DSA Cybersecurity Project Report

Part I: Virtual Cybersecurity Lab Setup

Student Name: Abioye Emmanuel

Program: 3-Month Cybersecurity Training Program

Email: eabioye54@gmail.com

Date: July 7, 2025

1. Introduction

The purpose of this project is to consolidate and demonstrate the practical skills acquired during the cybersecurity training program. This phase involves setting up a fully functional virtual cybersecurity lab to simulate a secure, real-world environment for conducting both offensive and defensive security operations.

2. Objectives

- To install and configure a virtual environment using a Type 2 hypervisor.

- To deploy and configure two virtual machines (VMs): Kali Linux as the attacker environment and Windows 7 as the target.

- To establish internal virtual networking between the machines.

- To verify communication and connectivity between the VMs using ping tests and network scanning.

3. Tools and Technologies Used

Tool/Technology	Purpose
Oracle VirtualBox	Type 2 Hypervisor
Kali Linux 2024.2	Attacker Virtual Machine (VM)
Windows 7 (64-bit)	Target Virtual Machine (VM)
Nmap	Network scanning and enumeration
Ping Utility	Connectivity testing

4. Lab Setup and Configuration

4.1 Hypervisor Installation

Oracle VirtualBox was installed on the host machine (Windows 10). The VirtualBox Extension Pack was also installed to enable support for USB and other additional features.

4.2 Virtual Machine Creation

Kali Linux VM
- OS Type: Debian 64-bit
- RAM: 4096 MB
- Disk: 40.91GB (VDI, dynamically allocated)
- Network Adapter: Internal Network (CyberLab)

Windows 7 VM
- OS Type: Windows 7, 32-bit
- RAM: 4096 MB
- Disk: 30 GB (VDI, dynamically allocated)
- Network Adapter: Internal Network (CyberLab)

4.3 Operating System Installation

Each VM was installed using official ISO images:
- Kali Linux was installed with default tools.
- Windows 10 was installed with basic configuration (no product key activation required for lab use).

4.4 Networking Configuration

Both VMs were configured to use an Internal Network named 'CyberLab', ensuring isolated communication without internet access.

Static IPs were assigned as follows:
- Kali Linux: 192.168.100.10
- Windows 10: 192.168.100.20
- Subnet Mask: 255.255.255.0

5. Connectivity Verification

5.1 Ping Test

From Kali:
```
ping 192.168.100.20
```
From Windows:

ping 192.168.100.10

Both tests confirmed successful communication, verifying proper network setup.

5.2 Service Enumeration

An Nmap scan was conducted from Kali to identify active services on the Windows machine:
nmap -sS 192.168.100.20

Results:
- Open ports such as 135 (RPC), 139 (NetBIOS), and 445 (SMB) were detected.

6. Observations and Challenges

- Networking Setup: Internal network required manual static IP assignment for reliable connectivity.

- Service Discovery: Basic services were detected on the target VM, confirming readiness for exploitation exercises.

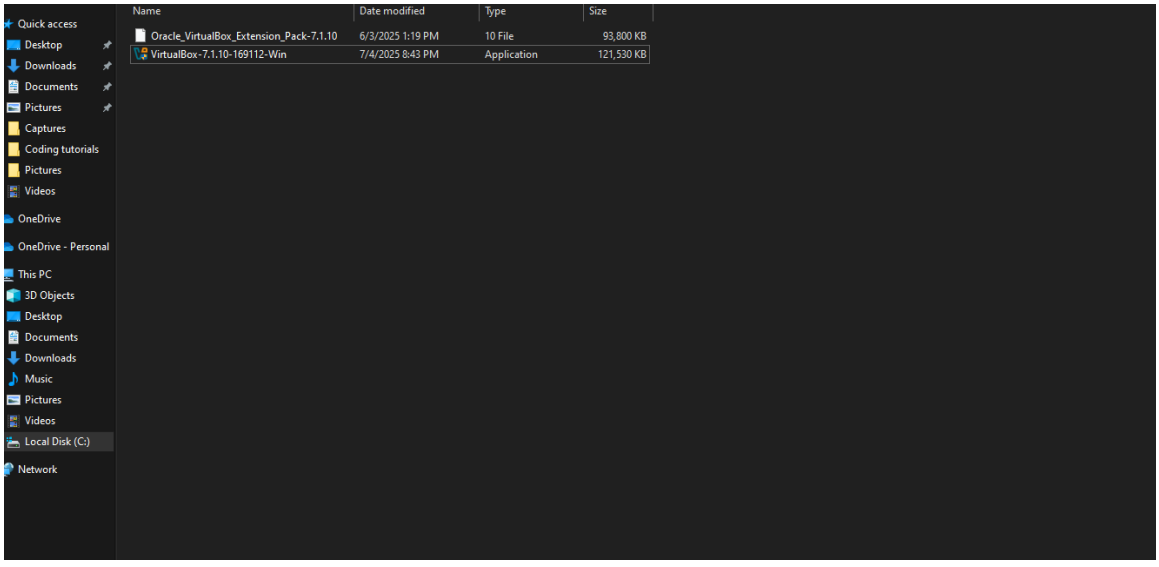
- User Permissions: Kali required root privileges for some commands; 'sudo' was used appropriately.

