CY201 PROJECT REPORT

- **COURSE NAME:** CYBER SECURITY CONCEPTS AND PRINCIPLES
- **COURSE CODE :** CY201
- **SUBMITTED TO :** Abdullah Bin Zarshaid

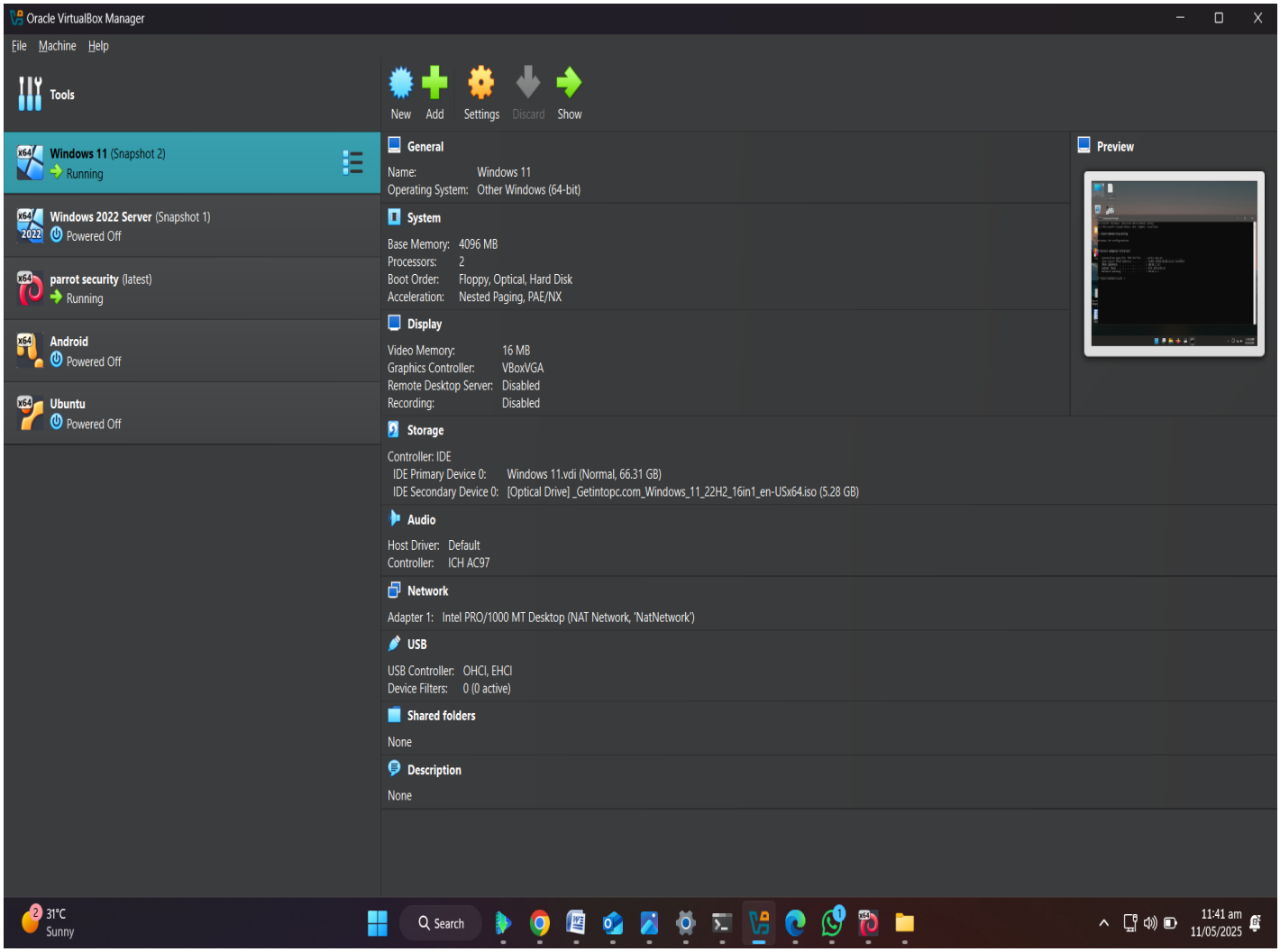
- **ASSIGNED LAB MODULES:**
  1. SNIFFING (MODULE 8)
  2. SOCIAL ENGINEERI NG (MODULE 9)

- **GROUP MEMBERS:**
  1. FAIZAN ALI 2023192
  2. MUJEEB U REHMAN2023558
  3. SHARIQ SAQIB 2023513

SNIFFING (MODULE 8)

➢ VIRTUAL MACHINES REQUIRED:

1. PARROT SECURITY OS
2. WINDOWS 11 VM
3. WINDOWS SERVER 2022
4. ANDROID VM
5. UBUNTU OS



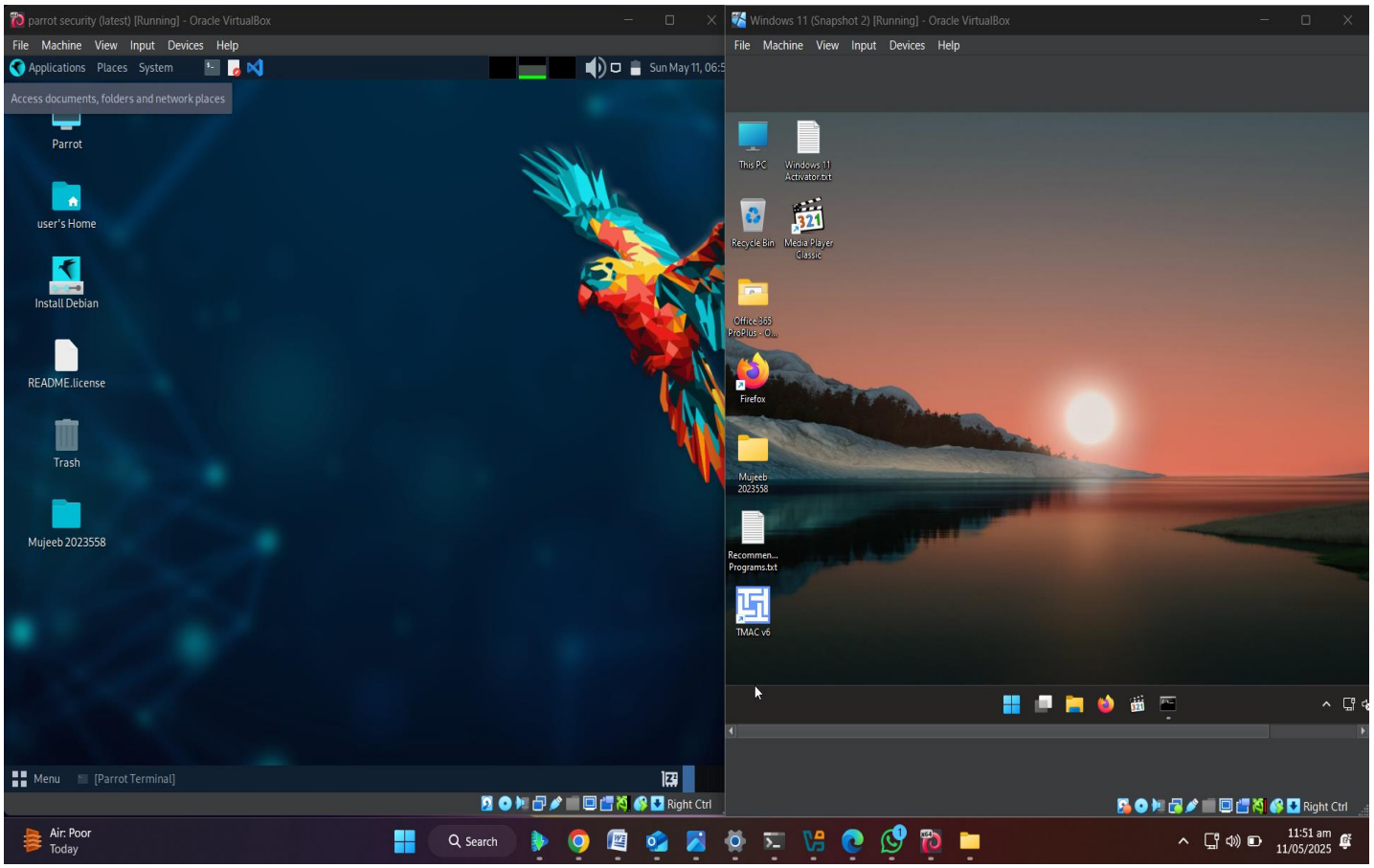
LAB 1 (PERFORM ACTIVE SNIFFING):

Lab Objectives :

1. Perform MAC flooding using macof
2. Perform a DHCP starvation attack using Yersinia
3. Perform ARP poisoning using arpspoof
4. Spoof a MAC address using TMAC and SMAC
5. Spoof a MAC address of Linux machine using macchanger

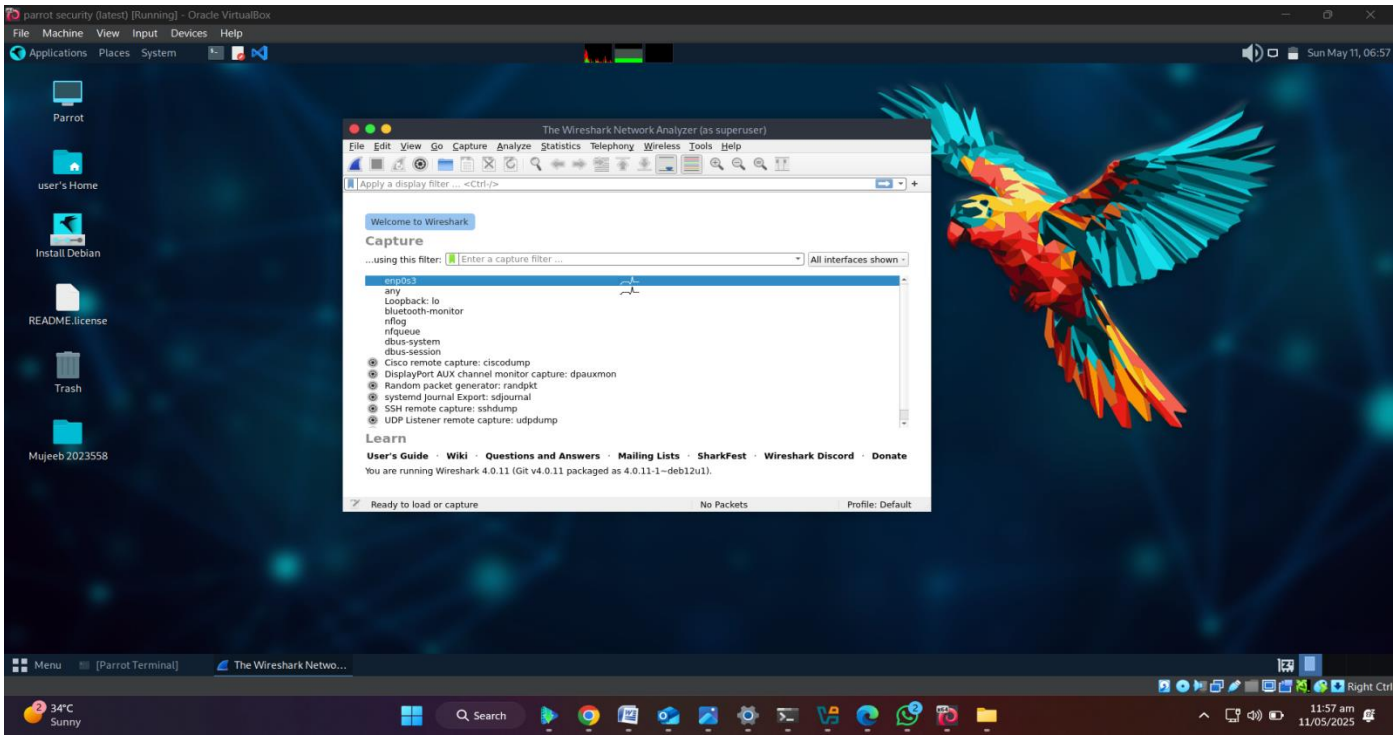
Task 1: Perform MAC Flooding using macof

➢ **STEP 1:** Turn on the Parrot Os and Windows 11 Virtual machines **:**

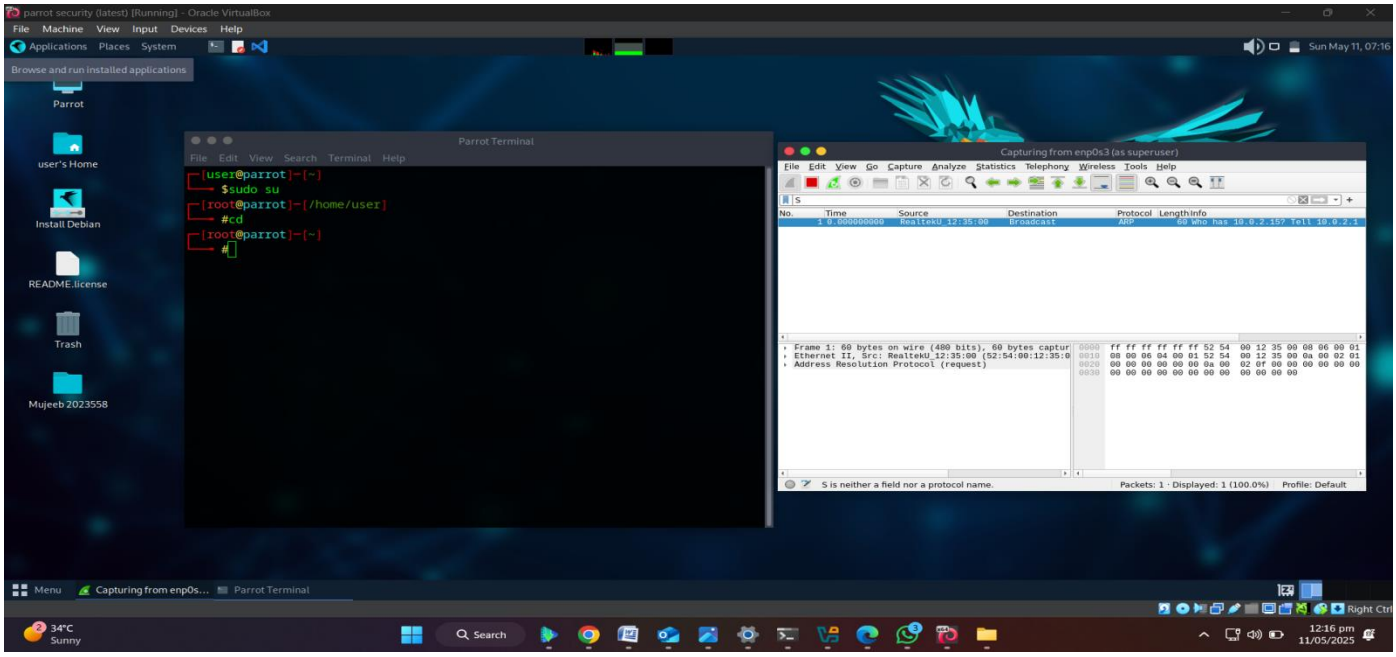


➢ Step 2 (Open Wireshark in Parrot Os) :

1. Click Applications in the top-left corner of Desktop and navigate to Pentesting -> Information Gathering ->wireshark.



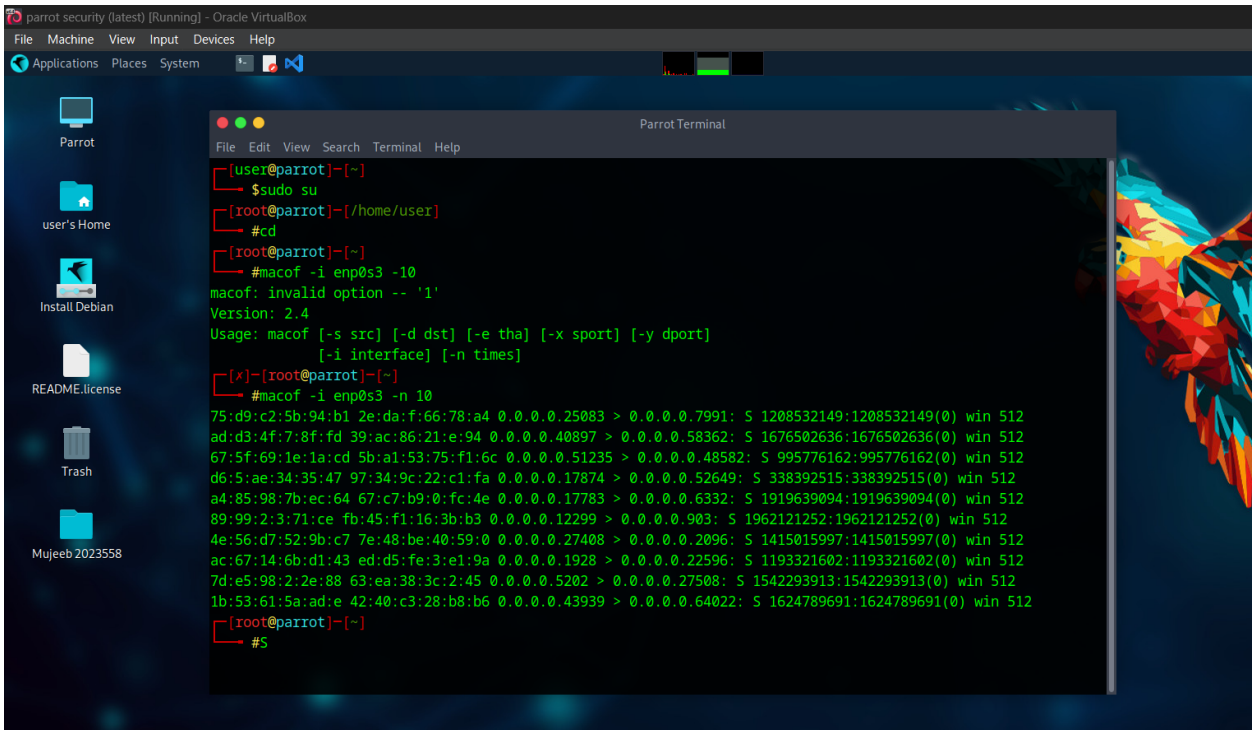
2. Double click on enp0s3 and leave the wireshark runningin background.
3. Open Terminal and type **sudosu** and press enter then type **cd** and press enter.



➢ STEP 3 (Type command for MAC Flooding in terminal):

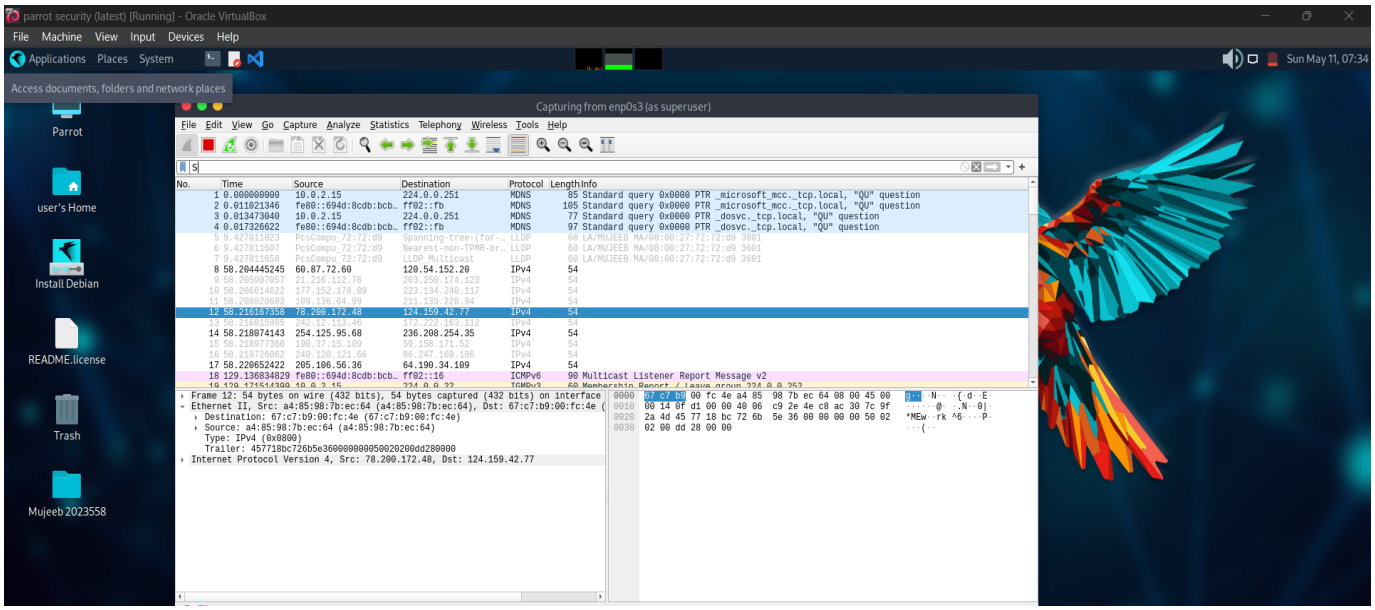
The Parrot Terminal window appears; type **macof -i enp0s3 -n 10** and press Enter.

Note: -i specifies the interface and -n: specifies the number of packets to be sent (here,10).



➢ STEP 4(ANALYZE PACKETS):

Open **WireShark** and Click on **IP4** packets captured and Click on **Ethernet 2** and see the **Source** and **Destination IP** address and **MAC** address.

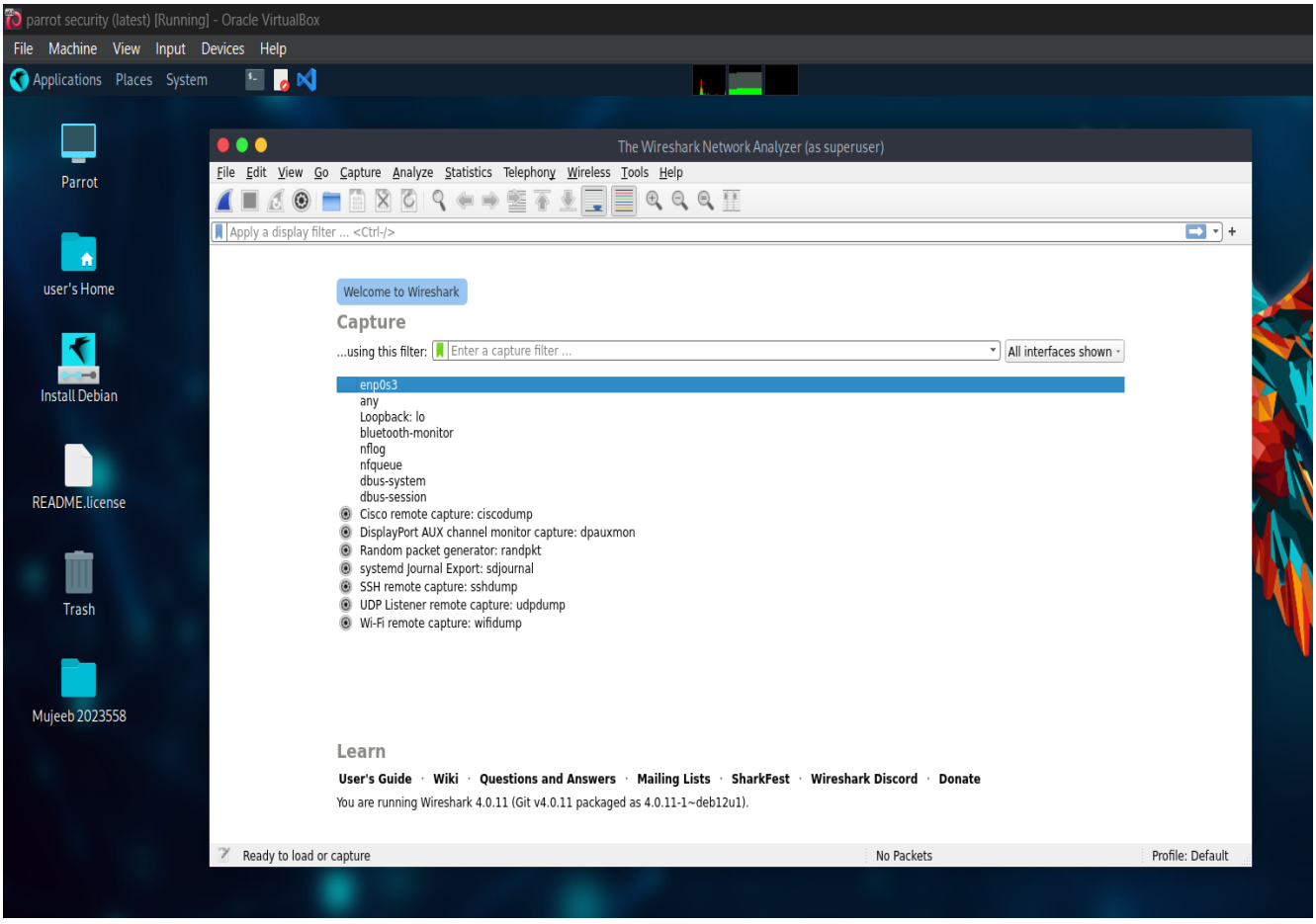


- Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.
- Close the wireshark and save the packets if you want.

TASK 2 : Perform a DHCP Starvation Attack using Yersinia

➢ Step 1 (Turn Machines On) :

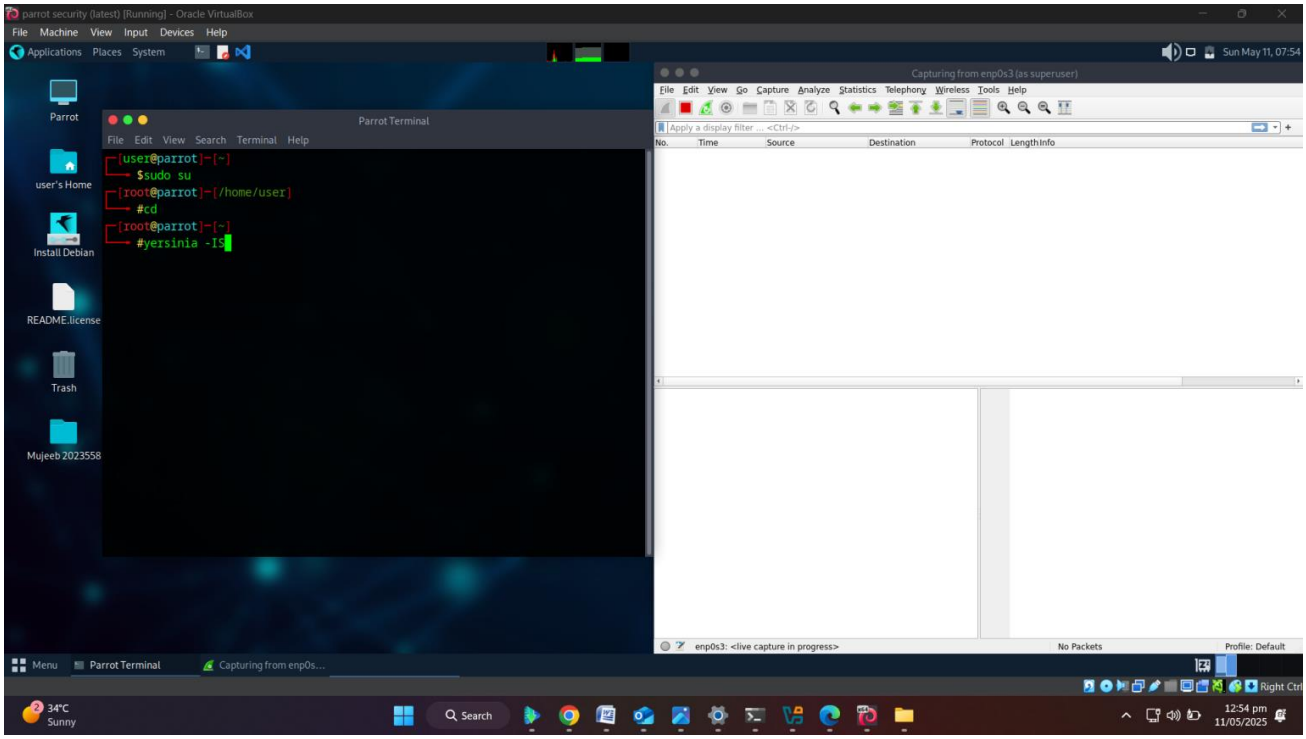
1. Turn on Parrot Os and Open Wireshark (click Applications in the top-left corner of Desktop and navigate to Pentesting-> Information Gathering ->wireshark.)



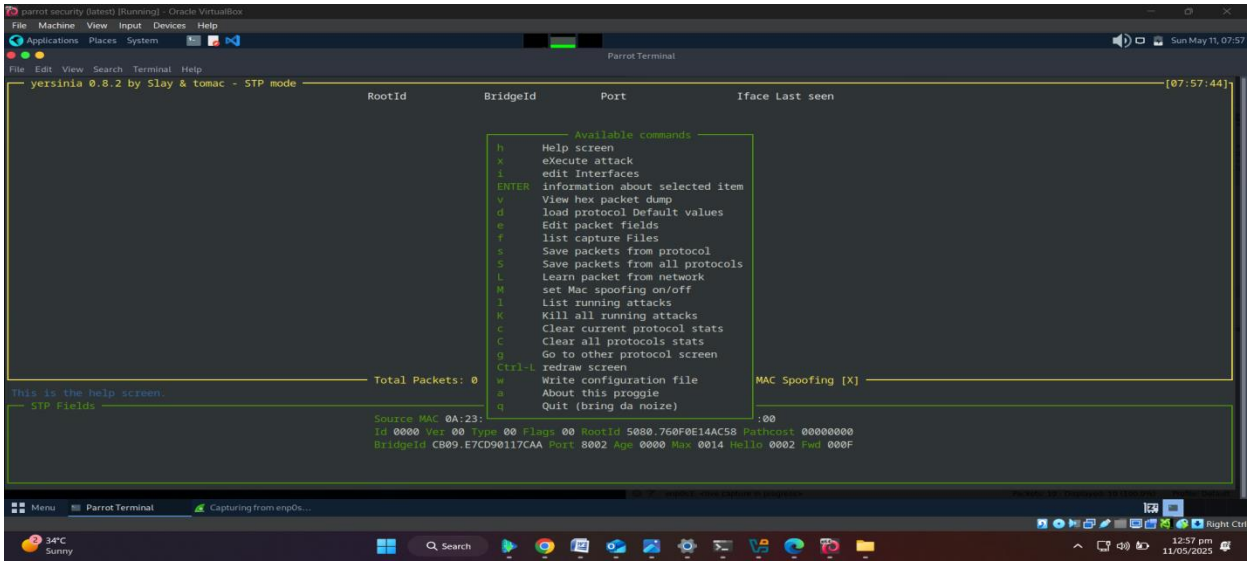
2. Double click enp0s3 and leave the WireShark Running in the background.

