12 Project network security

Names: Omar sherif Hosny 221010339

Mohamed ElSayed 221010750

To Eng : Abdelrhman Solyman

Part 2

1. Introduction

Secure Shell (SSH) is a cryptographic network protocol used for securing remote login and other secure network services over an insecure network. This project focuses on configuring SSH key-based authentication between two Linux Mint virtual machines (Client and Server).

---

2. Steps and Execution

Step 1: Install OpenSSH Server and Client

On both Client and Server VMs, install OpenSSH server and client:

sudo apt update

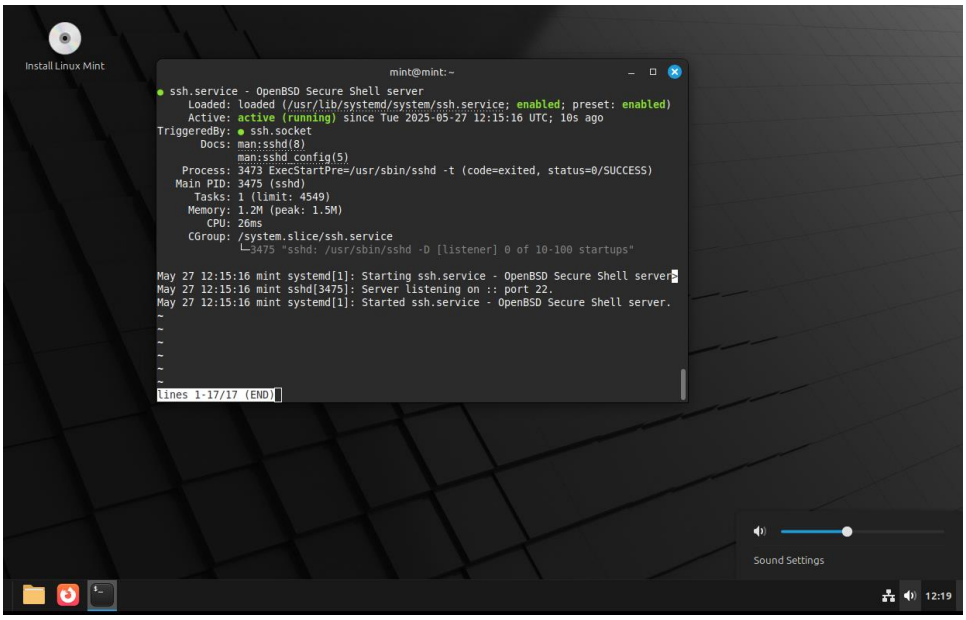
sudo apt install openssh-server openssh-client

Ensure the SSH service is active on the server:

sudo systemctl enable ssh

sudo systemctl start ssh

This commands make us to start use ssh and it make runing in server and client

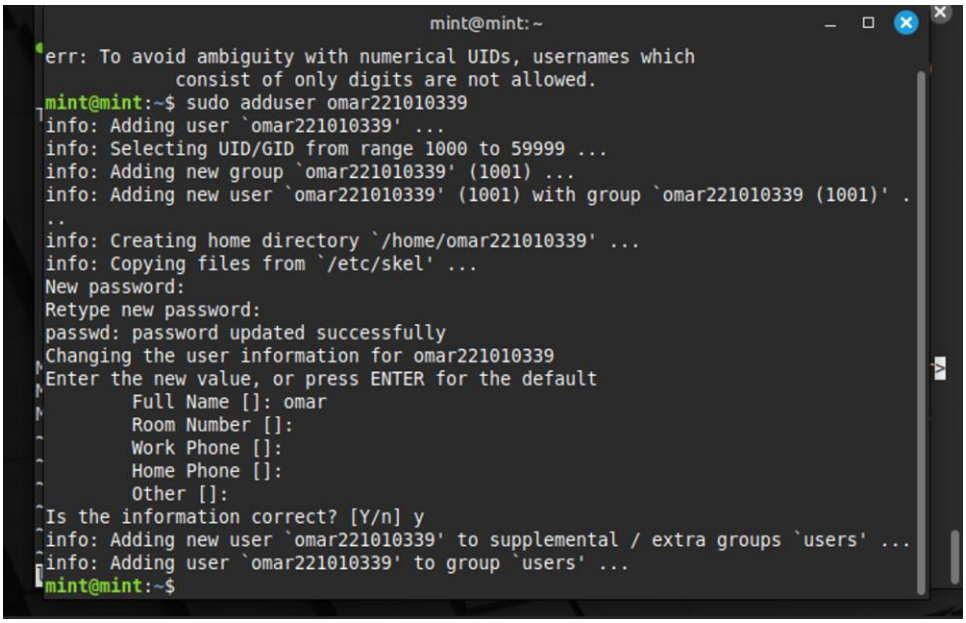


Step 2: Create a User on the Server

A new user was created on the server with the following command:

sudo adduser omar221010339

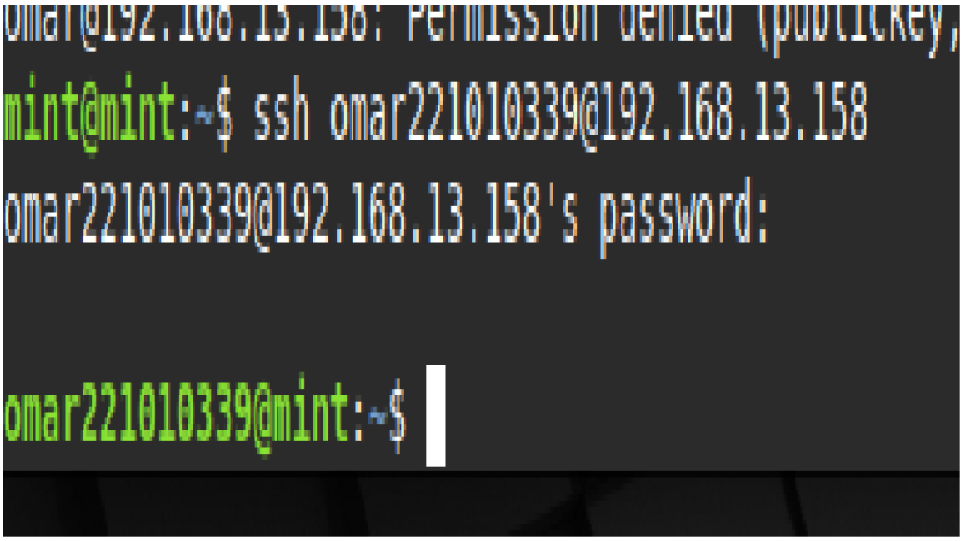
During the process, a password was set, and optional fields (Full Name, Room Number, etc.) were left empty.



Step 3: Connect to the Server Using Password Authentication

From the client machine, an SSH connection was established using the newly created username and password:

ssh omar221010339@<server-ip>

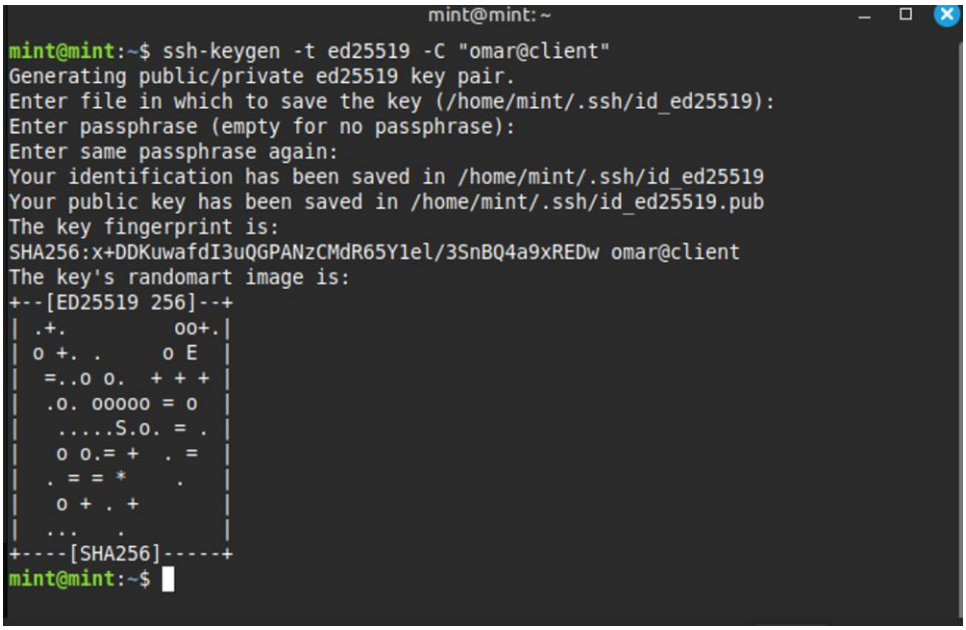


Step 4: Generate SSH Key Pair on Client

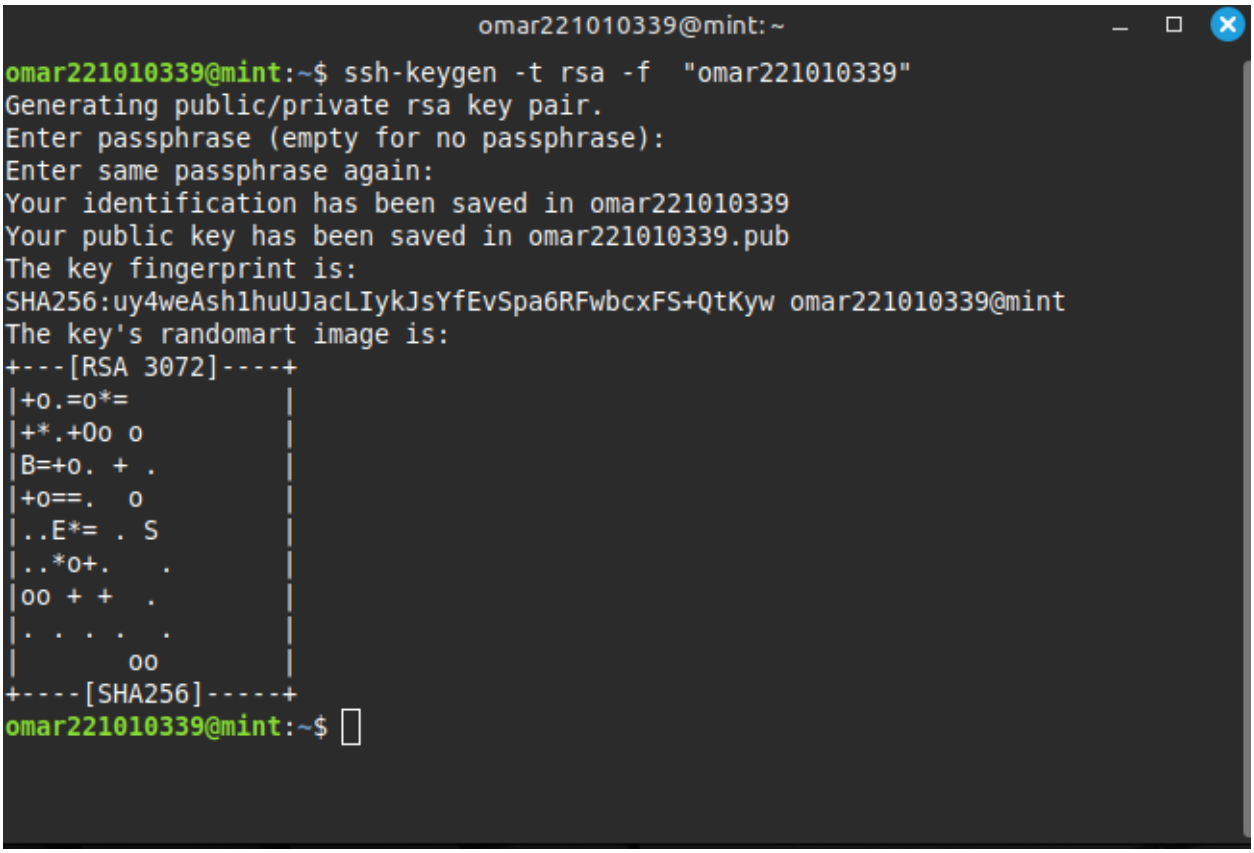
On the client machine, an ed25519 key pair was generated with:

ssh-keygen -t ed25519 -C "omar221010339@client"

Default save location was accepted (~/.ssh/id_ed25519), and passphrase was skipped.



