SNIFFING

-ATHARVA KATKAR

TABLE OF CONTENTS

1. **Sniffing**
    1.1 Introduction to Sniffing
    1.2 What is a Sniffer
    1.3 How Sniffing Works
2. **Types of Sniffing**
    2.1 Passive Sniffing
    2.2 Active Sniffing
3. **Protocols Vulnerable to Sniffing**
4. **MAC Flooding**
    4.1 Introduction to MAC Flooding
    4.2 Why MAC Flooding is Dangerous
    4.3 MAC Flooding Attack Using Macof
    4.4 Monitoring MAC Flooding Using Wireshark
5. **DHCP Starvation**
    5.1 Introduction to DHCP Starvation
    5.2 DHCP Starvation Attack Explanation
    5.3 DHCP Starvation Using Yersinia
    5.4 Analysis Using Wireshark

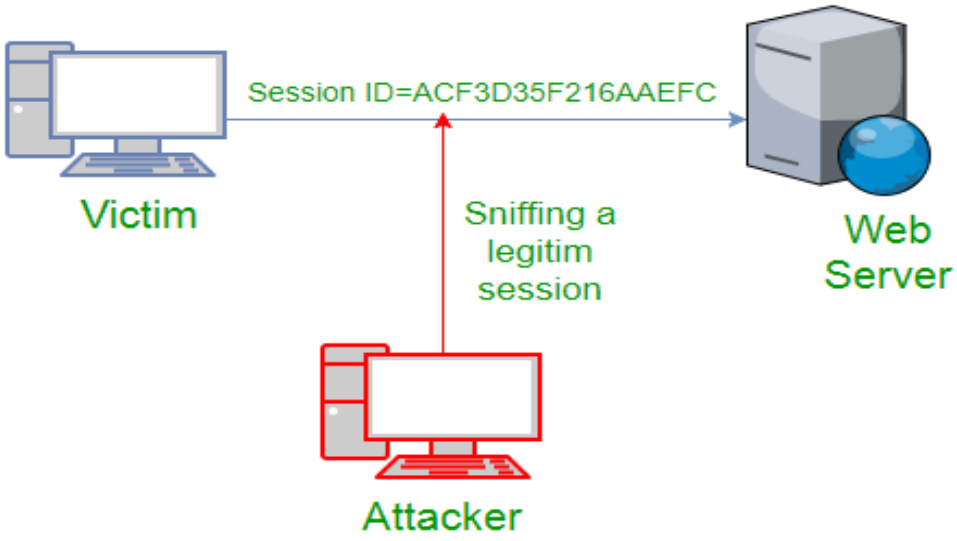
6. **ARP Poisoning**
    6.1 Introduction to ARP Poisoning
    6.2 How ARP Poisoning Works
    6.3 Why ARP Poisoning is Dangerous
    6.4 Detection of ARP Poisoning Using XARP
7. **MAC Spoofing**
    7.1 Introduction to MAC Spoofing
    7.2 Working of MAC Spoofing
    7.3 Detection of MAC Spoofing
8. **MAC Spoofing Tools**
    8.1 MAC Spoofing Using TMACv6
    8.2 MAC Spoofing Using Macchanger
9. **Extra Tools**
    9.1 MAC Flooding Using Scapy
    9.2 MAC Flooding Using Hping3
        9.2.1 Hping3 --fast
        9.2.2 Hping3 --faster
        9.2.3 Hping3 --flood
    9.3 ARP Poisoning Using Ettercap
    9.4 ARP Poisoning Using Bettercap

SNIFFING

Sniffing is the process of capturing and analyzing network data packets as they travel over a network.
A person or tool that performs sniffing is called a sniffer.

Packets may contain:

- Source & destination IP
- Protocol details (TCP, UDP, HTTP, etc.)
- Usernames, passwords (if not encrypted)
- Cookies and session data



How Sniffing Works:

1. Data is sent in packets over a network
2. A sniffer tool puts the network interface into promiscuous mode
3. It captures all packets, not just those meant for the device
4. Packets are decoded and analyzed

Types of Sniffing

1️⃣ Passive Sniffing

- Attacker only **listens**
- No traffic modification
- Works on **hub-based networks**
- Hard to detect

Example:
Monitoring traffic in an old LAN hub

2️⃣ Active Sniffing

- Attacker **injects packets**
- Used in **switched networks**
- Easier to detect

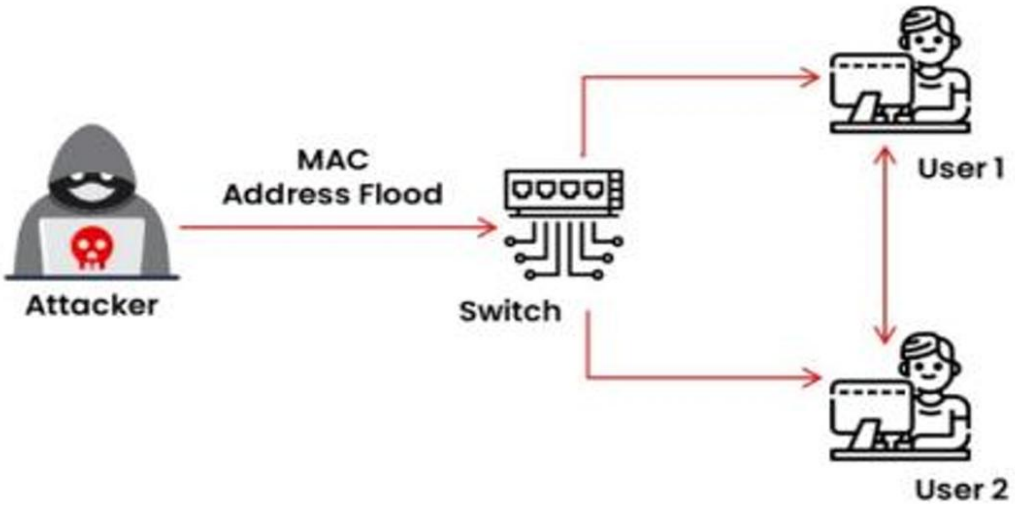
Techniques used:

- ARP Poisoning
- MAC Flooding
- DNS Spoofing

Protocol	**Risk**
HTTP	Passwords visible
FTP	Plain text credentials
Telnet	No encryption
SMTP	Email contents
POP3	Login credentials

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.



Why MAC Flooding is Dangerous?

- Allows packet sniffing
- Leads to Man-in-the-Middle (MITM) attacks
- Breaks switch security
- Steals sensitive data (passwords, sessions)

Mac Flooding Attack Using Macof (Linux Tool)

Macof is a MAC flooding tool from the dsniff suite used in cybersecurity labs to perform Layer 2 attacks on switches.

It generates thousands of fake MAC addresses to overflow the switch CAM table, forcing the switch to act like a hub.

📌 **Result:** Attacker can sniff network traffic

How to use it - :

- Open kali linux
- Type sudo apt install macof
- Then get detailed information about macof , simply type man macof

Figure 1

- See target system's IP
- Perform attack
- Type - : macof -I eth0 -d
  -I → network interface
  -d → destination ip

- Mac Flooding attack starts…..

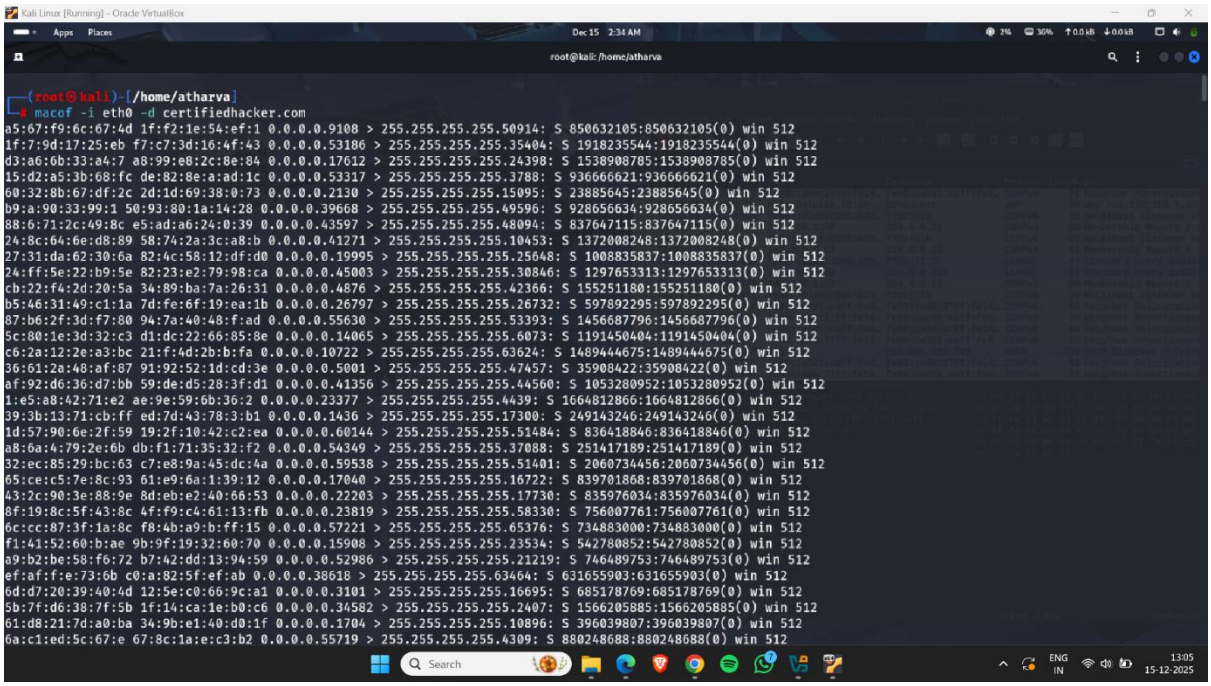


Figure 2

- Oen Wireshark and monitor the Attack

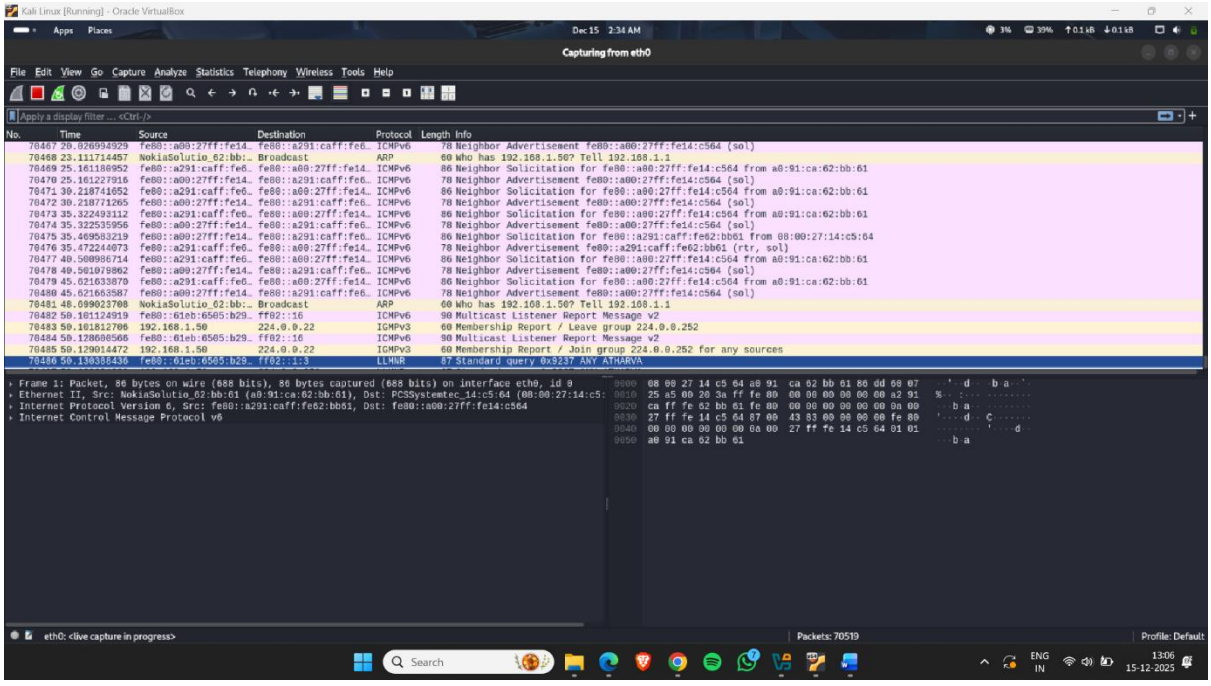


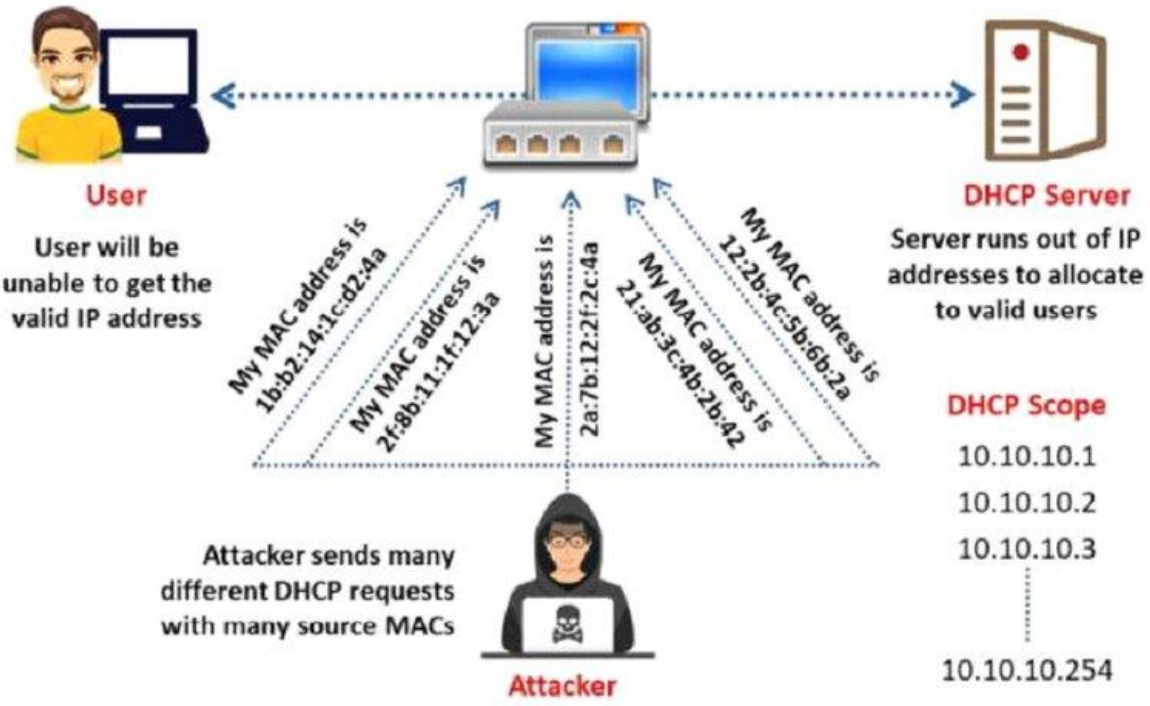
Figure 3

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 Using Yersinia (Linux Tool)