➢ STEP 2 (Perform Attack) :

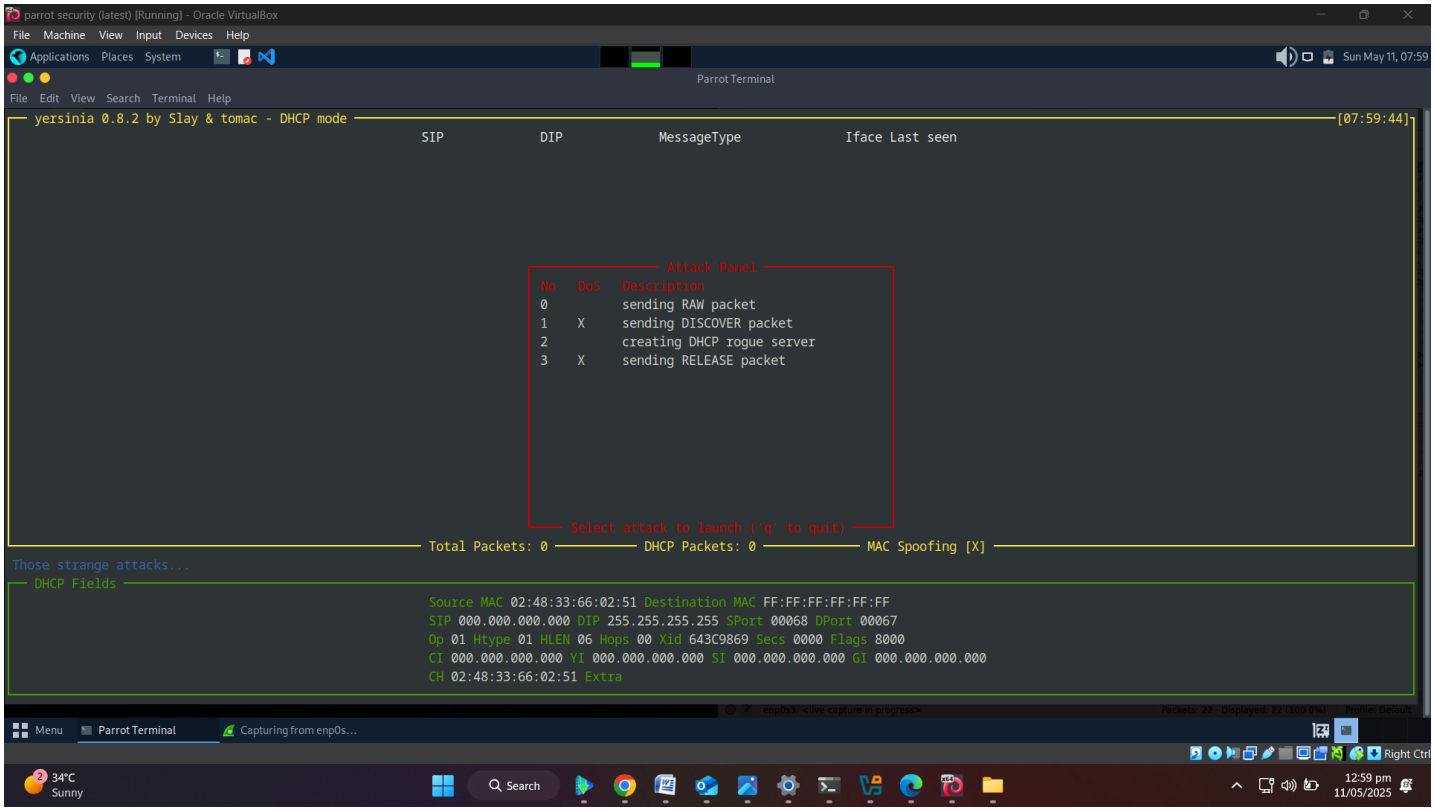
1. Open **Terminal** , Type **sudosu** and press enter and then type cd to jump into root directory.
2. Type **yersinia -I** and press Enter to open **Yersinia** in interactive mode. Note:
   -I: Starts an interactive session.



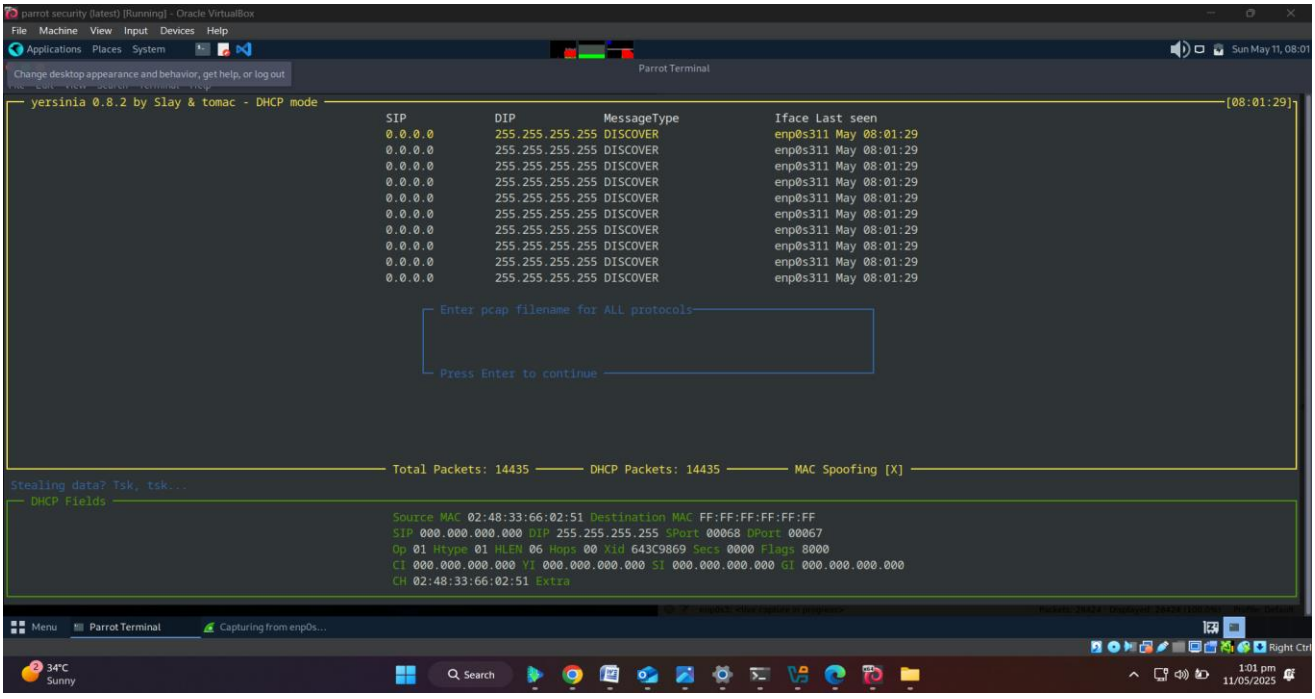
3. Yersinia Interactive mode will appear:



4. Press f2 To enter the DHCP mode and then press x to execute the attack.

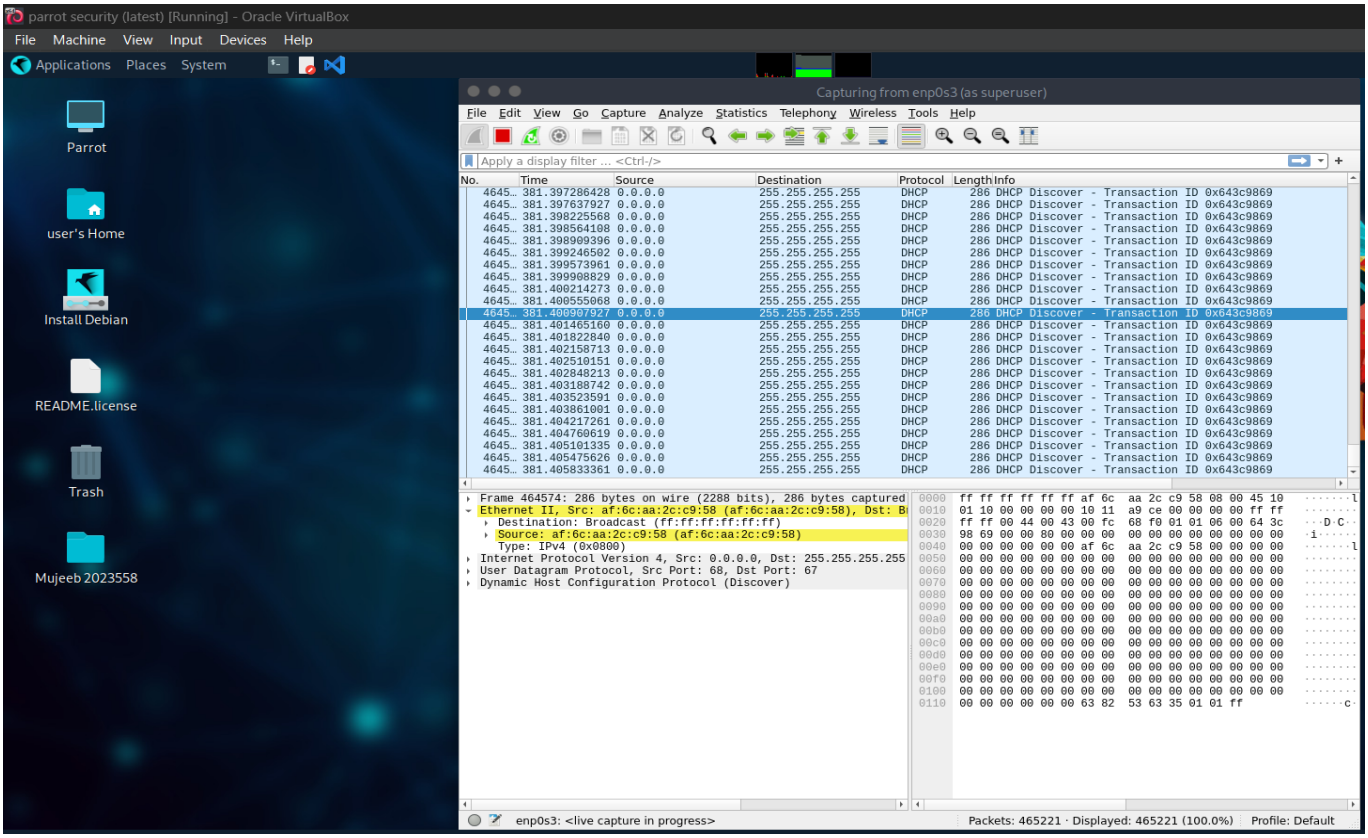


5. The Attack Panel window appears; press 1 to start a DHCP starvation attack.



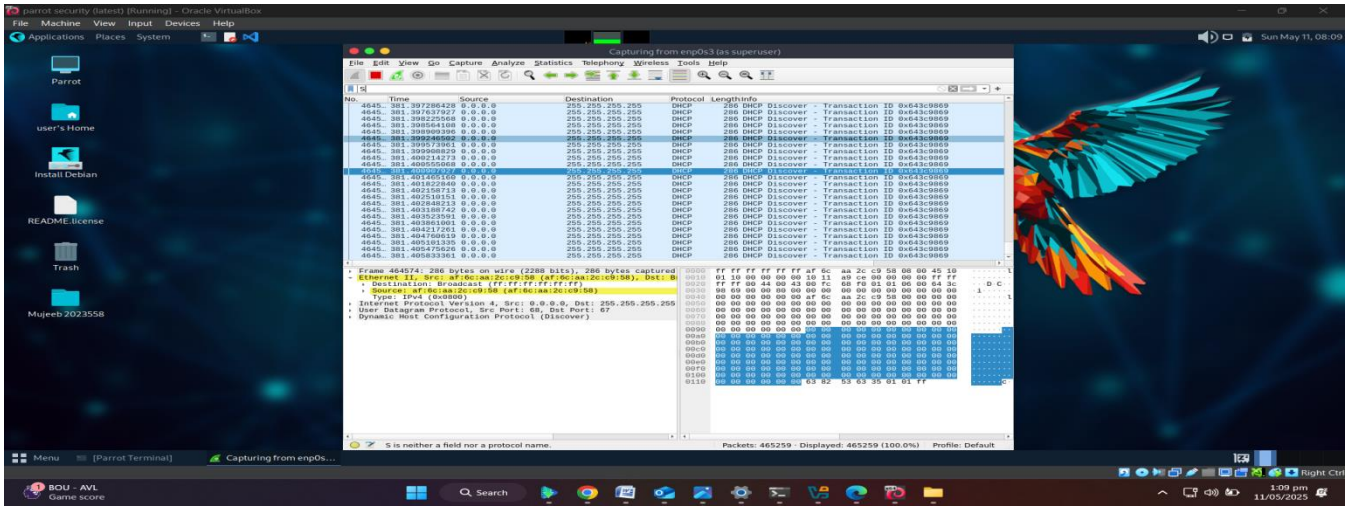
6.Press q to Stop the attack.

7. Now, switch to the Wireshark window and observe the huge number of captured DHCP packets, as shown in the screenshot.



➢ Step 3 (Analyze Attack):

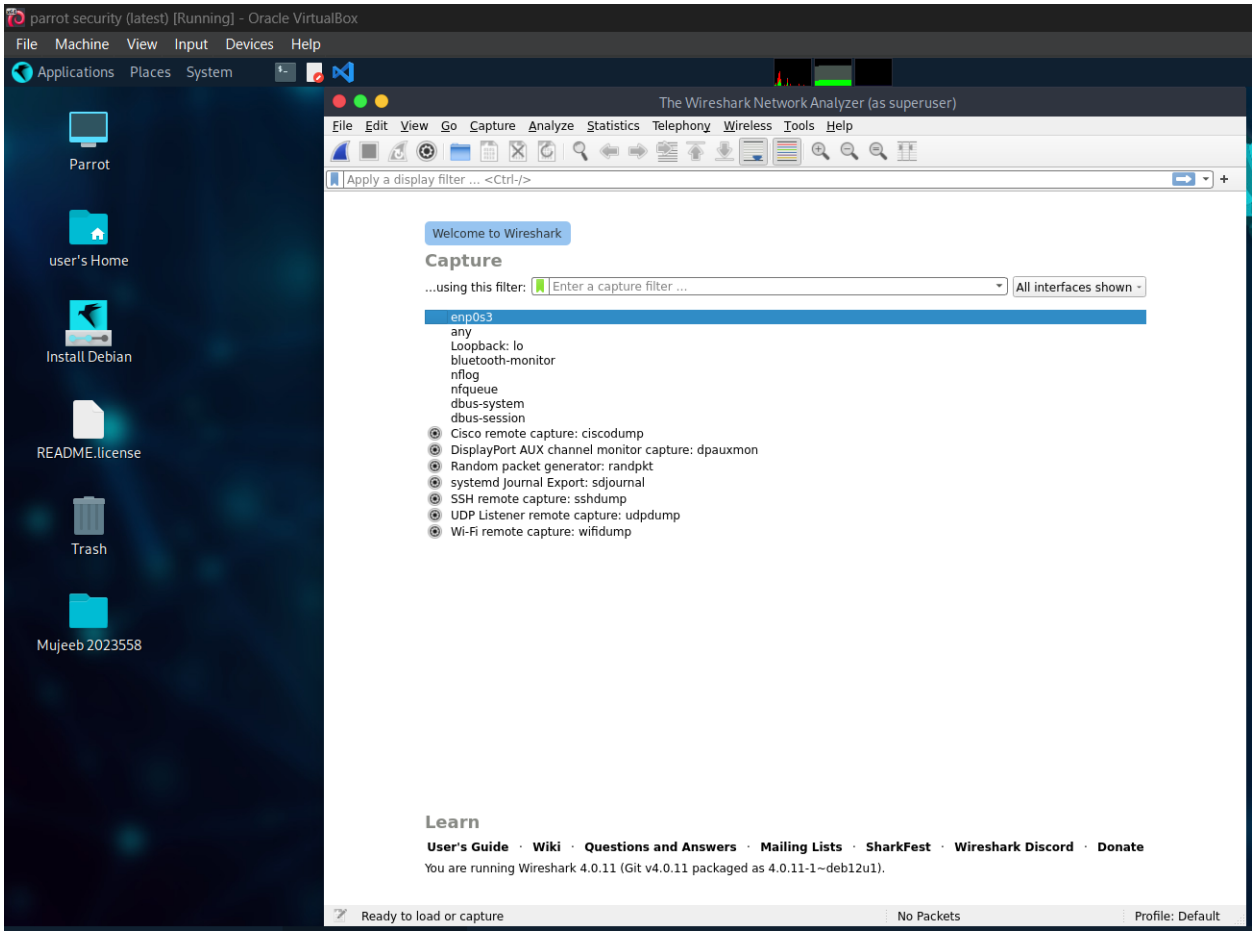
Click on any DHCP packet and expand the Ethernet II node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



Task 3: Perform ARP Poisoning using arpspoof

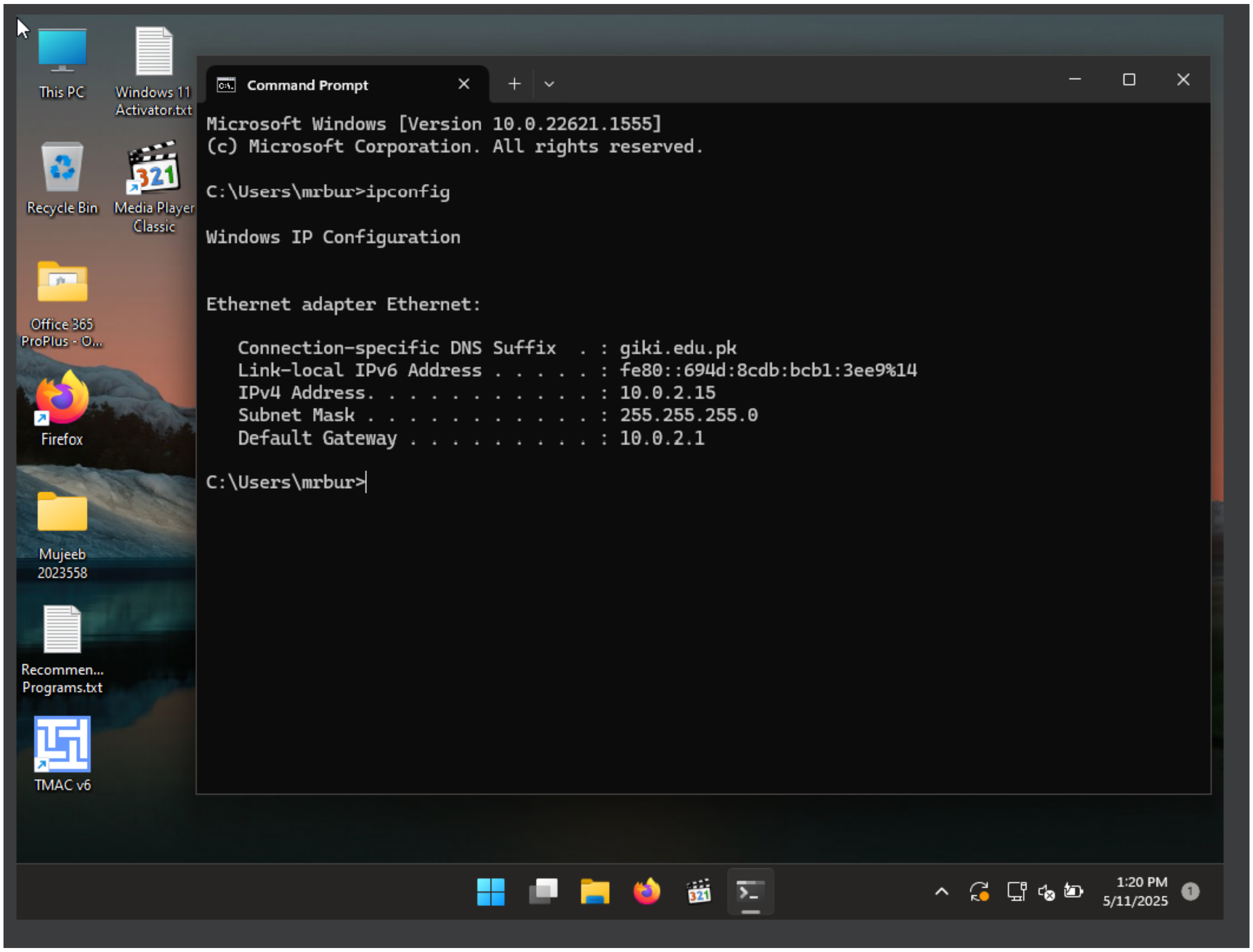
➢ Step 1 (turn on the machines):

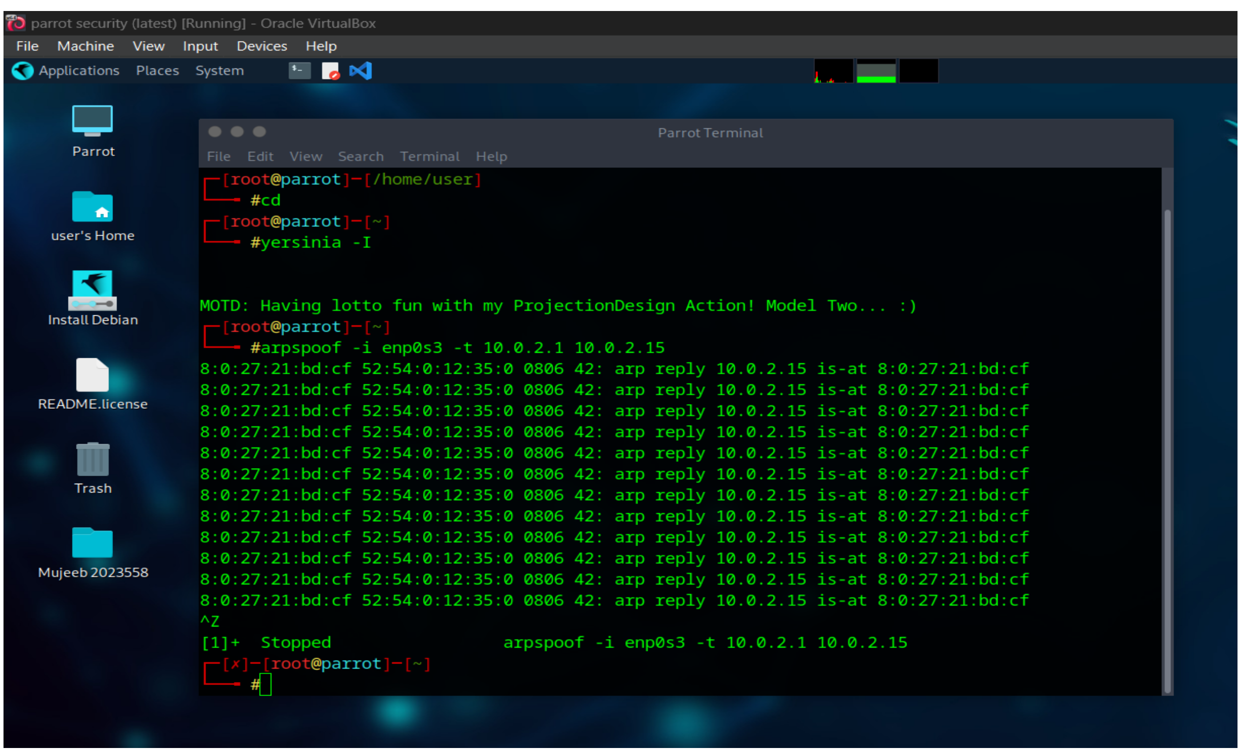
1. Turn On the parrot Os and Windows 11.
2. Open Wireshark in Parrot OS.
3. Double click the enp0s3 and leave the wireshark open in background.



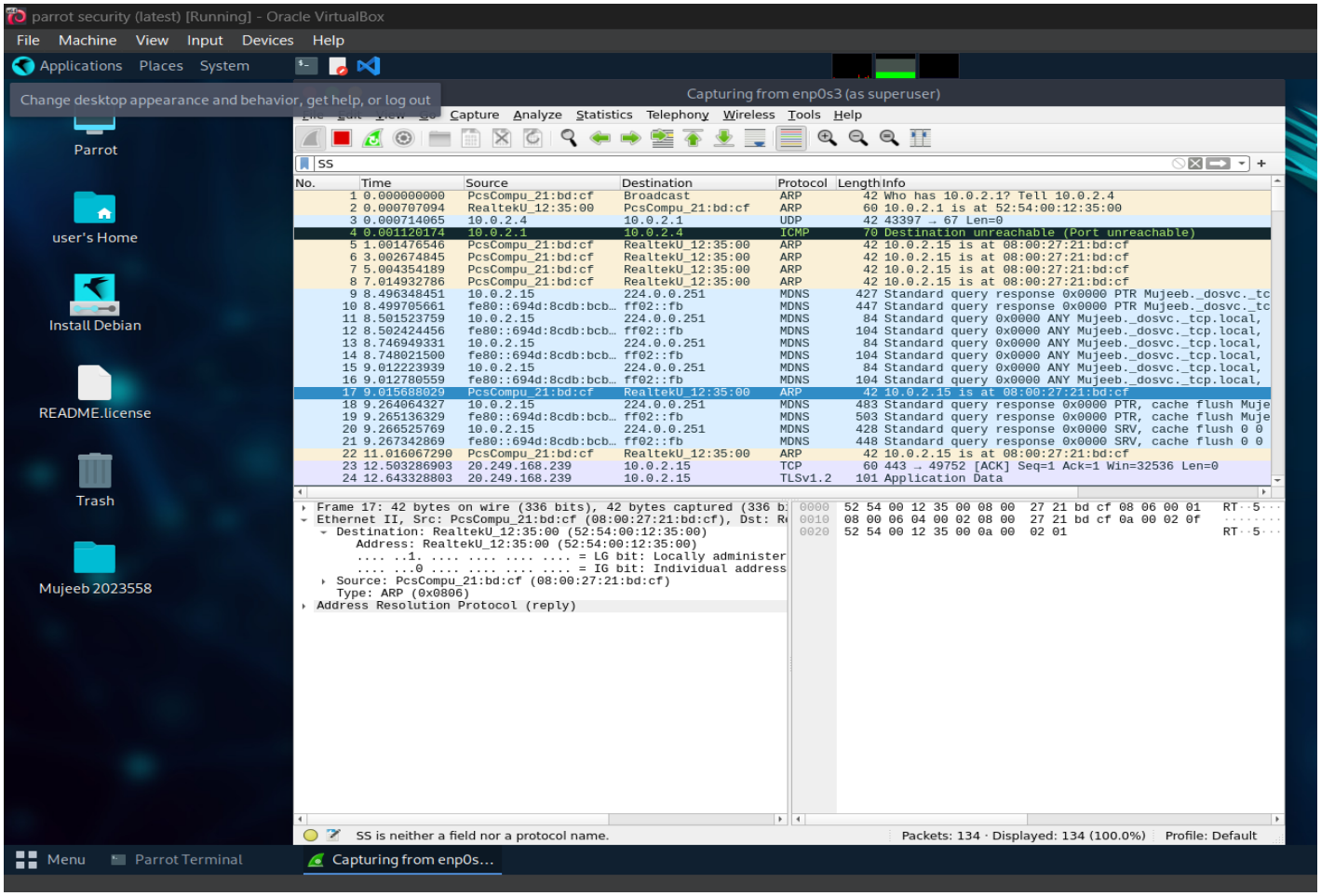
➢ Step 2 (Perform Attack):

1. Open **Terminal** , Type **sudosu** and press enter and then type **cd** to jump into root directory.
2. In the Terminal window, type **arpspoof -i enp0s3 -t 10.0.2.1 10.0.2.15** and press Enter. (Here, **10.0.2.15**is IP address of the target system [Windows 11], and **10.0.2.1** is IP address of the access point or gateway) Note: -i: specifies network interface and -t: specifies target IP address.


