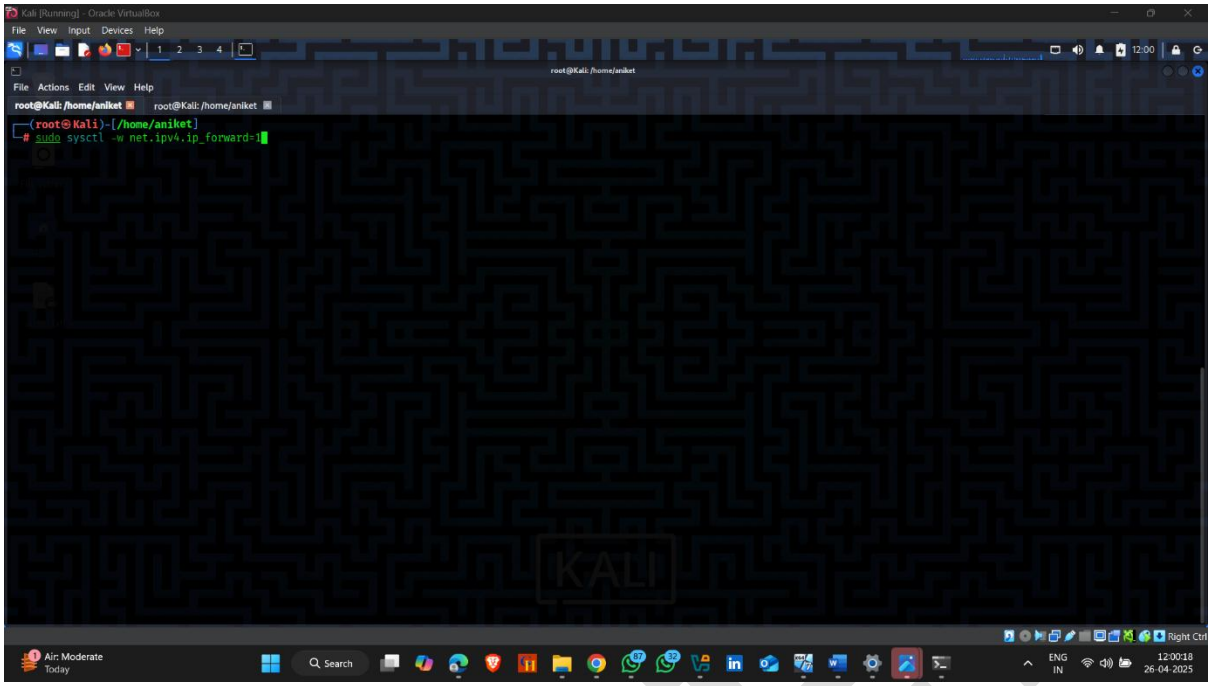
How to use it - :

