



COMPUTER NETWORK AND CYBER SECURITY

Advanced Cyber Security



Student Name: Gintota Vidanalage Samanthi Silve

Student Id: 2312700

Module Name: ACCB6000

Lecturer Name: Dr Mohammed Graham

Submission Date: 14 December 2025

Table of Contents

Task 1	3
Task 2	7
Setup of Security-Focused Operating System (Kali Linux)	7
Ping L-DC fromKali	8
Ping Client from Kali	8
Ping s-dc from Kali	9
Ping Linux Davian from Kali	9
Nmap scan	10
This screenshot provides evidence of an Nmap scan performed from Kali Linux ..	10
against the S-DC server to identify open ports and running services as part.....	10
of the vulnerability assessment. [2]	10
Blue Team perspective	11
Restricted Connectivity from Kali Linux.....	13
Task 3.	16
Task 3. Post-Exploitation (Unsuccessful Case)	17
Post-exploitation activities were not performed as no unauthorised access was obtained during the exploitation phase. The exploitation attempts were restricted by several security controls, including host-based firewall rules, restricted SMB responses, and network segmentation. These barriers effectively prevented privilege escalation, persistence, and lateral movement within the SWANSEA.ACCA network. [6]	17
Not Able to find the Screenshot	17
Task 4 – Network Security Measures.....	17
Conclusion	18
References	18

1. Introduction

This report presents a cybersecurity assessment of the SWANSEA.ACCA organisational network, operating across Swansea and London locations. The two sites are interconnected through a persistent site-to-site VPN, enabling secure communication between network resources.

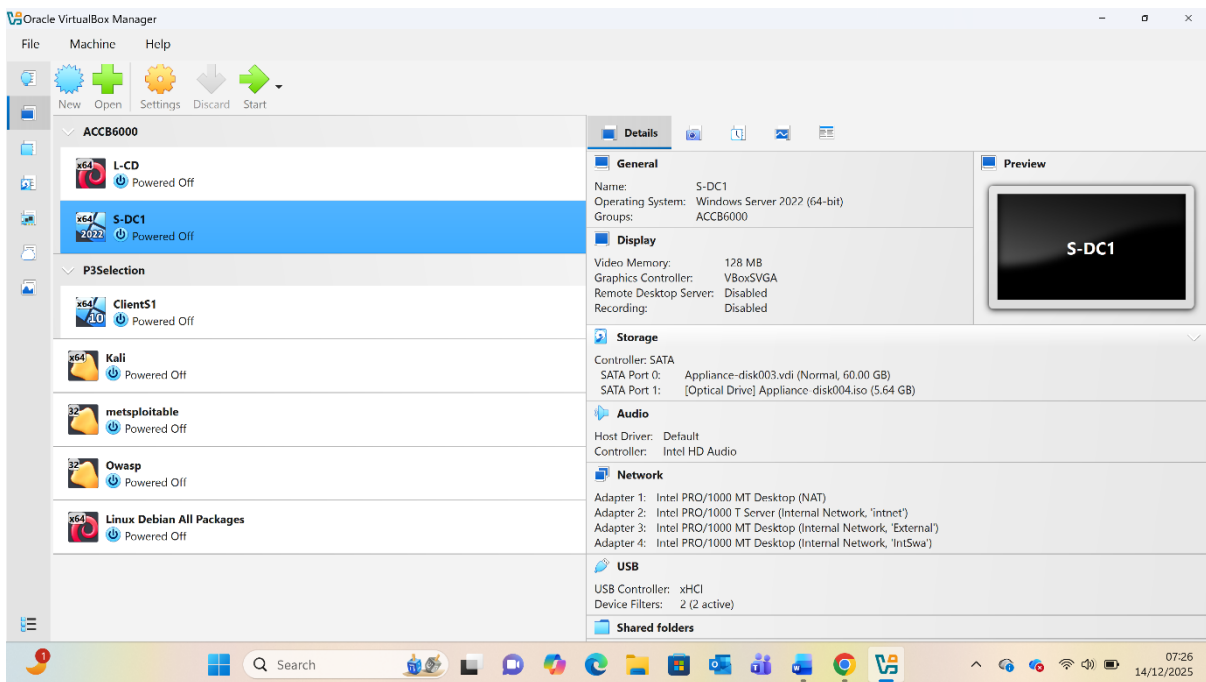
The purpose of this assessment is to examine the network's security posture by verifying connectivity, identifying weaknesses, and assessing exposure to potential threats using accepted cybersecurity practices. The evaluation follows a structured methodology informed by recognised standards, ensuring consistency and reliability in the assessment process.

The assessment environment comprises a Windows Server 2022 Domain Controller (S-DC), a Debian-based domain member server (L-CD), Windows and Linux client machines, and a Kali Linux system used to support internal security testing activities.

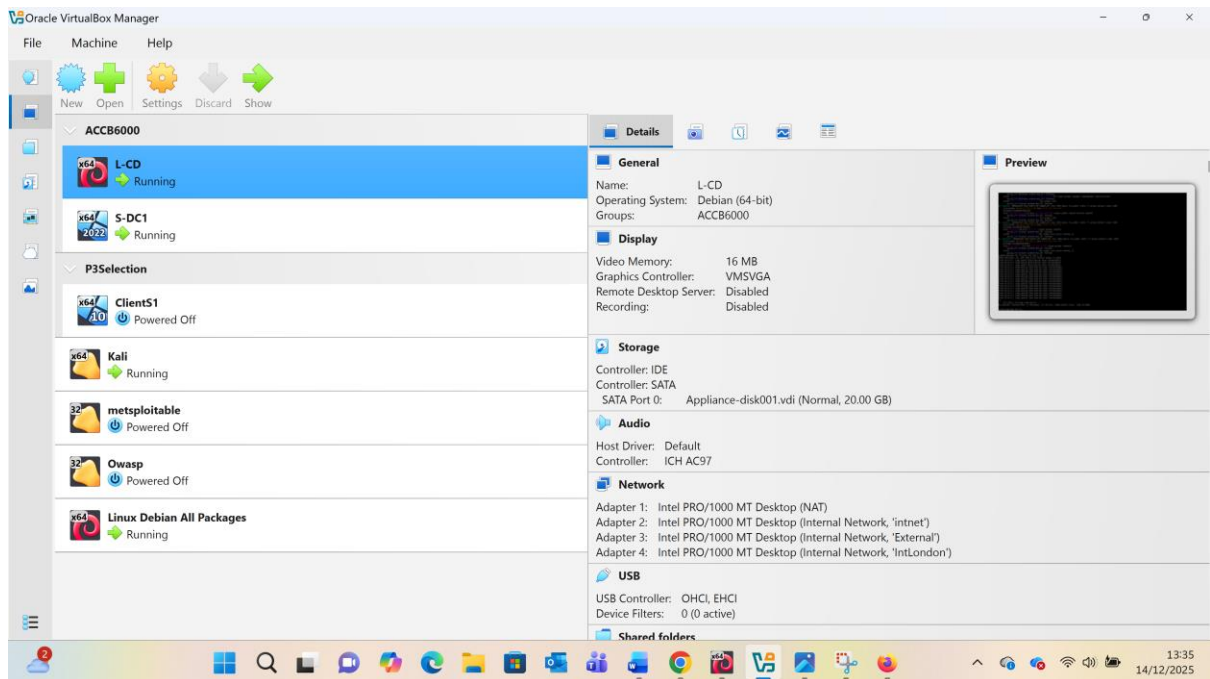
This report documents the testing performed, results observed, and evidence collected, providing a professional overview of network validation and security assessment outcomes. Screenshots are included to support the findings presented.

