Task 4: Firewall Configuration and Testing on Windows

Objective: Set up basic firewall settings to control network traffic and validate that the configured rules function as expected.

Tool Used: Windows Defender Firewall

Activity Overview: We configured a firewall rule that blocks specific inbound traffic to improve system security.

Steps Followed:

1. Firewall Rule Creation:
   * A custom inbound rule was created to deny traffic coming through a specific port.
   * Selected Port 23 (commonly used by Telnet) to demonstrate blocking an insecure service.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Telnet Client Setup:**
   * Enabled the **Telnet Client** feature from Windows optional features.
2. **Testing the Rule:**

**A screenshot of a computer

AI-generated content may be incorrect.**

* + Launched the Command Prompt and attempted to use Telnet to connect to a remote host.
  + The system displayed an error message indicating that the connection could not be established.
  + This confirmed that the firewall rule was effectively blocking Telnet on port 23.

A screenshot of a computer

AI-generated content may be incorrect.

Understanding Windows Firewall Behaviour:

Windows Firewall uses rules to evaluate and control traffic. Rules can be based on several criteria:

* Port (e.g., 23 for Telnet, 80 for HTTP)
* Protocol (TCP or UDP)
* Traffic Direction (Inbound/Outbound)
* Target Application or Service
* Network Type (Domain, Private, Public)

The firewall evaluates rules in the following order:

* If a matching allow rule is found, the traffic is permitted.
* If a matching block rule is found first, the traffic is denied.
* If no rule applies, default behaviour is used (typically blocks inbound, allows outbound).

Conclusion:

The test confirmed that the newly created firewall rule successfully blocked Telnet traffic. This illustrates how firewalls can prevent unauthorized access and protect against threats when properly configured.