

Employee Id : ST#IS#6248

Task 2

A) Sniffing - Identify the websites that have vulnerable protocols to sniff

o FTP

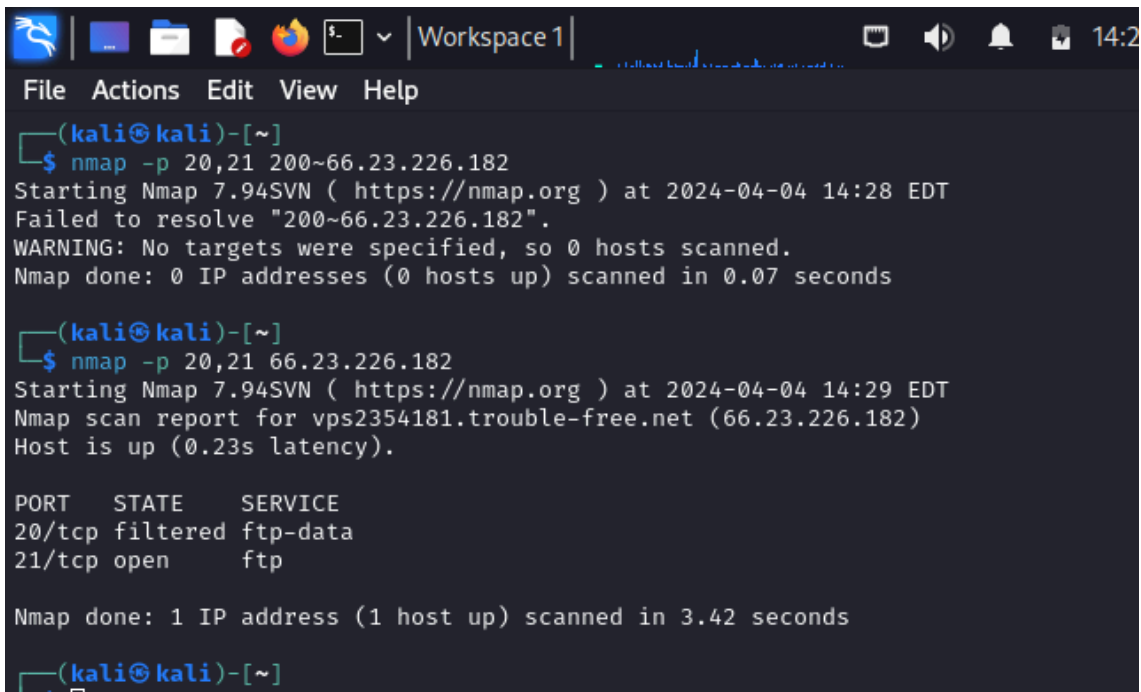
o POP3

o HTTP

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



```
(kali㉿kali)-[~]
└─$ nmap -p 20,21 200~66.23.226.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 14:28 EDT
Failed to resolve "200~66.23.226.182".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds

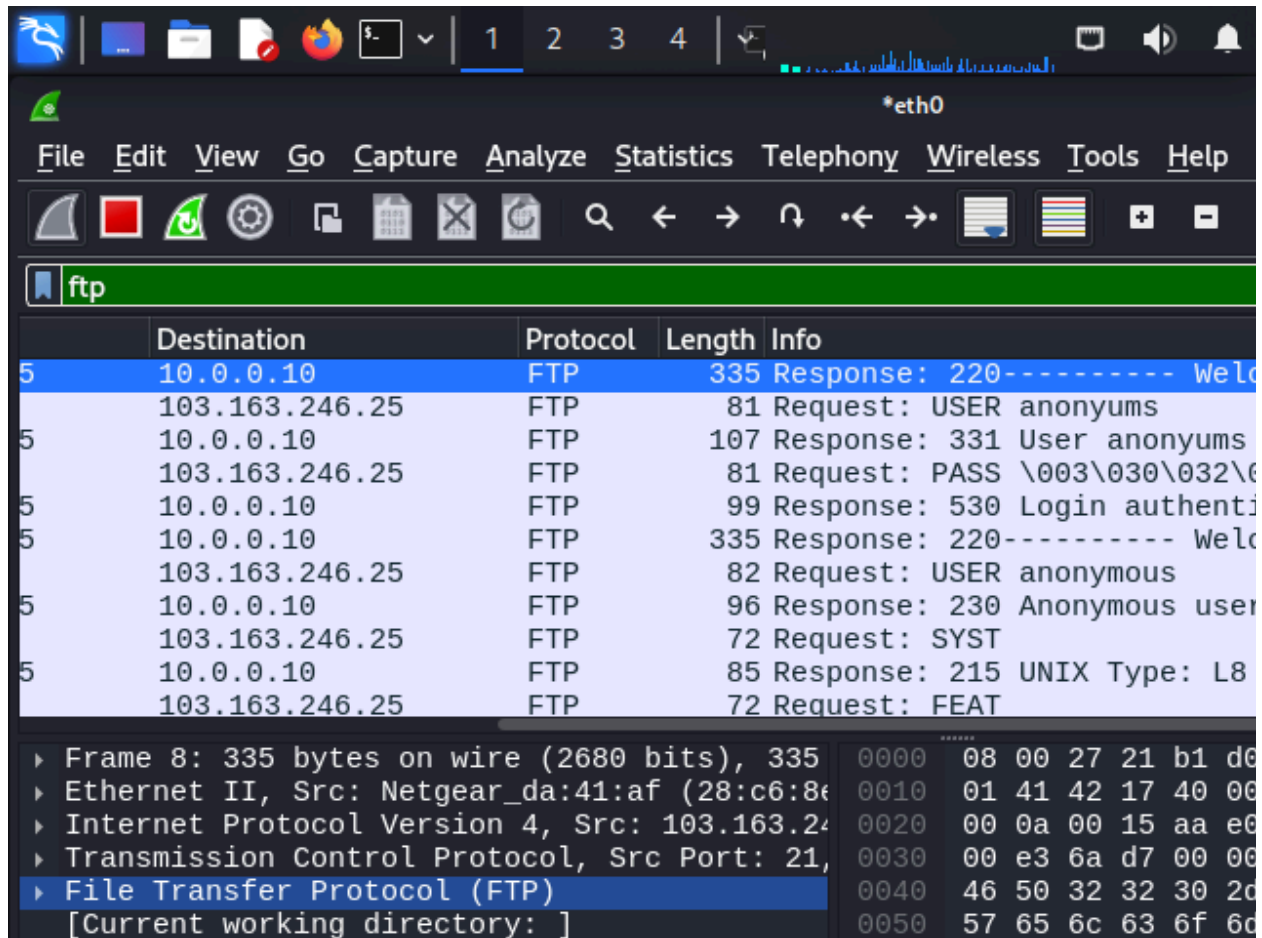
(kali㉿kali)-[~]
└─$ nmap -p 20,21 66.23.226.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 14:29 EDT
Nmap scan report for vps2354181.trouble-free.net (66.23.226.182)
Host is up (0.23s latency).

PORT      STATE      SERVICE
20/tcp    filtered  ftp-data
21/tcp    open       ftp

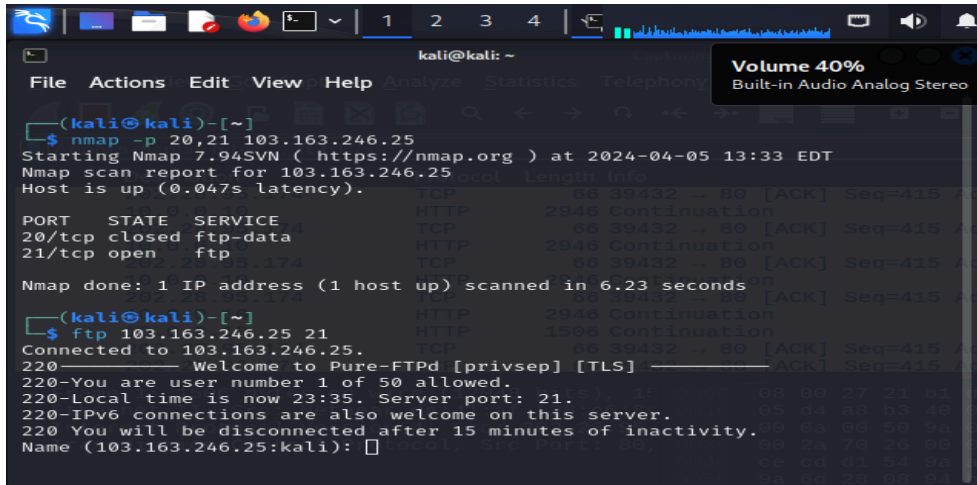
Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds

(kali㉿kali)-[~]
```