Task 1 – Network Testing

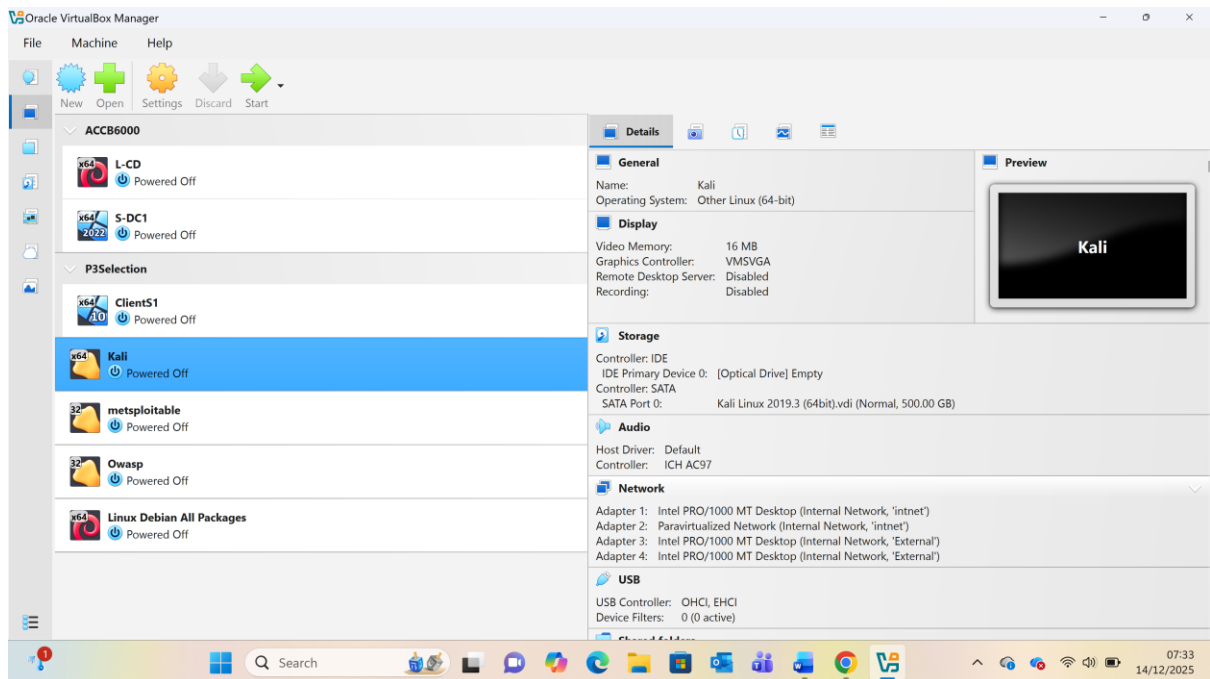
S-CD Network Setting



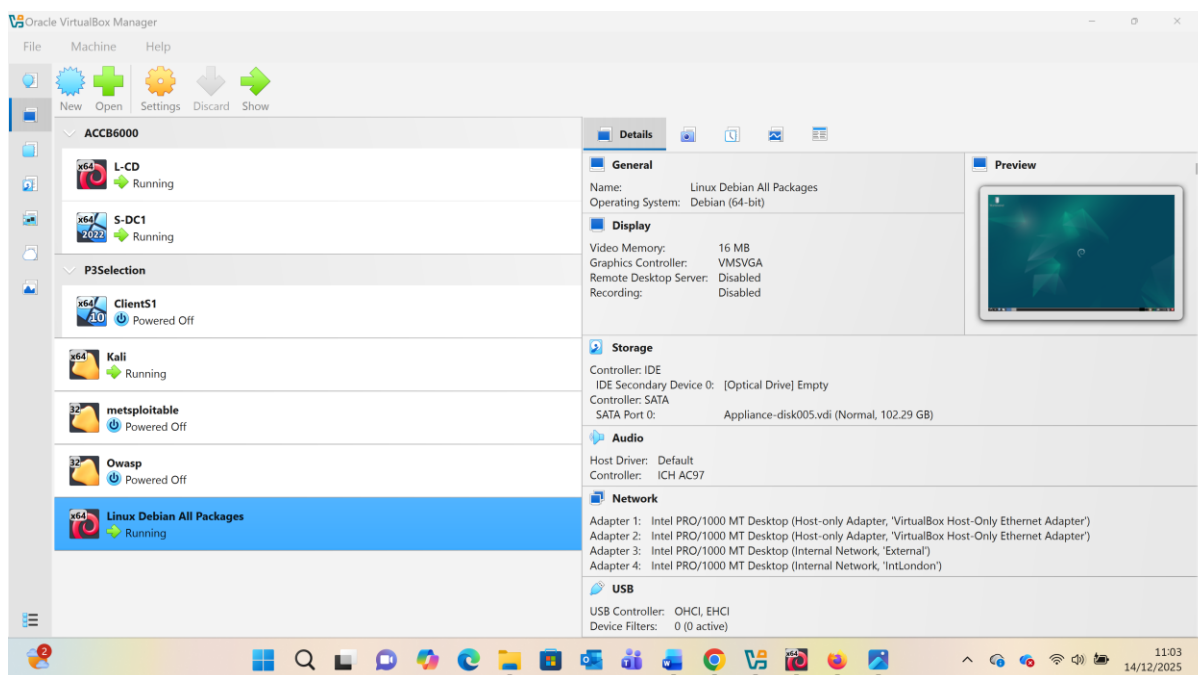
L-DC Network Setting



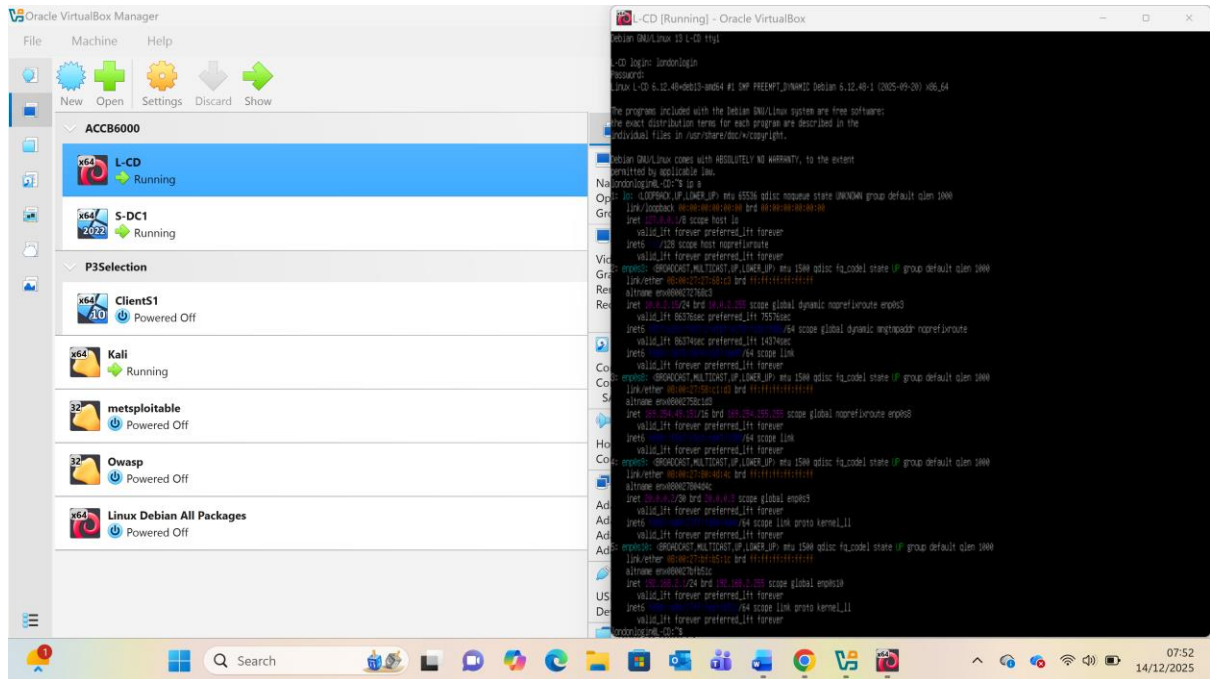
Kali Network Setting



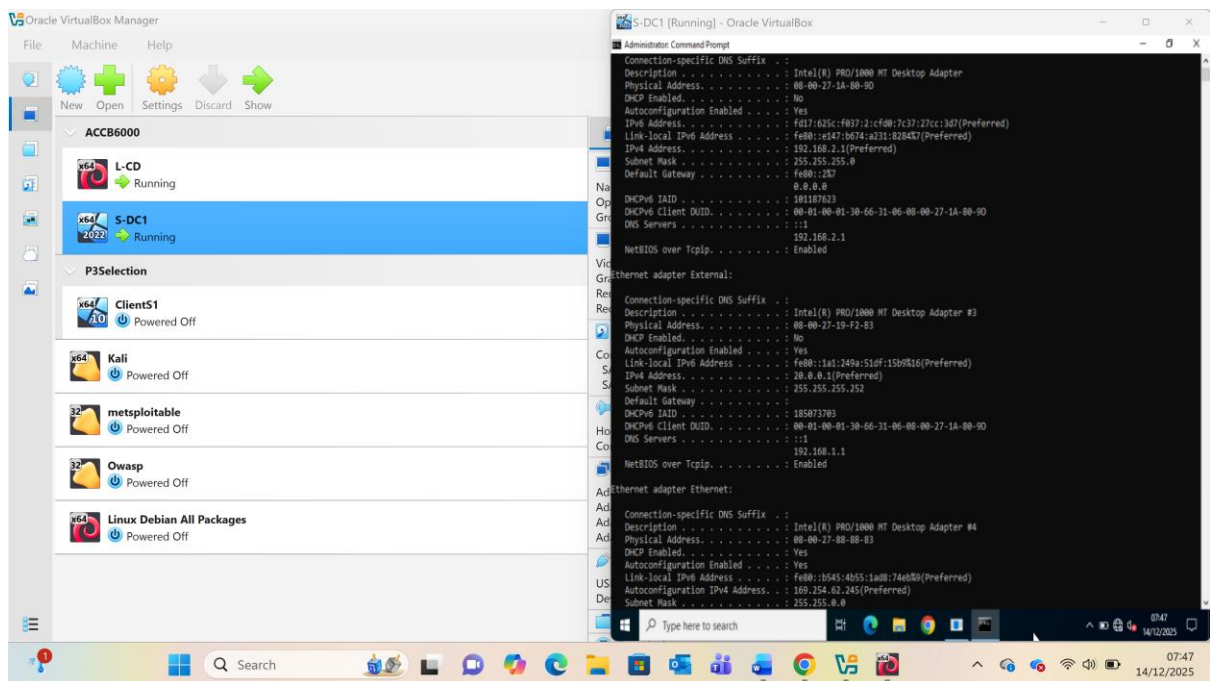
Linux Dabian Network Setting



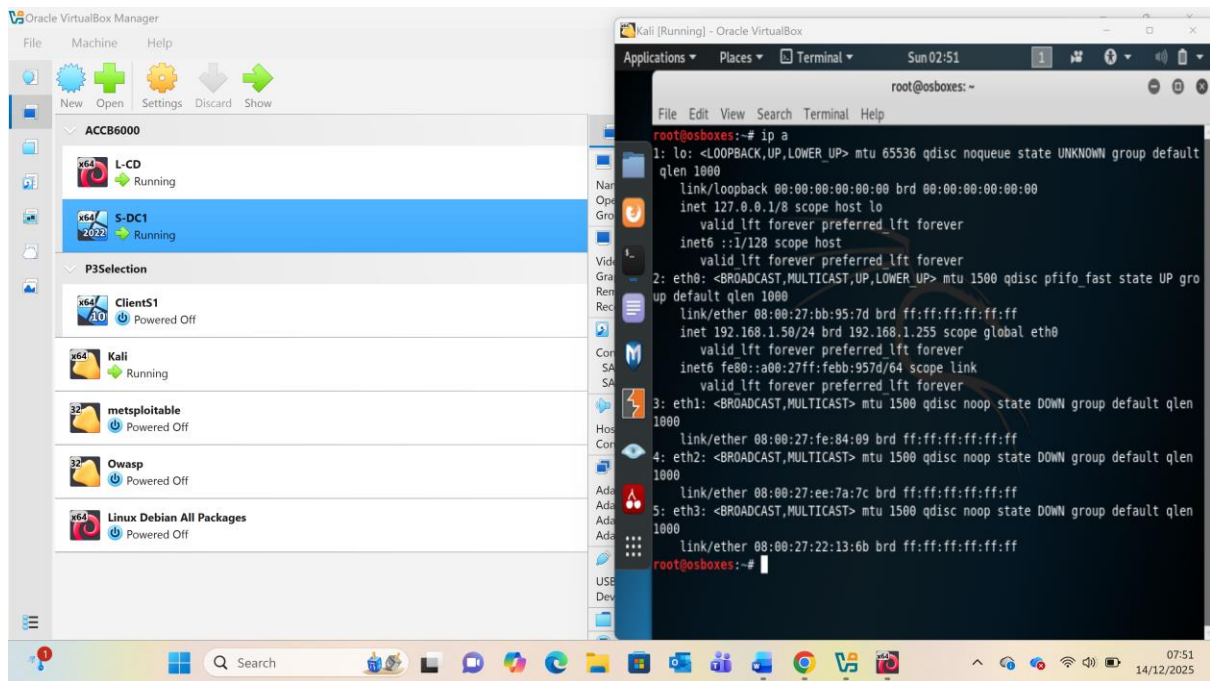
L-CD IP Configuration



S-DC IP Configuration

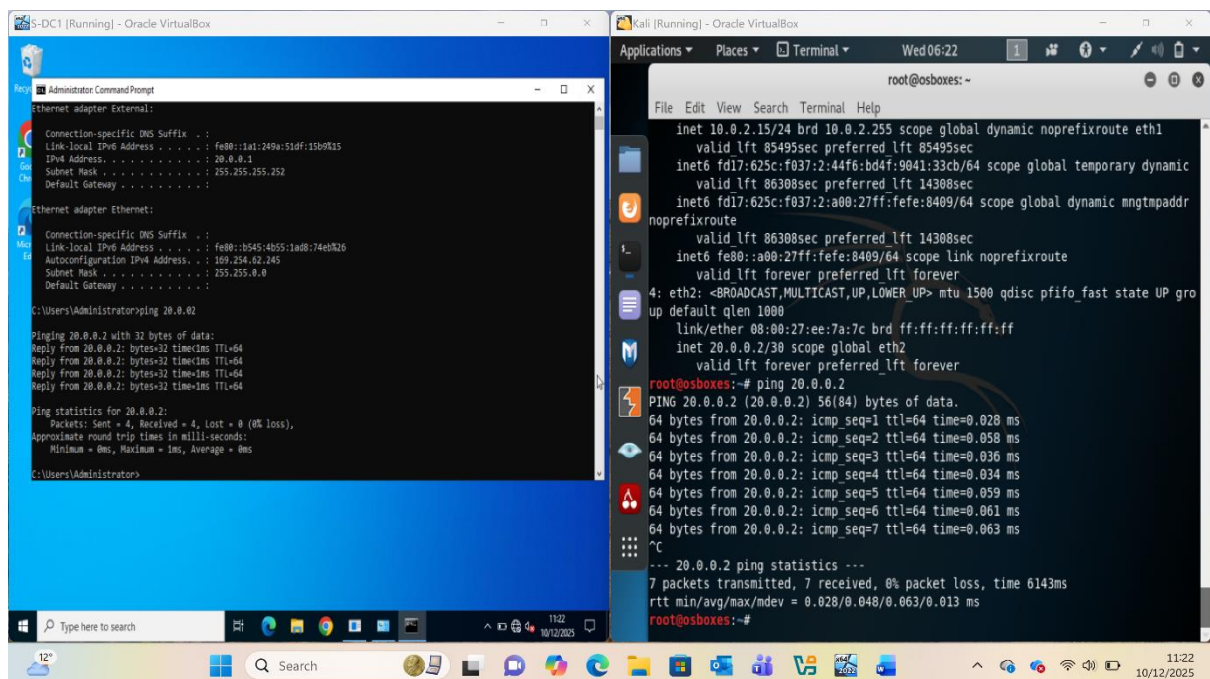


Kali IP Configuration



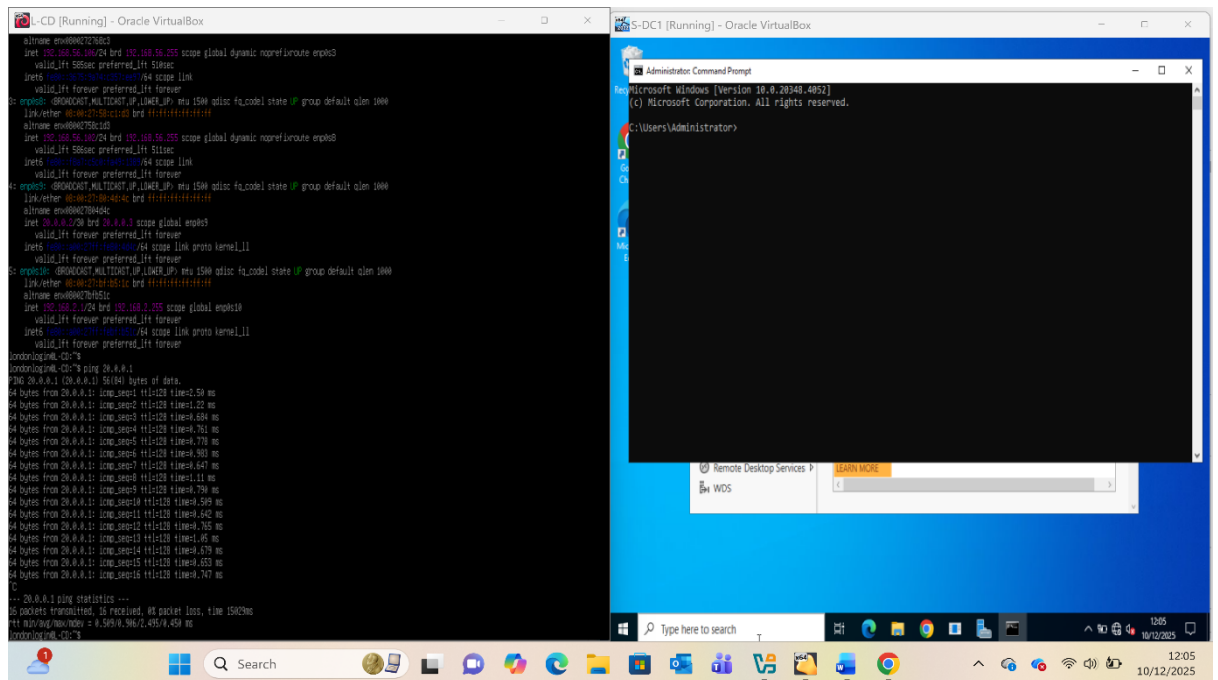
Network Connectivity Verification

This screenshot shows the network configuration and connectivity verification performed on the Swansea Domain Controller (S-DC).



