Cybersecurity Internship Task 4 Report

This report documents the steps taken to complete Task 4 of the Cybersecurity Internship program, which focused on setting up and using a firewall on a Windows 11 system. The main goal was to understand how to allow or block network traffic based on port configurations, thereby learning basic firewall management and network traffic filtering.

Objective:
- Block Port 23 (Telnet) to prevent insecure remote access.
- (Optional) Allow Port 22 (SSH) for secure remote access.
- Learn to create, view, and delete firewall rules using the Windows Defender Firewall.
- Understand the security implications of port management.

Tools Used:
- Windows 11
- Windows Defender Firewall with Advanced Security
- (Optional) PowerShell or Command Prompt

Steps Performed:
1. Opened Windows Defender Firewall with Advanced Security via 'wf.msc'.
2. Navigated to 'Inbound Rules' and created a new rule to block TCP Port 23 (Telnet).
3. Optionally created a rule to allow TCP Port 22 (SSH).
4. Verified the rules were created.
5. Deleted the Telnet block rule to restore original state.
6. Took screenshots at each step.

Port Explanation:
- **Telnet (Port 23):** Insecure protocol that transmits data in plain text. Blocking this port prevents unauthorized access.
- **SSH (Port 22):** Secure protocol for encrypted remote access. It is generally safe to allow this port when remote access is needed.

Conclusion:
This task helped reinforce the importance of managing firewall rules to protect a system from potential threats. Blocking unused or insecure ports like Telnet is a fundamental security measure, while allowing secure ports like SSH ensures safe connectivity.