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

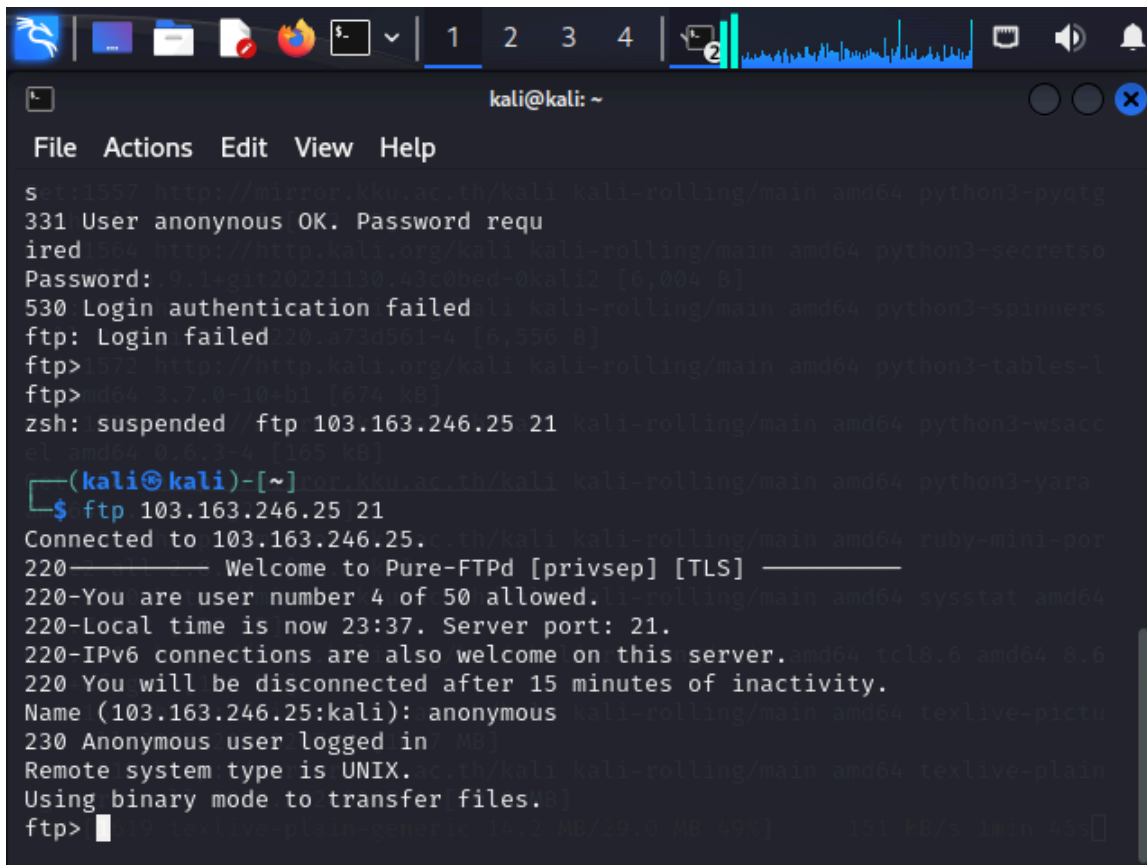


Step 3 : Start Sending the Ftp data to the Vulnerable Website - FTP example.com 21



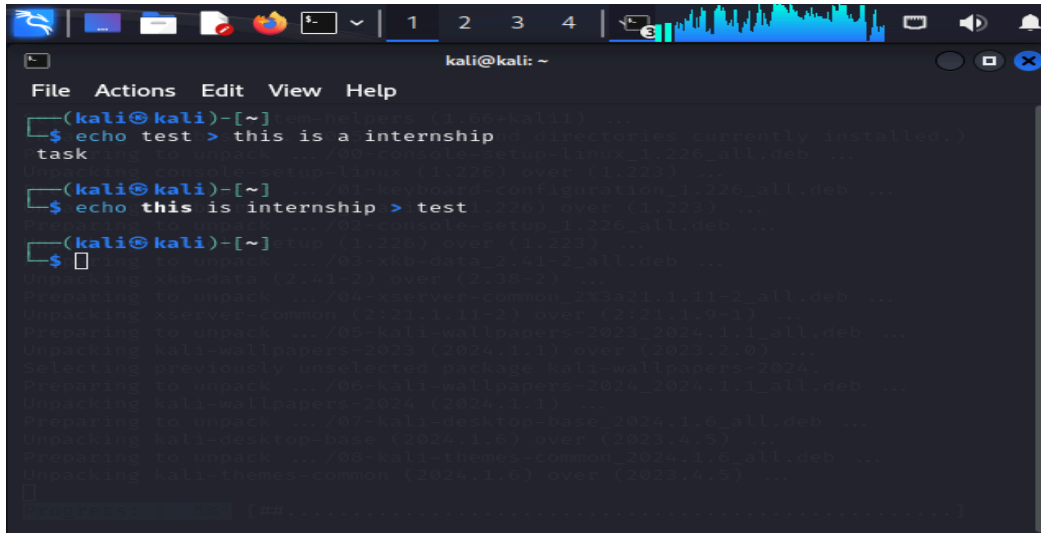
```
kali@kali: ~  
File Actions Edit View Help  
$(kali@kali)-[~]  
$ nmap -p 20,21 103.163.246.25  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 13:33 EDT  
Nmap scan report for 103.163.246.25  
Host is up (0.047s latency).  
PORT      STATE SERVICE  
20/tcp    closed ftp-data  
21/tcp    open  ftp  
Nmap done: 1 IP address (1 host up) scanned in 6.23 seconds  
$(kali@kali)-[~]  
$ ftp 103.163.246.25 21  
Connected to 103.163.246.25.  
220 Welcome to Pure-FTPD [privsep] [TLS]  
220-You are user number 1 of 50 allowed.  
220-Local time is now 23:35. Server port: 21.  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
Name (103.163.246.25:kali):
```