This screenshot shows network connectivity verification performed from the London Domain member server (L-CD). A successful ping test to the

internal host **20.0.0.1** confirms that the L-CD system is correctly configured and able to communicate within the internal network.



Task 2

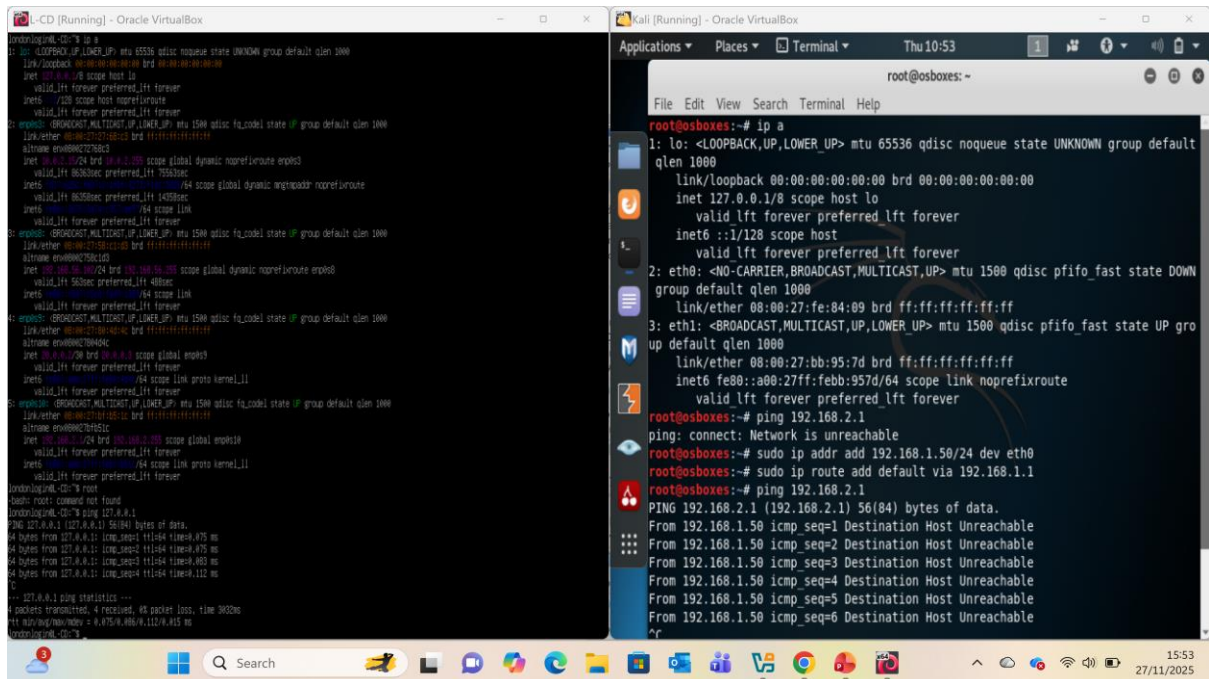
Setup of Security-Focused Operating System (Kali Linux)

A security-focused operating system, **Kali Linux**, was deployed to perform internal vulnerability assessment on the Swansea ACCA network. Kali Linux is widely used by security professionals due to its built-in penetration testing and network assessment tools.

