CYBER SECURITY INTERNSHIP

# Task 4: Firewall Configuration using UFW on Kali Linux

Prepared By: Oleti Chandini

Date: 08-08-2025

## Objective

The objective of this task is to configure and manage basic firewall rules on a Linux-based system using the Uncomplicated Firewall (UFW). The task helps build practical knowledge of network traffic filtering, port management, and Linux-based system hardening.

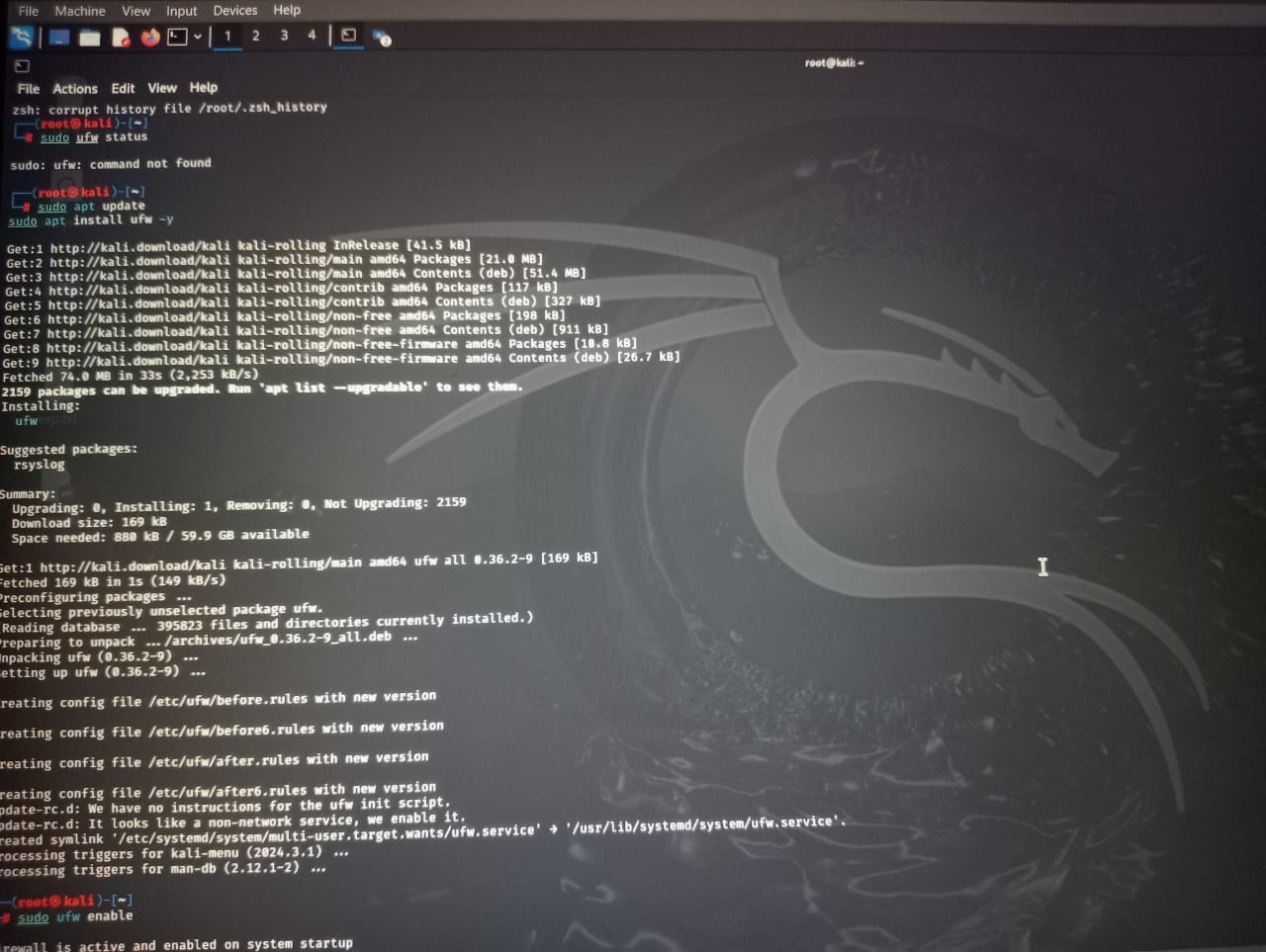
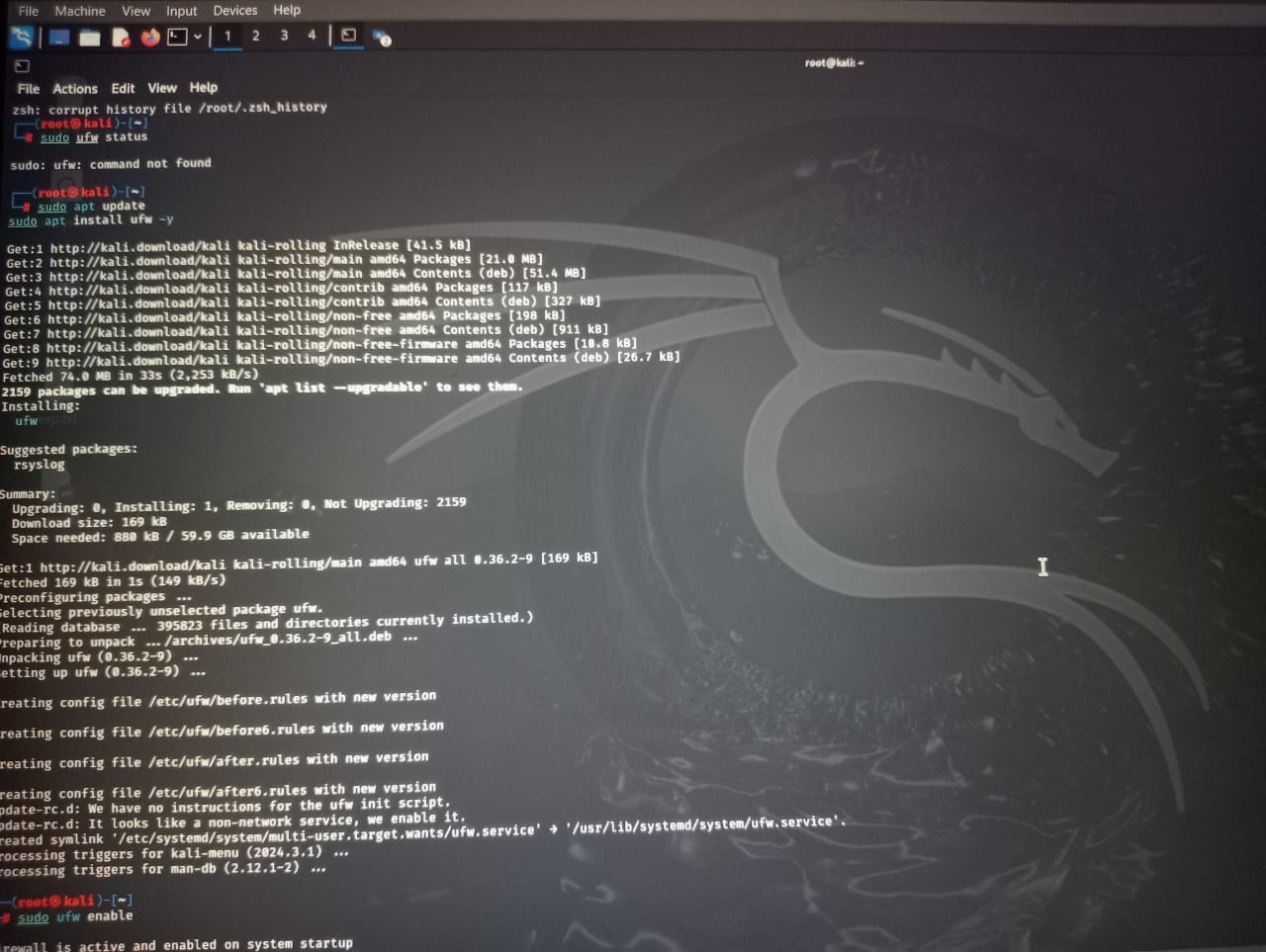
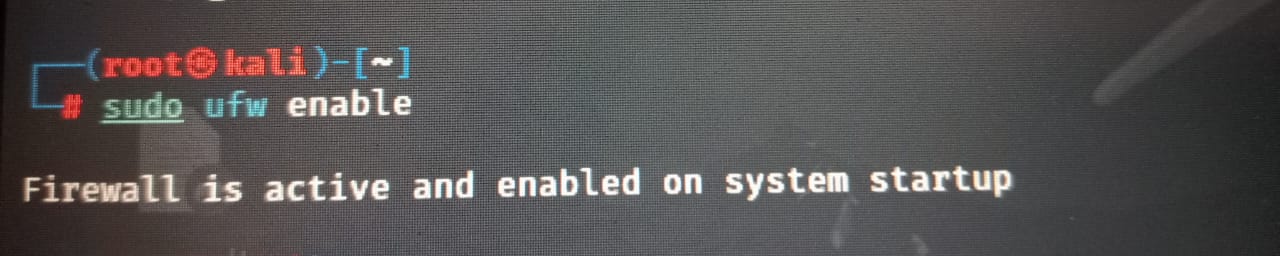
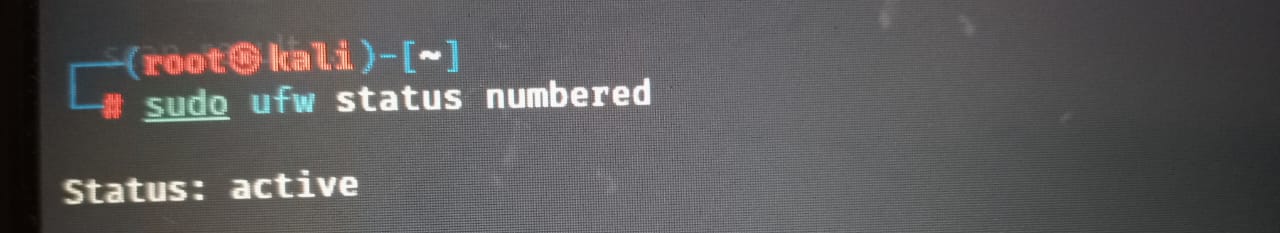
