Firewall Configuration & Testing Report (UFW – Linux)

1. Introduction

This report explains the process of configuring, applying, and testing firewall rules in a Linux environment using UFW (Uncomplicated Firewall). The objective was to understand how firewall rules filter network traffic and to perform operations such as listing rules, blocking ports, allowing ports, and verifying rule behavior.

2. System Used

- Operating System: Linux (Ubuntu/Debian-based)
- Firewall Tool: UFW (Uncomplicated Firewall)
- Objective: Basic firewall rule creation, testing inbound/outbound behavior

3. Step-by-Step Procedure

Below are the steps performed to configure and test firewall rules using UFW. Screenshots can be inserted after each step.

Step 1: Check Firewall Status

Commands:
sudo ufw status
sudo ufw enable

Step 2: List Existing Firewall Rules

Command:
sudo ufw status numbered

Step 3: Block Inbound Traffic on Port 23 (Telnet)

Command:
sudo ufw deny 23

Step 4: Test the Block Rule

Command:
telnet 127.0.0.1 23

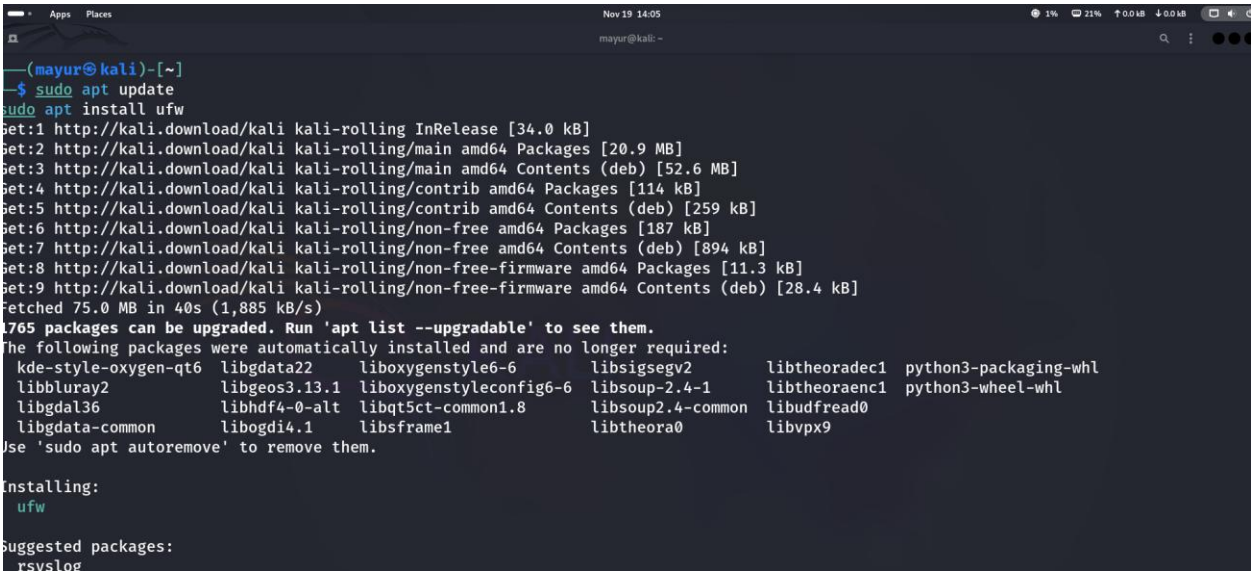
Step 5: Allow SSH (Port 22)