The Kali Linux virtual machine was configured within Oracle VirtualBox and connected to the same **Internal Network (IntSwa)** as the target systems. A temporary static IP address was assigned to Kali Linux to allow communication with other devices in the network.

This setup simulates an internal attacker or security consultant with authorised access to the organisation’s internal network. [1]

Ping L-DC from Kali

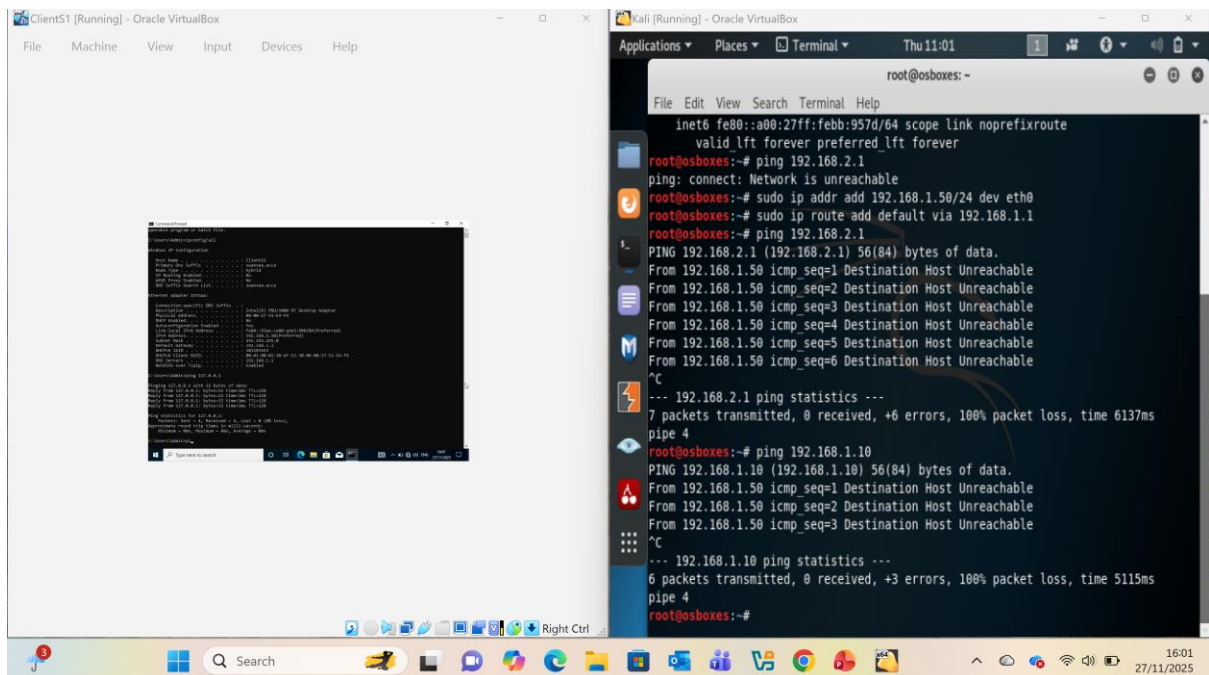


The image shows two side-by-side VirtualBox windows. The left window, titled 'L-DC [Running] - Oracle VirtualBox', displays the output of the 'ifconfig' command for the 'lo' interface. It shows the IP address 127.0.0.1, a netmask of 255.0.0.0, and a broadcast address of 127.0.0.1. The right window, titled 'Kali [Running] - Oracle VirtualBox', shows the output of the 'ip a' command for the 'lo' interface, displaying the same IP address and netmask. Below the 'ip a' output, the terminal shows the execution of 'ping 192.168.2.1', which results in 'ping: connect: Network is unreachable'.

```
root@kali:~# 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
        valid_lft forever preferred_lft forever

root@kali:~# ping 192.168.2.1
ping: connect: Network is unreachable
```

Ping Client from Kali

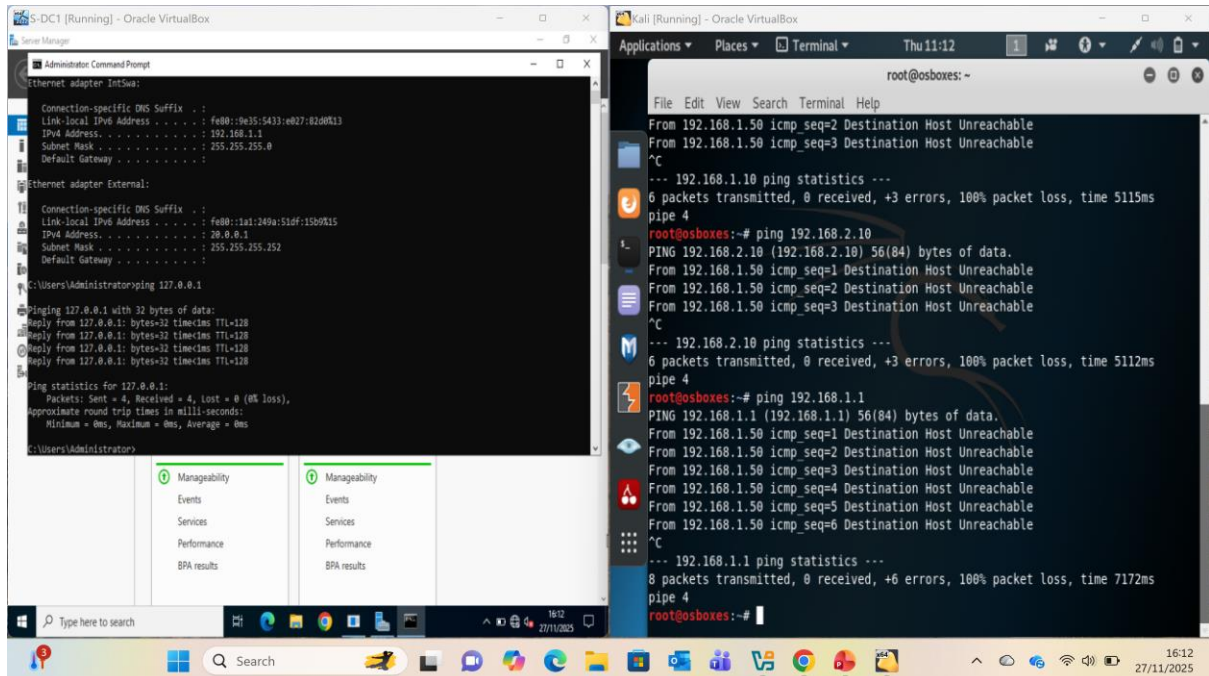


The image shows two side-by-side VirtualBox windows. The left window, titled 'ClientS1 [Running] - Oracle VirtualBox', displays the output of the 'ifconfig' command for the 'lo' interface. It shows the IP address 127.0.0.1, a netmask of 255.0.0.0, and a broadcast address of 127.0.0.1. The right window, titled 'Kali [Running] - Oracle VirtualBox', shows the output of the 'ip a' command for the 'lo' interface, displaying the same IP address and netmask. Below the 'ip a' output, the terminal shows the execution of 'ping 192.168.2.1', which results in 'ping: connect: Network is unreachable'.

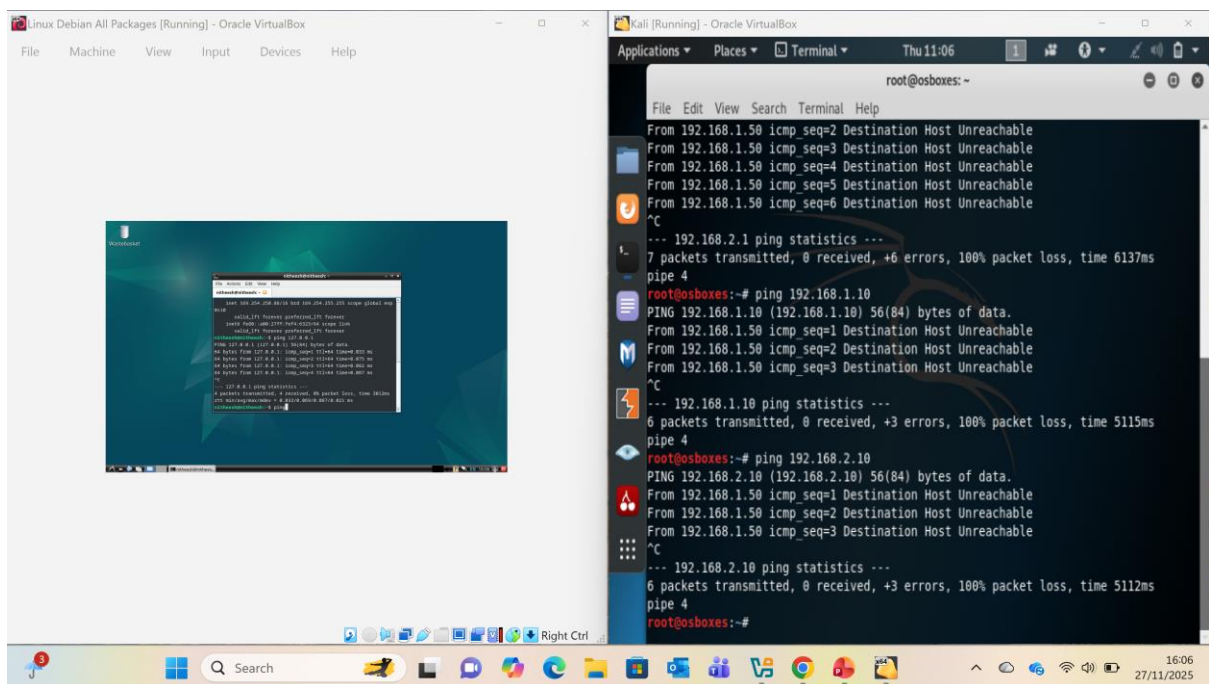
```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever

root@kali:~# ping 192.168.2.1
ping: connect: Network is unreachable
```

