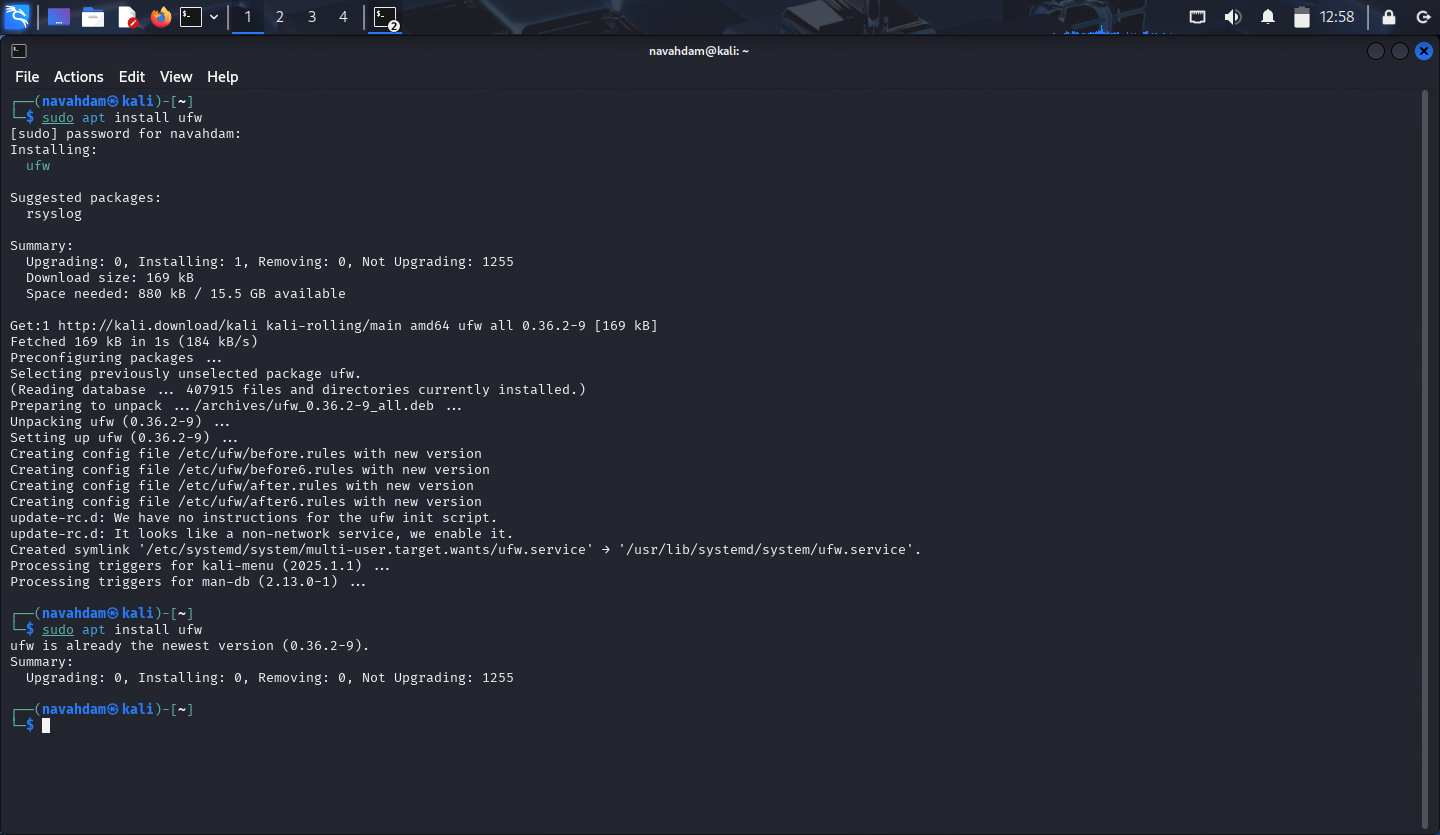
Objective

Configure and test basic firewall rules to allow or block traffic.

