# Task 4 – Setup and Use a Firewall (Windows)

## Objective

Configure and test basic firewall rules on Windows to allow or block specific network traffic.

## Tools Used

- Operating System: Windows 10 / 11

- Firewall Tool: Windows Defender Firewall with Advanced Security

- Command Prompt / PowerShell (for testing)

## Steps Performed

1. Open Windows Firewall  
- Press Windows + R, type: firewall.cpl → Press Enter.  
- Click Advanced Settings to open Windows Defender Firewall with Advanced Security.  
(Screenshot 1: Firewall main window)

2. View Current Inbound Rules  
- In the left panel, click Inbound Rules to view existing rules.  
(Screenshot 2: List of inbound rules)

3. Create a Rule to Block Port 23 (Telnet)  
- In the right panel, click New Rule…  
- Select Port → Next  
- Choose TCP, enter port 23 → Next  
- Select Block the connection → Next  
- Select all profiles (Domain, Private, Public) → Next  
- Name the rule Block Telnet → Finish  
(Screenshot 3: “Block Telnet” rule added)

4. Test the Rule  
- Open Command Prompt and try: telnet localhost 23  
- Connection failed, confirming the block is active.  
(Screenshot 4: Failed connection attempt)

5. Remove the Rule  
- In Inbound Rules, locate Block Telnet.  
- Right-click → Delete.  
(Screenshot 5: Rule removed)

## Summary

This task demonstrated how to configure the Windows Firewall to block traffic on a specific port (Telnet, port 23) and verify that the block was successful. The firewall filters traffic based on rules that allow or deny inbound and outbound connections, improving system security.

## Key Concepts Learned

- Viewing and managing firewall rules in Windows

- Blocking traffic on a specific port

- Understanding inbound vs. outbound rules

- Verifying firewall rules using network tools