NAME: JENNIFER ZACK

BATCH: NOVEMBER B1

DOMAIN: CYBERSECURITY

TABLE OF VALUES

LIST OF FIGURES

BEGINNERS 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.**

Ports are numerical identifiers for specific services on a network. They help distinguish between the different services running on a machine, allowing various types of communication over the network. They are essentially numbered gateways through which different network services communicate. For instance, port 80 is commonly used for web traffic, while port 25 is associated with email. By scanning for open ports, we can determine which services are active and potentially vulnerable.

The information gathered from port scanning allows us to identify potential risks and implement appropriate security measures. This proactive approach helps protect systems from unauthorized access and malicious attacks.

INFORMATION

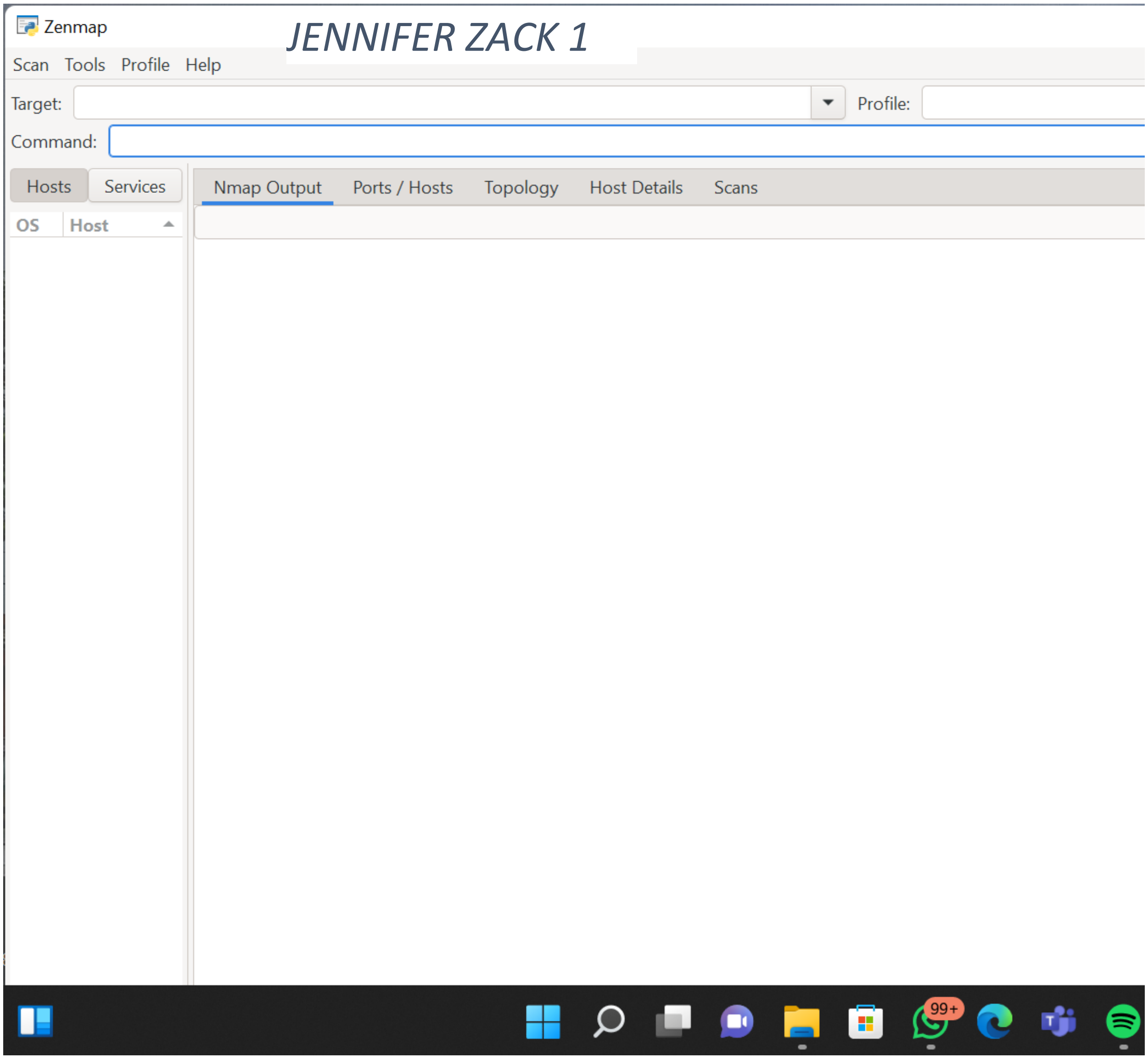
Operating system: windows 11
Domain name : http://testphp.vulnweb.com/
Tools used: Nmap
Method: Port Scanning.
Nmap Command: “nmap --open-44.228.249

ATTACK VECTOR PLANS

Attack name: Port Scanning
Severity: Medium (score-5.5)
Impact: open ports could be exploited by malicious actors