Tools used

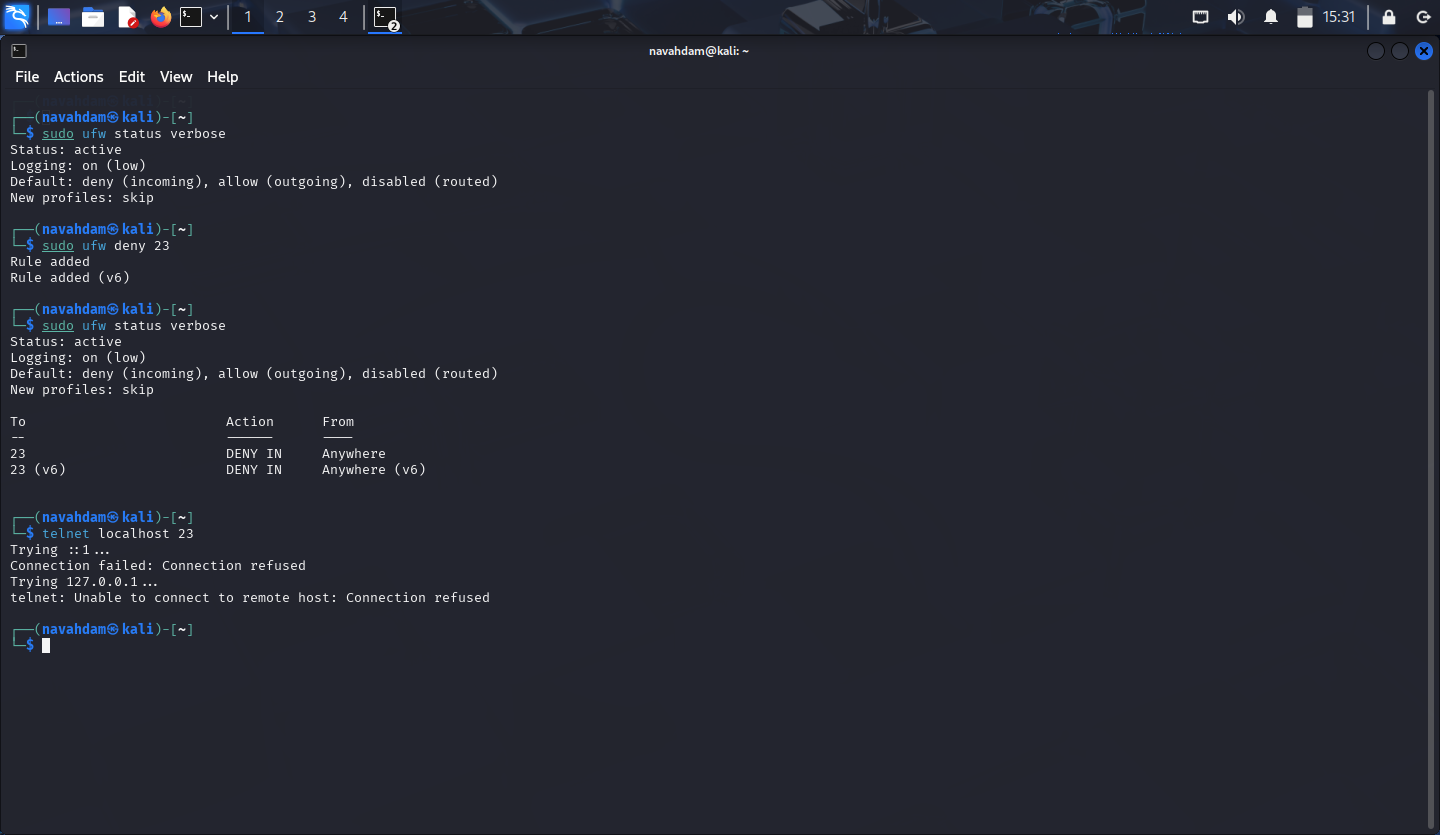
**UFW (Uncomplicated Firewall)** is a **user-friendly command-line tool** for managing a Linux firewall. It is a front-end for **iptables**, designed to make firewall configuration **simpler** and **easier** for users.