How to use it -:

- Open kali linux
- Type sudo apt install yersinia
- Get detailed information about macof , simply type man yersinia

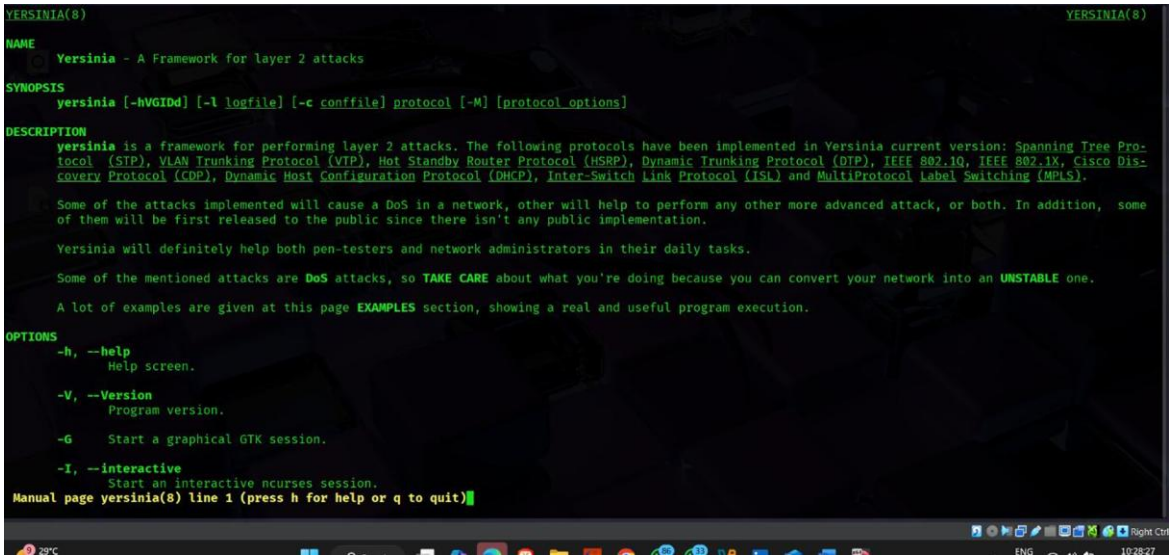


Figure 4

- Now find a DHCP attack commands

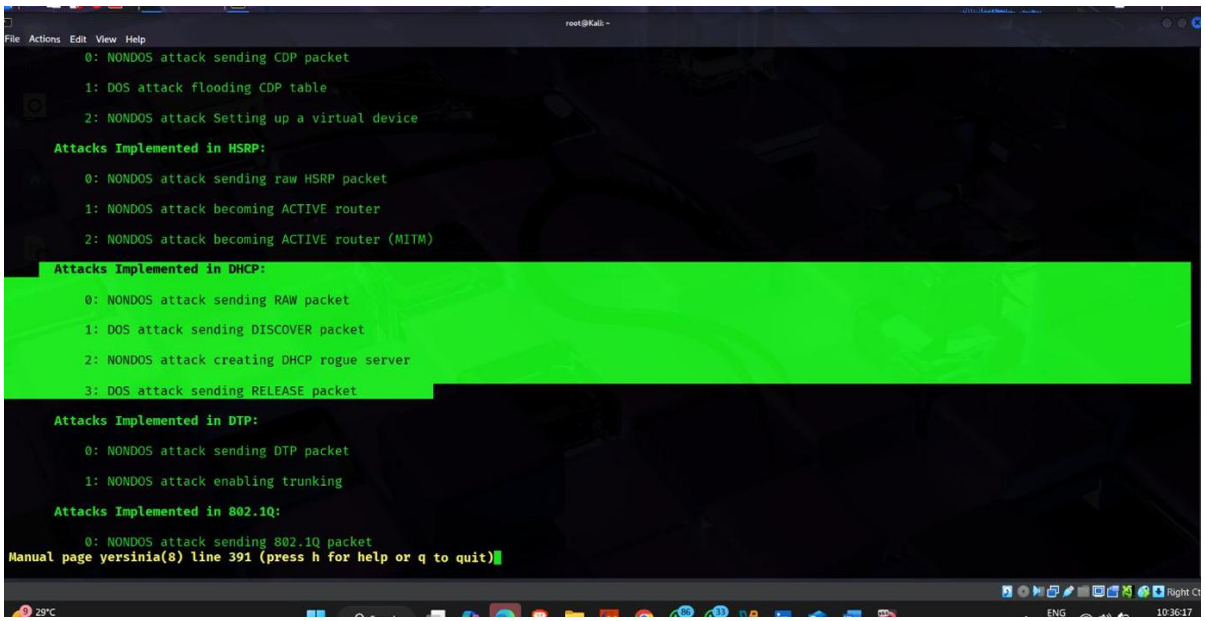


Figure 5

- Now find a target physical address/mac address
- Using → arp
- Now perform attack & start Wireshark
- yersinia DHCP -attack 1 –(dest)
    - ➢ DHCP – Perform DHCP attack -attack – perform attack
    - ➢ 1 – Send Raw data Packets
    - ➢ -dest – Destination

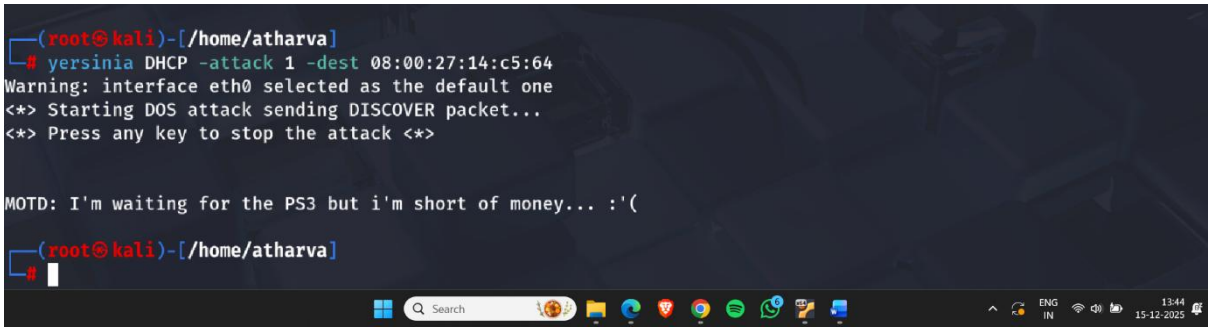


Figure 6

- DHCP Packets are send to the target

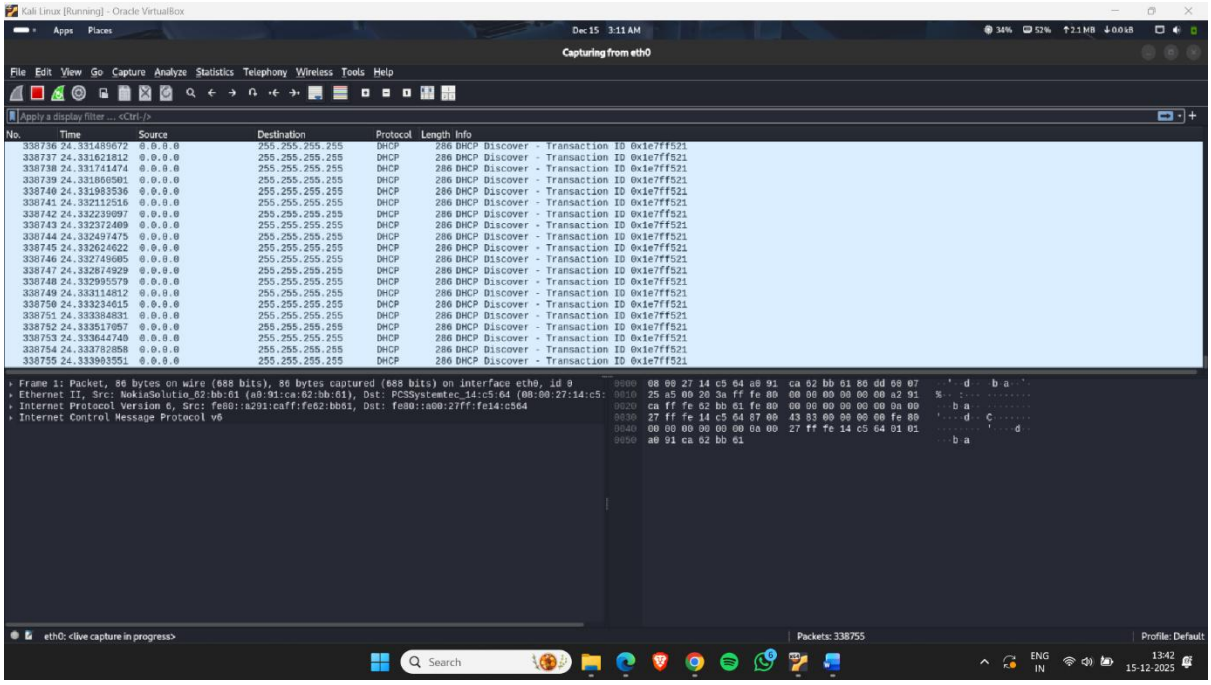


Figure 7

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

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.

Why ARP Poisoning is Dangerous?

- Steals usernames & passwords
- Hijacks sessions
- Modifies data in transit
- Performs DoS attacks

How ARP Poisoning Works (Step-by-Step)

1. Attacker sends fake ARP reply to victim
2. Victim believes attacker = router
3. Attacker sends fake ARP reply to router
4. Router believes attacker = victim
5. All traffic passes through attacker

Detect Arp Poisoning Using XARP Application

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 it.

Website Link:

https://search.brave.com/search?q=xarp+download

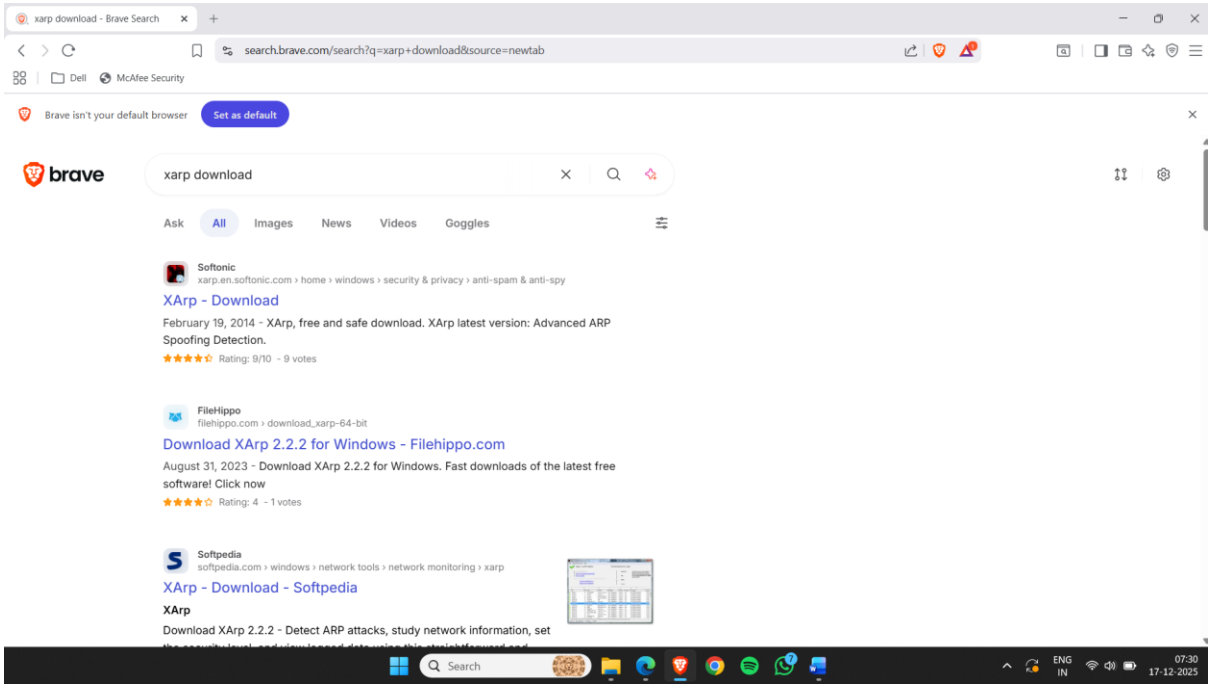


Figure 8

- Click on free Download for windows

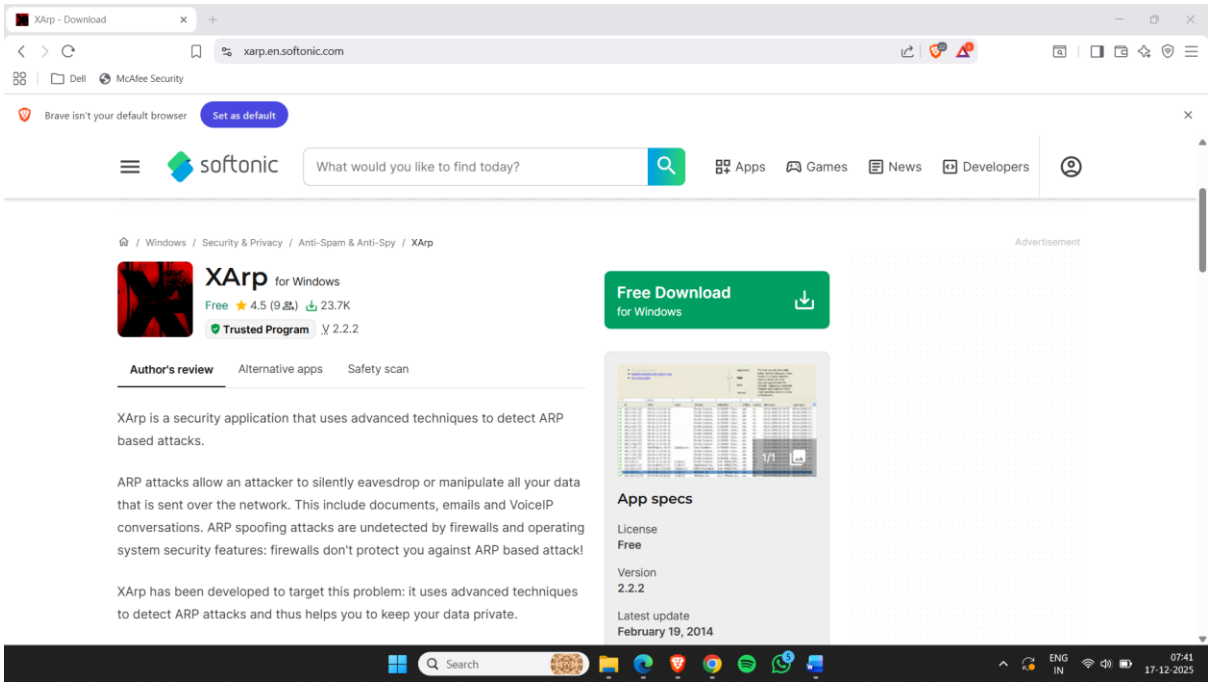


Figure 9

- Click on free Download for PC

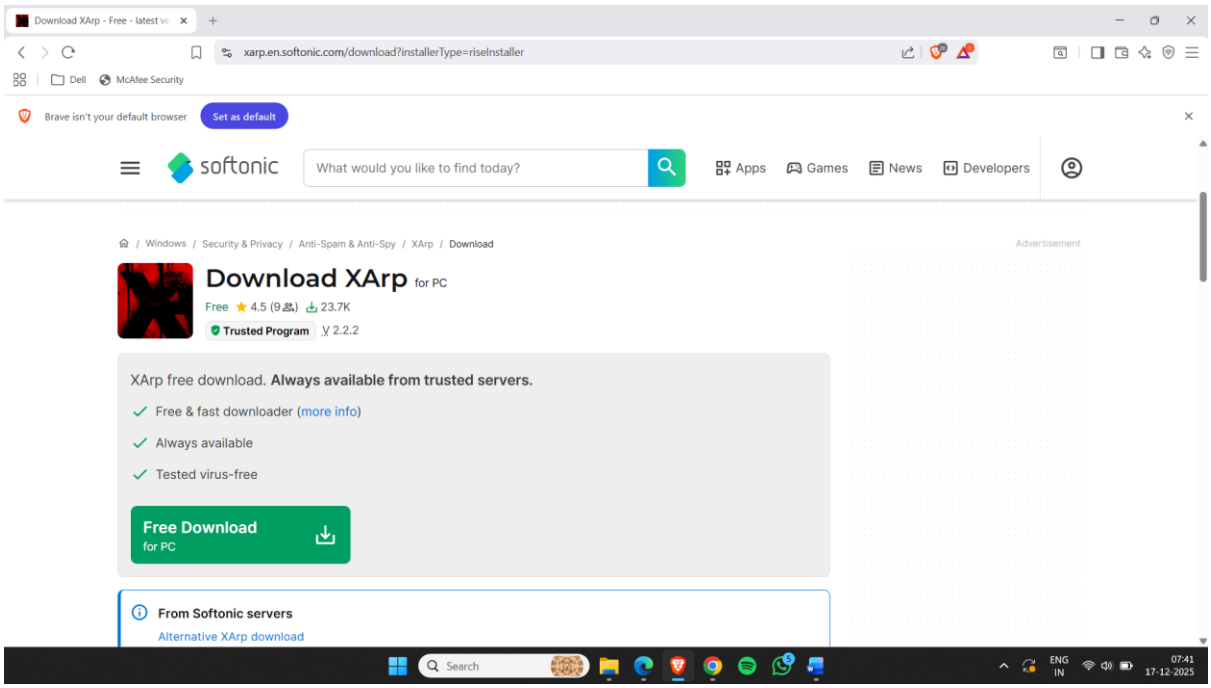


Figure 10

What XARP displays:

- It scans the Ip address of the network
- It display ARP attacks ip using marks and display a alerts (Right side of the screen).

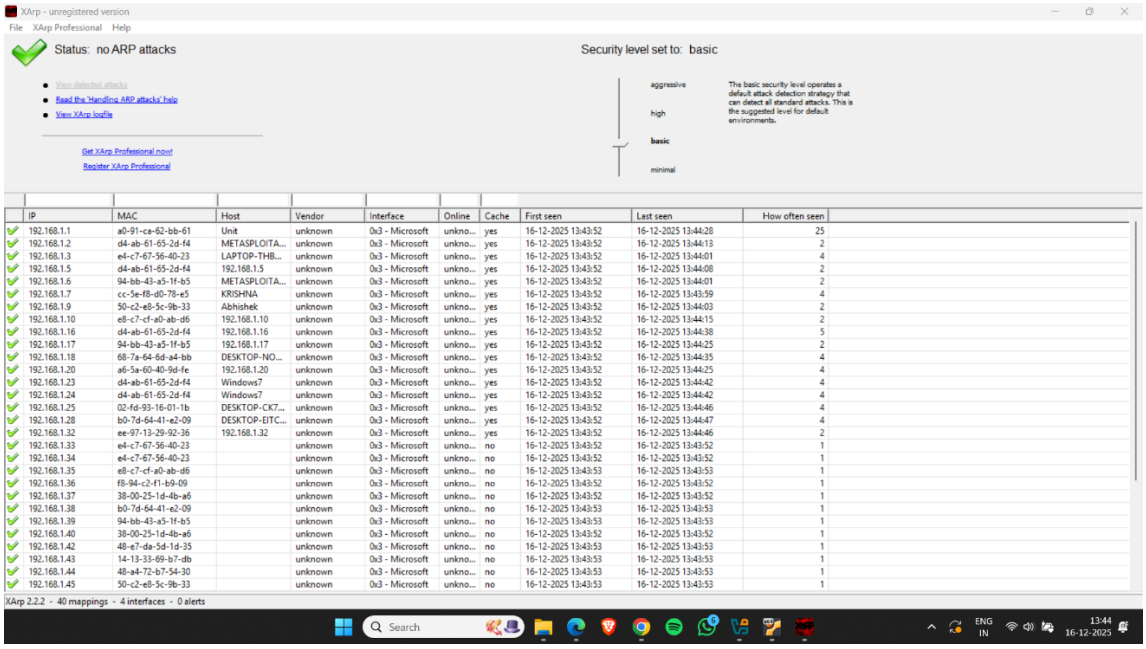


Figure 11

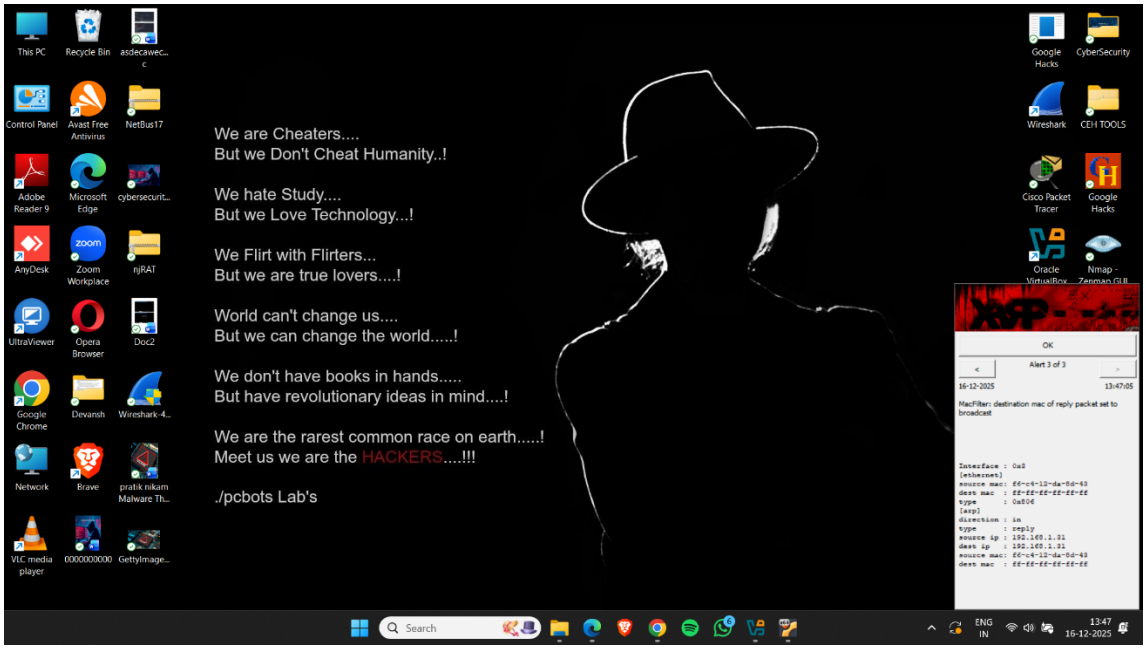


Figure 12

This popup indicates suspicious ARP (Address Resolution Protocol) activity, which is commonly seen during: ARP poisoning

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.

MAC Spoofing is an attack where:

An attacker changes their device’s MAC address to impersonate another device on the network.

This allows the attacker to:

- Bypass security controls
- Intercept traffic
- Perform Man-in-the-Middle (MITM) attacks

What happens During MAC Spoofing?

1. Attacker identifies trusted MAC address
2. Attacker changes own MAC to match it
3. Network believes attacker is the trusted device
4. Traffic is redirected or intercepted

Detection of MAC Spoofing

- **Signs:**
  - Duplicate MAC addresses
  - Frequent ARP changes
  - Broadcast ARP replies
  - Network IDS alerts (XArp, Snort)

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.

