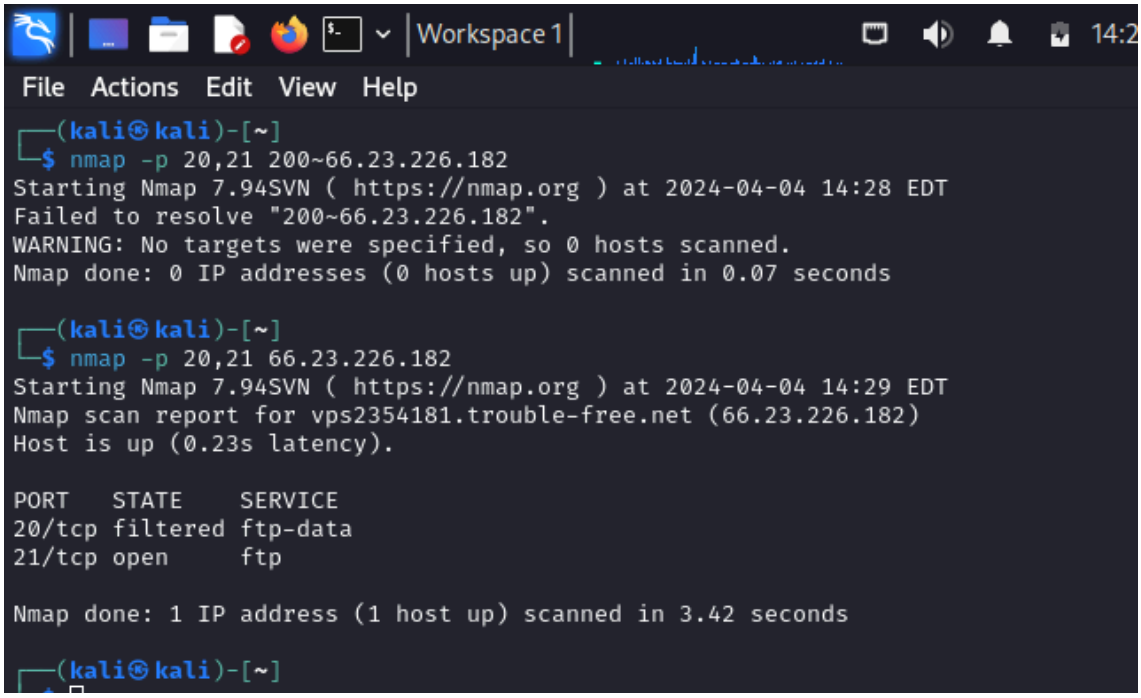
Employee Id : ST#IS#6248

Task 2

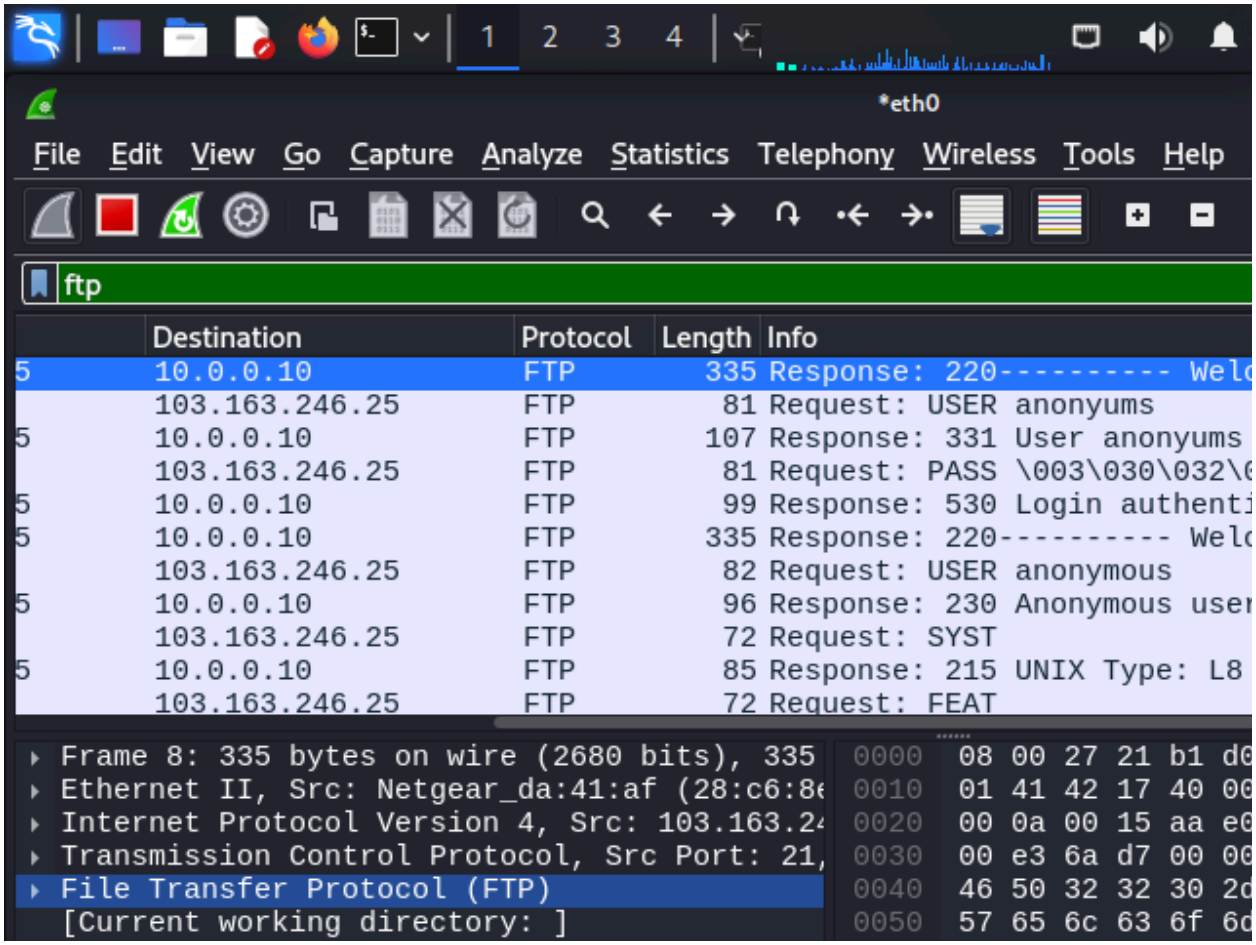
A) Sniffing - Identify the websites that have vulnerable protocols to sniff
o FTP
o POP3
oHTTP

