



MAN-IN-THE-MIDDLE ATTACK USING ARP SPOOFING

Penetration Testing (Assignment: 03)

NAME:

MOEEZ JAVED

REGISTRATION NO:

BCS203213

SECTION: 03

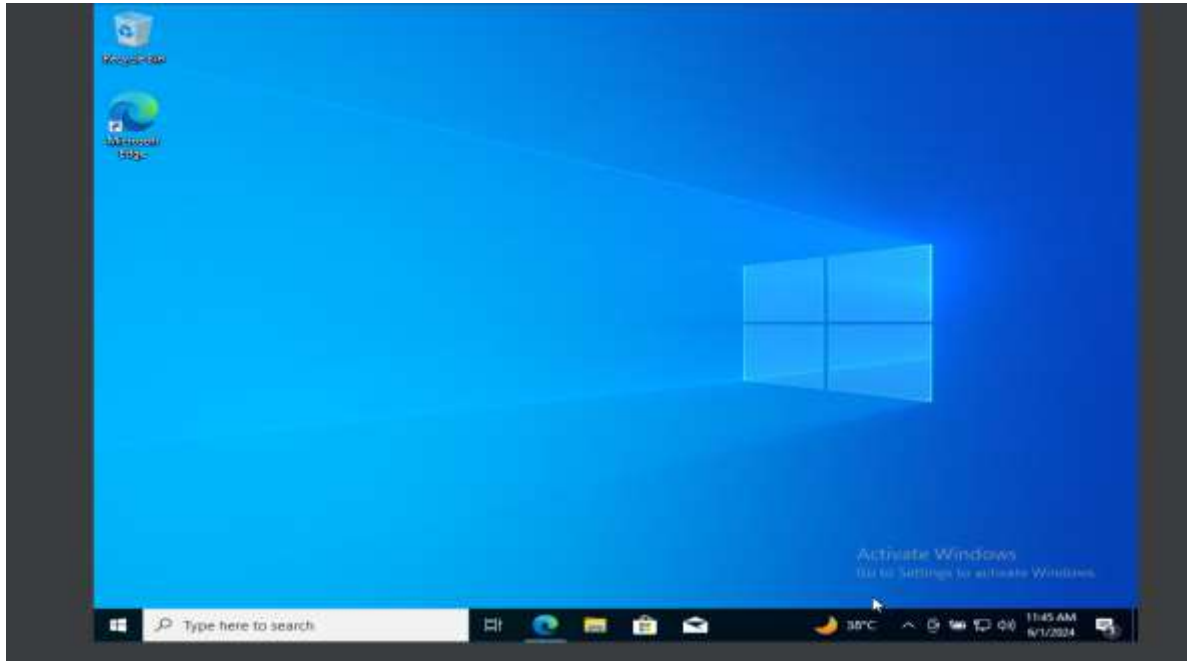
SUBMITTED TO:

RESPECTED MA'AM YAFRA KHAN

Overview: Man in the Middle Attack using ARP poisoning in Ettercap.

Step1:

Download the window 10 and open it



Open terminal

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\moeez>ipconfig#
'ipconfig#' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\moeez>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Home
    Link-local IPv6 Address . . . . . : fe80::fa1a:2299:aa6a:aa%6
    IPv4 Address. . . . . : 192.168.10.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\moeez>
```

Step2:

Metasploit IP Address

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

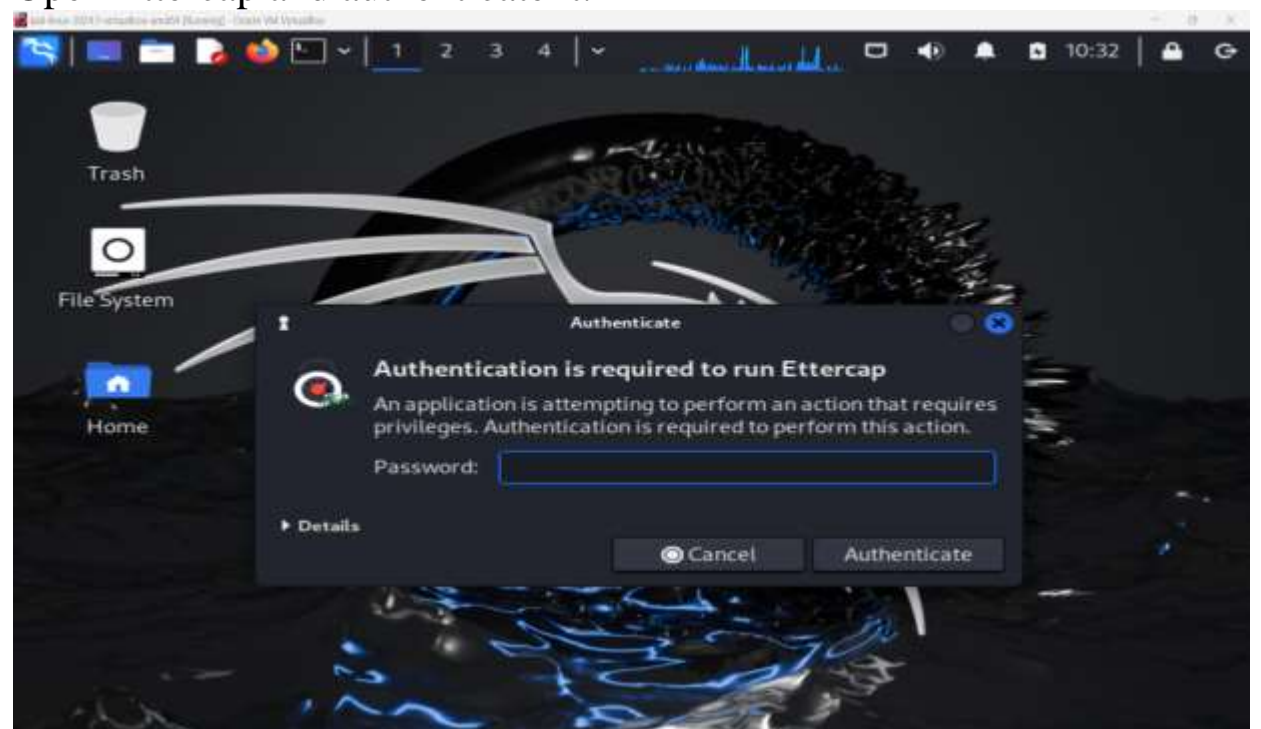