TMAC (Technitium MAC Address Changer) v6 allows you to:

- View current & original MAC address
- Change MAC address temporarily or permanently
- Enable/disable network adapters
- Reset MAC to factory value

How to install it - :

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

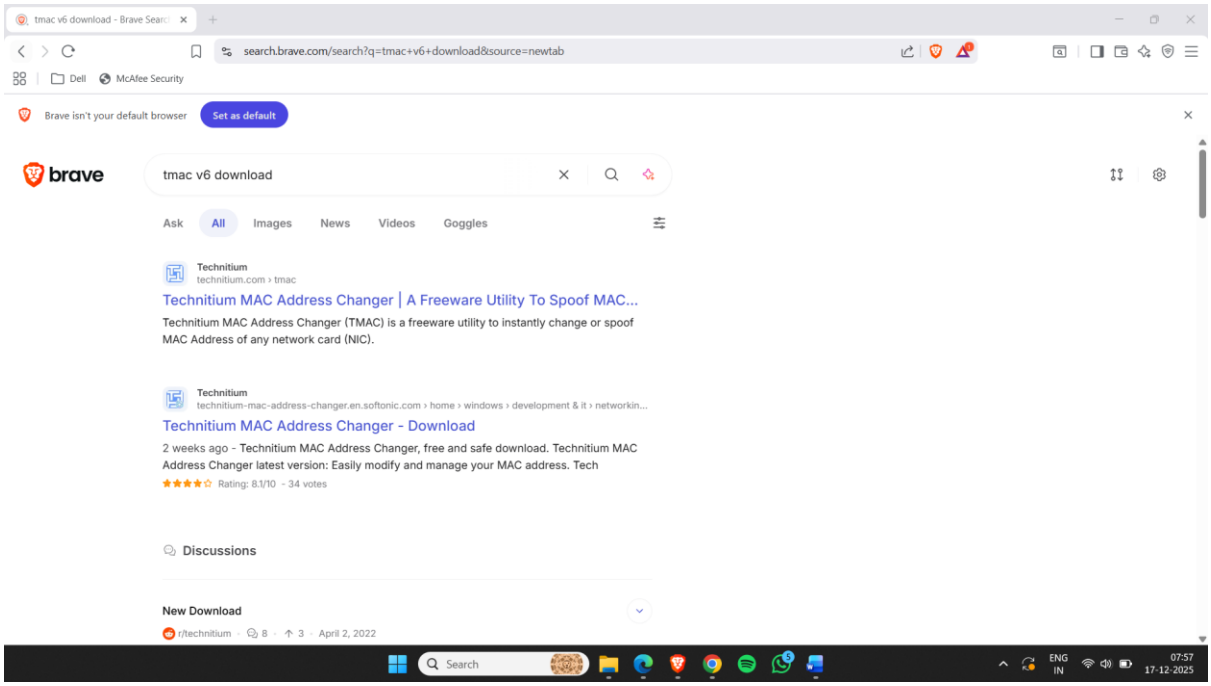


Figure 13

- Click on Download

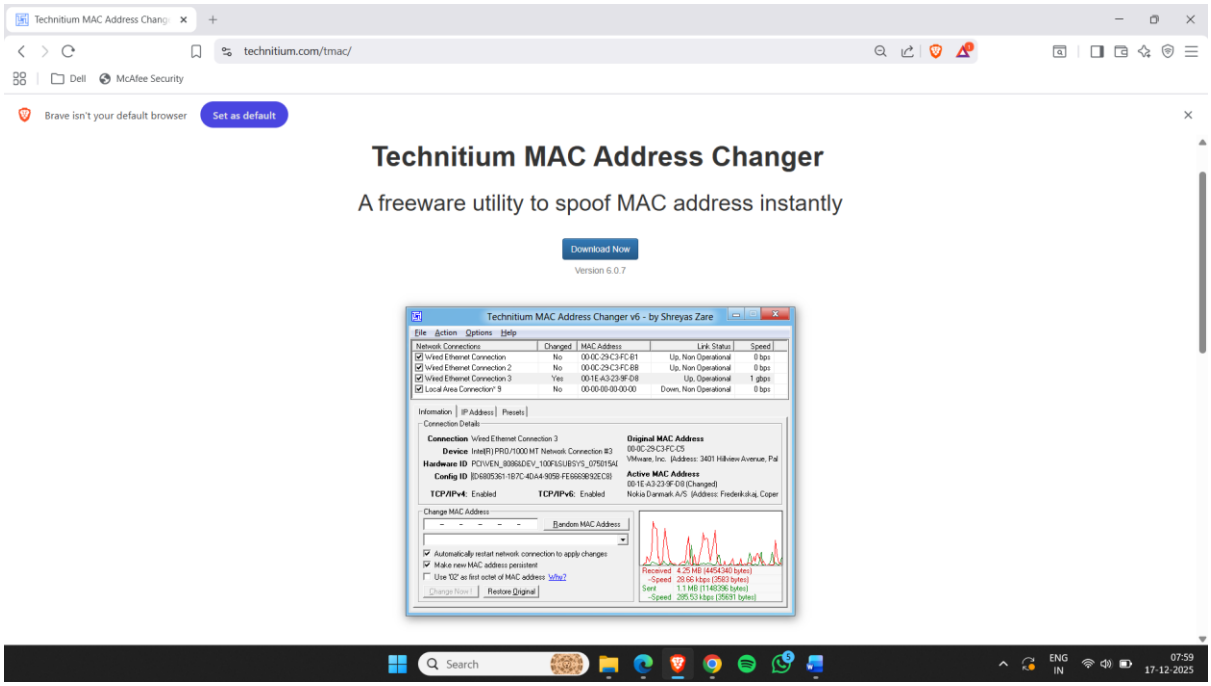


Figure 14

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

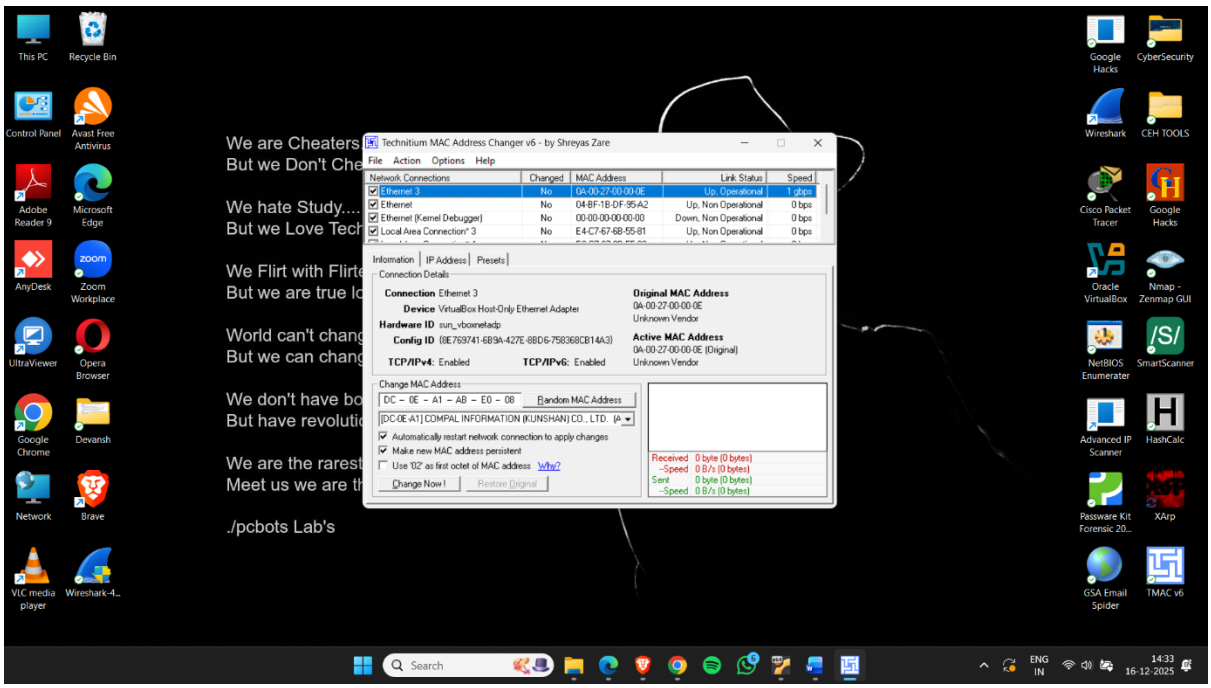


Figure 15

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

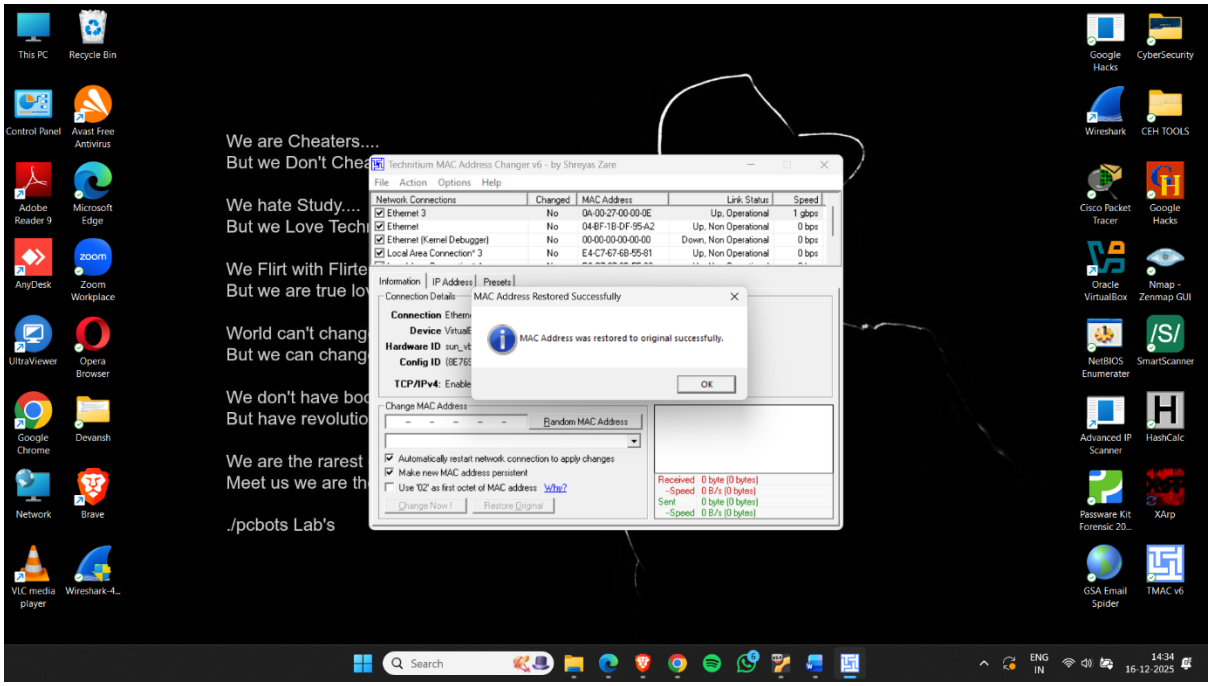


Figure 16

Perform MAC Spoofing using macchanger

How to use it -:

- Open kali linux
- Type sudo apt install macchanger
- To get detailed information about macchanger – man macchanger

