Task 4 – Setup and Use a Firewall (Windows)

Overview
This report demonstrates the configuration and testing of basic firewall rules on a Windows system as part of a Cyber Security Internship. The task focuses on understanding how firewalls filter network traffic by allowing or blocking connections based on security rules.

Objective
• Configure Windows Firewall rules
• Block insecure inbound traffic (Port 23 – Telnet)
• Test firewall behavior
• Restore firewall to original state
• Document the process

Tools Used
• Windows Defender Firewall
• PowerShell / Command Prompt
• Visual Studio Code
• GitHub

Procedure
1. Verified firewall status using netsh commands.
2. Listed existing firewall rules.
3. Created an inbound rule to block TCP Port 23 (Telnet).
4. Tested the rule to confirm traffic was blocked.
5. Removed the test rule to restore system state.

Why Port 23 Was Blocked
Telnet transmits data in plain text, making it vulnerable to interception. Blocking port 23 improves system security by preventing unauthorized access.

Outcome
Gained practical experience in firewall configuration, traffic filtering, and system security management.

Author
Jahanavi Pohar
Cyber Security Intern