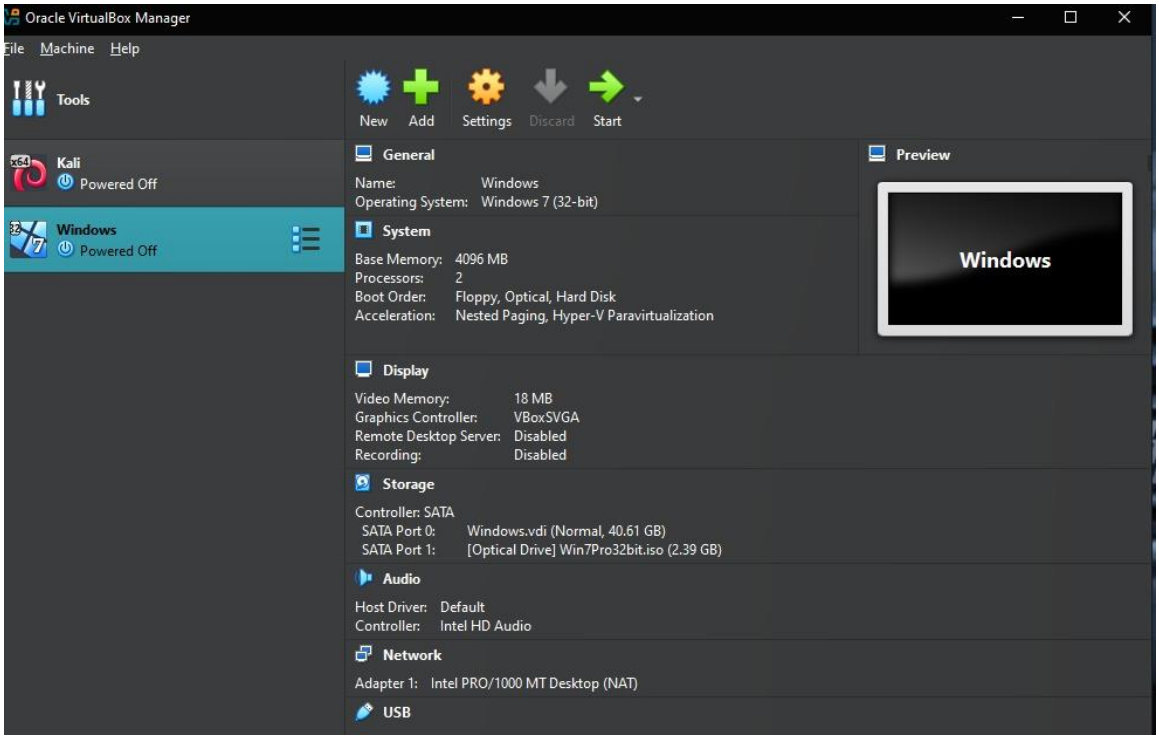
7. Conclusion

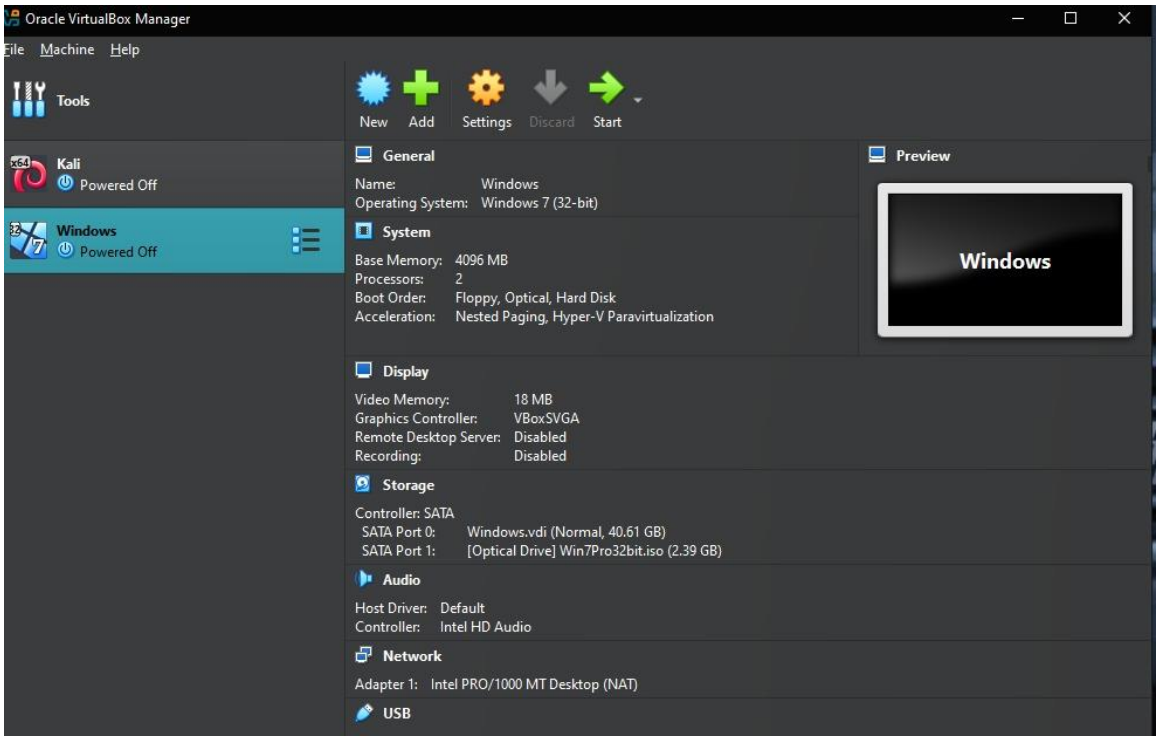
The virtual cybersecurity lab has been successfully set up. Both Kali Linux and Windows 7 VMs are fully functional, properly networked, and ready for penetration testing and defensive simulations. This environment provides a secure, isolated sandbox for future project tasks, including vulnerability scanning, exploitation, patching, and reporting.

