# Task 4 – Firewall Configuration using UFW (Kali Linux)

## Objective:

Configure and test a basic firewall using UFW on Kali Linux. Block Telnet (port 23), allow

## Tools Used:

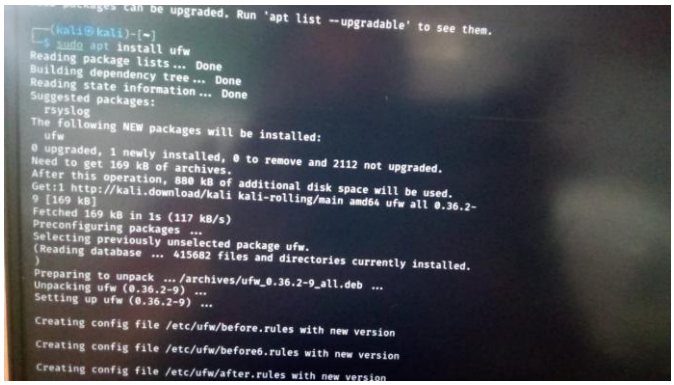
- Kali Linux

- UFW (Uncomplicated Firewall)

## Steps Performed:

1. Installed UFW

```bash
sudo apt update
sudo apt install ufw
```




2.Enabled the Firewall

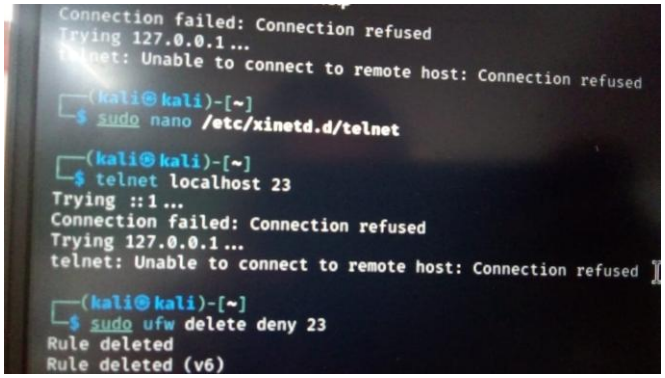
```bash
sudo ufw enable
```

3.Checked Current Firewall Rules

```bash
sudo ufw status verbose
```

4. Blocked Inbound Traffic on Port 23 (Telnet)

```bash
sudo ufw deny 23
```

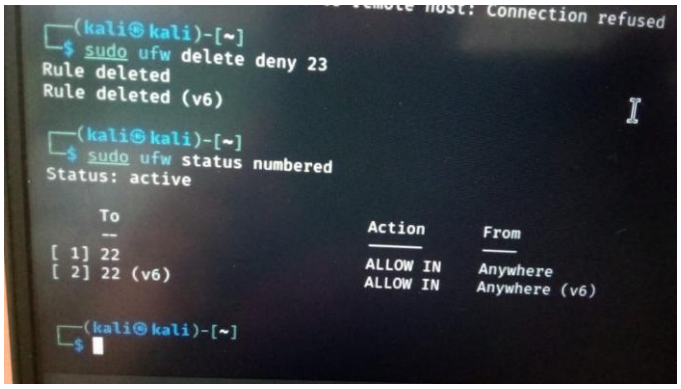



5.Allowed SSH Port (22)

```bash
sudo ufw allow 22
```

6.Verified Rules Applied

```bash
sudo ufw status numbered
```




<u>Expected Output:</u>

To Action From

-- ------ ----

22 ALLOW Anywhere

23 DENY Anywhere

7.Tested Blocked Port with Telnet

```bash
telnet localhost 23
```

Result:

Connection refused

⚠️ If telnet is not installed:

```bash
sudo apt install telnet
```

Removed the Block Rule

```bash
sudo ufw delete deny 23
```

**Summary: How Firewall Filters Traffic**

A firewall acts like a gatekeeper, inspecting incoming and outgoing traffic based on predefined rules. It filters traffic by:

- Allowing traffic on trusted ports (like **SSH on port 22**)

- Blocking insecure or unwanted traffic (like **Telnet on port 23**)

- Preventing unauthorized access to sensitive services

- Ensuring only permitted connections are allowed

In this task, UFW (Uncomplicated Firewall) was used to apply and verify rules that control which traffic is allowed or blocked, thus improving system security.