RSA



Step 5: Copy Public Key to Server

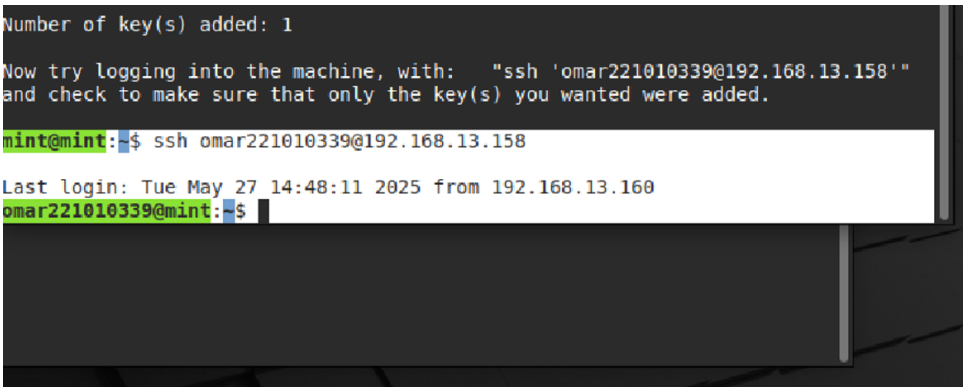
The public key was copied to the server's authorized_keys using:

ssh-copy-id omar221010339@<server-ip>

Step 6: SSH Login Without Password

The SSH connection was tested again, and it logged in successfully without prompting for a password:

ssh omar221010339@<server-ip>



Step 7: Disable Password Authentication on Server

To enforce key-based authentication only, password login was disabled on the server:

sudo nano /etc/ssh/sshd_config

Modified line: PasswordAuthentication no

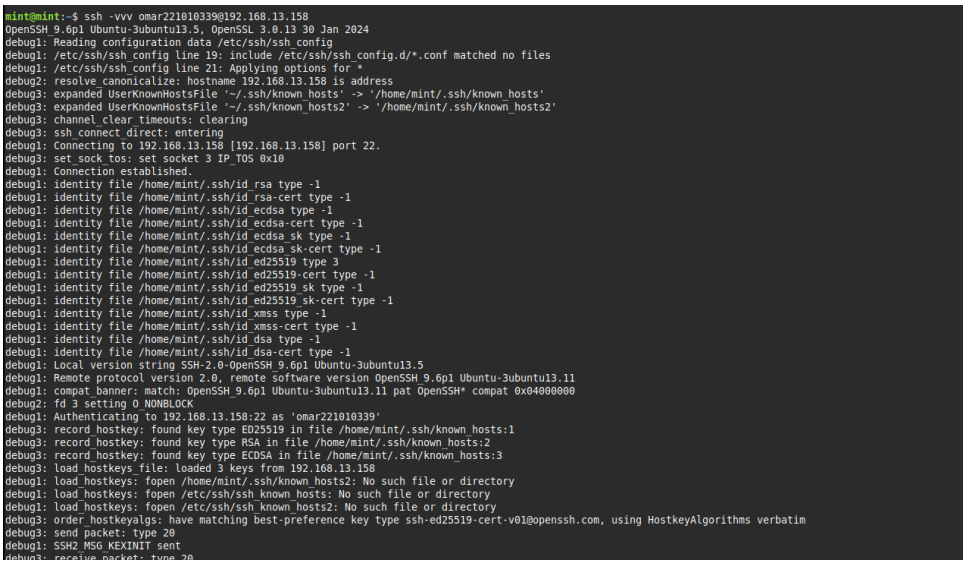
Then, SSH service was restarted: sudo systemctl restart ssh