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:cb:b6:88 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.13/24 brd 192.168.10.255 scope global eth0
    inet6 fe80::a00:27ff:feeb:b688/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

Step3:

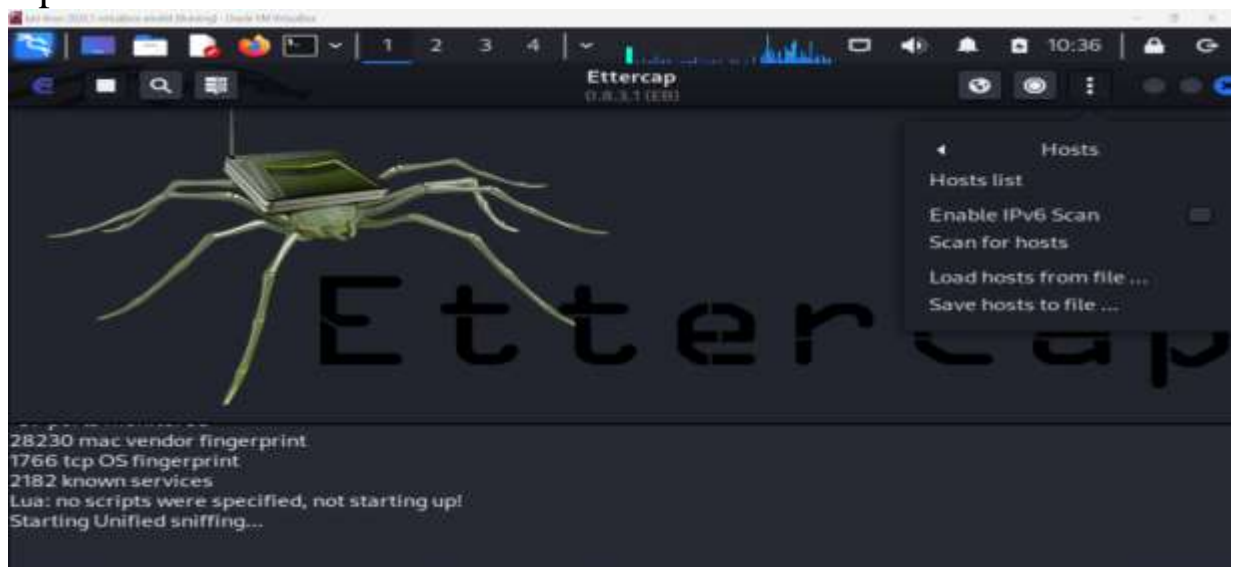
Open Ettercap and authenticate it.



Step4:
Accept the Ettercap



Step5:
Open the Host



Step6:

Scan the Hosts:



Step7:

Host List

Host List: ✕		
IP Address	MAC Address	Description
192.168.10.1	A8:63:7D:97:5E:61	
192.168.10.2	1C:1B:B5:0F:68:47	
192.168.10.3	34:C9:3D:46:EE:A7	
192.168.10.7	5A:FF:98:F4:AC:87	
192.168.10.13	08:00:27:CB:86:88	
