### **Objective**

To configure and test basic firewall rules using UFW to control network traffic by allowing or blocking specific ports.

### **Steps Performed**

**Opened Firewall Configuration Tool** Accessed the terminal.

Ensured UFW was installed:  
  
 sudo apt install ufw

Enabled UFW:  
  
 sudo ufw enable

**Listed Current Firewall Rules** sudo ufw status numbered

**Blocked Inbound Traffic on Port 23 (Telnet)**  sudo ufw deny 23

**Tested the Rule** Used telnet to attempt a connection:  
  
 telnet localhost 23

Result: Connection was refused, confirming that port 23 was blocked successfully.

**Allowed SSH on Port 22**  sudo ufw allow 22

**Removed the Block Rule on Port 23**  sudo ufw delete deny 23

**Documented Commands Used**

* + All commands were executed in the terminal.
  + See screenshots/configuration file for proof (attached separately if required).

**Summary of How Firewall Filters Traffic**

* + UFW uses rules to allow or deny network traffic based on port numbers and protocols.
  + Traffic filtering ensures only authorized communication is allowed, enhancing system security.
  + Rules can be listed, modified, and removed dynamically.

### **Commands Summary**

| **Action** | **Command** |
| --- | --- |
| Enable UFW | sudo ufw enable |
| Check Status | sudo ufw status numbered |
| Block Port 23 | sudo ufw deny 23 |
| Allow SSH (Port 22) | sudo ufw allow 22 |
| Remove Block on Port 23 | sudo ufw delete deny 23 |