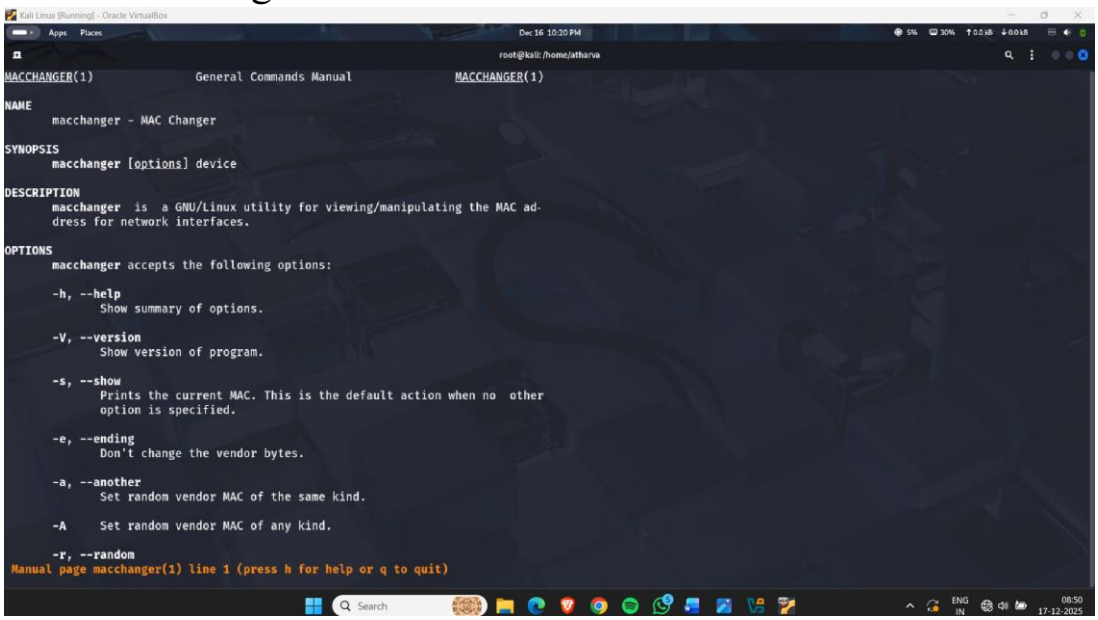


Figure 17

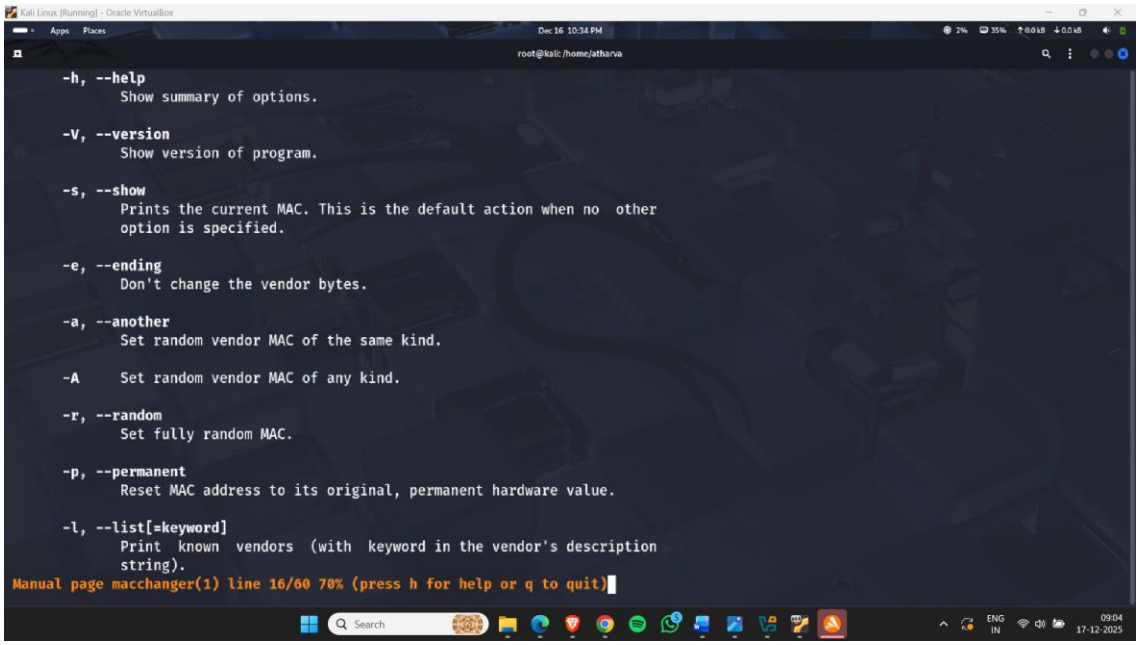


Figure 18

- Here some switches to generate random mac address

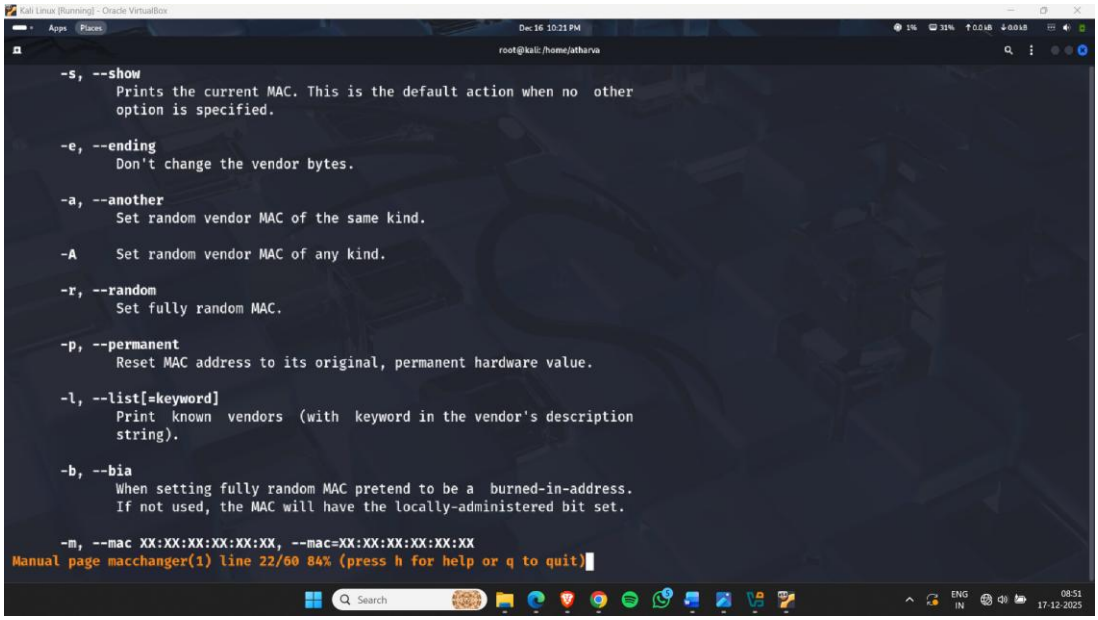


Figure 19

1)macchanger -r eth0 (-r – random)

2) macchanger -A eth0 (-A –random vendor mac of same kind)

3) macchanger -p eth0 (-p –permanent/original mac address)

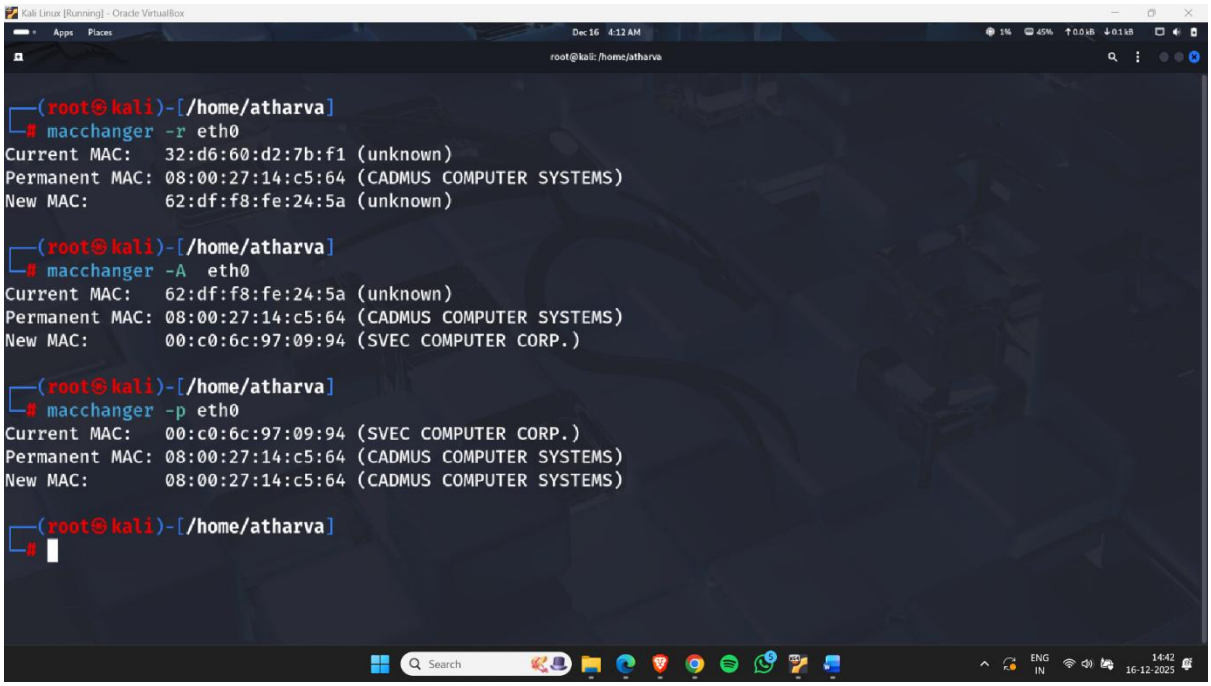


Figure 20

EXTRA TOOLS

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
- For Sending 1 packet:
  cmd – **send(IP(dst=target ip)/ICMP())**

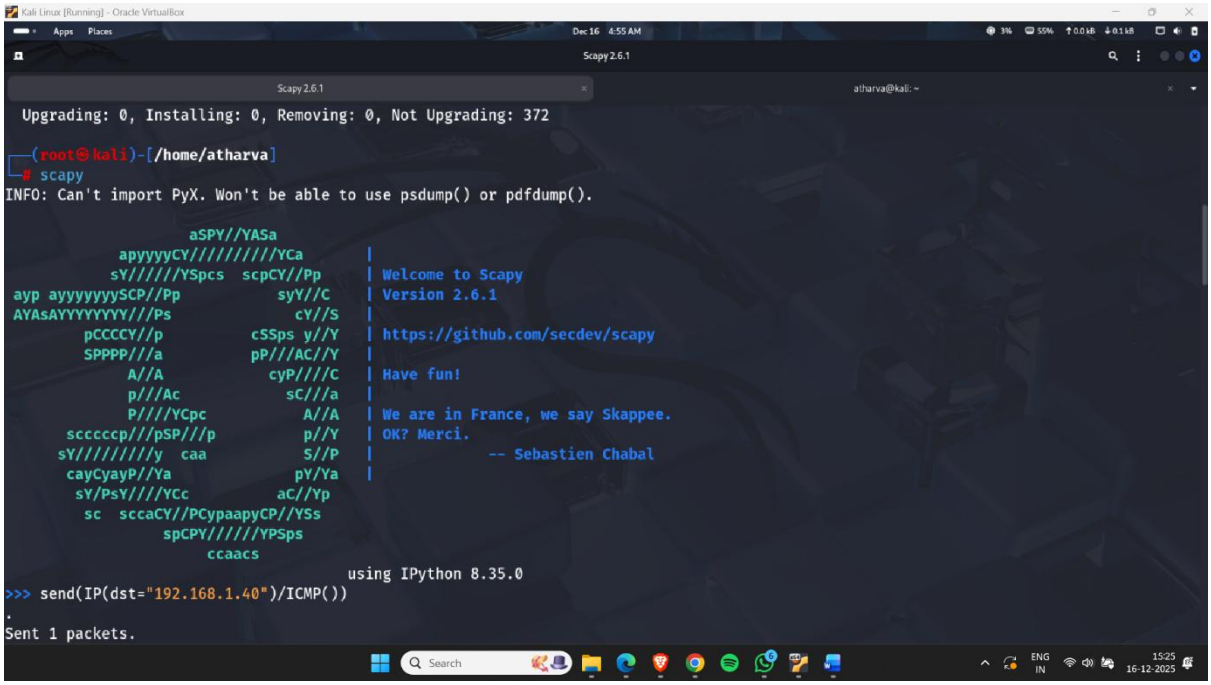


Figure 21

2) For sending Multiple packets:

cmd – **packet =IP(dst=”target ip ”)/ICMP())**
Send(packet,count=10000)

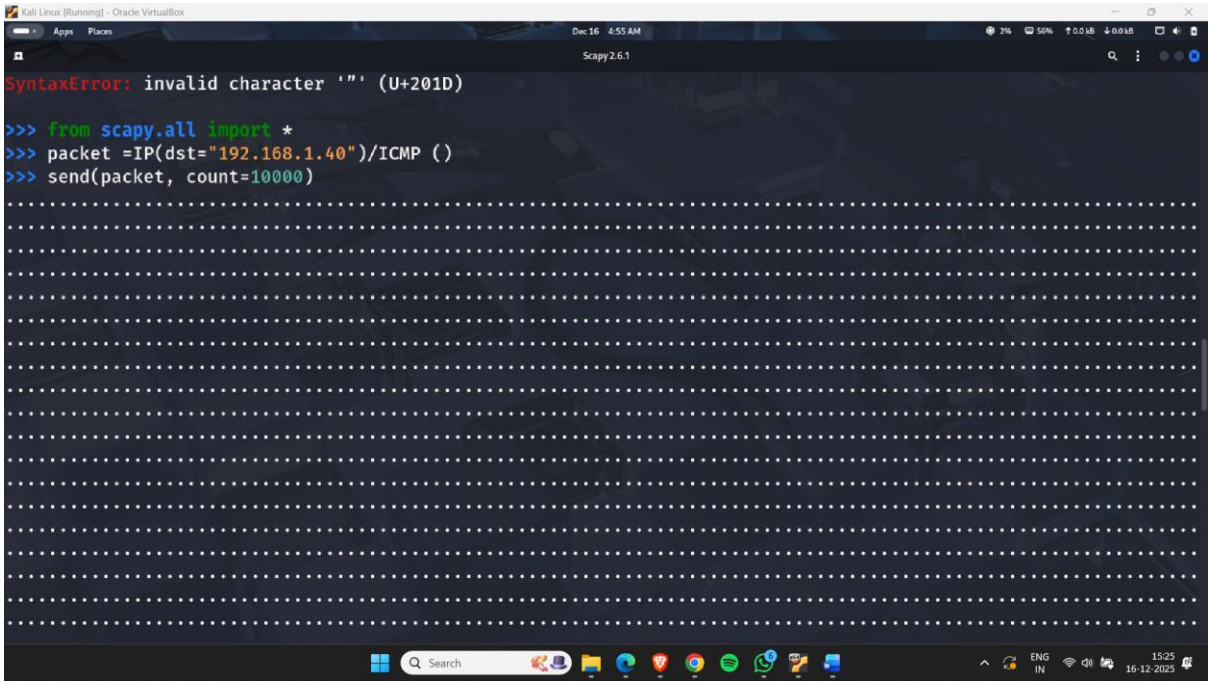


Figure 22

- Open Wireshark and you will see 10000 ICMP packets sending process begins…

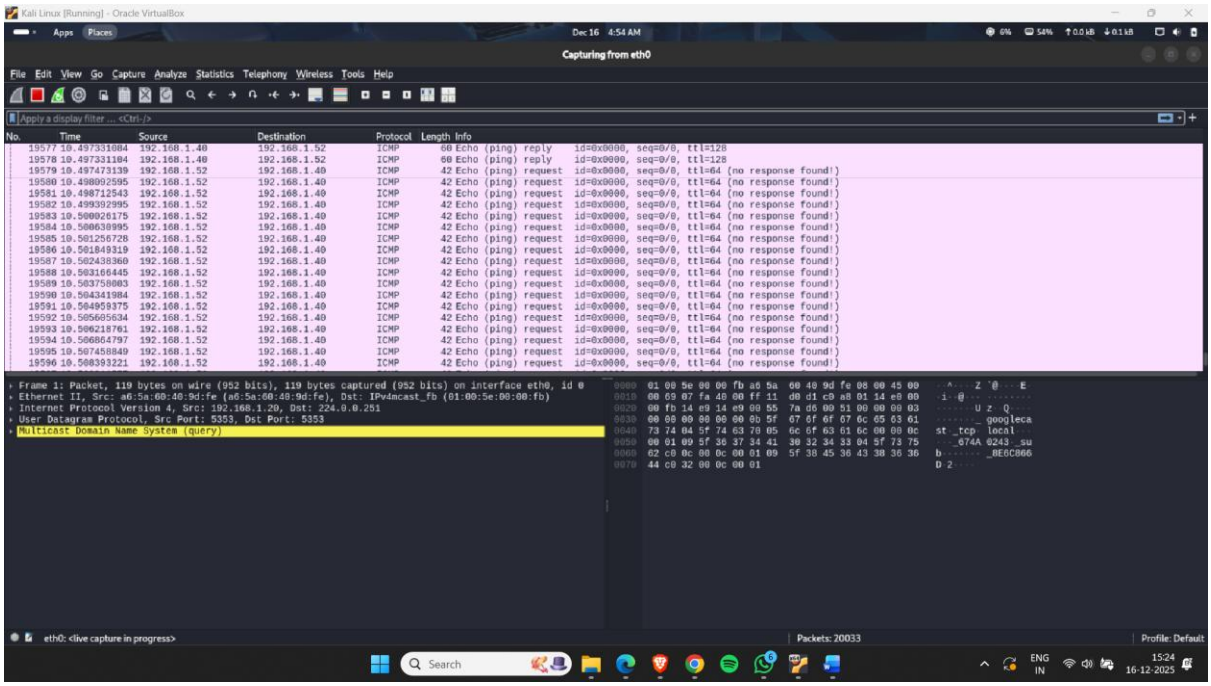


Figure 23

Perform MAC Flooding Using Hping3 (Linux Tool)

