Internship Report

Name: Divyanshu Singh

Topic: Firewall Configuration and Testing using UFW (Linux)

* **Tool/OS Used:** Ubuntu Linux (UFW - Uncomplicated Firewall)
* Telnet Client

Date: 27/06/2025

# Objective

To understand how to configure firewall rules in Linux using UFW (Uncomplicated Firewall), specifically to block Telnet (port 23), allow SSH (port 22), and test the rules through command-line tools.

# Procedure

## Step 1: Enable UFW

Command: sudo ufw enable

## 

## Step 2: Check Current Rules

Command: sudo ufw status numbered

## 

## Step 3: Block Port 23 (Telnet)

Command: sudo ufw deny 23

## 

## Step 4: Test with Telnet

Command: telnet localhost 23

## 

## Step 5: Allow SSH (Port 22)

Command: sudo ufw allow 22

## 

## 6: Delete the Block Rule (Restore)

Command: sudo ufw delete deny 23

## Step 7: Final Status Check

Command: sudo ufw status numbered

# 

# Commands Summary

sudo apt install ufw  
sudo ufw enable  
sudo ufw status numbered  
sudo ufw deny 23  
telnet localhost 23  
sudo ufw allow 22  
sudo ufw delete deny 23  
sudo ufw status numbered

# Conclusion

This task helped me understand basic Linux firewall management using UFW. I learned how to block and allow ports, test services using telnet, and manage firewall rules. Blocking unused ports like Telnet (23) helps enhance security, while allowing only required services like SSH (22) ensures secure access.