- Open Kali linux and type sudo apt install dsniff



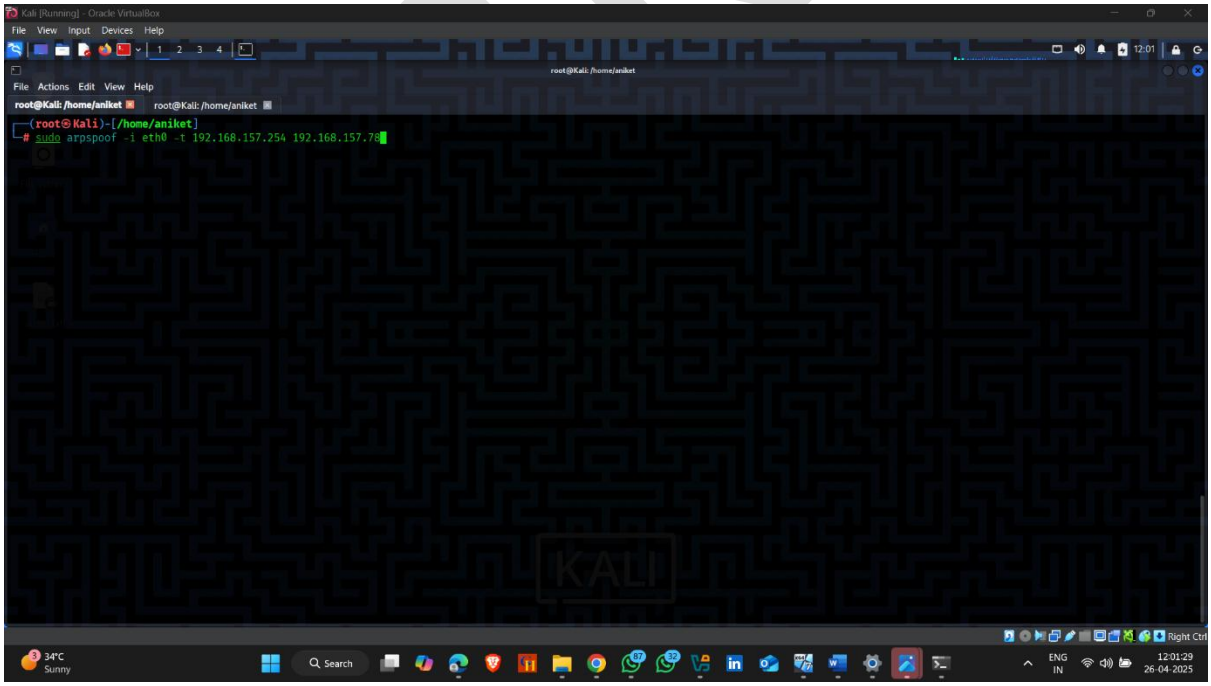
- Now ip forwarding

Command -: sudo sysctl -w net.ipv4.ip_forward=1

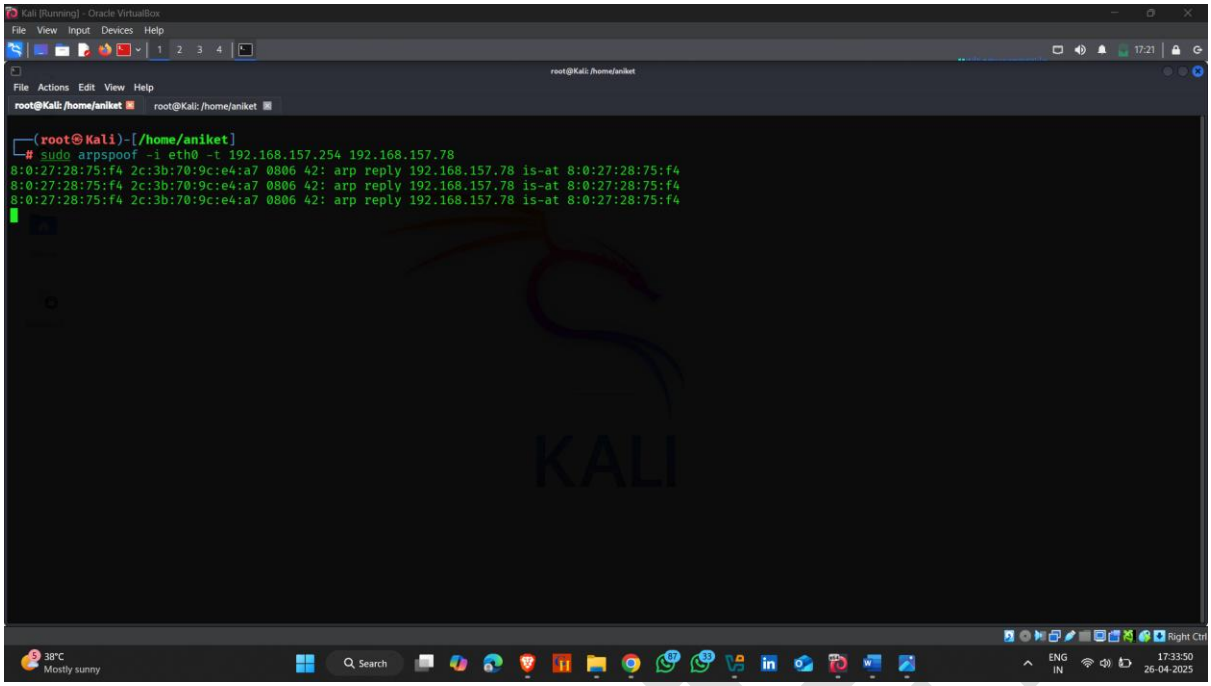


- **Now Start ARP Poisoining**

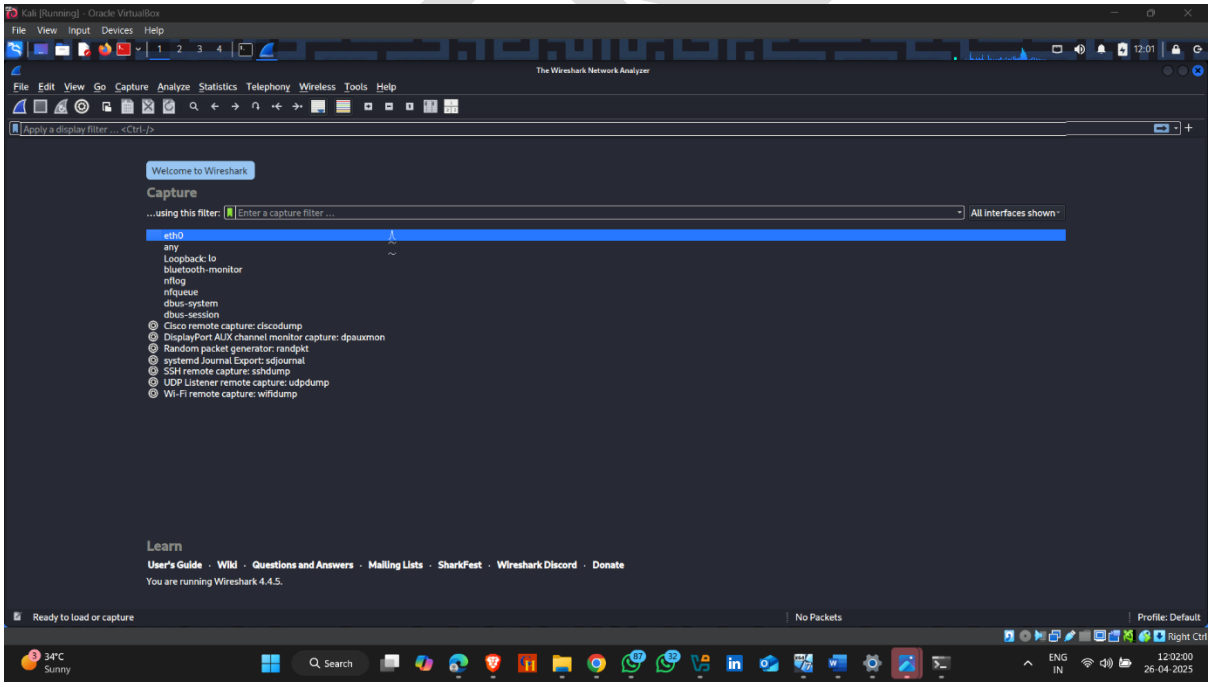
Command -: sudo arpspoof –i eth0 -t <target Ip > <gateway ip >