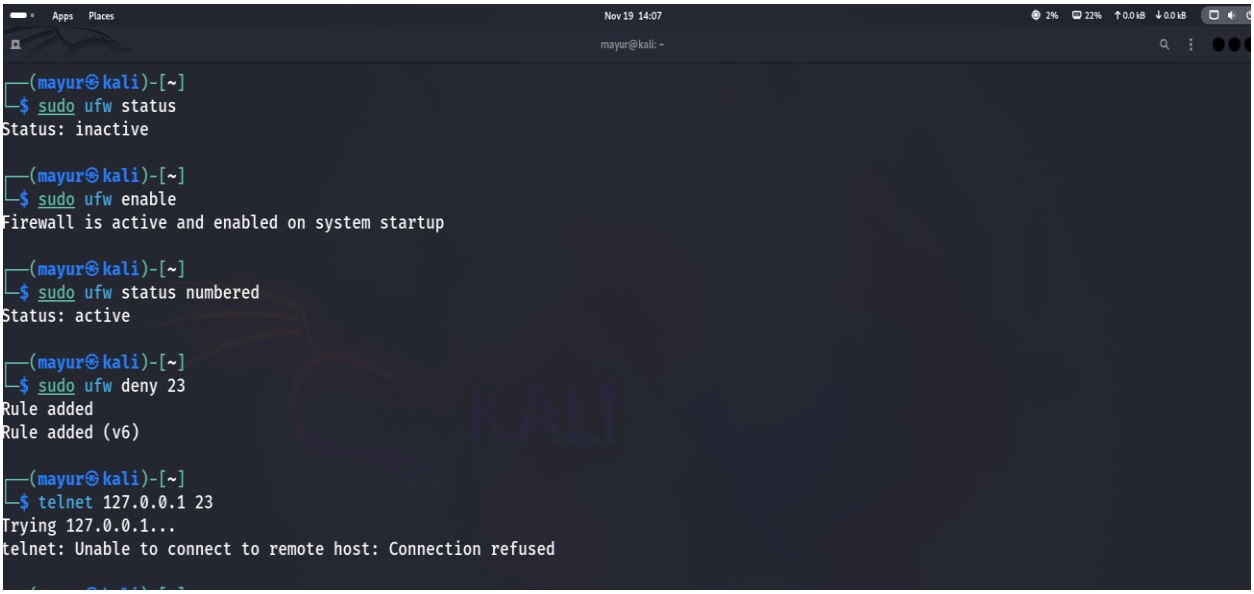
Command:
sudo ufw allow 22

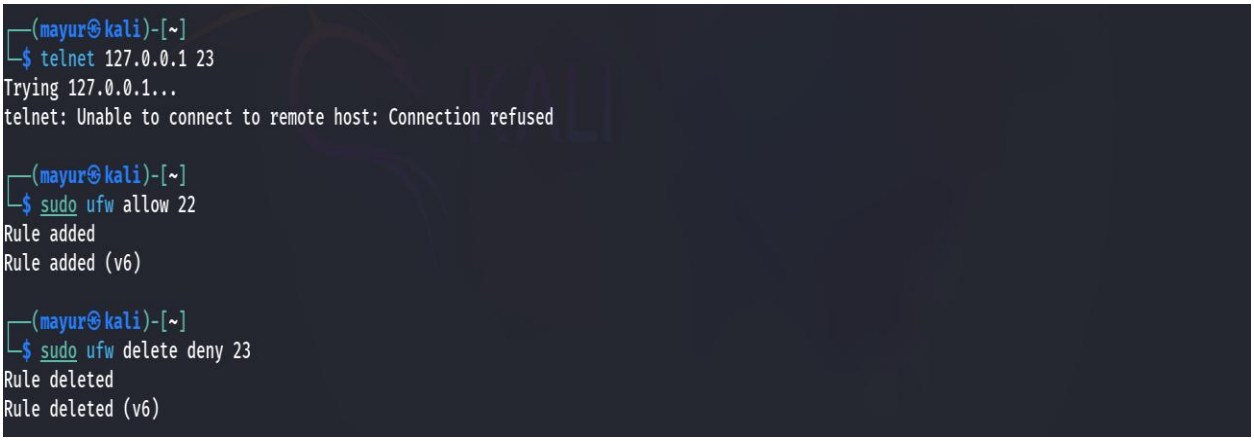
Step 6: Remove the Test Block Rule

Command:
sudo ufw delete deny 23

Screenshots:







4. Summary

A firewall filters traffic by inspecting incoming and outgoing packets and making decisions based on defined rules. UFW simplifies firewall rule creation, allowing administrators to permit or deny specific ports and services easily. This enhances system security by reducing the attack surface and controlling communication channels.

5. Conclusion

Through this task, practical experience was gained in managing UFW firewall rules. This strengthened understanding of traffic filtering, port management, and overall system security through firewall configuration.