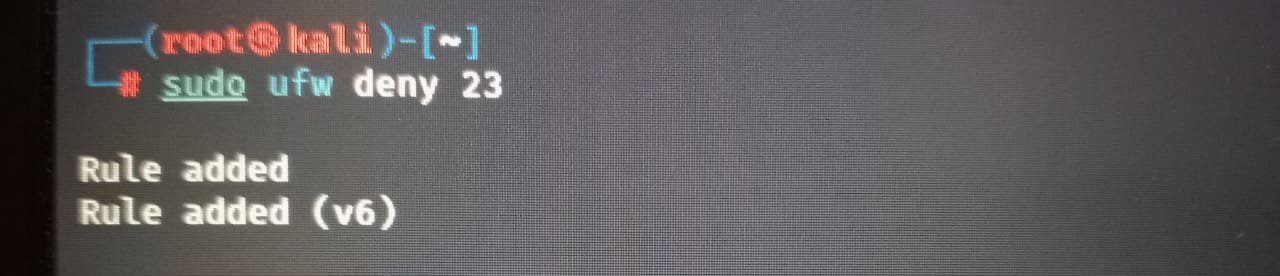
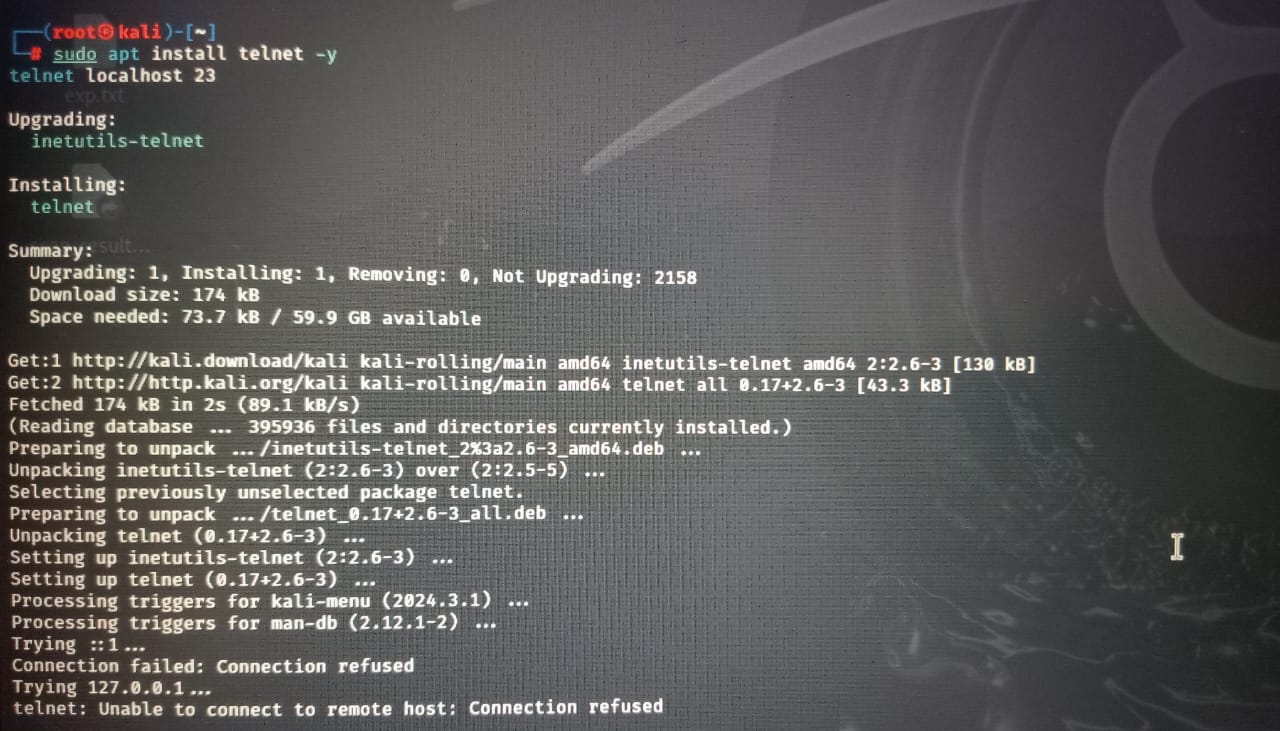
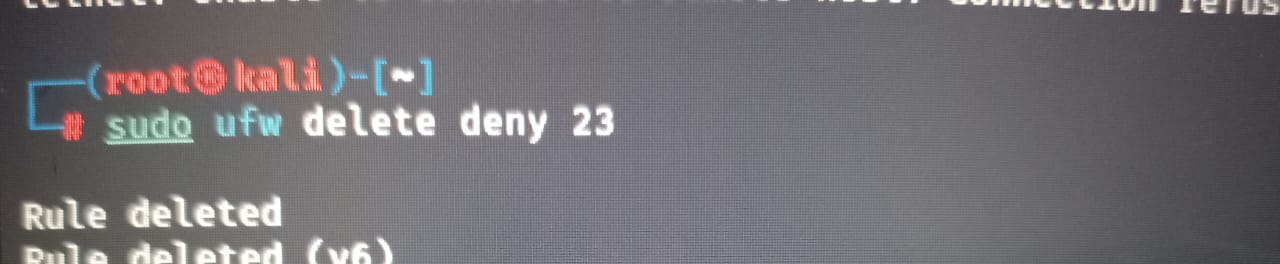
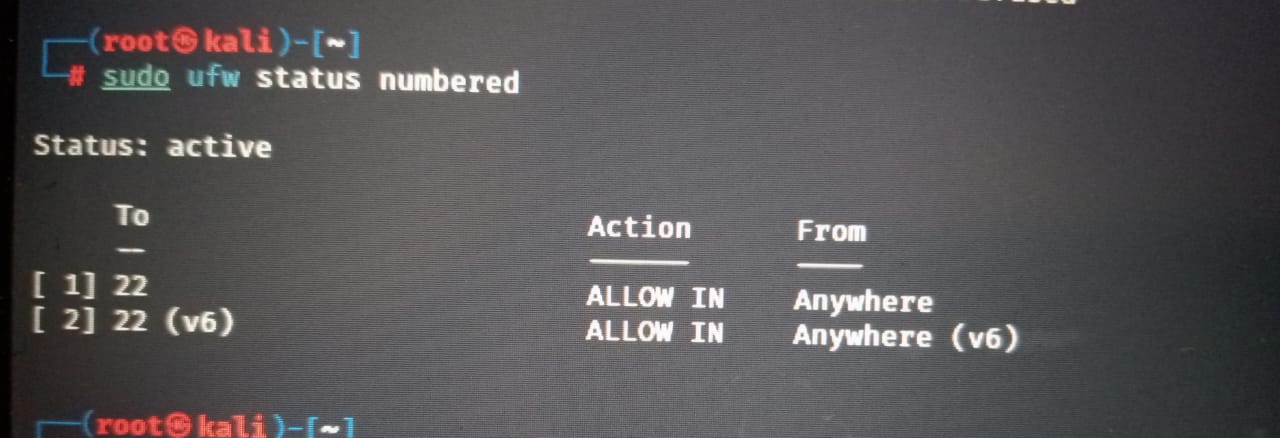
## Introduction