Ping s-dc from Kali

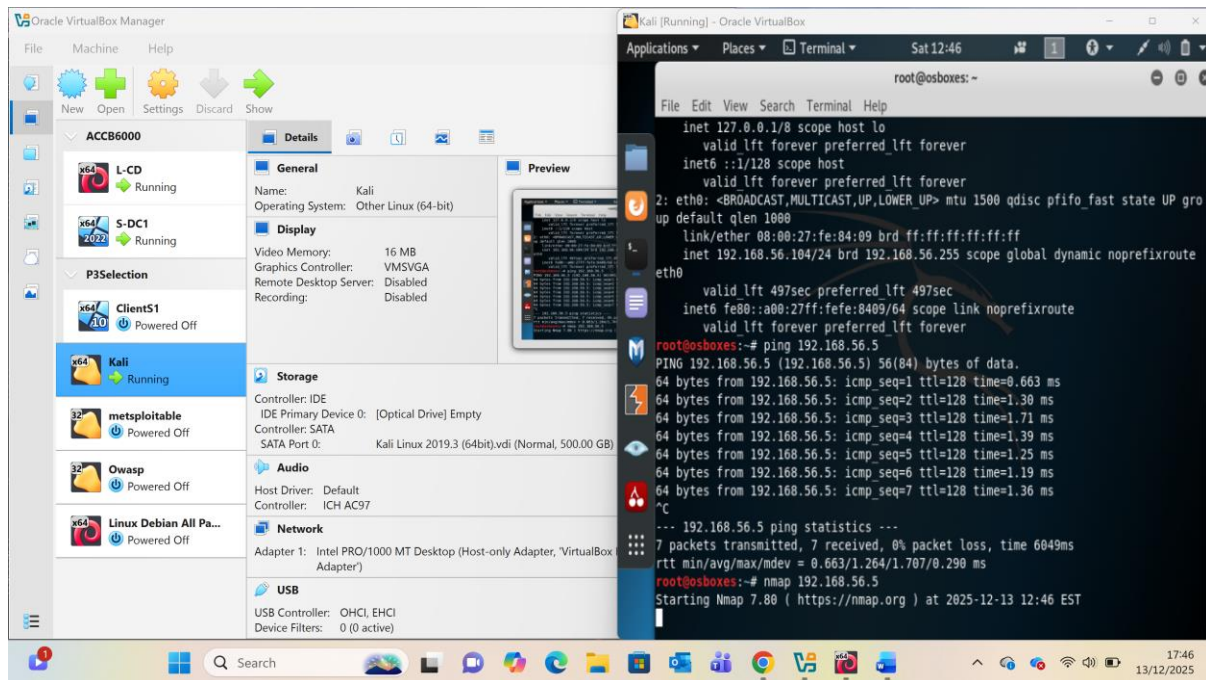


Ping Linux Davian from Kali

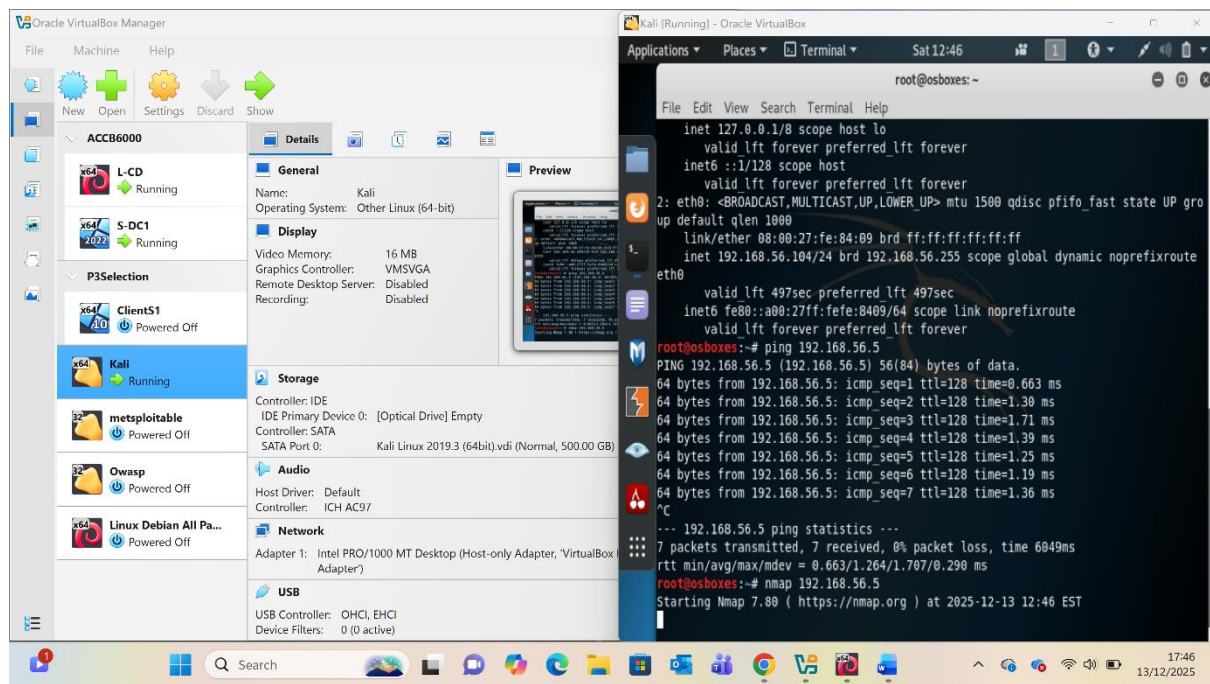


Nmap scan

This screenshot provides evidence of an Nmap scan performed from Kali Linux against the S-DC server to identify open ports and running services as part of the vulnerability assessment. [2]



Kali Linux was configured as a security-focused operating system within the Swansea network. Connectivity was verified by successfully pinging the S-DC server, followed by an Nmap scan to identify open ports and running services. [1]

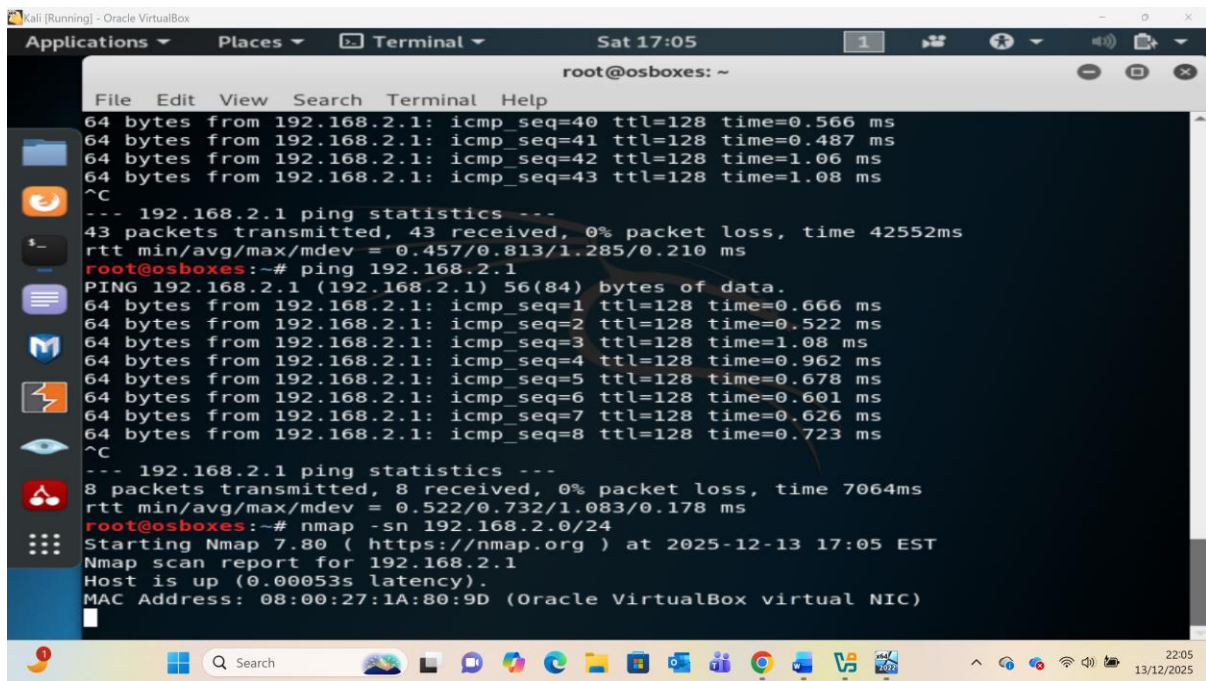


Blue Team perspective

From a Blue Team perspective, the S-DC network configuration was reviewed using the `ipconfig /all` command to understand exposed interfaces and

