**Module 1 Project: Designing Cybersecurity-Aware IT Infrastructure for a Small Office**

**Name: Seun Akinola**

**Email: Oluwaseun.akkinola@gmail.com**

**Date: April 2, 2025**

**Table of Contents**

**Introduction ............................................. 2**

**Solution Architecture Design .....................3**

**Virtual Machine Configurations ..................5**

**Virtual LAN Configuration ...........................7**

**1. Introduction**

This project demonstrates the design and implementation of a cybersecurity-aware IT infrastructure suitable for a small office environment. The project uses a host Windows system and a virtualized Linux workstation to emulate real-world administrative and development environments.

**Goals of the Design:**

Ensure secure communication between the host system and VM

Enable network connectivity on individual systems and efficient data sharing through cloud integration

Document setup process for reproducibility and clarity

**2. Solution Architecture Design**

The IT infrastructure consists of the following components:

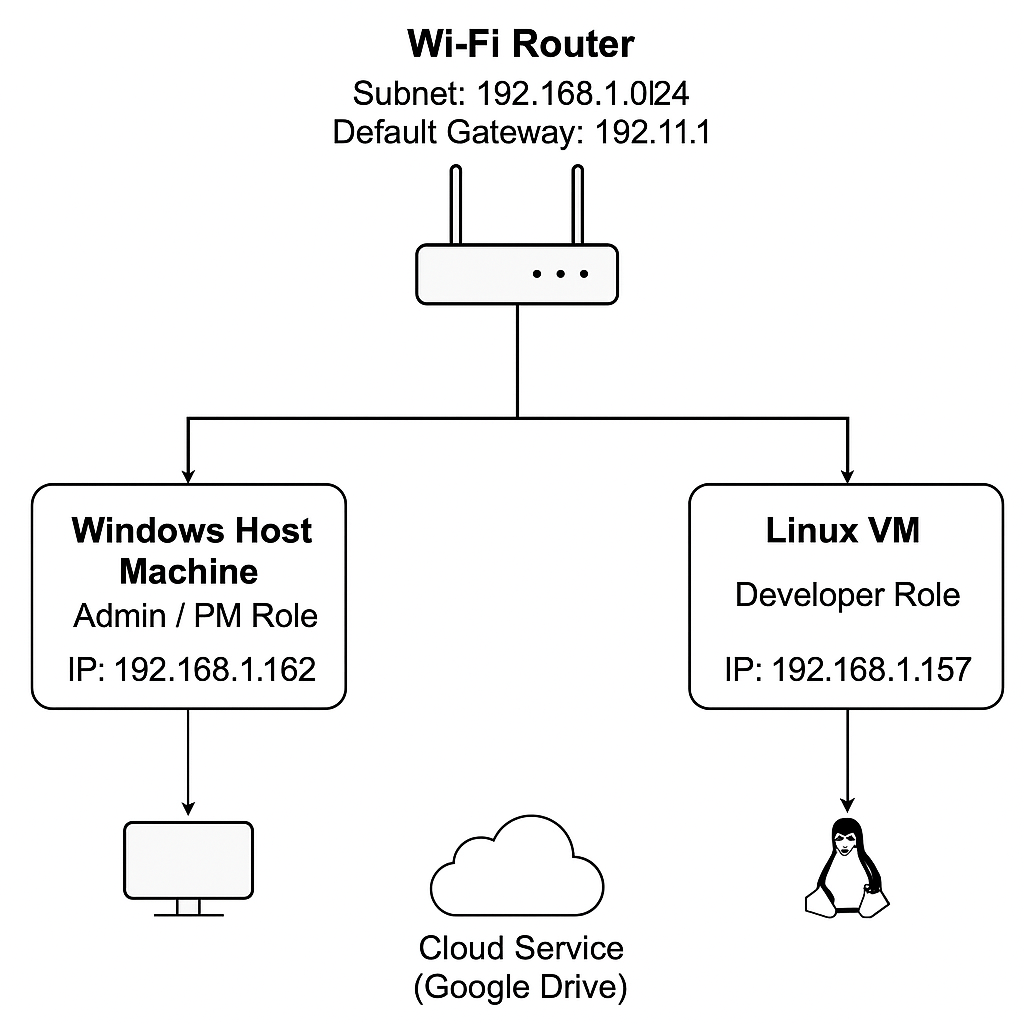
Windows Host Machine

Linux Virtual Machine

Wi-Fi Router (Physical LAN Access)

Google Drive (Cloud Storage Integration)

Network Topology Diagram:



Device Roles and Configurations:

Windows Host (IP: 192.168.1.152)

Linux VM (IP: 192.168.1.157, Bridged Adapter)

Router (Gateway: 192.168.1.1)

Cloud Service (Google Drive accessible from both systems)