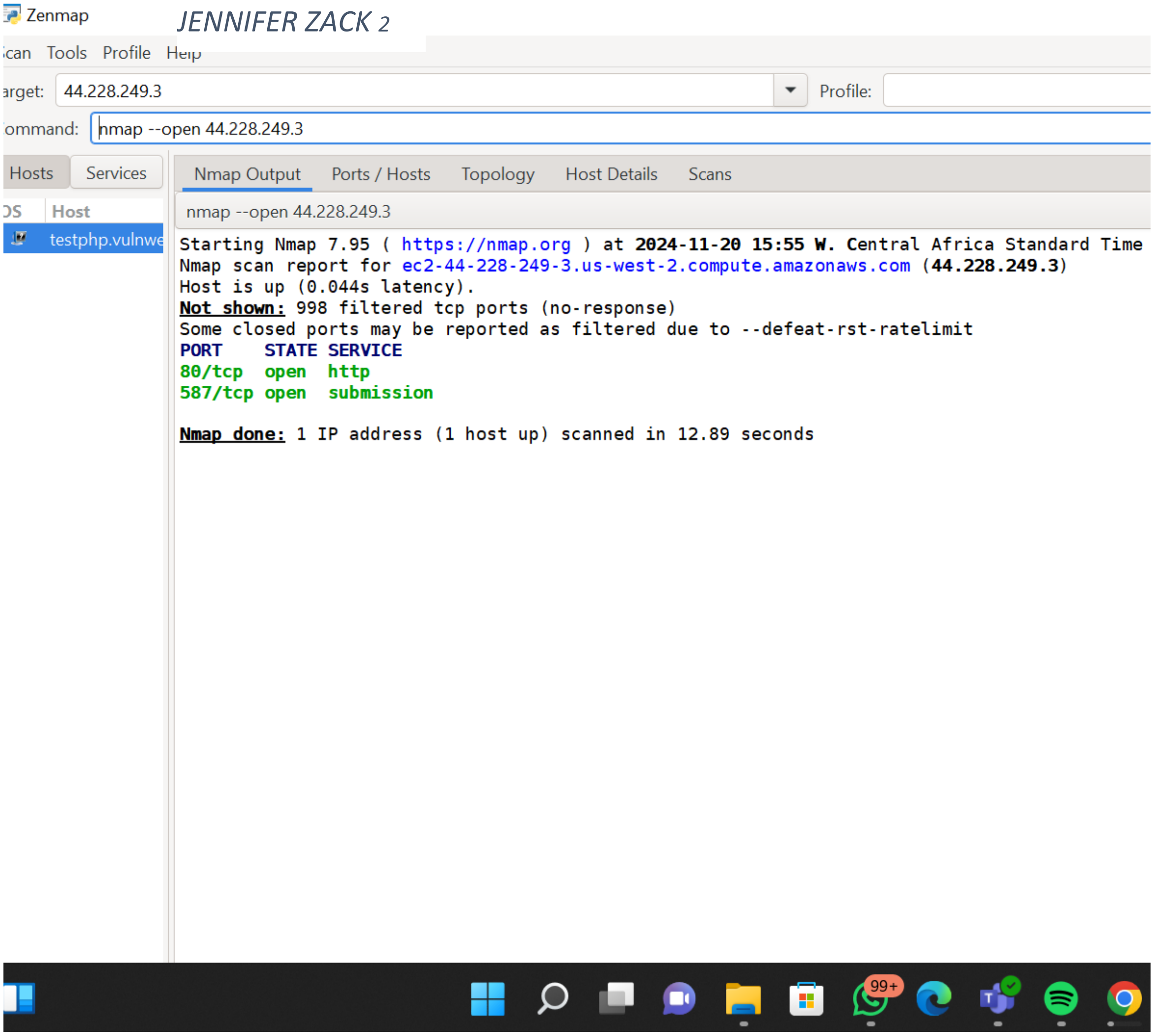
STEPS TO REPRODUCE

1. Download and install Nmap software on your computer.



2. Input Nmap command execution “ nmap -- open- 44.228.249”

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



Target: 44.228.249.3

Command: nmap --open 44.228.249.3

nmap --open 44.228.249.3

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-20 15:55 W. Central Africa Standard Time
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.044s latency).
Not shown: 998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```

4. Takes screenshot for documentation

MITIGATION STEPS:

1. ALL OPEN PORTS NOT IN USE SHOULD BE CLOSED TO PREVENT MALICIOUS USE OF THEM
2. CONFIGURE THE NECESSARY FIREWALL RULES TO PREVENT UNAUTHORIZED ACCESS TO OPEN PORTS
3. CONSISTENTLY MONITOR ONGOING ACTIVITIES ON THE NETWORK

REFERENCES

The Nmap documentation

RESOURCE 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 perform a Directory Enumeration (Directory enumeration is a process in cybersecurity where an attacker or a security tester attempts to discover directories and files on a web server that may not be visible or intended to be publicly accessible.)