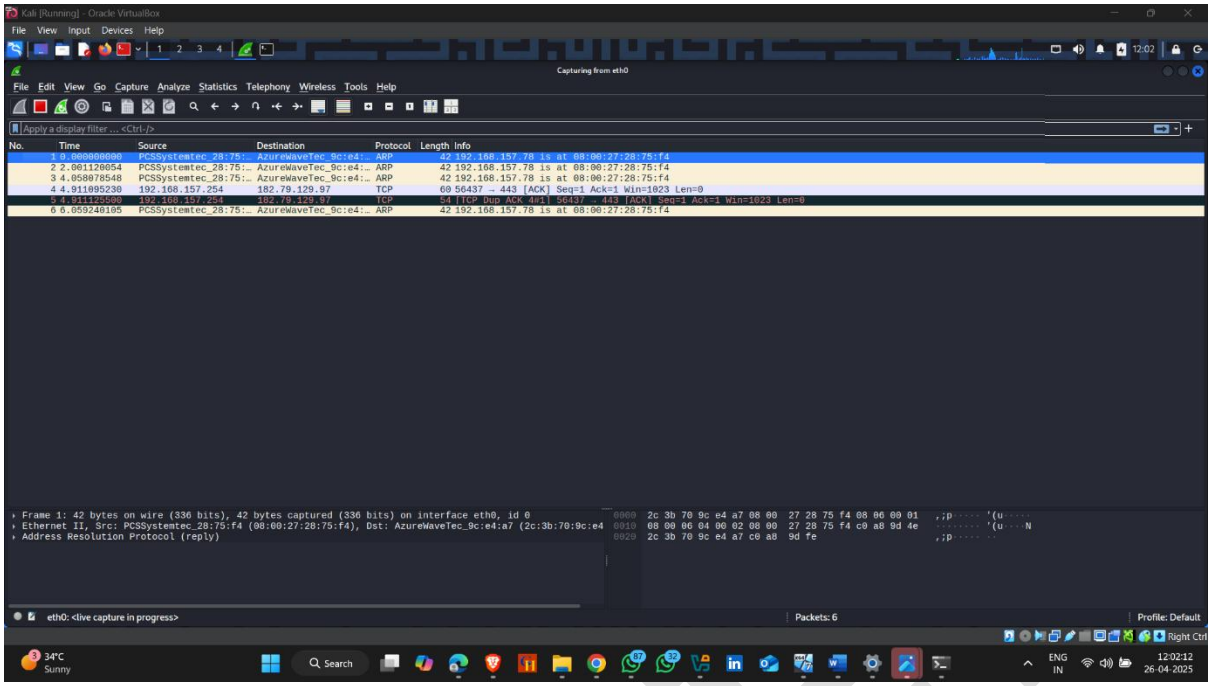
- Here it started



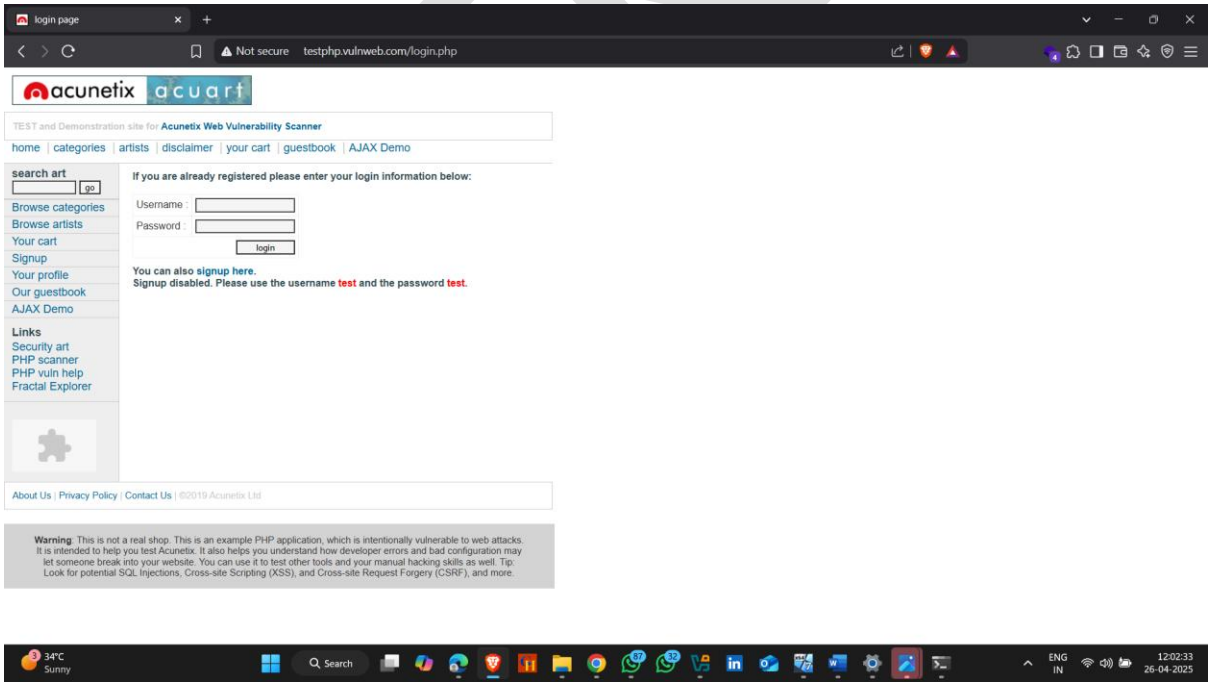
- Start Wireshark
- Click on eth0



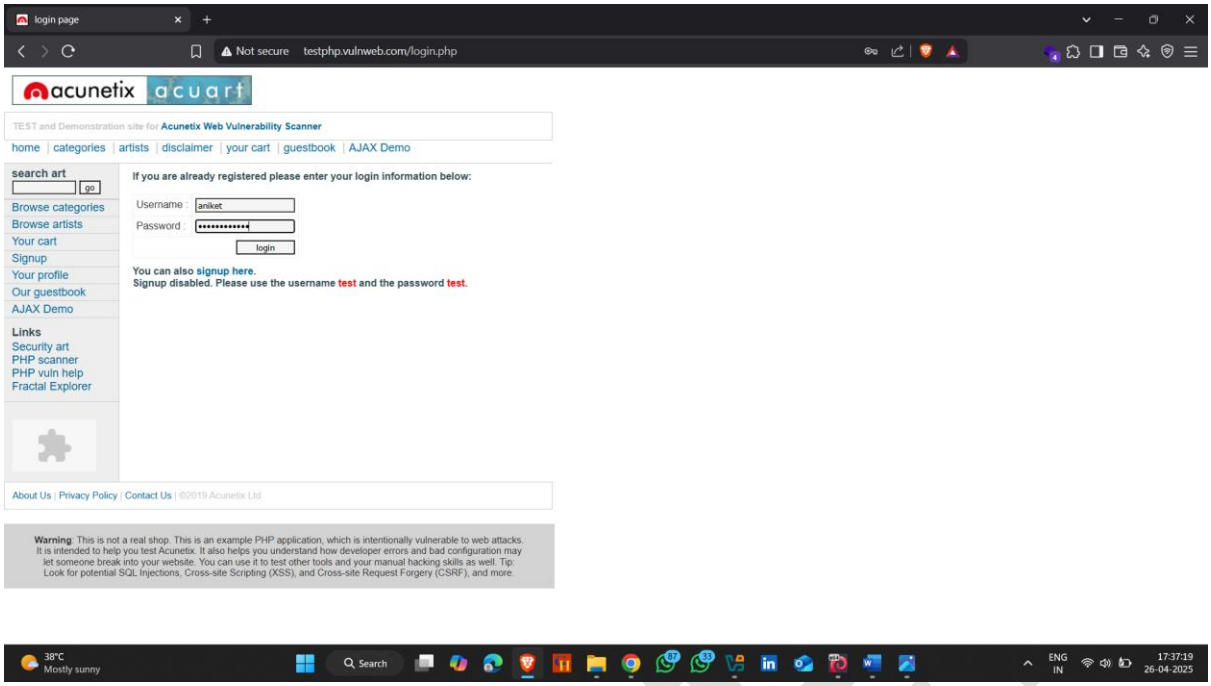
