TASK 4: Firewall Configuration (UFW –Linux)

1. Introduction

This report outlines the steps taken to configure, implement, and test firewall rules on a Linux system using UFW (Uncomplicated Firewall). The goal was to gain insight into how firewall rules regulate network traffic and to carry out tasks such as viewing existing rules, blocking specific ports, allowing ports, and verifying how these rules function.

2. System Used

- Operating System: Linux (Ubuntu/Debian-based)
- Firewall Tool: UFW (Uncomplicated Firewall)
- Objective: Configure and test basic firewall rules to allow or block traffic.

3. Step-by-Step Procedure

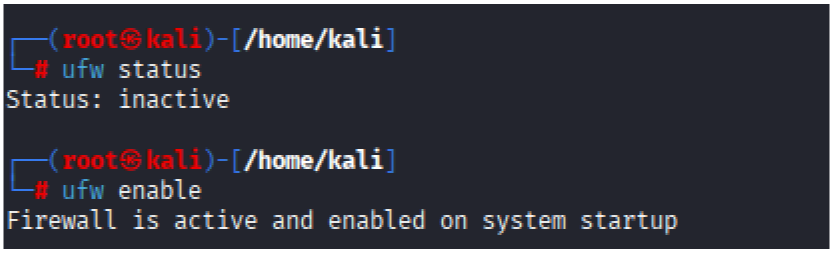
Below are the steps performed to configure and test firewall rules using UFW. Screenshots are inserted after each step.

Step 1: Check Firewall Status

Commands:

ufw status

ufw enable

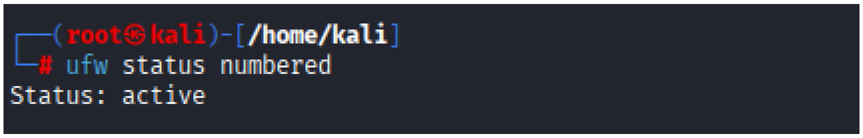


```
┌──(root㉿kali)-[/home/kali]
└─# ufw status
Status: inactive

┌──(root㉿kali)-[/home/kali]
└─# ufw enable
Firewall is active and enabled on system startup
```

Step 2: List Existing Firewall Rules

Command:

ufw status numbered

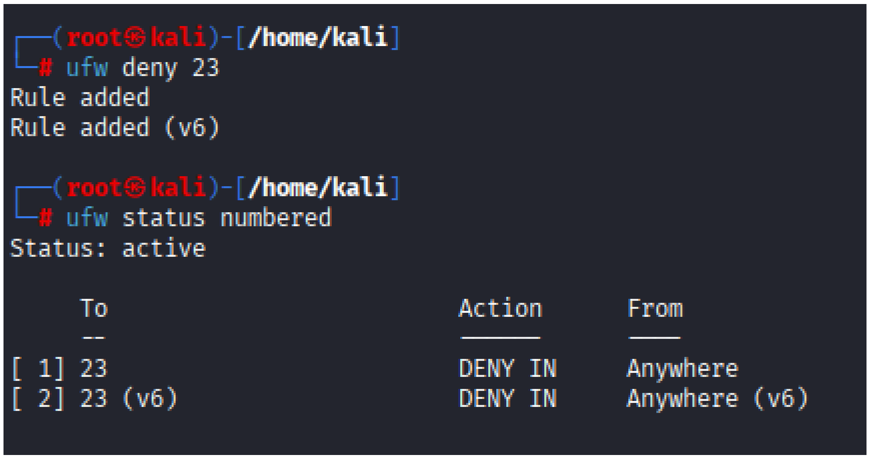


```
┌──(root㉿kali)-[/home/kali]
└─# ufw status numbered
Status: active
```

