MAN-IN-THE-MIDDLE ATTACK USING ARP SPOOFING

Penetration Testing (Assignment: 03)

NAME:
MOEEZ JAVED

REGISTRATION NO:
BCS203213

SECTION: 03

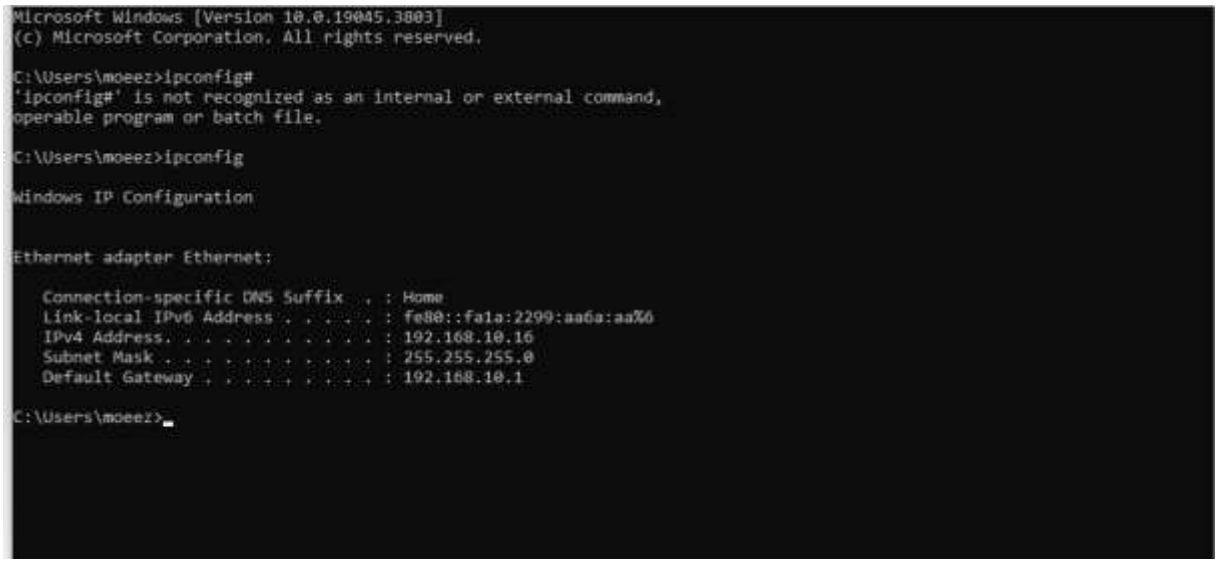
SUBMITTED TO:
RESPECTED MA'AM YAFRA KHAN

