

Programme: Computer Networks and Cyber Security

Module: Advanced Cybersecurity

Module code: ACCB6000

Assignment Title: Analysing, Ethically Hacking and Securing an Enterprise Network

Name: Andrian Morteau

Student ID: 2242425

Lecturer: Dr. Mohamed Ghanem



University of Wales

Trinity Saint David

Contents

<i>Task 1 – Network Setup</i>	3
<i>Task 2: Network Security Assessment</i>	9
<i>2.1. Environment Setup and Initial Configuration</i>	9
<i>Task 3 – Exploitation</i>	13
<i>3.1 Post-Exploitation</i>	13
<i>Task 4 – Security Measures</i>	18

Task 1 – Network Setup

*In this task, a virtual network was created using Oracle VirtualBox.
Three machines were used:*

ClientS1 (Windows 10)

S-DC1 (Windows Server)

L-DC (Linux machine)

All machines were started and working correctly, as shown in Figure 1.

IP Configuration

Each machine was given a manual (static) IP address so they can communicate with each other.

ClientS1 was configured in one network

S-DC1 was configured in another network

L-DC was connected to both networks so it can link them together

Figures 2, 3, and 4 show the IP settings on each machine.

Testing the Connection

*To check if the machines can communicate, the **ping command** was used.*

Figure 5 shows that ClientS1 can reach L-DC

Figure 7 shows that S-DC1 can communicate with the Linux machine

Figure 8 shows multiple successful connections between machines

Figure 9 shows ClientS1 successfully reaching the Linux machine

All tests showed successful replies, which means the network is working.

Routing (Connecting the Networks)

The Linux machine (L-DC) was used to connect both networks together.

This means:

Devices in one network can talk to devices in the other network

The Linux machine acts like a bridge between them

Figure 6 shows this configuration.

Final Result

At the end of the task:

All machines were correctly configured

All devices could communicate with each other

The network was working as expected

This setup is now ready for the next task (security testing).

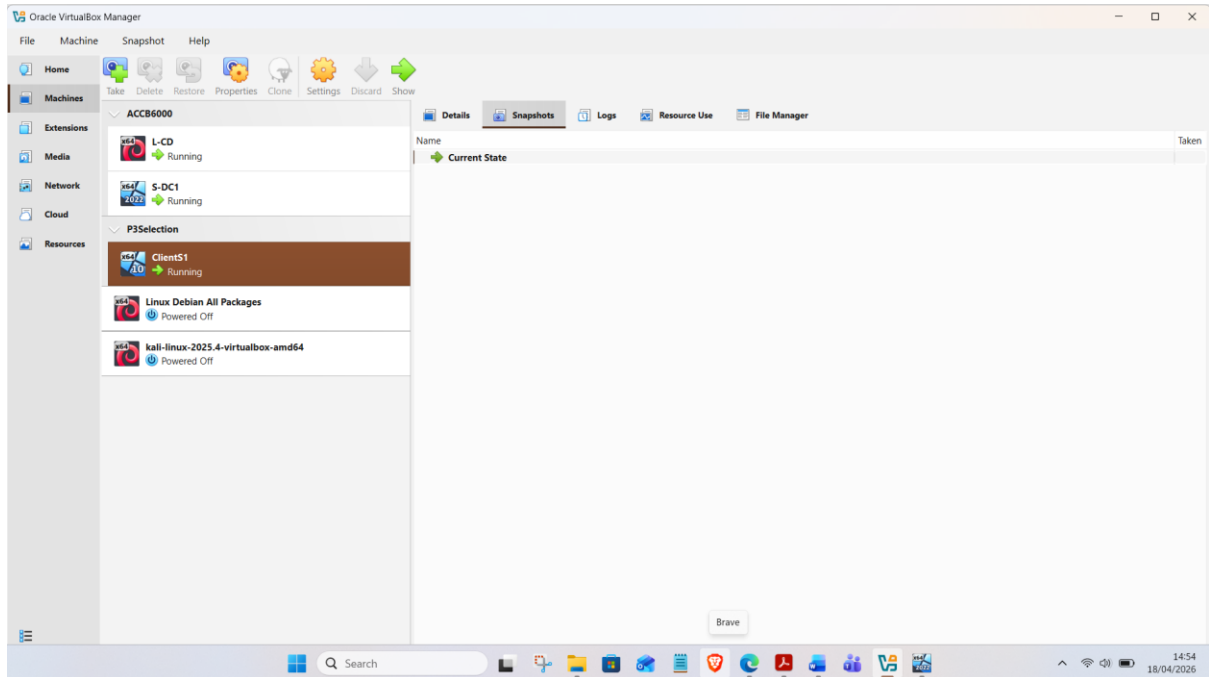


Figure 1: Virtual machine environment showing L-DC, S-DC, and Client1 all running in Oracle VirtualBox, prepared for network configuration and connectivity testing.

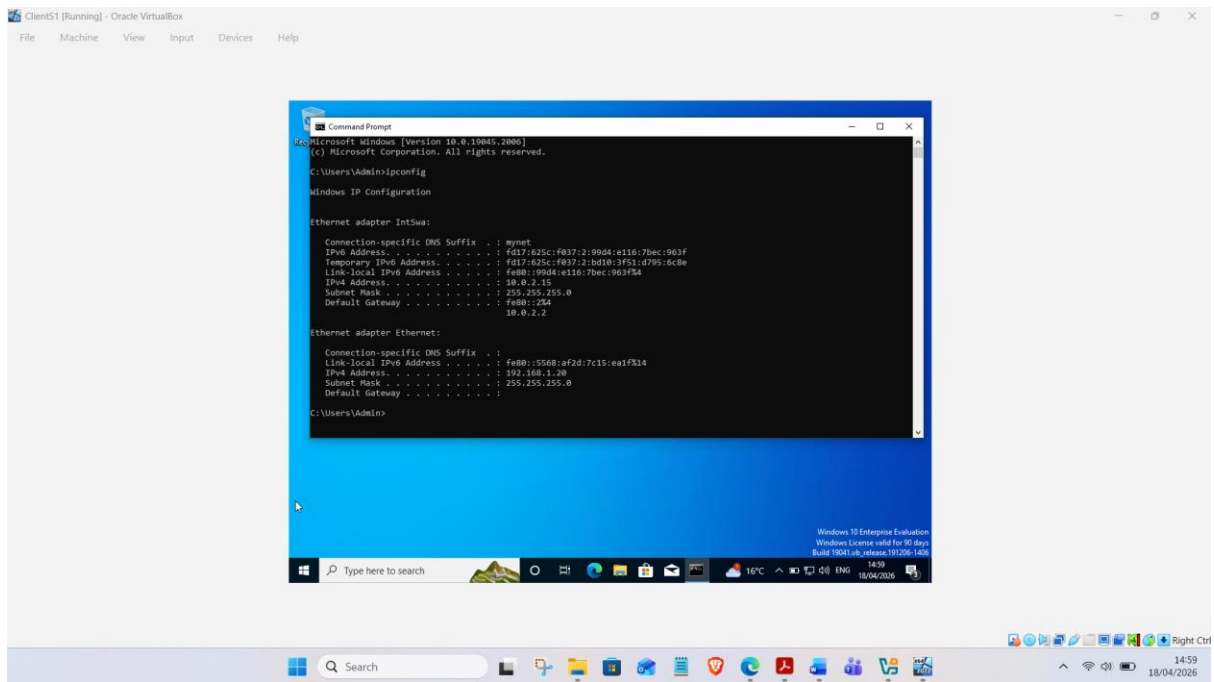


Figure 2: IP configuration of Client1 showing assignment within the London subnet (192.168.1.0/24).