This PC
Windows 11 Activator.txt
Recycle Bin
Media Player Classic
Office 365 ProPlus - O...
Firefox
Mujeeb 2023558
Recommen... Programs.txt
TMAC v6
Command Prompt
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.
C:\Users\mrbur>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : giki.edu.pk
Link-local IPv6 Address . . . . . : fe80::694d:8cdb:bcb1:3ee9%14
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 10.0.2.1
C:\Users\mrbur>
1:20 PM
5/11/2025


parrot security (latest) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot
user's Home
Install Debian
README.license
Trash
Mujeeb 2023558
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/user]
#cd
[root@parrot]-[~]
#yersinia -I
MOTD: Having lotto fun with my ProjectionDesign Action! Model Two... :)
[root@parrot]-[~]
#arpspoof -i enp0s3 -t 10.0.2.1 10.0.2.15
8:0:27:21:bd:cf 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:21:bd:cf
^Z
[1]+ Stopped arpspoof -i enp0s3 -t 10.0.2.1 10.0.2.15
[x]-[root@parrot]-[~]
#

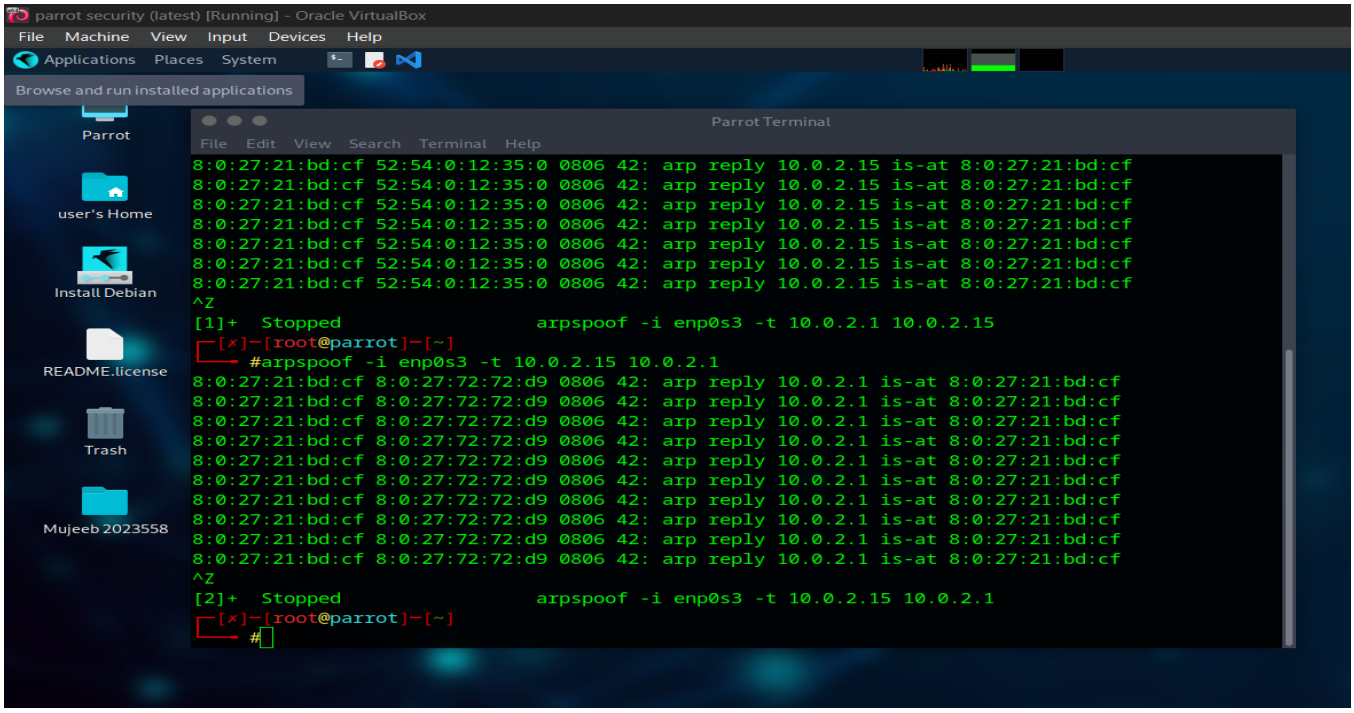
3. Switch to the Wireshark window and you can observe the captured ARP packets, as shown in the screenshot.



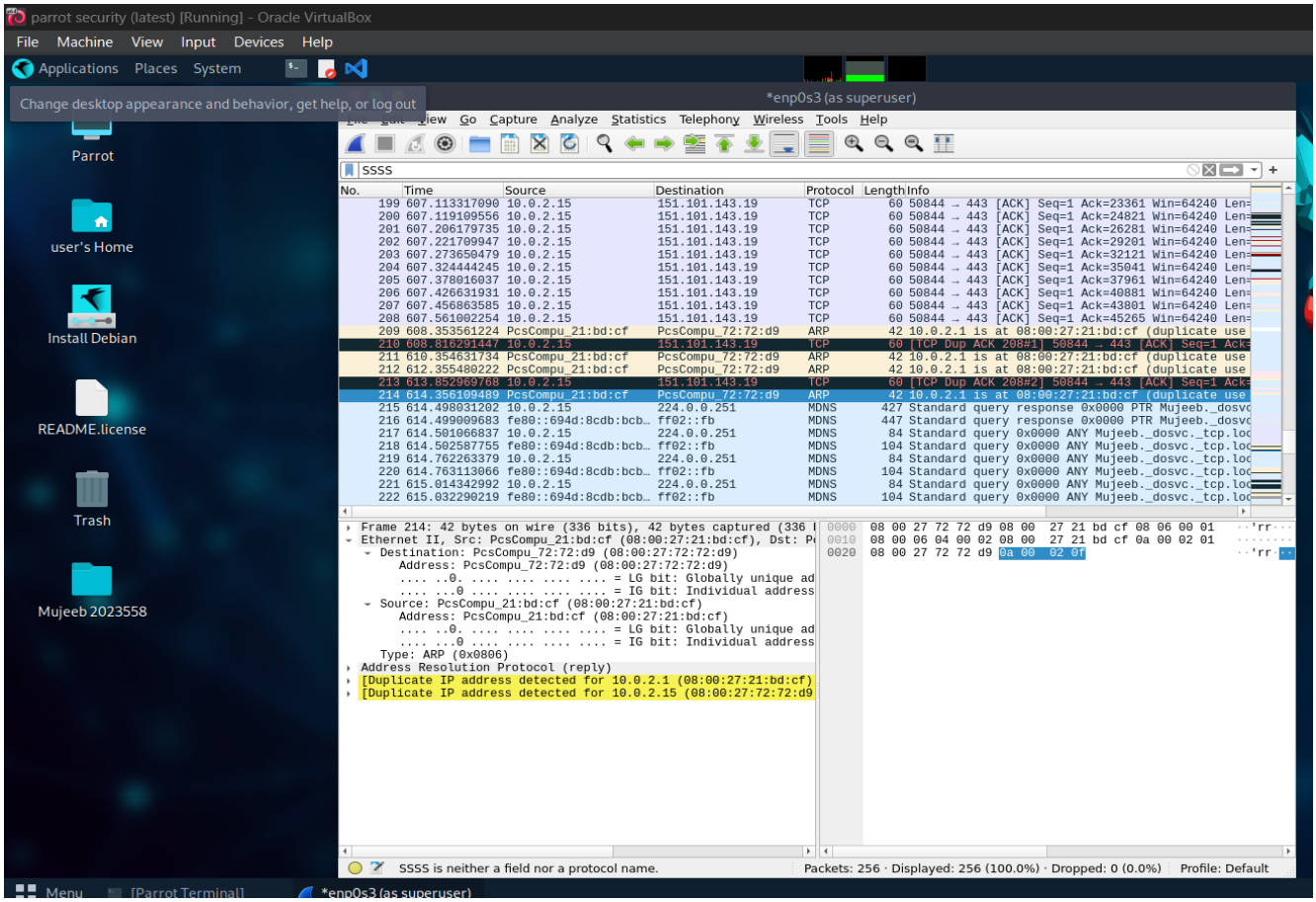
4. Switch back to the terminal window where arpspoof was running. Type arpspoof -i enp0s3 -t 10.10.1.11 10.10.1.1 and press Enter.

5. Through the above command, the host system informs the target system (10.10.1.11) that it is the access point (10.10.1.1)

6. After sending a few packets, press CTRL + z to stop sending the ARP packets.



7. In Wireshark, you can observe the ARP packets with an alert warning "**duplicate use of 10.0.2.15 detected**!"

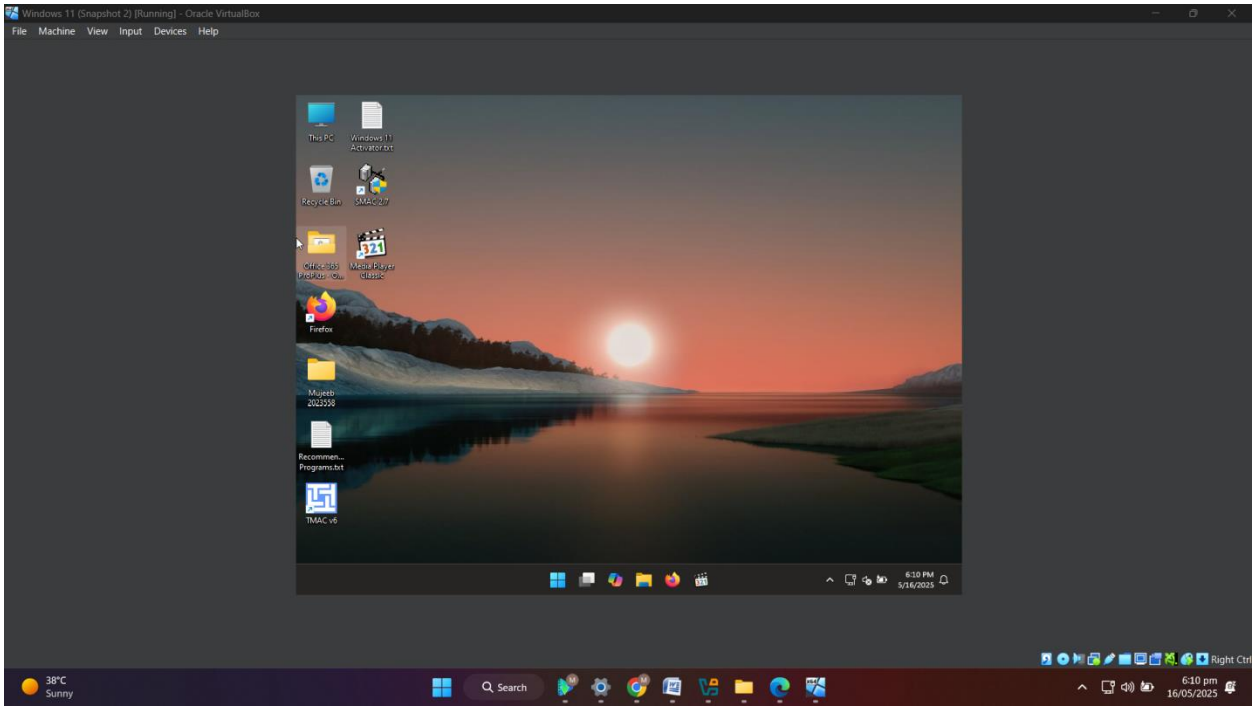


Note: You can navigate to the Windows 11 machine and see the IP addresses and their corresponding MAC addresses. You will observe that the MAC addresses of IP addresses 10.0.2.1 and 10.0.2.15 are the same, indicating the occurrence of an ARP poisoning attack, where 10.0.2.14 is the Parrot Security machine and 10.0.2.1 is the access point.

TASK 4 (Spoof a MAC Address using TMAC and SMAC)

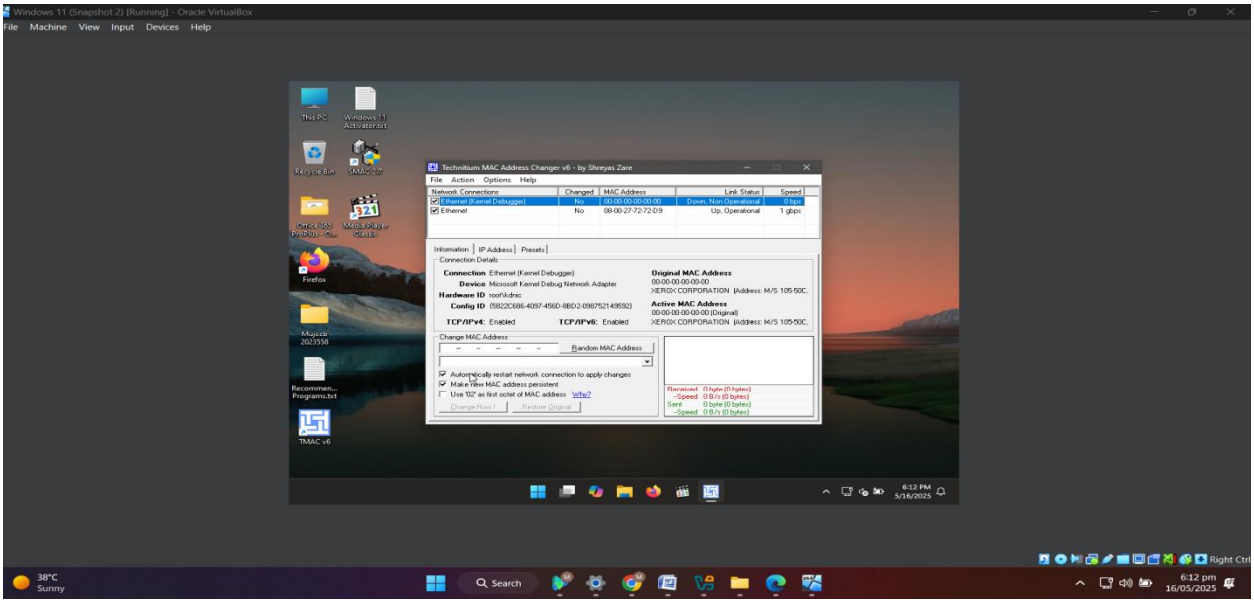
➢ Step 1 (Turn on machine):

1. Turn on the windows 11 VM, And Install TMAC and SMAC.

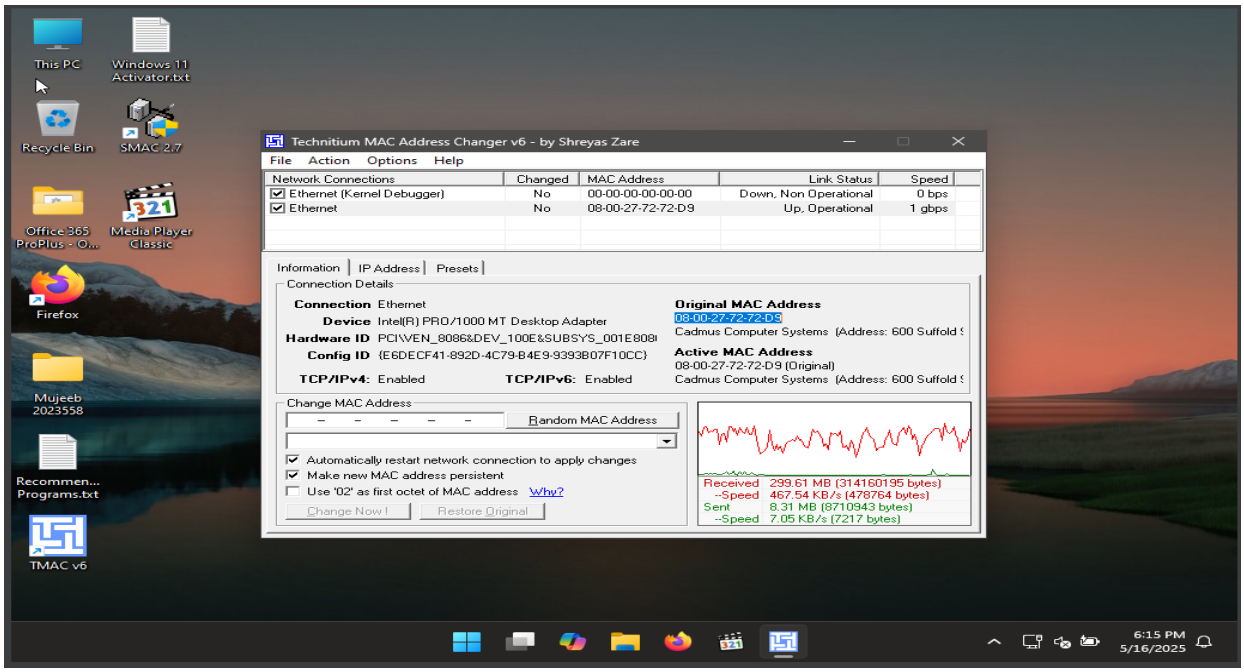


➢ Step 2 (Spoof MAC Address using TMAC):

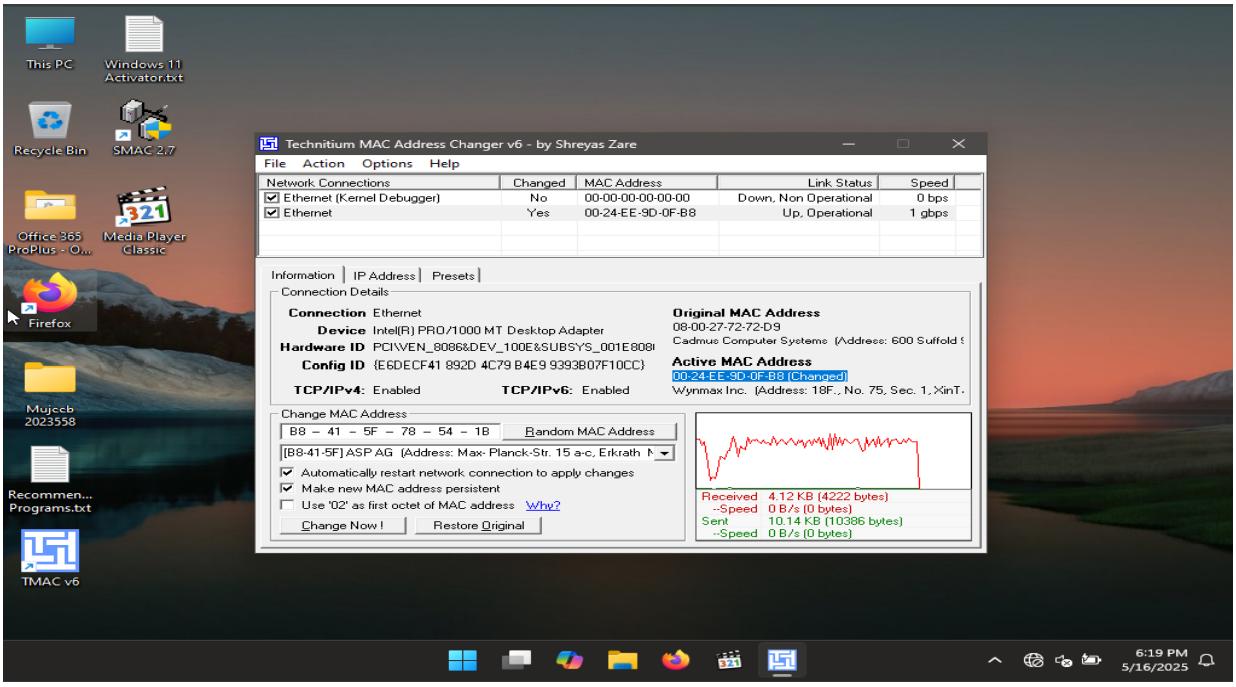
1. Open TMAC application.



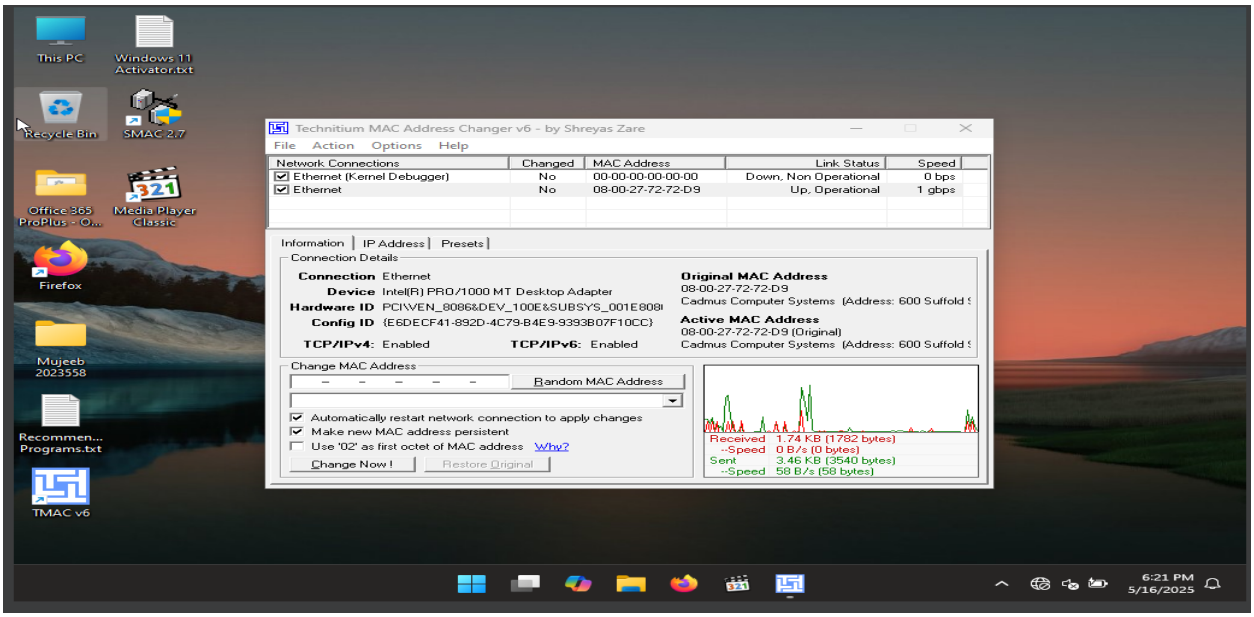
2. Select the connected Network Adapter (Here Ethernet). (Original Mac Address Selected).



3. Click the Random MAC Address button under the Change MAC Address option to generate a random MAC address for the network adapter and then click (change now).

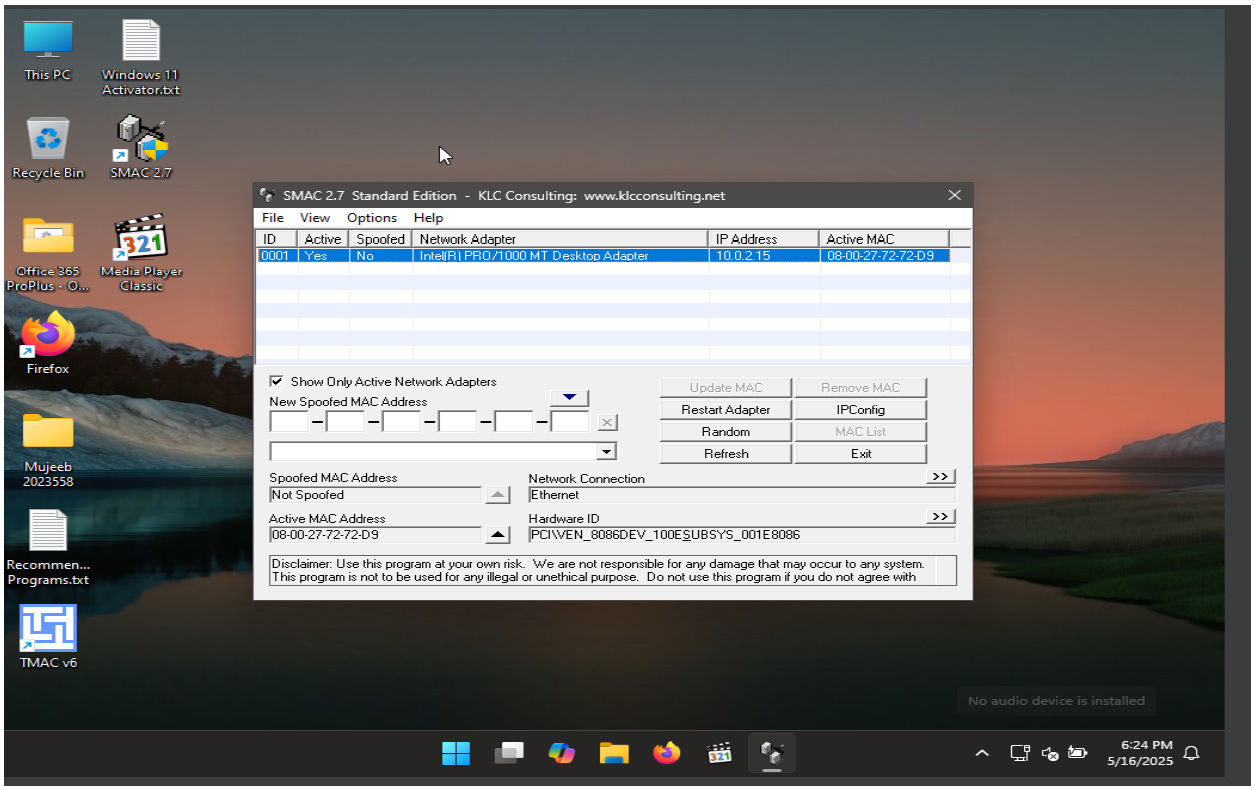


4. Spoofed Mac address is shown under (Active MAC Address).
5. Click Restore Original to bring back the original mac.

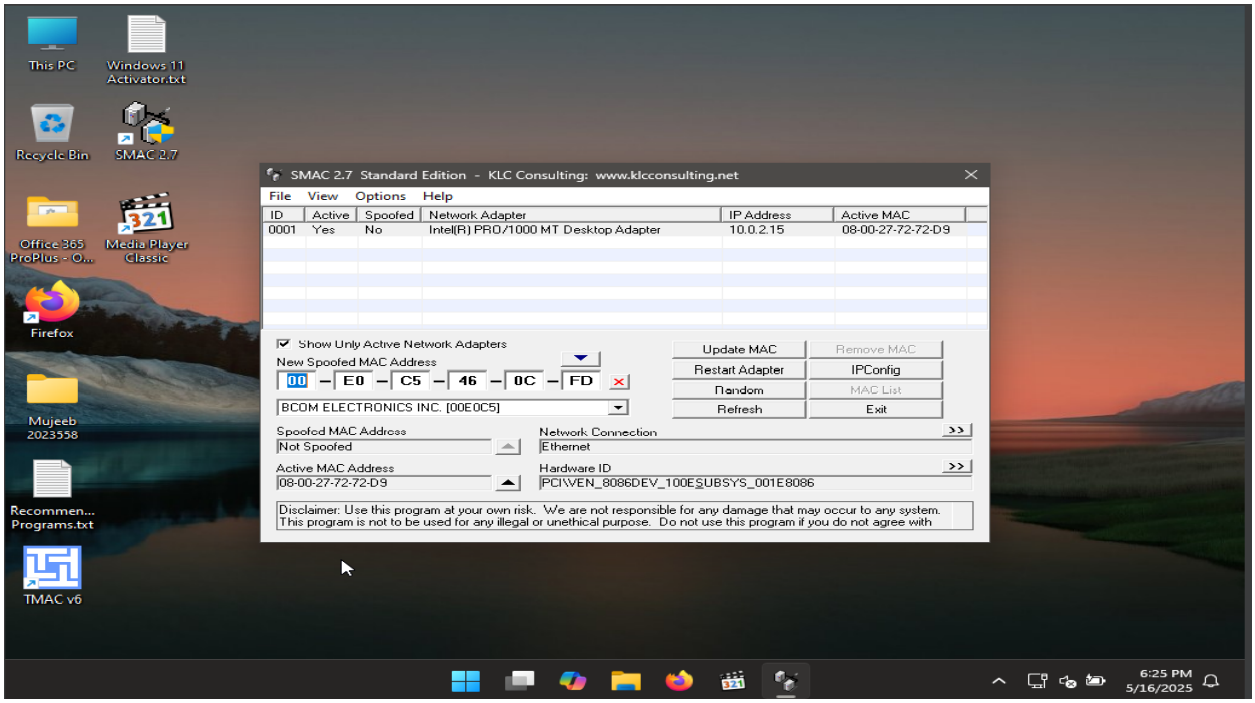


➢ Step 3 (MAC Spoofing by SMAC) :

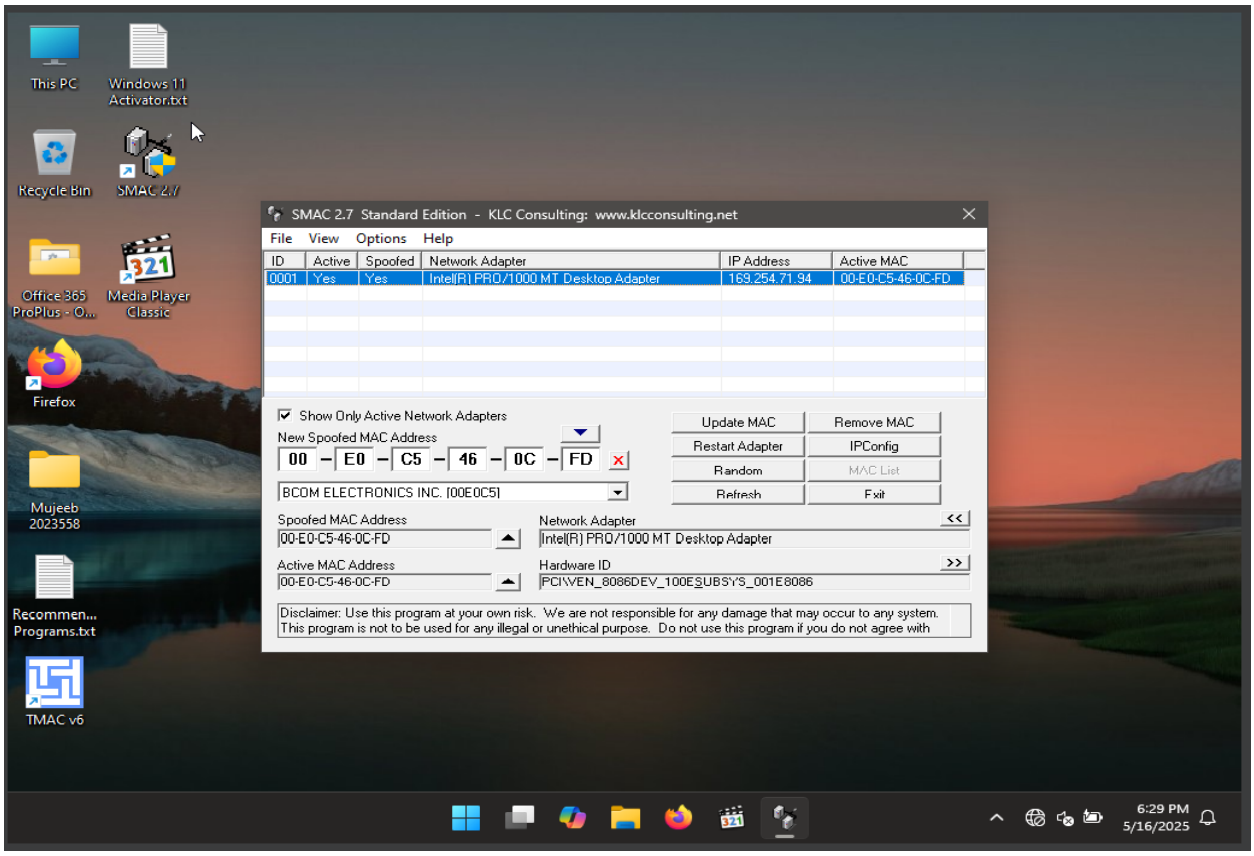
1. Open SMAC , Select the network adapter whose MAC is being spoofed .