How to use it -:

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

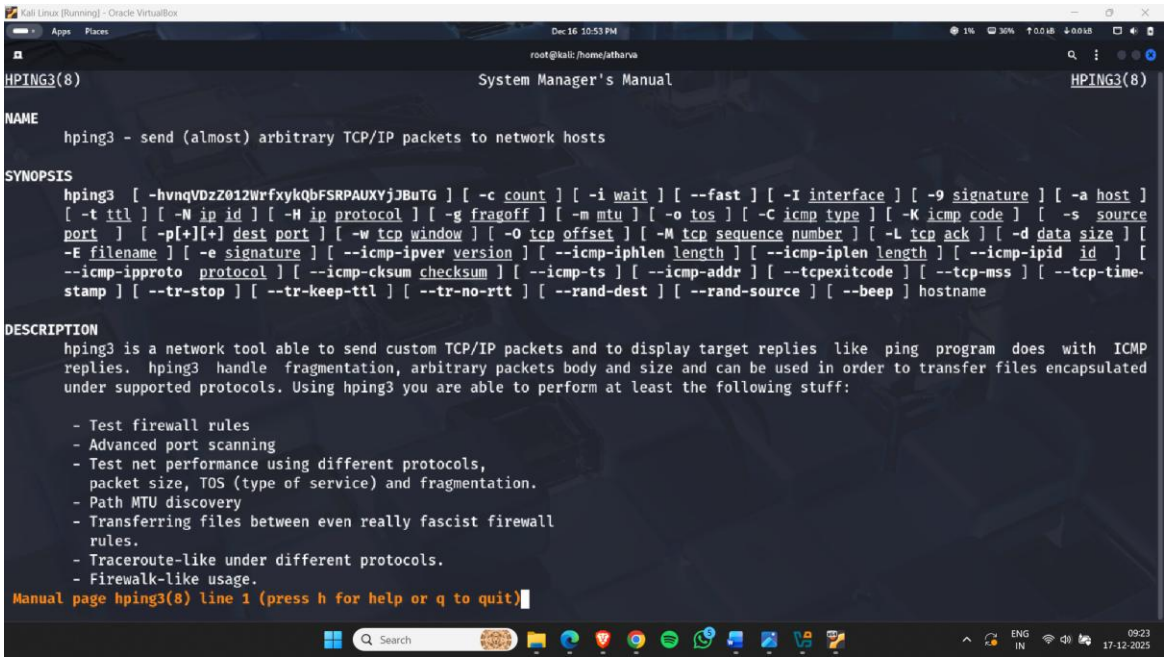


Figure 24

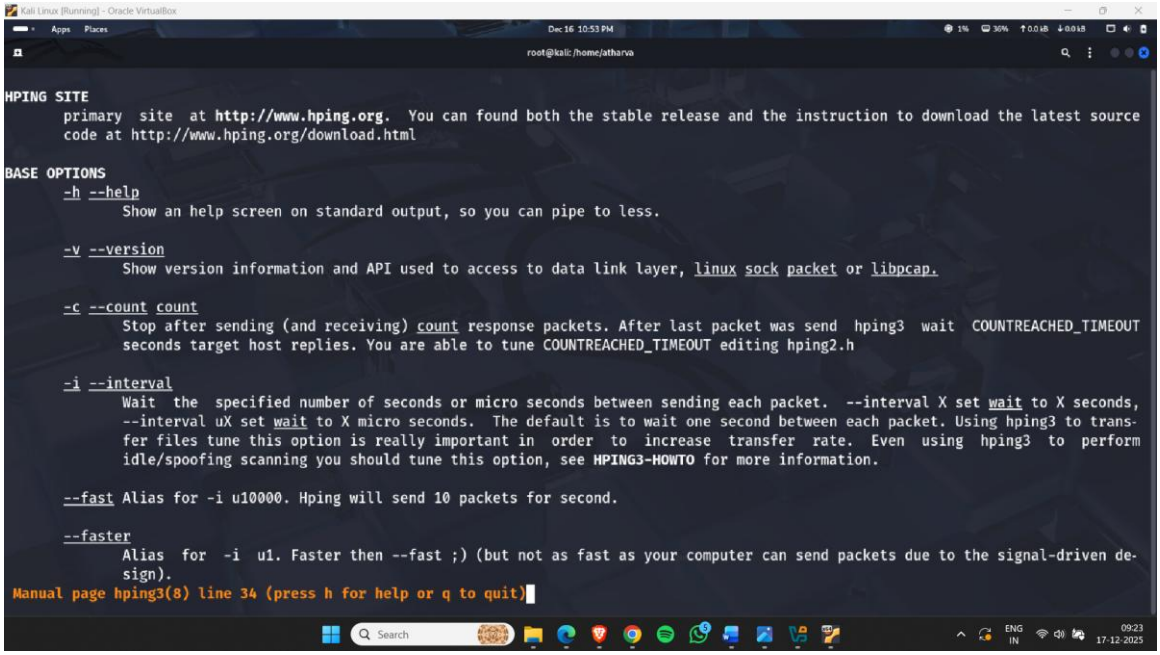


Figure 25

1)--fast

- Sends 10 packets per second.
- Use Case: Good for basic network discovery or testing firewall rules without overwhelming the target or your own CPU. It is slightly more aggressive than the default mode but still very "polite."

Command --: hping3 -1 192.168.1.40 --rand-source -p 80 --fast

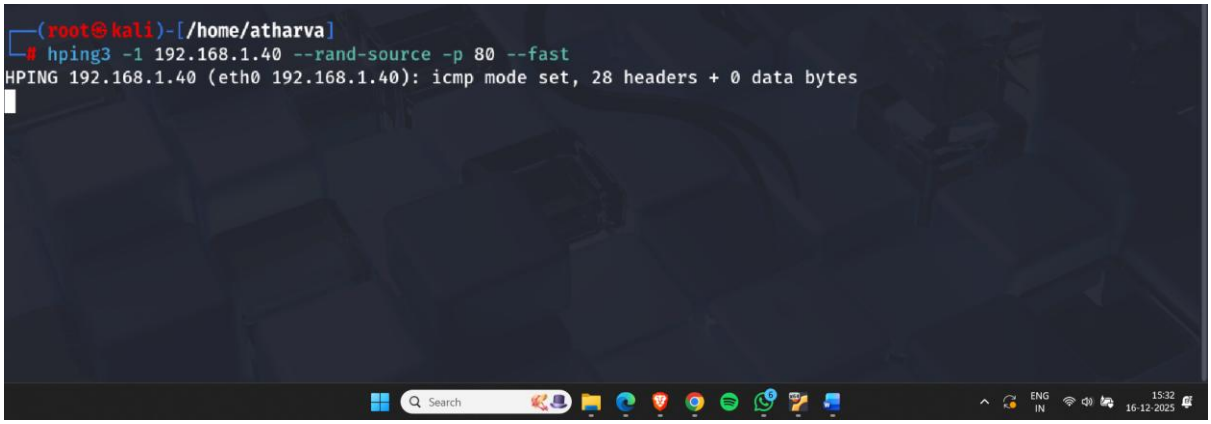


Figure 26

- Open Wireshark to analyse the packets….

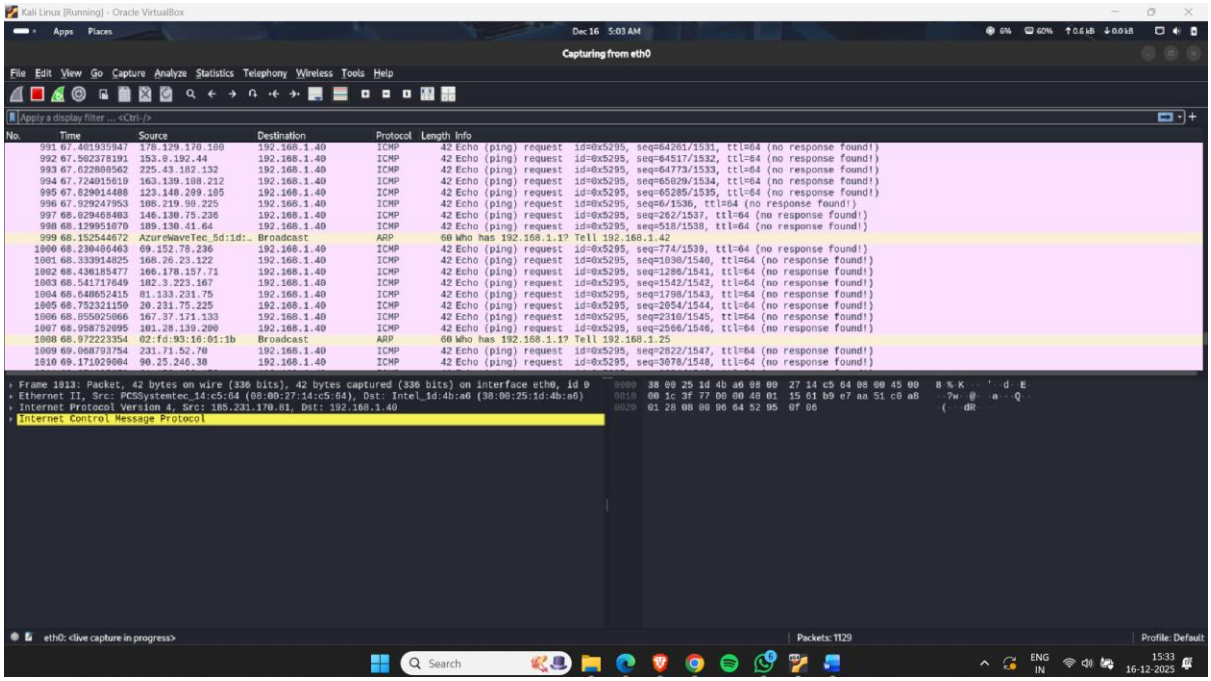


Figure 27

- Packets sent to the Target

2)--faster

- Sends 100 packets per second.
- Use Case: Useful for testing if a network device (like an entry-level router) can handle a moderate stream of traffic. It begins to consume more significant bandwidth and processing power.

Command -- hping3 -1 192.168.1.40 --rand-source -p 80 --faster

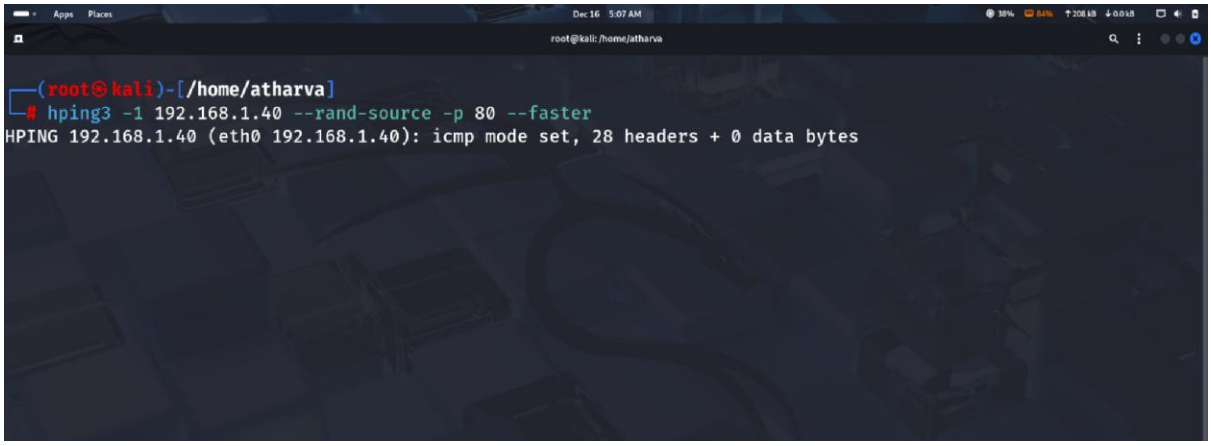


Figure 28

- Open Wireshark to analyse the packets….