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

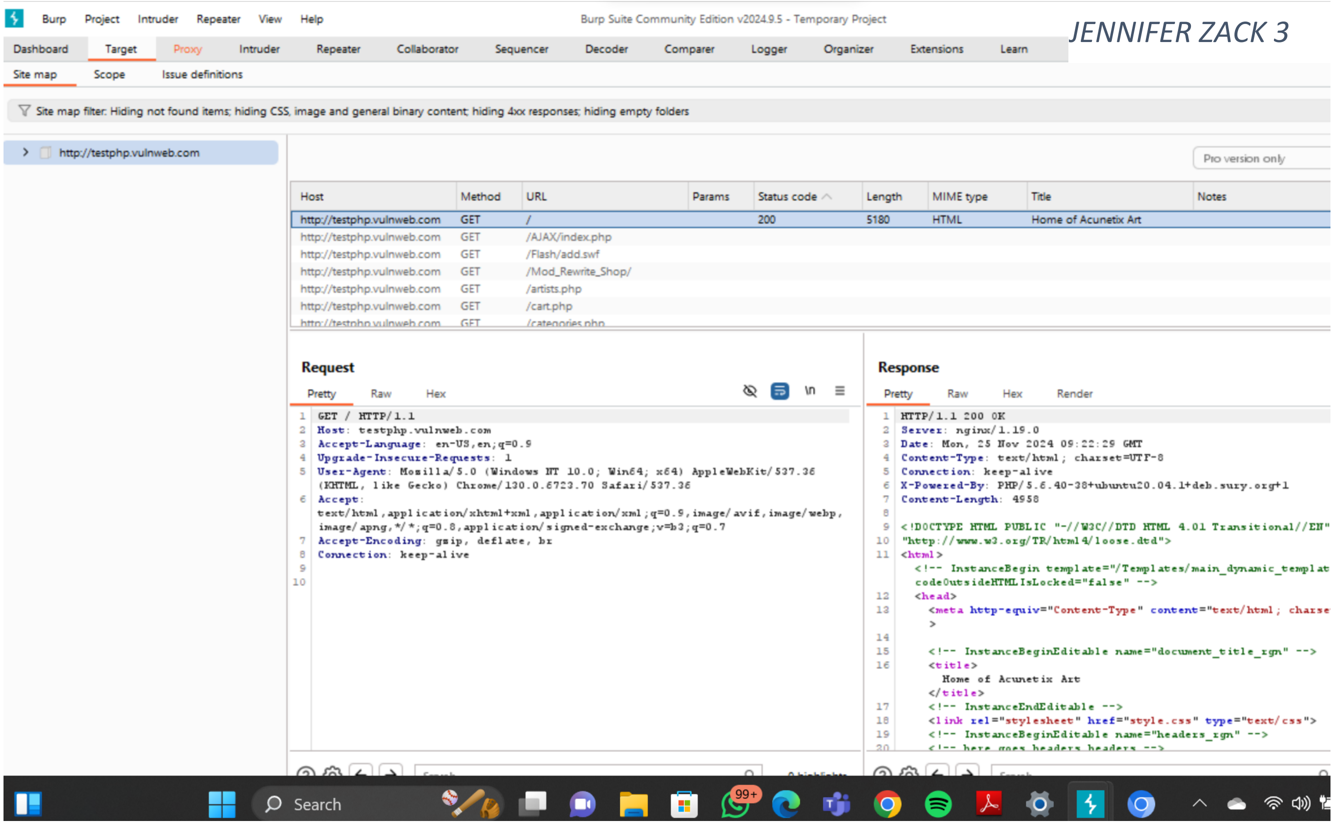
ATTACK VECTOR PLANS

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



JENNIFER ZACK 3

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
http://testphp.vulnweb.com	GET	/		200	5180	HTML	Home of Acunetix Art	
http://testphp.vulnweb.com	GET	/AJAX/index.php						
http://testphp.vulnweb.com	GET	/Flash/add.swf						
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/						
http://testphp.vulnweb.com	GET	/artists.php						
http://testphp.vulnweb.com	GET	/cart.php						
http://testphp.vulnweb.com	GET	/categories.php						

Request

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 25 Nov 2024 09:22:29 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 4958

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <!-- InstanceBegin template="/Templates/main_dynamic_templat
  codeOutsideHTMLIsLocked="false" -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charse
    >