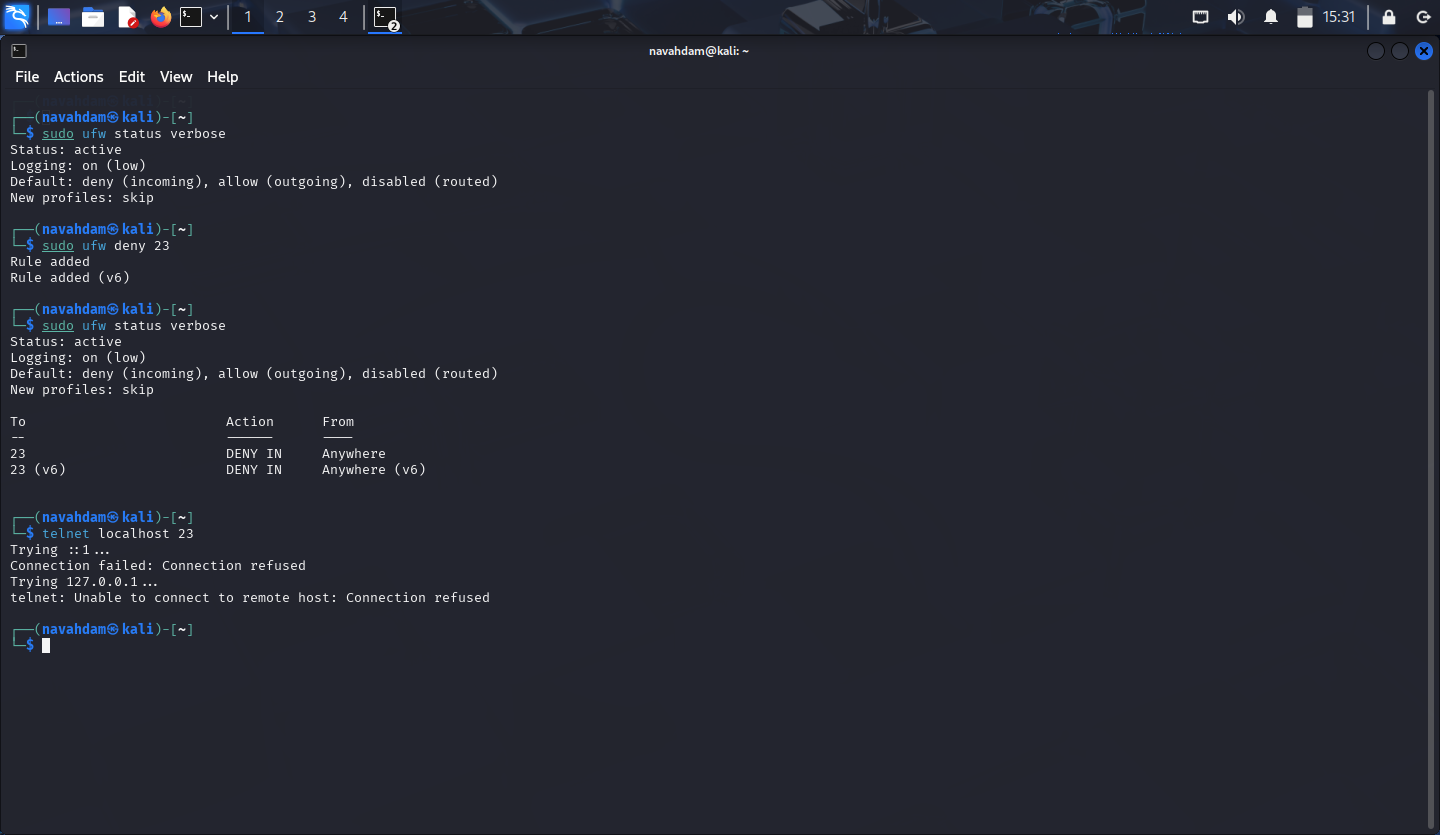
Firewall setup

Commands:

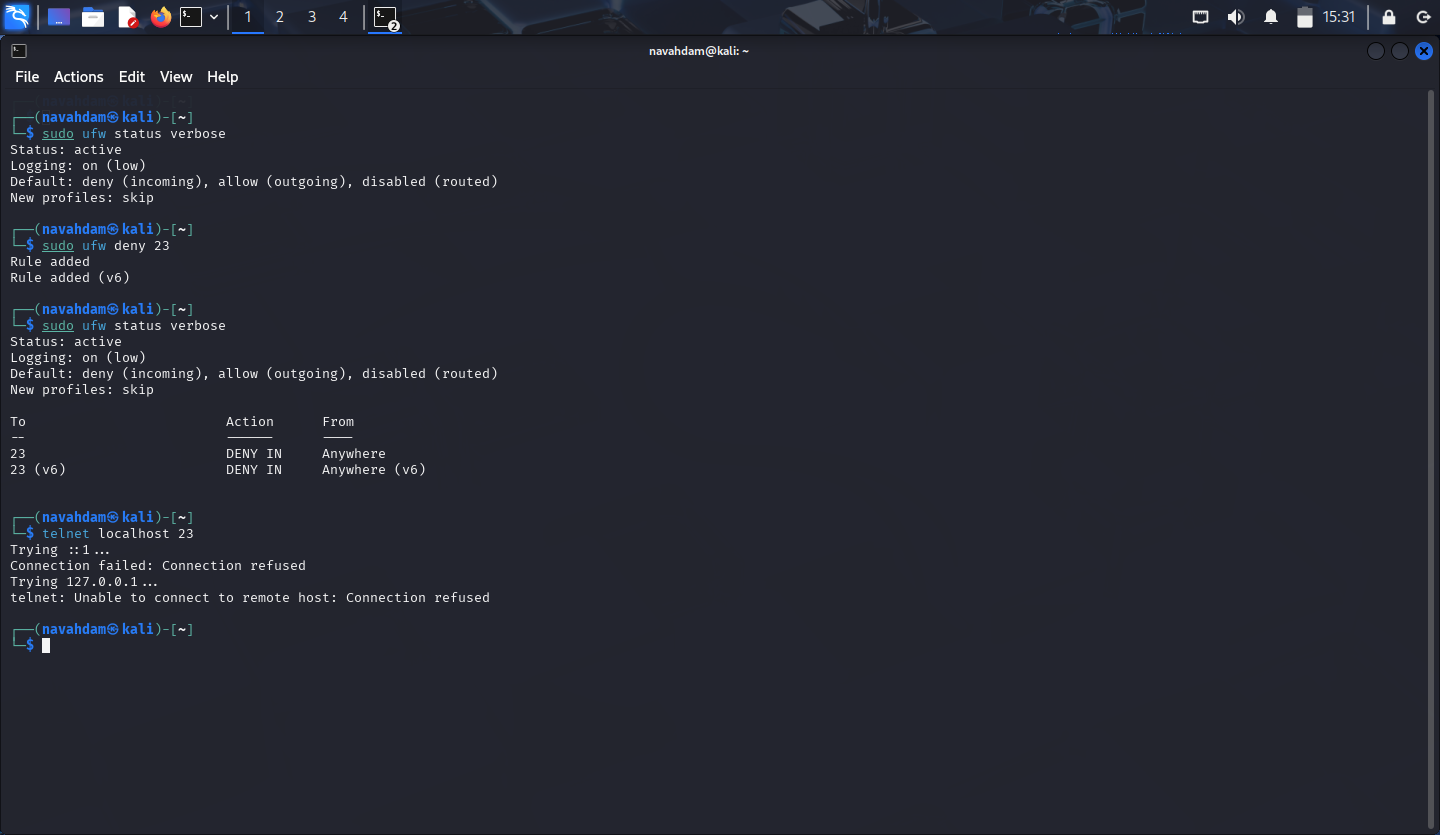
* Status of the firewall in the beginning:



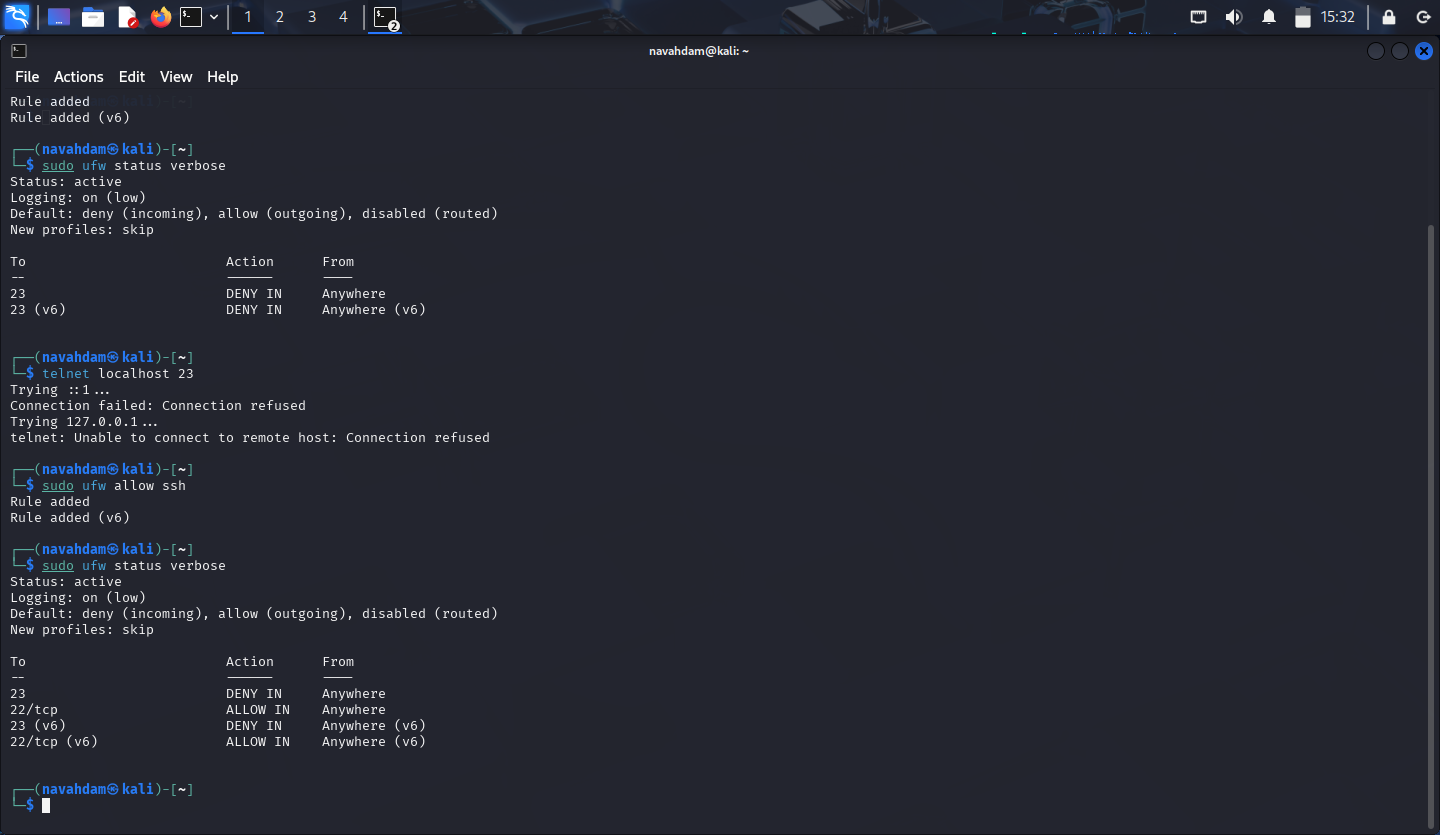
* Added a rule to block port 23(telnet) :