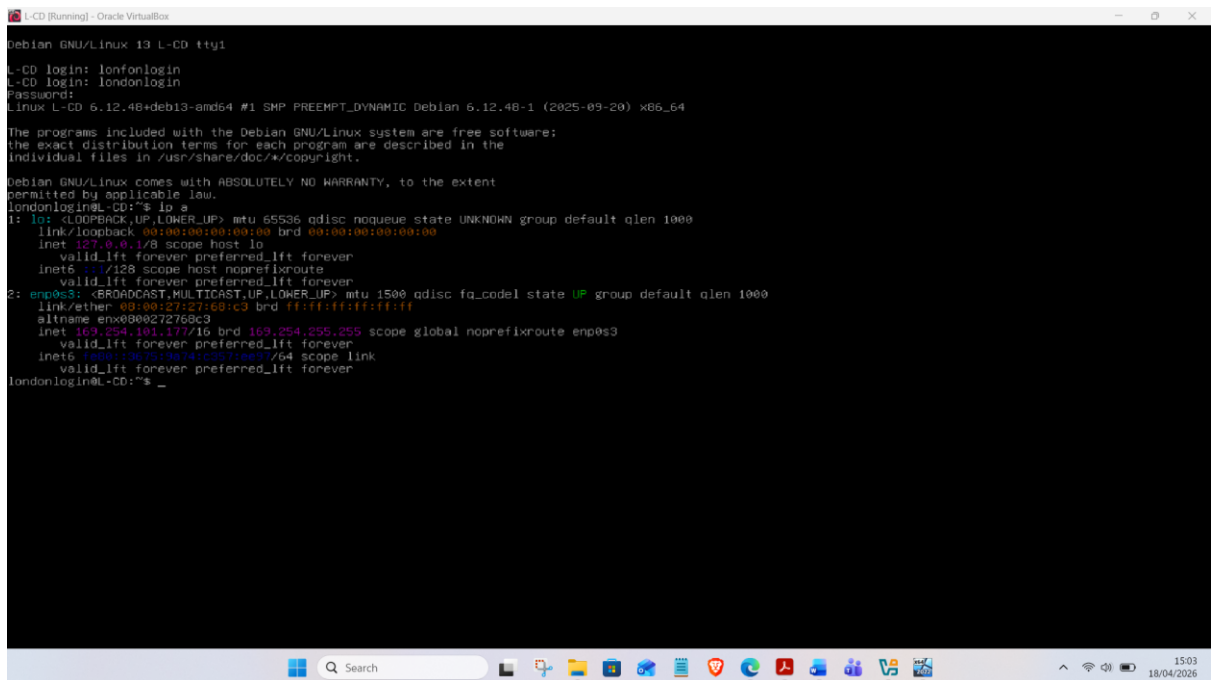


Figure 3: IP configuration of London Domain Controller (L-DC) showing network interfaces and IP assignment for routing between subnets.

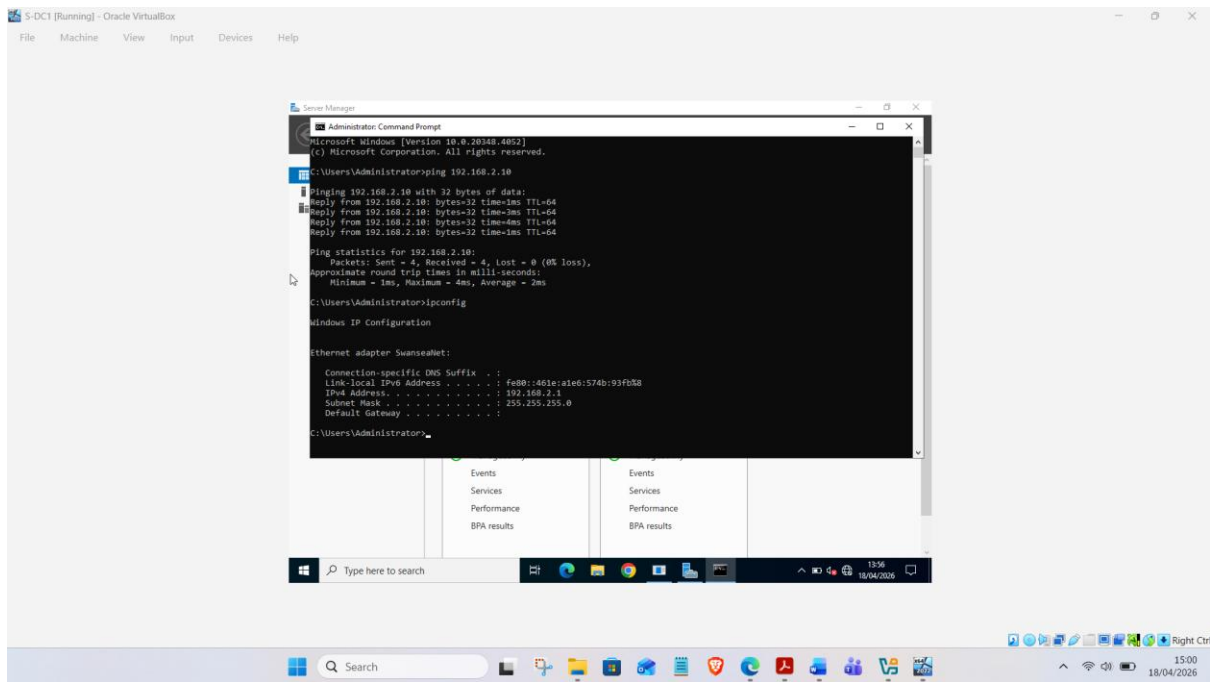


Figure 4: IP configuration of Swansea Domain Controller (S-DC) using ipconfig within the 192.168.2.0/24 network.