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



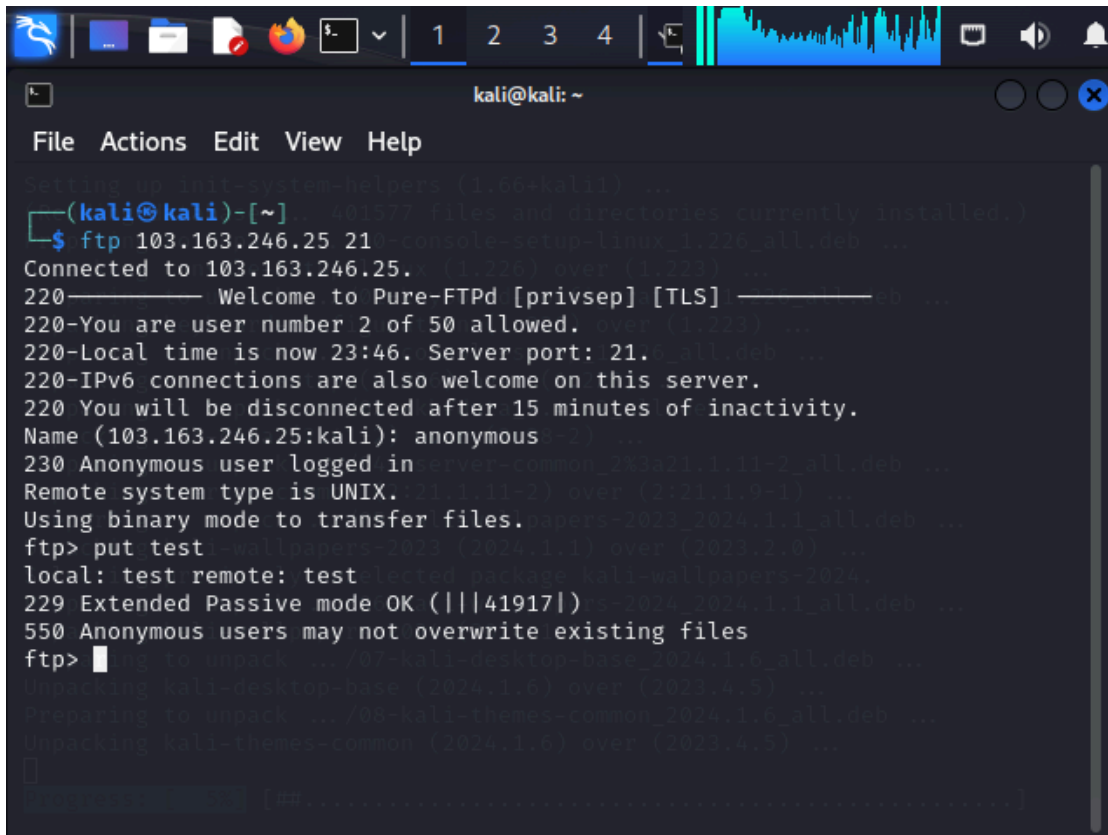
```
kali@kali: ~  
File Actions Edit View Help  
s 1:1537 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-pyotg  
331 User anonymous OK. Password requ  
ired  
500 http://http.kali.org/kali kali-rolling/main amd64 python3-secretso  
Password: 1:1git20231130-43-0bed-0kali2 [6,004 B]  
530 Login authentication failed [1 kali-rolling/main amd64 python3-spinners  
ftp: Login failed 10.73d561-4 [6,556 B]  
ftp> 573 http://http.kali.org/kali kali-rolling/main amd64 python3-tables-1  
ftp> amd64 3.7.0-10-b1 [674 kB]  
zsh: suspended ftp 103.163.246.25 21 kali-rolling/main amd64 python3-wsacc  
el amd64 0.6.0-4 [165 kB]  
$(kali@kali)-[~]  
$ ftp 103.163.246.25 21  
Connected to 103.163.246.25.  
220 Welcome to Pure-FTPD [privsep] [TLS]  
220-You are user number 4 of 50 allowed.  
220-Local time is now 23:37. Server port: 21.  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
Name (103.163.246.25:kali): anonymous  
230 Anonymous user logged in [No]  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

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



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ echo test > this is a internship task  
(kali@kali)-[~]  
$ echo this is internship > test  
(kali@kali)-[~]  
$  
Setting up init-system-helpers (1.66+kali1) ...  
Unpacking kali-wallpapers-2023_2024.1.1_all.deb ...  
Preparing to unpack .../kali-wallpapers-2024_2024.1.1_all.deb ...  
Unpacking kali-wallpapers-2024_2024.1.1_all.deb ...  
Setting up kali-wallpapers-2024 (2024.1.1) over (2023.2.0) ...  
Preparing to unpack .../kali-desktop-base_2024.1.6_all.deb ...  
Unpacking kali-desktop-base (2024.1.6) over (2023.4.5) ...  
Preparing to unpack .../kali-themes-common_2024.1.6_all.deb ...  
Unpacking kali-themes-common (2024.1.6) over (2023.4.5) ...  
$
```

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

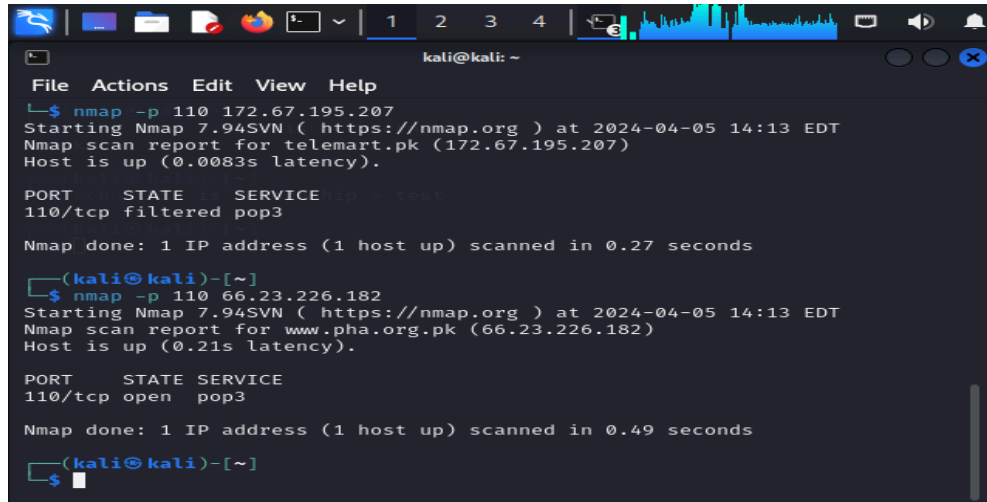


```
kali@kali: ~  
File Actions Edit View Help  
Setting up init-system-helpers (1.66+kali1) ...  
(kali@kali)-[~]  
$ ftp 103.163.246.25 21 -console-setup-linux_1.226_all.deb ...  
Connected to 103.163.246.25. (1.226) over (1.233) ...  
220----- Welcome to Pure-FTPd [privsep] [TLS] -----  
220-You are user number 2 of 50 allowed. over (1.233) ...  
220-Local time is now 23:46. Server port: 21. ...  
220-IPv6 connections are also welcome on this server.  
220 You will be disconnected after 15 minutes of inactivity.  
Name (103.163.246.25:kali): anonymous ...  
230 Anonymous user logged in. server-common_23021.1.11-2_all.deb ...  
Remote system type is UNIX. (1.111-2) over (2:21.1.9-1) ...  
Using binary mode to transfer files. papers-2023_2024.1.1_all.deb ...  
ftp> put test wallpapers-2023 (2024.1.1) over (2023.2.0) ...  
local: test remote: test tested package kali-wallpapers-2024.  
229 Extended Passive mode OK (|||41917|) s-2024_2024.1.1_all.deb ...  
550 Anonymous users may not overwrite existing files  
ftp>  
Preparing to unpack .../kali-desktop-base_2024.1.6_all.deb ...  
Unpacking kali-desktop-base (2024.1.6) over (2023.4.5) ...  
Preparing to unpack .../kali-themes-common_2024.1.6_all.deb ...  
Unpacking kali-themes-common (2024.1.6) over (2023.4.5) ...  
$
```