For FTP PORT
Vulnerable website : https://easyfashion.com.bd/

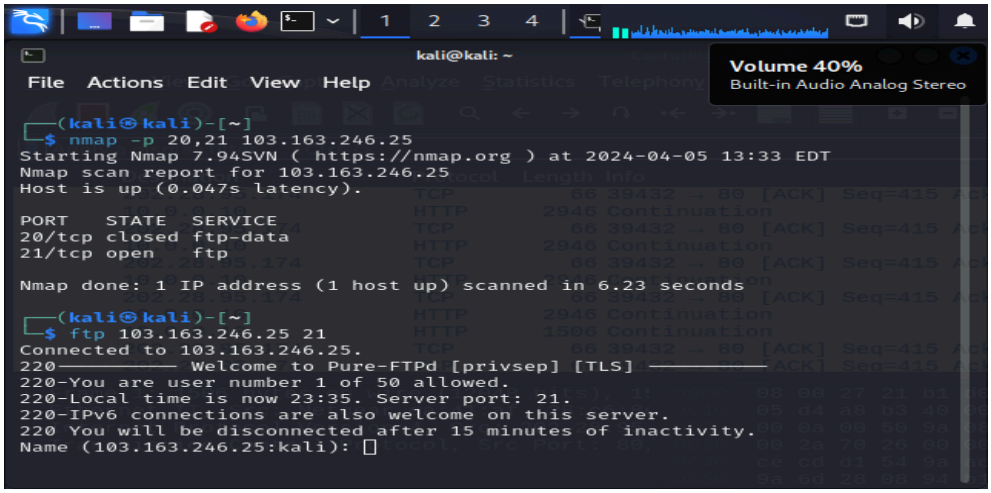
Step 1 : Open Kali Linux and open the terminal and use the nmap tool to scan the port, first we will scan for the open Ftp port i.e 20 or 21. Find the Vulnerable Website Ip



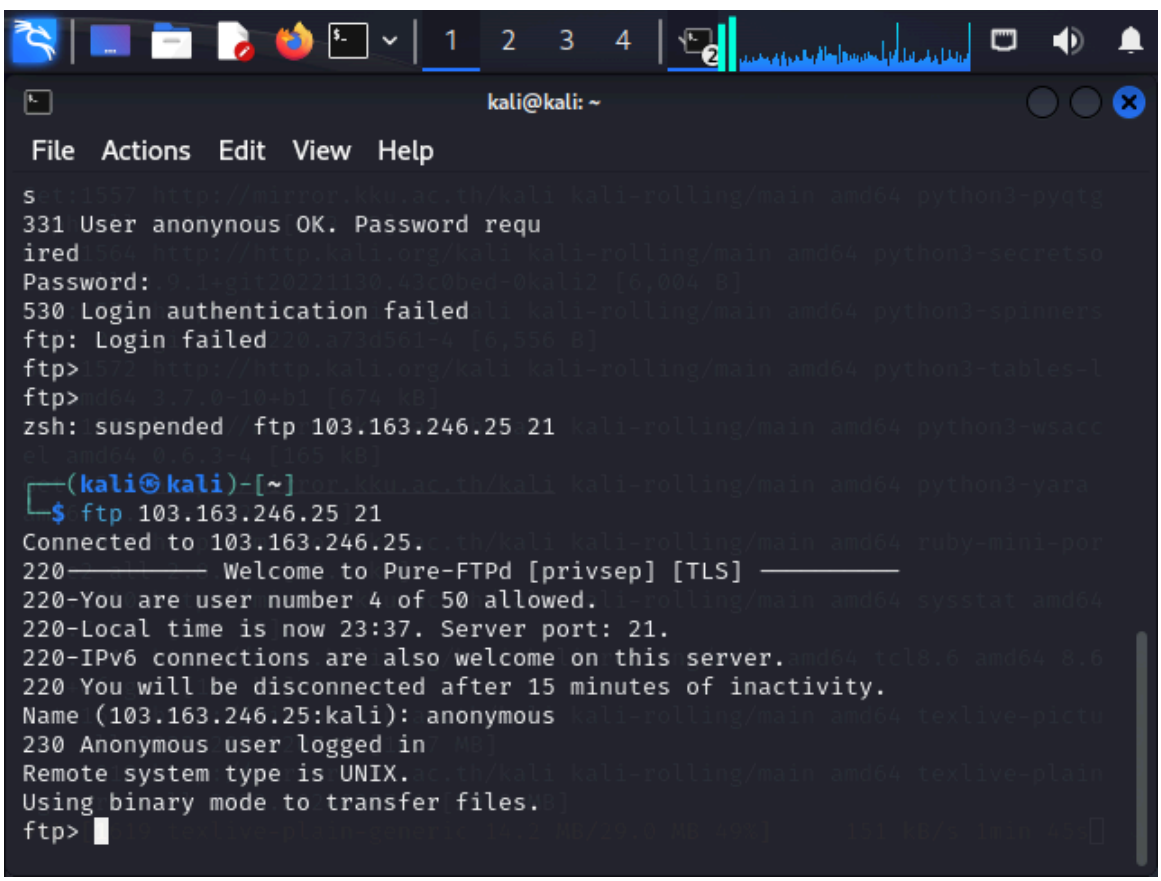
Step 2 : Start the Wireshark Tool in the Background and start capturing the packets



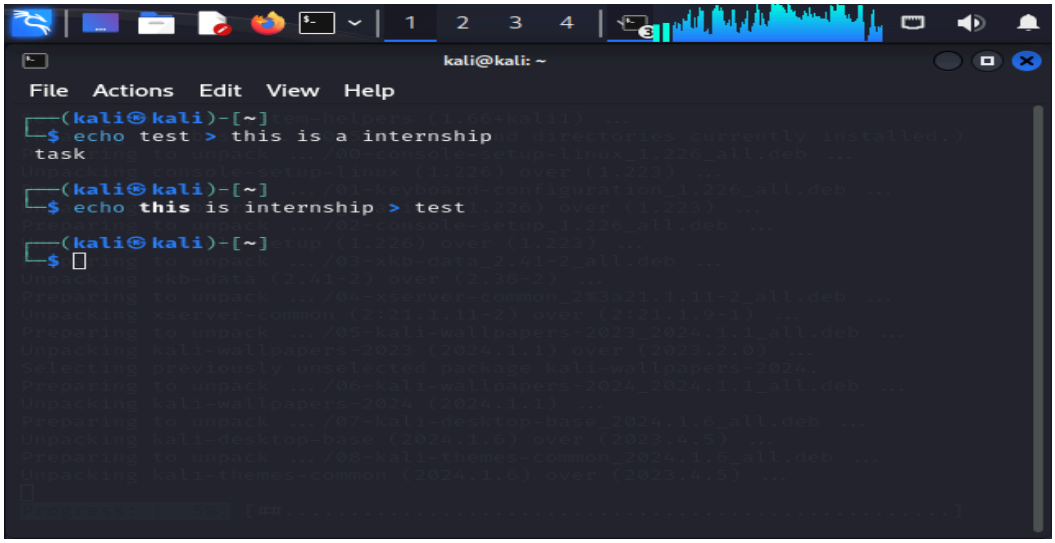
Step 3 : Start Sending the Ftp data to the Vulnerable Website - FTP example.com 21