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

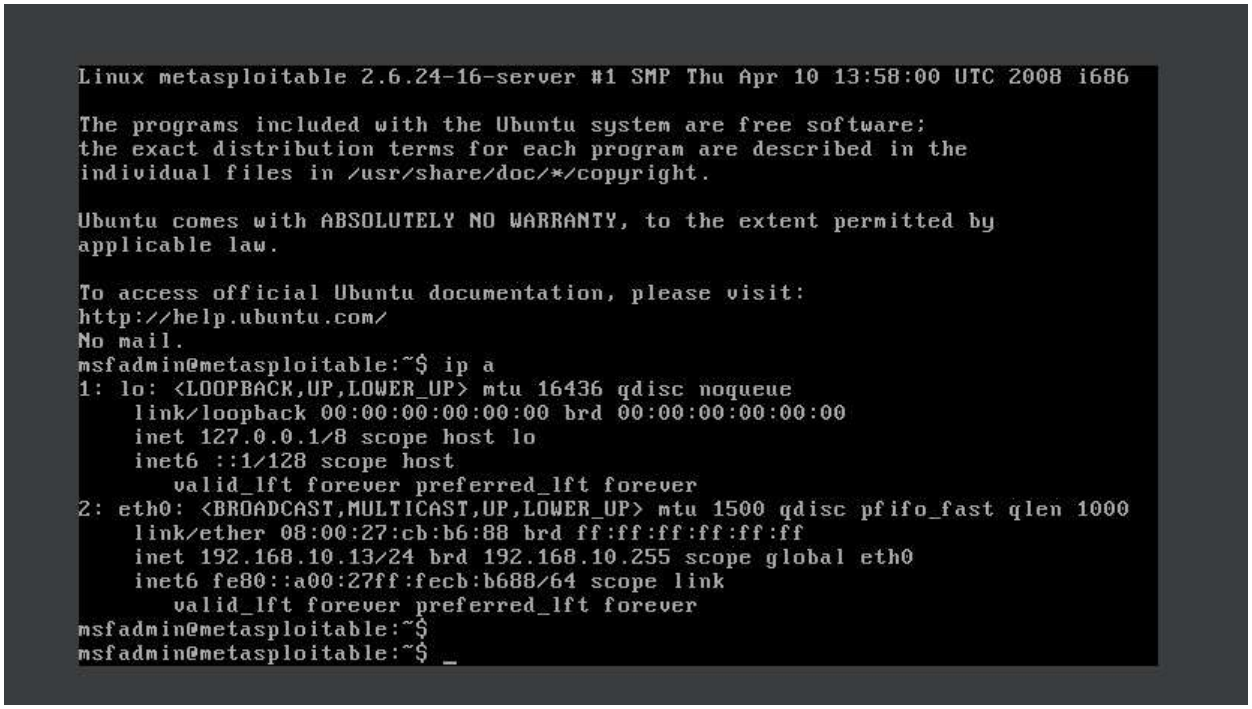
Step1:

Download the window 10 and open it

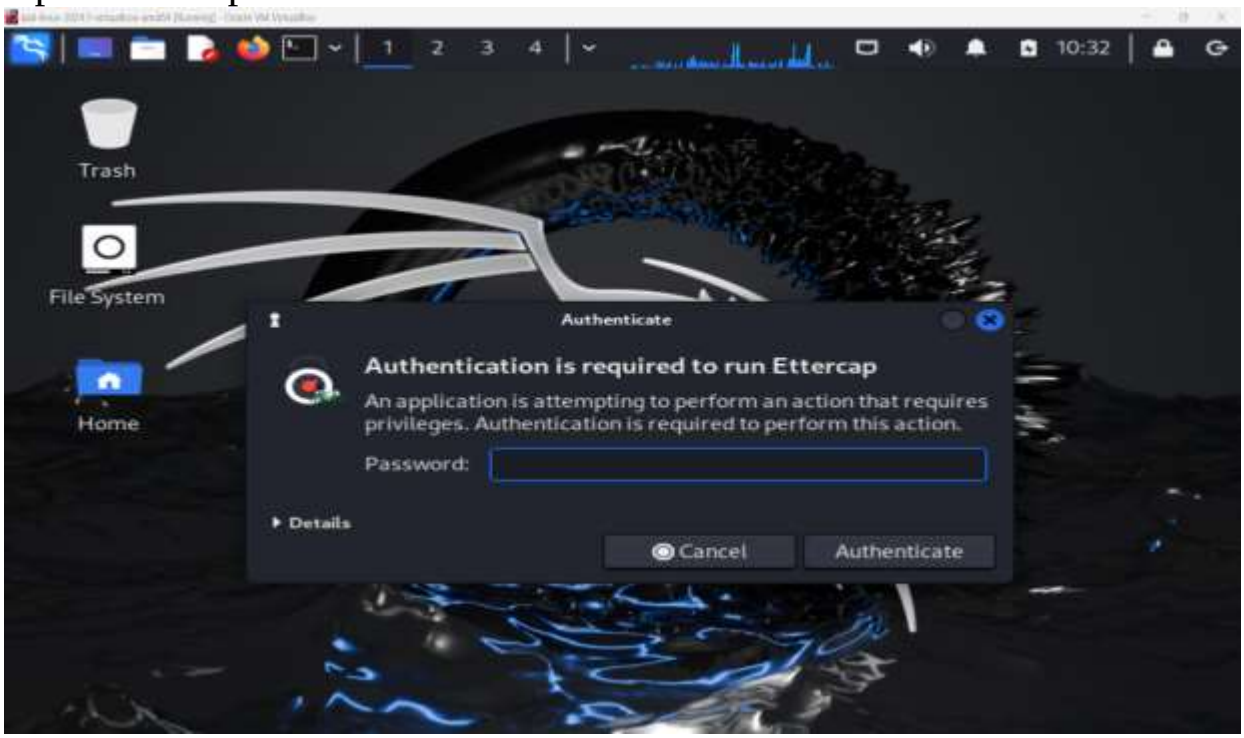
Open terminal



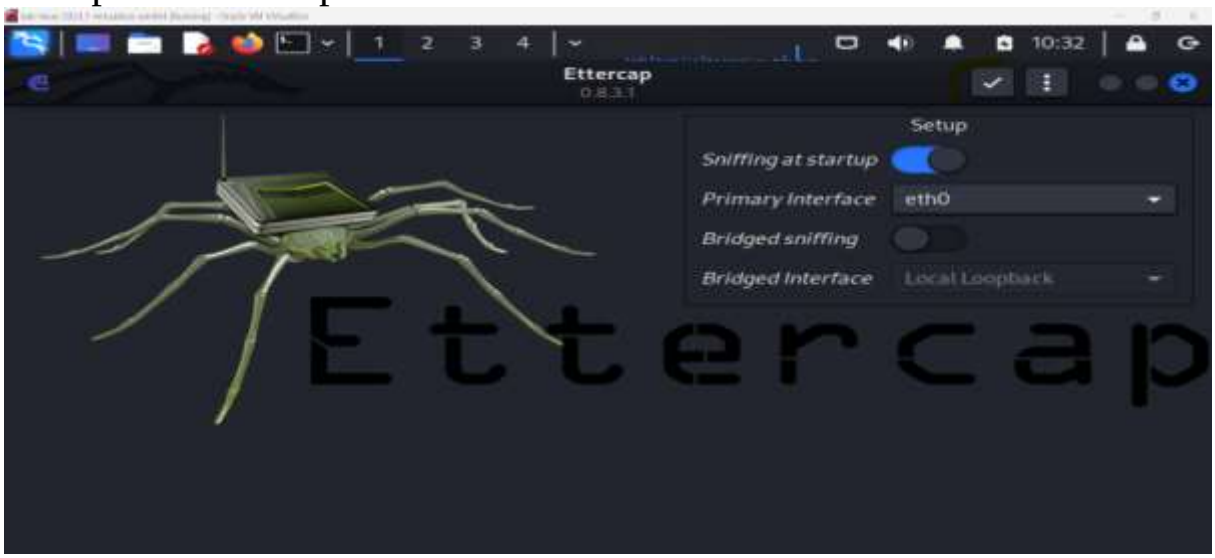
Step2:
Metasploit IP Address



Step3:
Open Ettercap and authenticate it.



Step4:
Accept the Ettercap



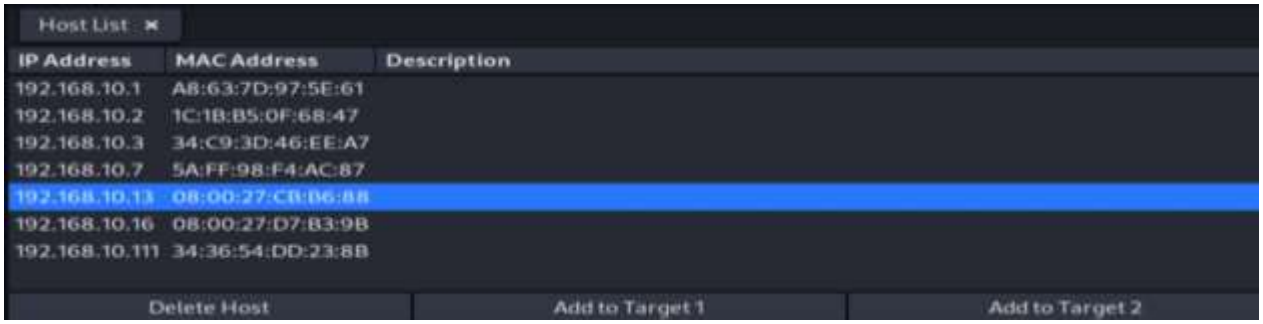
Step5:
Open the Host

Step6:

Scan the Hosts:

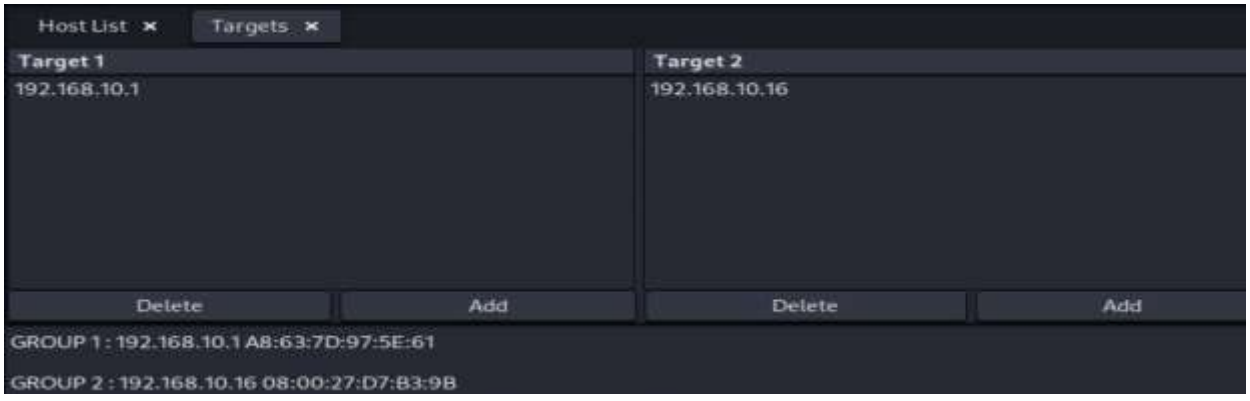
Step7:

Host List



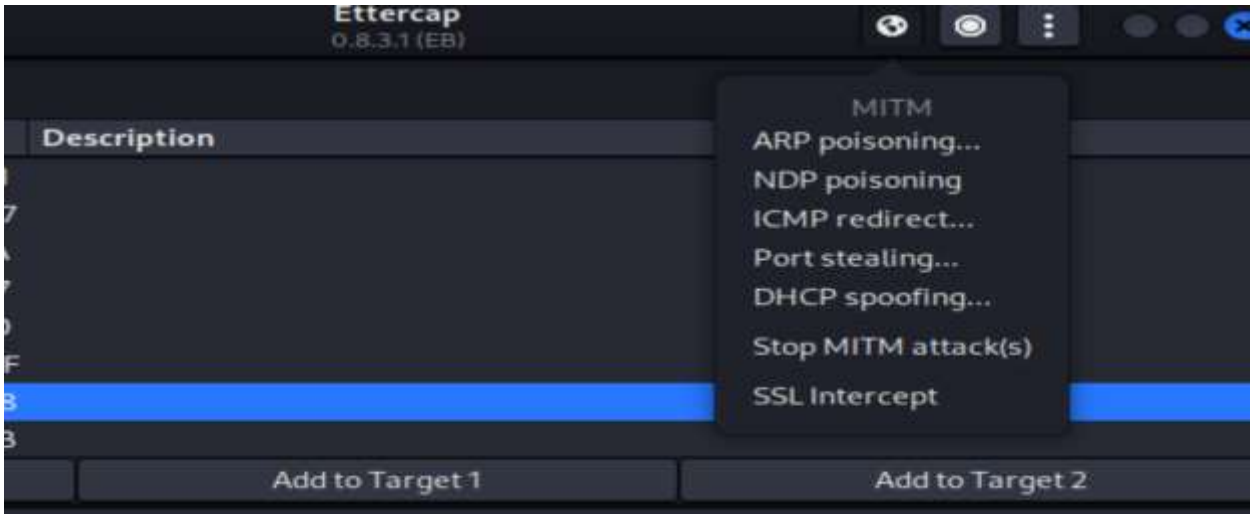
Step8:

Go to the Target and Current Target



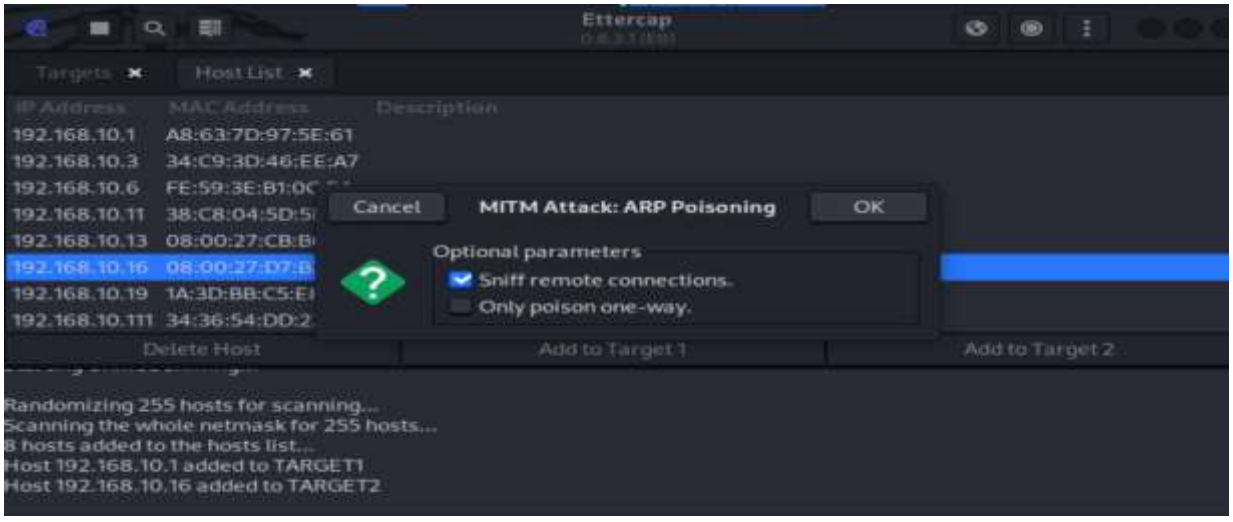
Step9:

Select the ARP poisoning



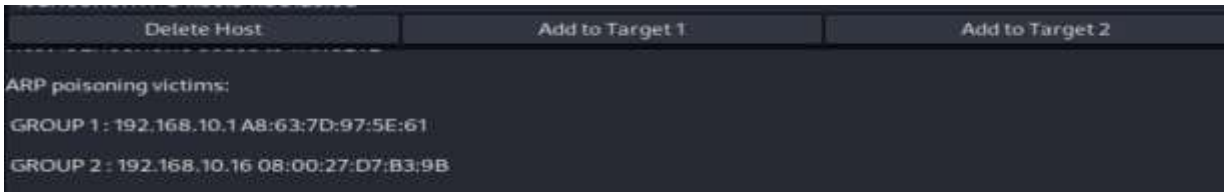
Step10:

Arp Poisoning applying



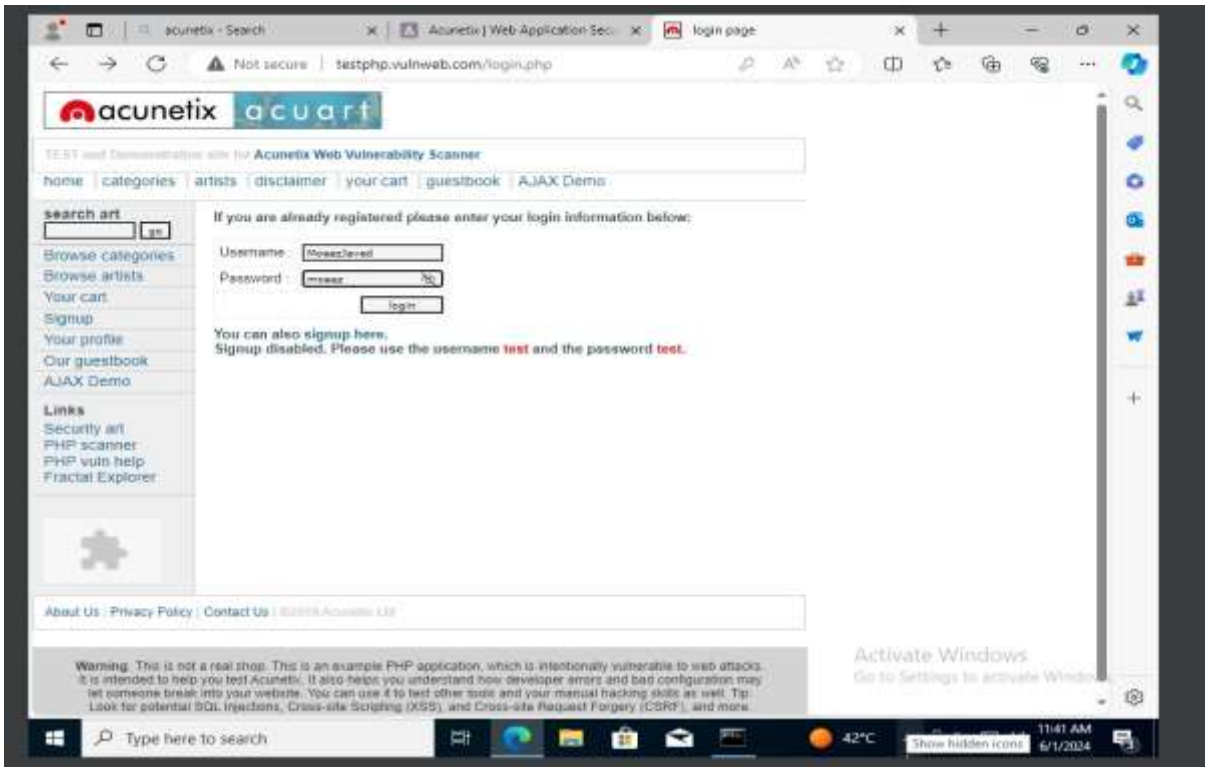
Step11:

Arp poisoning is applied

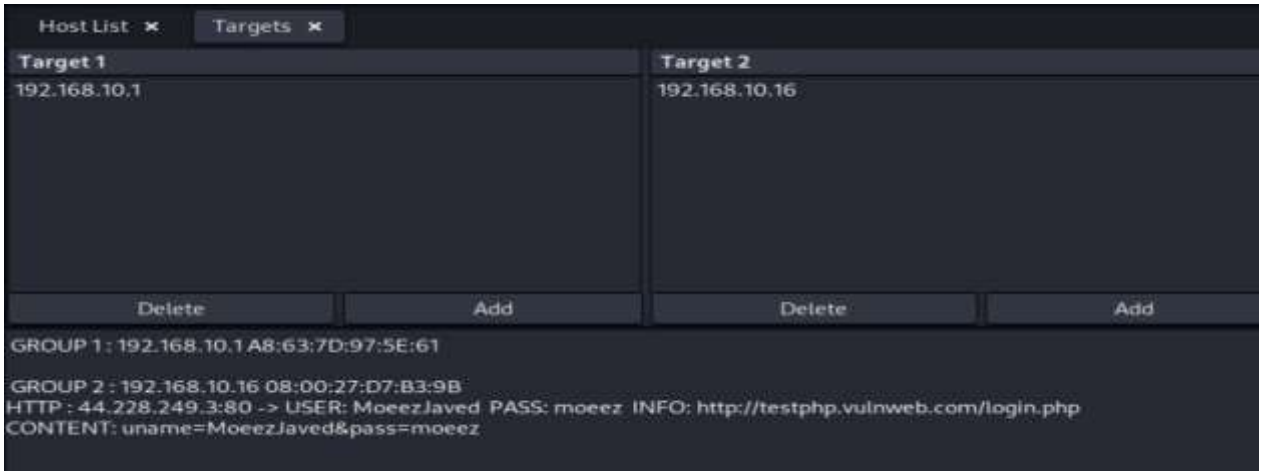


Step12:

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

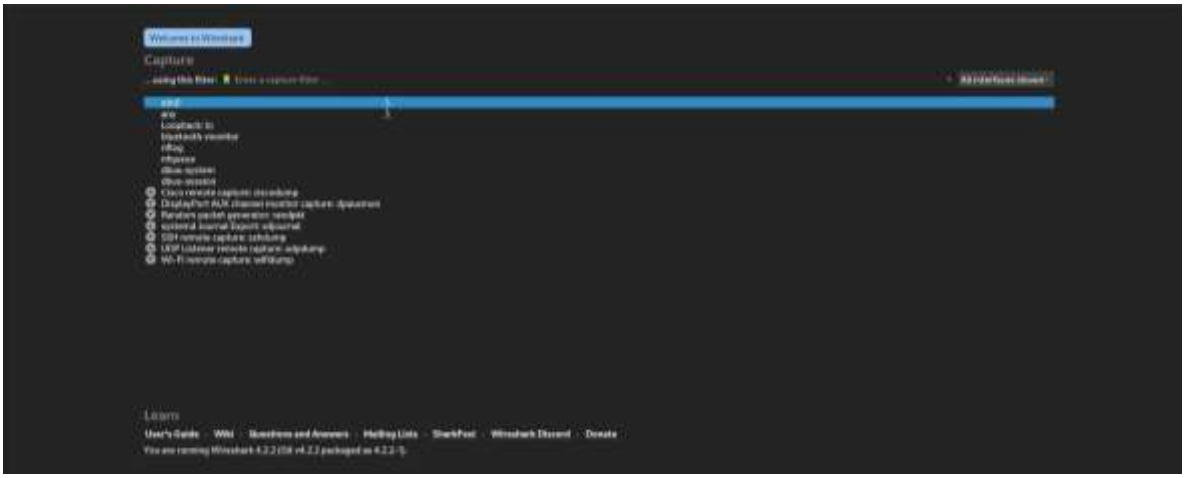


Step13:
The username and password is heard by the hacker.

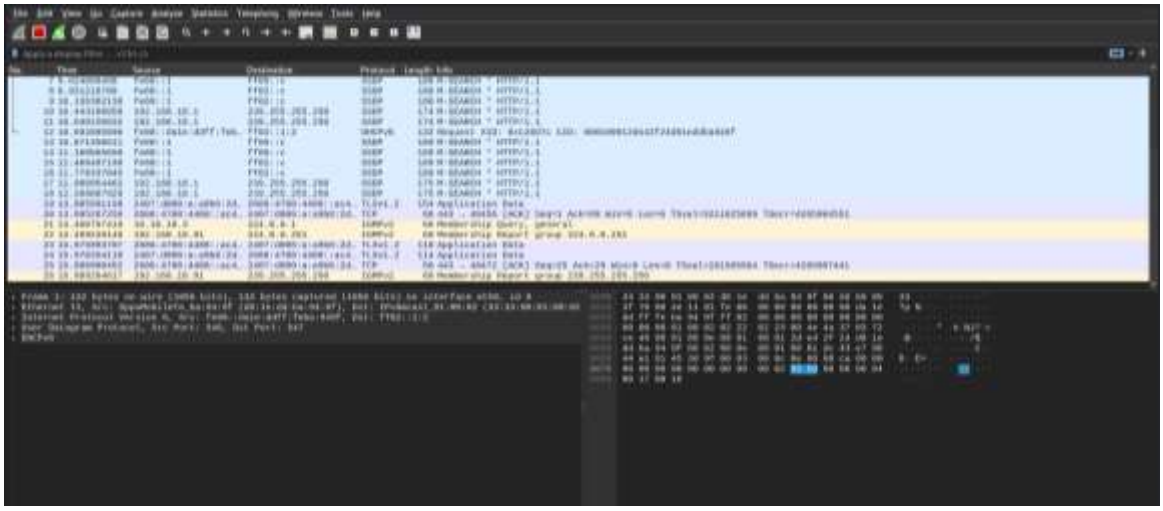


WireShark:

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.