# Firewall Configuration and Testing Report

Prepared by: Mohammad Arshan Basheer Ahmed Dafedar

## 1. Objective

The objective of this task is to configure and test basic firewall rules to allow or block specific network traffic using UFW (Uncomplicated Firewall) on Linux.

## 2. Tools Used

- UFW (Uncomplicated Firewall)

- Linux Virtual Machine

- Terminal for command execution

## 3. Procedure

Step 1: Install UFW

Command: sudo apt install ufw -y

Step 2: Enable UFW

Command: sudo ufw enable

Step 3: List current firewall rules

Command: sudo ufw status verbose

Step 4: Block inbound traffic on Telnet port (23)

Command: sudo ufw deny 23

Step 5: Test the rule

Attempt to connect to port 23 locally or remotely. The connection should be blocked.

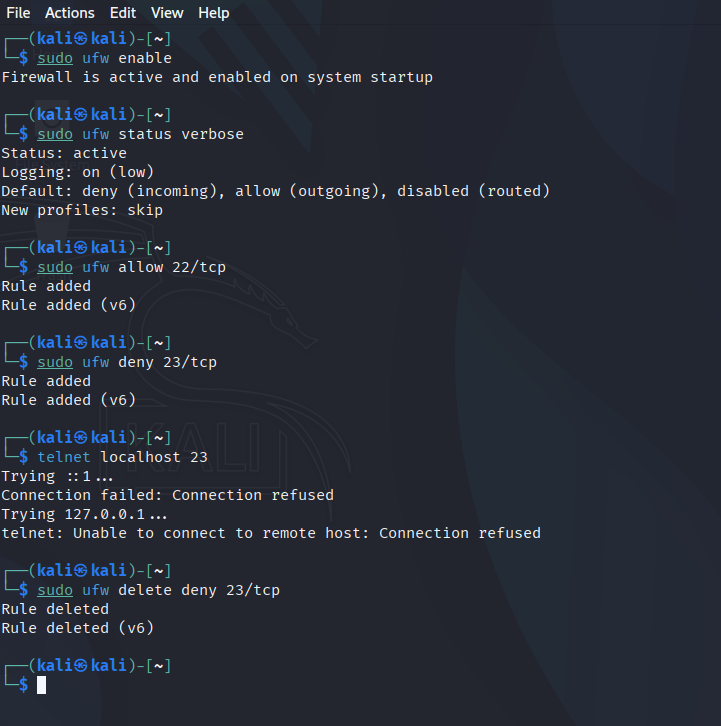
Step 6: Allow SSH traffic (port 22)

Command: sudo ufw allow 22

Step 7: Remove test block rule to restore the original state

Command: sudo ufw delete deny 23

## 4. Screenshots



## 5. Summary

The firewall acts as a security layer between the system and the network, filtering traffic based on predefined rules. Blocking port 23 successfully prevented Telnet connections, demonstrating how UFW can enforce security policies. Allowing port 22 ensured that SSH access was maintained. The test confirmed that firewall rules can be easily configured, tested, and reverted.