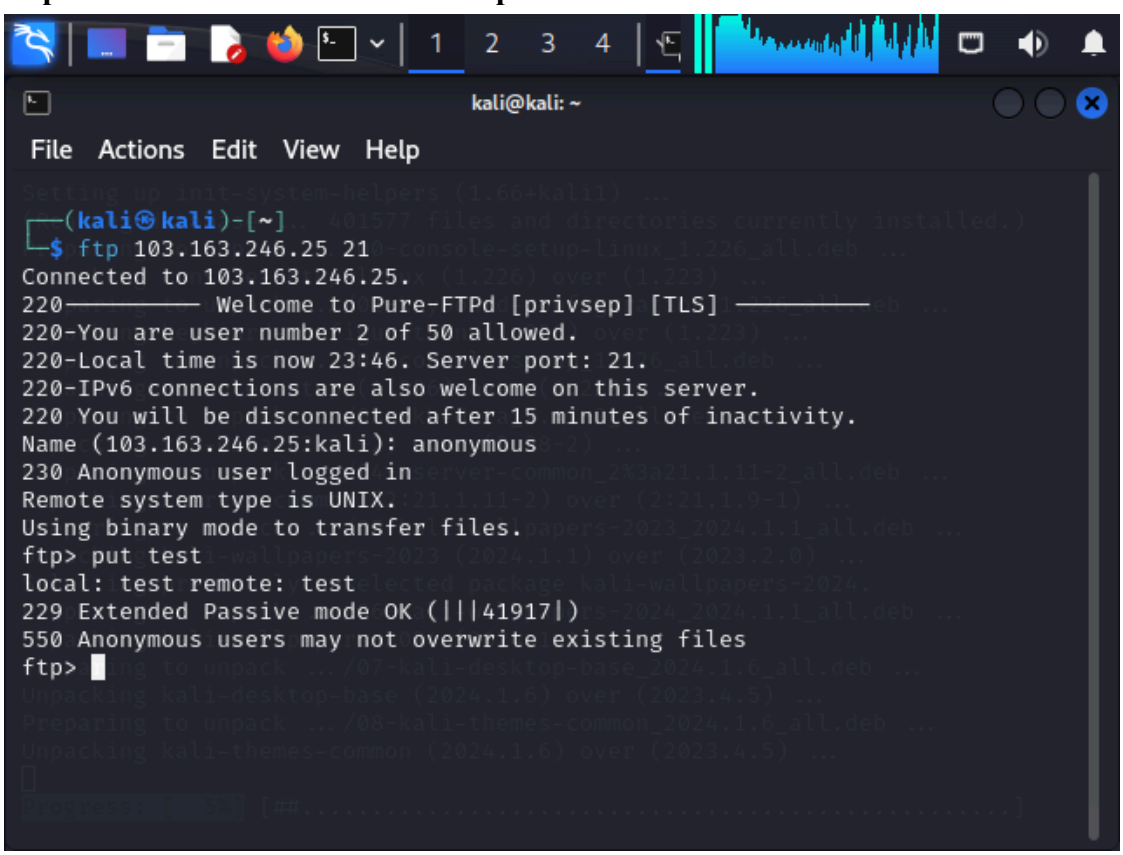
Step 4 : Enter the user name to send the data to the website it is usually anonymous - Name : anonymous