2. Click on Random to generate Random MAC address.



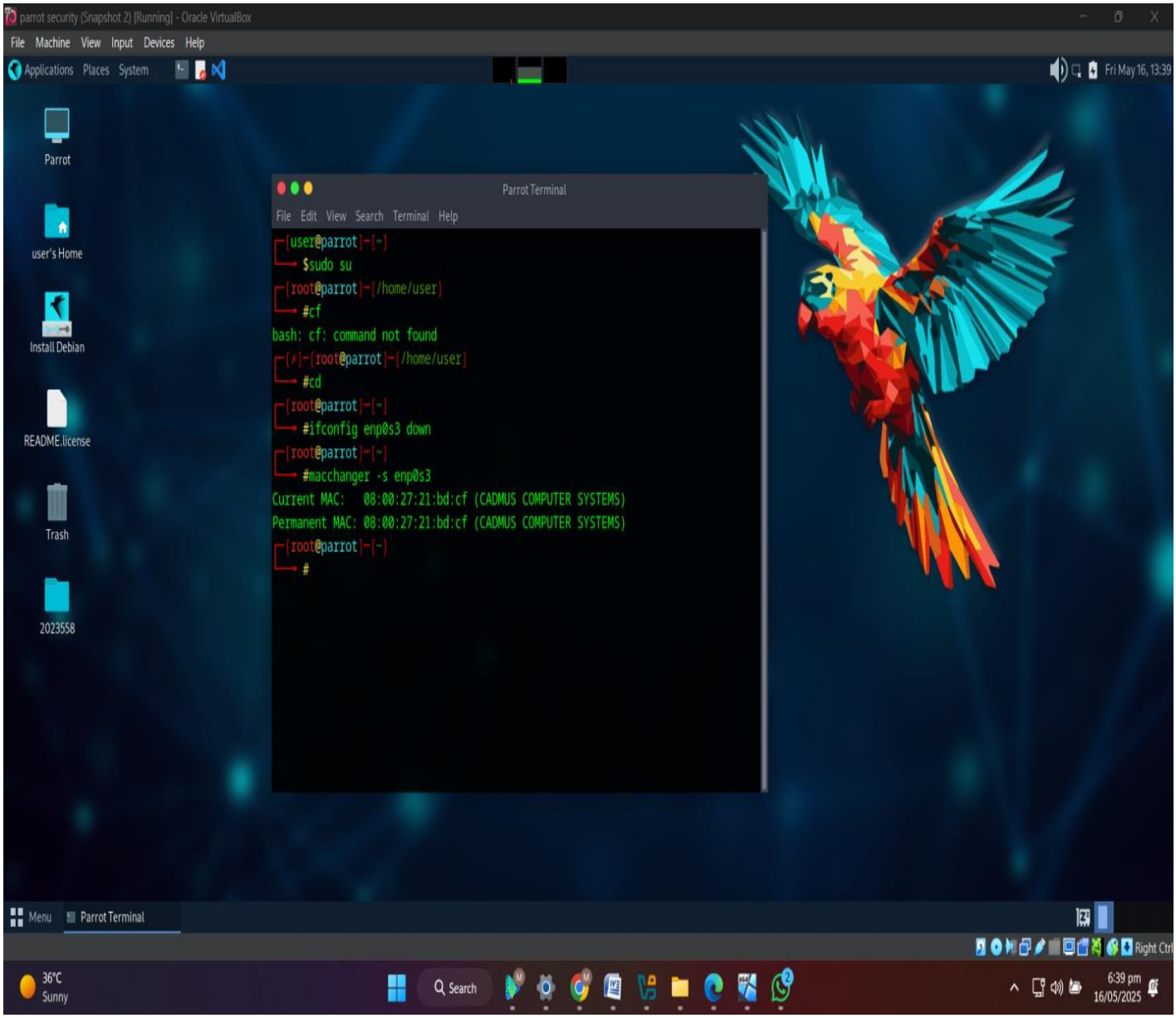
3. Click on update MAC (Random MAC will be assigned to adapter).



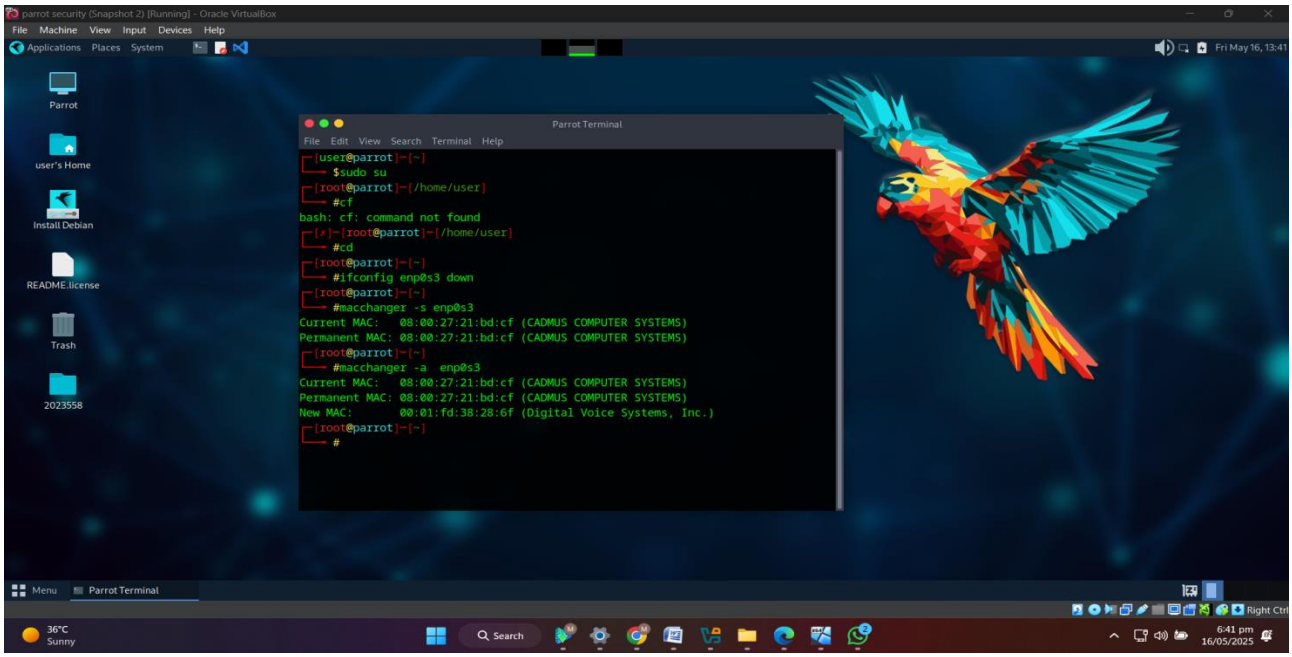
4. Click on Remove MAC to Restore Original.

TASK 5 (Spoof a MAC Address of Linux Machine using macchanger):

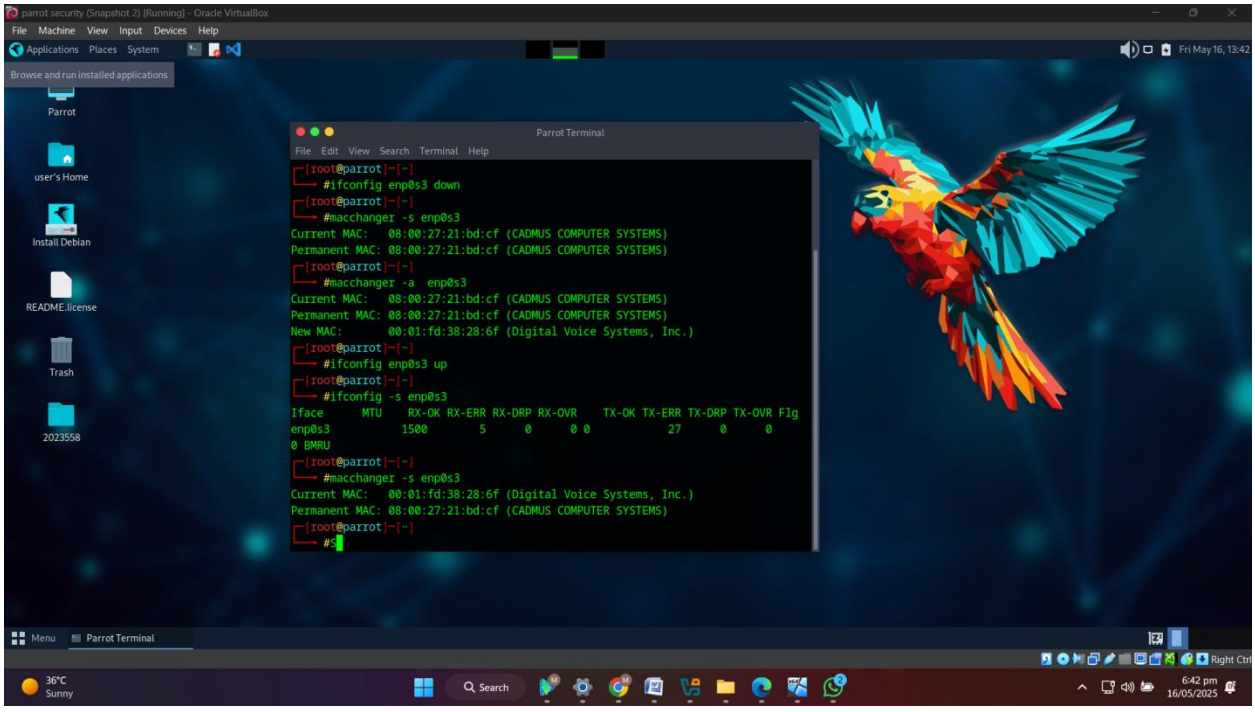
- **Step 1: Turn On Parrot Os, Open Terminal.**
  1. Type ifconfig enp0s3 down and press Enter, to turn off the network interface.
  2. To see the current MAC address of the Parrot Security machine, type macchanger -s enp0s3 and press Enter.



3. In the terminal type, macchanger -a enp0s3 and press Enter, to set a random vendor MAC address to the network interface.



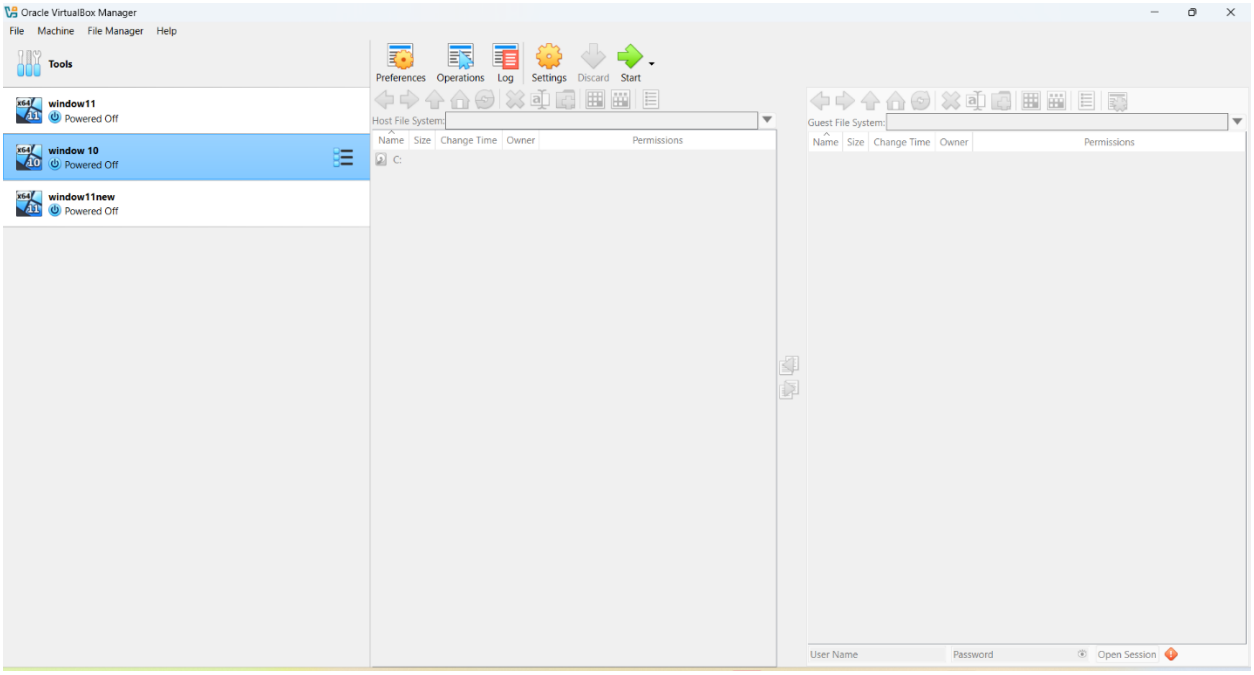
4. Check the current MAC Address by macchanger –s enp0s3.

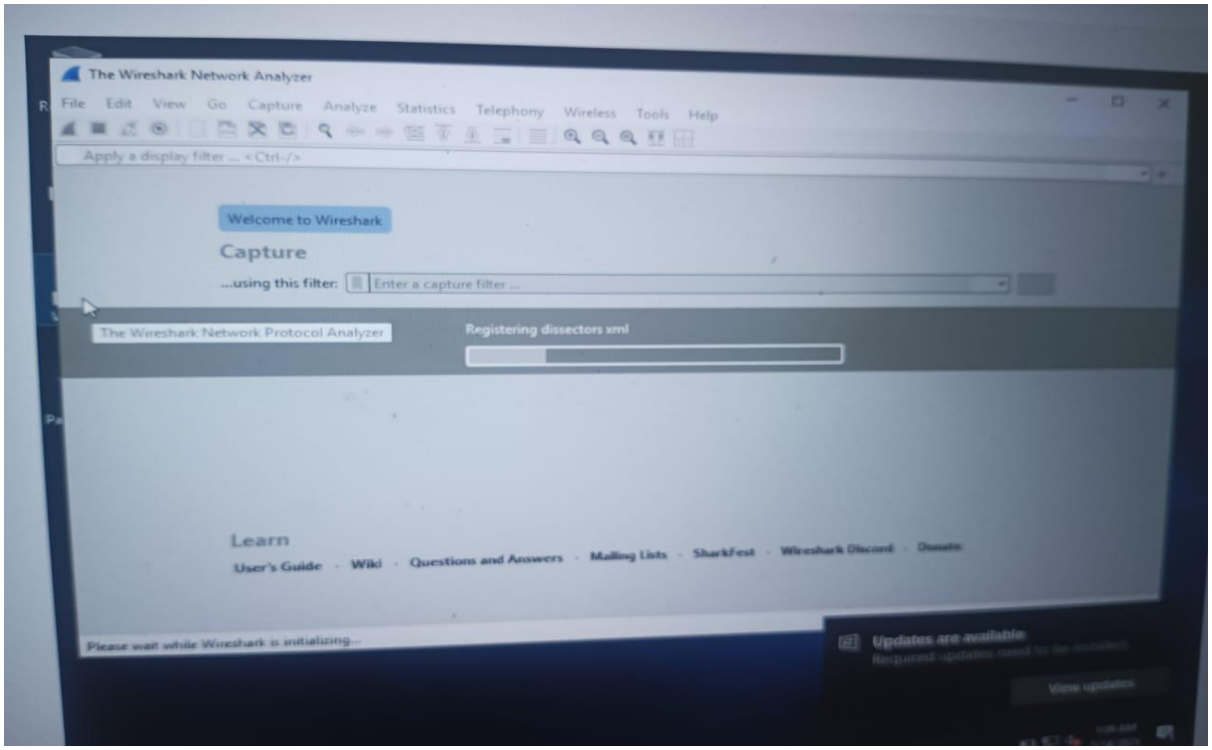


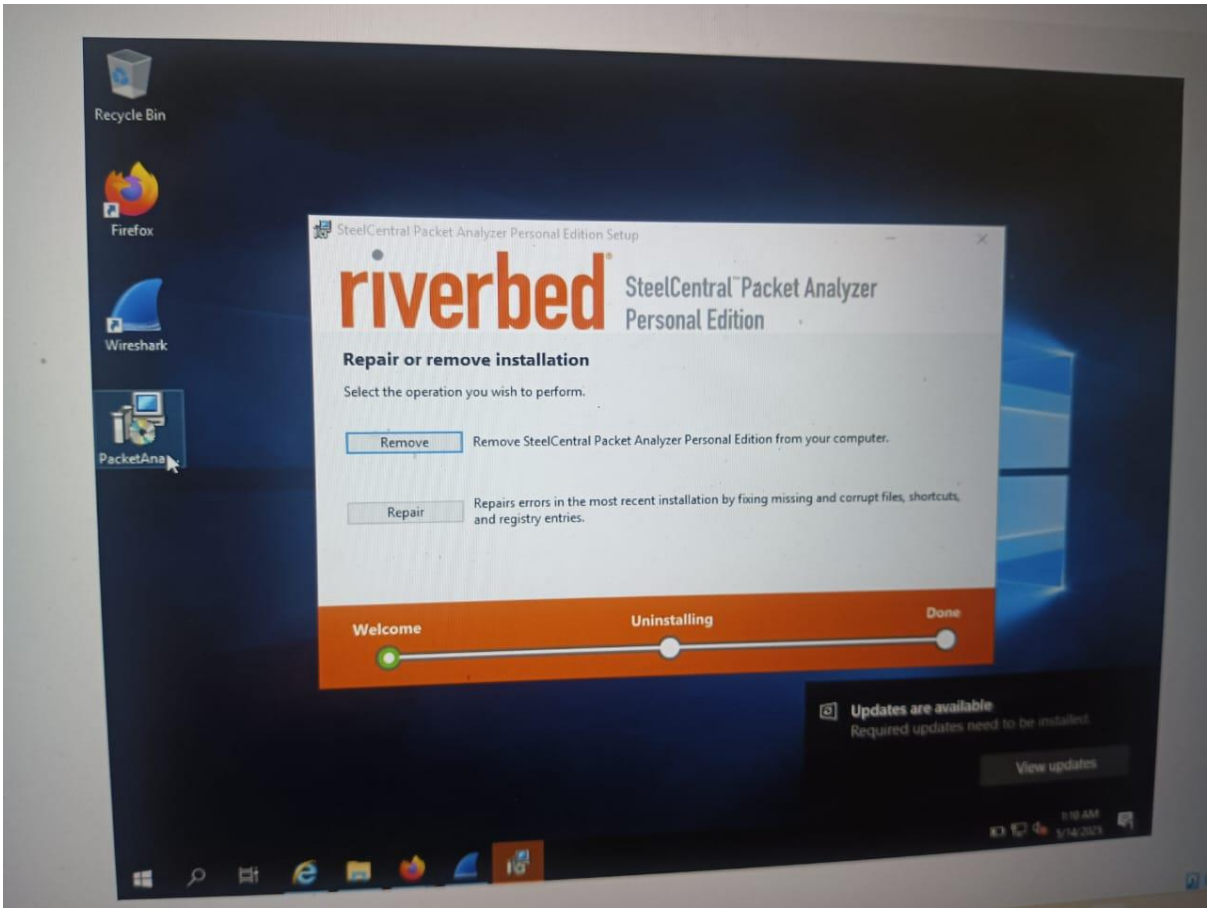
5. New MAC is Assigned to the Machine.

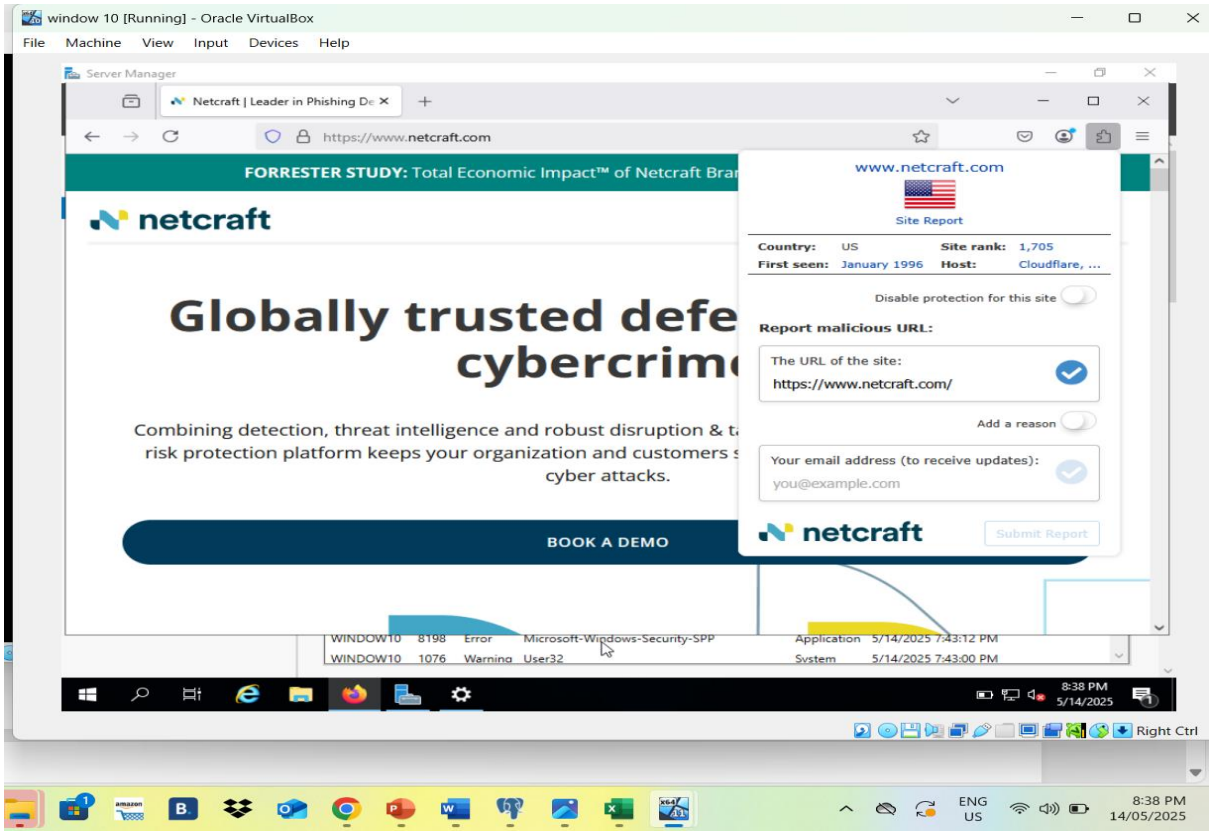
LAB 2 (Perform Network Sniffing using Various)

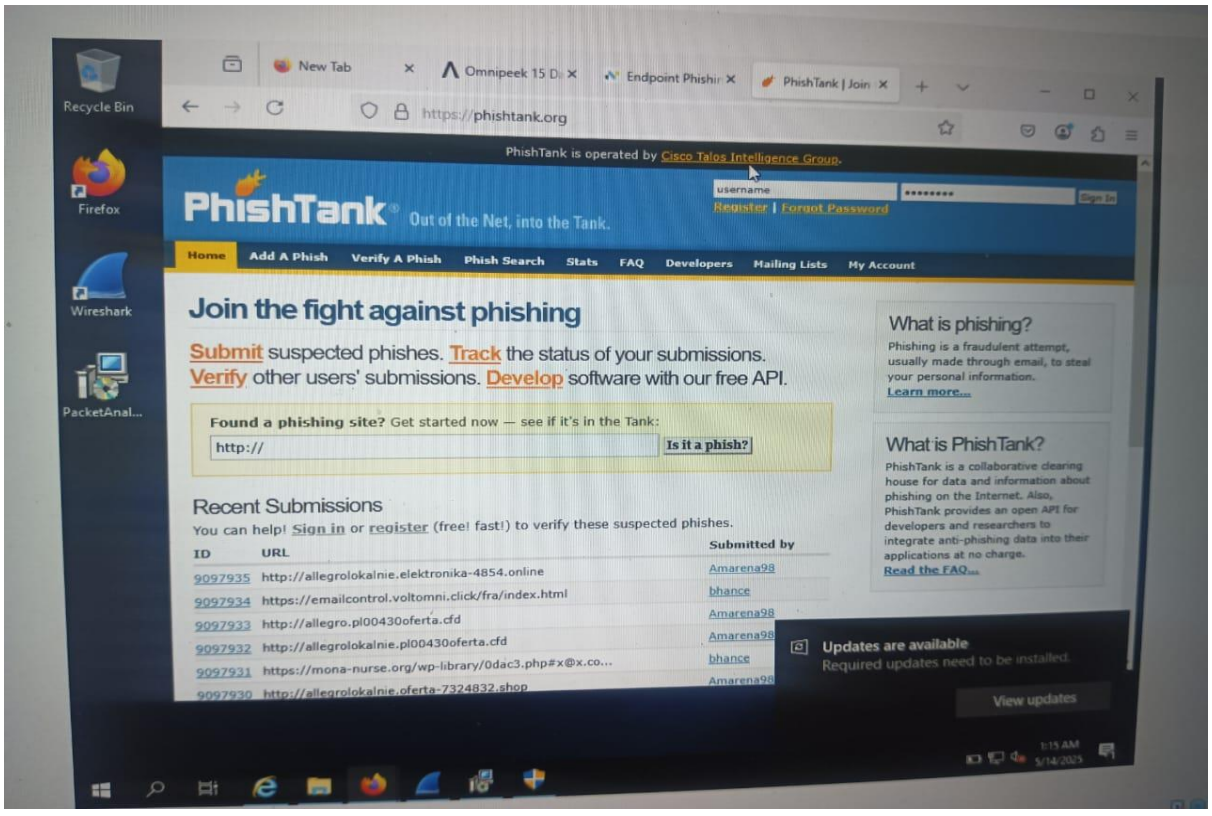
- **VIRTUAL MACHINE REQUIRED:**
  1. WINDOW SERVER 2019
  2. WINDOW 11
- **TOOLS REQUIRED:**
  1. WIRESHARK
  2. OMNIPEEK
  3. PHISHTANK
  4. NETCRAFT
- ***SETTING UP VIRTUAL MACHINE AND TOOLS***

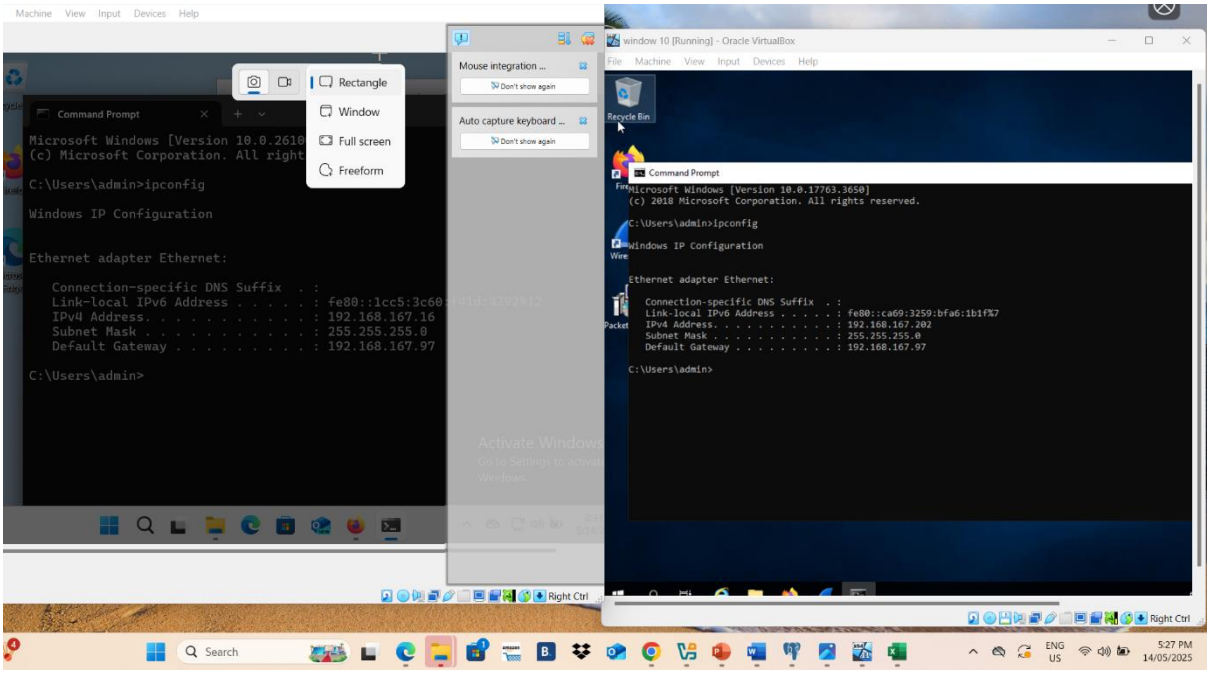


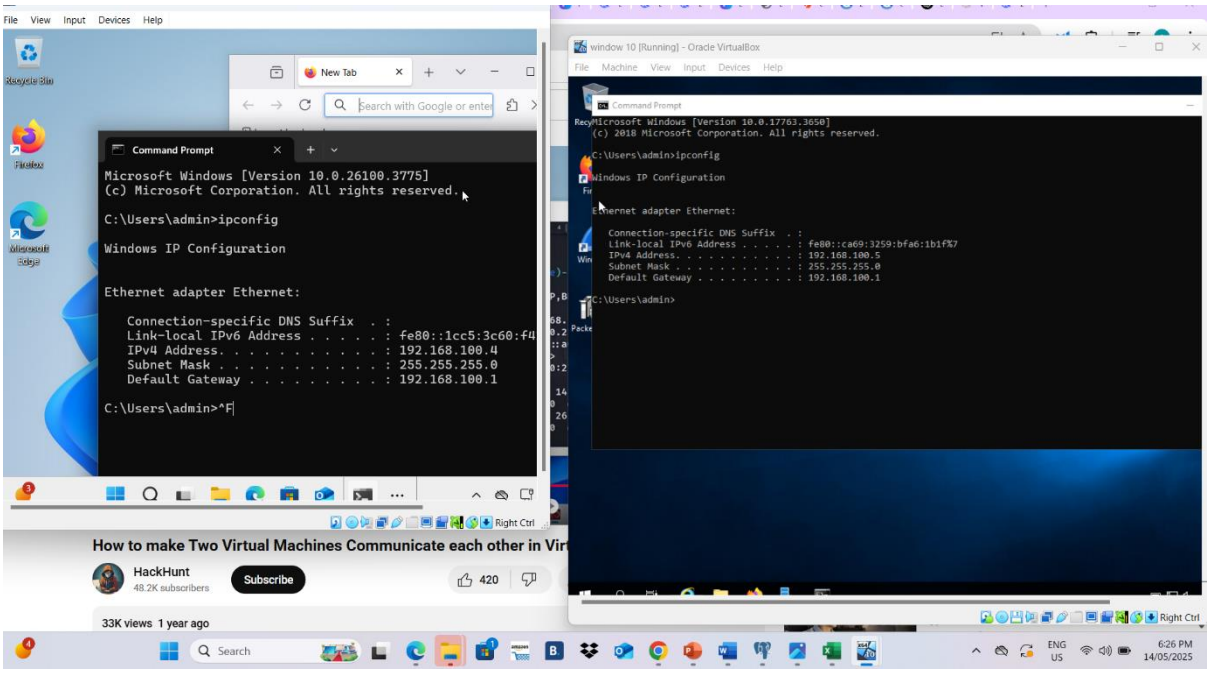

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
The Wireshark Network Protocol Analyzer
Registering dissectors xml
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Please wait while Wireshark is initializing...
Updates are available
View updates