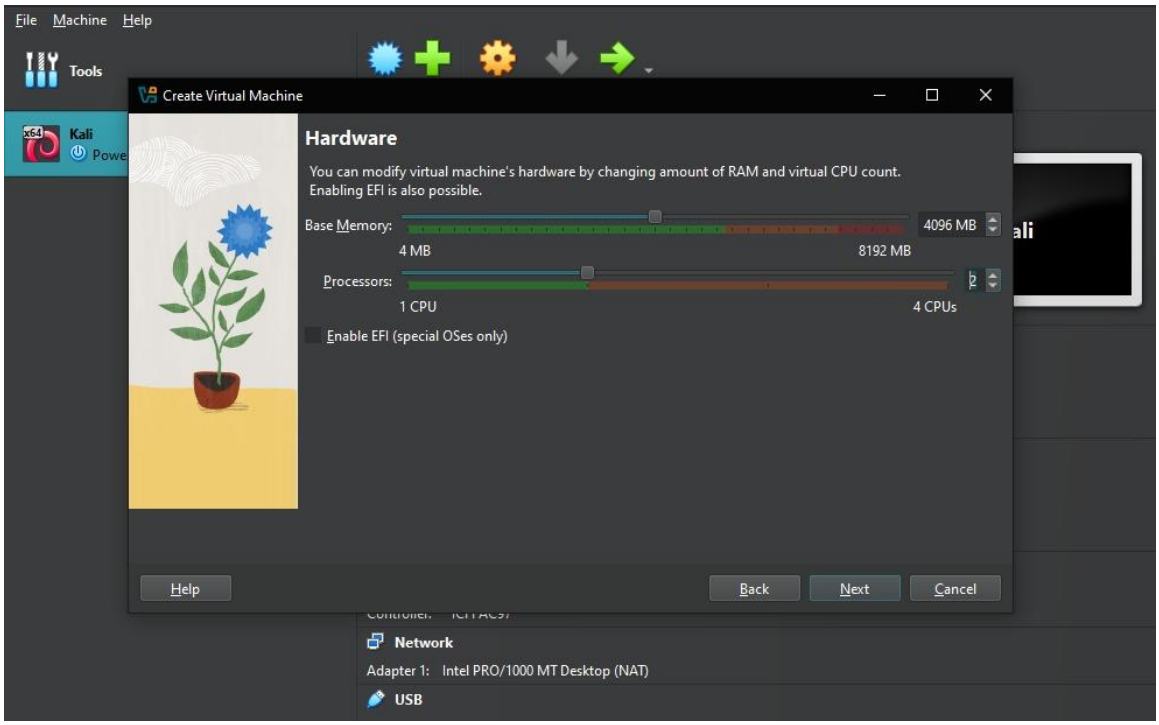
8. Screenshots and Evidence

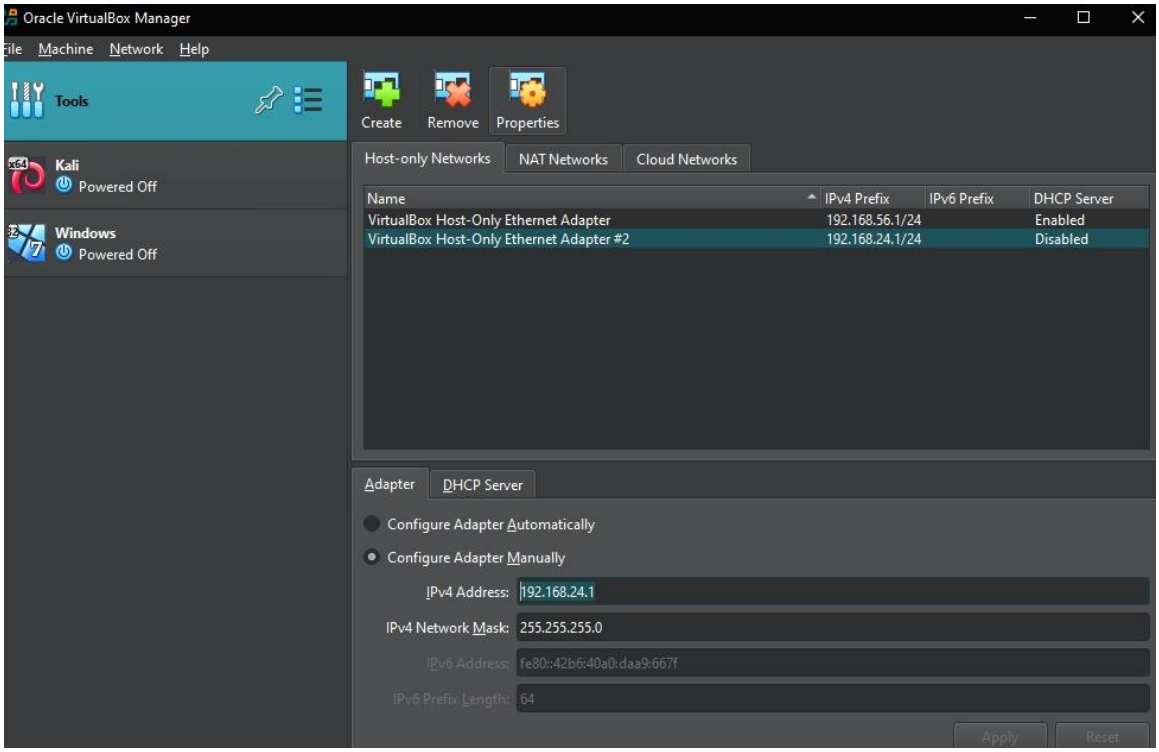
- VirtualBox settings for both VMs




Oracle VirtualBox Manager
File Machine Help
Tools
Kali
Powered Off
Windows
Powered Off
New Add Settings Discard Start
General
Name: Windows
Operating System: Windows 7 (32-bit)
System
Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Preview
Windows
Display
Video Memory: 18 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: Windows.vdi (Normal, 40.61 GB)
SATA Port 1: [Optical Drive] Win7Pro32bit.iso (2.39 GB)
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB


Oracle VirtualBox Manager
File Machine Help
Tools
Kali
Powered Off
Windows
Powered Off
New Add Settings Discard Start
General
Name: Windows
Operating System: Windows 7 (32-bit)
System
Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Preview
Windows
Display
Video Memory: 18 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: Windows.vdi (Normal, 40.61 GB)
SATA Port 1: [Optical Drive] Win7Pro32bit.iso (2.39 GB)
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB





- IP configuration outputs

- Ping test results from both machines

- Nmap scan output from Kali