    <!-- InstanceBeginEditable name="document_title_rgn" -->
    <title>
      Home of Acunetix Art
    </title>
    <!-- InstanceEndEditable -->
    <link rel="stylesheet" href="style.css" type="text/css">
    <!-- InstanceBeginEditable name="headers_rgn" -->
    <!-- here goes headers headers -->
```

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. Intrusion Detection and Prevention Systems (IDS/IPS) should be implemented to prevent Brute force attempts\

2. The system should be securely configured, with permissions limited to authorized users only, to prevent unauthorized access to directories intended to remain hidden.

REFERENCES

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

RESOURCES USED

1. Burp Suite community edition
2. OWASP guidelines

TASK THREE – NETWORK TRAFFIC INTERCEPTION

INTRODUCTION

Wireshark is a widely-used, open-source network protocol analyzer that allows users to capture, analyze, and visualize network traffic in real-time. It provides a detailed view of the data packets being transmitted across a network, enabling users to inspect individual packets for specific information, such as Username, passwords etc.

INFORMATION

The objective of this task is to locate credentials transmitted over the network. The Hypertext Transfer Protocol (HTTP) is used because it brings up a webpage when a URL is entered into a browser. Wireshark can capture network traffic using HTTP, especially when credentials are transmitted without proper encryption.

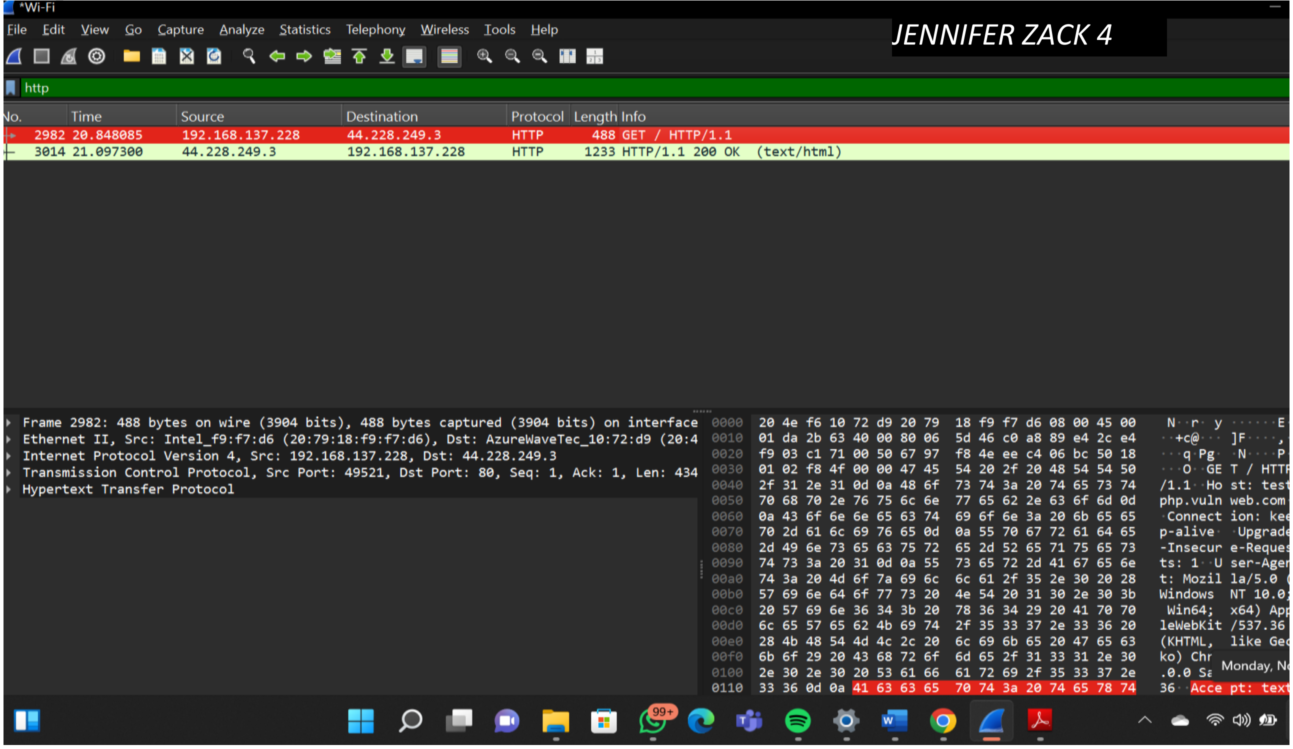
ATTACK VECTOR PLANS

Attack name: Network Traffic Interception
Severity: High, score = 7.5
Impact: Unencrypted credentials can be intercepted on the network and misused, potentially resulting in data breaches and causing further harm to the system.

Steps to reproduce:

1. Install the Wireshark 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 Wireshark interface once the Login process is completed
5. Input the filter command in the search panel to isolated HTTP POST Requests


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
JENNIFER ZACK 4
Monday, N

```
http
```

```
No.   Time        Source           Destination      Protocol Length Info
 2982 20.848085   192.168.137.228  44.228.249.3     HTTP       488 GET / HTTP/1.1
 3014 21.097300   44.228.249.3     192.168.137.228  HTTP      1233 HTTP/1.1 200 OK  (text/html)
```

```
Frame 2982: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface
Ethernet II, Src: Intel_f9:f7:d6 (20:79:18:f9:f7:d6), Dst: AzureWaveTec_10:72:d9 (20:4
Internet Protocol Version 4, Src: 192.168.137.228, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 49521, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
Hypertext Transfer Protocol
```