For POP3 Open port

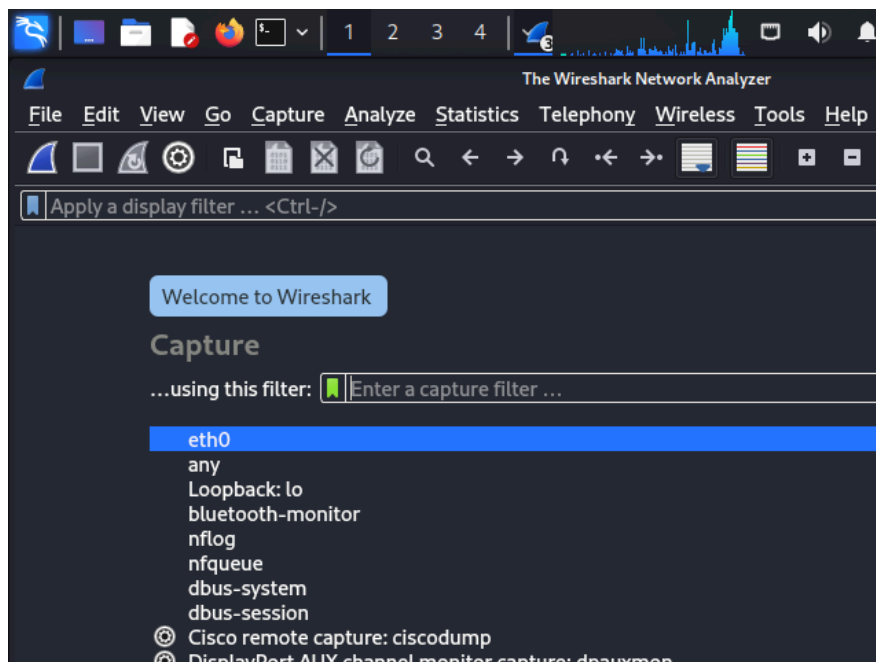
Website : <https://www.pha.org.pk/index.php>

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



```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -p 110 172.67.195.207  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 14:13 EDT  
Nmap scan report for telemart.pk (172.67.195.207)  
Host is up (0.0083s latency).  
  
PORT      STATE      SERVICE  
110/tcp   filtered  pop3  
  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds  
  
(kali@kali)-[~]  
└─$ nmap -p 110 66.23.226.182  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 14:13 EDT  
Nmap scan report for www.pha.org.pk (66.23.226.182)  
Host is up (0.21s latency).  
  
PORT      STATE      SERVICE  
110/tcp   open       pop3  
  
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds  
  
(kali@kali)-[~]  
└─$
```

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

The screenshot shows a Kali Linux terminal window. The terminal prompt is `kali@kali: ~`. The user has entered `telnet 66.23.226.182 110`. The output of the command is as follows:

```

(kali@kali)-[~]
$ telnet 66.23.226.182 110
Trying 66.23.226.182 ...
Connected to 66.23.226.182.
Escape character is '^J'
+OK Welcome to MailEnable POP3 Serve
r

```

Below the terminal window, a network monitor interface is visible. It shows a capture filter set to `any`. The interface includes a list of network interfaces and a search bar.

Step 4 : Open wireshark and see the pop3 packet send

The image shows a Wireshark packet capture of a POP3 session. The packet list on the left shows a series of POP3 messages. The selected packet (packet 2) is a POP3 'Welcome' message from 66.23.226.182 to 10.0.0.10. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, the Internet Protocol Version 4 header, and the Transmission Control Protocol header. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|-----------------------------|
| 1 | 0.000000 | 66.23.226.182 | 10.0.0.10 | POP3 | 71 | C: 0000 0006 |
| 2 | 0.000000 | 66.23.226.182 | 10.0.0.10 | POP3 | 71 | C: 0000 0006 |
| 3 | 0.000000 | 66.23.226.182 | 10.0.0.10 | POP3 | 69 | C: \030 |
| 4 | 0.000000 | 10.0.0.10 | 66.23.226.182 | POP3 | 88 | S: -ERR Unknown command |
| 5 | 0.000000 | 66.23.226.182 | 10.0.0.10 | POP3 | 71 | C: 0000 0006 |
| 6 | 0.000000 | 66.23.226.182 | 10.0.0.10 | POP3 | 71 | C: 0000 0006 |
| 7 | 0.000000 | 10.0.0.10 | 66.23.226.182 | POP3 | 105 | S: +OK Welcome to MailEnabl |

Packet 2 details:

- Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:00:21:b1:d0), Dst: 10.0.0.10 (08:00:00:08:00:08)
- Internet Protocol Version 4, Src: 10.0.0.10, Dst: 66.23.226.182
- Transmission Control Protocol, Src Port: 5855, Dst Port: 110
- Post Office Protocol

Packet 2 bytes:

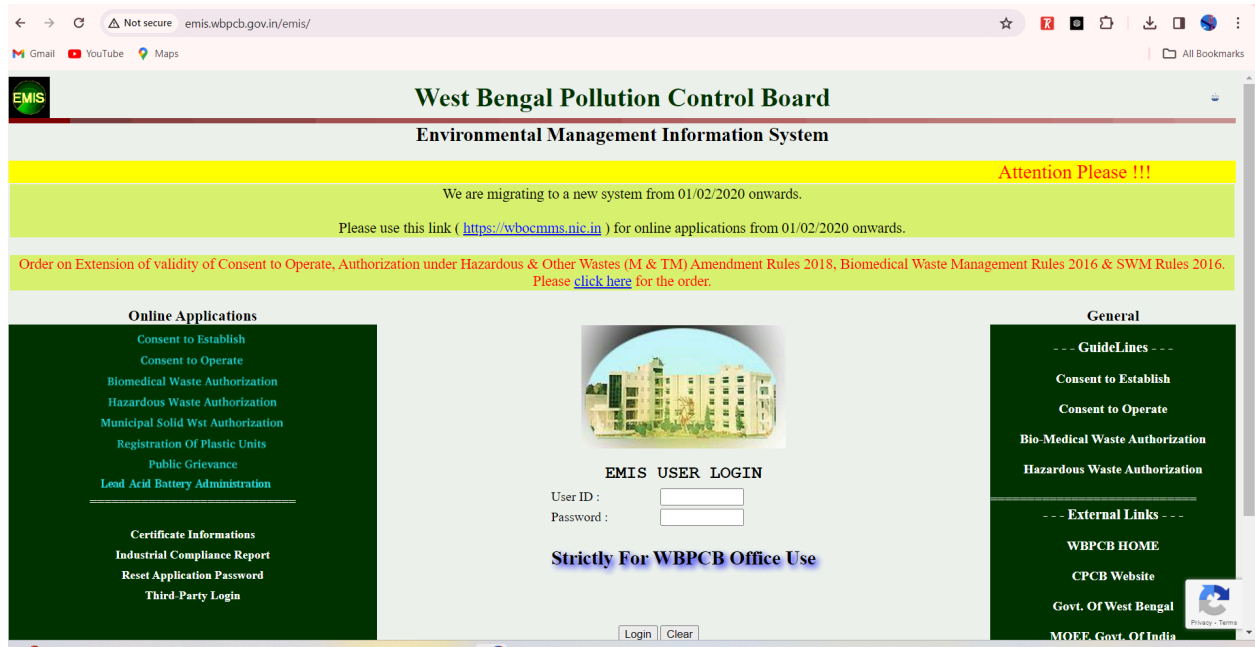
```

0000  28 c6 8e da 41 af 00 00 00 00 00 00 00 00 00 00
0010  00 39 06 bd 40 00 00 00 00 00 00 00 00 00 00 00
0020  e2 b6 e4 98 00 6e 00 00 00 00 00 00 00 00 00 00
0030  00 fb 2f 03 00 00 00 00 00 00 00 00 00 00 00 00
0040  2b 77 ff f4 ff fd
  