Step 5 : Create a text file that you want to upload on the website

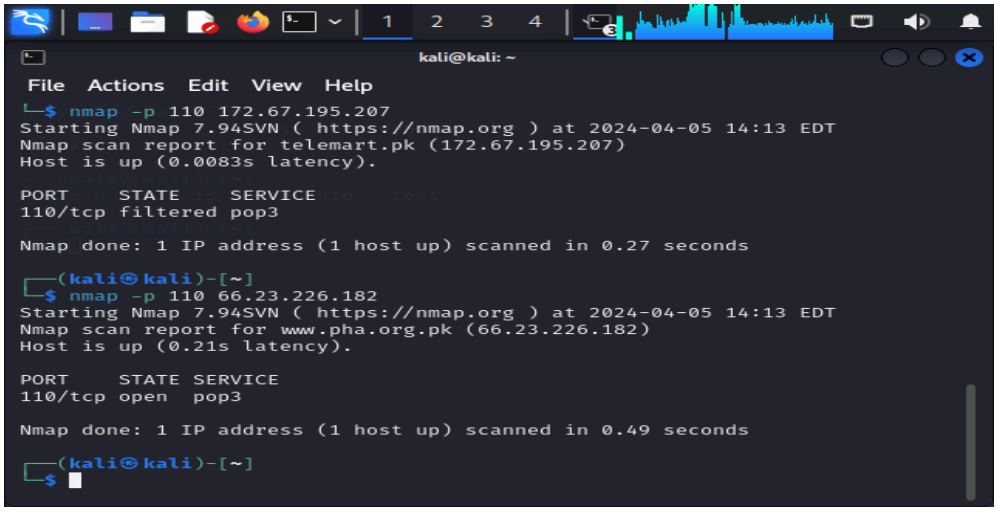


Step 6 : Use the Command PUT to upload the file on the server

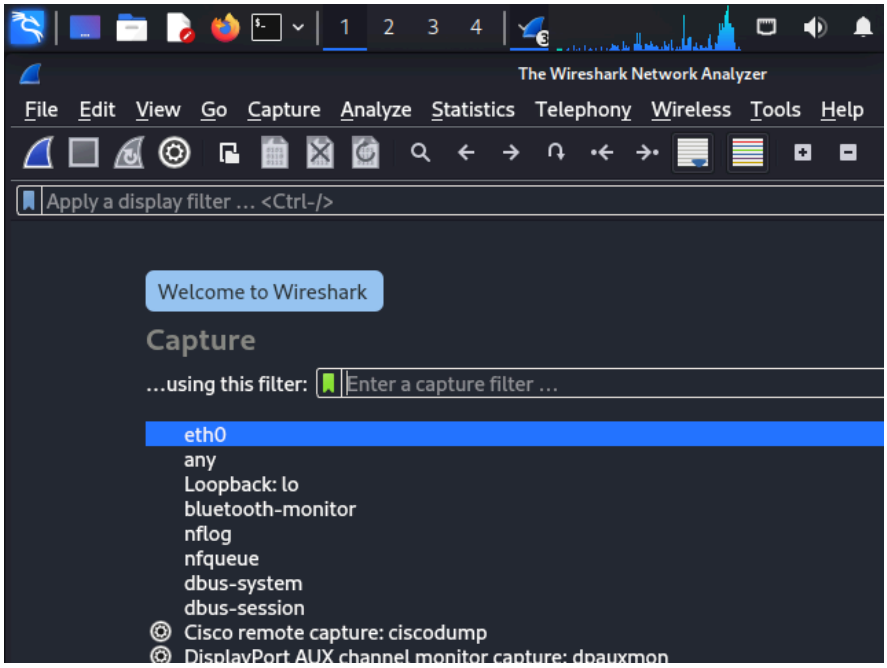


For POP3 Open port
Website : https://www.pha.org.pk/index.php

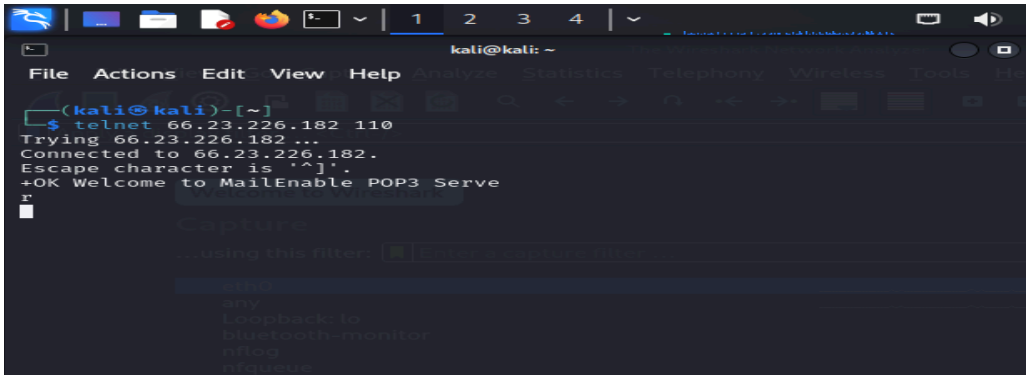
Step 1 : Find the Vulnerable Website that has open port for POP3 protocol



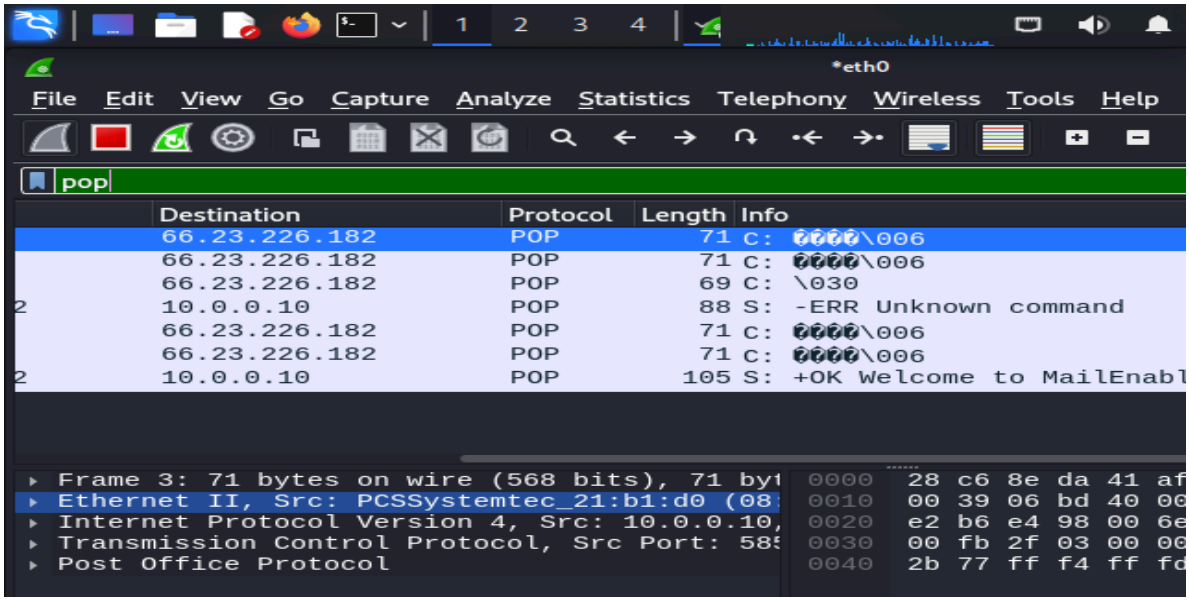
Step 2 : Start the Wireshark tool to capture the packets from the POP3 protocol that has open ports



Step 3 : Now we can use the telnet command with pop3 to sniff the pop3 open port



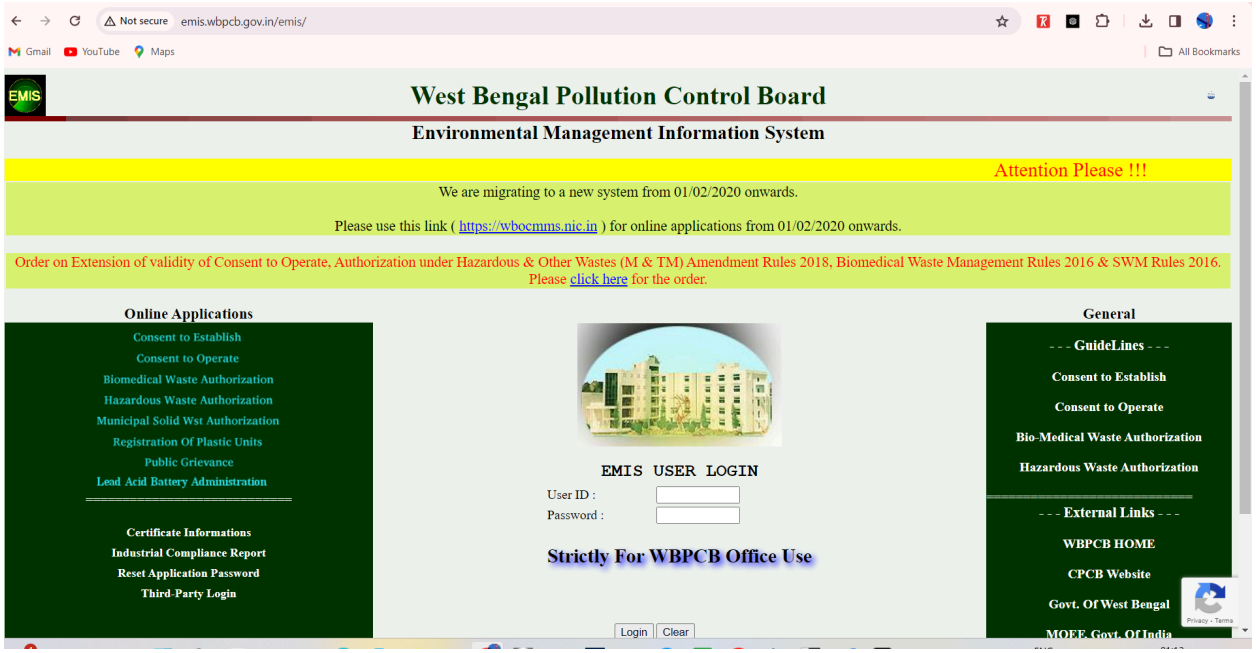
Step 4 : Open wireshark and see the pop3 packet send