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

Command:

ufw deny 23

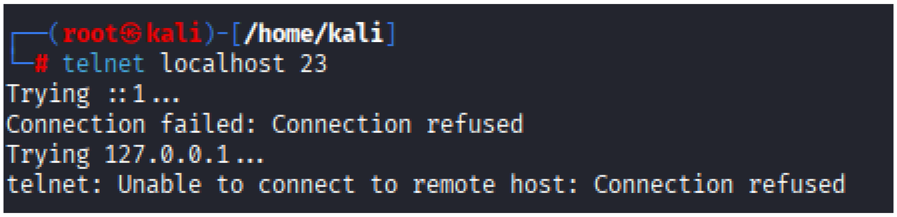


```
┌──(root㉿kali)-[/home/kali]
└─# ufw deny 23
Rule added
Rule added (v6)

┌──(root㉿kali)-[/home/kali]
└─# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 23 (v6)                    DENY IN     Anywhere (v6)
```

Step 4: Test the Block Rule

Command:

telnet localhost 23

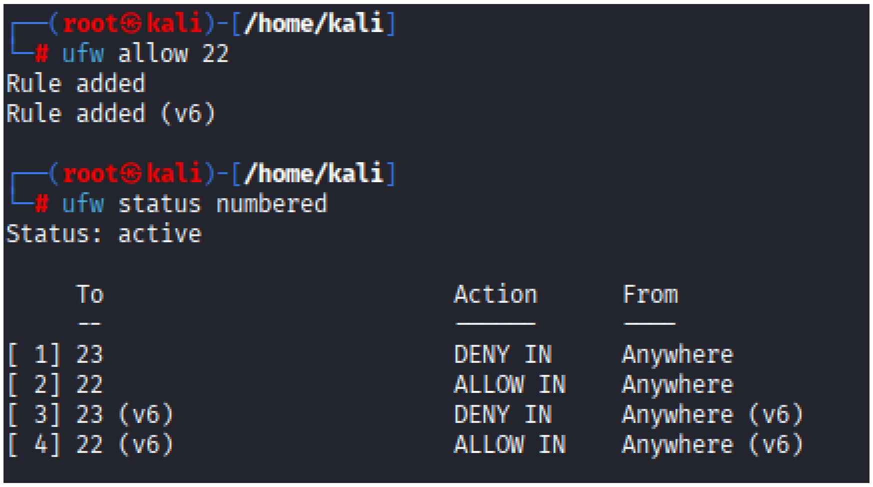


```
┌──(root㉿kali)-[/home/kali]
└─# telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

Step 5: Allow SSH (Port 22)

Command:

ufw allow 22

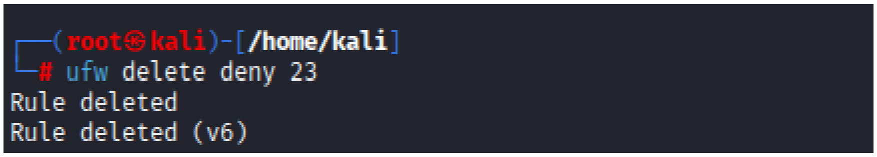


```
┌──(root㉿kali)-[/home/kali]
└─# ufw allow 22
Rule added
Rule added (v6)

┌──(root㉿kali)-[/home/kali]
└─# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 23 (v6)                    DENY IN     Anywhere (v6)
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
```

Step 6: Delete the Test Block Rule

Command:

ufw delete deny 23



```
┌──(root㉿kali)-[/home/kali]
└─# ufw delete deny 23
Rule deleted
Rule deleted (v6)
```

4. Summary

A firewall manages network traffic by examining packets entering or leaving a system and making decisions based on predefined rules. UFW streamlines the creation and management of these rules, enabling administrators to easily allow or restrict access to certain ports and services. This improves system security by limiting unnecessary exposure and tightening control over communication channels.

5. Conclusion

Completing this activity provided hands-on experience with configuring UFW firewall rules. It enhanced understanding of how traffic filtering works, how ports are managed, and how firewall settings contribute to strengthening overall system security.