```

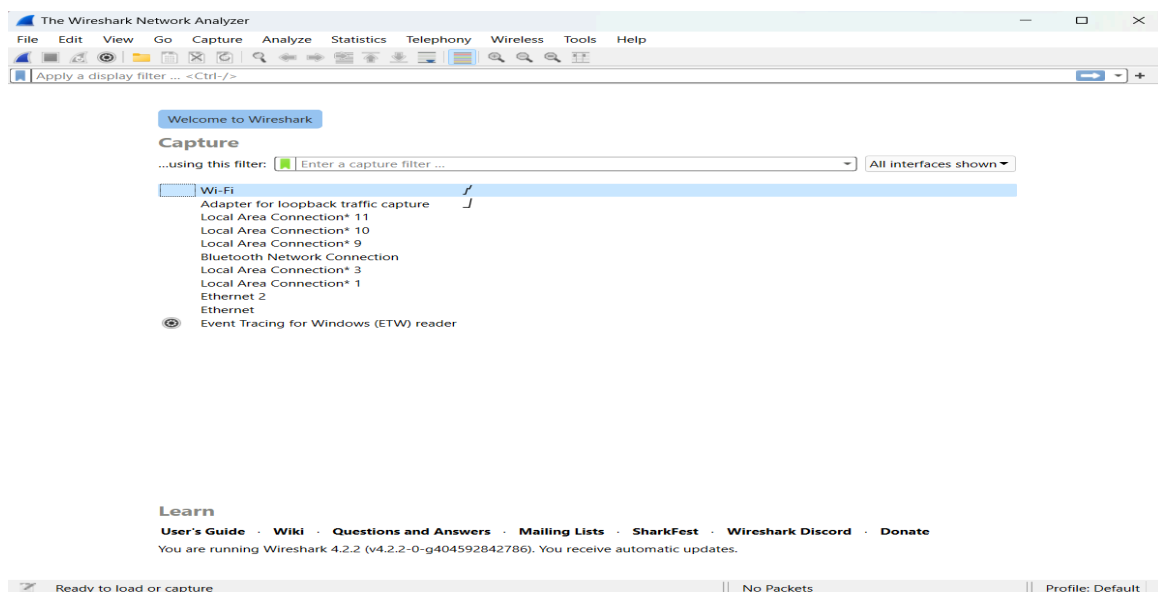
For Http Website

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

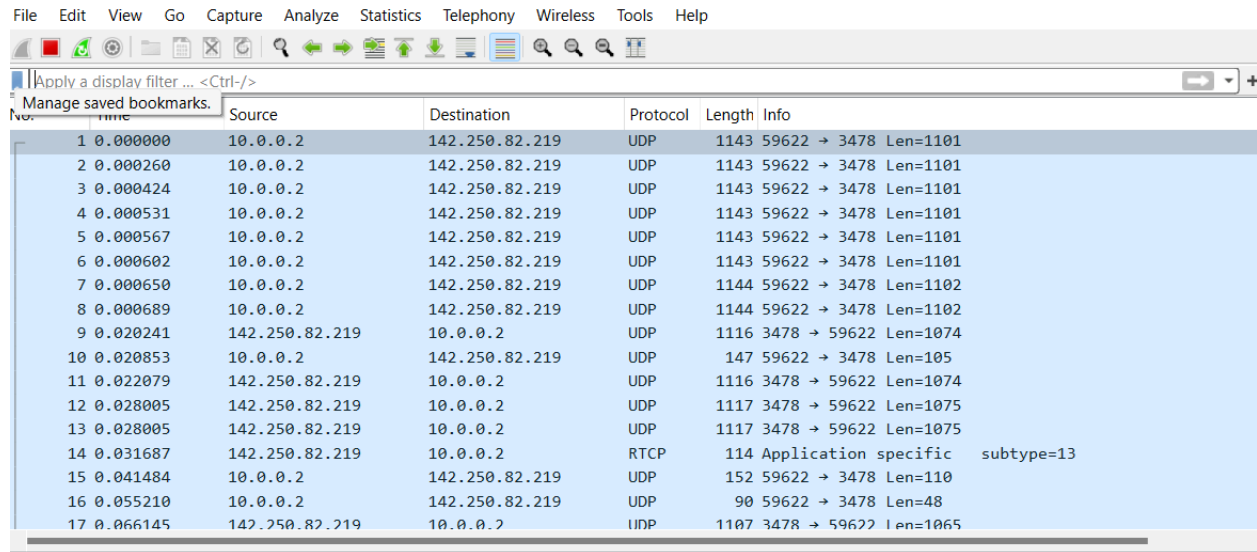
1. Find a website with the protocol HTTP and not HTTPS, this websites are not secured and vulnerable http sniffing



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

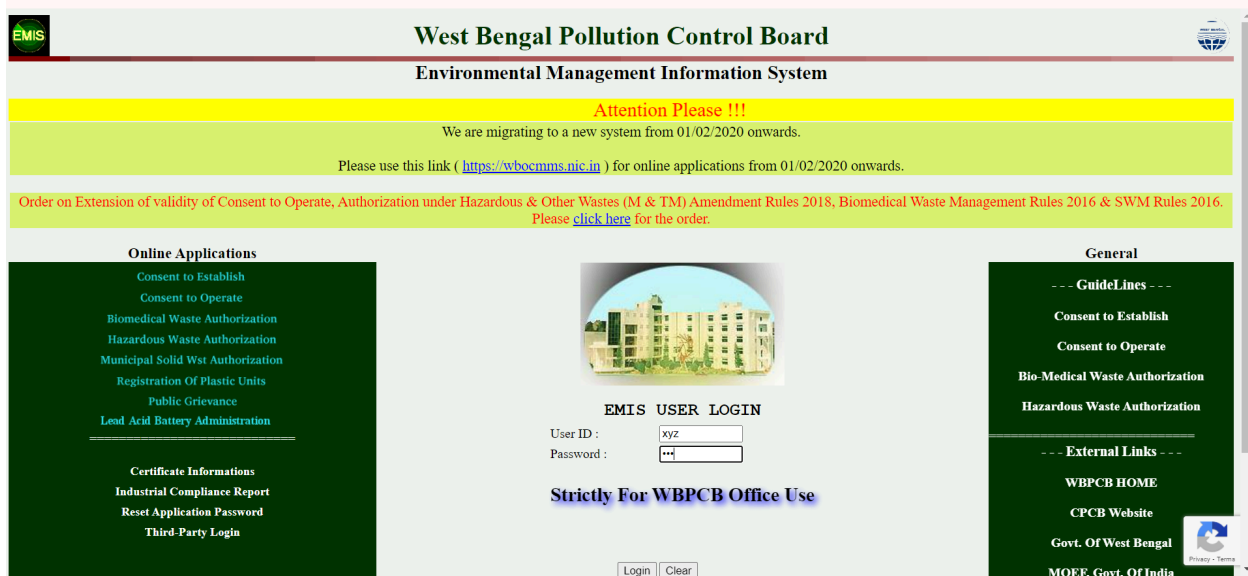


3. Start Capturing the Packets from that website in the wireshark tool



| 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



West Bengal Pollution Control Board
Environmental Management Information System

Attention Please !!!
We are migrating to a new system from 01/02/2020 onwards.
Please use this link (<https://wbpcmis.nic.in>) for online applications from 01/02/2020 onwards.