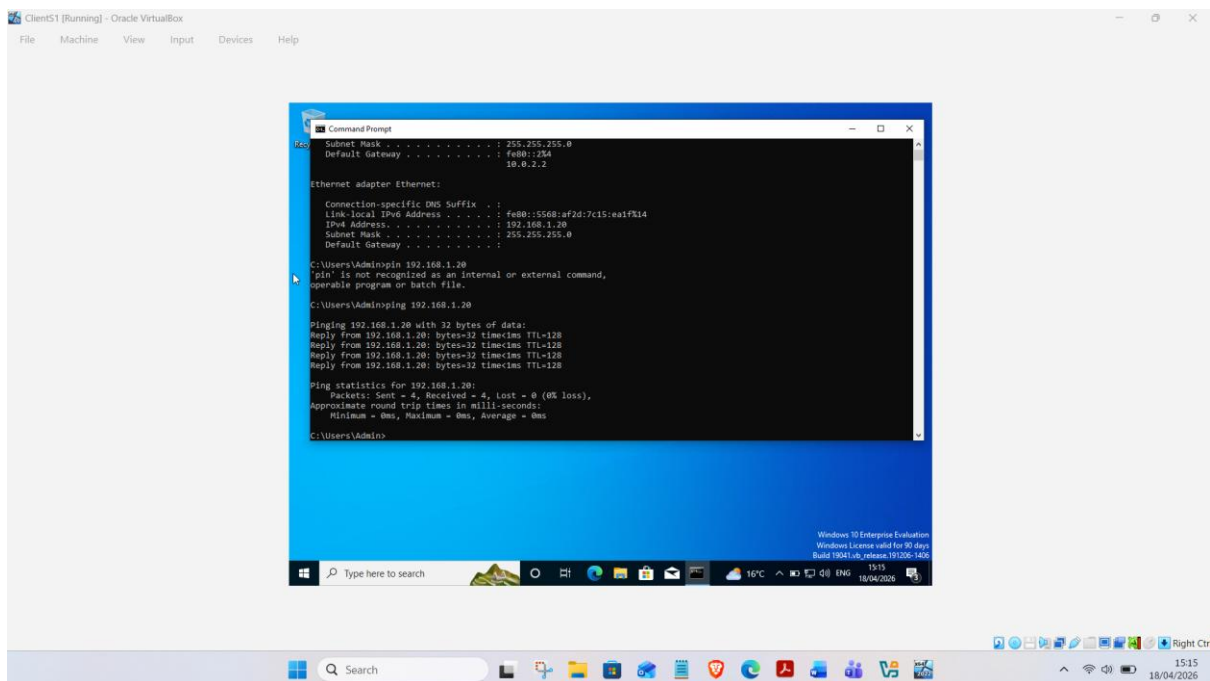


Figure 5: ICMP connectivity test from Client1 to London Domain Controller (L-DC) showing successful communication within the London subnet (192.168.1.0/24)

```
l-CD [Running] - Oracle VM VirtualBox
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
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:c3 brd ff:ff:ff:ff:ff:ff
    altname enx000272768c3
    inet 169.254.101.177/16 brd 169.254.255.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::19c5:3a74:c039:1a63/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:b4 brd ff:ff:ff:ff:ff:ff
    altname enx0800272768b4
    inet 169.254.248.17/16 brd 169.254.255.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::19c5:3a74:c039:1a63/64 scope link
        valid_lft forever preferred_lft forever
londonlogin@L-CD:~$ sudo ip addr add 192.168.1.20/24 dev enp0s3
[sudo] password for londonlogin:
londonlogin@L-CD:~$ sudo ip addr add 192.168.2.1/24 dev enp0s8
londonlogin@L-CD:~$ sudo ip link set enp0s3 up
londonlogin@L-CD:~$ sudo ip link set enp0s8 up
londonlogin@L-CD:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:c3 brd ff:ff:ff:ff:ff:ff
    altname enx000272768c3
    inet 169.254.101.177/16 brd 169.254.255.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.1.20/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::19c5:3a74:c039:1a63/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:b4 brd ff:ff:ff:ff:ff:ff
    altname enx0800272768b4
    inet 169.254.248.17/16 brd 169.254.255.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet 192.168.2.1/24 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::19c5:3a74:c039:1a63/64 scope link
        valid_lft forever preferred_lft forever
londonlogin@L-CD:~$
```

Figure 6: Network configuration on L-DC showing preparation for routing and interface configuration between London and Swansea networks.

```
S-DC1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Server Manager
Administrator Command Prompt
Default Gateway . . . . .
C:\Users\Administrator>netsh interface ip set address "External" static 192.168.2.10 255.255.255.0
C:\Users\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter External:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a775:4b51:570b:1fb4315
    IPv4 Address. . . . . : 192.168.2.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=5ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\Users\Administrator>
```

Figure 7: Connectivity test between S-DC1 and the Linux machine demonstrating successful communication across subnets.

```
L-CD [Running] - Oracle VM VirtualBox
[sudo] password for londonlogin:
londonlogin@L-CD:~$ sudo ip link set enp0s3 up
londonlogin@L-CD:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:c3 brd ff:ff:ff:ff:ff:ff
    altname enp0s3.272768c3 scope link
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.2.1/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::27:27:68:c3%3 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8a:1b:04 brd ff:ff:ff:ff:ff:ff
    altname enp0s8.278ab004 scope link
    inet 192.168.2.20/24 brd 192.168.2.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::27:8a:1b:04%8 scope link
        valid_lft forever preferred_lft forever
londonlogin@L-CD:~$ ping 192.168.2.10 (192.168.2.10) 56(84) bytes of data:
64 bytes from 192.168.2.10: icmp_seq=1 ttl=128 time=2.40 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=128 time=1.54 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=128 time=0.899 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=128 time=0.704 ms
64 bytes from 192.168.2.10: icmp_seq=5 ttl=128 time=2.11 ms
^C
-- 192.168.2.10 ping statistics --
5 packets transmitted, 5 received, 0% packet loss, time 4401ms
rtt min/avg/max/mdev = 0.704/1.530/2.401/0.650 ms
londonlogin@L-CD:~$ ping 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 56(84) bytes of data:
64 bytes from 192.168.2.20: icmp_seq=1 ttl=128 time=10.7 ms
64 bytes from 192.168.2.20: icmp_seq=2 ttl=128 time=0.918 ms
64 bytes from 192.168.2.20: icmp_seq=3 ttl=128 time=0.933 ms
64 bytes from 192.168.2.20: icmp_seq=4 ttl=128 time=0.744 ms
64 bytes from 192.168.2.20: icmp_seq=5 ttl=128 time=0.785 ms
64 bytes from 192.168.2.20: icmp_seq=6 ttl=128 time=0.462 ms
64 bytes from 192.168.2.20: icmp_seq=7 ttl=128 time=0.785 ms
^C
-- 192.168.2.20 ping statistics --
7 packets transmitted, 7 received, 0% packet loss, time 6193ms
rtt min/avg/max/mdev = 0.462/2.191/10.736/3.491 ms
londonlogin@L-CD:~$
```

Figure 8: A successful connectivity tests to S-DC1 (192.168.2.10) and ClientS1.

```
ClientS1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Command Prompt
C:\Users\Admin\ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\Users\Admin>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\Users\Admin>
```

Figure 9 ClientS1 successfully pinging Linux machine (192.168.2.1), confirming network connectivity across LAN2

Task 2: Network Security Assessment

2.1. Environment Setup and Initial Configuration

*In this task, a **Kali Linux machine** was used to perform security testing on the network.*

Kali Linux was connected to the Swansea network

Network settings and routing were checked to confirm connectivity

Figure 10 shows the IP configuration and routing table of Kali Linux.

Connectivity Testing

*Before starting security testing, the connection was verified using the **ping command**.*

Kali Linux successfully communicated with:

Swansea Server (192.168.2.10)

Client machine (192.168.2.20)

Figure 11 shows successful ping results.

This confirms that Kali Linux has proper access to the internal network.

Network Scanning (Information Gathering)

*After confirming connectivity, **Nmap** was used to scan the network and collect information.*

Swansea Server Scan

The server (192.168.2.10) was scanned

Open ports and running services were identified

Figure 12 shows the scan results for the server.

Client Machine Scan

The client machine (192.168.2.20) was also scanned

Open ports and active services were discovered

Figure 13 shows the scan results for the client.

Vulnerability Detection

After gathering information, a vulnerability scan was performed.

