Firewall Configuration Task Report

Task 4: Setup and Use a Firewall on Windows

Objective

To configure and test firewall rules on Windows to block and allow specific network traffic using PowerShell commands.

Steps Performed

1. **Opened PowerShell as Administrator**
   Accessed elevated PowerShell to run firewall commands.

2. **Added a firewall rule to block inbound traffic on port 23 (Telnet)**
   Command:

New-NetFirewallRule -DisplayName "Block Telnet Port 23" -Direction Inbound -LocalPort 23 -Protocol TCP -Action Block

Result: Rule successfully created and enabled to block Telnet traffic.

3. **Tested the firewall rule**
   Verified that incoming connections on port 23 were blocked (via external tool or manual test).

4. **Removed the firewall rule**
   Command:

   Remove-NetFirewallRule -DisplayName "Block Telnet Port 23"

   Result: Rule successfully removed, restoring original firewall settings

---

Summary

The firewall acts as a barrier that filters network traffic based on rules. Blocking port 23 (Telnet) prevents unsecured remote access attempts. Managing firewall rules through PowerShell provides precise control over network security.