Recycle Bin
Firefox
Wireshark
PacketAna
SteelCentral Packet Analyzer Personal Edition Setup
riverbed
SteelCentral Packet Analyzer
Personal Edition
Repair or remove installation
Select the operation you wish to perform.
Remove
Remove SteelCentral Packet Analyzer Personal Edition from your computer.
Repair
Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.
Welcome
Uninstalling
Done
Updates are available
Required updates need to be installed
View updates


window 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Netcraft | Leader in Phishing De
https://www.netcraft.com
FORRESTER STUDY: Total Economic Impact™ of Netcraft Bra
netcraft
Globally trusted defe
cybercrime
Combining detection, threat intelligence and robust disruption & t
risk protection platform keeps your organization and customers s
cyber attacks.
BOOK A DEMO
www.netcraft.com
Site Report
Country: US
Site rank: 1,705
First seen: January 1996
Host: Cloudflare, ...
Disable protection for this site
Report malicious URL:
The URL of the site:
https://www.netcraft.com/
Add a reason
Your email address (to receive updates):
you@example.com
netcraft
Submit Report
WINDOW10 8198 Error Microsoft-Windows-Security-SPP Application 5/14/2025 7:43:12 PM
WINDOW10 1076 Warning User32 System 5/14/2025 7:43:00 PM
8:38 PM
5/14/2025
Right Ctrl
ENG
US
8:38 PM
14/05/2025


Recycle Bin
Firefox
Wireshark
PacketAnal...
New Tab
Omnipeek 15 D
Endpoint Phishi
PhishTank | Join
https://phishtank.org
PhishTank is operated by Cisco Talos Intelligence Group.
PhishTank Out of the Net, into the Tank.
username
Register | Forgot Password
Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account
Join the fight against phishing
Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.
Found a phishing site? Get started now — see if it's in the Tank:
http://
Is it a phish?
What is phishing?
Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
Learn more...
What is PhishTank?
PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
Read the FAQ...
Recent Submissions
You can help! Sign in or register (free! fast!) to verify these suspected phishes.
ID URL Submitted by
9097935 http://allegrolokalnie.elektronika-4854.online Amarena98
9097934 https://emailcontrol.voltomni.click/fra/index.html bhance
9097933 http://allegro.pl00430oferta.cfd Amarena98
9097932 http://allegrolokalnie.pl00430oferta.cfd Amarena98
9097931 https://mona-nurse.org/wp-library/0dac3.php#x@x.co... bhance
9097930 http://allegrolokalnie.oferta-7324832.shop Amarena98
Updates are available
Required updates need to be installed.
View updates


Machine View Input Devices Help
Rectangle
Window
Full screen
Freeform
Command Prompt
Microsoft Windows [Version 10.0.2610
(c) Microsoft Corporation. All right
C:\Users\admin>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1cc5:3c60:
IPv4 Address. . . . . : 192.168.167.16
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.167.97
C:\Users\admin>
Mouse integration ...
Don't show again
Auto capture keyboard ...
Don't show again
window 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\admin>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ca69:3259:bfa6:1b1f%7
IPv4 Address. . . . . : 192.168.167.202
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.167.97
C:\Users\admin>
Right Ctrl
Search
ENG
US
5:27 PM
14/05/2025


File View Input Devices Help
Recycle Bin
Firefox
Microsoft Edge
New Tab
Search with Google or enter
Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.
C:\Users\admin>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1cc5:3c60:f4
IPv4 Address. . . . . : 192.168.100.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
C:\Users\admin>^F
window 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\admin>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ca69:3259:bfa6:1b1f%7
IPv4 Address. . . . . : 192.168.100.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
C:\Users\admin>
How to make Two Virtual Machines Communicate each other in Vir
HackHunt
48.2K subscribers
Subscribe
420
33K views 1 year ago
Right Ctrl
Search
ENG
US
6:26 PM
14/05/2025

➢ **TASK PERFOMANCE:**

➢ **CONNECTING TWO VIRTUAL MACHINES:**

First, I created the same interface for both VMs, then configured a NAT Network and assigned IP addresses — 192.168.100.4 to one VM and 192.168.100.5 to the other. Finally, I used Command Prompt to successfully ping between them and verify connectivity.

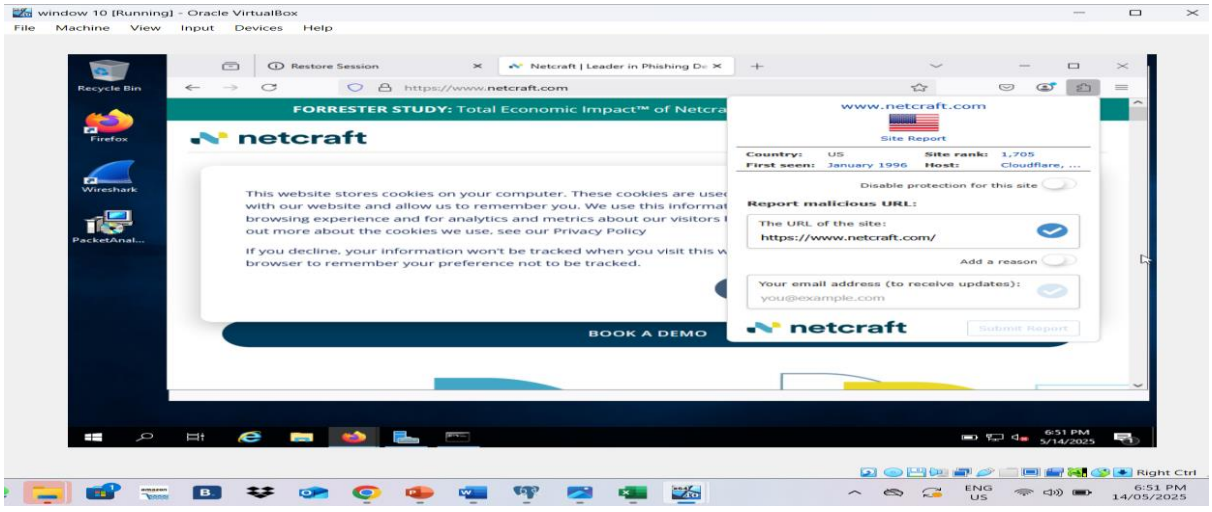
Netcraft is a cybersecurity tool that helps detect phishing, fraudulent, and malicious websites.
I used the Netcraft extension to check the authenticity of websites by reporting suspicious ones, helping me avoid phishing attacks.

➢ **OBJECTIVES:**

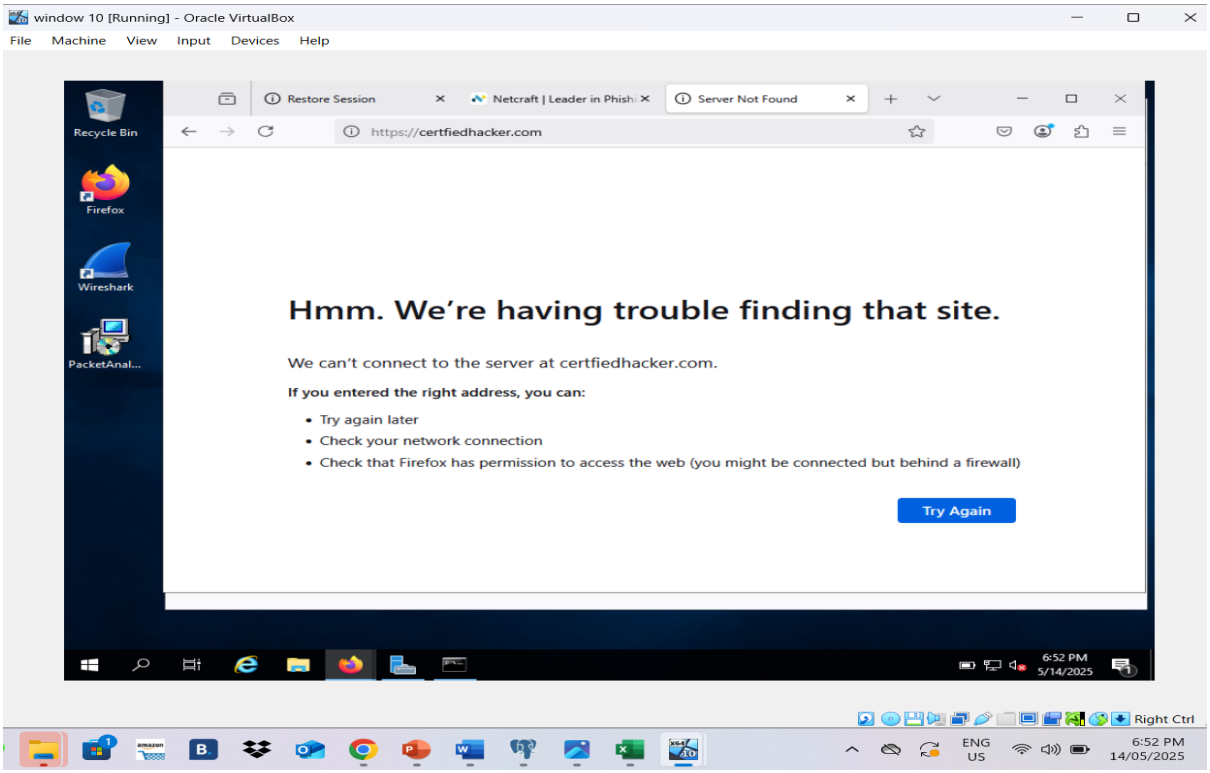
- *Use Netcraft to check site reports and verify website authenticity.*
- *Use PhishTank to check if a site is flagged as phishing.*
- *Report suspicious websites to PhishTank for public safety.*
- *Help users avoid fake or phishing websites.*
- *Promote safe browsing through regular site verification.*

TASK PERFOMANCE:

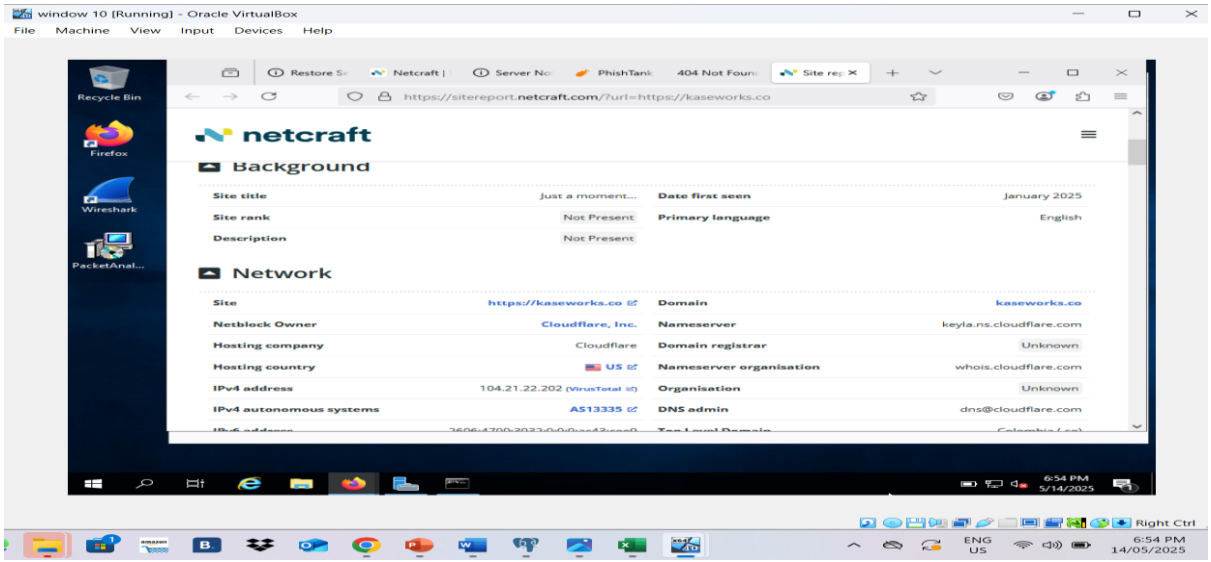
1) First I downloaded netcraft extension on my window.

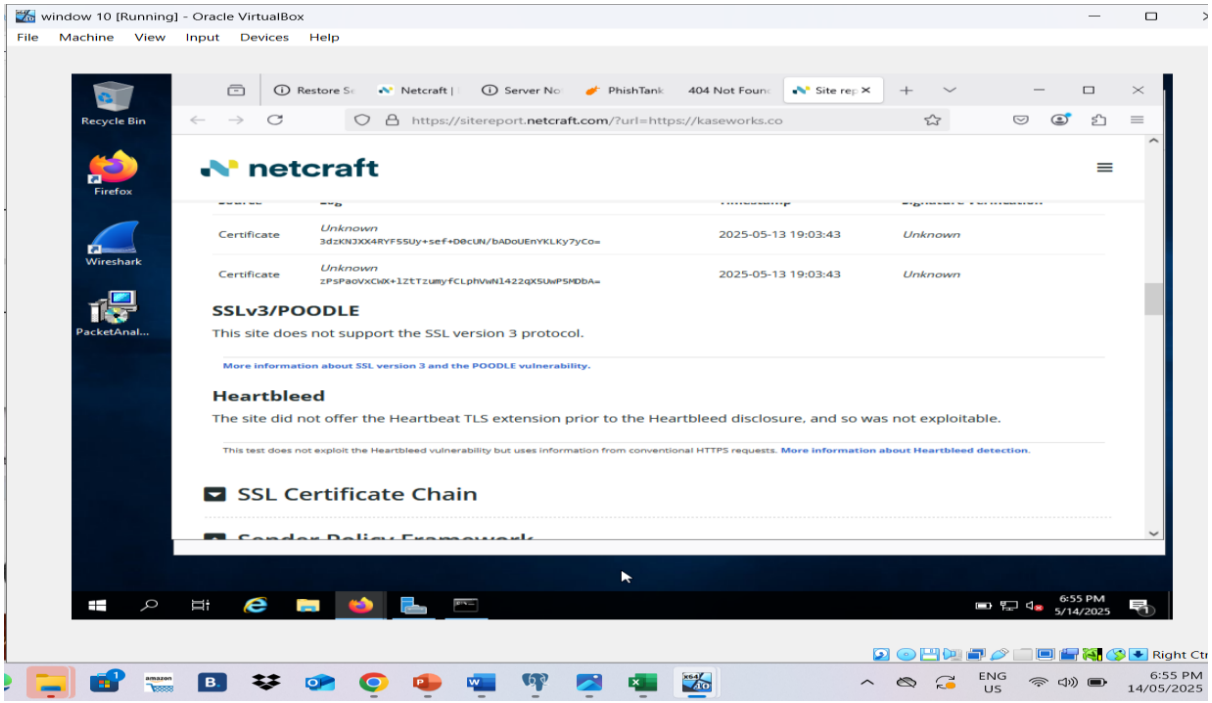


2)Then I opened any specific website to check it.

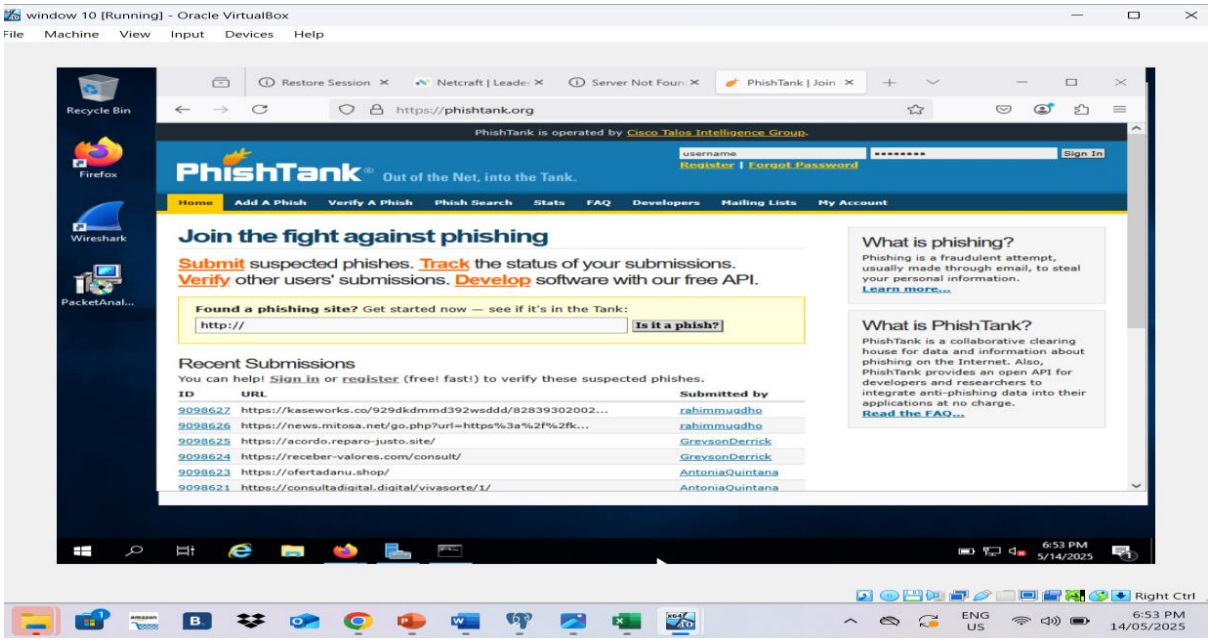


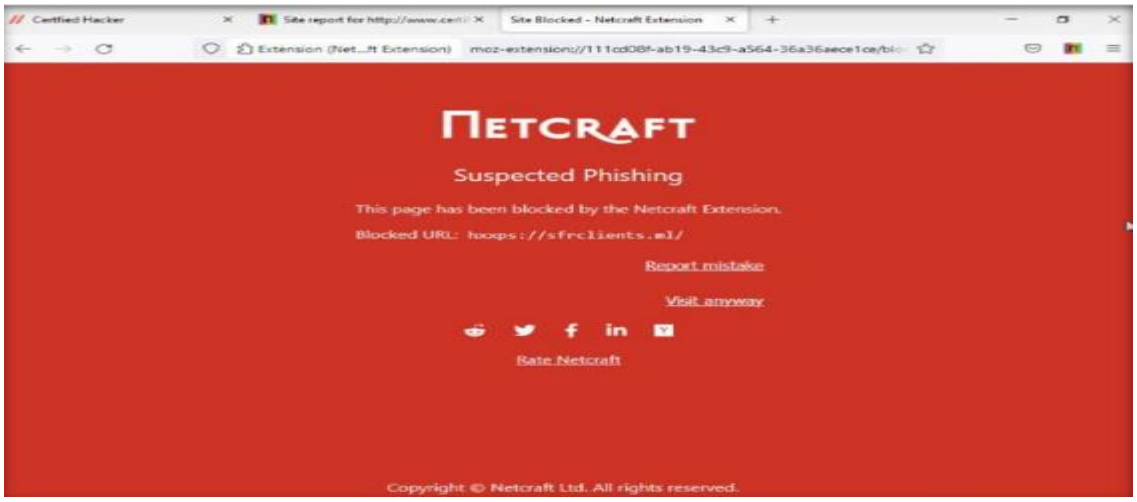
3)I used an **authentic website** and clicked on **Site Report**, where I found details such as the **network's geographical location** and the **protocol used by the website**.





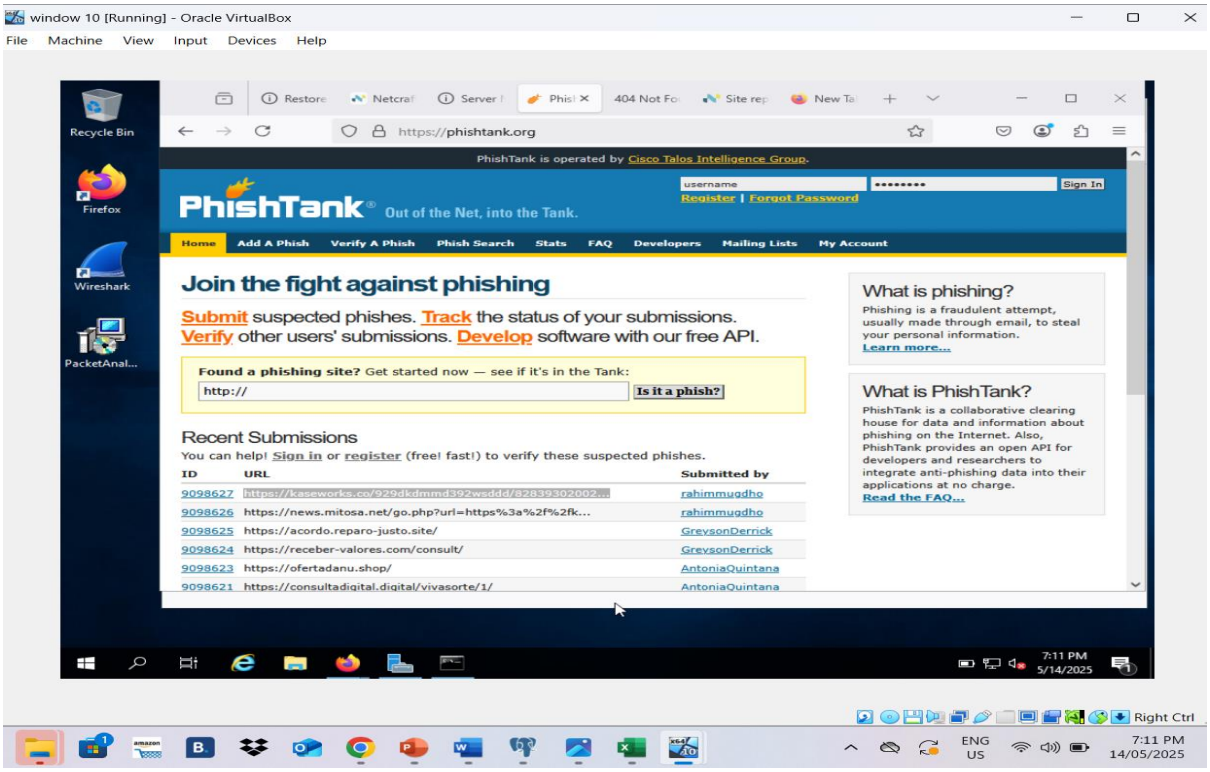
4)Then I found a **phishing site** from the **PhishTank** website and tried to **report the site using Netcraft.**





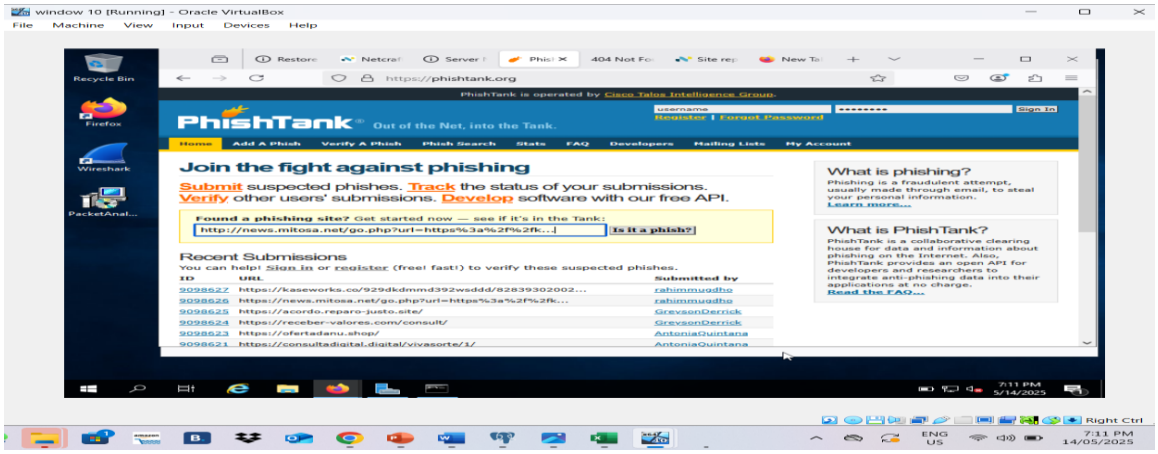
- **Phish Tank** is a community-based tool that identifies and tracks phishing websites.
- I used Phish Tank to search suspicious links and confirm if they were reported as phishing, helping me stay safe online.
- Using **PhishTank** to analyze whether a website is **authentic or fake** to stay safe from sharing personal data.

1. opened the **PhishTank** website and found many websites **submitted by others** as **phishing websites**.

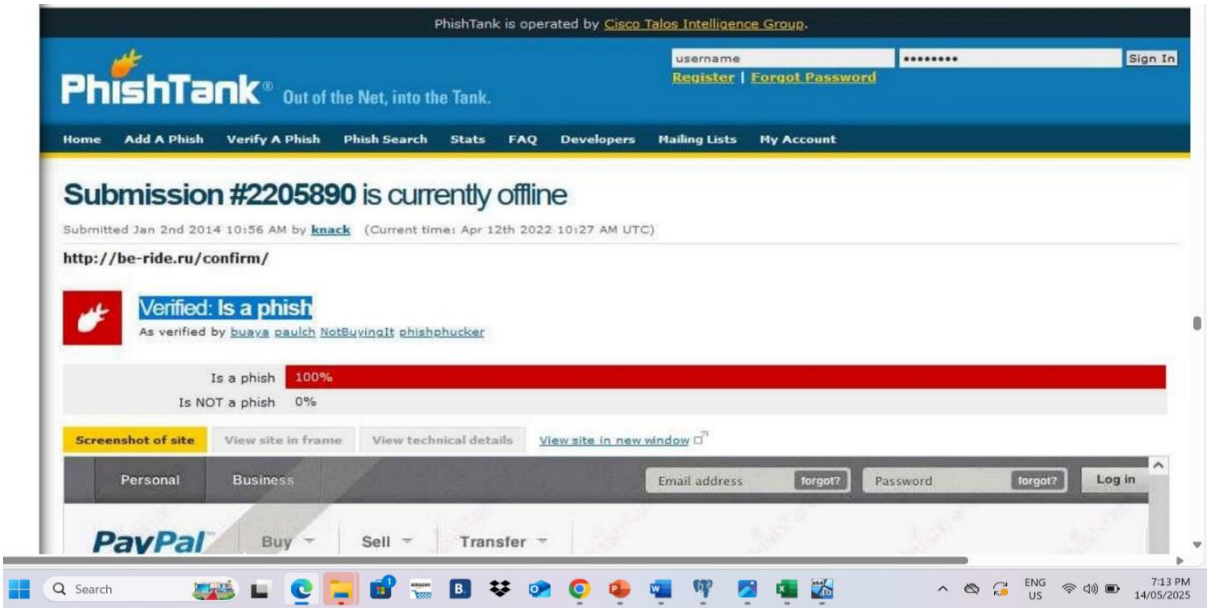


2) Then I picked one website that seemed **fake or not authentic** to check if it was a **phishing site** or not.

3) I inserted the website into the **search bar** and clicked on the **'Is it a Phish?**



4) Then it told me whether the site was **phishing or not**, so I could **avoid using or browsing** such websites.



➢ Importance of Cyber Tools (Netcraft & PhishTank)

- **Detect Phishing Attacks**: Identify fake or malicious websites trying to steal personal data.
- **Verify Website Authenticity**: Help confirm if a website is genuine or suspicious.
- **Protect User Privacy**: Prevent users from sharing sensitive information on unsafe sites.
- **Raise Cyber Awareness**: Educate users about online threats and safe browsing.
- **Contribute to Public Safety**: Reporting phishing sites helps protect the global online community.
- **Prevent Financial Loss & Data Theft**: Early detection avoids scams and frauds.