**3. Virtual Machine Configurations**

**Windows Workstation (Host)**

Role: Administrative and Project Management

OS: Windows 11 Pro

CPU: 6 Cores

Memory: 8 GB

Storage: 238 GB

**Linux Workstation (VM)**

Role: Developer

OS: Ubuntu 22.04 LTS

CPU: 2 Cores

Memory: 2048MB

Storage: 25 GB VDI

**Installation Steps:**

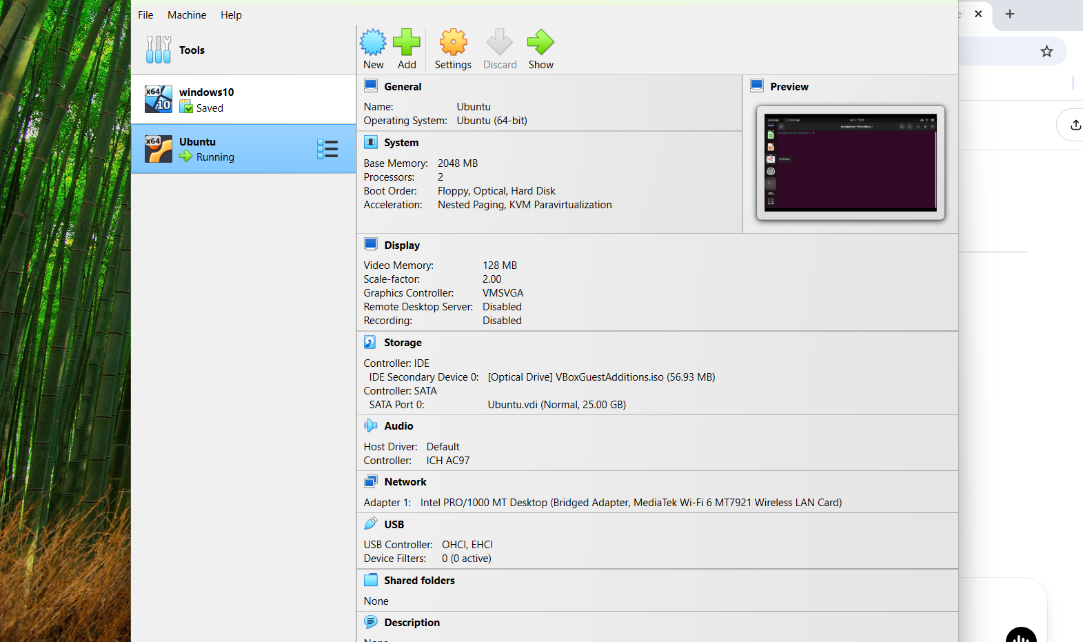
Installed VirtualBox on Windows host

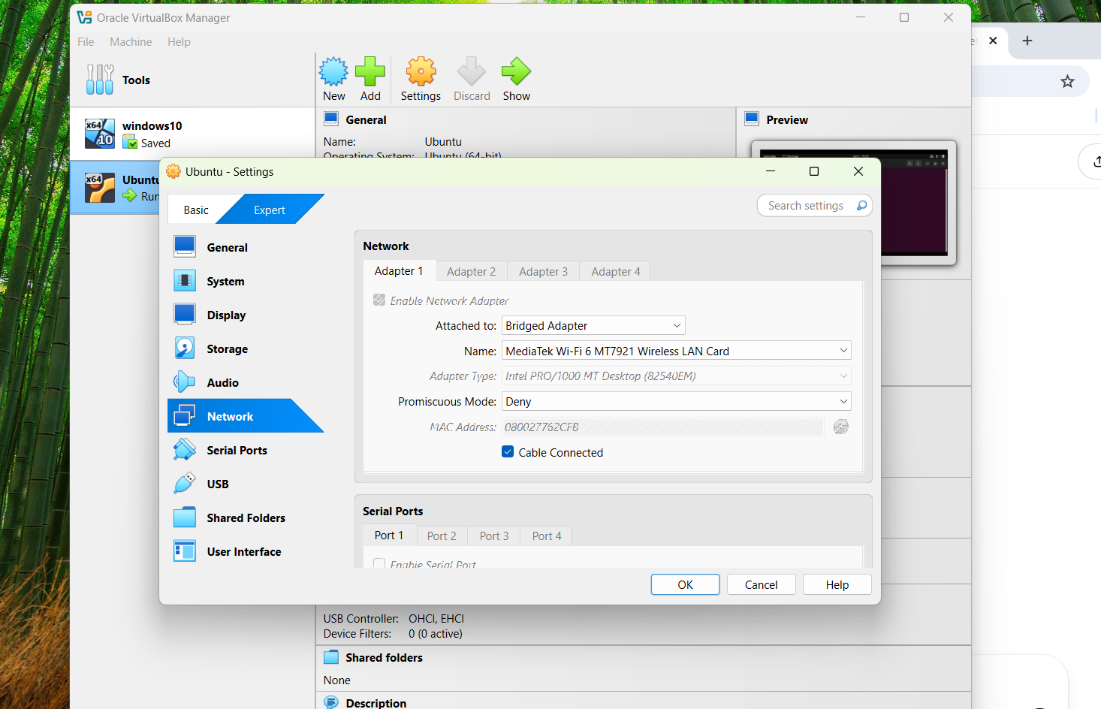
Downloaded Ubuntu ISO from official site

Created new VM with specified resources

Configured network to Bridged Adapter

Installed Ubuntu and updated packages





**4. Virtual LAN Configuration**

Configuration Method:

Network Type: Bridged Adapter

Both systems connected to the same subnet (192.168.1.0/24)