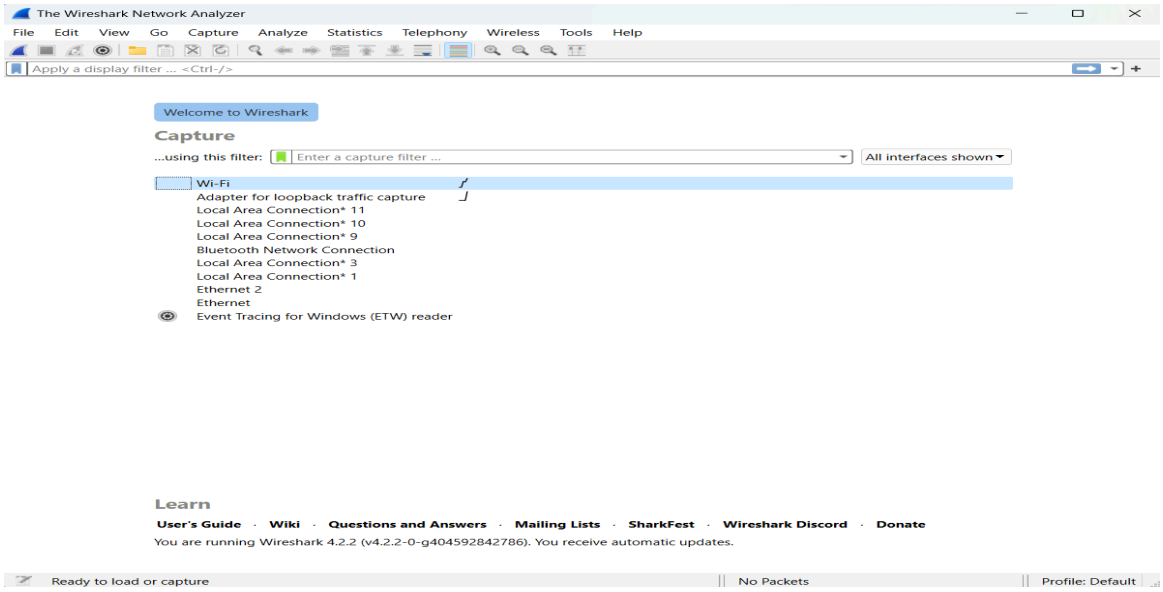
For Http Website

Website : http://emis.wbpcb.gov.in/emis/login.do

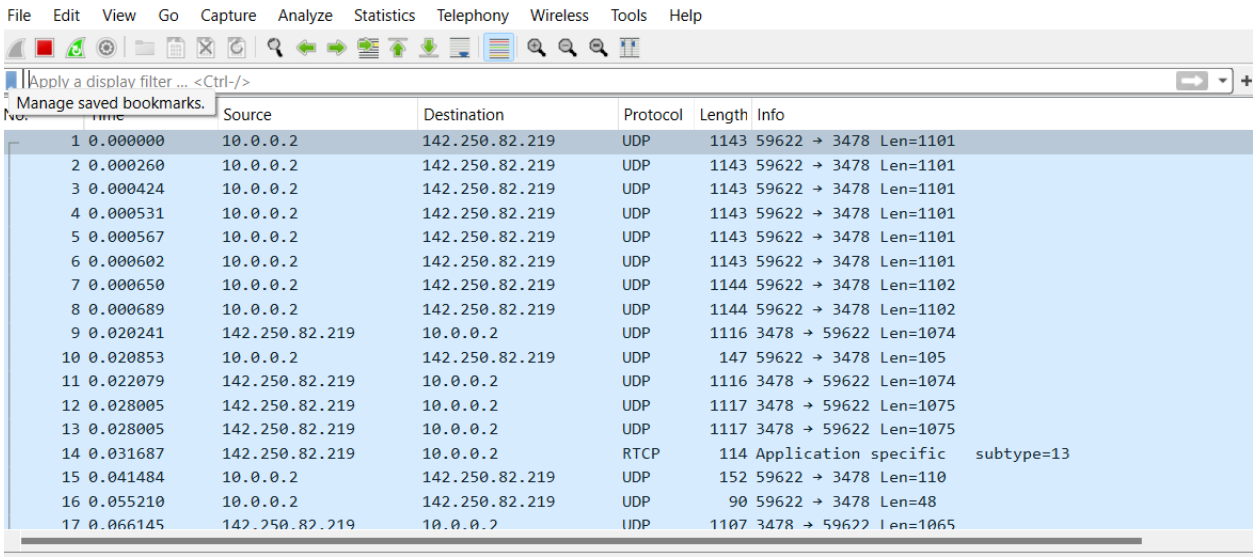
1. Find a website with the protocol HTTP and not HTTPS, this websites are not secured and vulnerable http sniffing