- **It capturing the packets**



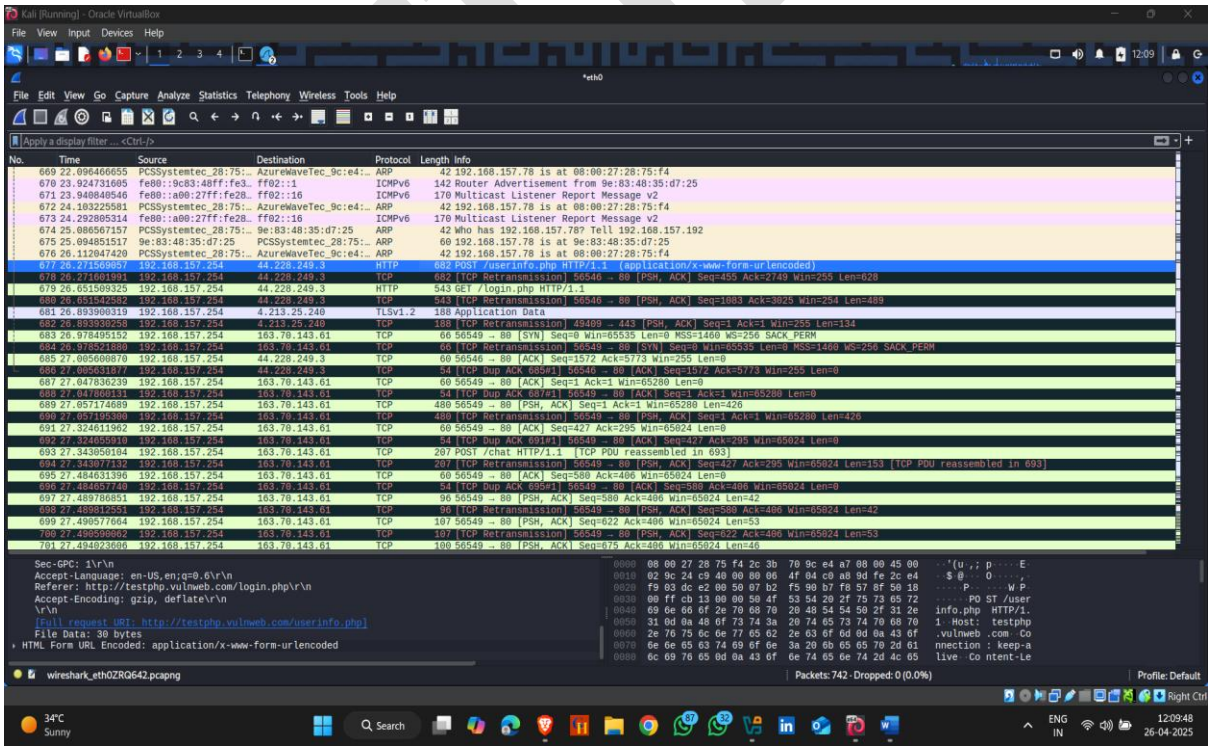
- **Now go to attacker machine browser**
- **Type Credentials**



