Task 4: Setup and Use a Firewall on Linux (UFW)

# Objective:

Configure and test basic firewall rules to allow or block traffic using UFW on Linux.

# Tools Used:

- UFW (Uncomplicated Firewall)  
- Telnet  
- Netcat (for testing)

# Steps Performed:

1. Installed UFW using the command:  
 sudo apt install ufw

2. Enabled UFW:  
 sudo ufw enable

3. Listed current firewall rules:  
 sudo ufw status verbose

4. Added a rule to block port 23 (Telnet):  
 sudo ufw deny 23

5. Verified the block by attempting to connect using telnet:  
 telnet localhost 23

6. Allowed SSH on port 22 to ensure continued access:  
 sudo ufw allow 22

7. Removed the test block rule:  
 sudo ufw delete deny 23

8. Listed current firewall rules again to confirm changes:  
 sudo ufw status numbered

# Summary:

UFW was successfully configured to manage basic firewall rules. Port 23 was blocked and tested using Telnet. The system demonstrated how UFW filters traffic based on rules and helps protect against unwanted connections. This task provided hands-on experience with Linux firewall management.

