Task 4: Cyber security Internship – Firewall Configuration Report

Objective:

To configure and test basic firewall rules that allow or block traffic using UFW on Linux and Windows Firewall on Windows. This task demonstrates basic firewall management skills and an understanding of network traffic filtering.

Part 1: Linux (UFW) Firewall Configuration

Commands Used:

- sudo ufw enable
- sudo ufw status
- sudo ufw status numbered
- sudo ufw deny 23
- sudo ufw allow 22
- sudo ufw delete deny 23
- sudo ufw disable
- sudo ufw reset

Part 2: Windows Firewall Configuration (Command Line)

Step-by-Step via CMD or PowerShell (Run as Administrator):

- Enable Telnet Client (needed for testing):
  dism /online /Enable-Feature /FeatureName:TelnetClient
- Test Telnet Connection on Port 23:
  telnet localhost 23
  (Expected: Connection will fail if port 23 is blocked)
- Create Rule to Block Inbound TCP Traffic on Port 23:
  netsh advfirewall firewall add rule name="Block Telnet Port 23" dir=in action=block protocol=TCP localport=23
- Verify the Rule Exists:
  netsh advfirewall firewall show rule name=all | findstr "Block Telnet Port 23"
- Delete the Rule After Testing:
  netsh advfirewall firewall delete rule name="Block Telnet Port 23"

Outcome:

Successfully blocked and tested port 23 (Telnet) on both Linux and Windows.
Allowed port 22 (SSH) on Linux for secure remote access.
Demonstrated ability to manage basic firewall configurations via CLI tools on both platforms.