```
0000  20 4e f6 10 72 d9 20 79  18 f9 f7 d6 08 00 45 00   N··r· y ······E
0010  01 da 2b 63 40 00 80 06  5d 46 c0 a8 89 e4 2c e4  ··+c@···]F····,
0020  f9 03 c1 71 00 50 67 97  f8 4e ee c4 06 bc 50 18  ···q·Pg··N····P
0030  01 02 f8 4f 00 00 47 45  54 20 2f 20 48 54 54 50  ···O··GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74  /1.1··Ho st: test
0050  70 68 70 2e 76 75 6c 6e  77 65 62 2e 63 6f 6d 0d  php.vuln web.com
0060  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65  ·Connect ion: kee
0070  70 2d 61 6c 69 76 65 0d  0a 55 70 67 72 61 64 65  p-alive··Upgrade
0080  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73  -Insecur e-Reques
0090  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e  ts: 1··U ser-Agen
00a0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28  t: Mozil la/5.0 (
00b0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b  Windows  NT 10.0;
00c0  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70   Win64;  x64) App
00d0  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20  leWebKit /537.36
00e0  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63  (KHTML,  like Gec
00f0  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 33 31 2e 30  ko) Chr
0100  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e  .0.0 Sa
0110  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74  36··Acce pt: text
```

6. Finally search through the packet to identify the credentials that are transferred in plaintext

Mitigation Steps

1. Implement strong and reliable encryption protocols, such as TLS, to ensure secure communication across the network.
2. Ensure that all data transmitted over the network is securely encrypted.

REFERENCE

1. Wireshark user guide
2. OWASP Secure Communication Guidelines: https://owasp.org/wwwproject-secure-headers/

RESOURCES USED

1. Wireshark: Used for capturing and analyzing network traffic.