2. Open the Tool Wireshark to sniff the HTTP protocol and select WIFI if you are on Wifi else select ethernet

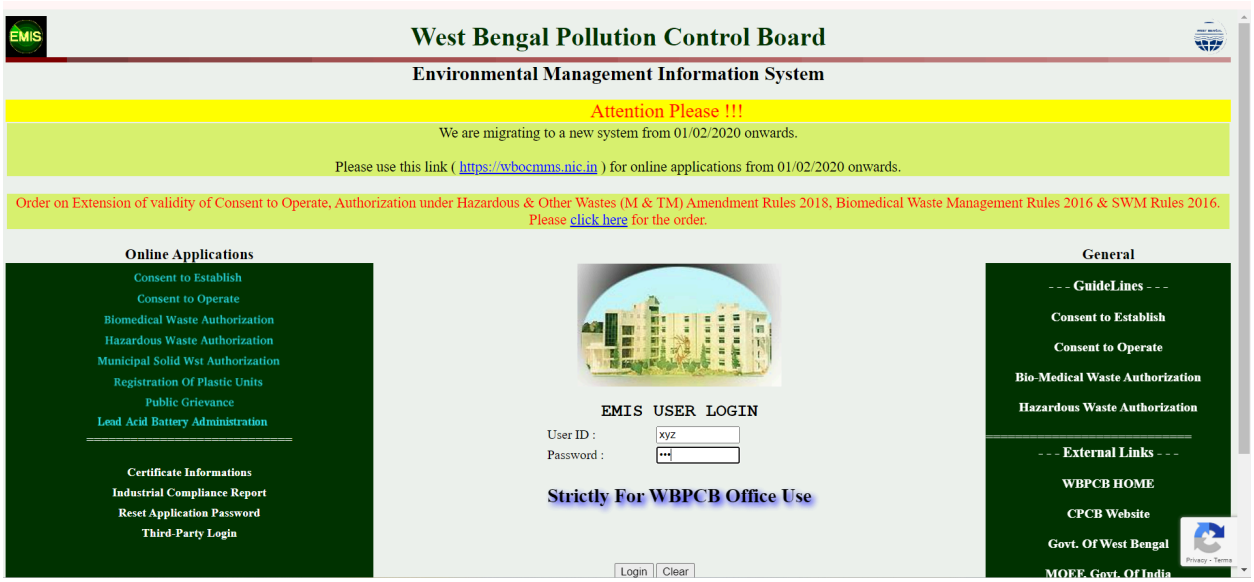


3. Start Capturing the Packets from that website in the wireshark tool

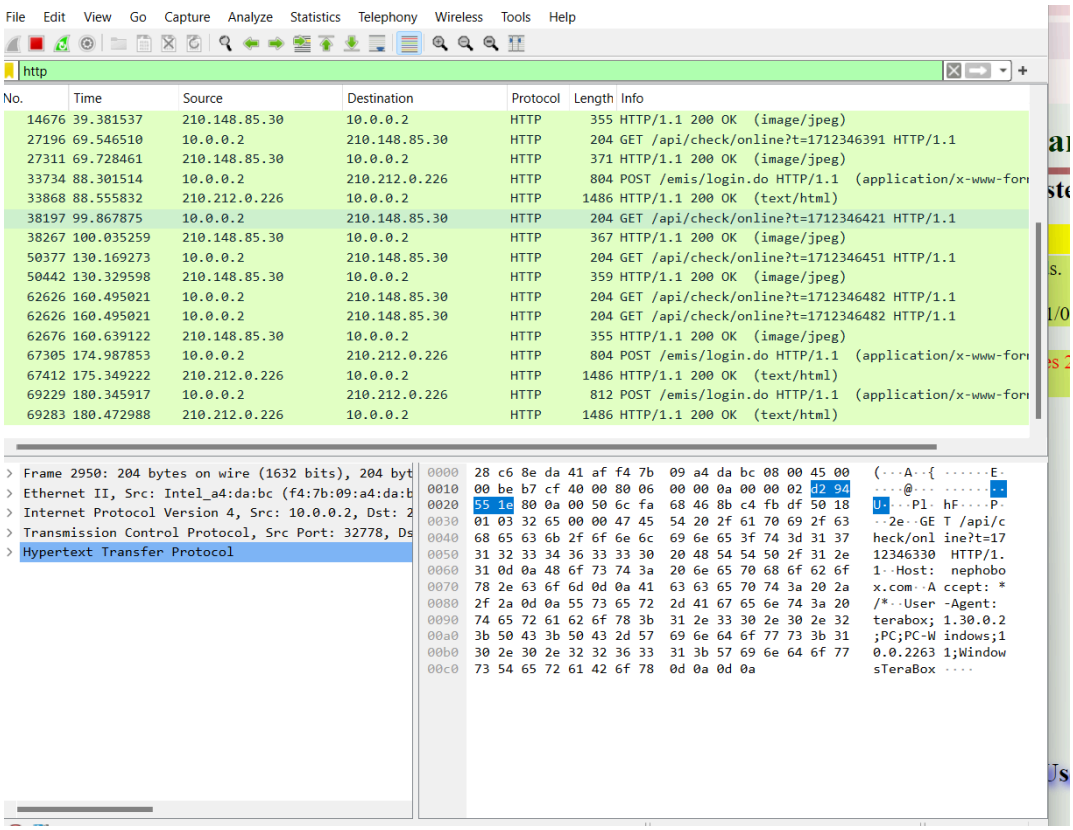


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
2	0.000260	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
3	0.000424	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
4	0.000531	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
5	0.000567	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
6	0.000602	10.0.0.2	142.250.82.219	UDP	1143	59622 → 3478 Len=1101
7	0.000650	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102
8	0.000689	10.0.0.2	142.250.82.219	UDP	1144	59622 → 3478 Len=1102
9	0.020241	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074
10	0.020853	10.0.0.2	142.250.82.219	UDP	147	59622 → 3478 Len=105
11	0.022079	142.250.82.219	10.0.0.2	UDP	1116	3478 → 59622 Len=1074
12	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075
13	0.028005	142.250.82.219	10.0.0.2	UDP	1117	3478 → 59622 Len=1075
14	0.031687	142.250.82.219	10.0.0.2	RTCP	114	Application specific subtype=13
15	0.041484	10.0.0.2	142.250.82.219	UDP	152	59622 → 3478 Len=110
16	0.055210	10.0.0.2	142.250.82.219	UDP	90	59622 → 3478 Len=48
17	0.066145	142.250.82.219	10.0.0.2	UDP	1107	3478 → 59622 Len=1065

4. In the Website of the vulnerable Http, perform some activities like invalid user details or login or etc



5. Apply filter to the wireshark by selecting only HTTP protocol and see the data we sniffed



B) Perform the ARP Poisoning Attack on your local network and perform sniffing.

Tool used : Ettercap and Wireshark

Step 1 : Open the Windows 11 Machine and go to the command prompt and check for the Ip address and default gateway that is your router with Ipconfig command

```
C:\Users\simon>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4fff:6eec:d16b:4ca2%3
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4689:d9ea:841a:68f8%9
   IPv4 Address. . . . . . . . . . . : 10.0.0.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

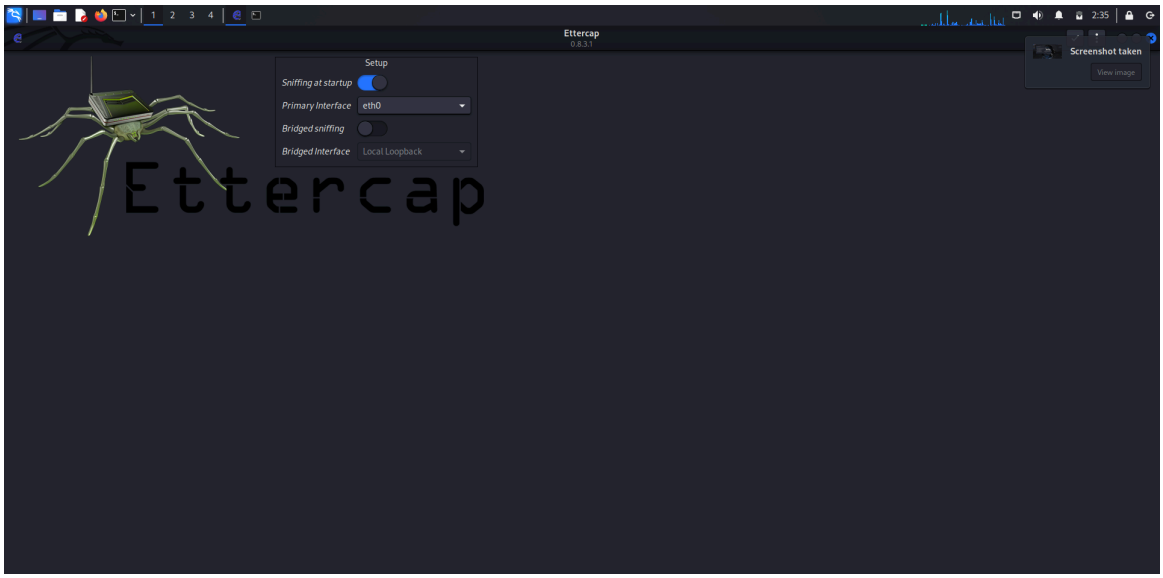
Step 2 : Type the arp -a command to check the mac address associated with the ip address