A known vulnerability was identified:

MS08-067 (Remote Code Execution)

This vulnerability could allow an attacker to gain control of the system

Figure 14 shows the vulnerability scan result.

Final Result

At the end of this task:

Kali Linux was successfully connected to the network

Network communication was verified

Nmap scans identified open ports and services

A real vulnerability was detected on the system

This shows that the network can now be properly analysed for security risks.

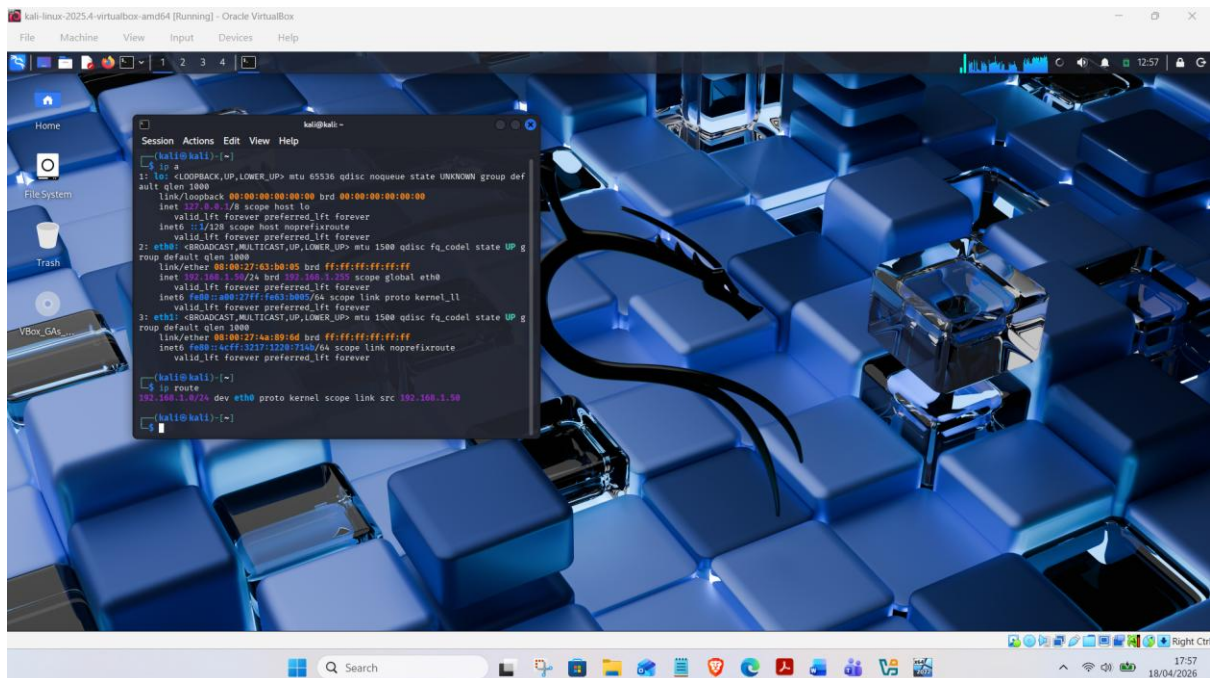


Figure 10: Kali Linux IP configuration and routing table showing active connection to Swansea network

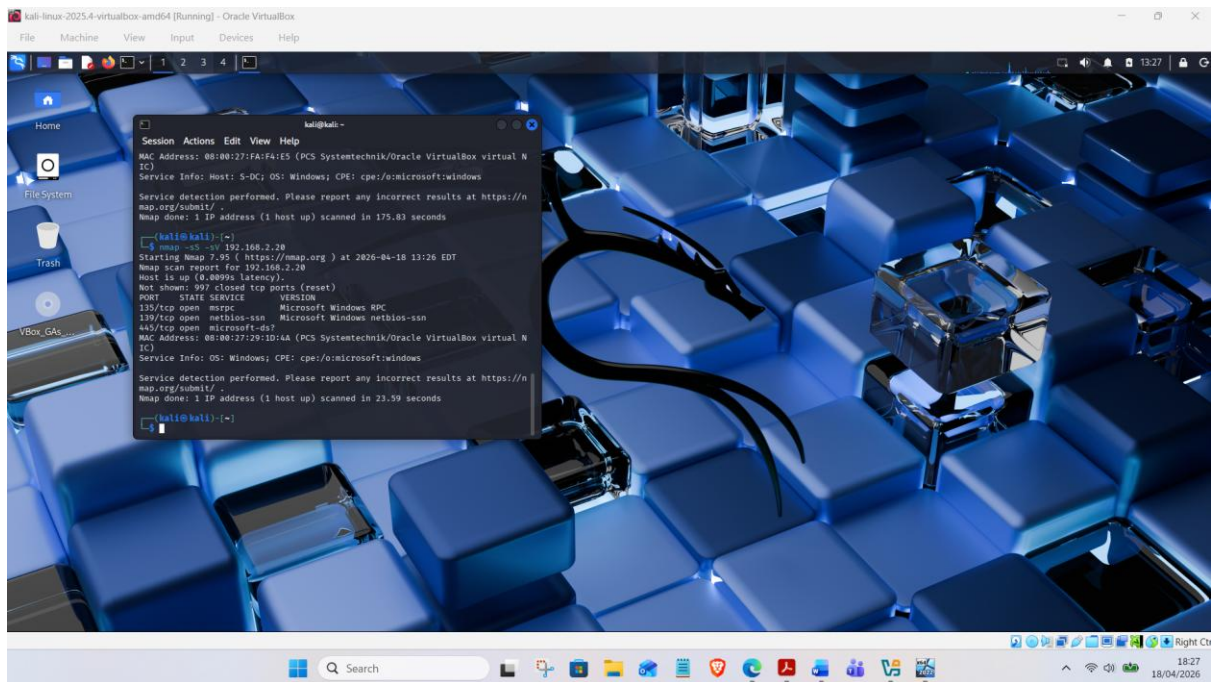


Figure 13: Nmap scan of Swansea Client (192.168.2.20) showing open ports and running services