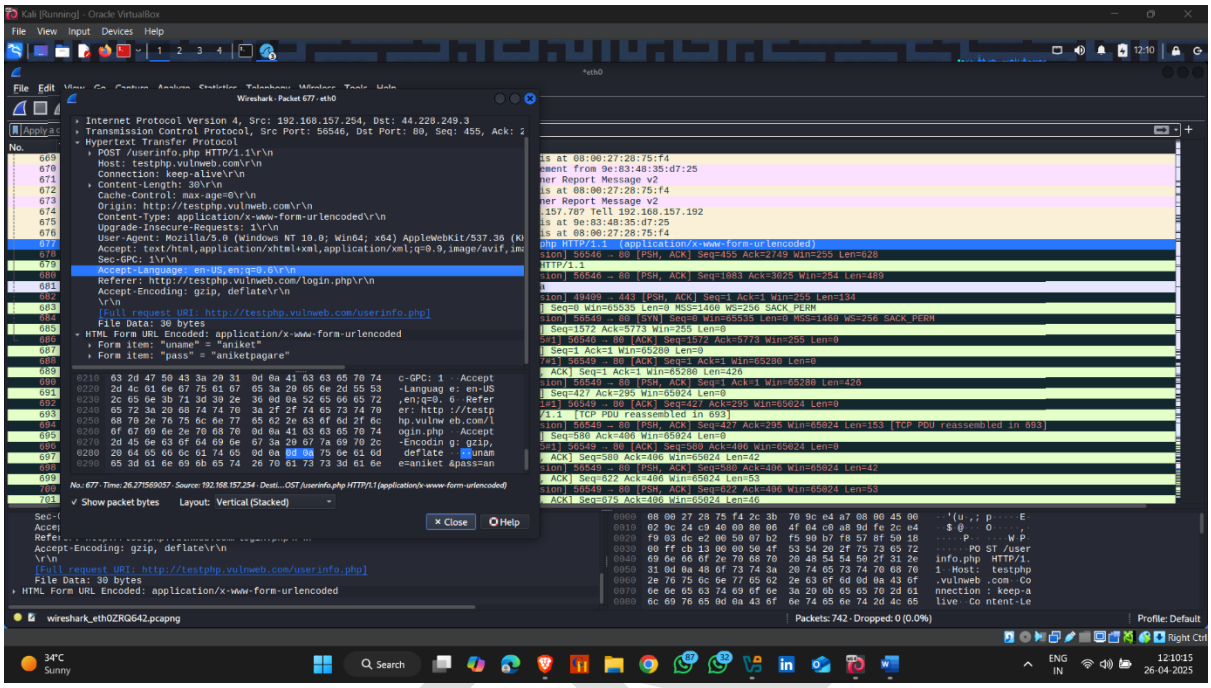
- **Entered username and passwords**



- Now back to the wireshark and find **POST** packet
- Here , post packet .. Open it



- **It captures the Credentials**



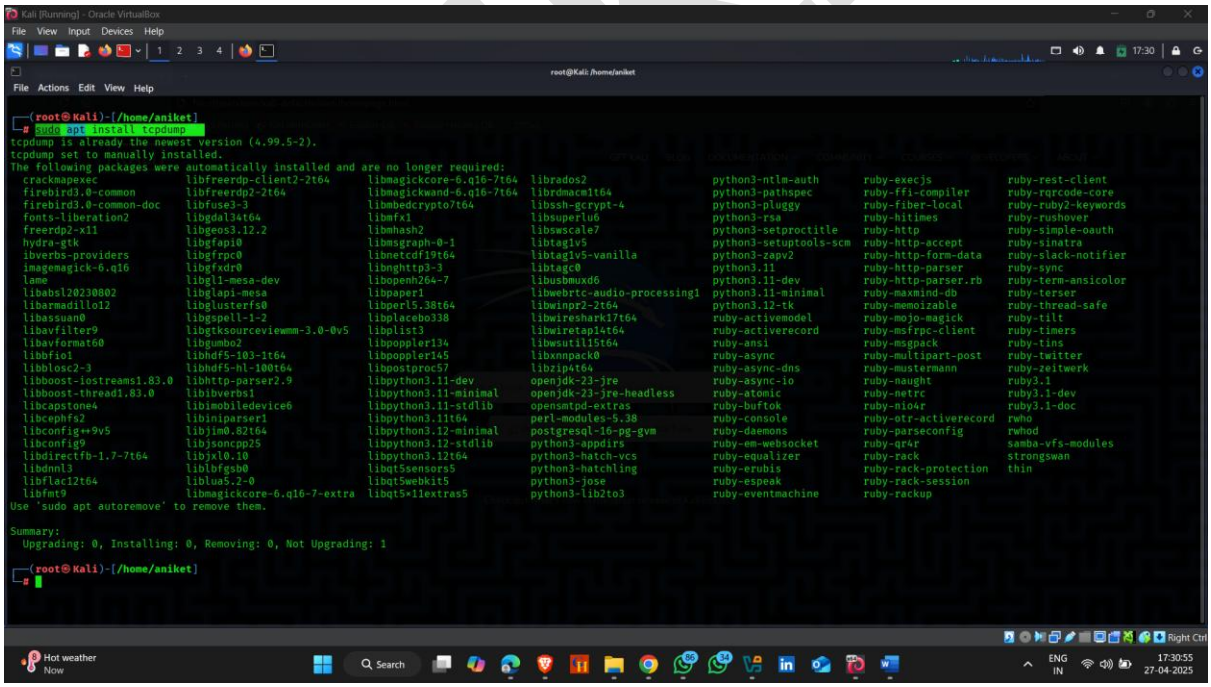
Passive Sniffing

Perform Passive Sniffing Using TCPDump

tcpdump is a command-line network packet analyzer tool that captures and displays network traffic in real-time.
It allows users to monitor, filter, and record packets flowing through a network interface for troubleshooting, analysis, and security testing.

