Week 4 reflection

Objective
The goal of this week's task was to set up an Ubuntu Server virtual machine in VirtualBox and establish a secure SSH connection from the host machine. This demonstrates practical networking and remote access skills.

Steps Taken
Reinstalled Ubuntu Server VM

Created a new VM in VirtualBox and installed Ubuntu Server.

Configured a user account (rabin) and enabled the OpenSSH server during installation.

Configured Networking in VirtualBox

Set Adapter 1 to NAT for internet access.

Added Adapter 2 as a Host-Only Adapter to allow direct communication between host and VM.

Verified adapter settings and adjusted Promiscuous Mode to Allow VMs Only.

Verified IP Address

Ran ip addr inside the VM.

Confirmed the loopback address (127.0.0.1) and then configured networking until a usable IP was available.

Used NAT + Port Forwarding as a fallback method, mapping host port 2222 to guest port 22.

Tested SSH Service

Checked SSH status with systemctl status ssh.

Restarted the service to ensure it was listening on 0.0.0.0:22.

Allowed SSH traffic through the firewall using ufw allow 22.

Connected from Host Machine

From the host terminal, ran:

bash
ssh -p 2222 rabin@localhost
Accepted the fingerprint prompt and entered the password.

Successfully logged into the Ubuntu Server VM remotely.

Evidence
Screenshot 1: ip addr output showing network configuration.

Screenshot 2: SSH command executed from host machine.

Screenshot 3: Successful login prompt inside the VM (rabin@ubuntu-server:~$).

Reflection
This exercise taught me how to configure VirtualBox networking, troubleshoot SSH
connectivity, and use port forwarding as a reliable method to connect when
host-only networking was unavailable. I now understand the difference between
NAT, Host-Only, and Bridged adapters, and how SSH depends on proper IP
assignment and firewall rules.