Order on Extension of validity of Consent to Operate, Authorization under Hazardous & Other Wastes (M & TM) Amendment Rules 2018, Biomedical Waste Management Rules 2016 & SWM Rules 2016.
Please [click here](#) for the order.

Online Applications
Consent to Establish
Consent to Operate
Biomedical Waste Authorization
Hazardous Waste Authorization
Municipal Solid Wst Authorization
Registration Of Plastic Units
Public Grievance
Lead Acid Battery Administration

General
--- GuideLines ---
Consent to Establish
Consent to Operate
Bio-Medical Waste Authorization
Hazardous Waste Authorization

EMIS USER LOGIN
User ID :
Password :

Strictly For WBPCB Office Use

Login Clear

External Links
WBPCB HOME
CPCB Website
Govt. Of West Bengal
MOEF, Govt. Of India

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. A filter 'http' is applied to the top. The list shows packets 14676 through 69283, all of which are HTTP requests or responses. The 'Info' column shows details like 'HTTP/1.1 200 OK (image/jpeg)' or 'HTTP/1.1 200 OK (text/html)'.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 2950). It includes Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII. The ASCII column shows the text of the HTTP response, including status codes and headers.

The selected packet (Frame 2950) is an HTTP 200 OK response from 10.0.0.2 to 10.0.0.2. The details pane shows the Hypertext Transfer Protocol section, which includes the status line 'HTTP/1.1 200 OK (image/jpeg)' and various headers like 'Host: nephob' and 'User-Agent: sTeraBox'.

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

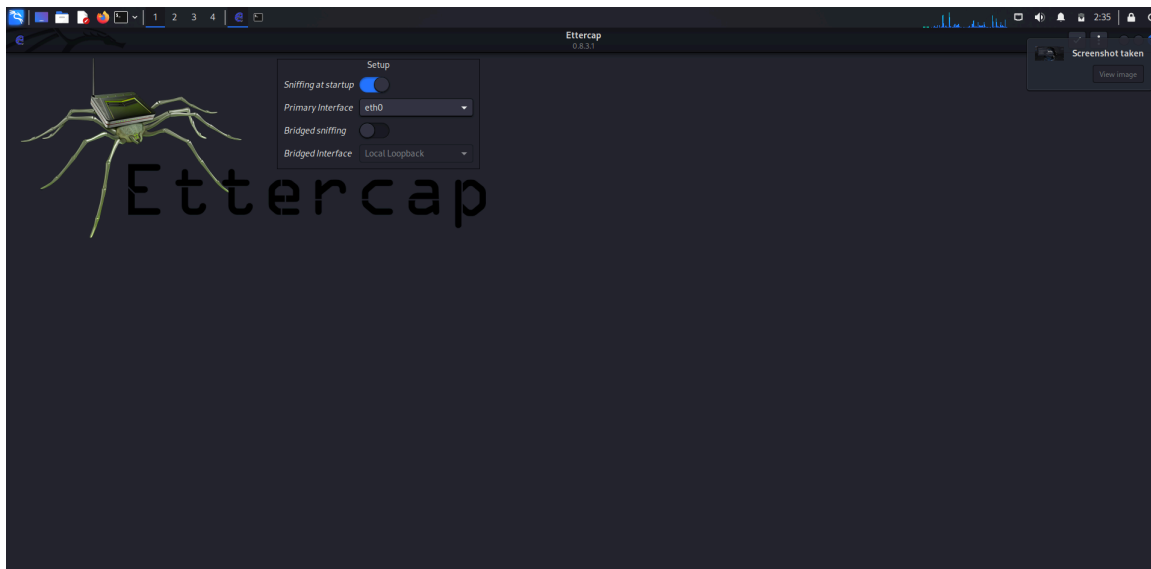
Interface: 10.0.0.5 --- 0x9
    Internet Address      Physical Address         Type
    10.0.0.1              28-c6-8e-da-41-af       dynamic
    10.0.0.8              08-00-27-1e-36-4a       dynamic
    10.0.0.255            ff-ff-ff-ff-ff-ff       static
    224.0.0.2              01-00-5e-00-00-02       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

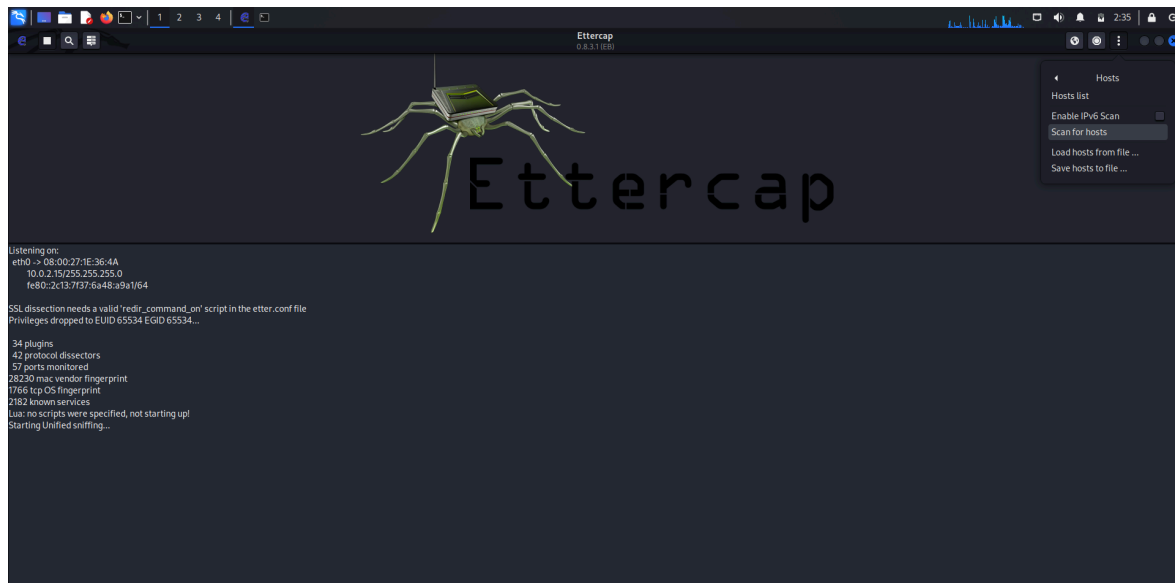


Step 4 : Then Go to the kali linux icon and search for sniffing and spoofing section and click on the tool ettercap on right side