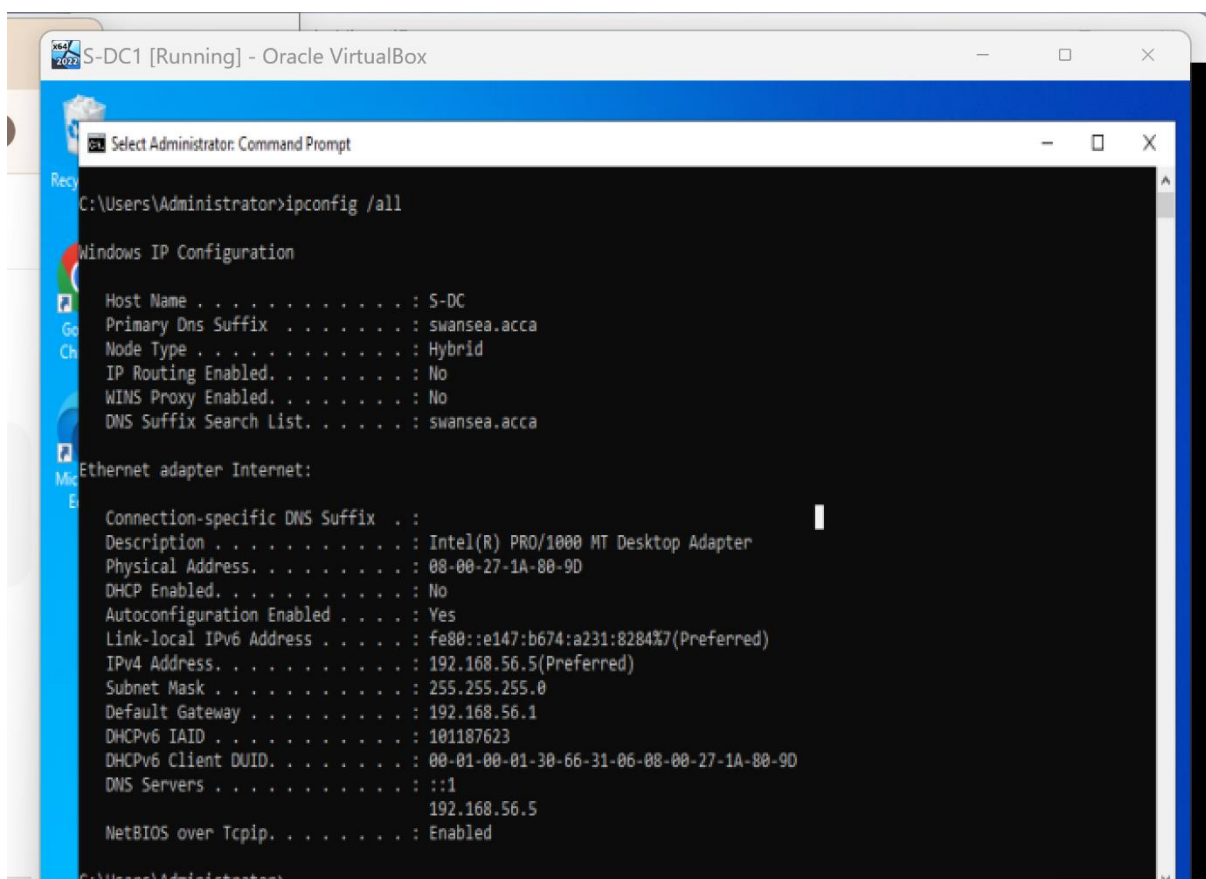
services. This helps establish a baseline and ensures that only necessary services are accessible, reducing the overall attack surface. [3]

This screenshot shows successful connectivity testing and Nmap host discovery performed from Kali Linux, confirming that the target host is reachable prior to vulnerability scanning. [4]



The screenshot shows a Kali Linux terminal window titled "Kali (Running) - Oracle VirtualBox". The terminal output displays the results of a ping command to 192.168.2.1, followed by a second ping command, and then an nmap scan. The nmap scan report indicates that the host is up and provides the MAC address 08:00:27:1A:80:9D.

```
root@osboxes: ~  
File Edit View Search Terminal Help  
64 bytes from 192.168.2.1: icmp_seq=40 ttl=128 time=0.566 ms  
64 bytes from 192.168.2.1: icmp_seq=41 ttl=128 time=0.487 ms  
64 bytes from 192.168.2.1: icmp_seq=42 ttl=128 time=1.06 ms  
64 bytes from 192.168.2.1: icmp_seq=43 ttl=128 time=1.08 ms  
^C  
--- 192.168.2.1 ping statistics ---  
43 packets transmitted, 43 received, 0% packet loss, time 42552ms  
rtt min/avg/max/mdev = 0.457/0.813/1.285/0.210 ms  
root@osboxes:~# ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=128 time=0.666 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=128 time=0.522 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=128 time=1.08 ms  
64 bytes from 192.168.2.1: icmp_seq=4 ttl=128 time=0.962 ms  
64 bytes from 192.168.2.1: icmp_seq=5 ttl=128 time=0.678 ms  
64 bytes from 192.168.2.1: icmp_seq=6 ttl=128 time=0.601 ms  
64 bytes from 192.168.2.1: icmp_seq=7 ttl=128 time=0.626 ms  
64 bytes from 192.168.2.1: icmp_seq=8 ttl=128 time=0.723 ms  
^C  
--- 192.168.2.1 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7064ms  
rtt min/avg/max/mdev = 0.522/0.732/1.083/0.178 ms  
root@osboxes:~# nmap -sn 192.168.2.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-13 17:05 EST  
Nmap scan report for 192.168.2.1  
Host is up (0.00053s latency).  
MAC Address: 08:00:27:1A:80:9D (Oracle VirtualBox virtual NIC)
```

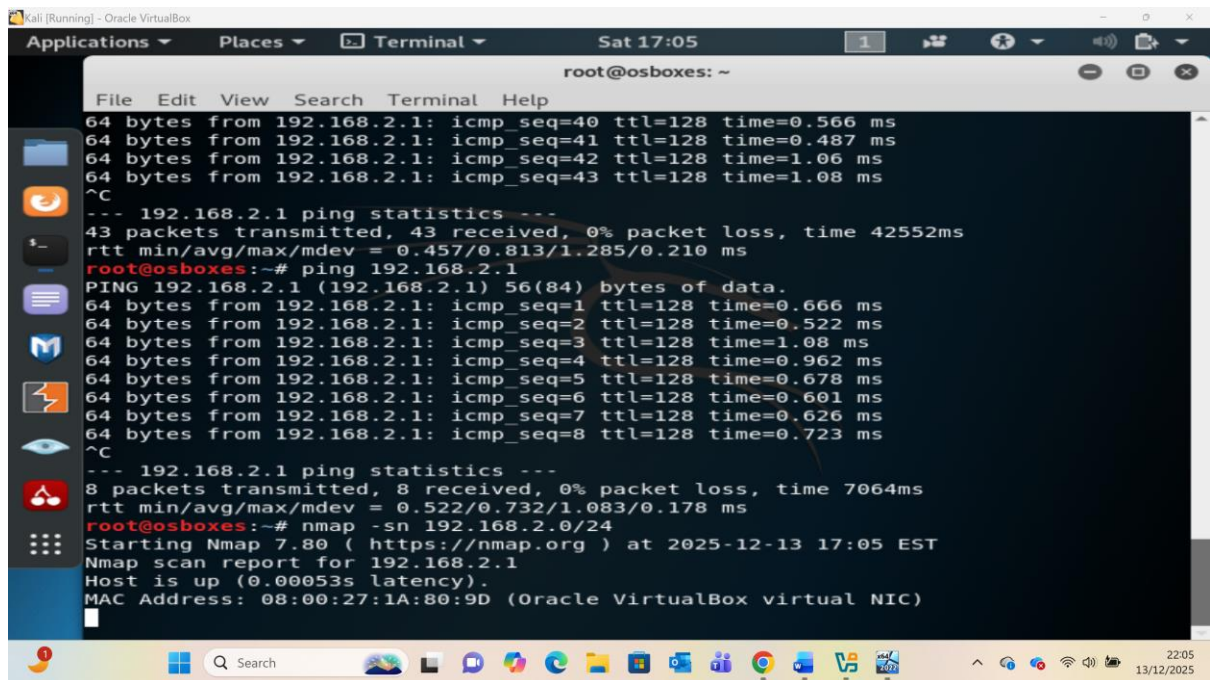


The screenshot shows a Windows Command Prompt window titled "S-DC1 [Running] - Oracle VirtualBox". The command prompt displays the output of the ipconfig /all command, showing the IP configuration for the S-DC1 host. The configuration includes the host name, primary DNS suffix, node type, IP routing, WINS proxy, DNS suffix search list, and the Ethernet adapter Internet configuration, including the physical address, DHCP settings, and IP address.

```
Microsoft Windows [Version 10.0.22000.1000] (c) Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>ipconfig /all  
  
Windows IP Configuration  
  
Host Name . . . . . : S-DC  
Primary Dns Suffix . . . . . : swansea.acca  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : swansea.acca  
  
Ethernet adapter Internet:  
  
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter  
Physical Address. . . . . : 08-00-27-1A-80-9D  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::e147:b674:a231:8284%7(Preferred)  
IPv4 Address. . . . . : 192.168.56.5(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.56.1  
DHCPv6 IAID . . . . . : 101187623  
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-66-31-06-08-00-27-1A-80-9D  
DNS Servers . . . . . : ::1  
192.168.56.5  
NetBIOS over Tcpip. . . . . : Enabled
```

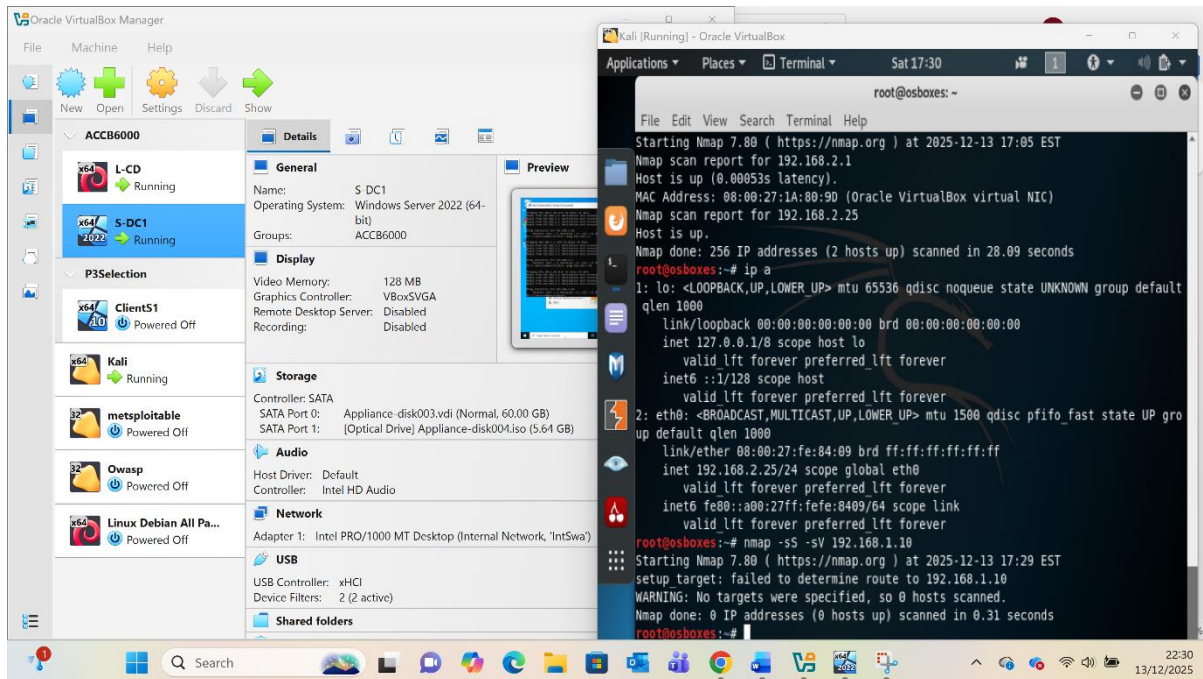
This screenshot shows successful ICMP connectivity testing and Nmap host discovery performed from Kali Linux, confirming that the target system is reachable prior to conducting vulnerability assessment scans. [5]