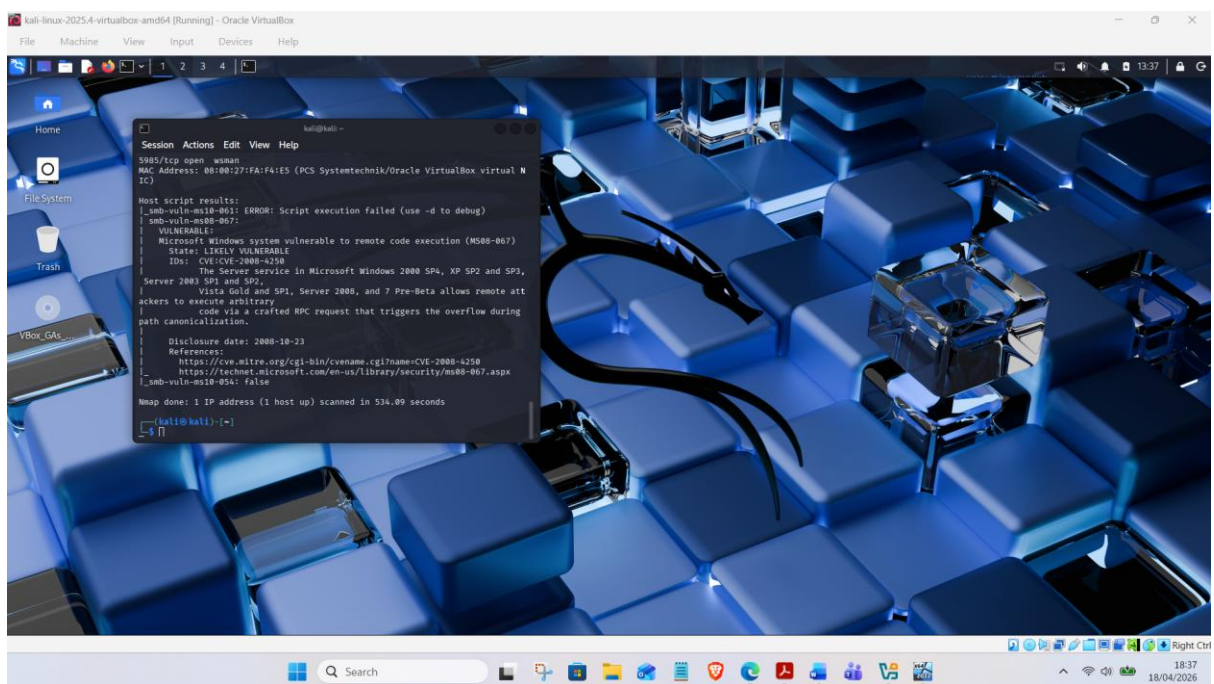


Figure 14: Vulnerability scan results showing MS08-067 remote code execution vulnerability (CVE-2008-4250) on Swansea Server

Task 3 – Exploitation

An exploitation attempt was conducted against the target system (192.168.2.10) using the Metasploit Framework. Based on the results of the Nmap scan, port 445 (SMB) was identified as open, indicating a potential attack vector. The EternalBlue exploit (MS17-010), a well-known vulnerability affecting Windows systems, was selected for the attack.

The exploit module `exploit/windows/smb/ms17_010_eternalblue` was configured with the target IP address and the attacker's machine IP. The attack was then launched using the Metasploit Framework.

However, the result of the exploitation attempt indicated that the target system was not vulnerable to the EternalBlue exploit. The system responded with a message stating that no session was created, suggesting that the vulnerability has likely been patched or mitigated.

3.1 Post-Exploitation

Since the exploitation attempt was unsuccessful, no post-exploitation activities could be performed. No shell access or remote control over the target system was obtained.

This outcome demonstrates that the target system has appropriate security measures in place, such as patching known vulnerabilities. Despite the unsuccessful attempt, the process highlights the importance of identifying vulnerabilities and attempting controlled exploitation in a secure environment.