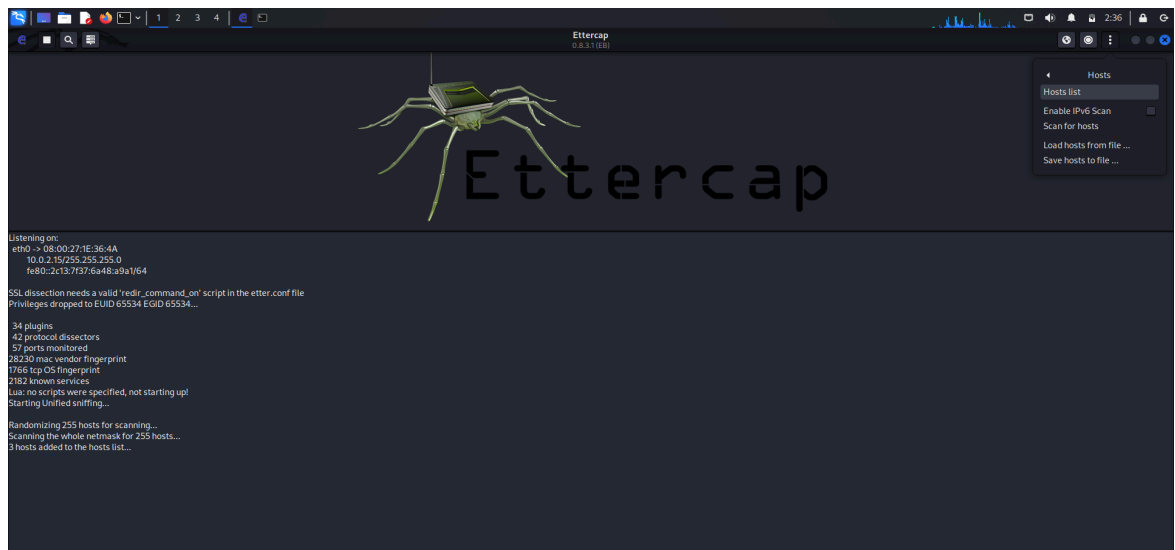
Step 5 : Open the ettercap and keep the default settings as it is and click on the tick on the right side



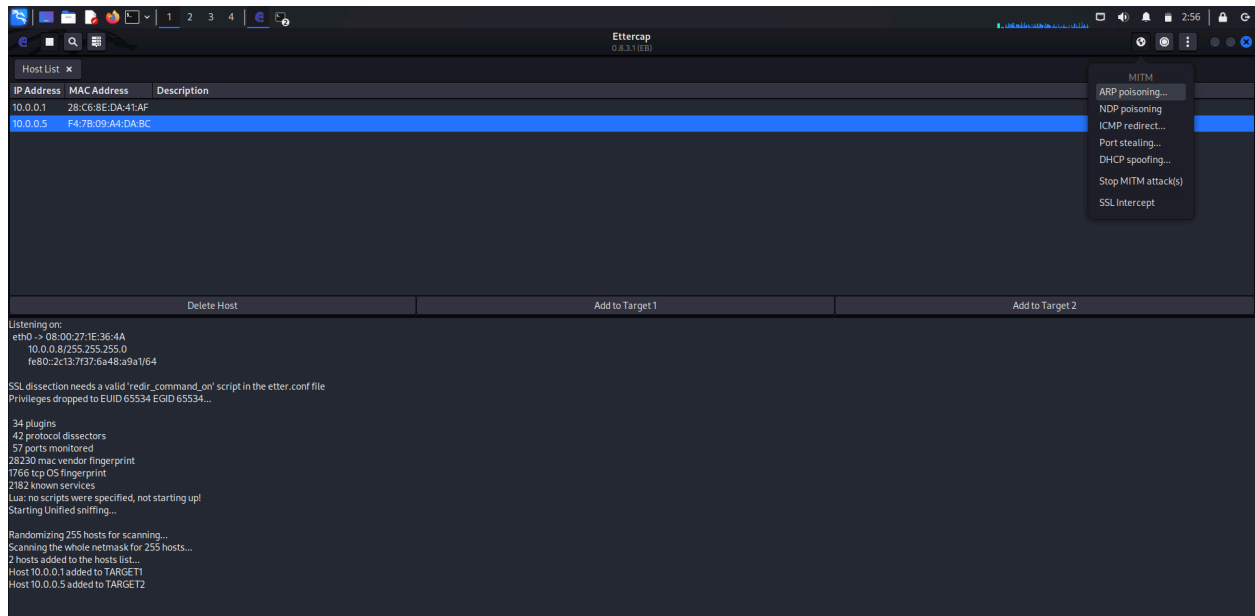
Step 6 : Click on three hamburger icon and select host and in hosts select scan for host, this will scan all the active host in your Network



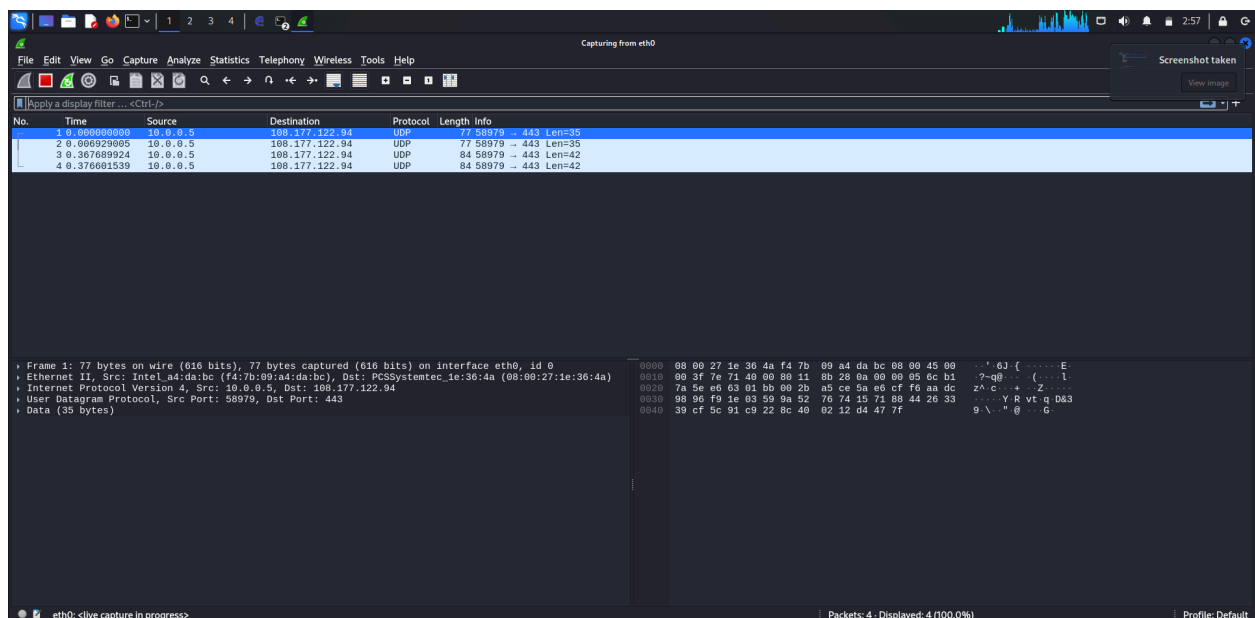
Step 7 : After it is done scanning for the host, again click on Hosts and click on Hosts list to see all the host in the network