```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.0.0.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.0.1              28-c6-8e-da-41-af     dynamic
  10.0.0.8              08-00-27-1e-36-4a     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

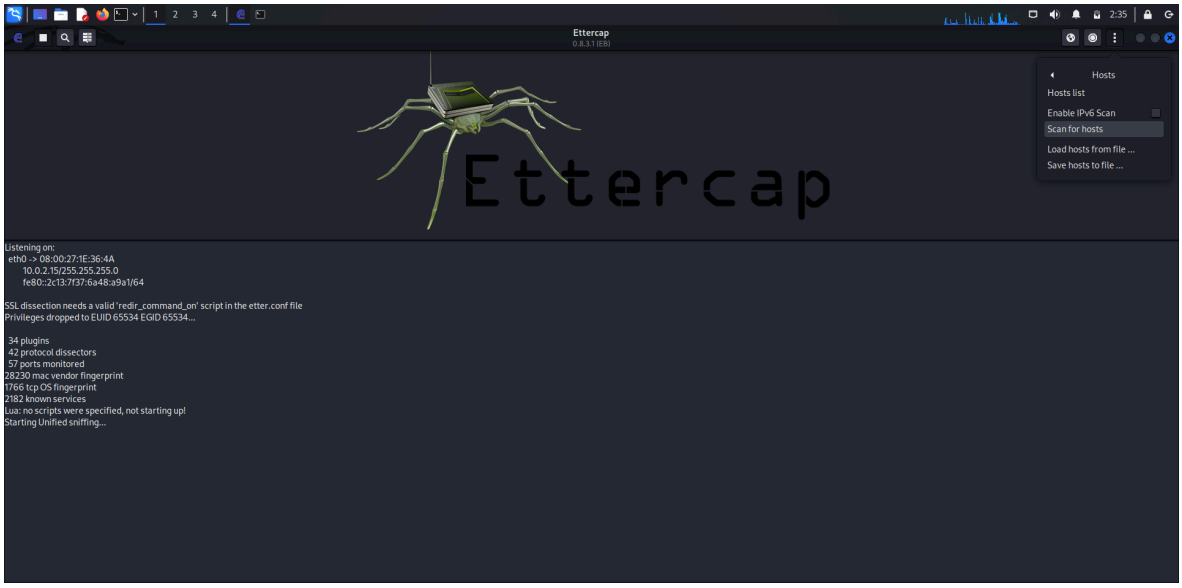
Step 3 : Go to the attacker machine called kali linux and open the terminal and check for the ip address with ifconfig command

Step 4 : Then Go to the kali linux icon and search for sniffing and spoofing section and click on the tool ettercap on right side

Step 5 : Open the ettercap and keep the default settings as it is and click on the tick on the right side

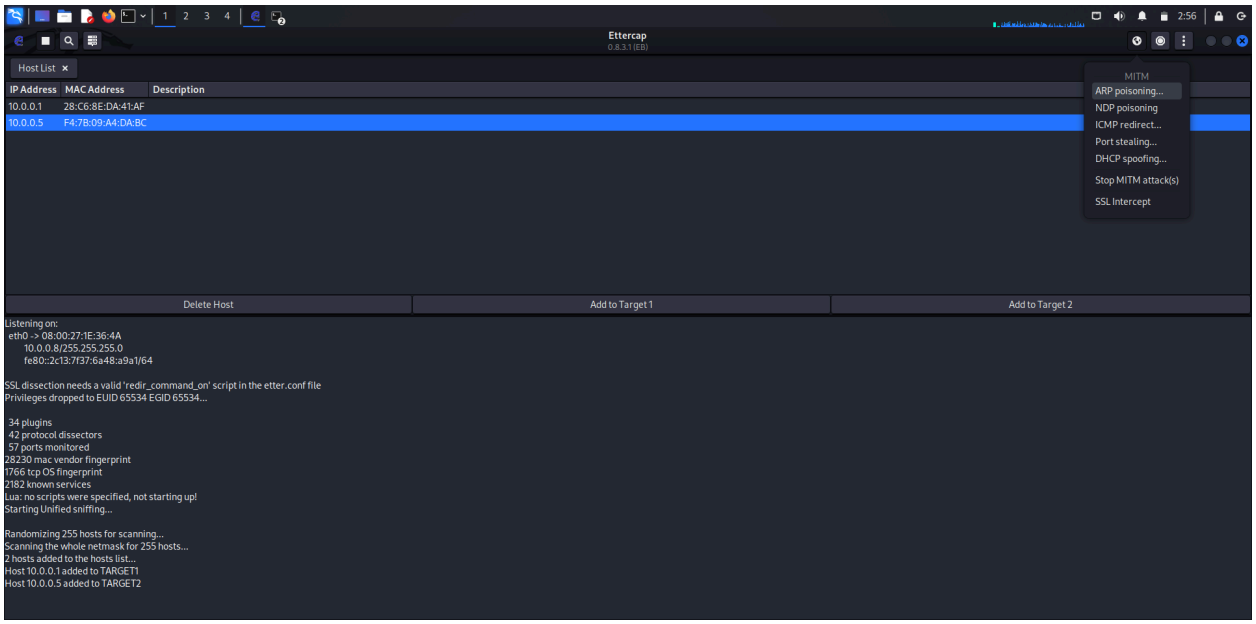


Step 6 : Click on three hamburger icon and select host and in hosts select scan for host, this will scan all the active host in your Network

