**Objective:** Block and test inbound Telnet (port 23) traffic using Windows Defender Firewall GUI and document outcomes.

🔧 **Step 1: Open Firewall Management**

- Press Win + R
- Type wf.msc → **Enter**
- This opens the "Windows Defender Firewall with Advanced Security" console.

📜 **Step 2: List Existing Rules**

- Click **Inbound Rules** in the left panel
- View current rule set: name, profile, port, status

🚫 **Step 3: Block Inbound Port 23**

1. Click **New Rule** in right-hand panel
2. Choose **Port** → Next
3. Protocol = **TCP**, Specific local port = 23 → Next
4. Action = **Block the connection** → Next
5. Apply to all profiles → Next
6. Name = Block_Telnet_23 → Finish

📸 Taken screenshot of rule created

🧪 **Step 4: Test With Telnet**

**Enable Telnet Client:**

- Go to: *Control Panel → Programs → Turn Windows features on or off*
- Enable **Telnet Client**

**Test Command in CMD:**

telnet localhost 23

**Expected Result:**

Could not open connection to the host, on port 23: Connect failed

📸 Taken screenshot of failure message

✅ **Step 5: Remove the Rule**

- Go back to **Inbound Rules**
- Right-click on Block_Telnet_23 → **Delete**

📸 Taken screenshot the clean rule list

🧠 **Summary: How Firewall Filters Traffic**

- Firewalls inspect network packets and enforce rules on:
    - Ports
    - Protocols
    - IP addresses
- This rule blocked **TCP port 23 (Telnet)** to prevent insecure access
- Firewall acts as a control point to block unwanted inbound/outbound connections