Firewalls play a crucial role in securing systems by filtering network traffic based on rules. In this task, the Uncomplicated Firewall (UFW), a user-friendly command-line interface for managing iptables in Linux, was used to configure basic allow and deny rules on Kali Linux. The goal was to block a vulnerable port (Telnet) and ensure secure ports like SSH are allowed.

## Tools and Environment

Tool Used: UFW (Uncomplicated Firewall)  
OS: Kali Linux  
Port Blocked: 23 (Telnet)  
Port Allowed: 22 (SSH)  
Test Tool: Telnet

## Steps Followed (Clear and Detailed)

* Step 1: Update System Repositories.
* sudo apt update
* 
* Step 2: Install UFW (Uncomplicated Firewall)
* sudo apt install ufw -y
* 
* Step 3: Enable UFW
* sudo ufw enable
* 
* Firewall is active and enabled on system startup
* Step 4: Check Firewall Status
* sudo ufw status numbered
* 
* Step 5: Block Inbound Traffic on Port 23 (Telnet)
* sudo ufw deny 23
* 
* Step 6: Allow Inbound SSH (Port 22)
* sudo ufw allow 22
* 
* Step 7: Install Telnet for Testing
* sudo apt install telnet -y
* 
* Step 8: Remove the Test Rule (Cleanup)
* sudo ufw delete deny 23
* 
* Rule deleted and Rule deleted (v6)
* Step 9: Final Status Check
* sudo ufw status numbered
* 

## Test Output Summary

After blocking port 23, the system was tested using telnet. The result showed 'connection refused', confirming that the firewall rule was working. The SSH port (22) remained accessible, ensuring remote management was still possible.

## Learning Outcomes

- Learned to install and use UFW on a Linux system.  
- Understood how to apply, list, and delete firewall rules.  
- Identified the importance of blocking insecure ports like Telnet.  
- Gained confidence in using command-line tools for system hardening.

## Conclusion

This task provided practical experience with Linux-based firewall management. By configuring and testing rules using UFW, I gained a deeper understanding of how network ports can be controlled to protect systems from unauthorized access. This skill is essential for cybersecurity professionals in both offensive and defensive roles.