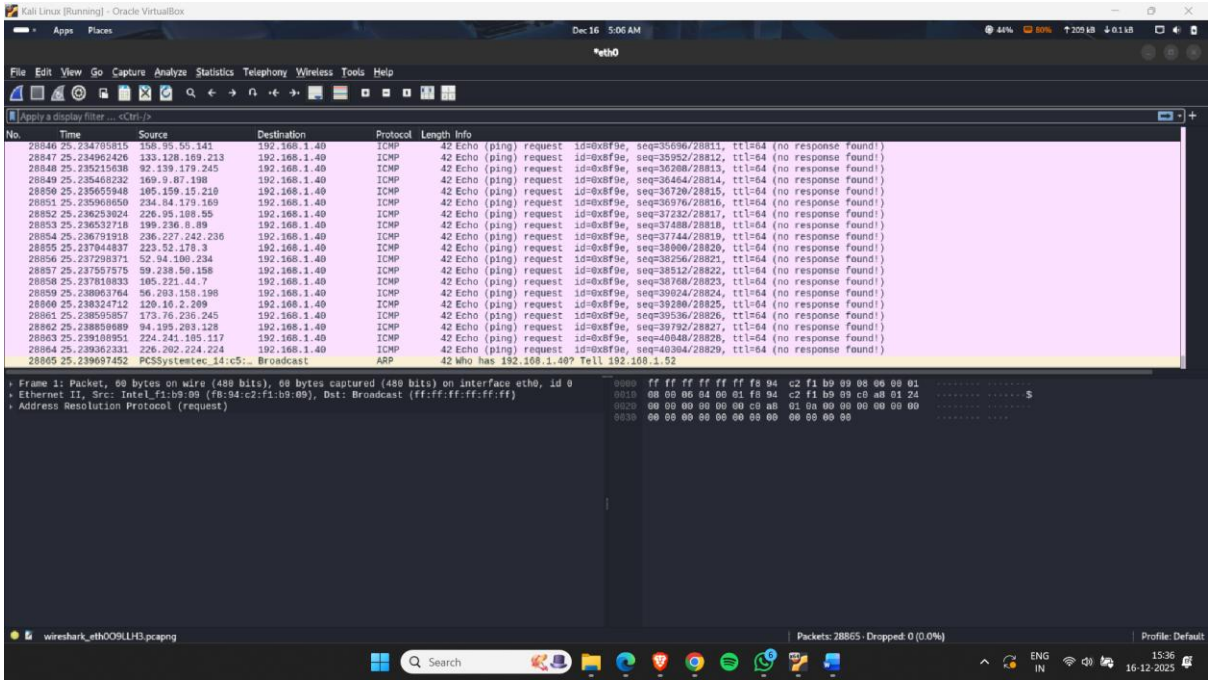


Figure 29

- Packets sent to the Target

3)—flood

- Sends packets as fast as possible (as fast as your CPU and network interface can push them out).
- Mechanism: It does not wait for any incoming replies; it simply blasts the target.This can easily crash a service, saturate a network link, or even cause your own machine to become unresponsive.

Command -: hping3 -1 192.168.1.40 --rand-source -p 80 --flood

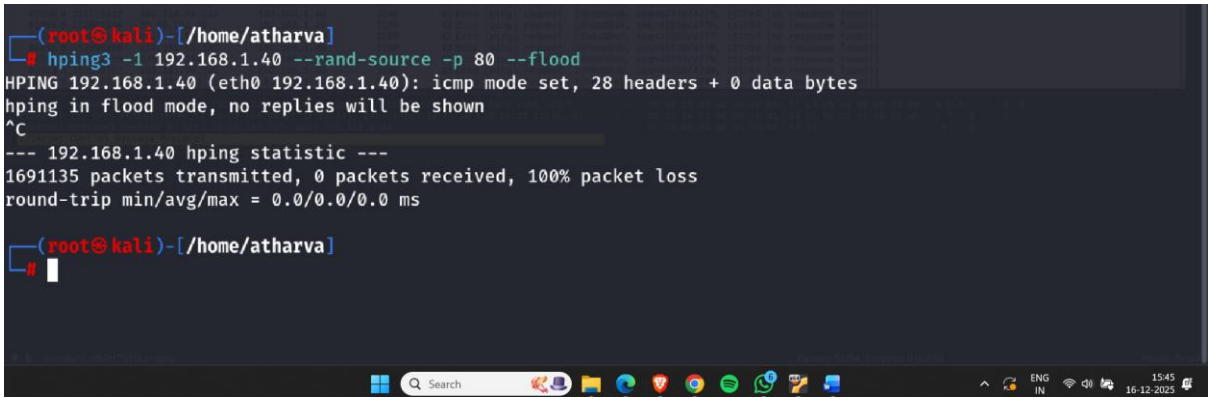


Figure 30

- Open Wireshark to analyse the packets….