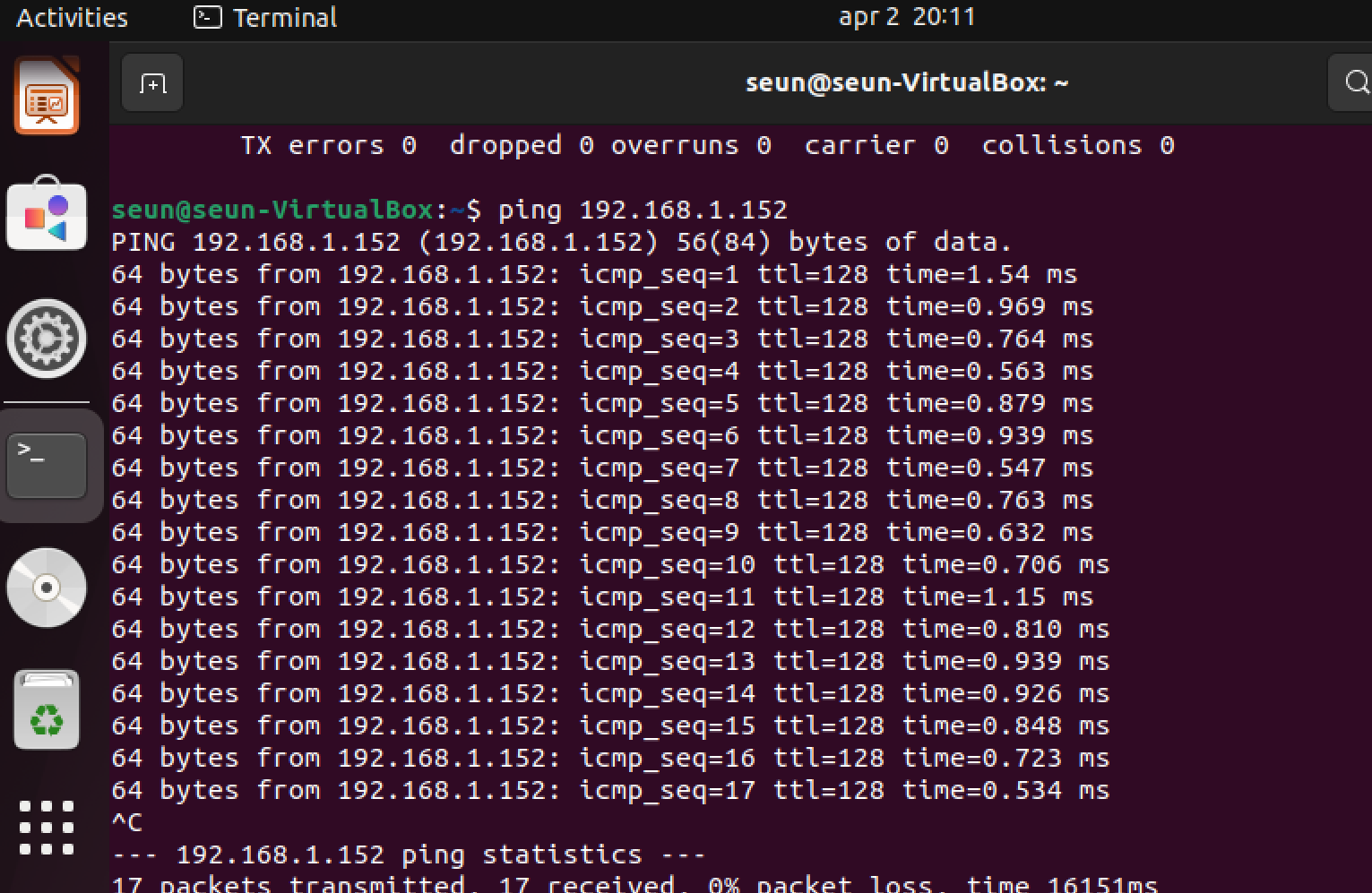
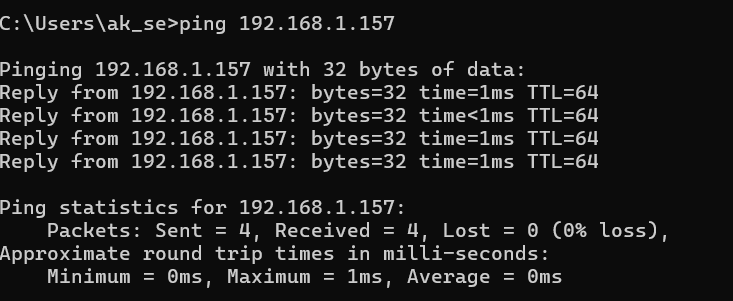