Restricted Connectivity from Kali Linux

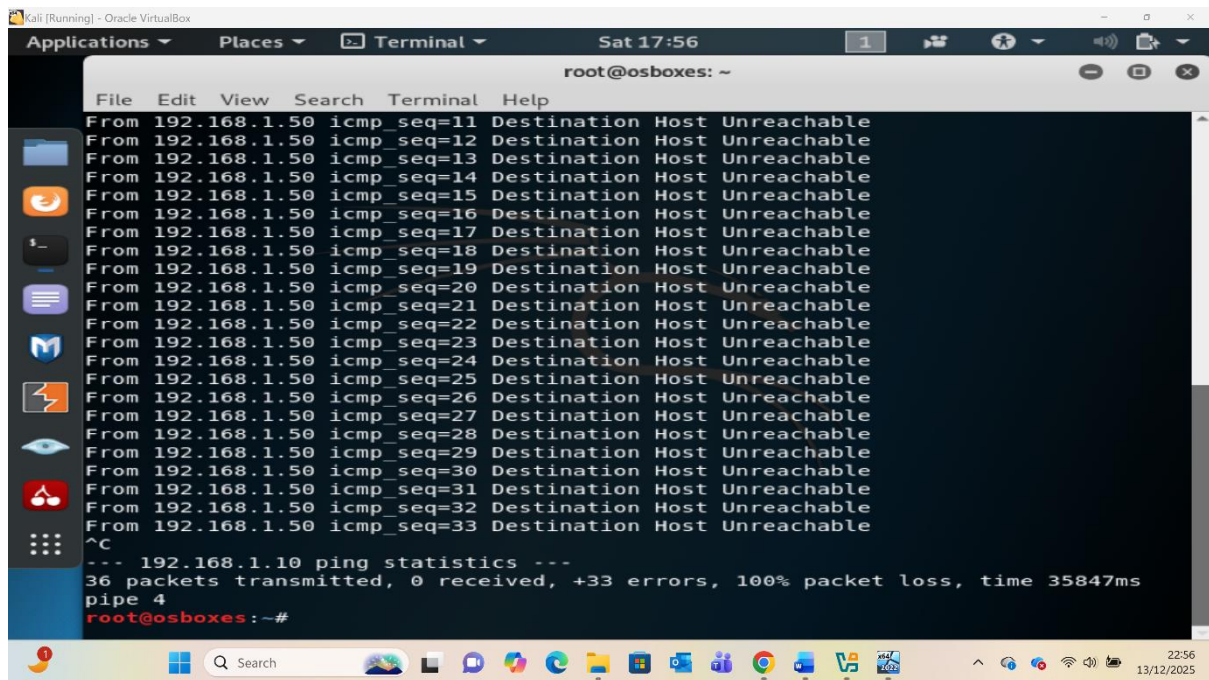


```
root@osboxes: ~  
File Edit View Search Terminal Help  
64 bytes from 192.168.2.1: icmp_seq=40 ttl=128 time=0.566 ms  
64 bytes from 192.168.2.1: icmp_seq=41 ttl=128 time=0.487 ms  
64 bytes from 192.168.2.1: icmp_seq=42 ttl=128 time=1.06 ms  
64 bytes from 192.168.2.1: icmp_seq=43 ttl=128 time=1.08 ms  
^C  
--- 192.168.2.1 ping statistics ---  
43 packets transmitted, 43 received, 0% packet loss, time 42552ms  
rtt min/avg/max/mdev = 0.457/0.813/1.285/0.210 ms  
root@osboxes:~# ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=128 time=0.666 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=128 time=0.522 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=128 time=1.08 ms  
64 bytes from 192.168.2.1: icmp_seq=4 ttl=128 time=0.962 ms  
64 bytes from 192.168.2.1: icmp_seq=5 ttl=128 time=0.678 ms  
64 bytes from 192.168.2.1: icmp_seq=6 ttl=128 time=0.601 ms  
64 bytes from 192.168.2.1: icmp_seq=7 ttl=128 time=0.626 ms  
64 bytes from 192.168.2.1: icmp_seq=8 ttl=128 time=0.723 ms  
^C  
--- 192.168.2.1 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7064ms  
rtt min/avg/max/mdev = 0.522/0.732/1.083/0.178 ms  
root@osboxes:~# nmap -sn 192.168.2.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-13 17:05 EST  
Nmap scan report for 192.168.2.1  
Host is up (0.00053s latency).  
MAC Address: 08:00:27:1A:80:9D (Oracle VirtualBox virtual NIC)
```

This screenshot shows Nmap host discovery scans performed from Kali Linux to identify active hosts within the network, along with verification of the Kali system's IP configuration prior to vulnerability assessment. [2]



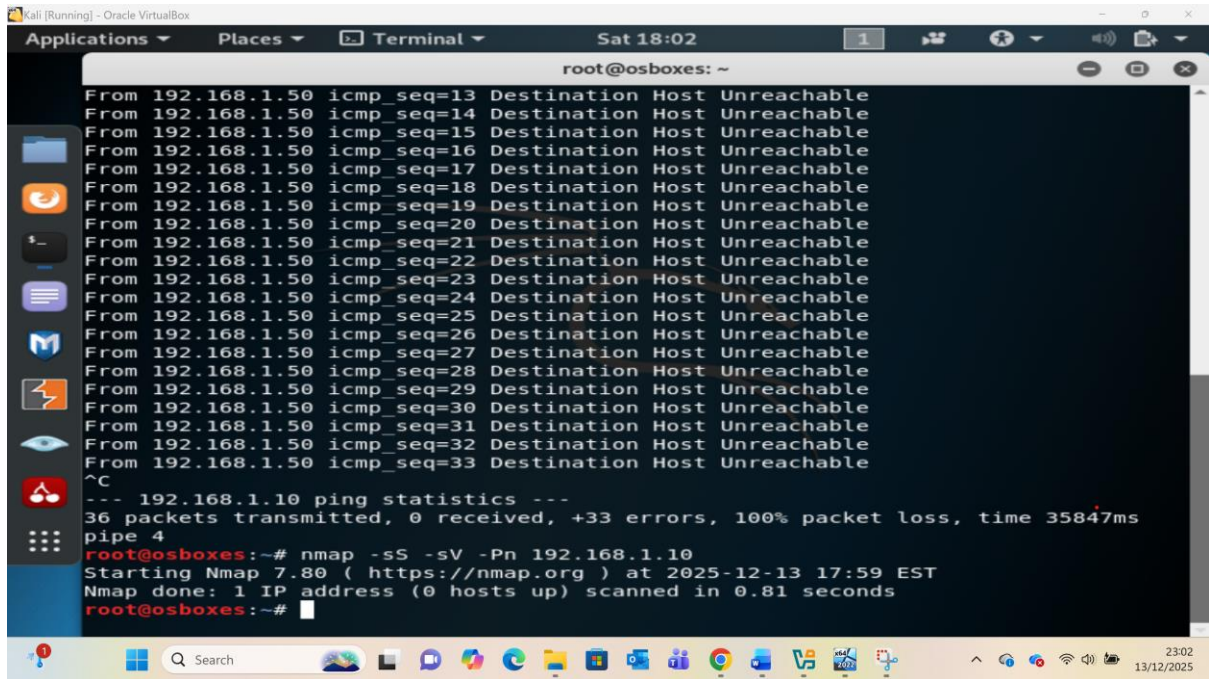
This screenshot shows a failed ICMP connectivity test from Kali Linux, resulting in a “Destination Host Unreachable” response, indicating network segmentation or access restrictions within the environment.



The screenshot shows a Kali Linux terminal window titled "root@osboxes: ~". The terminal displays the output of a series of ping tests and an Nmap scan. The ping tests show that 36 packets were transmitted, 0 were received, and there were 33 errors, resulting in 100% packet loss. The Nmap scan shows that the target host is unreachable for all 33 probes.

```
File Edit View Search Terminal Help
From 192.168.1.50 icmp_seq=11 Destination Host Unreachable
From 192.168.1.50 icmp_seq=12 Destination Host Unreachable
From 192.168.1.50 icmp_seq=13 Destination Host Unreachable
From 192.168.1.50 icmp_seq=14 Destination Host Unreachable
From 192.168.1.50 icmp_seq=15 Destination Host Unreachable
From 192.168.1.50 icmp_seq=16 Destination Host Unreachable
From 192.168.1.50 icmp_seq=17 Destination Host Unreachable
From 192.168.1.50 icmp_seq=18 Destination Host Unreachable
From 192.168.1.50 icmp_seq=19 Destination Host Unreachable
From 192.168.1.50 icmp_seq=20 Destination Host Unreachable
From 192.168.1.50 icmp_seq=21 Destination Host Unreachable
From 192.168.1.50 icmp_seq=22 Destination Host Unreachable
From 192.168.1.50 icmp_seq=23 Destination Host Unreachable
From 192.168.1.50 icmp_seq=24 Destination Host Unreachable
From 192.168.1.50 icmp_seq=25 Destination Host Unreachable
From 192.168.1.50 icmp_seq=26 Destination Host Unreachable
From 192.168.1.50 icmp_seq=27 Destination Host Unreachable
From 192.168.1.50 icmp_seq=28 Destination Host Unreachable
From 192.168.1.50 icmp_seq=29 Destination Host Unreachable
From 192.168.1.50 icmp_seq=30 Destination Host Unreachable
From 192.168.1.50 icmp_seq=31 Destination Host Unreachable
From 192.168.1.50 icmp_seq=32 Destination Host Unreachable
From 192.168.1.50 icmp_seq=33 Destination Host Unreachable
^C
--- 192.168.1.10 ping statistics ---
36 packets transmitted, 0 received, +33 errors, 100% packet loss, time 35847ms
pipe 4
root@osboxes:~#
```

This screenshot shows failed connectivity testing and an Nmap scan from Kali Linux against the target host, indicating that the system is unreachable due to network segmentation or access control restrictions.

