Firewall Configuration and Testing Report

Date: 12-06-2025

Step-by-Step Implementation

1. Opened Windows Defender Firewall with Advanced Security.

2. Clicked on Inbound Rules.

3. Created a new rule:

   - Type: Port

   - Protocol: TCP

   - Port: 23

   - Action: Block the connection

   - Applied to all profiles

   - Named: Block Telnet

4. Tested with command: telnet localhost 23 (connection failed as expected).

5. Created another rule:

   - Type: Port

   - Protocol: TCP

   - Port: 22

   - Action: Allow the connection

   - Named: Allow SSH

6. Removed the test block rule (Block Telnet) to restore original state.

Step 7: Commands / GUI Steps Used

- Used Windows GUI (Firewall with Advanced Security) for all configurations.

- Created and removed firewall rules using 'New Rule' wizard.

- Verified block using: telnet localhost 23

- Used DISM command to install Telnet if not already present:

  dism /online /Enable-Feature /FeatureName:TelnetClient

Step 8: Summary - How Firewall Filters Traffic

A firewall filters incoming and outgoing network traffic based on a set of security rules.

In this task:

- Port 23 (Telnet) was blocked, preventing unauthorized remote access.

- Port 22 (SSH) was allowed, ensuring secure connections.

- The firewall allowed or denied connections based on protocol and port matching rules.

This practical task demonstrated essential firewall management skills using Windows Firewall.