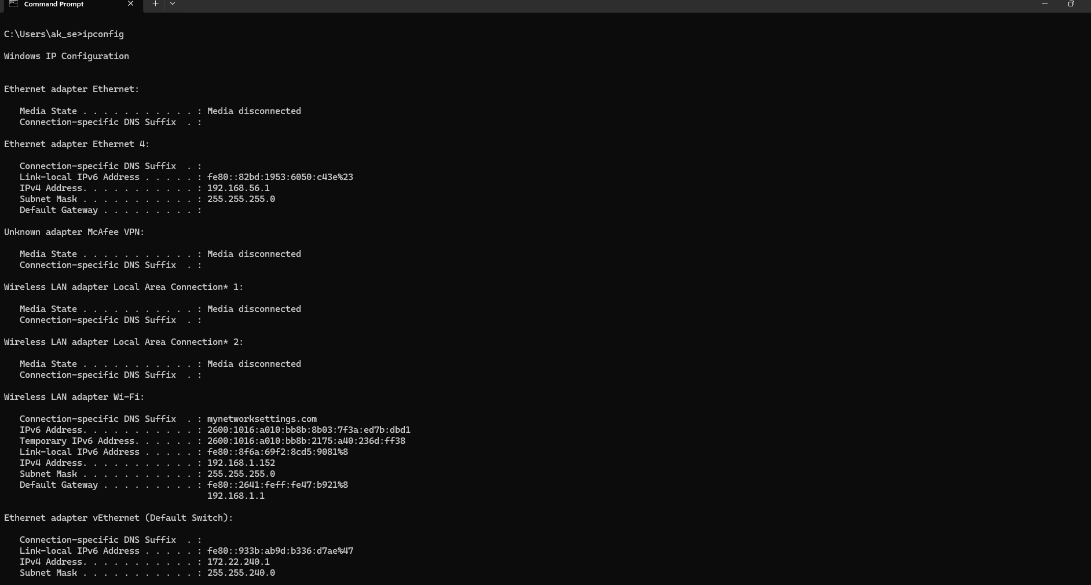
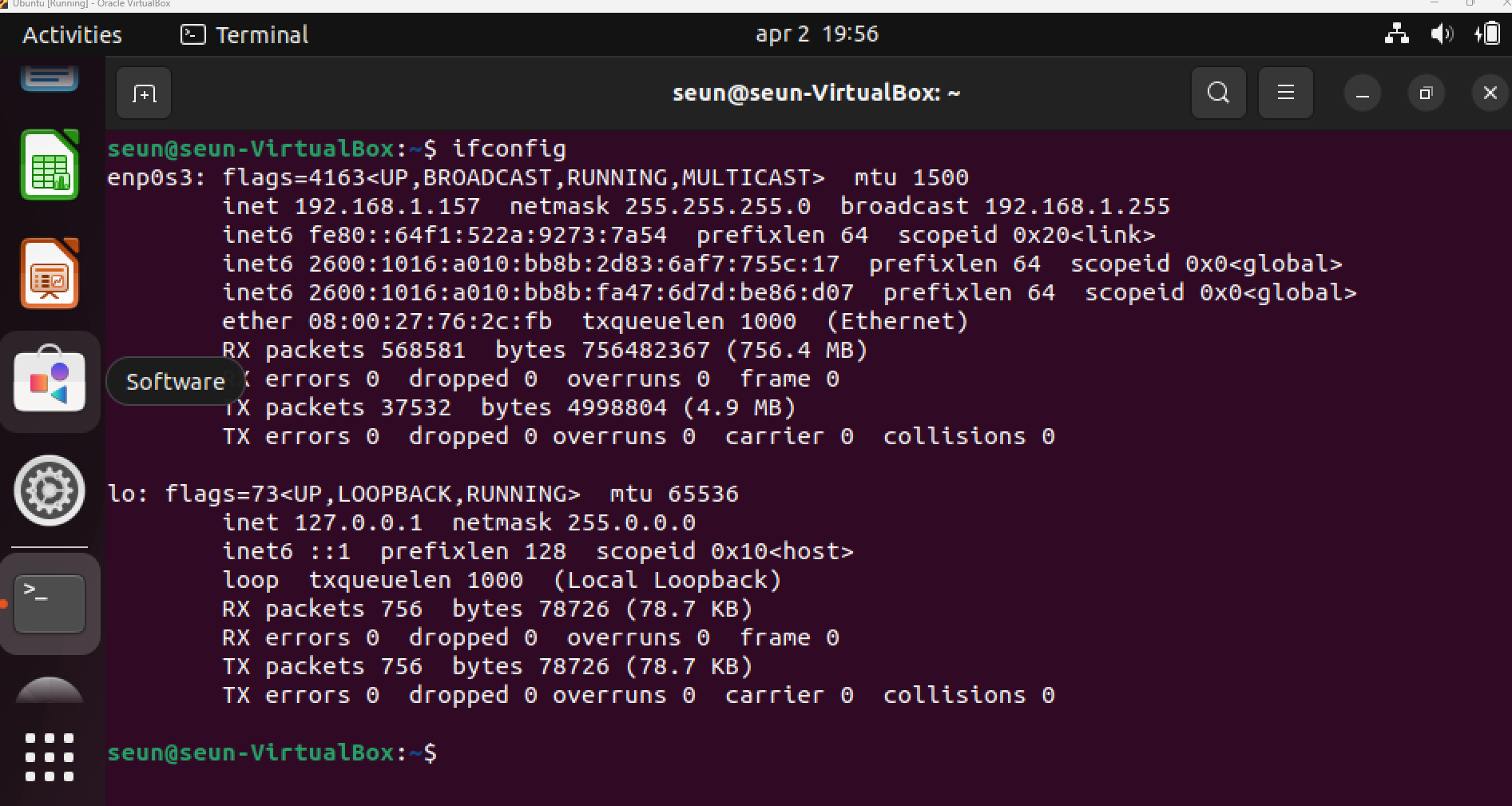
IPs assigned via DHCP from home router

