Cybersecurity Internship Report — Task 4

Intern Name: Sai Aditya
Organization: Elevate Labs
Task Title: Setup and Use a Firewall on Kali Linux (UFW)
Date: August 8, 2025

Objective

To configure and test basic firewall rules using UFW (Uncomplicated Firewall) on Kali Linux in order to manage network traffic filtering. The focus was on allowing secure services and blocking legacy/insecure ports such as Telnet.

Tools Used

- Operating System: Kali Linux 2024.2
- Firewall Tool: UFW (Uncomplicated Firewall)
- Terminal Used: GNOME Terminal
- Target IP: 192.168.150.133

Scenario

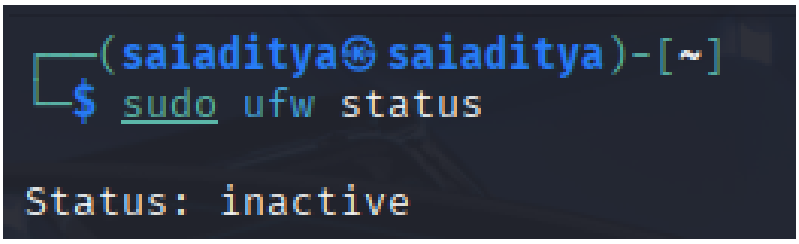
A Kali Linux system is connected to a local network and has SSH service enabled. As part of basic hardening, I applied firewall rules using UFW to block inbound traffic to Telnet (port 23), while allowing SSH (port 22) for remote management. After configuring the firewall, I verified the rules and removed the Telnet block to restore the original state.

Disclaimer ⚠️

This project was completed as part of a cybersecurity internship at Elevate Labs and is intended solely for educational and training purposes. All firewall configurations, IP addresses, and procedures were performed in a controlled environment on local or simulated systems.
No unauthorized testing or exploitation was conducted on any external or third-party networks.

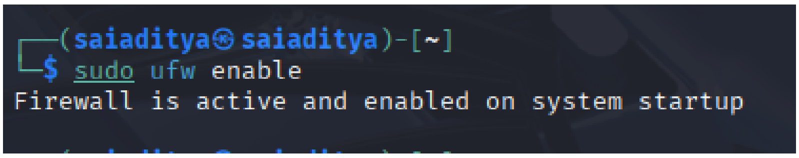
Commands Executed

sudo ufw status



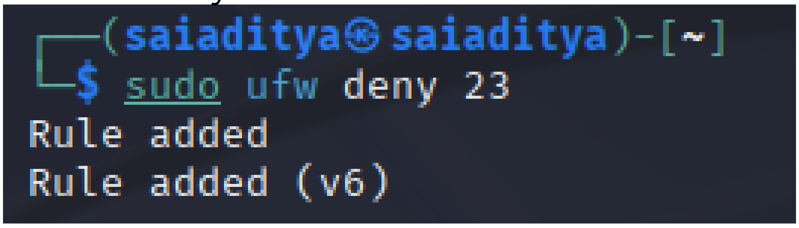
```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw status

Status: inactive
```

sudo ufw enable



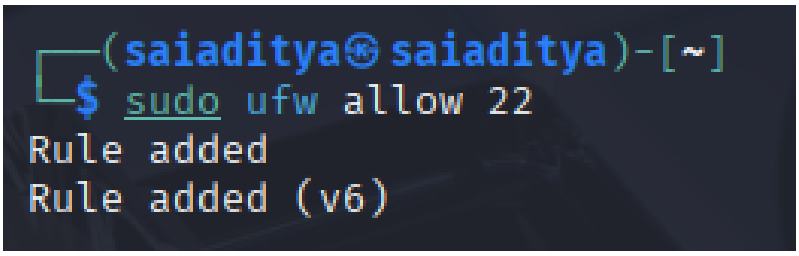
```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

sudo ufw deny 23



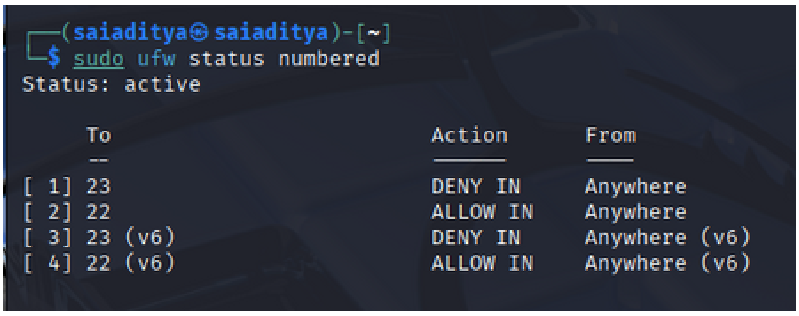
```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)
```

sudo ufw allow 22



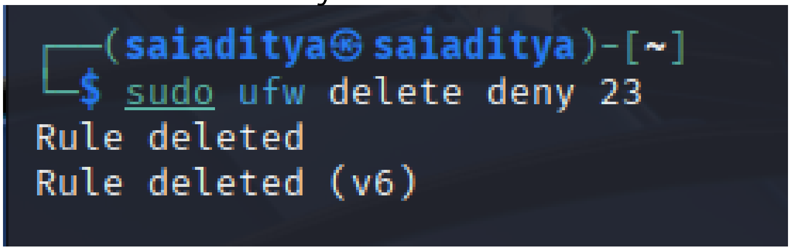
```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)
```

sudo ufw status numbered



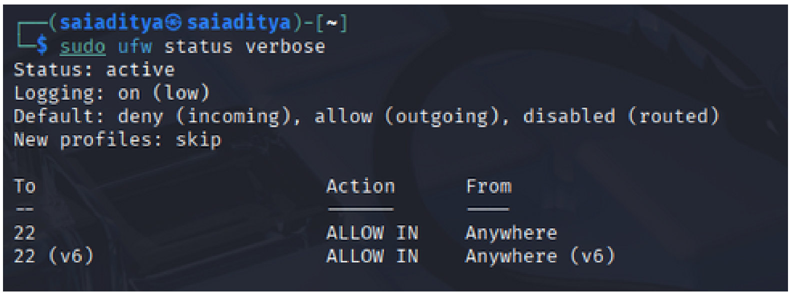
```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw status numbered
Status: active

     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)
```

sudo ufw delete deny 23



```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)
```

sudo ufw status verbose



```
┌──(saiaditya㉿saiaditya)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
```

Firewall Rule Summary

Action	Port	Service	Status
Deny incoming	23	Telnet	Applied
Allow incoming	22	SSH	Applied
Remove rule	23	Telnet	Reverted

Key Learnings

UFW provides an intuitive interface for managing firewall rules on Linux. Blocking legacy protocols like Telnet helps reduce the attack surface. Testing each rule ensures critical services like SSH remain unaffected. Understanding stateful firewall behavior improves system-level defense skills.