How to use it -:

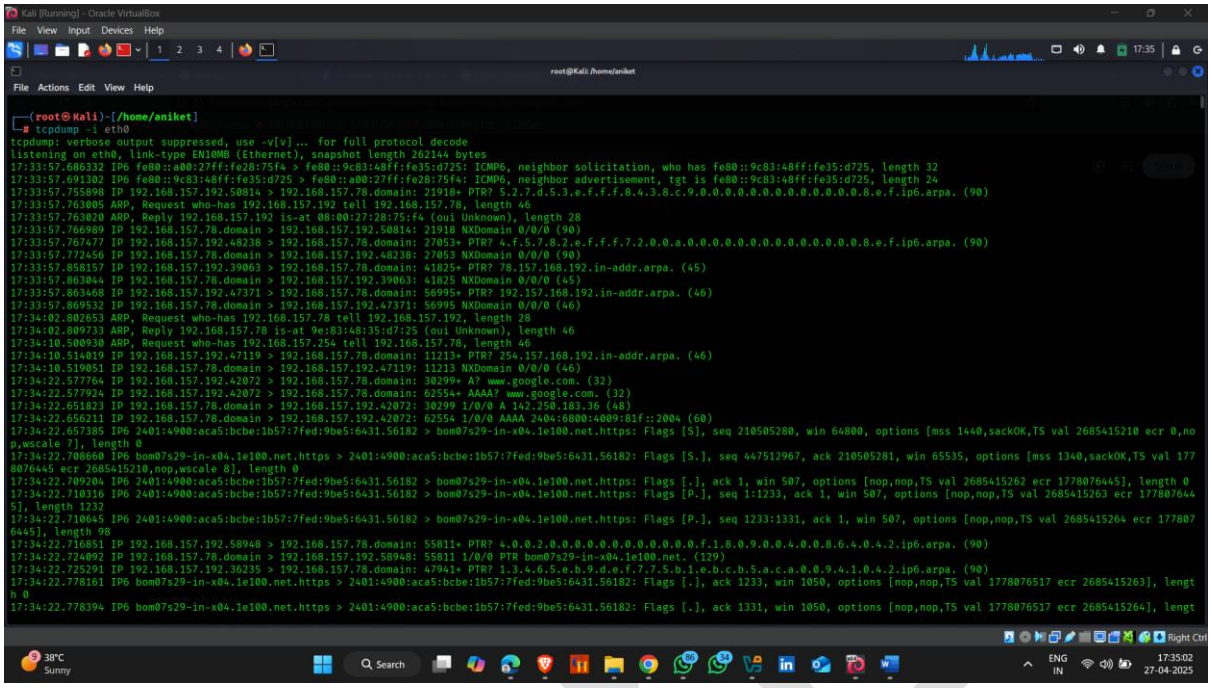
- Open Kali linux terminal and type sudo **apt install tcpdump**