➢ LAB 3 (Detecting Network Sniffing in Promiscuous Mode and Switch-Based Network)

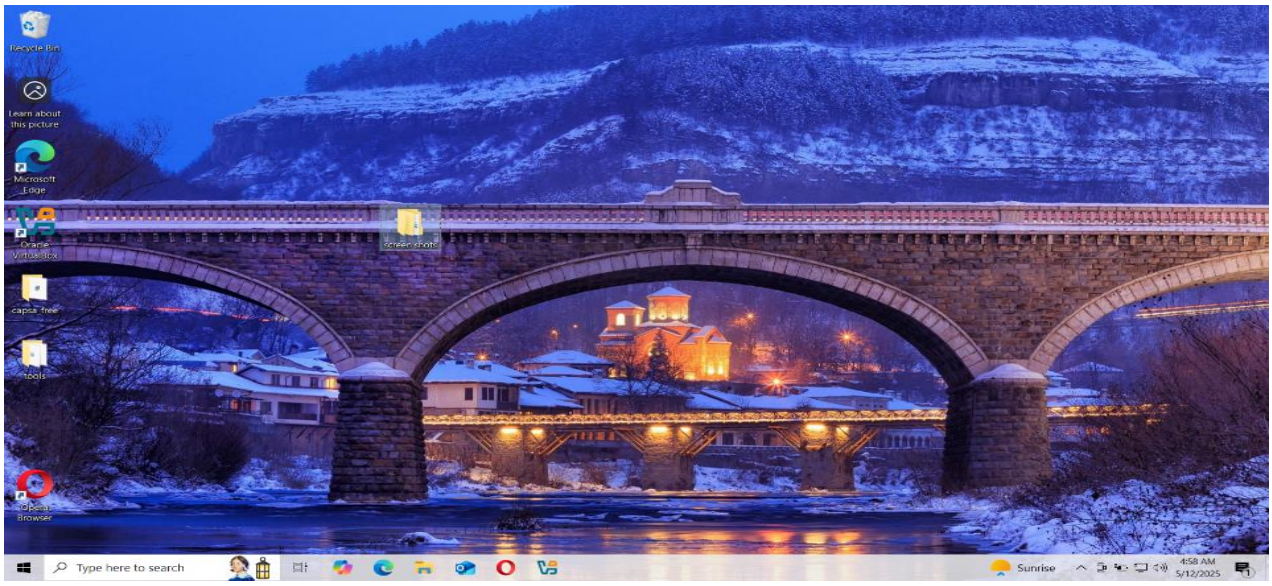
- **Objective:**
  The objective of this lab is to detect network sniffing activities, specifically ARP poisoning and promiscuous mode, in a switch-based network using tools like Wireshark, Cain & Abel, and Nmap. Network sniffing is a common attack where an attacker captures network traffic to extract sensitive information. Detecting such activities helps in securing the network against unauthorized access.

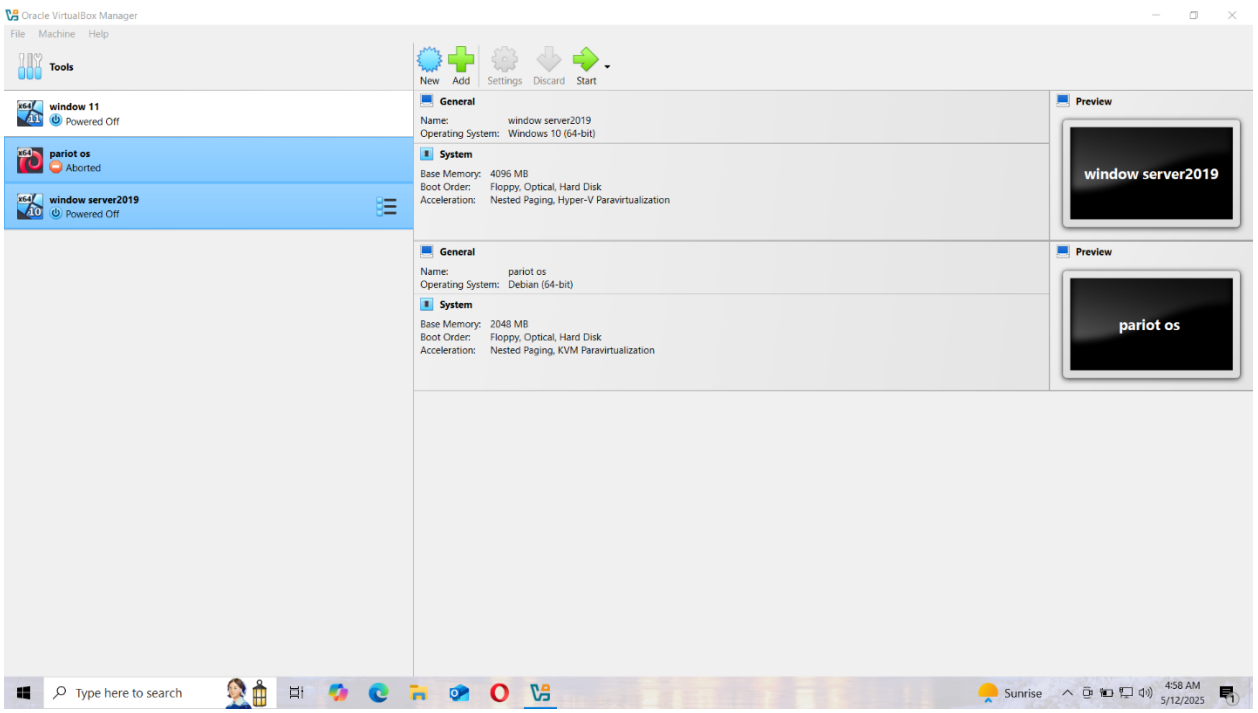
Lab Setup:

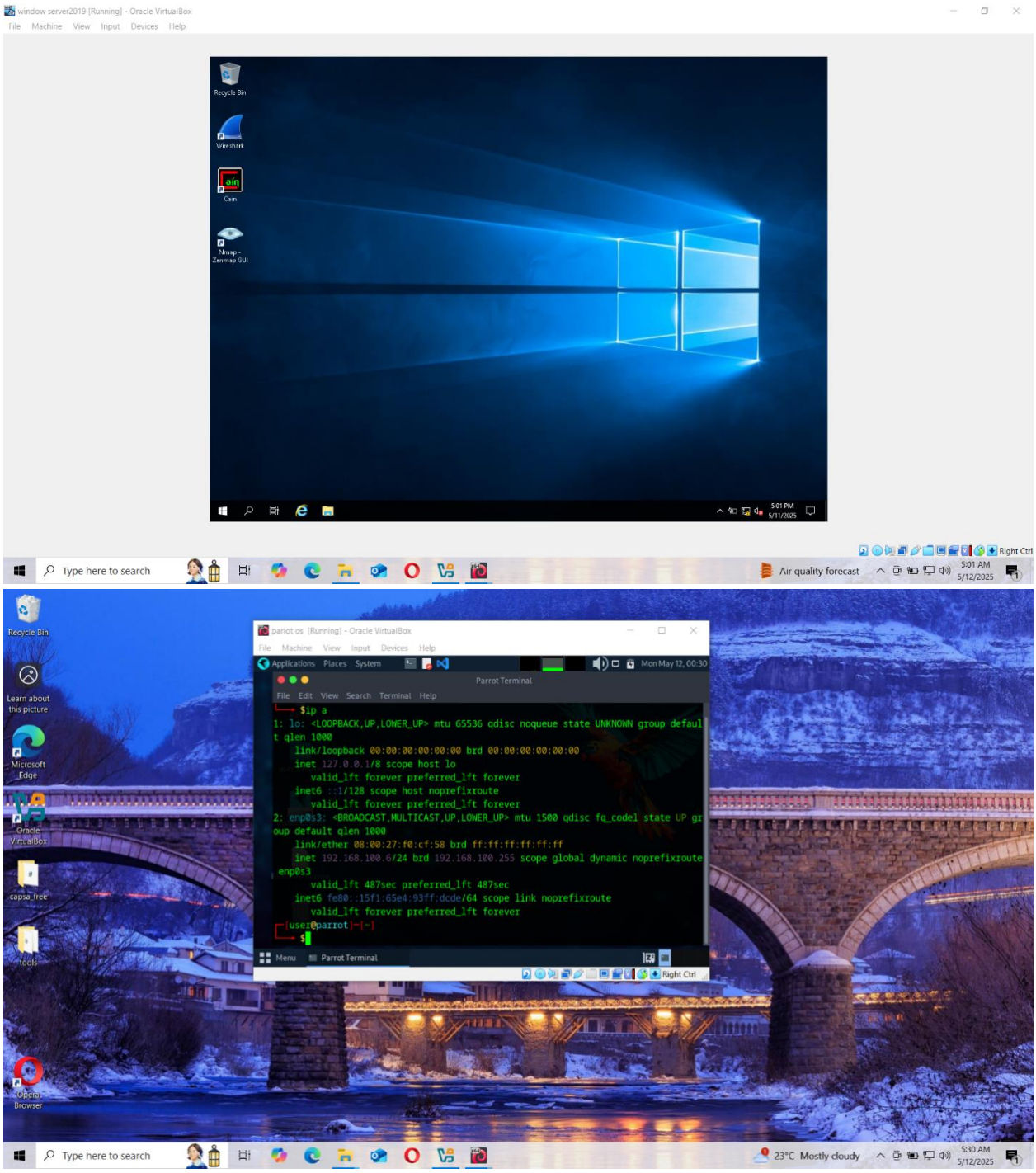
- Tools Used:
  - Wireshark (Network Traffic Analyzer)
  - Cain & Abel (ARP Poisoning)
  - Nmap (Promiscuous Mode Detection)
- Virtual Machines:
  - Windows 11
  - Windows Server 2019
  - Parrot Security

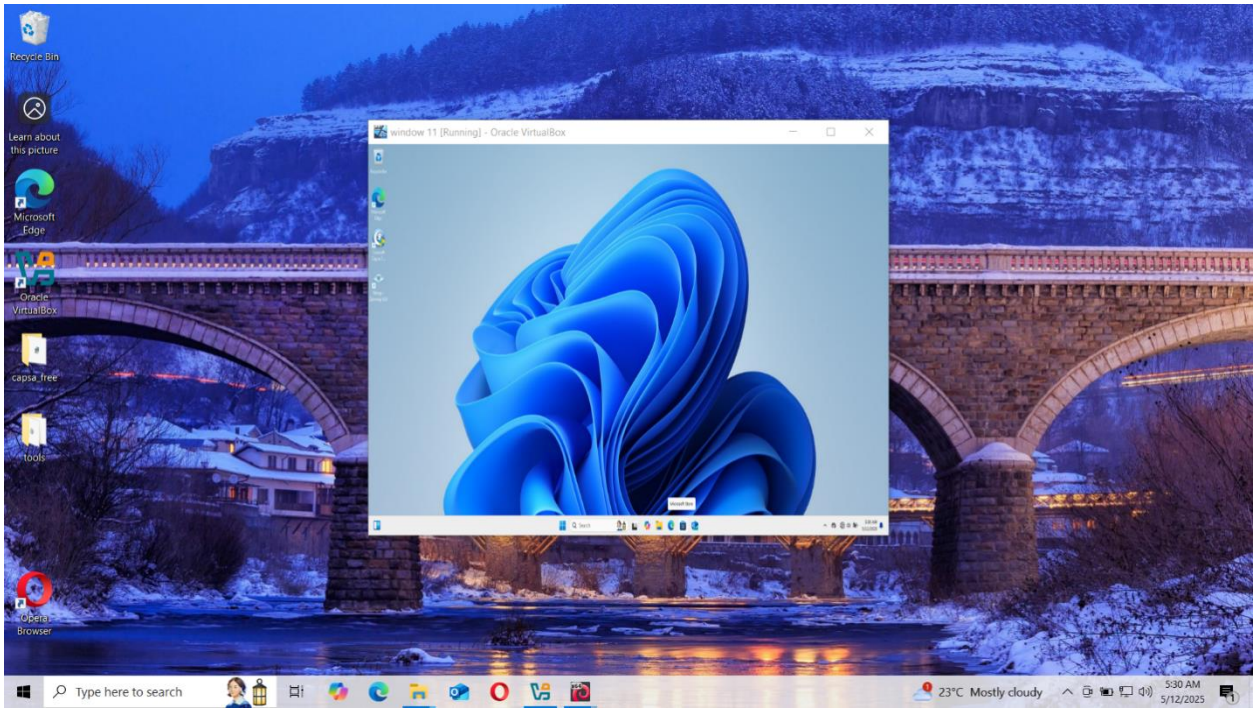
Task 1: Detecting ARP Poisoning and Promiscuous Mode in a Switch-Based Network

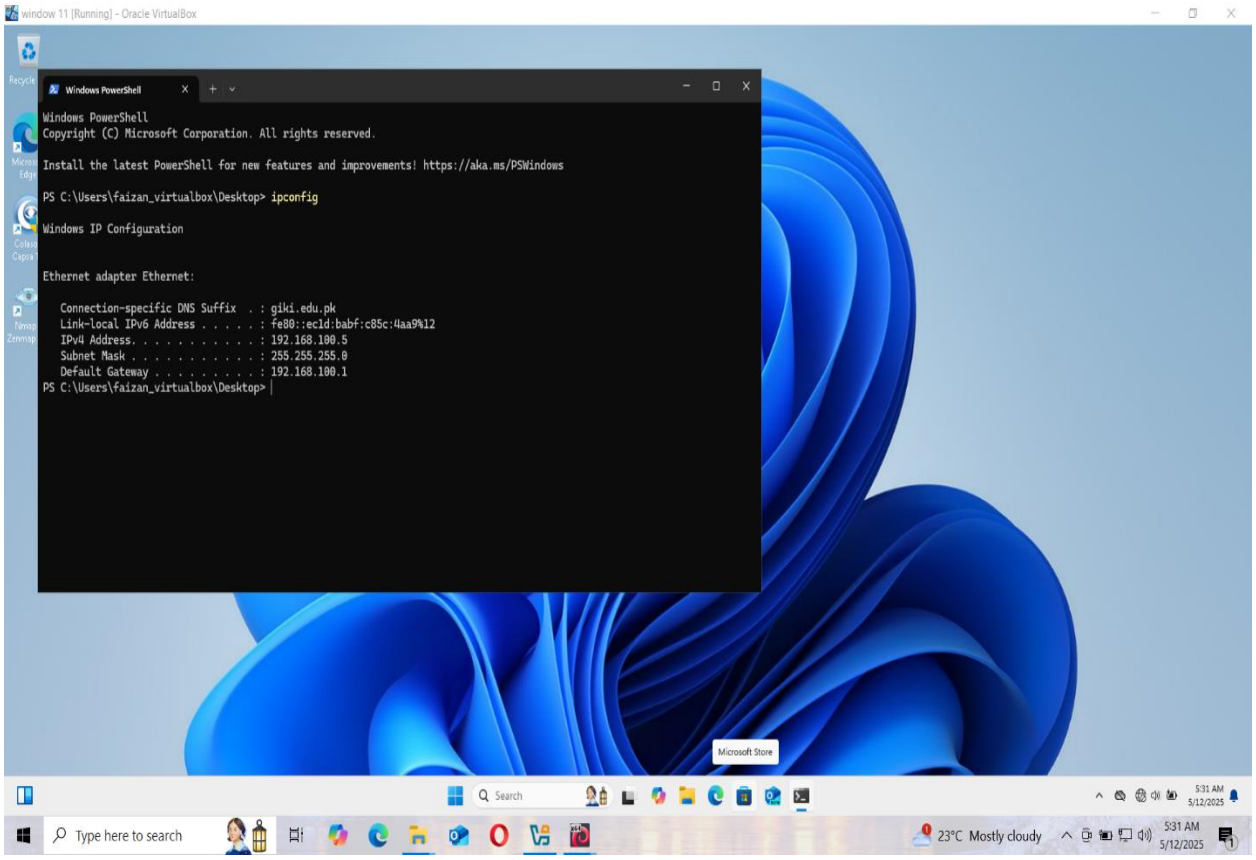
Screenshots of IP configuration different machines .






window server2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
5:01 PM
5/11/2025
Type here to search
Air quality forecast
5:01 AM
5/12/2025
parrot os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon May 12, 00:30
Parrot Terminal
File Edit View Search Terminal Help
$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:f0:cf:58 brd ff:ff:ff:ff:ff:ff
inet 192.168.100.6/24 brd 192.168.100.255 scope global dynamic noprefixroute enp0s3
valid_lft 487sec preferred_lft 487sec
inet6 fe80::15f1:65e4:93ff:dcde/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(user@parrot)-[~]
$
Menu
Parrot Terminal
Right Ctrl
Recycle Bin
Learn about this picture
Microsoft_Edge
Oracle VirtualBox
capsa_free
tools
Opera Browser
Type here to search
23°C Mostly cloudy
5:30 AM
5/12/2025


Recycle Bin
Learn about this picture
Microsoft Edge
Oracle VirtualBox
capsa_free
tools
Opera Browser
window 11 [Running] - Oracle VirtualBox
Type here to search
23°C Mostly cloudy
5:30 AM
5/12/2025

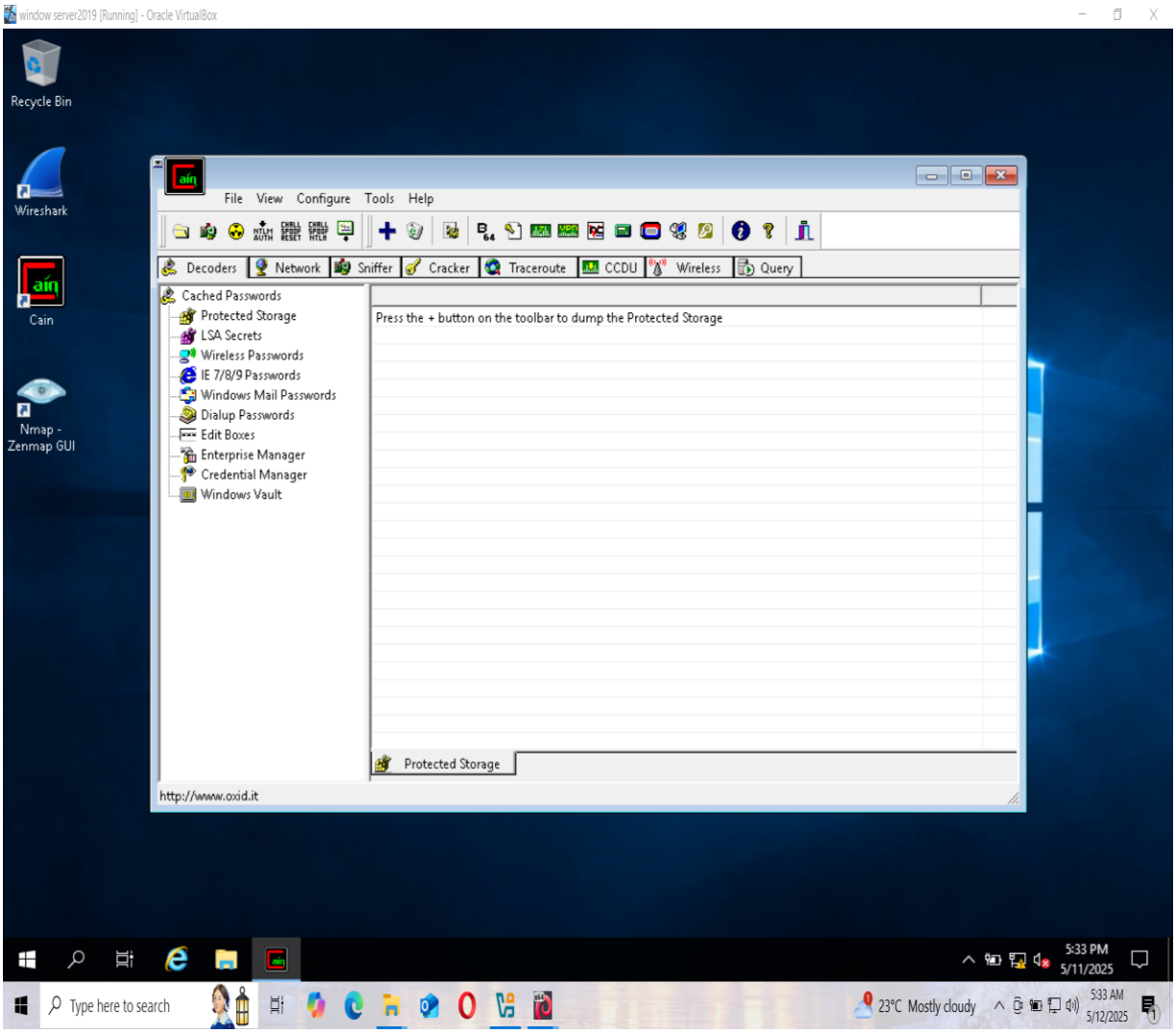

window 11 [Running] - Oracle VirtualBox
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\faizan_virtualbox\Desktop> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : giki.edu.pk
Link-local IPv6 Address . . . . . : fe80::ec1d:babf:c85c:4aa9%12
IPv4 Address. . . . . : 192.168.100.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
PS C:\Users\faizan_virtualbox\Desktop>
Microsoft Store
Search
Type here to search
23°C Mostly cloudy
5:31 AM
5/12/2025

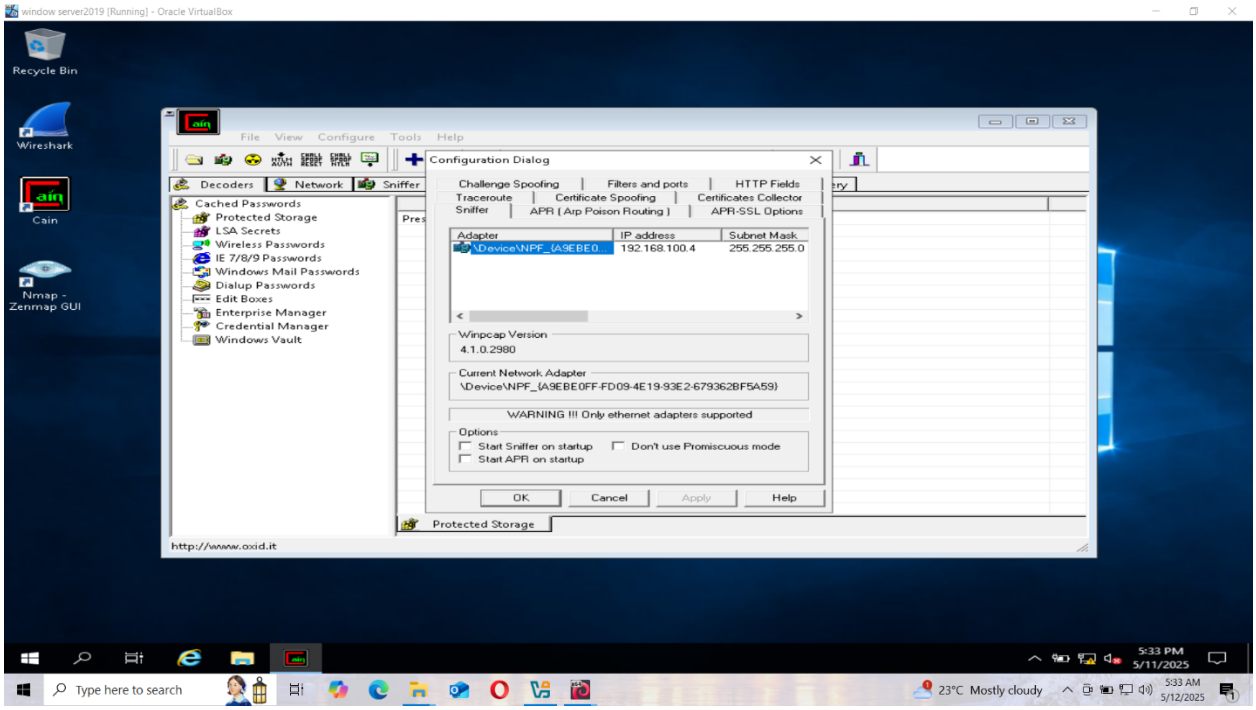
➢ Step 1: Launch Cain & Abel for ARP Poisoning Detection.

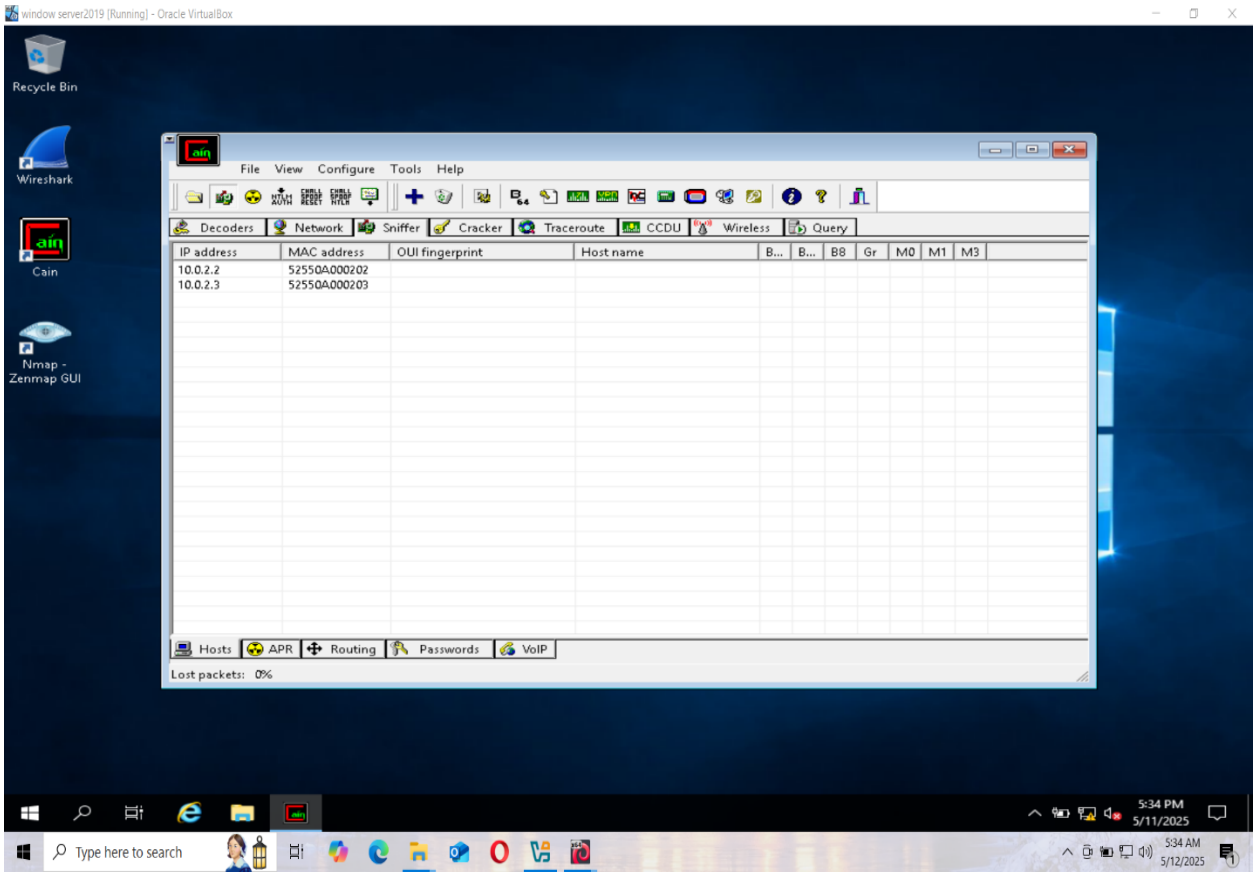
1. Open Cain & Abel on Windows Server 2019.
2. Start the Sniffer to capture network traffic.

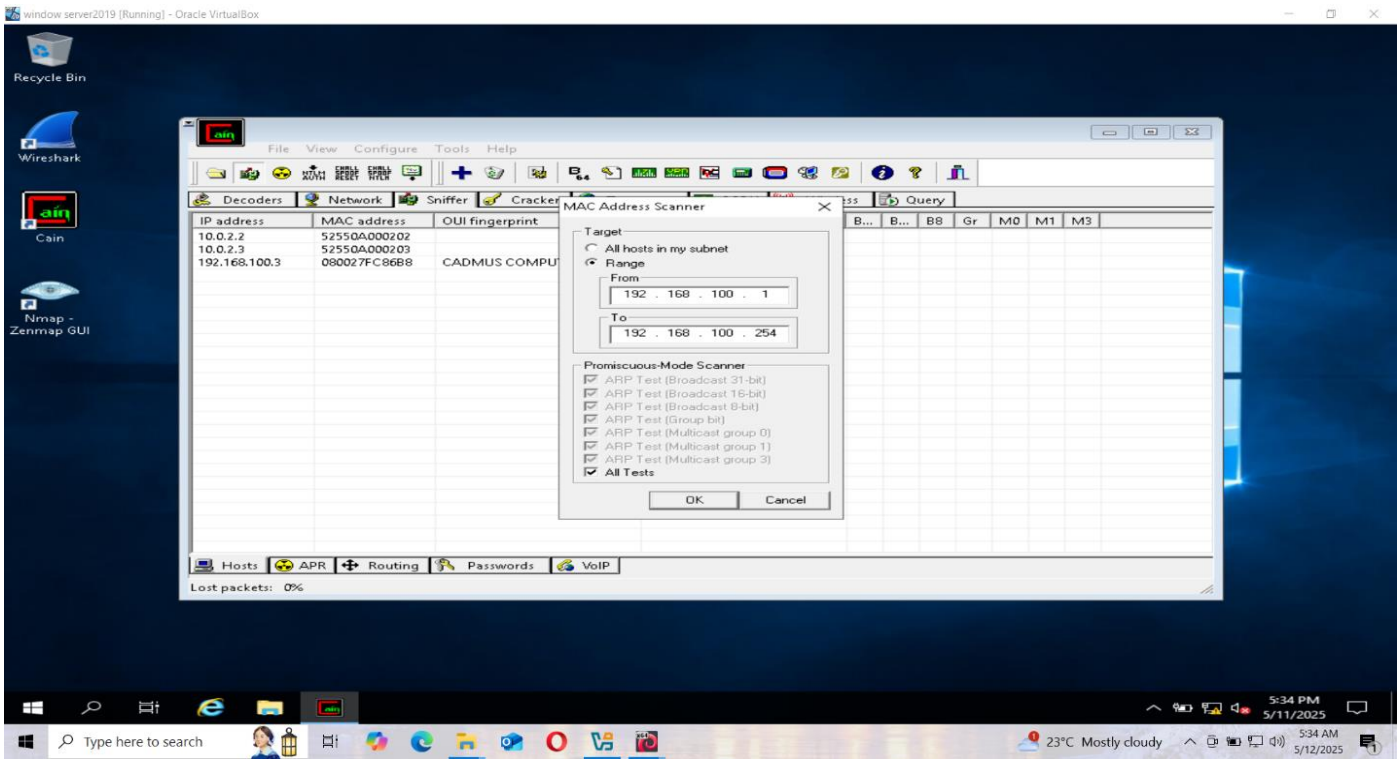
Sniffing tools like Cain & Abel intercept packets in promiscuous mode, allowing detection of ARP spoofing.