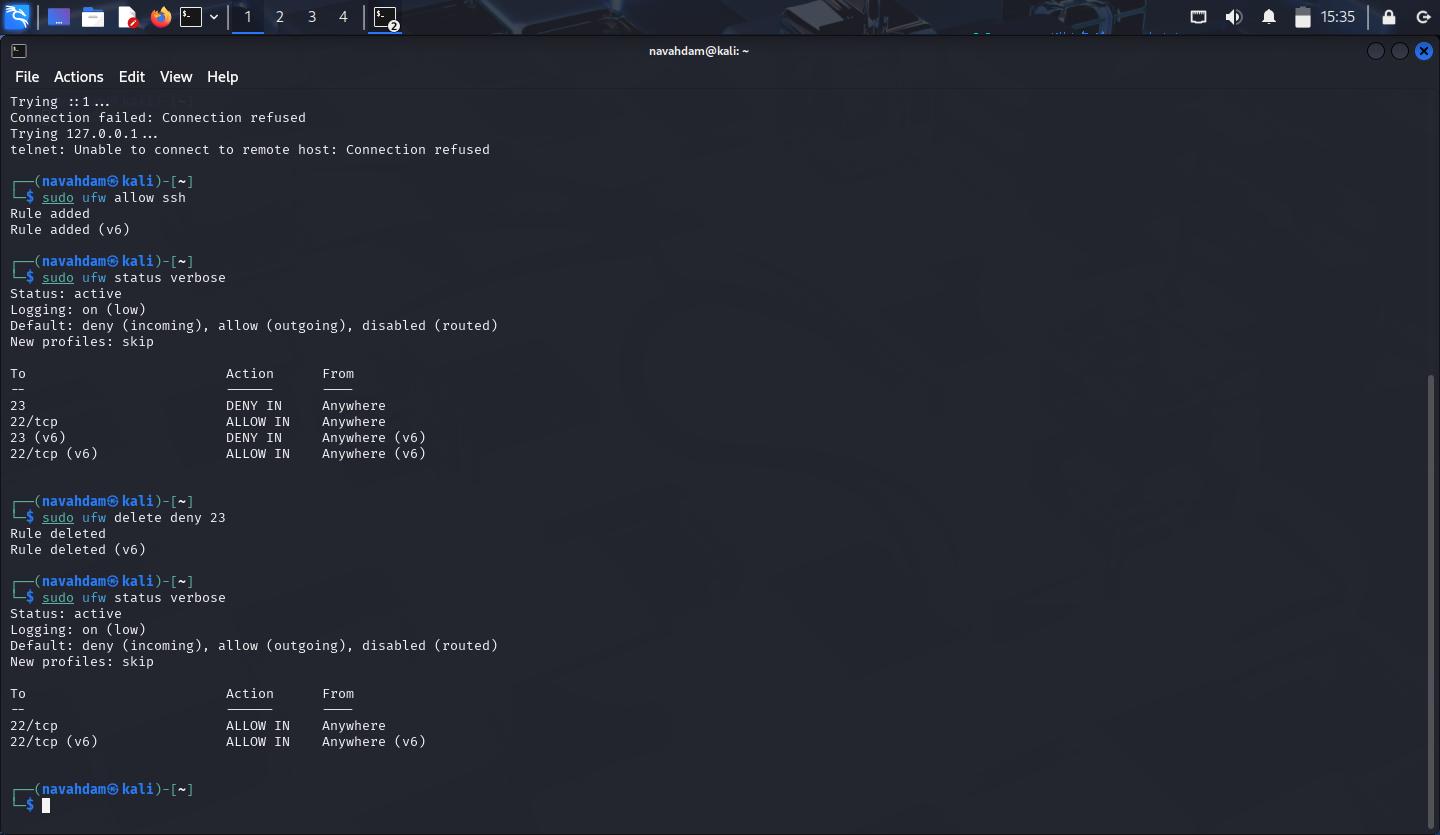
* Tested the rule:



* Added a rule to allow ssh(port 22):



* Removed the test block rule to restore original state:



Summary

A **firewall filters network traffic** by checking each data packet against a set of **rules**. Based on these rules, it decides to **allow** or **block** the traffic.

* **Inbound rules** control what comes **into** your system.
* **Outbound rules** control what goes **out**.

Rules are based on things like:

* **Port numbers** (e.g., 22 for SSH)
* **IP addresses**
* **Protocols** (TCP/UDP)

Example: Blocking port 23 prevents Telnet access for security.