interception process.

2. OWASP Guidelines

INTERMEDIATE LEVEL

TASK ONE – VERACRYPT FILE DECRYPTION

INTRODUCTION

VeraCrypt is an open-source encryption software that allows you to create secure, encrypted virtual disks or encrypt entire drives, helping to protect sensitive data.
This task provides a step-by-step guide on how to decrypt a file that has been encrypted with VeraCrypt, a disk encryption tool. The encrypted file will first be decoded using a decryption tool or website in the browser. Then, the password will be entered into VeraCrypt to decrypt the file and retrieve the secret code.

INFORMATION

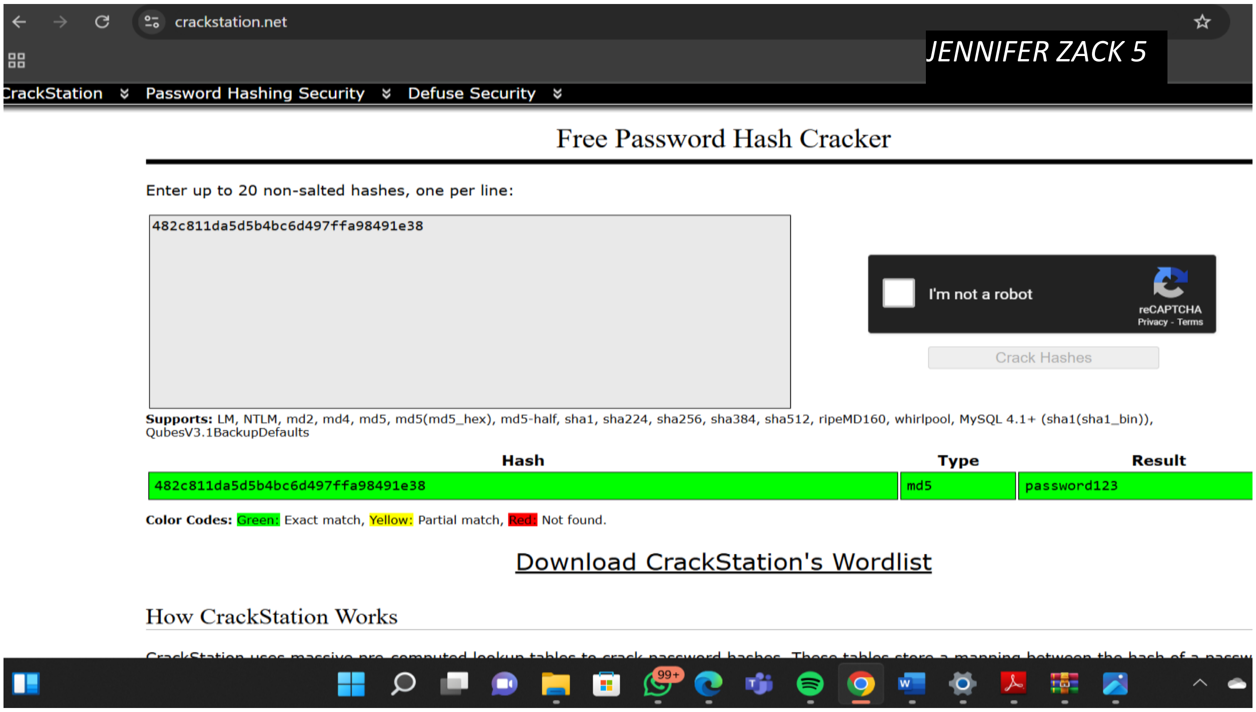
For this task, the password is encoded in hashed format which means it password file must be decrypted first before proceeding to the rest of the task
This report focuses on identifying the type of encryption used for the password to choose the right decryption method. Since there are various types of encryption, each one requires a different approach.

ATTACK VECTOR PLANS

Attack Name: Password Decoding and File Decryption
Severity: Medium (Score: 5.5)
Impact: Once the file is successfully decrypted, you'll be able to access the sensitive information inside.

STEPS TO REPRODUCE:

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



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
482c811da5d5b4bc6d497ffa98491e38
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
482c811da5d5b4bc6d497ffa98491e38	md5	password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

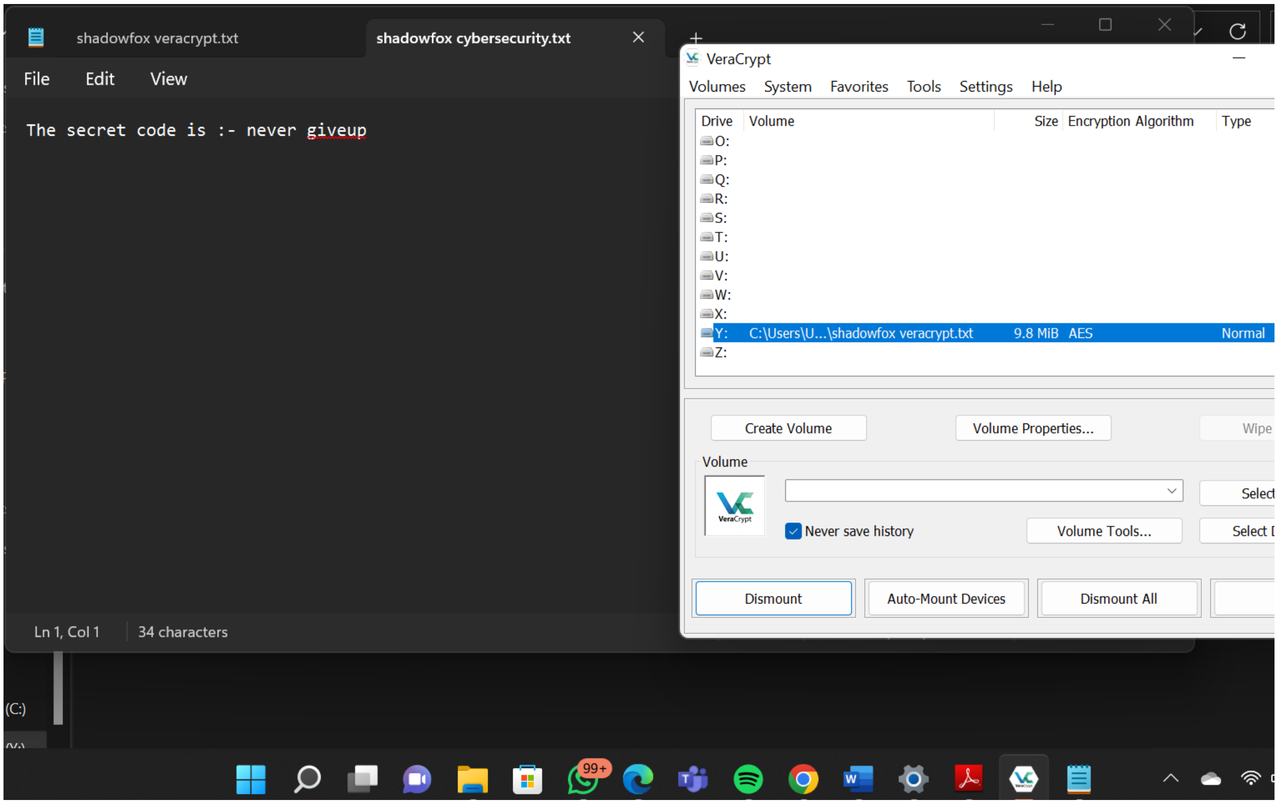
How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a passw

3. Create your volume in VeraCrypt and use the decrypted text as your file

4. input the password “password123” to open the decrypted file

5. open the decrypted file and retrieve the secret code