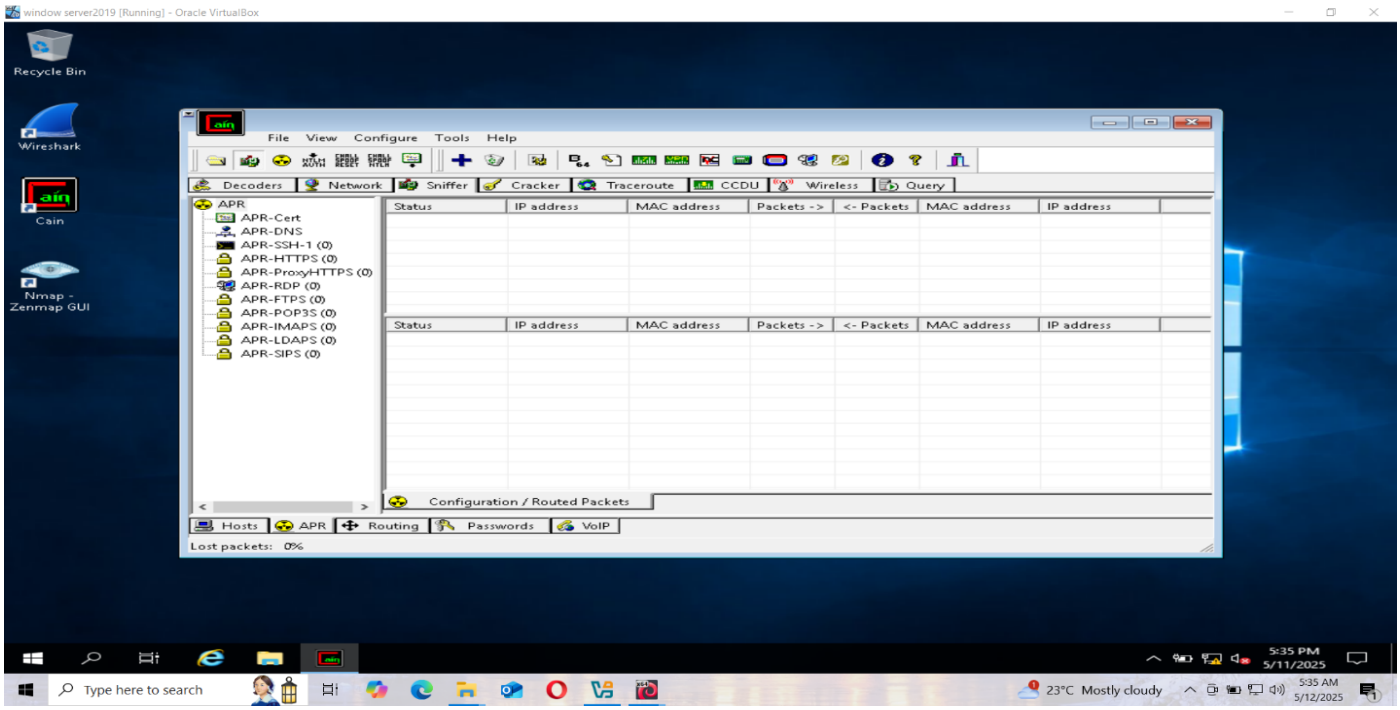
3. Scan MAC Addresses to identify connected hosts.
    - Why? This helps in mapping IP-MAC relationships to detect anomalies.

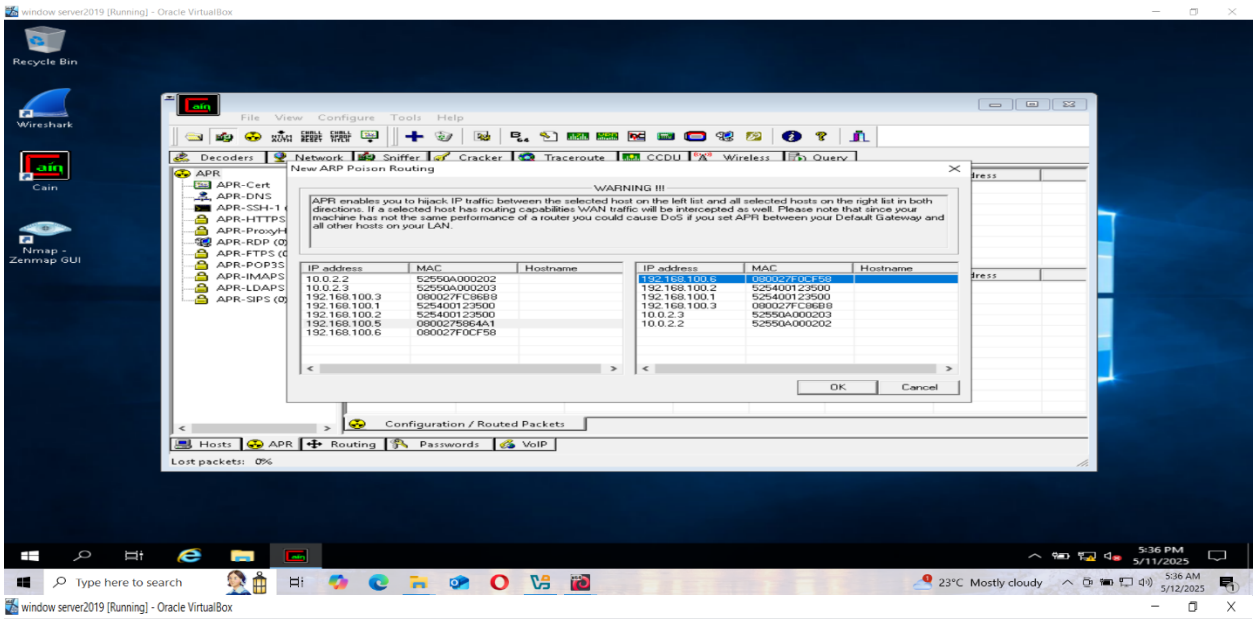


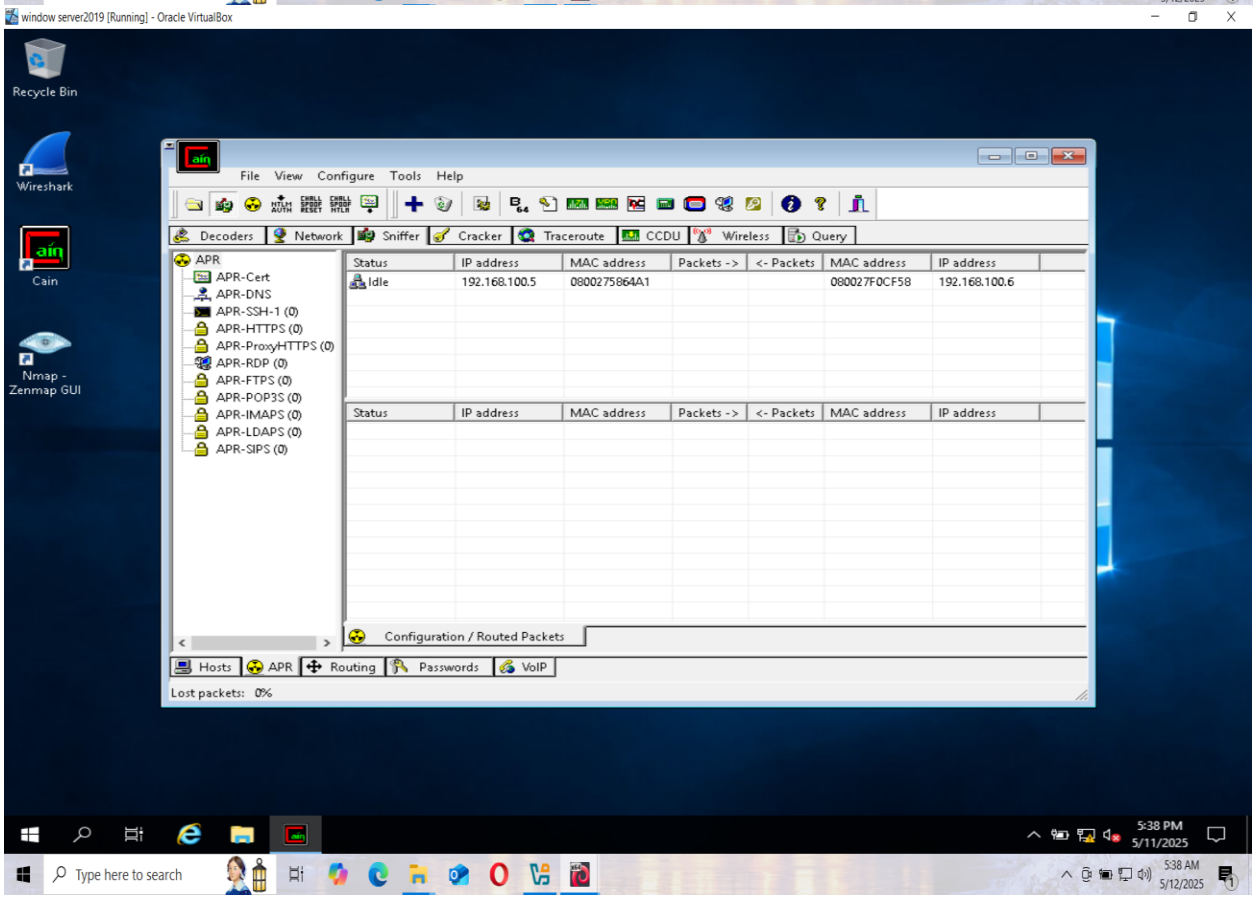

window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Configuration Dialog
Decoders Network Sniffer
Challenge Spoofing Filters and ports HTTP Fields
Traceroute Certificate Spoofing Certificates Collector
Sniffer APR (Arp Poison Routing) APR-SSL Options
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Adapter
IP address
Subnet Mask
\Device\NPF_{A9EBE0...
192.168.100.4
255.255.255.0
Winpcap Version
4.1.0.2980
Current Network Adapter
\Device\NPF_{A9EBE0FF-FD09-4E19-93E2-679362BF5A59}
WARNING !!! Only ethernet adapters supported
Options
Start Sniffer on startup
Don't use Promiscuous mode
Start APR on startup
OK
Cancel
Apply
Help
Protected Storage
http://www.oxid.it
Type here to search
23°C Mostly cloudy
5:33 PM
5/11/2025
5:33 AM
5/12/2025


window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address
MAC address
OUI fingerprint
Host name
B...
B...
B8
Gr
M0
M1
M3
10.0.2.2
52550A000202
10.0.2.3
52550A000203
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
5:34 PM
5/11/2025
5:34 AM
5/12/2025


window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Decoders Network Sniffer Cracker Query
IP address MAC address OUI fingerprint
10.0.2.2 52550A000202
10.0.2.3 52550A000203
192.168.100.3 080027FC86B8 CADMUS COMPU
MAC Address Scanner
Target
All hosts in my subnet
Range
From 192 . 168 . 100 . 1
To 192 . 168 . 100 . 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
OK Cancel
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
23°C Mostly cloudy
5:34 PM 5/11/2025
5:34 AM 5/12/2025

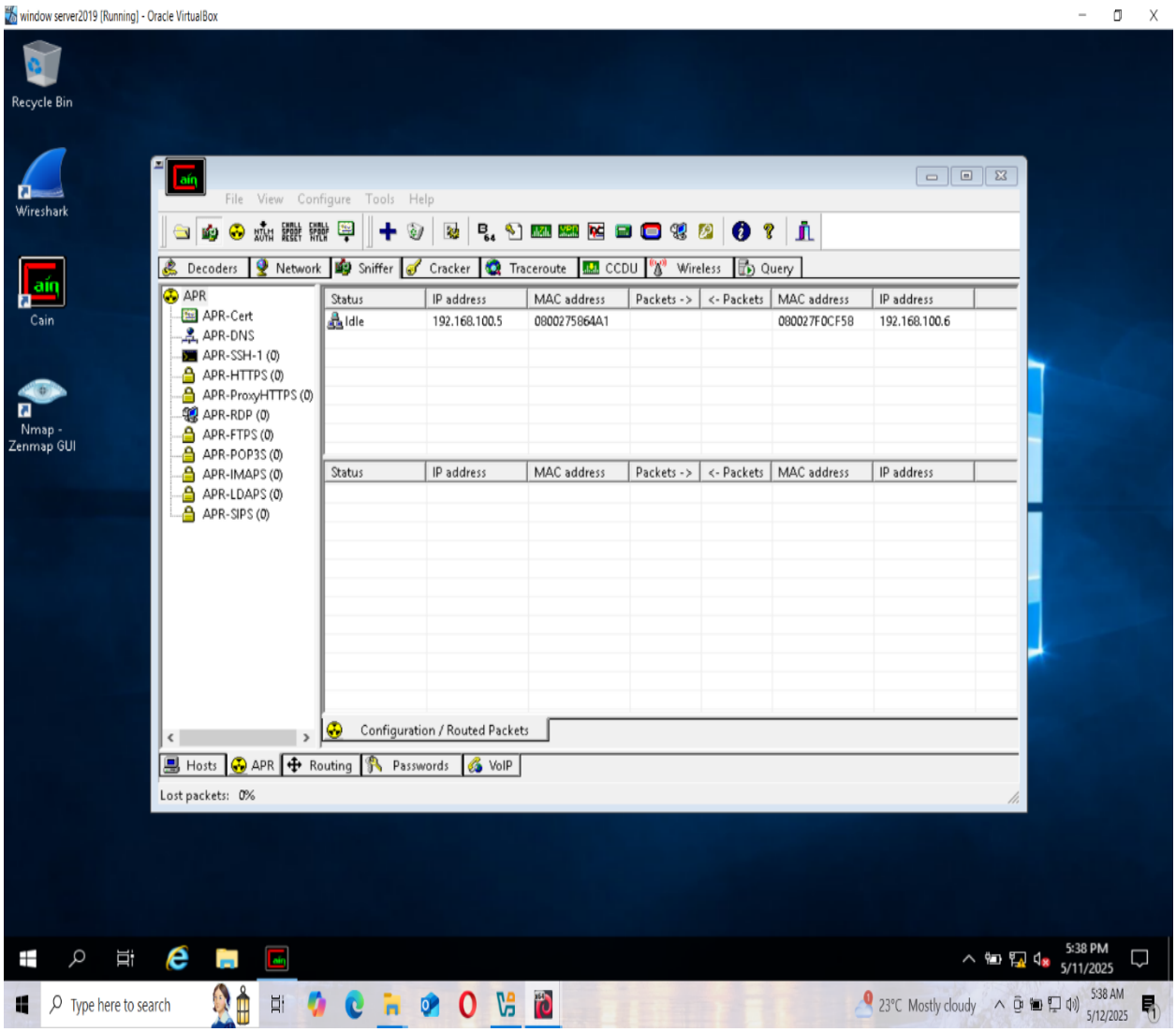

window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
23°C Mostly cloudy
5:35 PM 5/11/2025
5:35 AM 5/12/2025

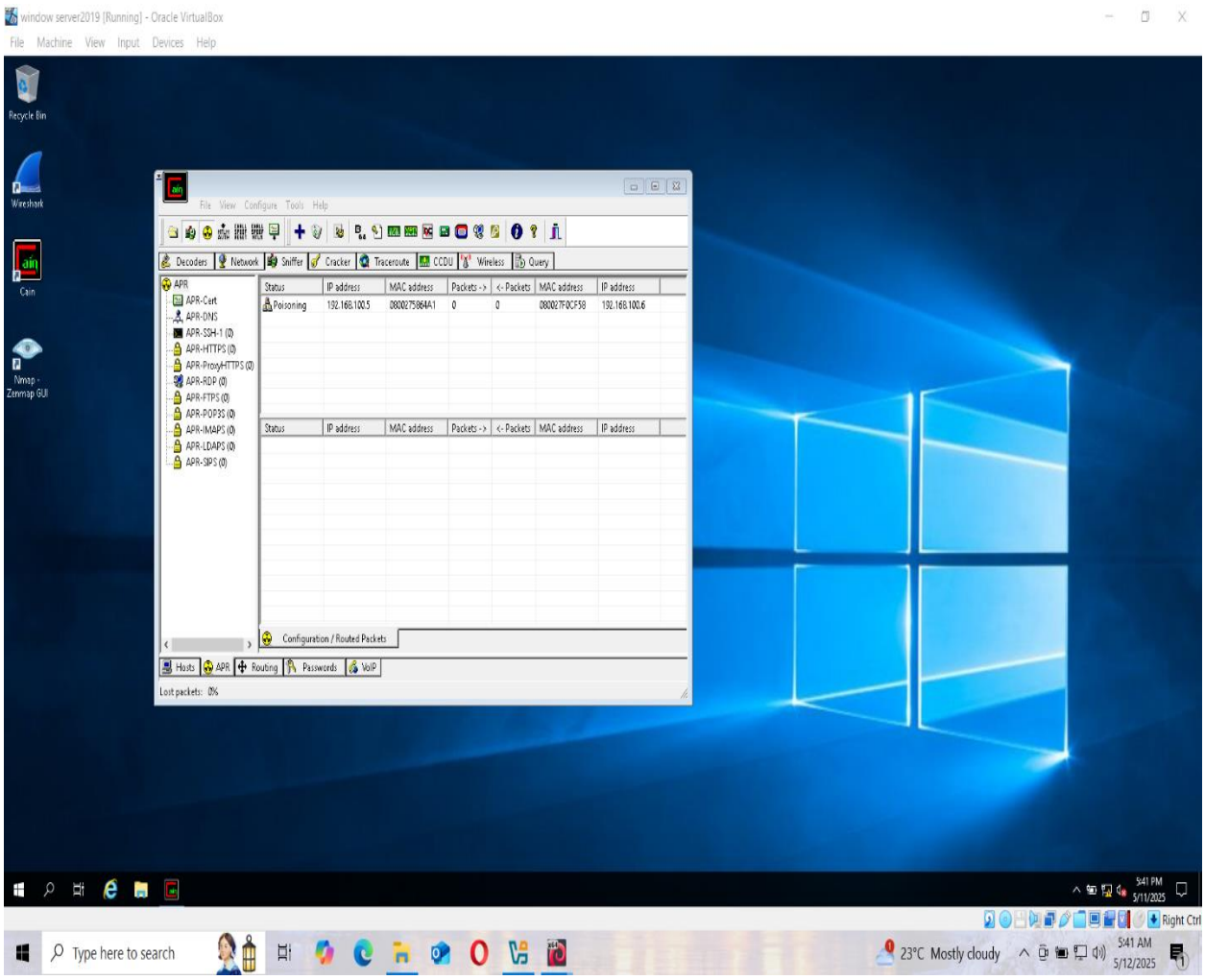

window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address MAC Hostname
10.0.2.2 52550A000202
10.0.2.3 52550A000203
192.168.100.3 080027FC86B8
192.168.100.1 525400123500
192.168.100.2 525400123500
192.168.100.5 0800275864A1
192.168.100.6 080027F0CF58
OK Cancel
APR
APR-Cert
APR-DNS
APR-SSH-1
APR-HTTPS
APR-ProxyH
APR-RDP (0)
APR-FTPS
APR-POP3S
APR-IMAPS
APR-LDAPS
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
23°C Mostly cloudy
5:36 PM 5/11/2025
5:36 AM 5/12/2025


window server2019 [Running] - Oracle VirtualBox
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.100.5 0800275864A1 080027F0CF58 192.168.100.6
Status IP address MAC address Packets -> <- Packets MAC address IP address
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
5:38 PM 5/11/2025
5:38 AM 5/12/2025

➢ Step 2: Perform ARP Poisoning Attack

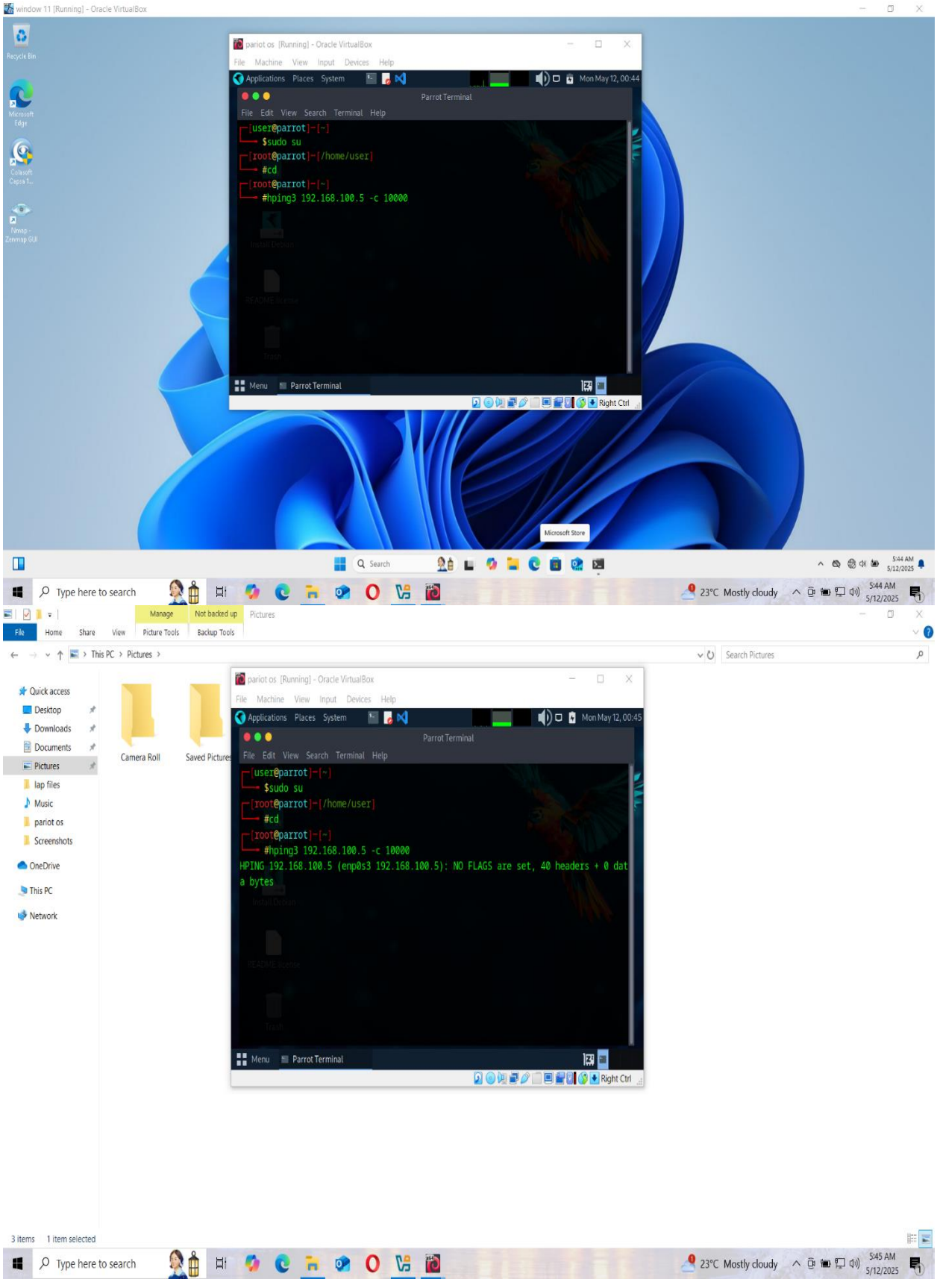
1. **Select Target IPs** (Windows 11 and Parrot Security).
2. **Activate ARP Poisoning** to redirect traffic.
    - Why? ARP poisoning tricks devices into sending data to the attacker instead of the legitimate destination.

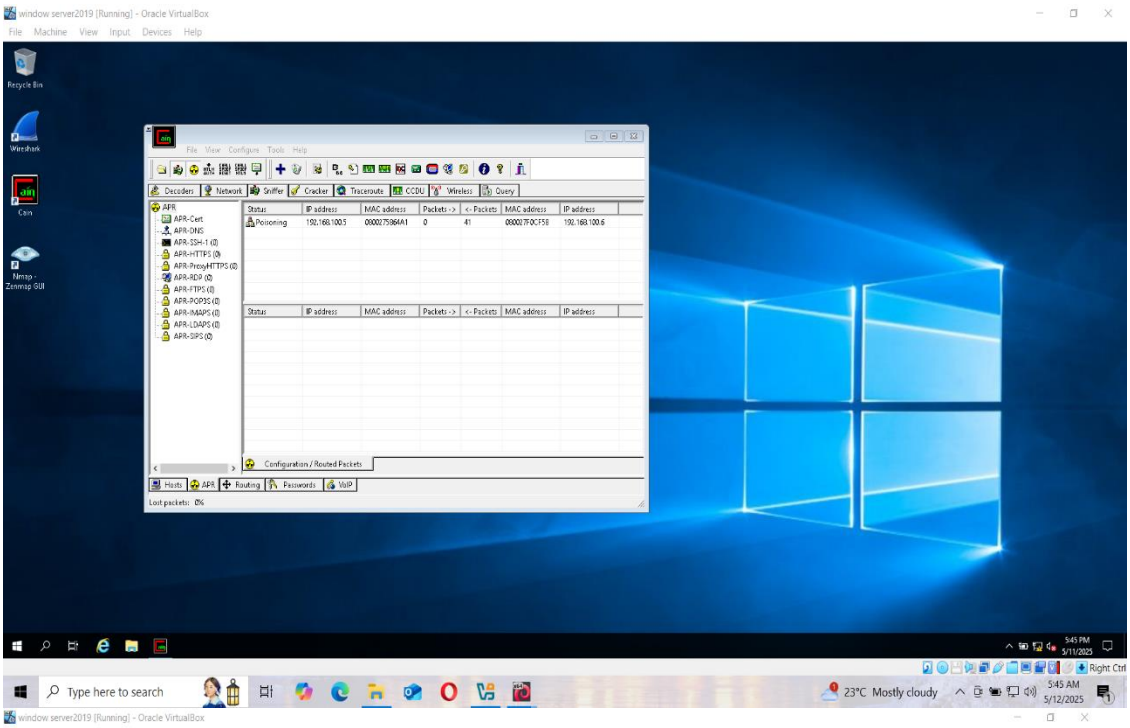


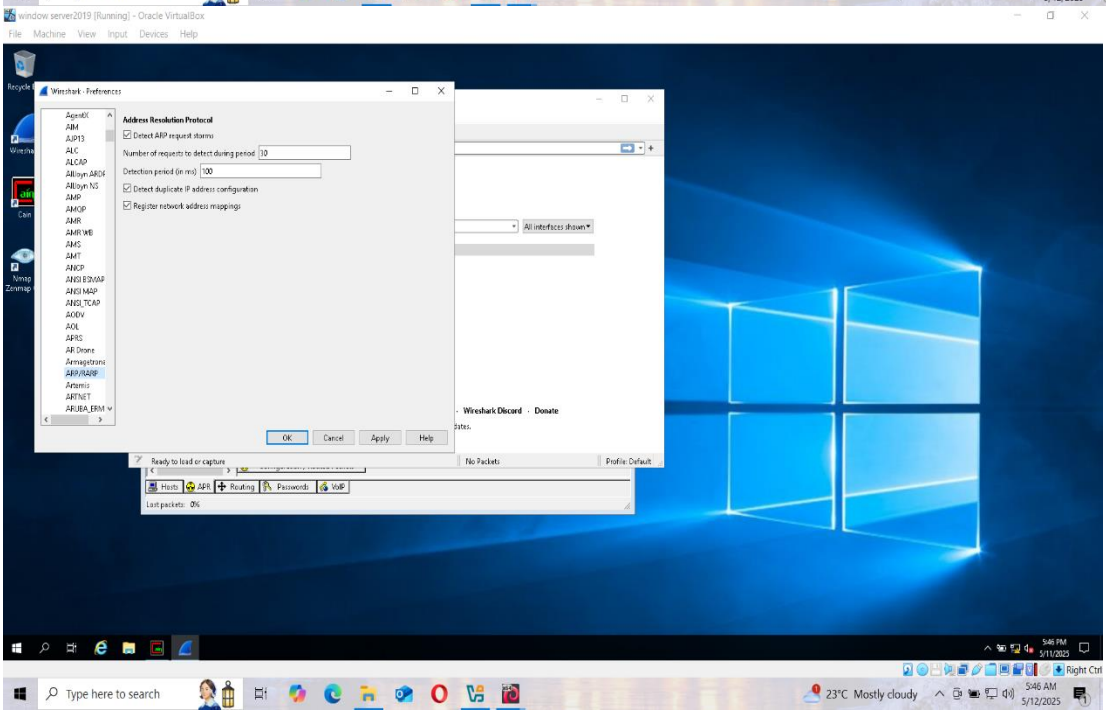


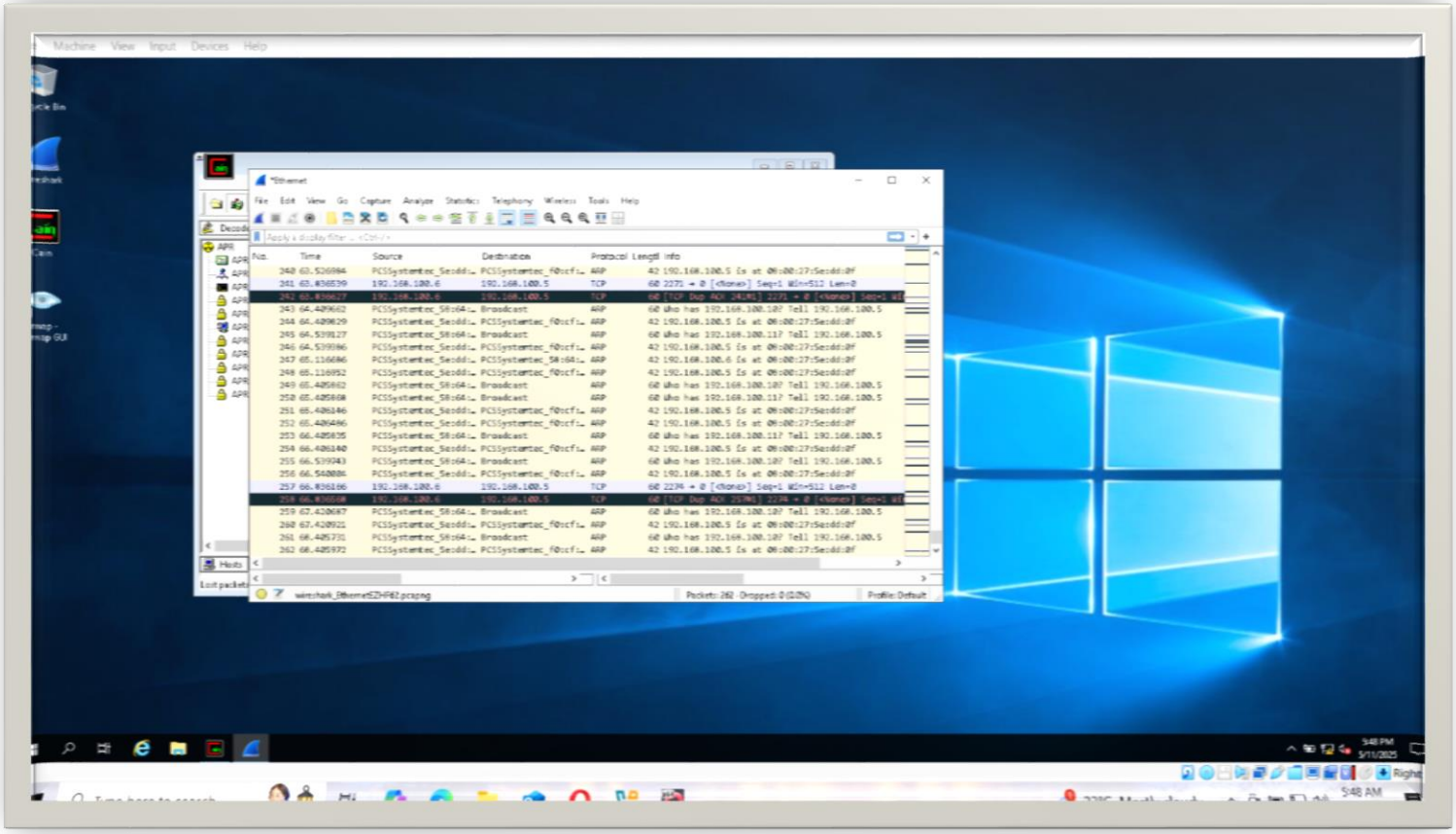
Step 3: Detect ARP Poisoning Using Wireshark