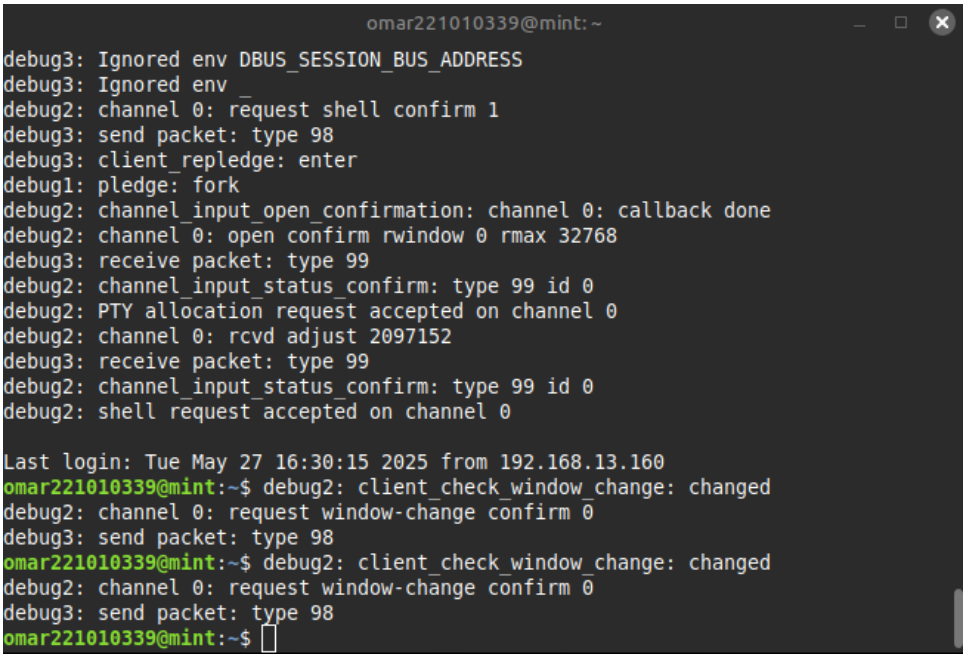
Step 8: SSH Verbose Log

To analyze the SSH connection, the following command was used:

ssh -v omar221010339@<server-ip>

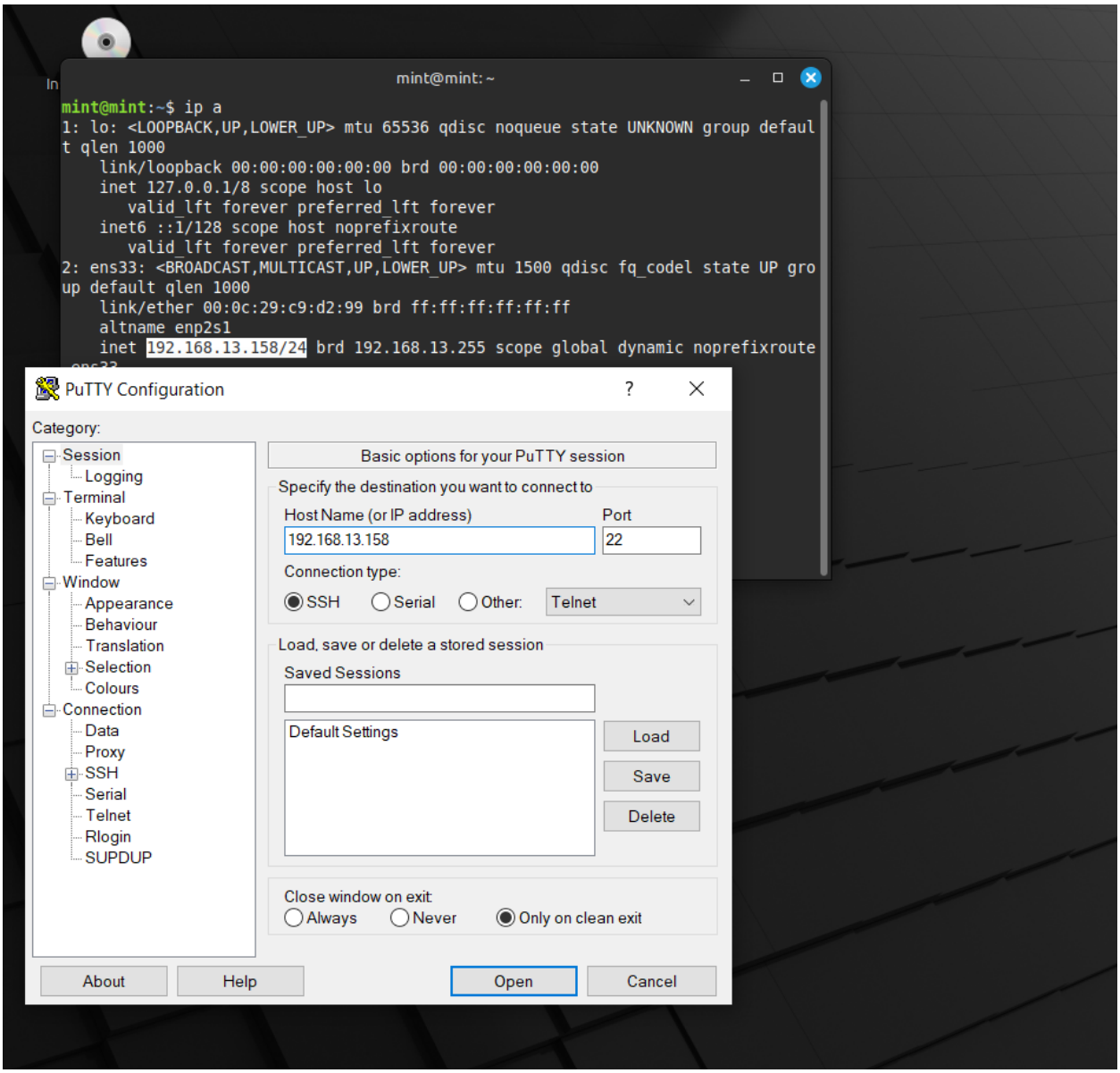
The verbose log shows stages like key exchange, authentication, and session establishment