```
The secret code is :- never giveup
```

Ln 1, Col 1 | 34 characters

Drive	Volume	Size	Encryption Algorithm	Type
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:	C:\Users\U...\shadowfox veracrypt.txt	9.8 MiB	AES	Normal
Z:				

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
6. Implement the Principle of Least Privileged system

REFERENCE

1. Veracrypt set up file documentation
2. Password decoder website (https://crackstation.net/)

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

TASK TWO – ENTRY POINT ADDRESS OF VERACRYPT EXECUTABLE

INTRODUCTION

The entry point address is where a computer program starts running when it's opened. It's like a starting line that tells the computer, "Begin here," and then the program runs step by step from that point. This is the first stage in turning the program's code into a fully working application.

The requirement of this task to identify this 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. Understanding entry points is a key concept in reverse engineering and analyzing how executable files work.

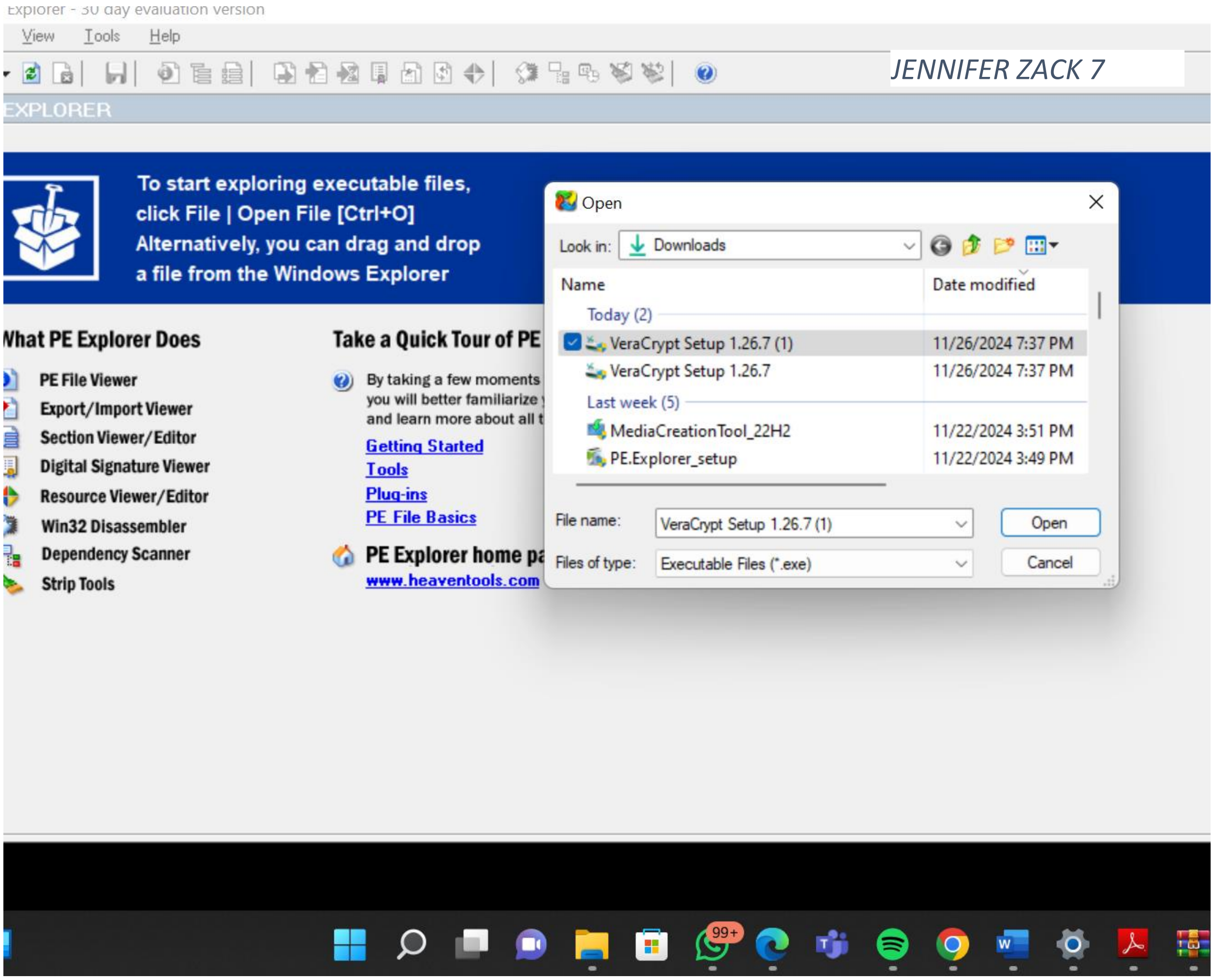
Windows was used for this task because it's compatible with PE Explorer and offers a variety of features useful for software analysis. These techniques are especially helpful for security professionals and developers, as they play a vital role in processes like debugging and troubleshooting.

ATTACK VECTOR PLANS

Attack name: reverse engineering
Severity: Medium (Score: 5.0)
Impact: unauthorized access by bypassing authentication systems, system crashes caused by altering the executable, and the corruption or loss of sensitive data during 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 too



To start exploring executable files, click File | Open File [Ctrl+O] Alternatively, you can drag and drop a file from the Windows Explorer

