TASK 1: Virtual Cybersecurity Lab Report

Student Information

Name: Adebowale Emmanuel Okikiola

GitHub: https://github.com/Secunuel

Course: Cybersecurity Capstone

Date: July 2025

Objective

The objective of this task is to set up a virtual cybersecurity lab using VirtualBox, install Kali Linux and Windows 10 VMs, configure an internal network between them, assign manual static IP addresses, and perform a successful ping test between both systems.

Tools & Platforms Used

Tool/Platform	Purpose
VirtualBox	Virtualization environment
Kali Linux	Attacker/analyst machine
Windows 10	Target machine
ip / ipconfig	IP configuration and ping test
ping	Test network connectivity

Lab Configuration Steps

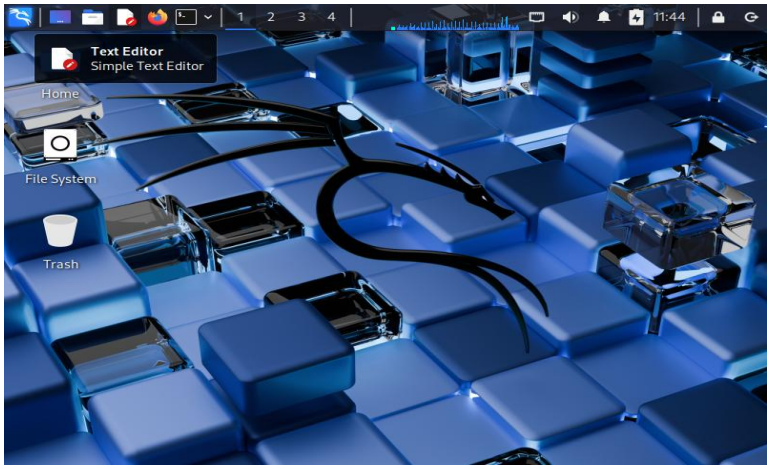
1. Created two virtual machines (Kali Linux and Windows 10) in VirtualBox.
2. Assigned each VM 1GB of RAM and 20–25 GB virtual storage.
3. Set network adapters to 'Internal Network' with the same name: IntNet.
4. Enabled Promiscuous Mode (Allow VMs) and Cable Connected.
5. Manually assigned static IPs as follows:

VM	IP Address	Subnet Mask
Kali	192.168.56.101	255.255.255.0

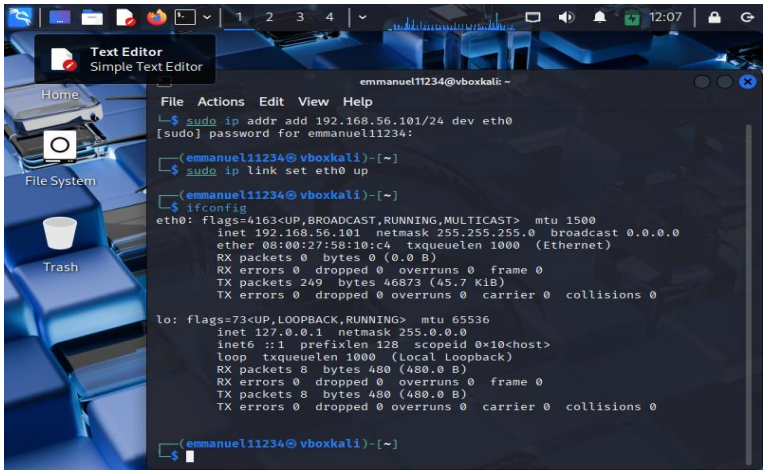
Windows	192.168.56.102	255.255.255.0

Screenshot of lab1 task

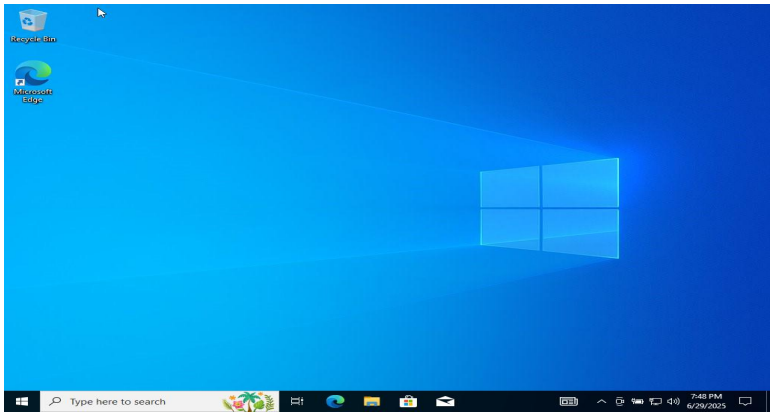
[Insert Screenshot: Kali Desktop]