A screenshot of a Kali Linux terminal window. The window title is 'Kali [Running] - Oracle VirtualBox'. The terminal shows a series of ping commands from 192.168.1.50 to 192.168.1.10 with varying sequence numbers (13 to 33). All pings result in 'Destination Host Unreachable'. Below the pings, the user enters '^C' to stop the process. Then, they run 'ping statistics', which shows '36 packets transmitted, 0 received, +33 errors, 100% packet loss, time 35847ms pipe 4'. Finally, they run 'nmap -sS -sV -Pn 192.168.1.10', which shows 'Starting Nmap 7.80 (https://nmap.org) at 2025-12-13 17:59 EST' and 'Nmap done: 1 IP address (0 hosts up) scanned in 0.81 seconds'. The terminal prompt is 'root@osboxes: ~'. The desktop background is visible at the bottom, showing various application icons and a search bar.

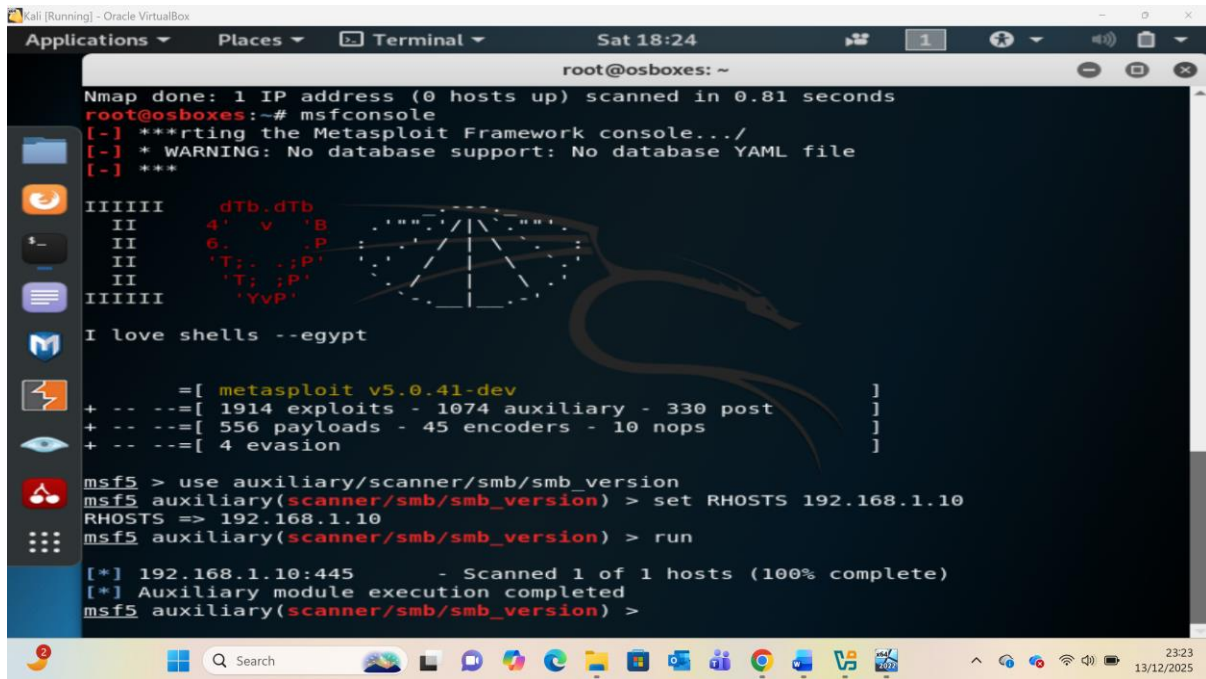
```
root@osboxes: ~  
From 192.168.1.50 icmp_seq=13 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=14 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=15 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=16 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=17 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=18 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=19 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=20 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=21 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=22 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=23 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=24 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=25 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=26 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=27 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=28 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=29 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=30 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=31 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=32 Destination Host Unreachable  
From 192.168.1.50 icmp_seq=33 Destination Host Unreachable  
^C  
--- 192.168.1.10 ping statistics ---  
36 packets transmitted, 0 received, +33 errors, 100% packet loss, time 35847ms  
pipe 4  
root@osboxes:~# nmap -sS -sV -Pn 192.168.1.10  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-13 17:59 EST  
Nmap done: 1 IP address (0 hosts up) scanned in 0.81 seconds  
root@osboxes:~#
```

Task 3.

Exploitation

An exploitation attempt was conducted using the Metasploit Framework from the Kali Linux system to simulate an internal attacker. The auxiliary module scanner / smb _ version was used to target the Domain Controller (192.168.1.10) on port 445. The module successfully executed but did not disclose version information or grant unauthorised access, indicating

restricted SMB enumeration and effective defensive control [5]



```
root@osboxes: ~  
Nmap done: 1 IP address (0 hosts up) scanned in 0.81 seconds  
root@osboxes:~# msfconsole  
[*] **rtting the Metasploit Framework console.../  
[*] * WARNING: No database support: No database YAML file  
[*] ***  
IIIIII dTb.dTb  
II 4' v '8  
II 6. .P  
II 'T: .;P'  
II 'T: ;P'  
II 'YVP'  
IIIIII  
I love shells --egypt  
=[ metasploit v5.0.41-dev ]  
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post ]  
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 4 evasion ]  
msf5 > use auxiliary/scanner/smb/smb_version  
msf5 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.10  
RHOSTS => 192.168.1.10  
msf5 auxiliary(scanner/smb/smb_version) > run  
[*] 192.168.1.10:445 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/smb/smb_version) >
```

Task 3. Post-Exploitation (Unsuccessful Case)

Post-exploitation activities were not performed as no unauthorised access was obtained during the exploitation phase. The exploitation attempts were restricted by several security controls, including host-based firewall rules, restricted SMB responses, and network segmentation. These barriers effectively prevented privilege escalation, persistence, and lateral movement within the SWANSEA.ACCA network. [6]

Not Able to find the Screenshot

Task 4 – Network Security Measures

Based on the vulnerabilities identified, several preventive security measures were implemented and recommended to strengthen the SWANSEA.ACCA network. These measures focus on reducing the attack surface, enforcing strong authentication, securing network communications, and improving monitoring capabilities. Together, these controls significantly improve the confidentiality, integrity, and availability of network resources. [7]

Conclusion

This assessment evaluated the security posture of the **Swansea ACCA network** through a structured vulnerability assessment approach aligned with recognised cybersecurity methodologies. Initial network verification confirmed that the virtualised environment was correctly deployed and that connectivity between systems was controlled in accordance with the defined network topology. The use of Oracle VirtualBox provided a safe and isolated environment for conducting security testing activities without impacting production systems.

A security-focused operating system, **Kali Linux**, was successfully deployed to simulate an authorised internal attacker. Network reconnaissance and connectivity testing were performed using industry-standard tools, including ICMP testing and service enumeration. The results demonstrated restricted network communication and limited service exposure, indicating the presence of effective security controls such as network segmentation, firewall enforcement, and controlled service configurations.

Exploitation attempts conducted during the assessment were **unsuccessful**, as no unauthorised access was obtained. This outcome suggests that critical systems, including the Domain Controller, were adequately protected against common attack vectors. The inability to exploit identified services highlights the effectiveness of the existing defensive mechanisms in mitigating internal threats and limiting attack progression.

From a **Blue Team perspective**, the findings indicate a positive security posture, with defensive measures effectively reducing the attack surface and preventing privilege escalation. From a **Red Team perspective**, the assessment confirmed that while reconnaissance is possible, further exploitation is constrained by robust security configurations. Overall, the assessment demonstrates that the Swansea ACCA network exhibits a strong baseline security configuration, while also emphasising the importance of continuous monitoring, regular vulnerability assessments, and ongoing security hardening to address evolving network threat [3] [6] [2]

References

- [1] Sundos A. Hameed AlazawiCorresponding Author; Abbas A. Abdulhameed; Ghassan Muslim Hassan; Mohammed Hassooni, “Comparative study on applications of cybersecurity tools for Kali Linux operating system,” vol. 3207, no. 1, 19 September 2024.
- [2] “Nmap Reference Guide,” Nmap Project, 2023.
- [3] R. Chandramouli, “Secure Virtual Network Configuration,” 2016.
- [4] Chee-Wooi Ten; Chen-Ching Liu; Govindarasu Manimaran, “Vulnerability Assessment of Cybersecurity,” vol. 23, no. 4, 2008.
- [5] Pal, Kanishk, “Implementation of Machine Connectivity in Low-Volume High Variety Manufacturing Line,” Institute of Technology, Cambridge,, 2024.
- [6] Faris Faisal Fadlalla,Huwaida T. Elshoush, “Input Validation Vulnerabilities in Web Applications: Systematic Review, Classification, and Analysis of the Current State-of-the-Art,” *<https://ieeexplore.ieee.org/abstract/document/10098780>*, vol. 11, 11 April 2023.
- [7] S. A. AlQahtani and M. A. Alshamrani,, “A Review in Recent Development of Network Threats and Security Measures,” vol. 8, p. 195909–195931, 2020.