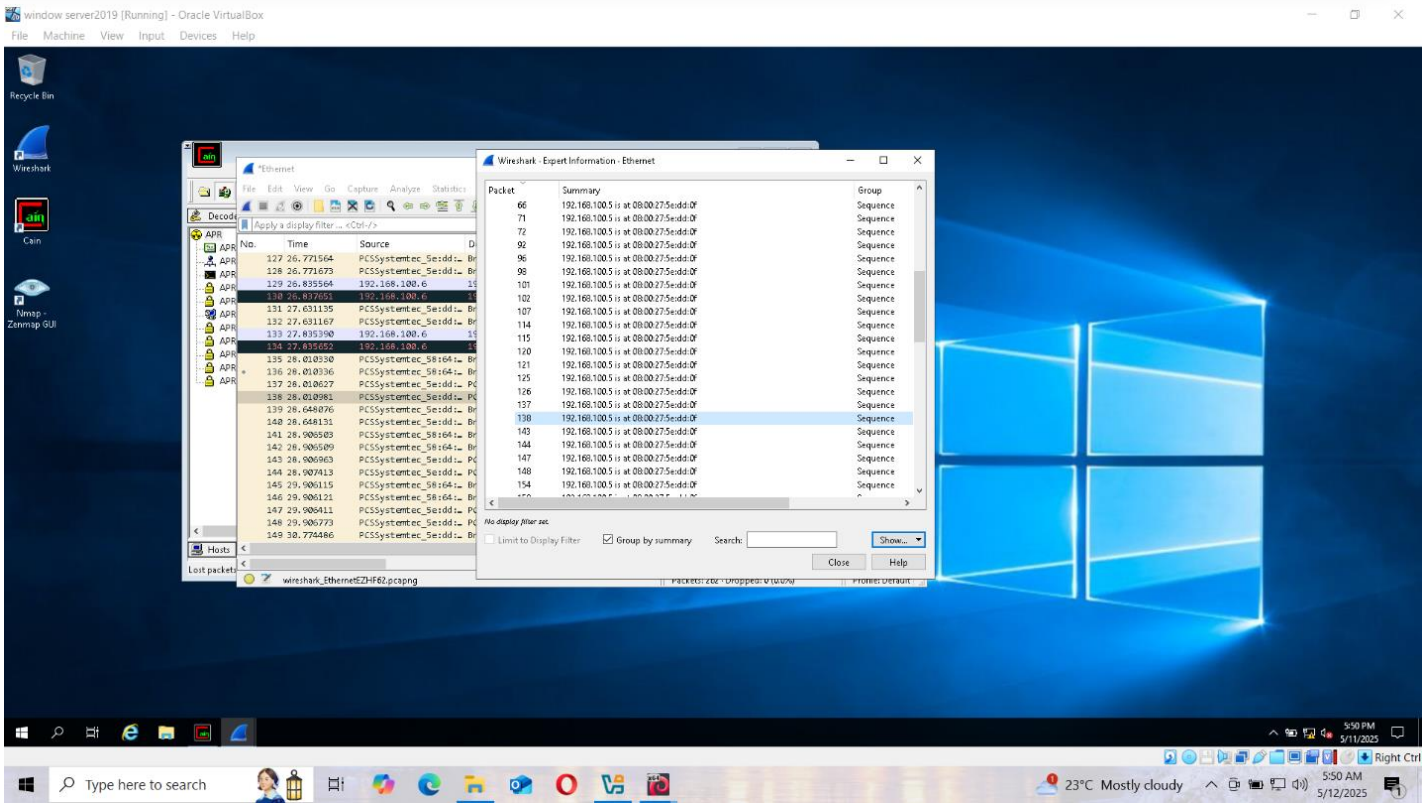
1. Open Wireshark on Windows Server 2019.
2. Filter for ARP Packets (arp filter).
3. Look for Duplicate IP-MAC Entries (indicating ARP spoofing).
    - Why? Legitimate networks should not have multiple MACs for the same IP


window 11 [Running] - Oracle VirtualBox
pariot os [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon May 12, 00:44
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~[~]
$sudo su
[root@parrot]~[/home/user]
#cd
[root@parrot]~[~]
#hping3 192.168.100.5 -c 10000
Menu
Parrot Terminal
Right Ctrl
Microsoft Store
Search
Type here to search
23°C Mostly cloudy
5:44 AM
5/12/2025
Manage
Not backed up
Pictures
File Home Share View Picture Tools Backup Tools
This PC > Pictures >
Search Pictures
Quick access
Desktop
Downloads
Documents
Pictures
lap files
Music
pariot os
Screenshots
OneDrive
This PC
Network
Camera Roll
Saved Pictures
Mon May 12, 00:45
#hping3 192.168.100.5 -c 10000
HPING 192.168.100.5 (enp0s3 192.168.100.5): NO FLAGS are set, 40 headers + 0 data bytes
3 items
1 item selected
5:45 AM


window server2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
Cain
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 192.168.100.5 000027586A1 0 41 00007FOCF58 192.168.100.6
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
23°C Mostly cloudy
5:45 AM
5/12/2025
Right Ctrl


window server2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Wireshark - Preferences
Address Resolution Protocol
Detect ARP request storms
Number of requests to detect during period 10
Detection period (in ms) 100
Detect duplicate IP address configuration
Register network address mappings
OK Cancel Apply Help
Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Type here to search
23°C Mostly cloudy
5:46 AM
5/12/2025
Right Ctrl

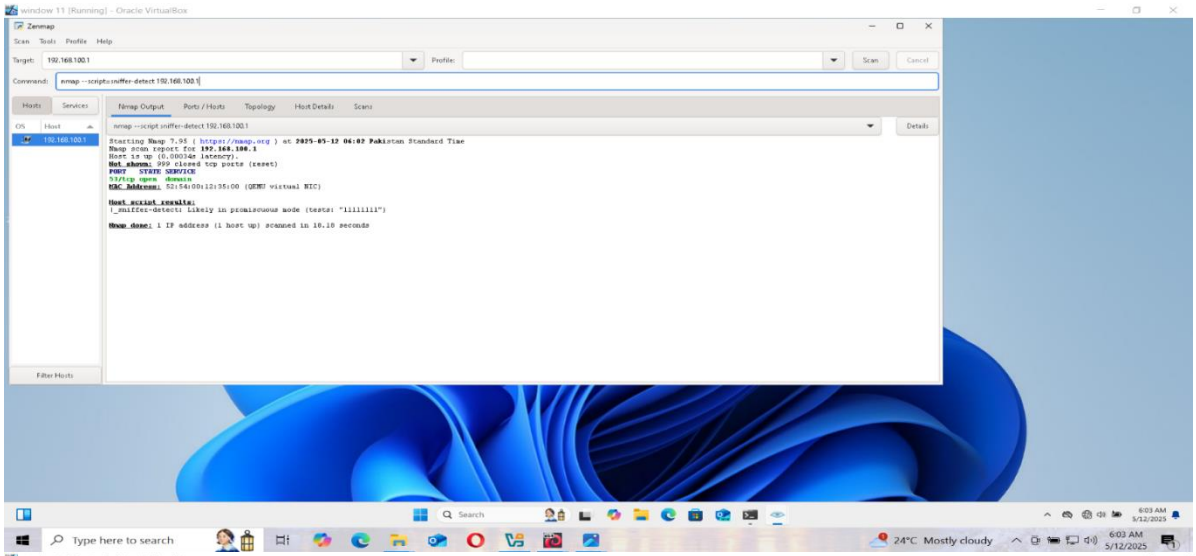


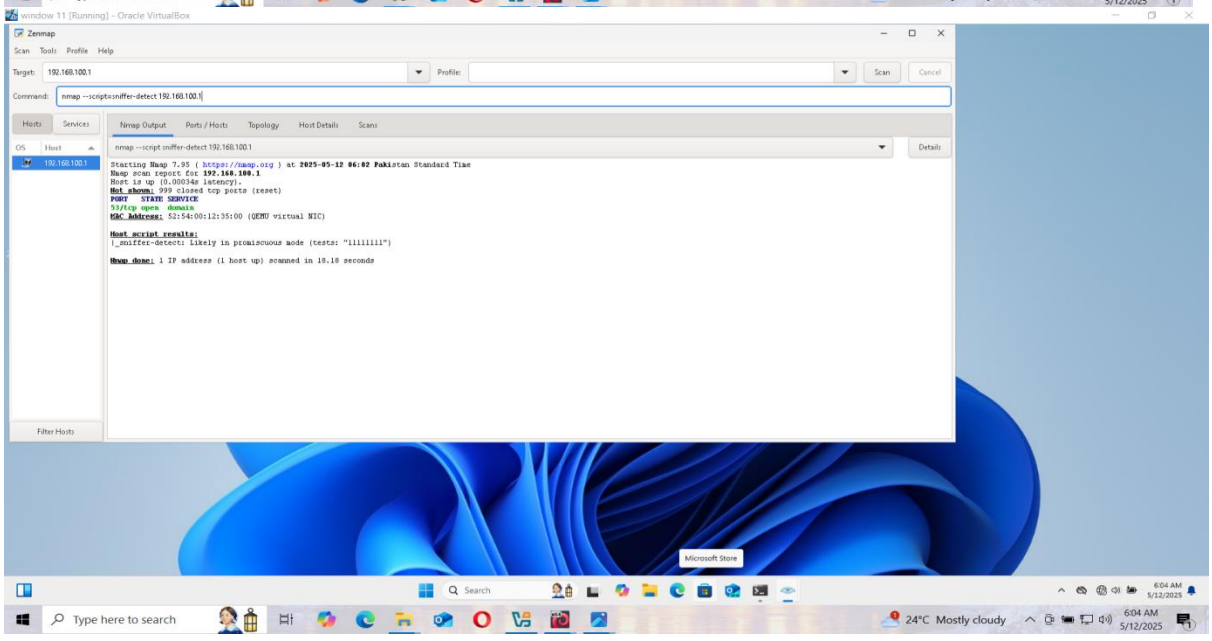

window server2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Wireshark
Cain
Nmap - Zenmap GUI
Wireshark · Expert Information · Ethernet
Type here to search
23°C Mostly cloudy
5:50 AM
5/12/2025

➢ Task 2: Detecting Promiscuous Mode Using Nmap

➢ Step 1: Check for Promiscuous Mode on Windows 11

1. Open Zenmap (Nmap GUI) on Windows 11.
2. Run Command: nmap --script=sniffer-detect [Target IP]
3. Analyze Results: If "Likely in promiscuous mode" appears, the target is sniffing traffic.
    - Why? Promiscuous mode allows a NIC to capture all traffic, not just intended packets.





➢ Lab Analysis & Conclusion

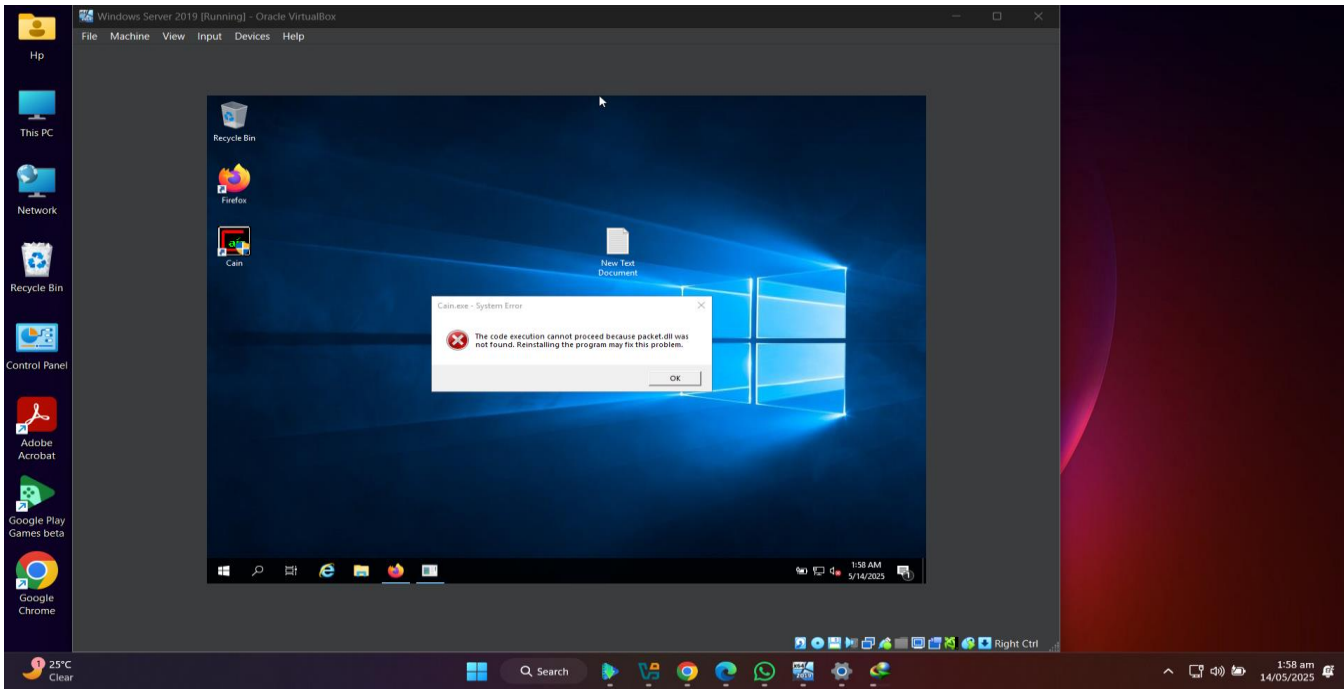
- **Findings:**
    - ARP poisoning was successfully detected using Wireshark (duplicate ARP responses).
    - Promiscuous mode was identified via Nmap's sniffer-detect script.
- **Security Implications:**
    - ARP poisoning can lead to Man-in-the-Middle (MITM) attacks.
    - Promiscuous mode enables unauthorized traffic capture.

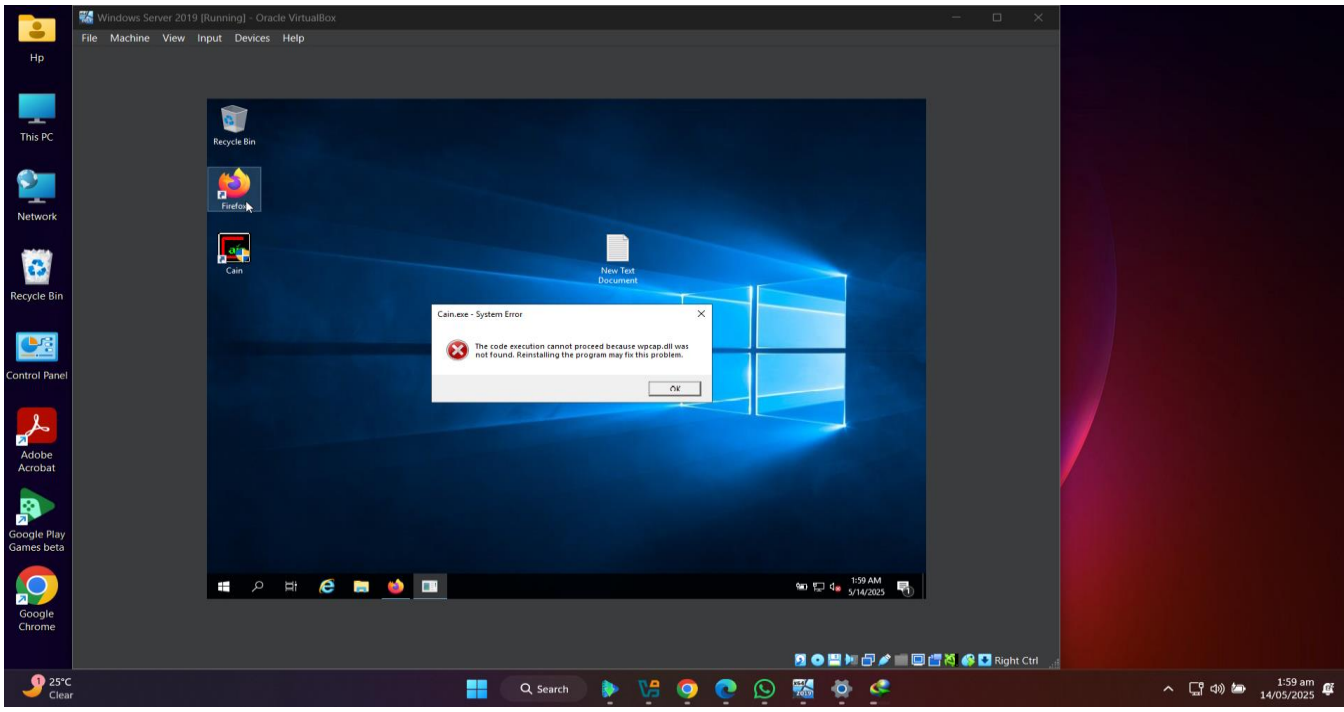
➢ Final Notes:

This lab demonstrated how attackers exploit ARP poisoning and promiscuous mode for sniffing, and how defenders can detect such activities using Wireshark, Cain & Abel, and Nmap. Implementing network monitoring and hardening measures is crucial to prevent such attacks.

➢ ERRORS FACED DURING PERFORMANCE OF LABS

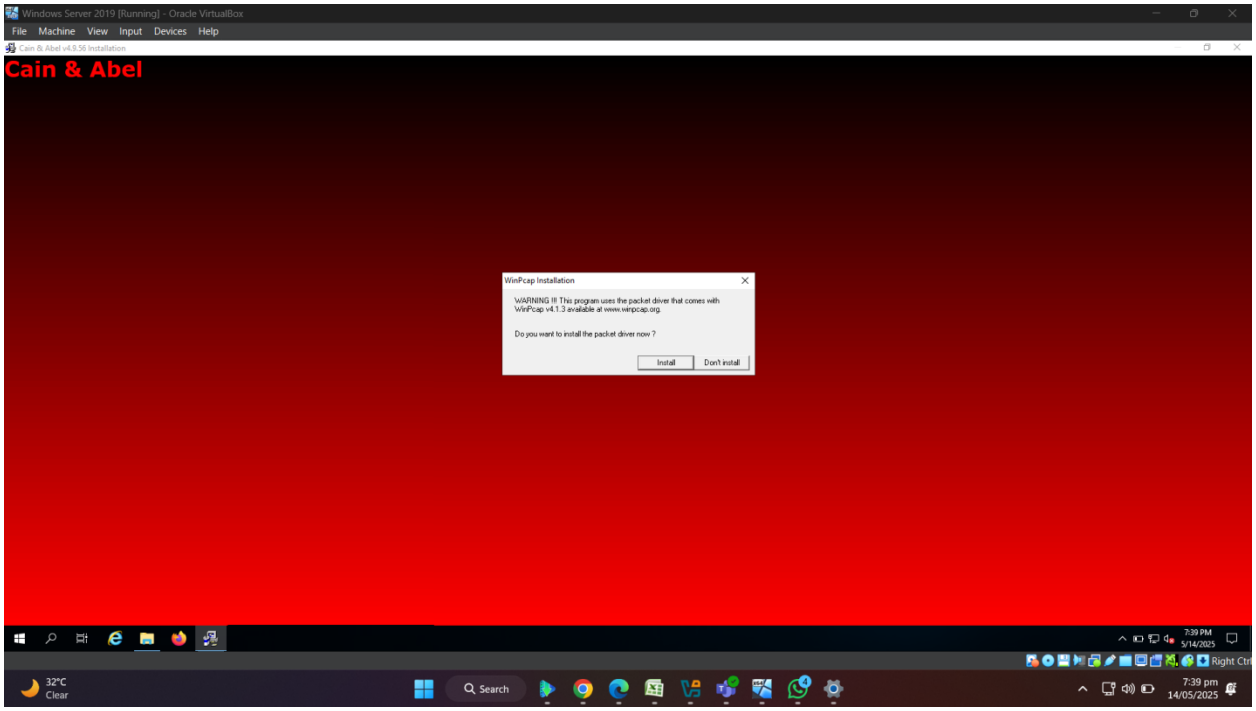
- **Error 1: Compatibility Issues with Windows Server 2019:**
    - The lab environment used Windows Server 2019 on Oracle VirtualBox. Cain & Abel installation failed due to compatibility issues (e.g., "data not found" or missing files like "words all was not found").
    - The program referenced an unsupported OS version ("Windows 9.1.3.2" in resolved.png), likely a typo or misconfiguration.

➢ 



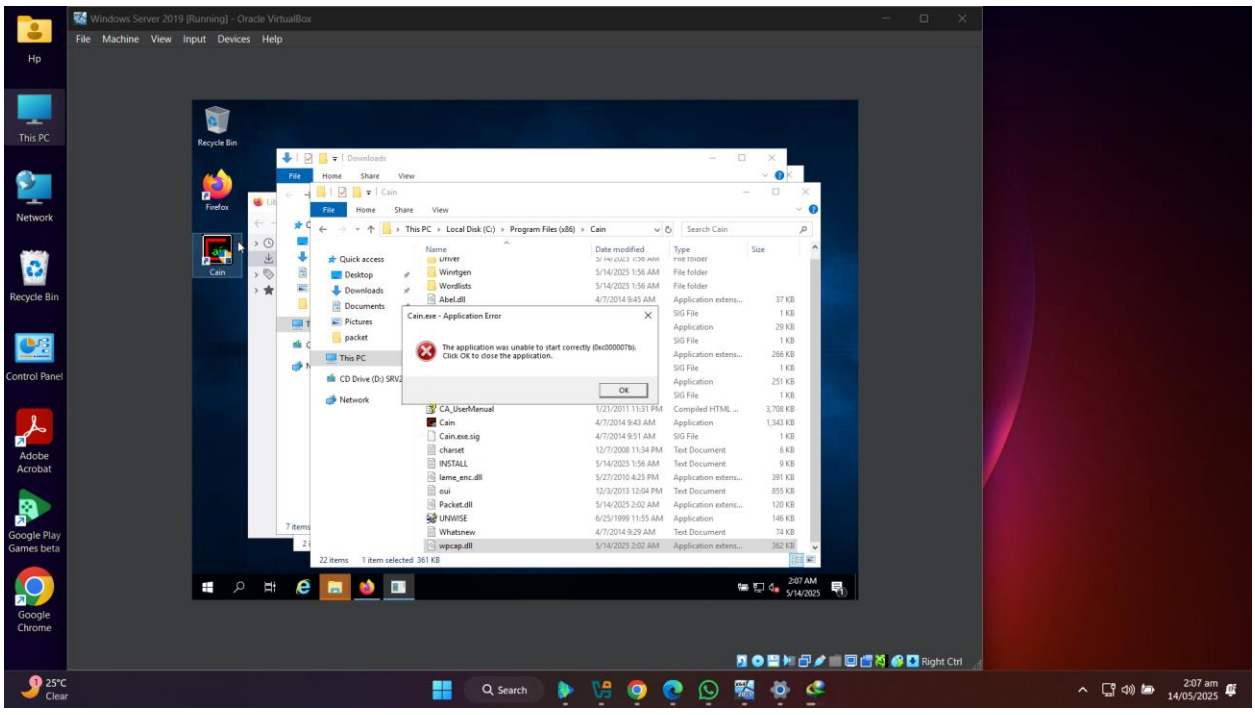
➢ **Solution:**

- Switched to a compatible OS (e.g., Windows 10 or Windows 7 VM) for Cain & Abel.
- Verified VM settings in Oracle VirtualBox to ensure proper resource allocation (RAM, storage).



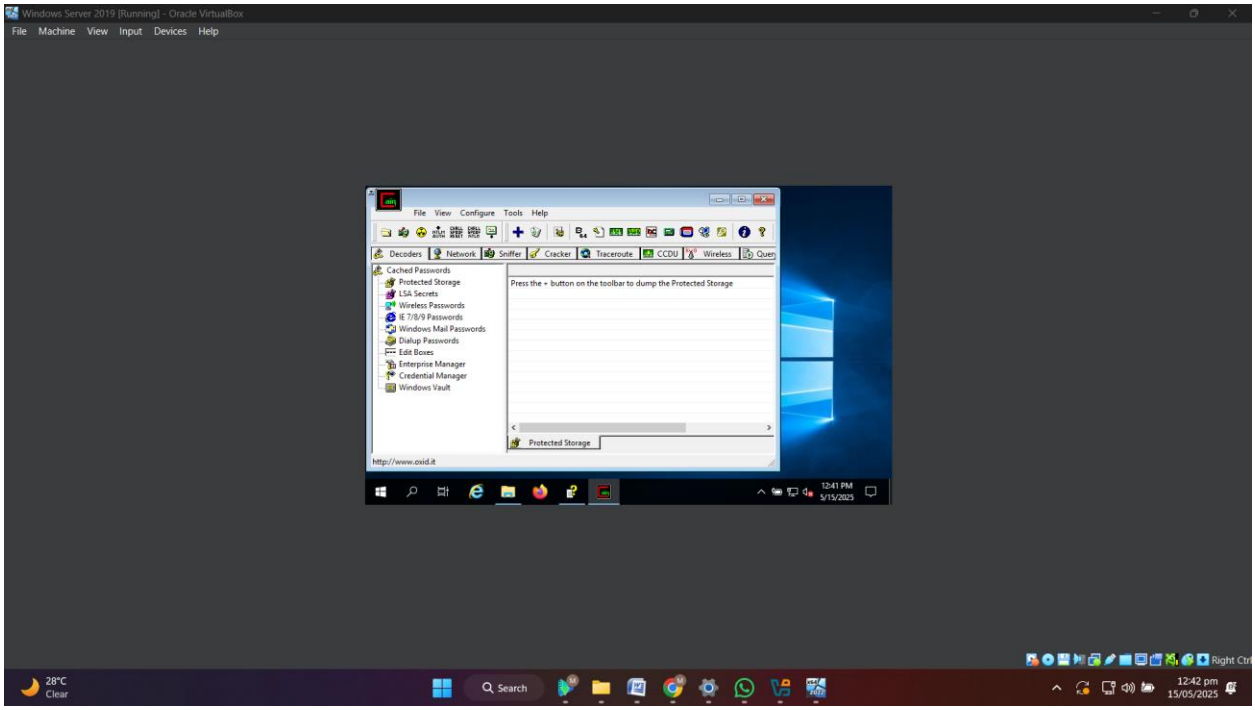
➢ Error 2: Missing Dependencies/Packets

- **Issue Observed (resolved.png):**
  - The installer prompted: "Do you want to install the packet after now?" indicating missing dependencies.



➢ Solution:

- Installed required frameworks like .NET Framework 3.5/4.0 and WinPcap manually before running Cain & Abel.
- Downloaded the correct version of Cain & Abel compatible with the OS.



➢ FINAL LEARNING:

Performing social engineering and sniffing labs underscored the critical intersection of human and technical vulnerabilities in cybersecurity. Social engineering tactics revealed how psychological manipulation can bypass even robust technical defenses, emphasizing the need for continuous user education to combat phishing and pretexting. Sniffing attacks (e.g., ARP poisoning, MAC spoofing) demonstrated the ease of intercepting unencrypted traffic, reinforcing the necessity of encryption (HTTPS, VPNs) and network monitoring tools. These labs highlighted that security is a layered effort—combining technical safeguards like DHCP snooping, static ARP entries, and MAC filtering with human-centric policies. Ethically, these exercises stress the importance of using such skills responsibly to fortify defenses rather than exploit weaknesses. Ultimately, proactive mitigation and awareness are pivotal in defending against both technical exploits and human-targeted attacks.