192.168.10.16	08:00:27:D7:B3:9B	
192.168.10.111	34:36:54:DD:23:8B	
Delete Host Add to Target 1 Add to Target 2		

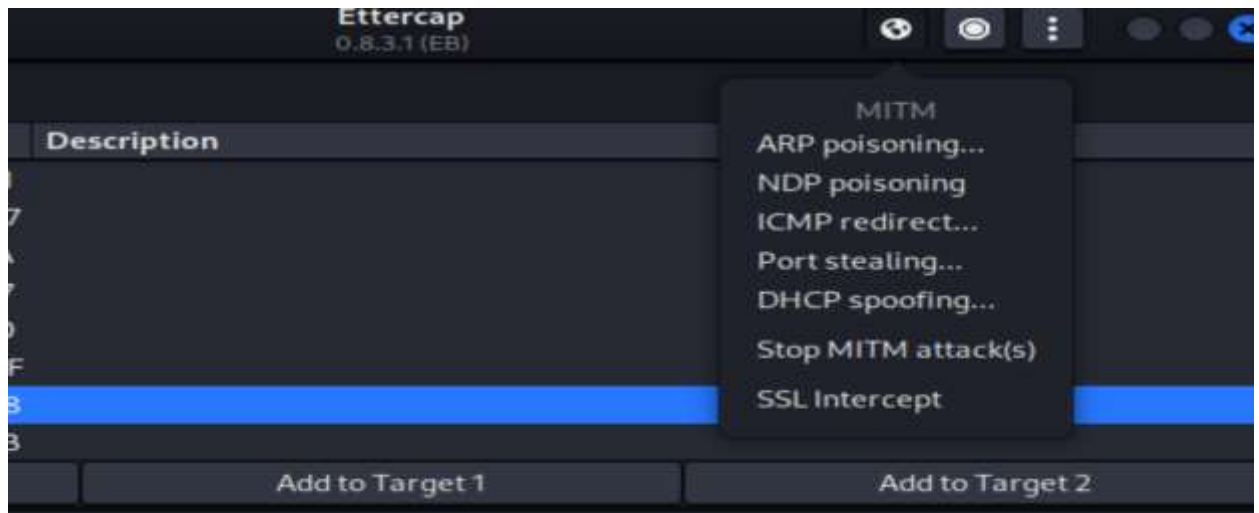
Step8:

Go to the Target and Current Target

Host List ✕		Targets ✕	
Target 1		Target 2	
192.168.10.1		192.168.10.16	
Delete		Delete	
Add		Add	
GROUP 1 : 192.168.10.1 A8:63:7D:97:5E:61			
GROUP 2 : 192.168.10.16 08:00:27:D7:B3:9B			

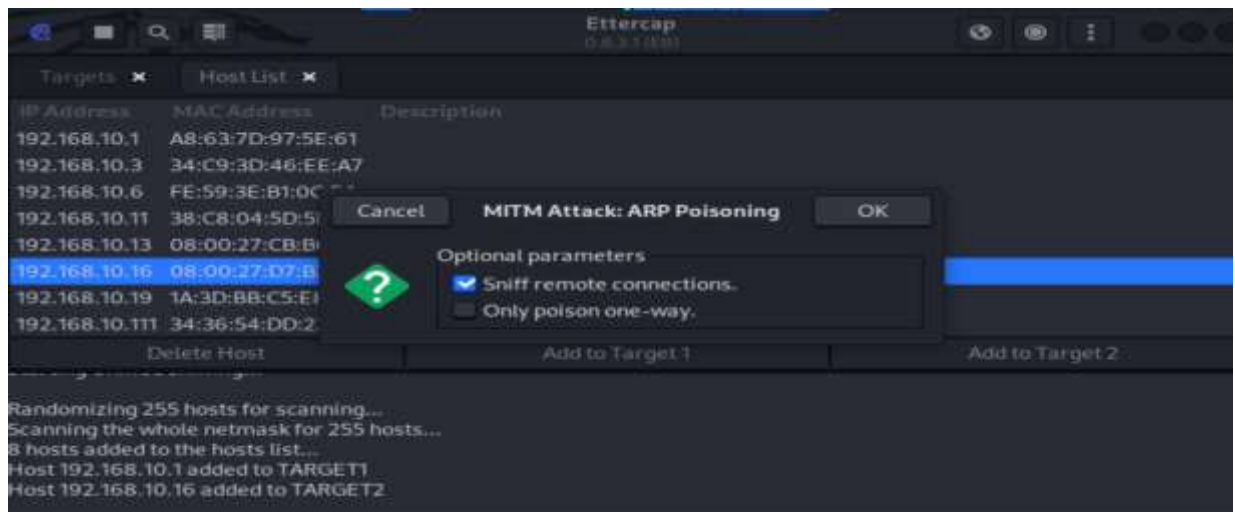
Step9:

Select the ARP poisoning



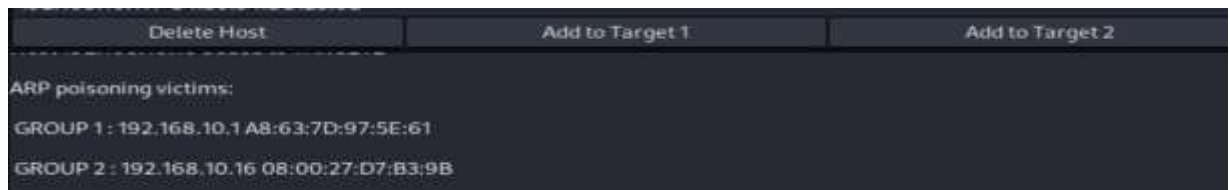
Step10:

Arp Poisoning applying



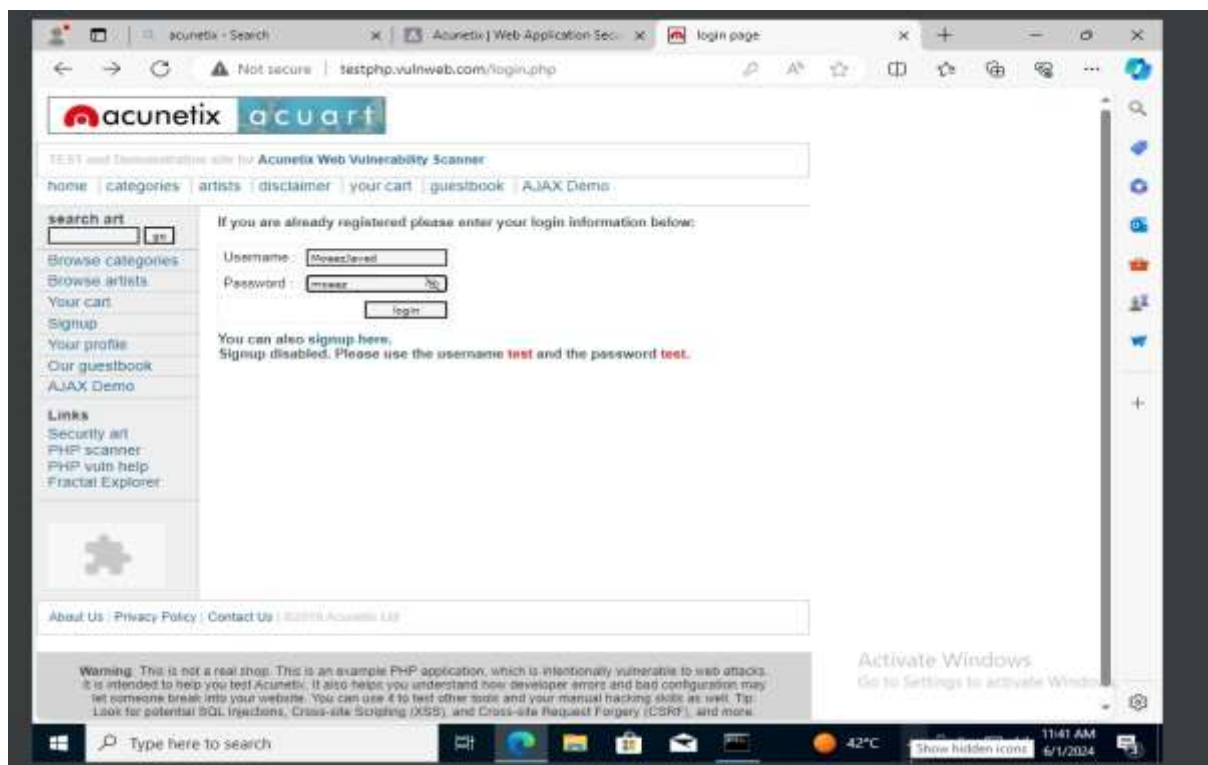
Step11:

Arp poisoning is applied