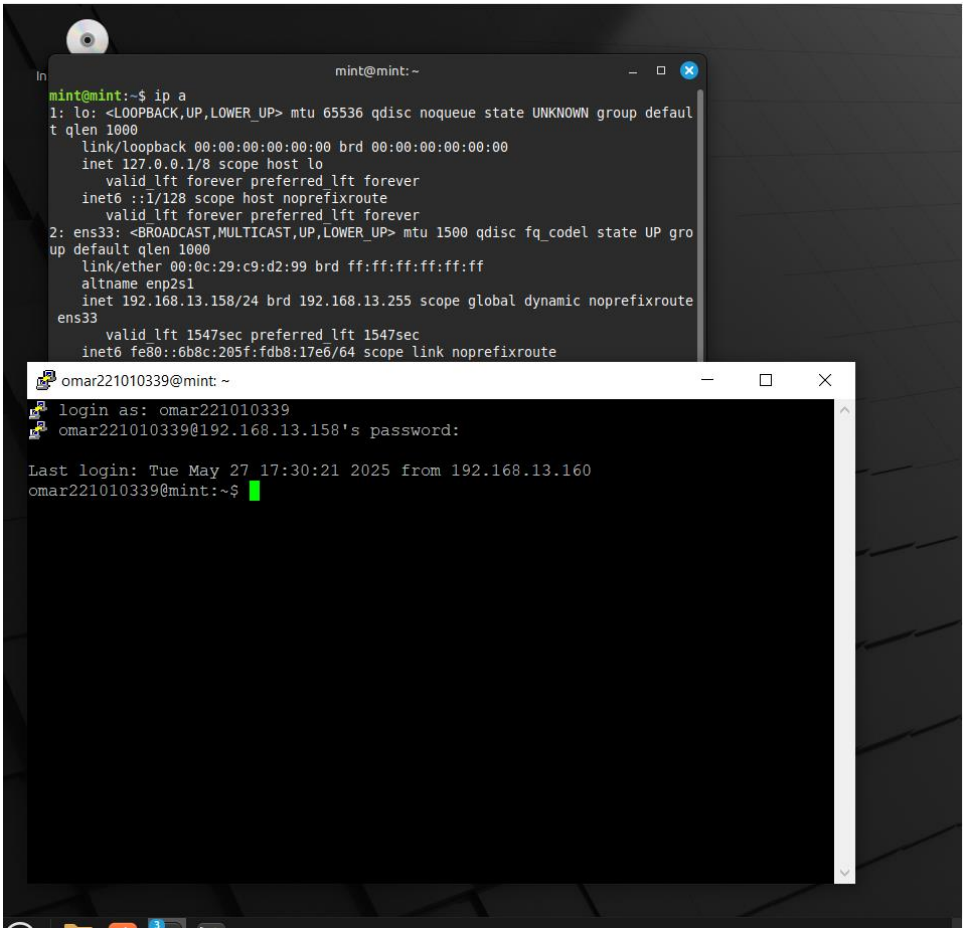


Putty configuration

First download it in windows after that know ip of server by use “ip a” then write ip in putty and port 22 and make connection type ssh then press open



After press open we found login as we write client name and password then we will be client



COMMANDS USE IN PART 2:

1-sudo apt update

2- sudo apt install openssh-server openssh-client

3-sudo systemctl enable ssh

4-sudo systemctl start ssh

5-sudo adduser omar221010339

6-ssh-keygen -t ed25519 -C "omar221010339@client"

7-ssh-copy-id omar221010339@<server-ip>

8-ssh omar221010339@<server-ip>

9-sudo nano /etc/ssh/sshd_config

10-sudo systemctl restart ssh

11-ssh -v omar221010339@<server-ip>

Server IP: <192.168.13.158>

Client IP: <192.168.13.160>

---

3. Conclusion

The SSH key-based login was successfully configured and tested. Compared to password-based authentication, key-pair login provides stronger security and avoids brute-force attacks. All steps were implemented and verified through terminal output and screenshots.