- Now , capture the Network Traffic

Command – tcpdump -I eth0 – to capture all traffic in eth0 network interface

- Here it started capturing the packets

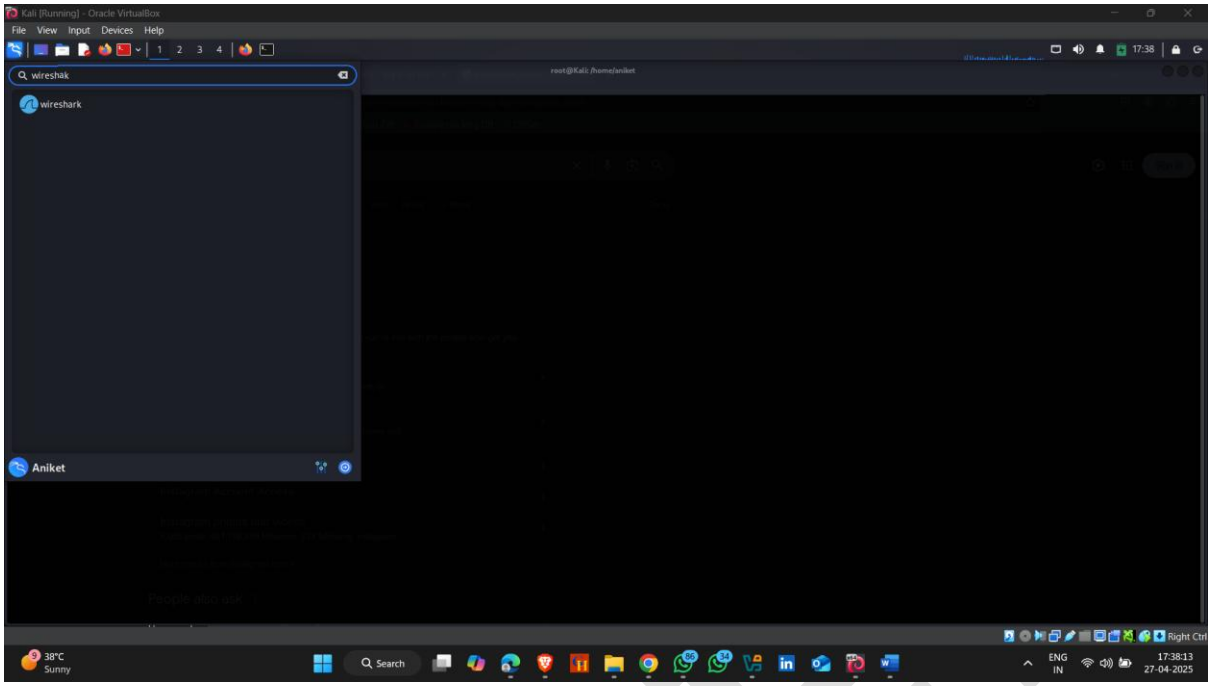


Perform Passive Sniffing Using Wireshark

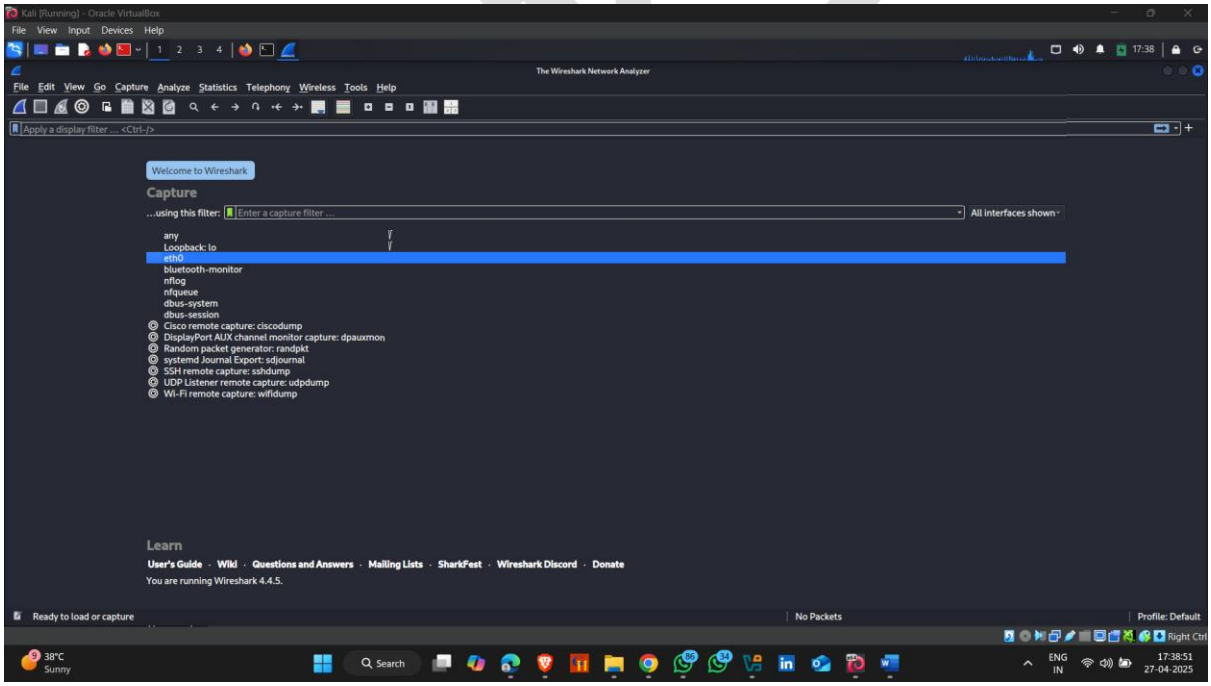
Wireshark is a free, open-source network protocol analyzer that captures, inspects, and displays network packets in real-time through a graphical interface.
It helps users analyze network traffic, troubleshoot problems, and study communication protocols in detail.

How to use it -:

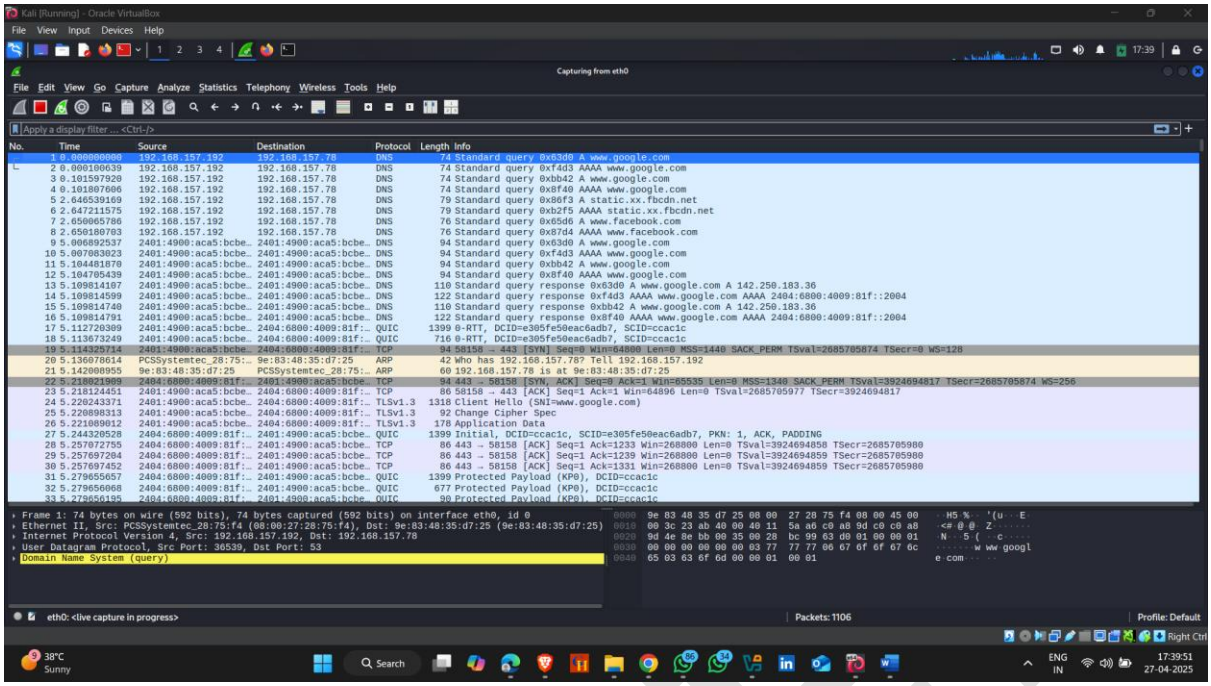
- Open kali linux , go to application section and search wireshark and open it