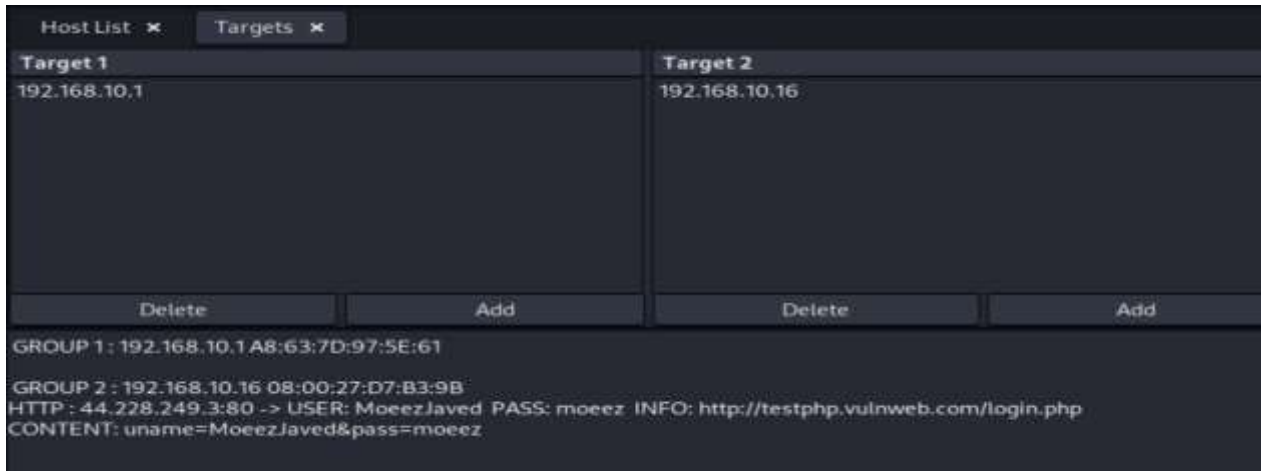
Step12:

Inserting the data in login page that will get sniffed by hacker using ARP poisoning.



Step13:

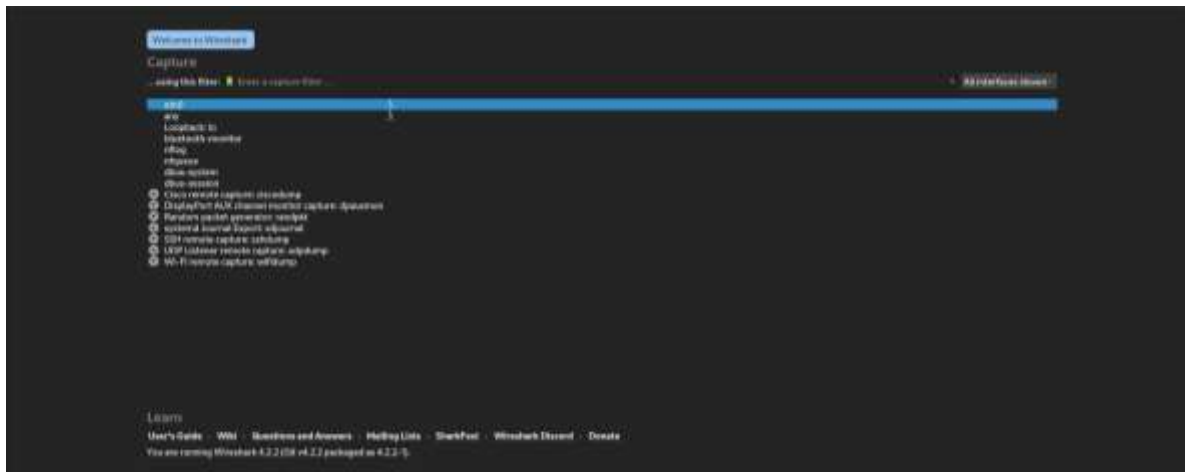
The username and password is heard by the hacker.



WireShark:

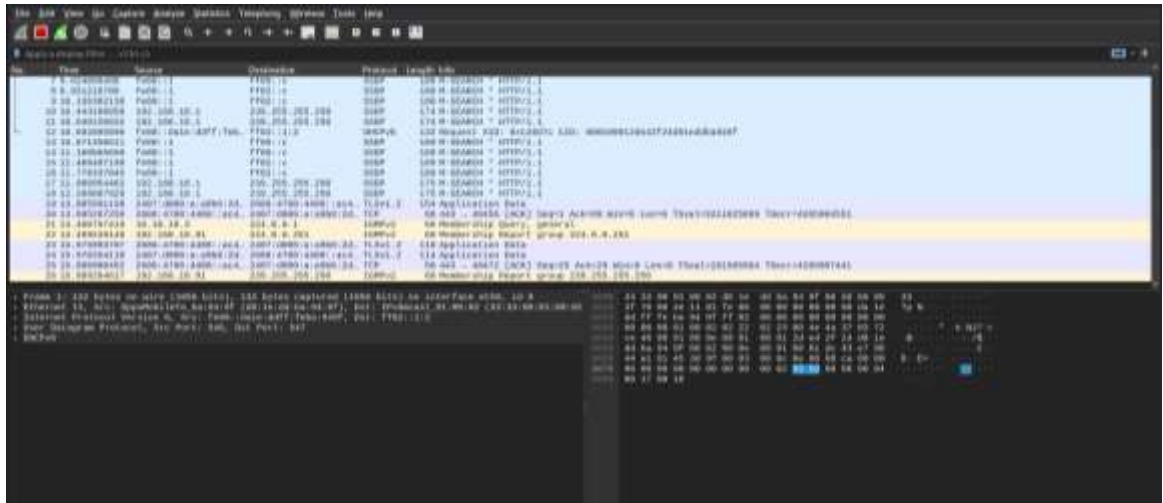
Step14:

Open Wireshark tool for capturing and analyzing network traffic to monitor data packets over the network.



Step15:

Select eth0 option from the list and its interface will get opened.



Conclusions:

This activity taught me about the weaknesses in network communication and how Man-in-the-Middle (MitM) attacks work. Using Ettercap and ARP poisoning, I intercepted traffic between two computers, showing how attackers can steal or change information.

Here are the main things I learned:

- Attackers can make computers send information to them instead of the right person. This is called a Man-in-the-Middle attack.
- They do this by messing with a computer's messaging system (ARP) to give wrong directions. This way, they can steal or change information before it reaches its destination.
- Ettercap is a tool that attackers use to listen in on computer conversations and even change what's being said.