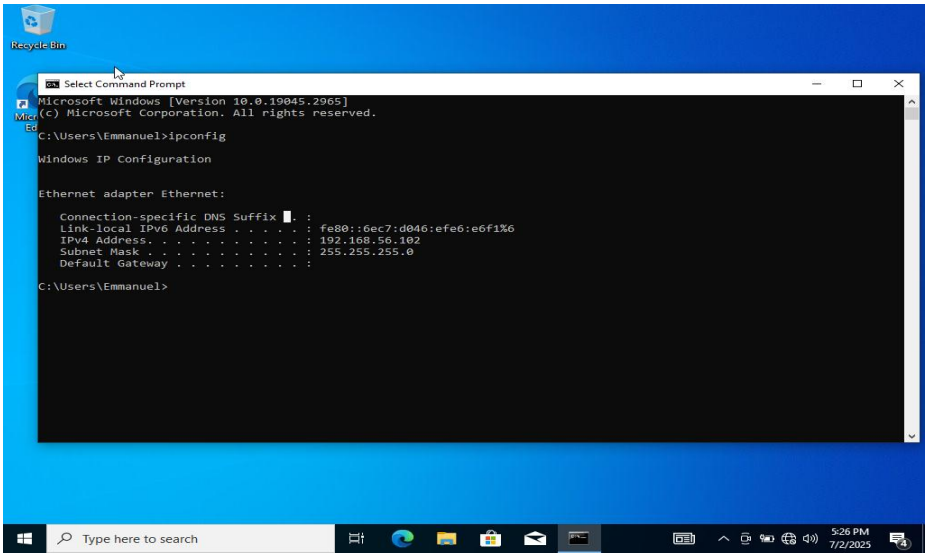
[Screenshot of manualy assigned Kali IP Address (`ip a`)]



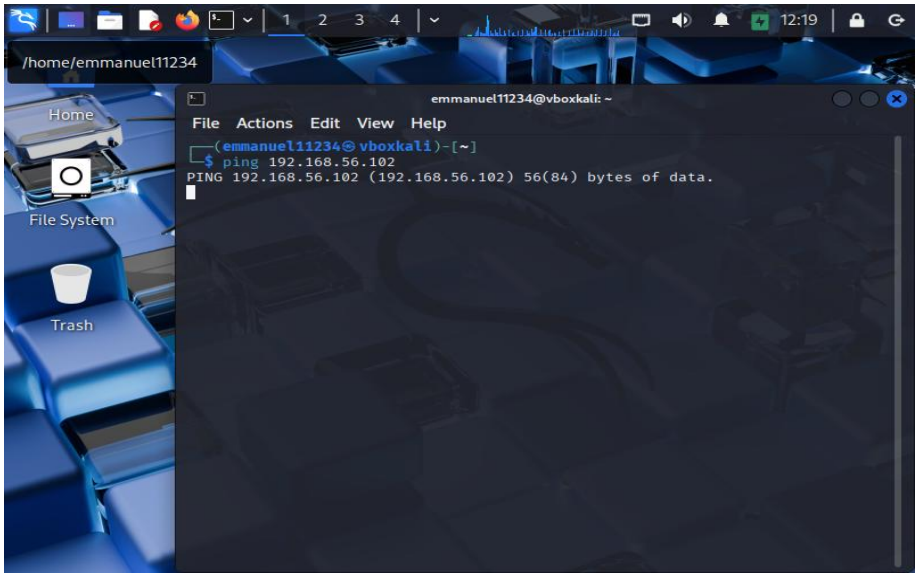
[Screenshot of Windows Desktop]



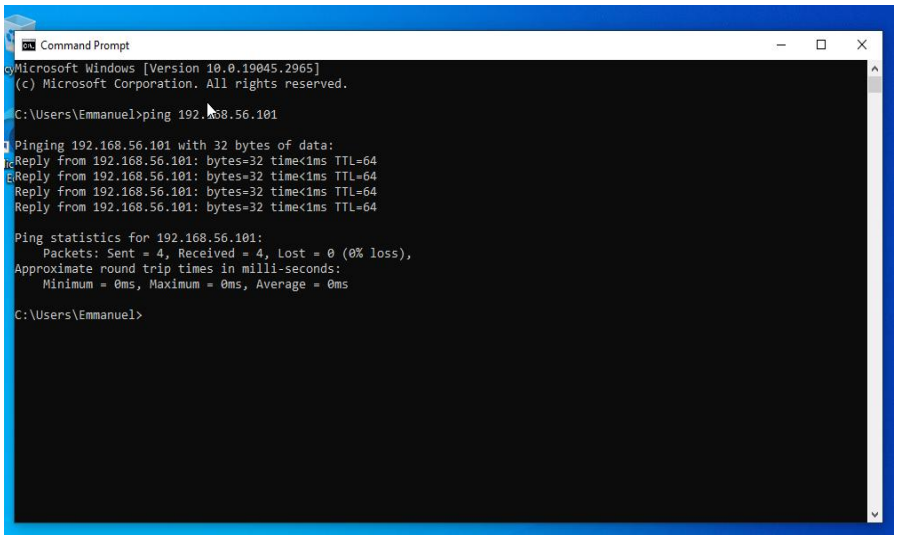
[screenshot of Windows IP Address (`ipconfig`)]



[Here is my Ping from Kali to Windows]



[Here is my Ping from Windows to Kali]



Conclusion

The virtual cybersecurity lab setup was successful. Kali Linux and Windows 10 VMs were able to communicate with each other through an internal VirtualBox network using manually assigned IP addresses. The ping tests verified bidirectional connectivity, completing the foundational setup for future cyber defense and forensic analysis labs.