Firewall Configuration Task – Windows

Objective

To configure the Windows Firewall to block a specific port (e.g., port 23 – Telnet), test the rule, allow a safe port (SSH/22 as reference), and then remove the rule to restore the system.

Tools Used

- Windows Defender Firewall with Advanced Security (GUI)
- PowerShell

GUI Steps Followed

1. Open Firewall Configuration Tool

- Press Windows + R → type: wf.msc → press Enter
- This opens **Windows Defender Firewall with Advanced Security**

2. View Existing Firewall Rules

- In the left pane, click **Inbound Rules**
- Observed and reviewed current rules controlling incoming traffic

3. Block Inbound Traffic on Port 23 (Telnet)

- In the right-hand pane → click **New Rule**
- Select **Port** → click **Next**
- Choose **TCP** → enter **23** for specific local ports → Next
- Choose **Block the connection** → Next
- Apply to all profiles (Domain, Private, Public) → Next
- Name it: Block Port 23 - Telnet → Finish

4. Remove the Test Rule

- Go back to **Inbound Rules**
- Right-click on Block Port 23 - Telnet → click **Delete**

PowerShell Commands Used

1. Check Port Availability Using PowerShell Command:
   Test-NetConnection -ComputerName localhost -Port 23

Summary: How the Firewall Filters Traffic

Windows Firewall uses inbound rules to control:

- What **external connections are allowed to reach your computer**
- Based on **port number, protocol, profile (private/public), and direction**

Inbound rules are like gatekeepers for your system — blocking ports means certain traffic can't get in, even if something is listening.