By taking a few moments you will better familiarize and learn more about all t

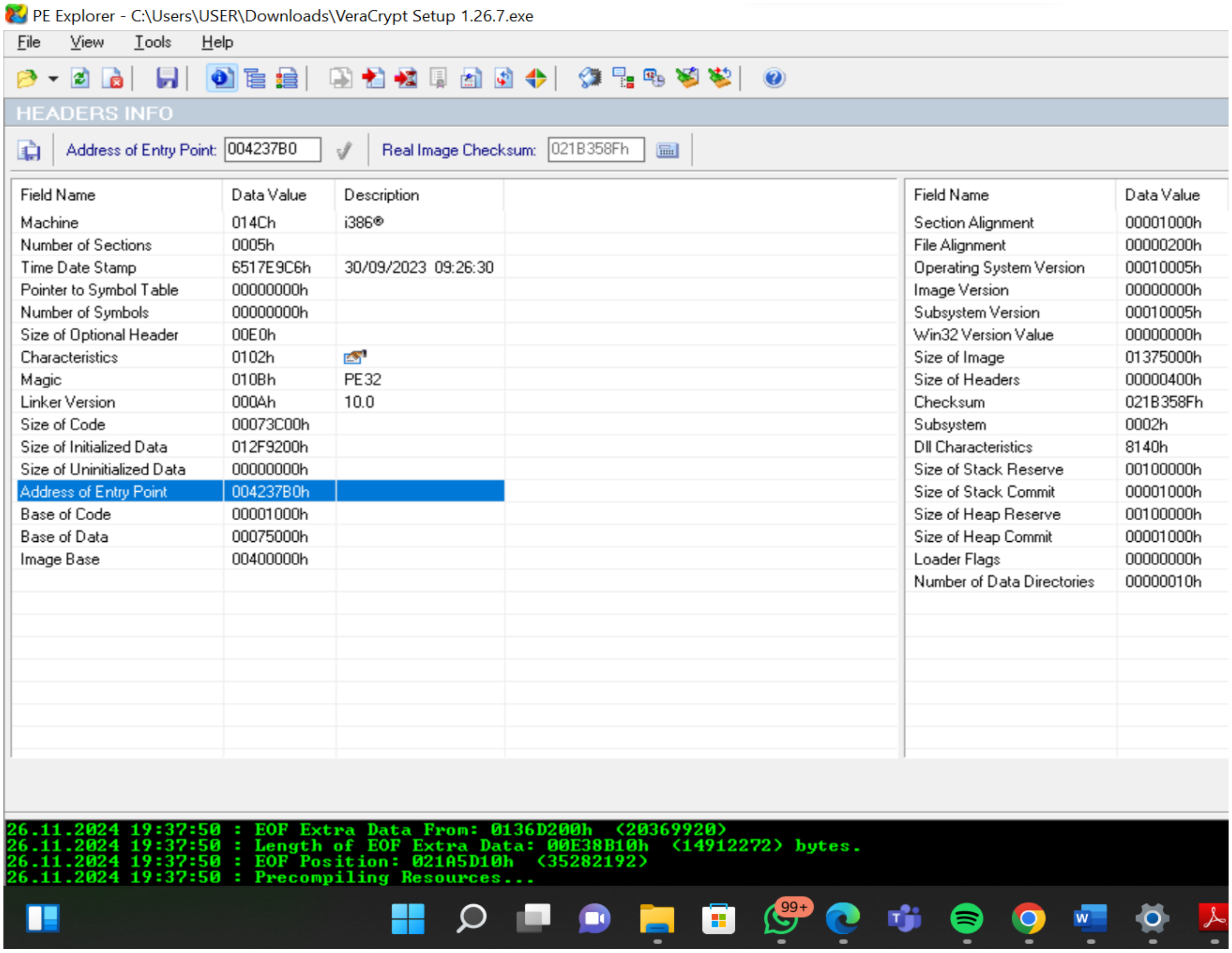
Look in: Downloads

Name	Date modified
Today (2)	
☑ VeraCrypt Setup 1.26.7 (1)	11/26/2024 7:37 PM
VeraCrypt Setup 1.26.7	11/26/2024 7:37 PM
Last week (5)	
MediaCreationTool_22H2	11/22/2024 3:51 PM
PE.Explorer_setup	11/22/2024 3:49 PM

File name: VeraCrypt Setup 1.26.7 (1)

Files of type: Executable Files (*.exe)

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


PE Explorer - C:\Users\USER\Downloads\VeraCrypt Setup 1.26.7.exe
File
View
Tools
Help
HEADERS INFO

Address of Entry Point: 004237B0

Real Image Checksum: 021B358Fh

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0005h	
Time Date Stamp	6517E9C6h	30/09/2023 09:26:30
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0102h	
Magic	010Bh	PE32
Linker Version	000Ah	10.0
Size of Code	00073C00h	
Size of Initialized Data	012F9200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004237B0h	
Base of Code	00001000h	
Base of Data	00075000h	
Image Base	00400000h	

Field Name	Data Value
Section Alignment	00001000h
File Alignment	00000200h
Operating System Version	00010005h
Image Version	00000000h
Subsystem Version	00010005h
Win32 Version Value	00000000h
Size of Image	01375000h
Size of Headers	00000400h
Checksum	021B358Fh
Subsystem	0002h
Dll Characteristics	8140h
Size of Stack Reserve	00100000h
Size of Stack Commit	00001000h
Size of Heap Reserve	00100000h
Size of Heap Commit	00001000h
Loader Flags	00000000h
Number of Data Directories	00000010h

```
26.11.2024 19:37:50 : EOF Extra Data From: 0136D200h  <20369920>
26.11.2024 19:37:50 : Length of EOF Extra Data: 00E38B10h  <14912272> bytes.
26.11.2024 19:37:50 : EOF Position: 021A5D10h  <35282192>
26.11.2024 19:37:50 : Precompiling Resources...
```

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. Chatgpt