Testing Network Connectivity:

Verified IP addresses using ipconfig on Windows and ip a or ifconfig on Linux

Ping test from Windows to Linux: Successful

Ping test from Linux to Windows: Successful



**5. Cloud Integration**

Cloud services were integrated using Google Drive to enable secure and shared access to files across both Windows and Linux systems. A test file named hello.txt was created and uploaded from each system to ensure accessibility.

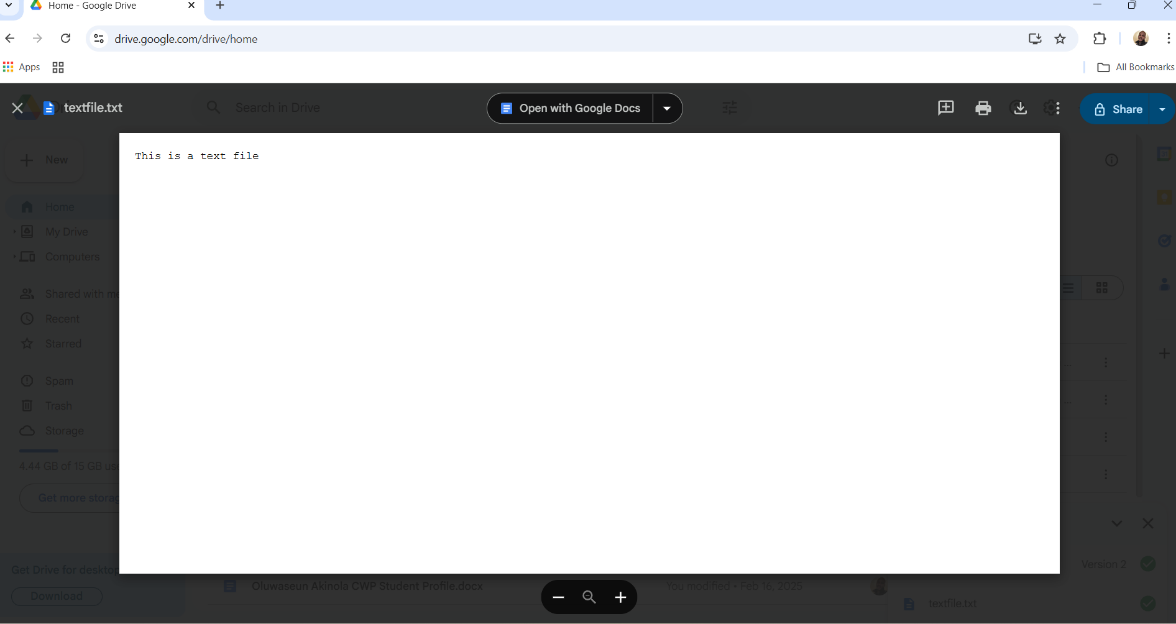
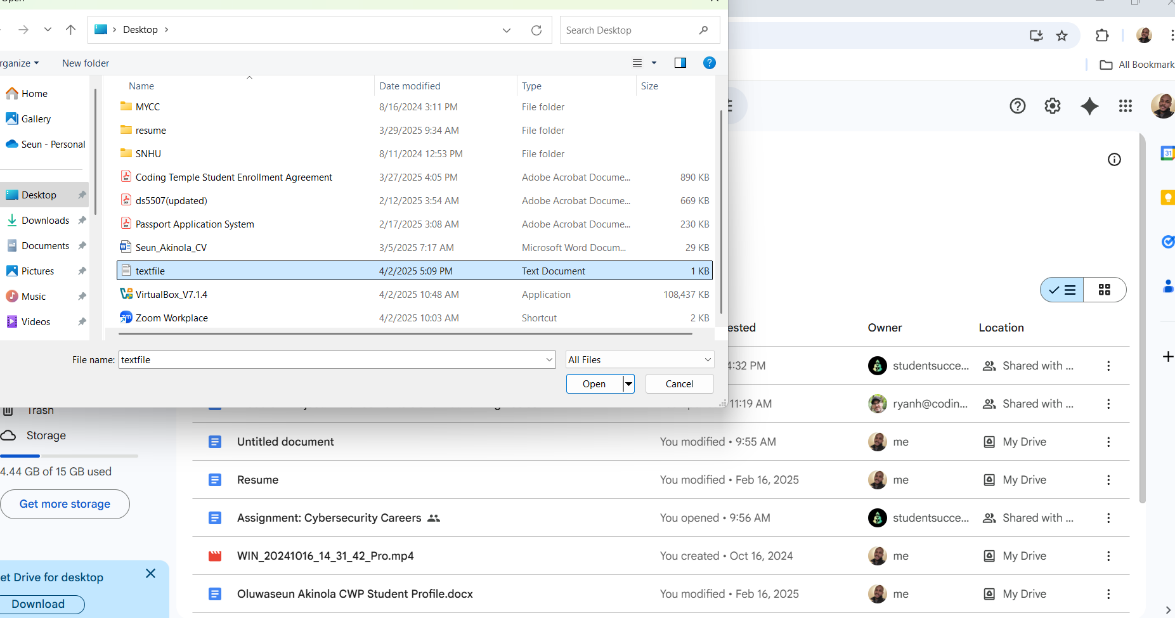
**Steps:**