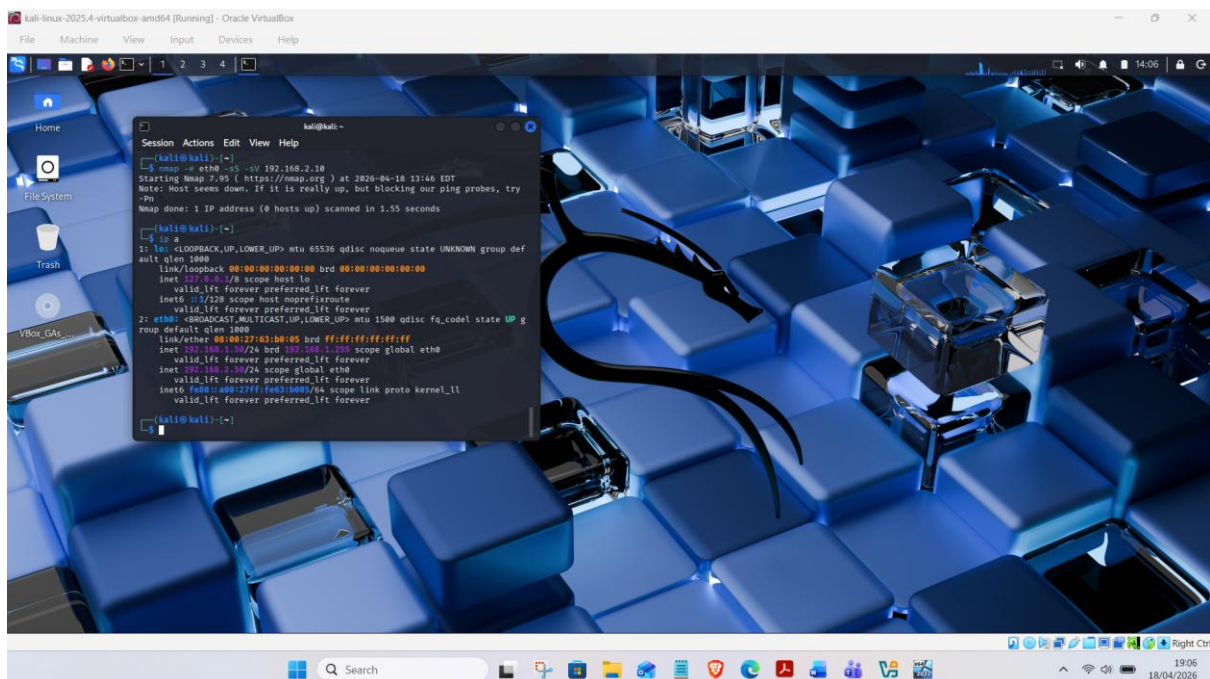


Figure 15 – Kali Linux IP Configuration

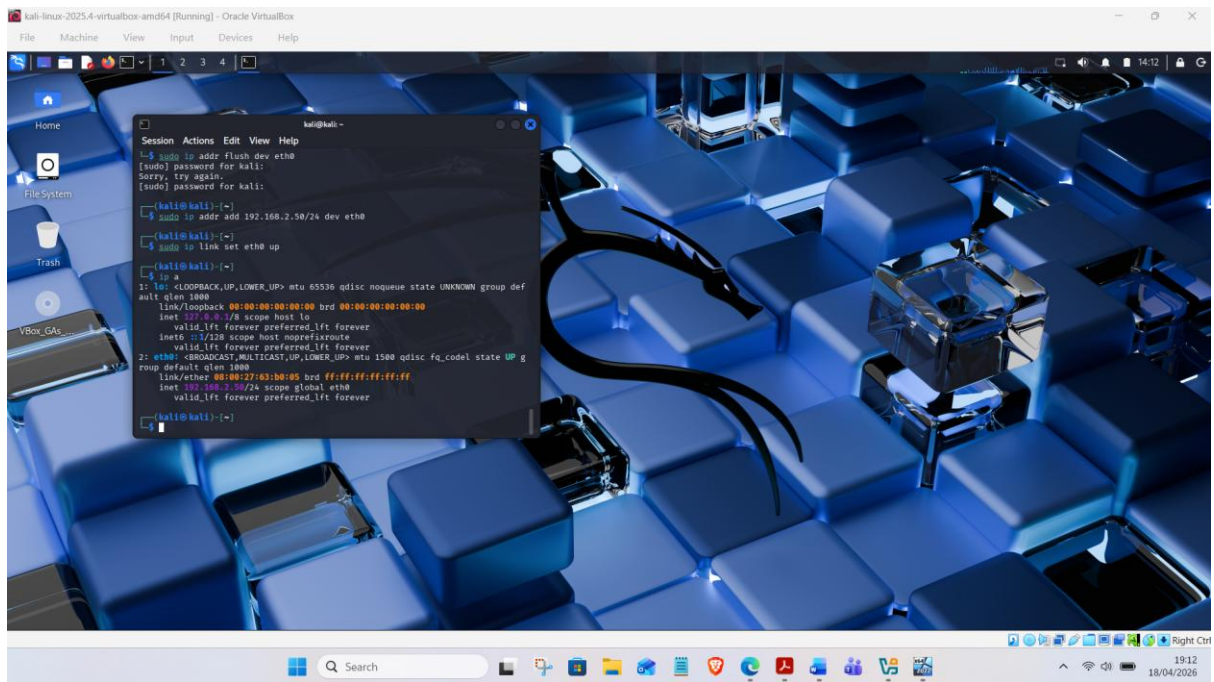


Figure 16 – Kali Network Reconfiguration to Target Network

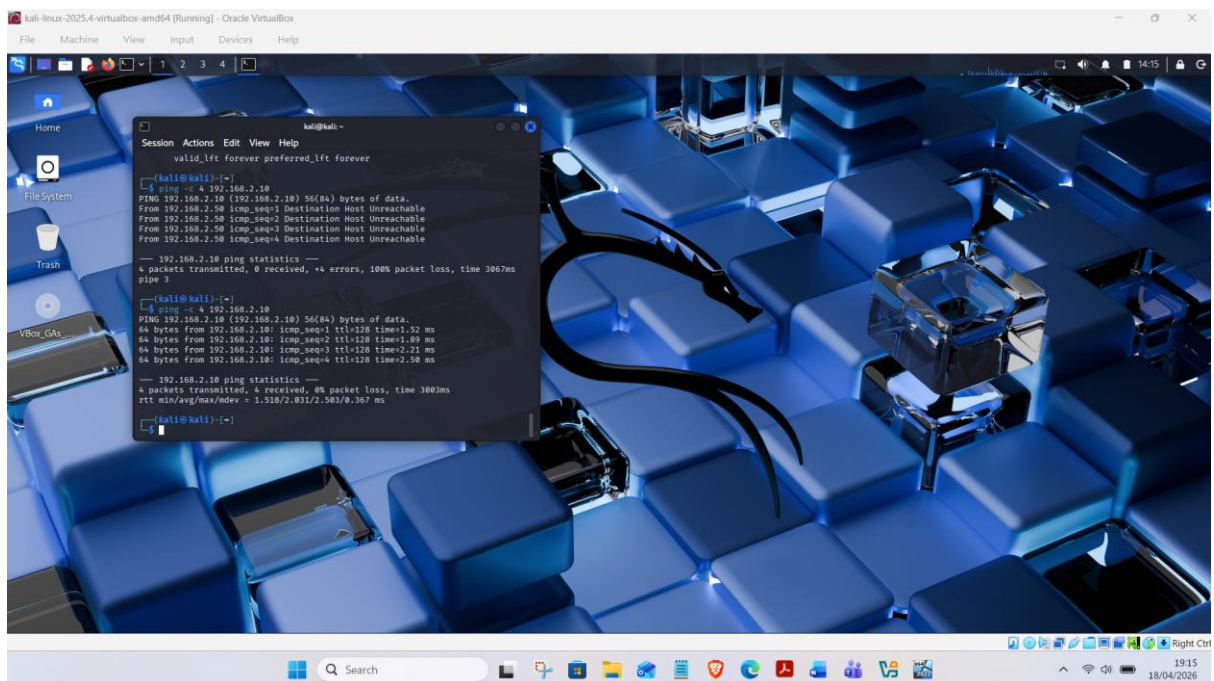


Figure 17 – Successful Connectivity to Target Machine (Ping Test)