- Click on eth0 network interface



- Here , it started capturing the packets


Kali [Running] - Oracle VirtualBox
File 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
1 0.000000000 192.168.157.192 192.168.157.78 DNS 74 Standard query 0x63d0 A www.google.com
2 0.000100639 192.168.157.192 192.168.157.78 DNS 74 Standard query 0xf4d3 AAAA www.google.com
3 0.101597920 192.168.157.192 192.168.157.78 DNS 74 Standard query 0xbb42 A www.google.com
4 0.101807606 192.168.157.192 192.168.157.78 DNS 74 Standard query 0x8f40 AAAA www.google.com
5 2.646539169 192.168.157.192 192.168.157.78 DNS 79 Standard query 0x86f3 A static.xx.fbcdn.net
6 2.647211575 192.168.157.192 192.168.157.78 DNS 79 Standard query 0xb2f5 AAAA static.xx.fbcdn.net
7 2.650065786 192.168.157.192 192.168.157.78 DNS 76 Standard query 0x65d6 A www.facebook.com
8 2.650180703 192.168.157.192 192.168.157.78 DNS 76 Standard query 0x87d4 AAAA www.facebook.com
9 5.006892537 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 94 Standard query 0x63d0 A www.google.com
10 5.007083023 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 94 Standard query 0xf4d3 AAAA www.google.com
11 5.104481870 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 94 Standard query 0xbb42 A www.google.com
12 5.104705439 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 94 Standard query 0x8f40 AAAA www.google.com
13 5.109814107 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 110 Standard query response 0x63d0 A www.google.com A 142.250.183.36
14 5.109814599 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 122 Standard query response 0xf4d3 AAAA www.google.com AAAA 2404:6800:4009:81f::2004
15 5.109814740 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 110 Standard query response 0xbb42 A www.google.com A 142.250.183.36
16 5.109814791 2401:4900:aca5:bcbe... 2401:4900:aca5:bcbe... DNS 122 Standard query response 0x8f40 AAAA www.google.com AAAA 2404:6800:4009:81f::2004
17 5.112720309 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... QUIC 1399 0-RTT, DCID=e305fe50eac6adb7, SCID=ccac1c
18 5.113673249 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... QUIC 716 0-RTT, DCID=e305fe50eac6adb7, SCID=ccac1c
19 5.114325714 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... TCP 94 58158 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=2685705874 TSecr=0 WS=128
20 5.136078614 PCSSystemtec_28:75:... 9e:83:48:35:d7:25 ARP 42 Who has 192.168.157.78? Tell 192.168.157.192
21 5.142000955 9e:83:48:35:d7:25 PCSSystemtec_28:75:... ARP 60 192.168.157.78 is at 9e:83:48:35:d7:25
22 5.218021909 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... TCP 94 443 → 58158 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1340 SACK_PERM TSval=3924694817 TSecr=2685705874 WS=256
23 5.218124451 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... TCP 86 58158 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=2685705977 TSecr=3924694817
24 5.220243371 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... TLSv1.3 1318 Client Hello (SNI=www.google.com)
25 5.220898313 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... TLSv1.3 92 Change Cipher Spec
26 5.221089012 2401:4900:aca5:bcbe... 2404:6800:4009:81f:... TLSv1.3 178 Application Data
27 5.244320528 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... QUIC 1399 Initial, DCID=ccac1c, SCID=e305fe50eac6adb7, PKN: 1, ACK, PADDING
28 5.257872755 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... TCP 86 443 → 58158 [ACK] Seq=1 Ack=1233 Win=268800 Len=0 TSval=3924694858 TSecr=2685705980
29 5.257697204 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... TCP 86 443 → 58158 [ACK] Seq=1 Ack=1239 Win=268800 Len=0 TSval=3924694859 TSecr=2685705980
30 5.257697452 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... TCP 86 443 → 58158 [ACK] Seq=1 Ack=1331 Win=268800 Len=0 TSval=3924694859 TSecr=2685705980
31 5.279655657 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... QUIC 1399 Protected Payload (KP0), DCID=ccac1c
32 5.279656068 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... QUIC 677 Protected Payload (KP0), DCID=ccac1c
33 5.279656195 2404:6800:4009:81f:... 2401:4900:aca5:bcbe... QUIC 90 Protected Payload (KP0), DCID=ccac1c
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_28:75:f4 (08:00:27:28:75:f4), Dst: 9e:83:48:35:d7:25 (9e:83:48:35:d7:25)
Internet Protocol Version 4, Src: 192.168.157.192, Dst: 192.168.157.78
User Datagram Protocol, Src Port: 36539, Dst Port: 53
Domain Name System (query)
0000 9e 83 48 35 d7 25 08 00 27 28 75 f4 08 00 45 00
0010 00 3c 23 ab 40 00 40 11 5a a6 c0 a8 9d c0 c0 a8
0020 9d 4e 8e bb 00 35 00 28 bc 99 63 d0 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c
0040 65 03 63 6f 6d 00 00 01 00 01
eth0: <live capture in progress>
Packets: 1106
Profile: Default
Right Ctrl
38°C
Sunny
Search
ENG
IN
17:39:51
27-04-2025

THANK YOU