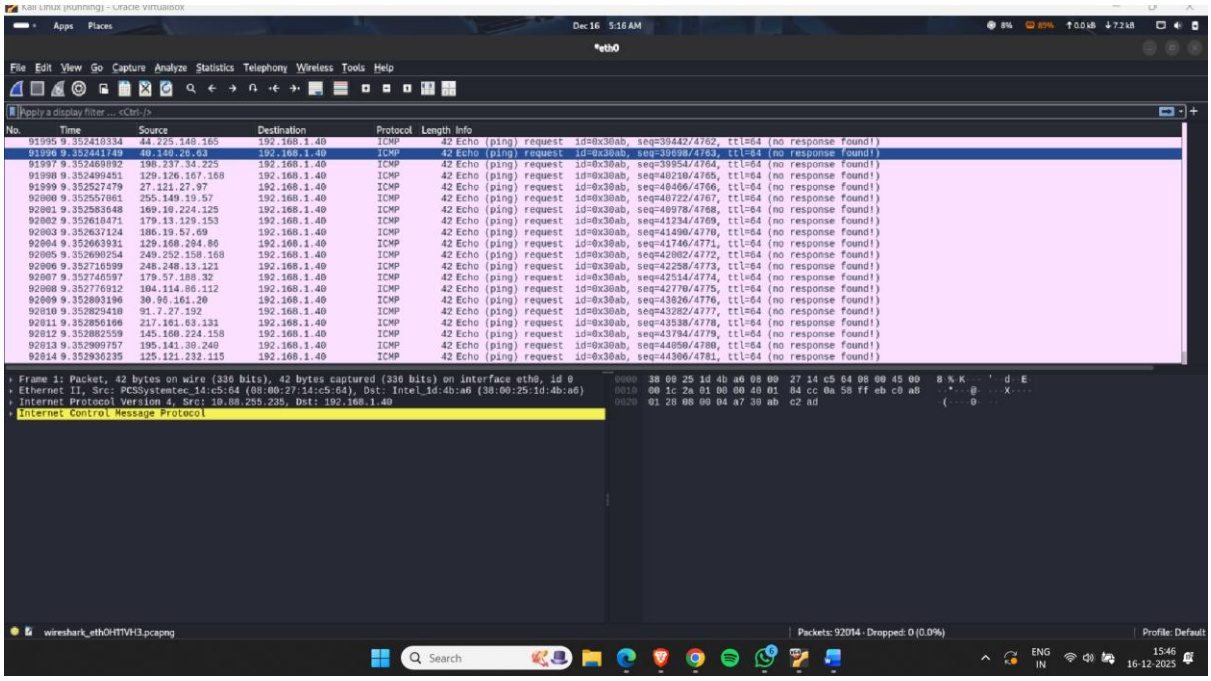


Figure 31

- Packets sent to the Target

Perform ARP Poisoning Using Ettercap

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

Figure 32

- Click on three dots and then click Plugins

Figure 33

- And then click on manage plugins

Figure 34

- Double click on rand_floor
- It will activate rand plugins

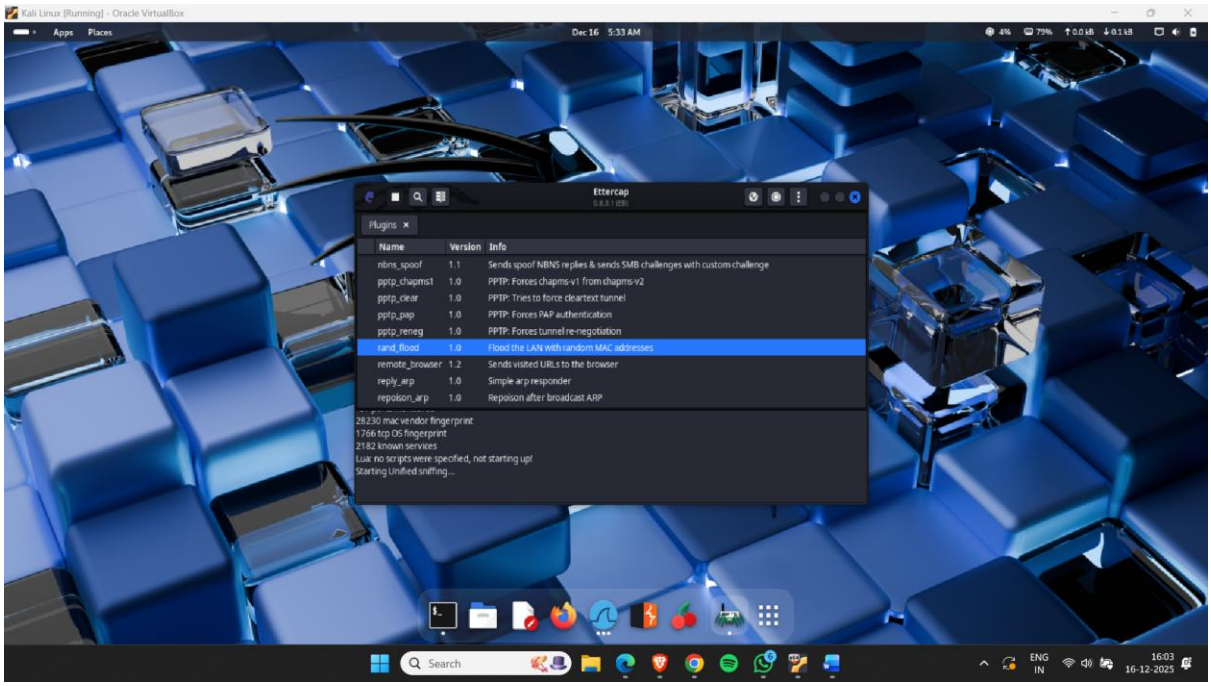


Figure 35

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

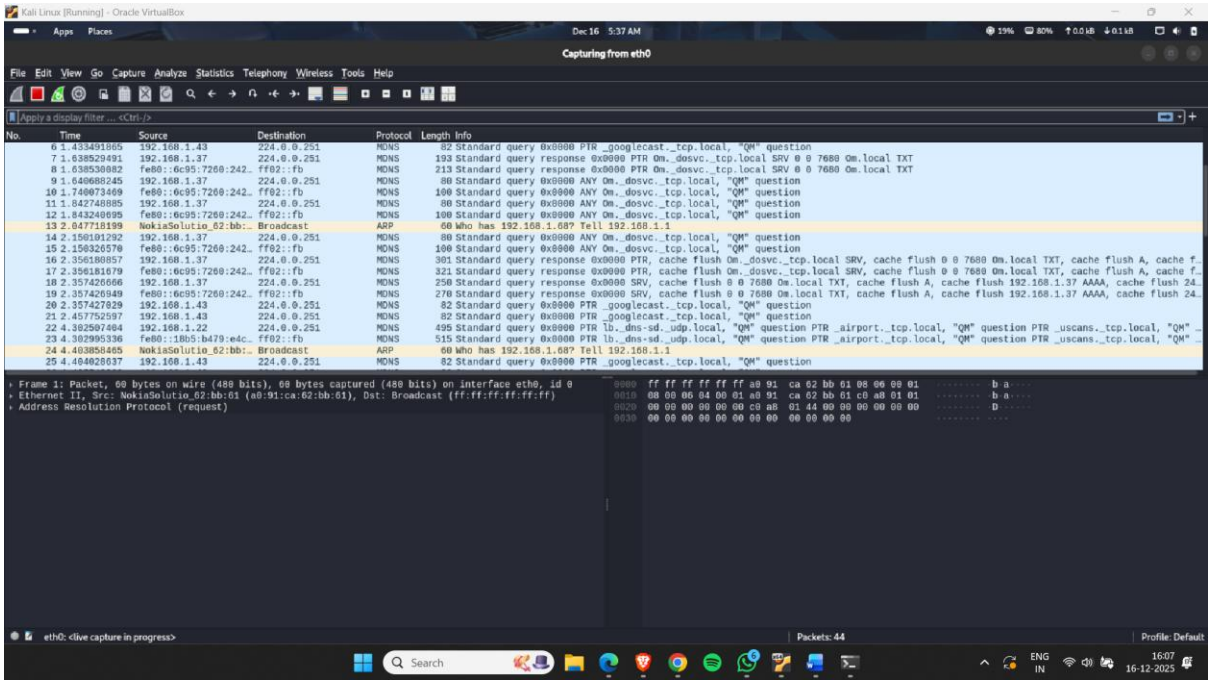


Figure 36

Perform ARP Poisoning 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

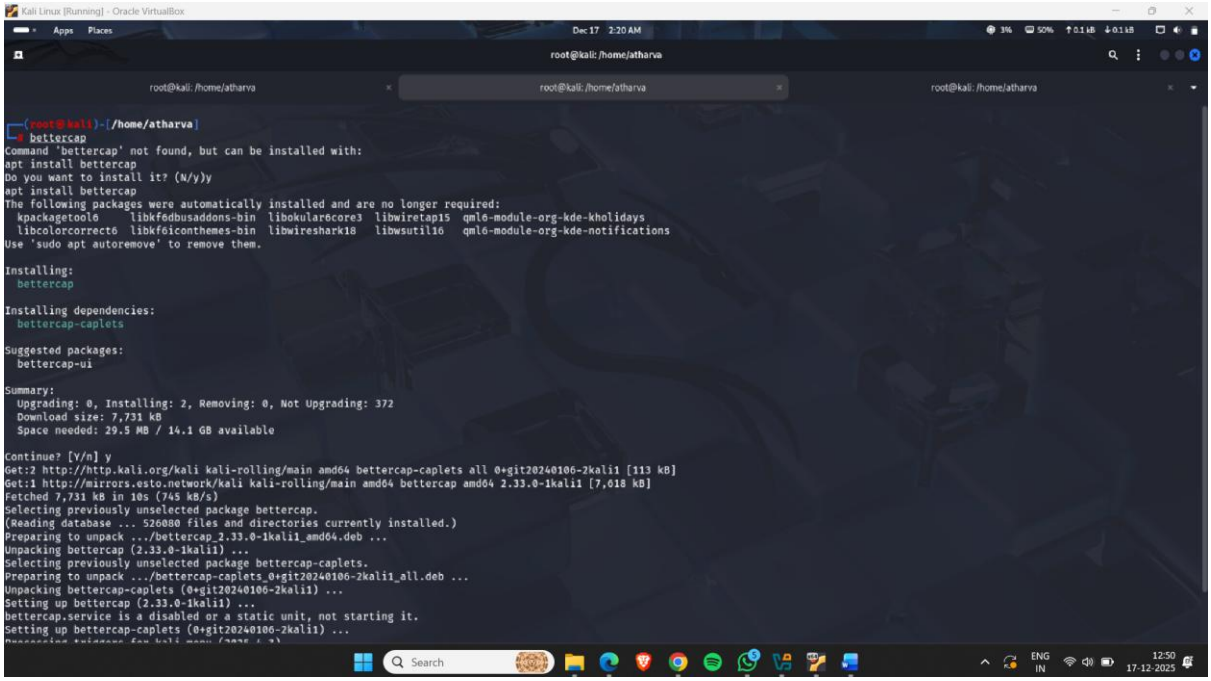


Figure 37

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

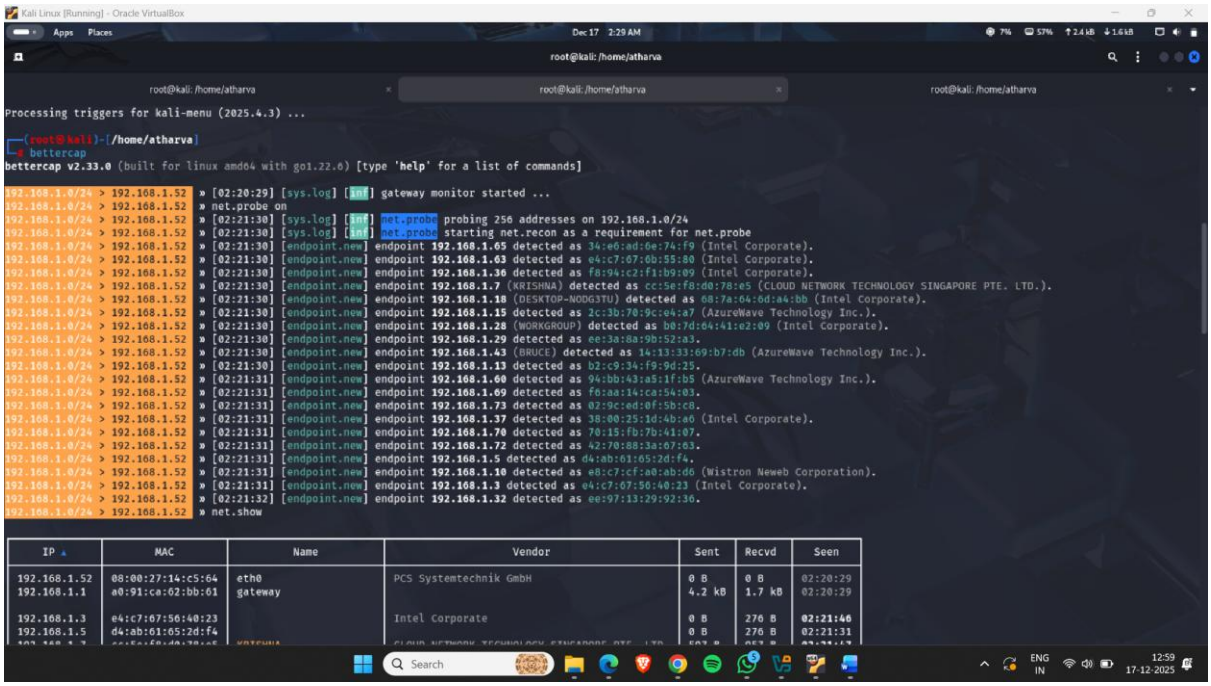


Figure 38

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

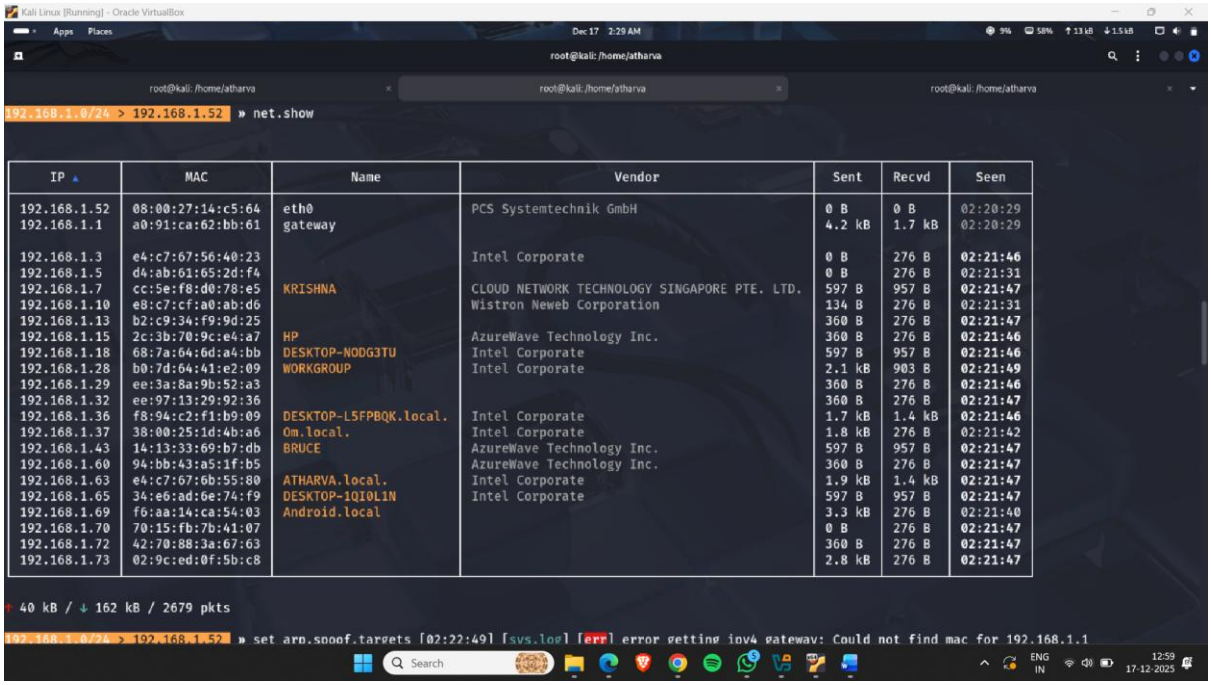


Figure 39

- Use arp.spoof.targets(target ip) to set your target

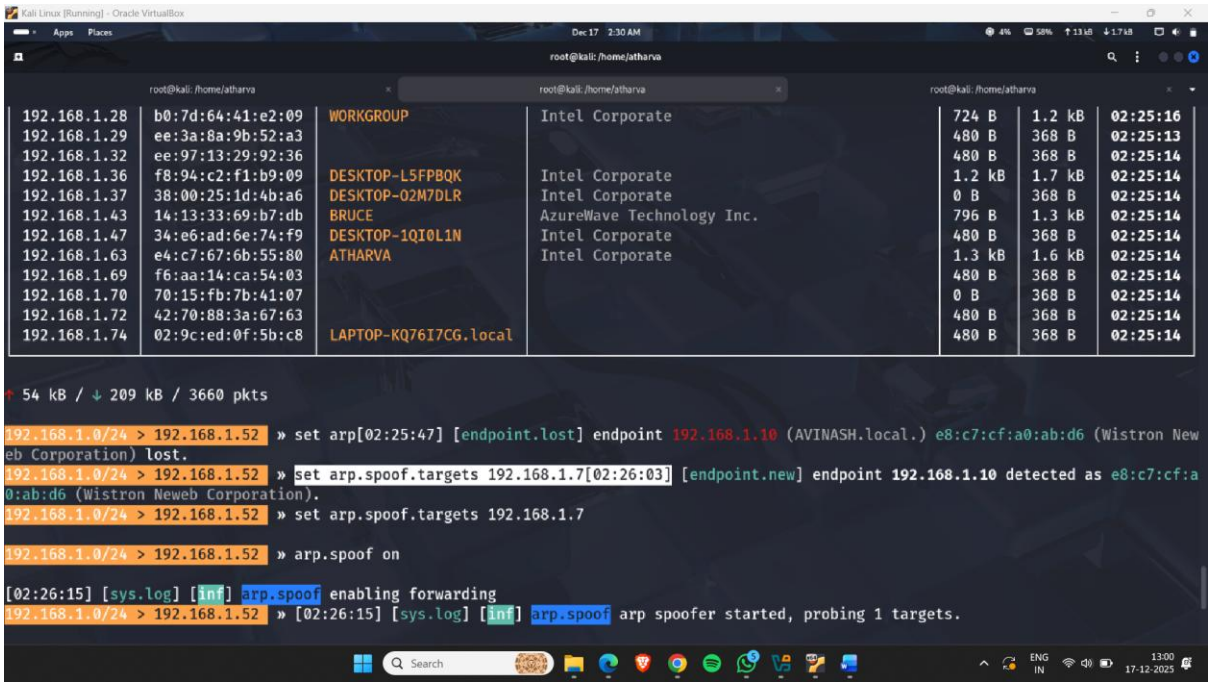
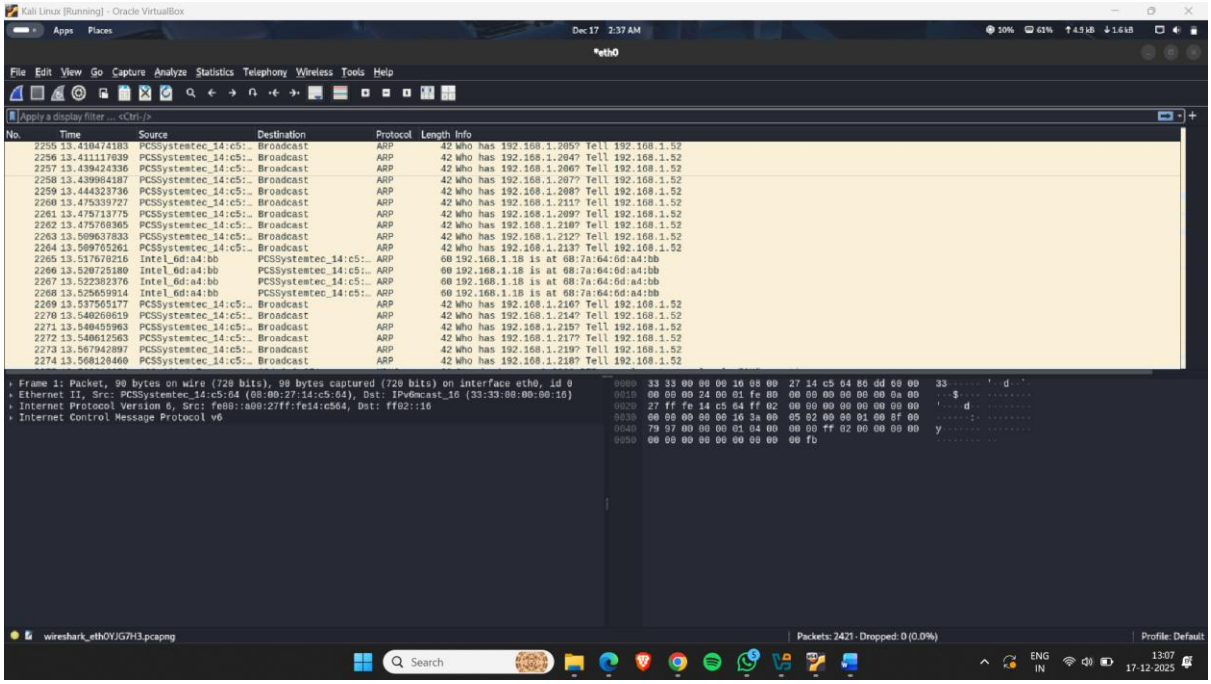


Figure 40

- Now open wireshark to see ARP packets are sent or not…



- ARP packets are sent ..