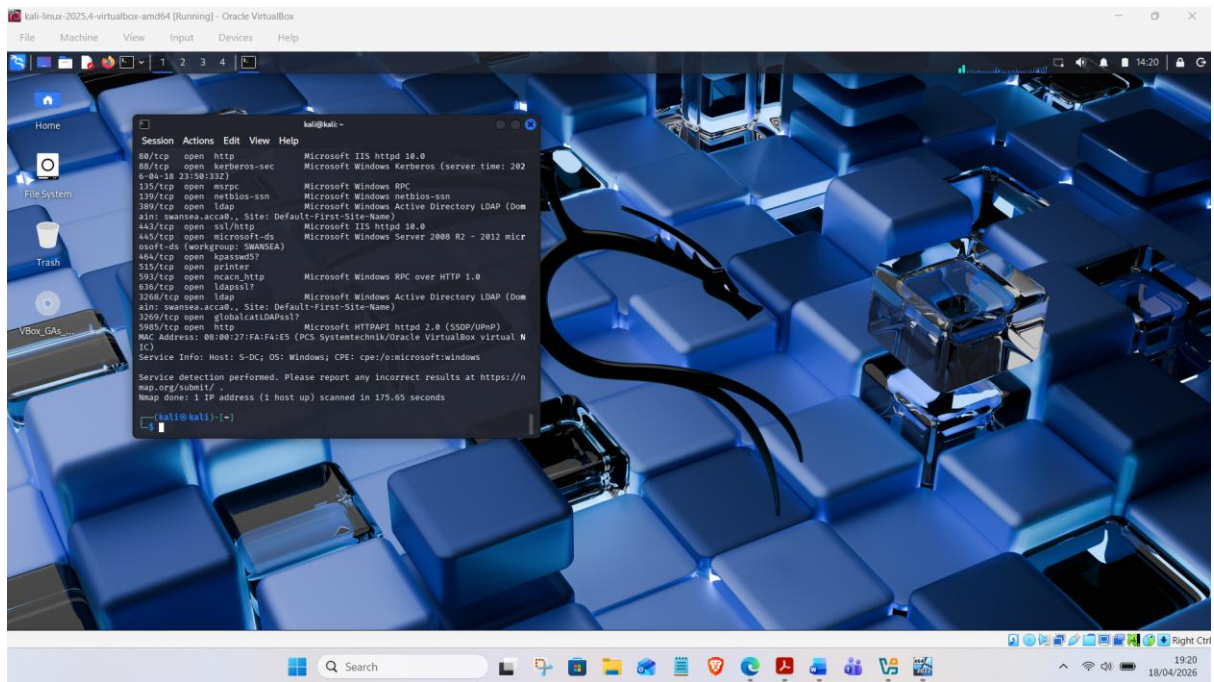


Figure 18 – Nmap Scan Results Identifying Open Ports and Services

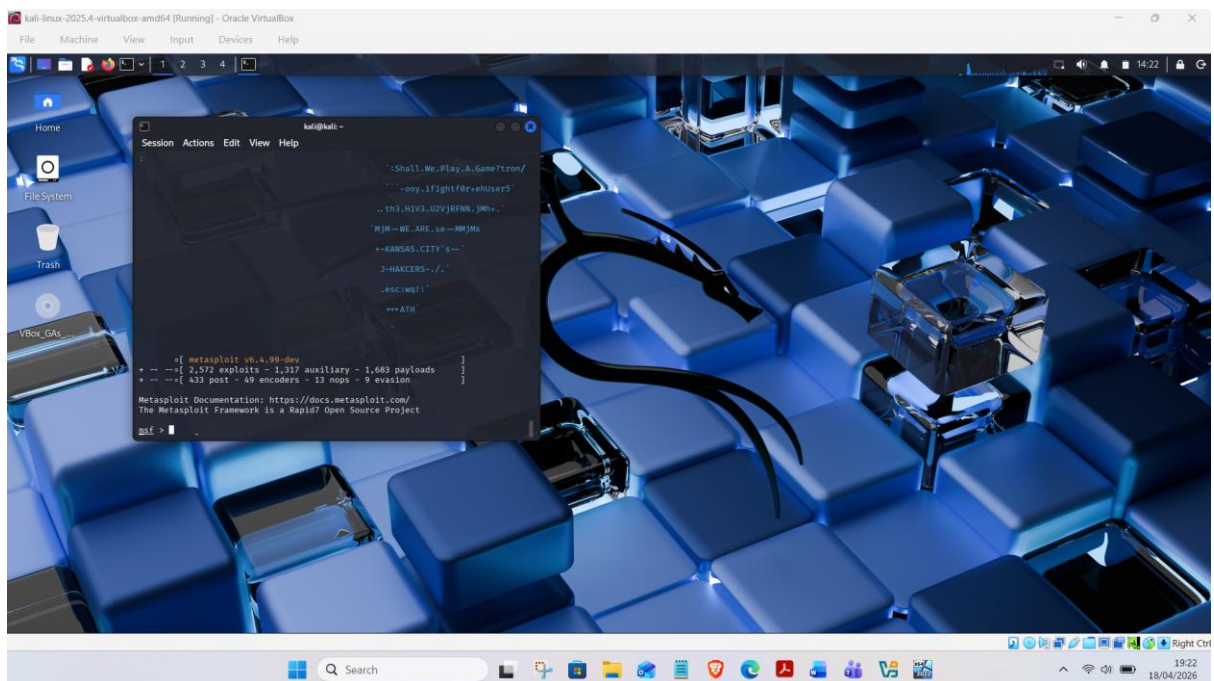


Figure 19 – Metasploit Framework Initialization

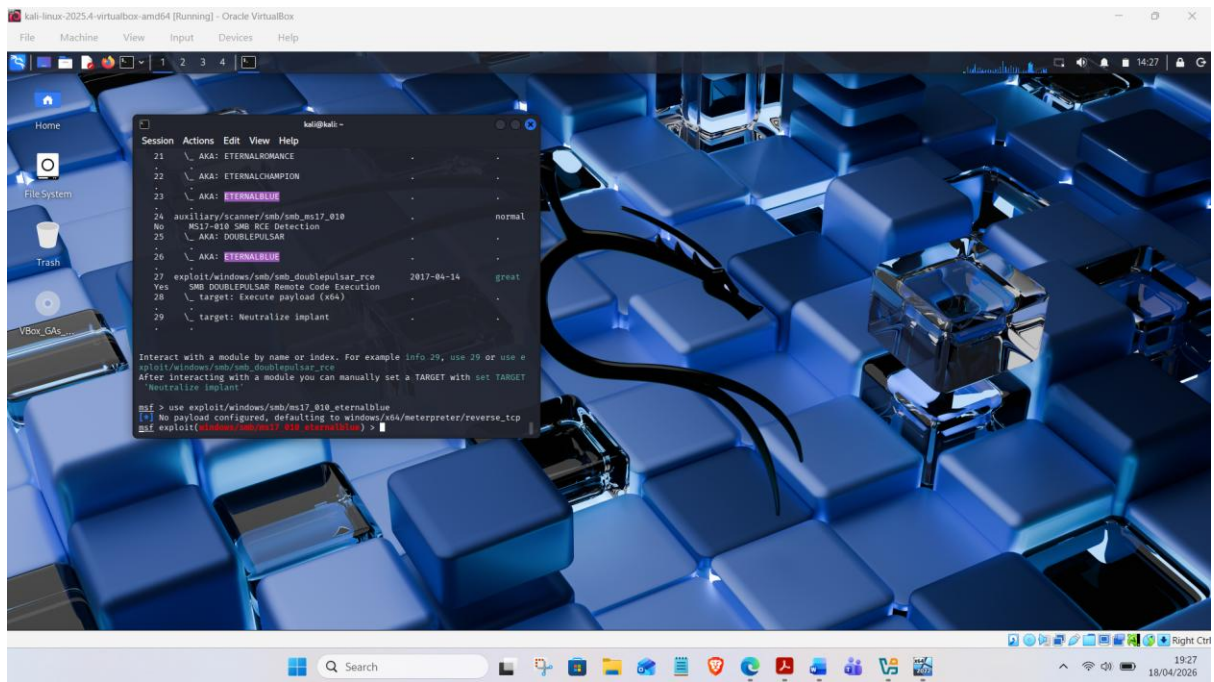


Figure 20 – EternalBlue Exploit Module Selected

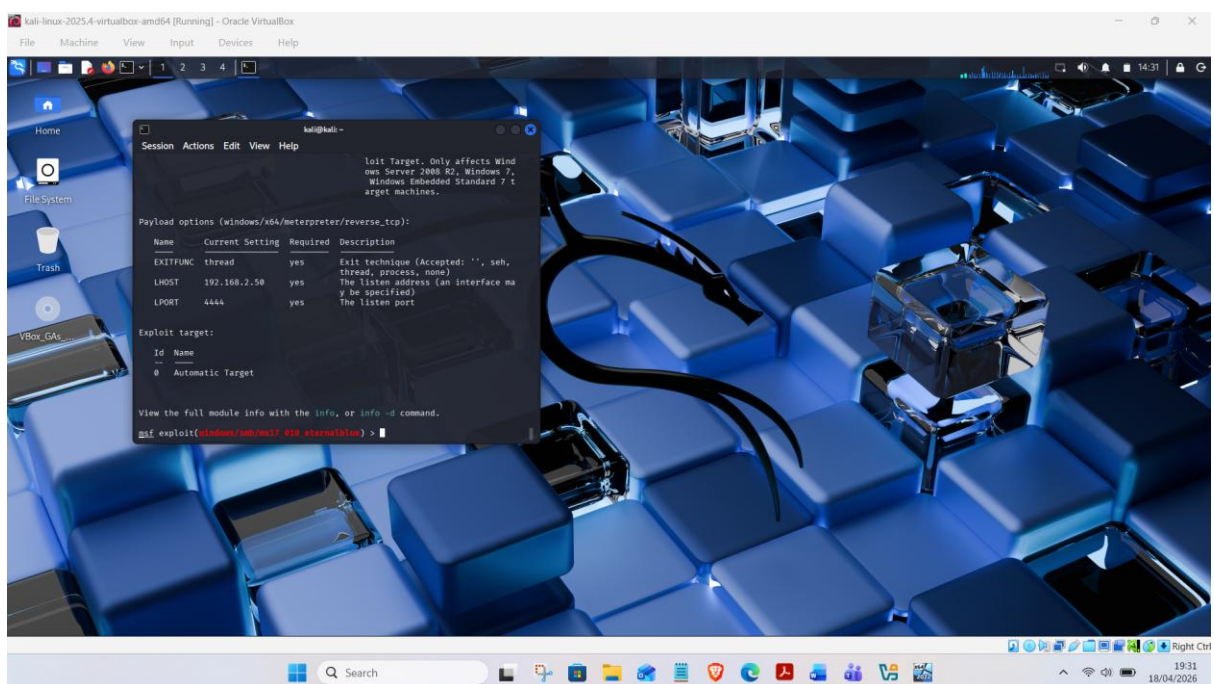


Figure 21 – Exploit Configured with Correct Target and Local Host

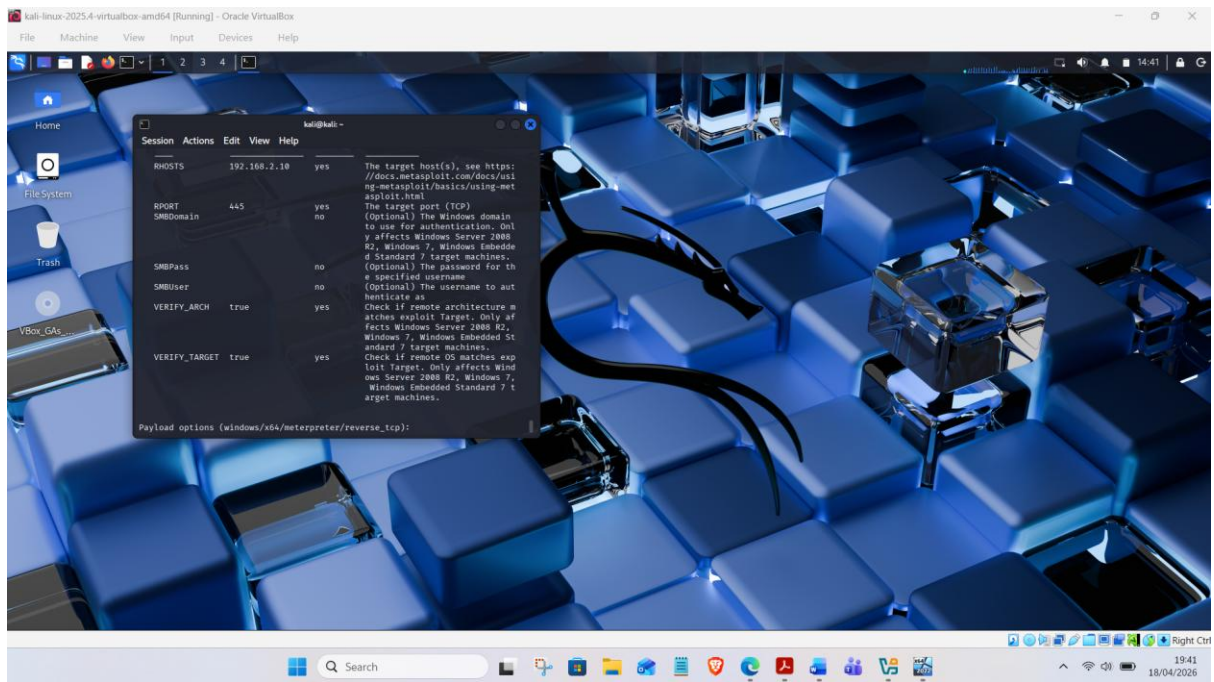


Figure 22 – Full Exploit Configuration Including Target (RHOSTS) and Attacker (LHOST)

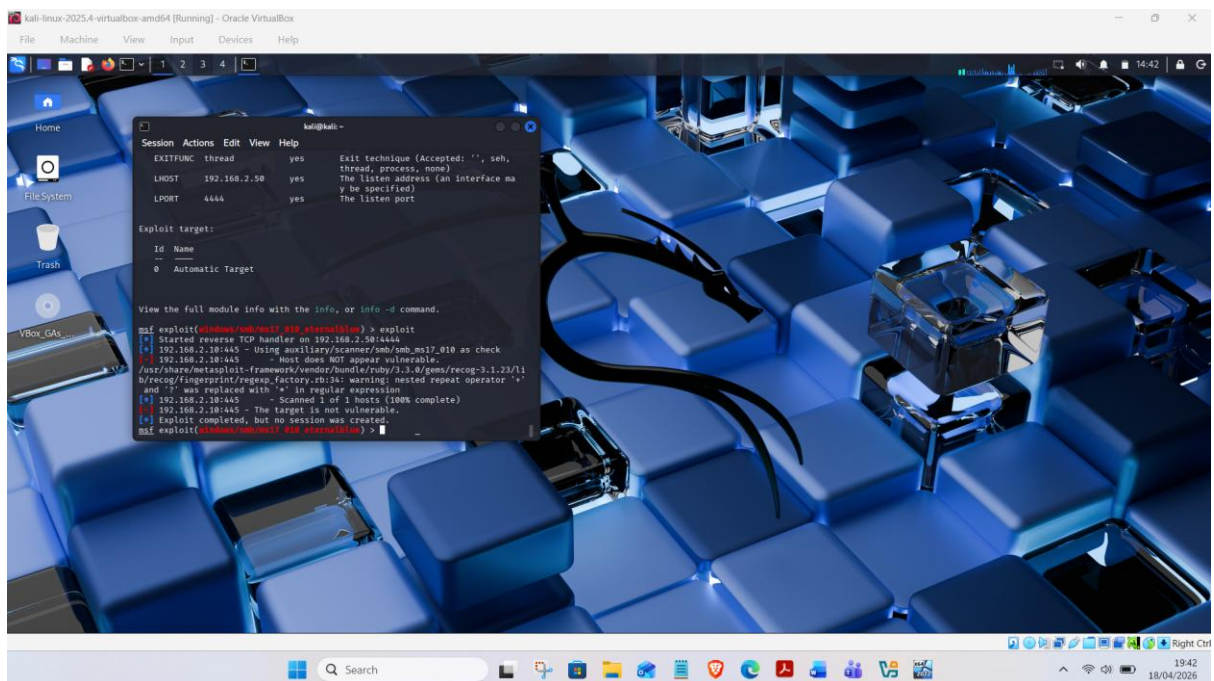


Figure 23 – Exploitation Attempt Result Showing Target Not Vulnerable

Task 4 – Security Measures

Based on the findings from the assessment, several security measures are recommended to enhance the protection of the network:

Systems should be regularly updated and patched to prevent exploitation of known vulnerabilities such as EternalBlue (MS17-010).

Firewalls should be configured to restrict access to critical ports, particularly port 445 (SMB), which is commonly targeted in attacks.

Access Control Lists (ACLs) should be implemented to ensure that only authorized users can access sensitive services.

Strong authentication mechanisms, including complex passwords and account lockout policies, should be enforced to prevent brute-force attacks.

Encryption protocols such as VPN and TLS should be used to protect data in transit across the network.

Continuous monitoring using tools such as Wireshark or intrusion detection systems should be implemented to identify suspicious network activity.

References:

1. [Microsoft Security Bulletin MS17-010 - Critical | Microsoft Learn](#)
2. [MS17-010: Security update for Windows SMB Server: March 14, 2017 - Microsoft Support](#)
3. [Service and Version Detection | Nmap Network Scanning](#)
4. [EternalBlue: Metasploit Module for MS17-010 | Rapid7 Blog](#)
5. [Rapid7 Vulnerability Database](#)
6. [Page Not Found | CSRC](#)