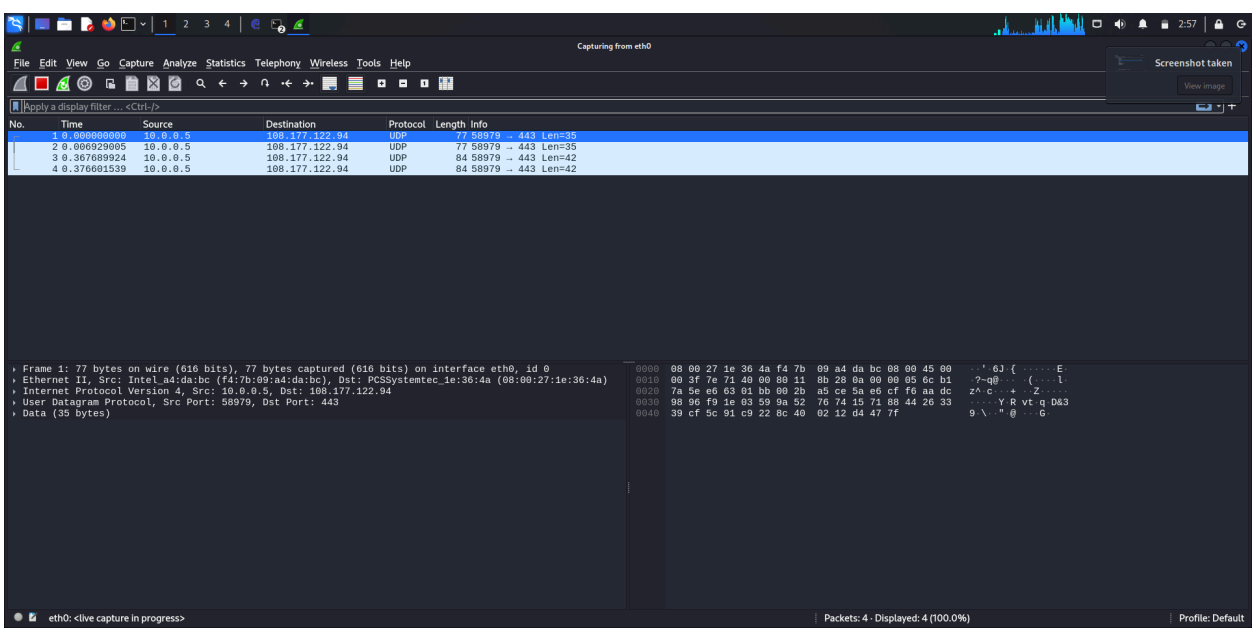


Step 7 : After it is done scanning for the host, again click on Hosts and click on Hosts list to see all the host in the network

Step 8 : After this all active hosts will be added to ettercap and now we can spoof the arp, Click on the target1 and add to target1 and then click on target2 and add to the target2, using the arp spoofing, click on small globe icon on the right side and then click on arp spoofing



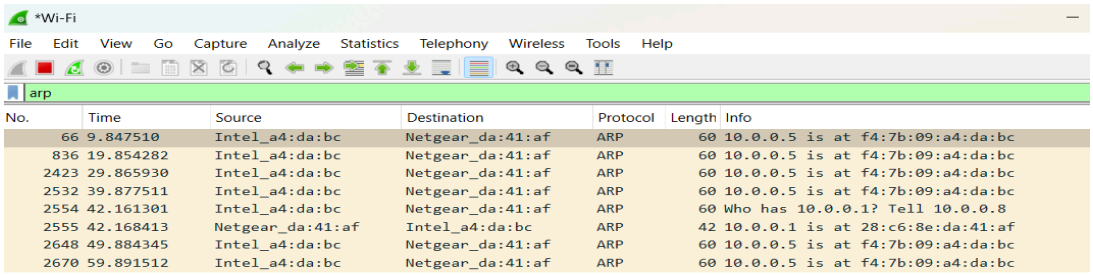
Step 9 : Click on the wireshark tool and then start sniffing of the packet in your kali linux machine

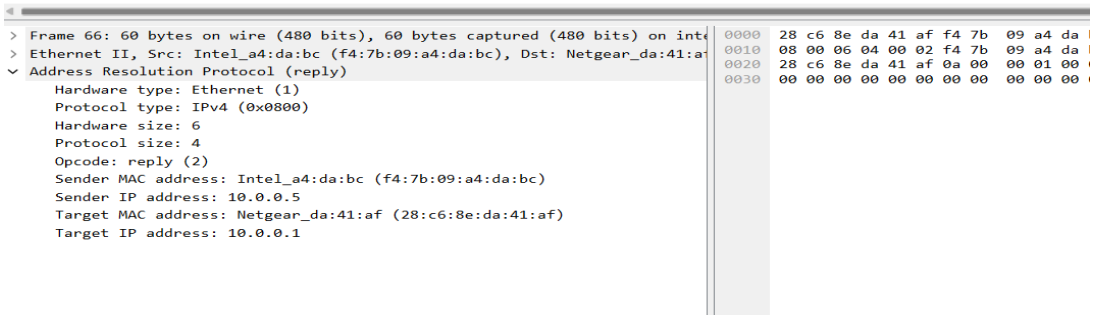


Step 10 : Now go to your local machine and type the arp -a command in cmd to check the mac address, if it is changed or no, we can see that the mac address of the local mac is changed to attackers mac address

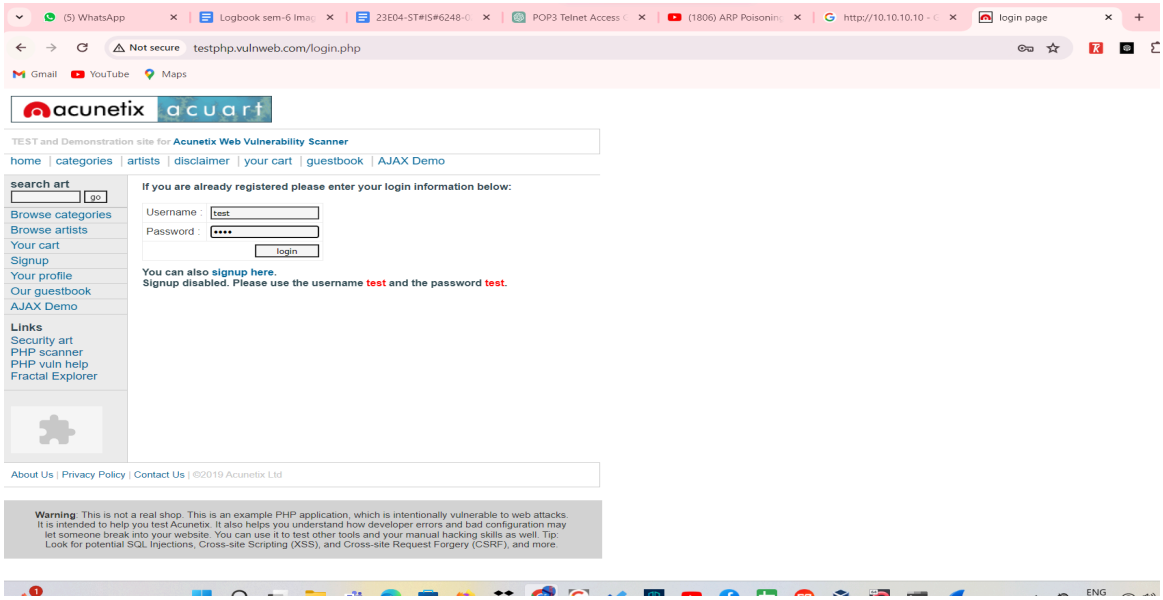
```
C:\Users\simon>arp -a

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.0.0.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.0.1              08-00-27-1e-36-4a     dynamic
  10.0.0.8              08-00-27-1e-36-4a     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Step 11 : Now open the Wireshark on your local machine and start capturing the packets and we can filter the packets by typing arp





Step 12 : Open any http Website on your local machine and login with username and password



Step 13 : Now to your ettercap tool and you see that the password and username is gone to the attackers machine like this we can do ARP poisoning