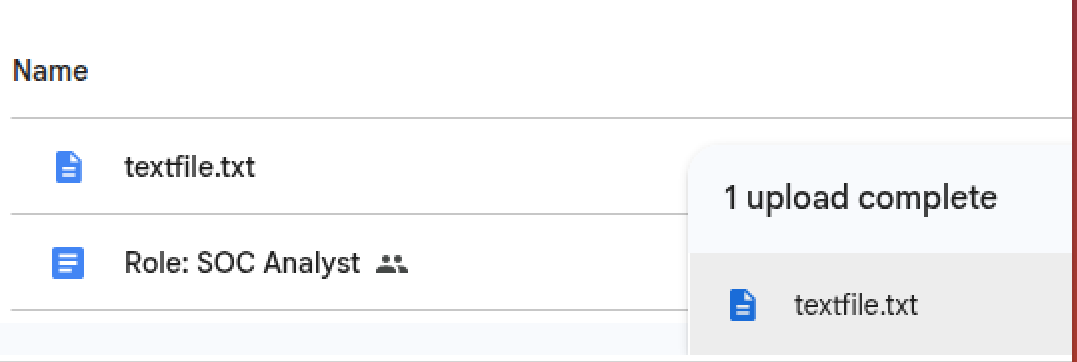
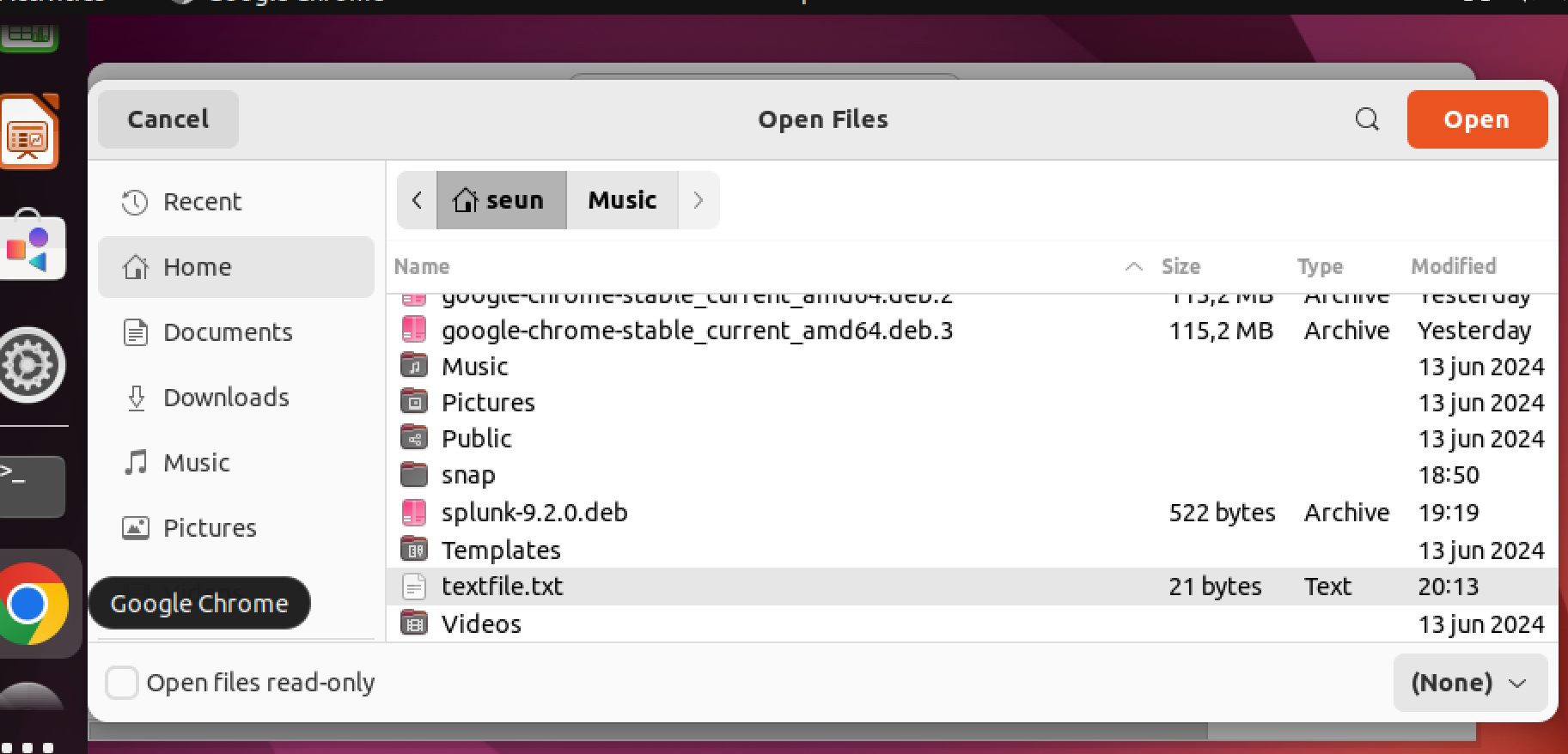
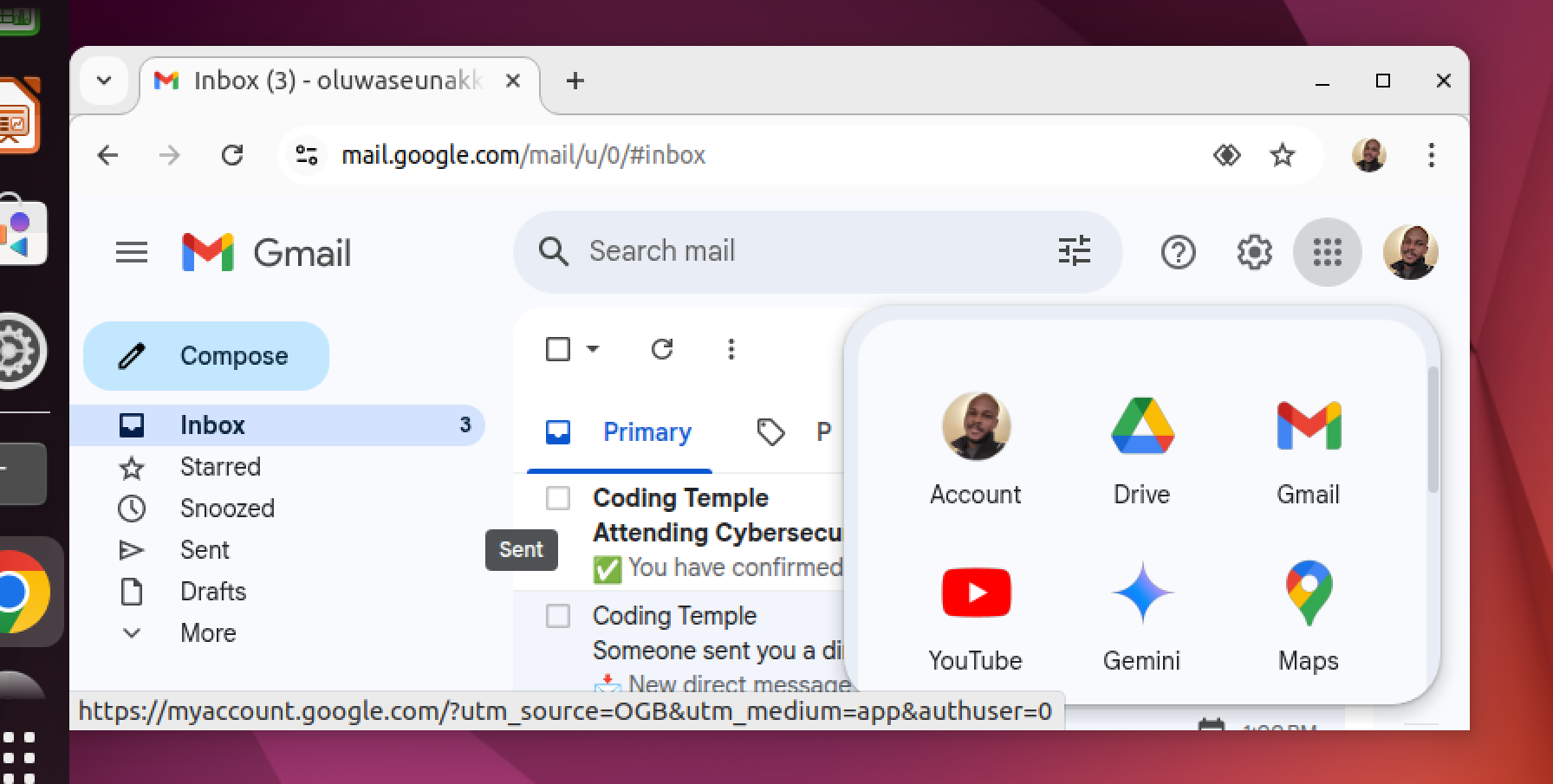
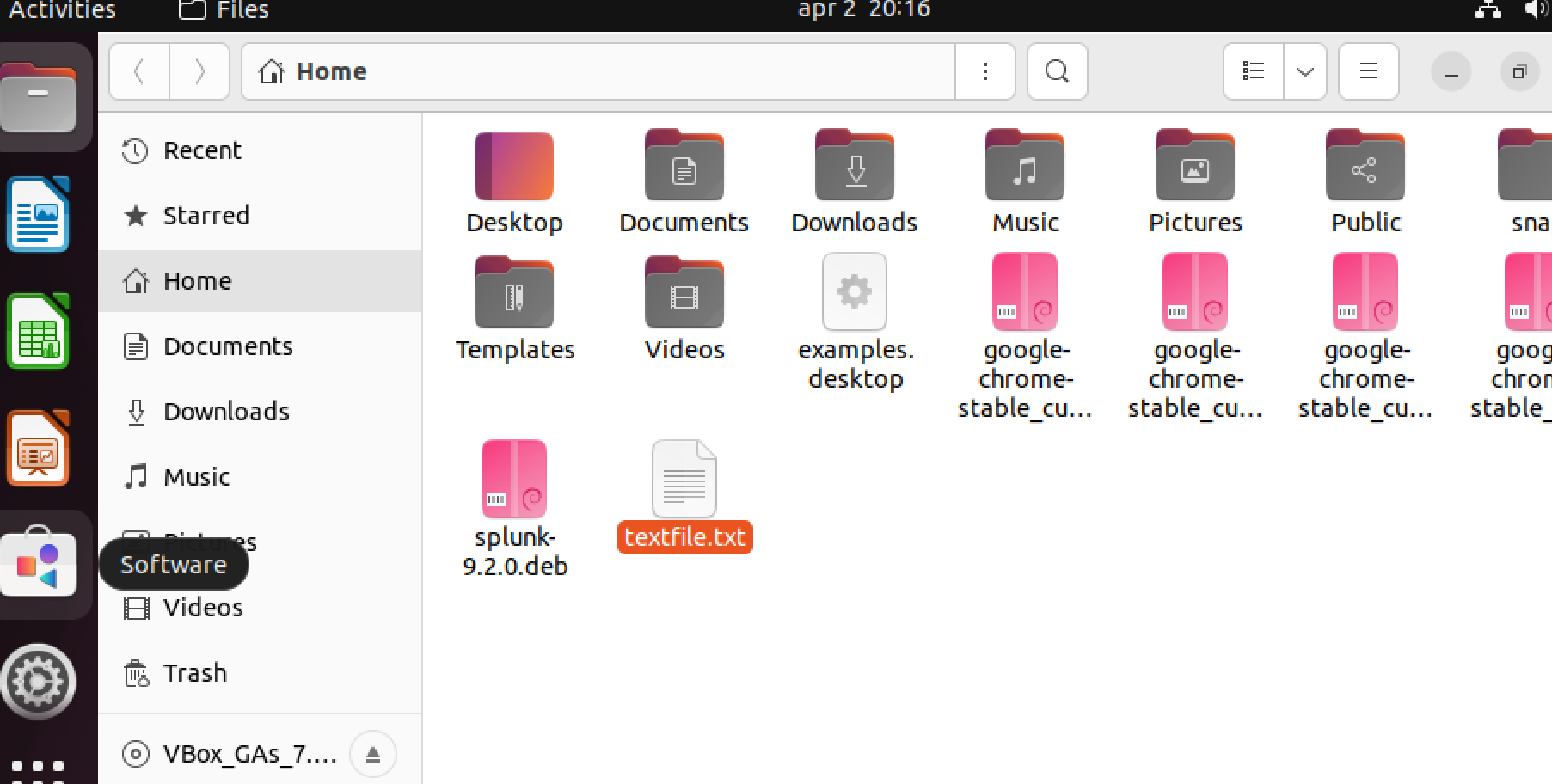
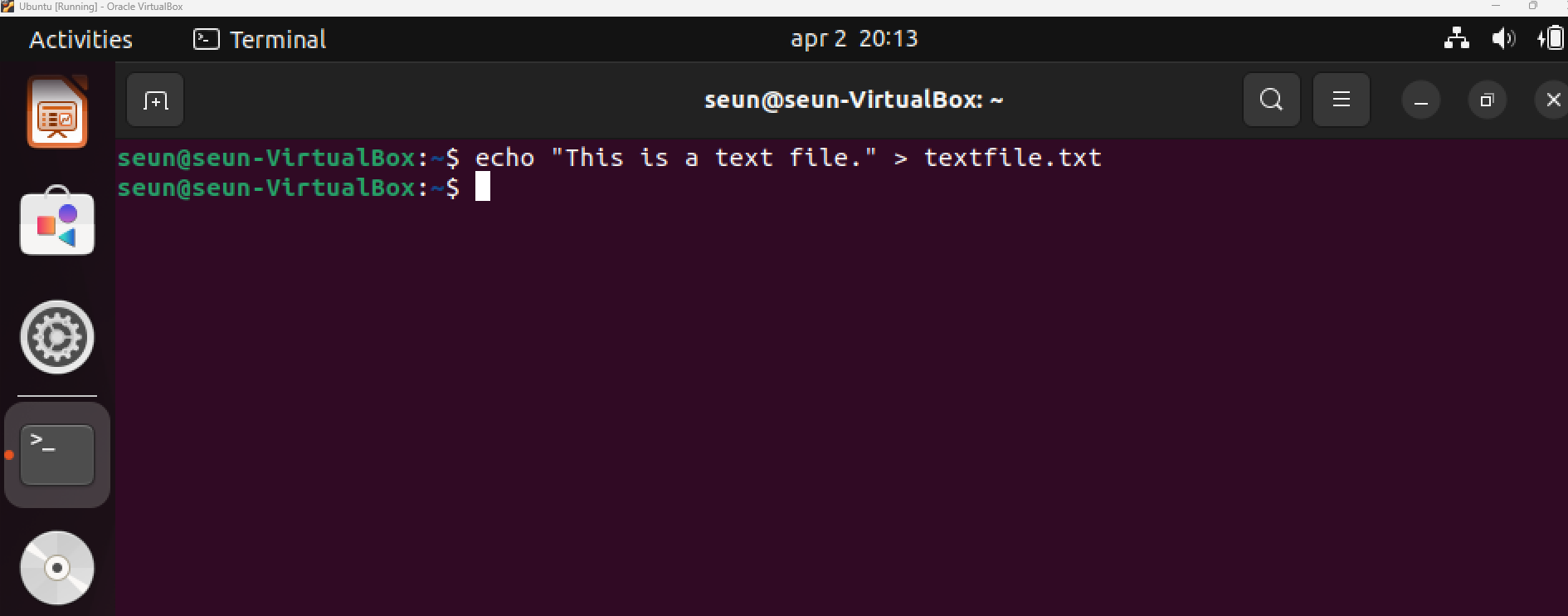
Created a text file: "This is a text file."

Uploaded from Windows using Chrome to Google Drive

Uploaded from Linux using Chrome to Google Drive

Verified the shared link was accessible on both systems





**Challenges**: Initially, the Linux VM couldn’t ping the Windows machine due to a firewall rule.

**Mitigation:** Accessed the firewall through Windows Defender and enabled the inbound rules for File and Printer Sharing (Echo Request – ICMPv4)

**8. Conclusion and Recommendations**

This project successfully demonstrates the implementation of a secure and functional small-office IT infrastructure using a Windows host and a Linux VM. Network communication and cloud-based collaboration were tested and validated.

**Future Improvements:**

Add a firewall or configure UFW on Linux for more control

Implement a VPN for secure remote access

Use a Host-Only Adapter to fully isolate development traffic