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
```

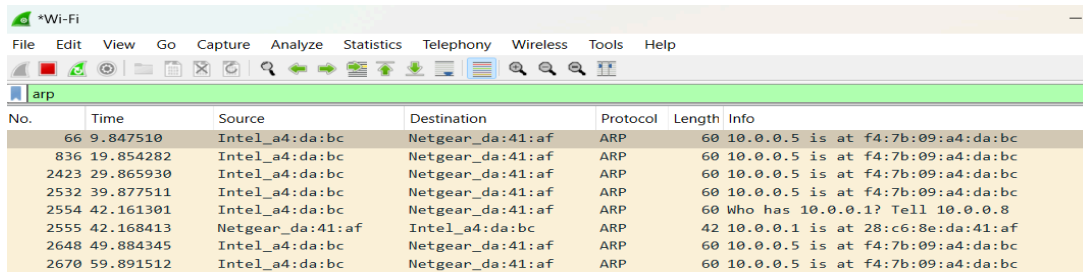
```
Interface: 192.168.56.1 --- 0x3
```

| 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
```

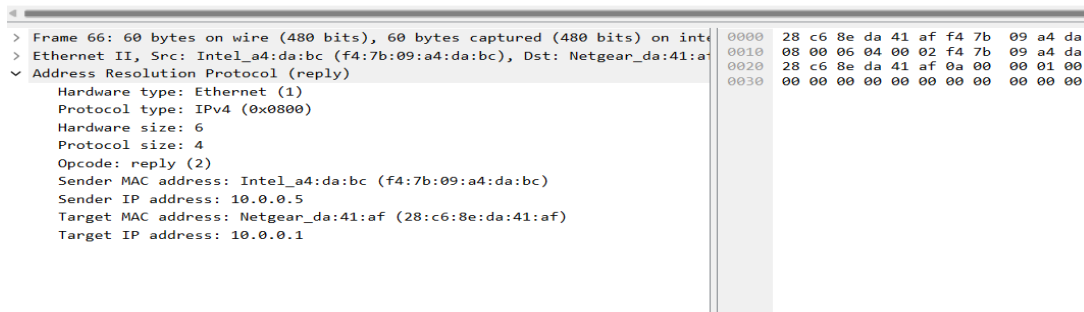
| Internet Address | Physical Address | Type |
|------------------|-------------------|---------|
| 10.0.0.1 | 08-00-27-1e-36-4a | dynamic |
| 10.0.0.8 | 08-00-27-1e-36-4a | dynamic |
| 10.0.0.255 | ff-ff-ff-ff-ff-ff | static |
| 224.0.0.2 | 01-00-5e-00-00-02 | static |
| 224.0.0.22 | 01-00-5e-00-00-16 | 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



Wireshark interface showing a packet capture filter 'arp' and a list of ARP packets. The filter is applied to the 'arp' protocol. The packet list shows several ARP requests and replies between Intel_a4:da:bc and Netgear_da:41:af.

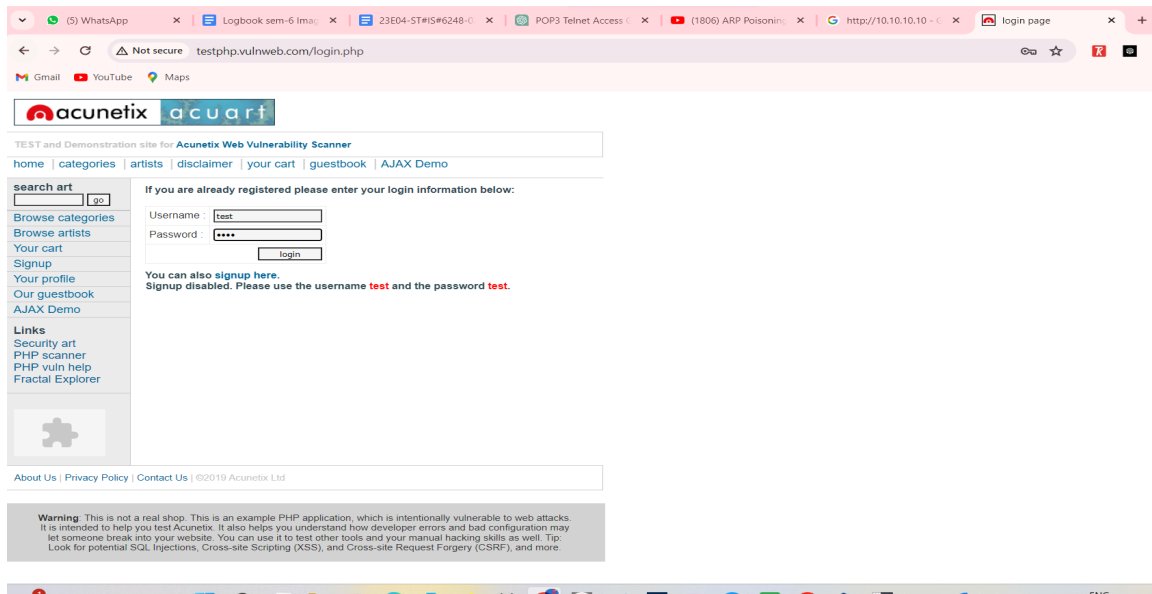
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|------------------|------------------|----------|--------|----------------------------------|
| 66 | 9.847510 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |
| 836 | 19.854282 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |
| 2423 | 29.865930 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |
| 2532 | 39.877511 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |
| 2554 | 42.161301 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | Who has 10.0.0.1? Tell 10.0.0.8 |
| 2555 | 42.168413 | Netgear_da:41:af | Intel_a4:da:bc | ARP | 42 | 10.0.0.1 is at 28:c6:8e:da:41:af |
| 2648 | 49.884345 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |
| 2670 | 59.891512 | Intel_a4:da:bc | Netgear_da:41:af | ARP | 60 | 10.0.0.5 is at f4:7b:09:a4:da:bc |



Wireshark packet details pane for frame 66. The packet is an ARP reply from Intel_a4:da:bc to Netgear_da:41:af. The details show the hardware type as Ethernet (1), protocol type as IPv4 (0x0800), hardware size as 6, protocol size as 4, opcode as reply (2), sender MAC address as Intel_a4:da:bc (f4:7b:09:a4:da:bc), sender IP address as 10.0.0.5, target MAC address as Netgear_da:41:af (28:c6:8e:da:41:af), and target IP address as 10.0.0.1.

```
> Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Intel_a4:da:bc (f4:7b:09:a4:da:bc), Dst: Netgear_da:41:af (28:c6:8e:da:41:af)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Intel_a4:da:bc (f4:7b:09:a4:da:bc)
    Sender IP address: 10.0.0.5
    Target MAC address: Netgear_da:41:af (28:c6:8e:da:41:af)
    Target IP address: 10.0.0.1
```

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



Screenshot of the Acunetix Web Vulnerability Scanner login page. The page is titled "Acunetix acunetix" and includes a search bar, navigation links, and a login form. The login form has fields for Username (test) and Password (****), and a login button. A message states: "You can also signup here. Signup disabled. Please use the username test and the password test." The footer includes links for About Us, Privacy Policy, and Contact Us, and a copyright notice for 2019 Acunetix Ltd.

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

If you are already registered please enter your login information below:

Username:
Password:

You can also signup here.
Signup disabled. Please use the username test and the password test.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

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

| Delete Host | Add to Target 1 | Add to Target 2 |
|--|-----------------|-----------------|
| <pre>Lua: no scripts were specified, not starting up! Starting Unified sniffing... Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 2 hosts added to the hosts list... Host 10.0.0.1 added to TARGET1 Host 10.0.0.5 added to TARGET2 ARP poisoning victims: GROUP 1 : 10.0.0.128:C6:8E:DA:41:AF GROUP 2 : 10.0.0.5:F4:7B:09:A4:DA:BC HTTP - 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php CONTENT: uname=test&pass=test HTTP - 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php CONTENT: uname=test&pass=test</pre> | | |