# Cybersecurity Internship Report

Task 4: Windows Firewall Configuration and Testing

Submitted by: Golla venkatesham

Platform: Microsoft Windows 10

Tool Used: Windows Defender Firewall with Advanced Security

🔍 Objective

To configure and test basic firewall rules on Windows, demonstrating how to block insecure traffic and verify rule effectiveness using Telnet.

*No table of contents entries found.*

.

🛠️ Tools Required

Windows Defender Firewall (Advanced Settings)

Telnet Client (for testing blocked port)

Command Prompt

Screenshot tool

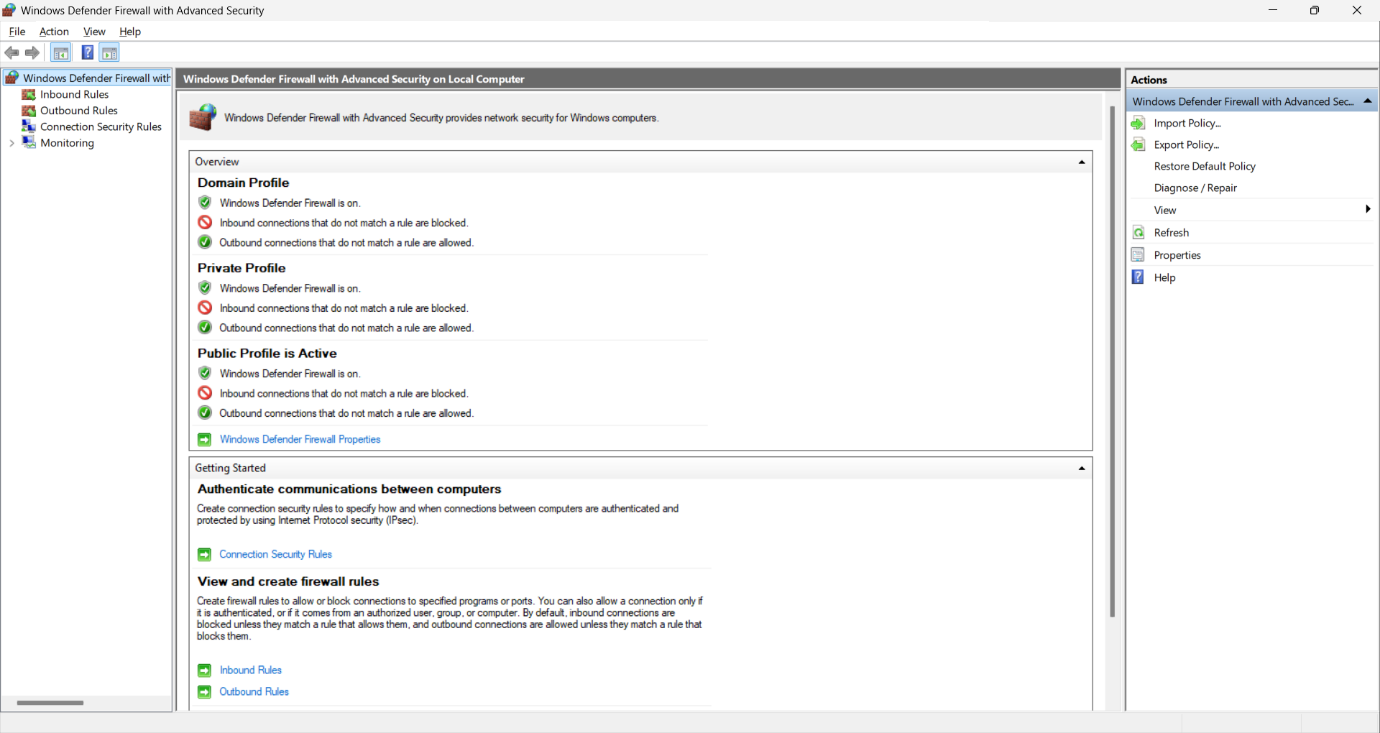
**🧭 Step-by-Step Procedure**

Step 1: Open Windows Firewall

Press Windows + R, type wf.msc, and hit Enter.

This opens Windows Defender Firewall with Advanced Security.

📸 *Screenshot: Firewall interface opened*



Step 2: Create a New Inbound Rule

Click Inbound Rules → New Rule (right pane).

Select Port → Click Next

Choose TCP, enter 23 → Click Next

Select Block the connection → Click Next

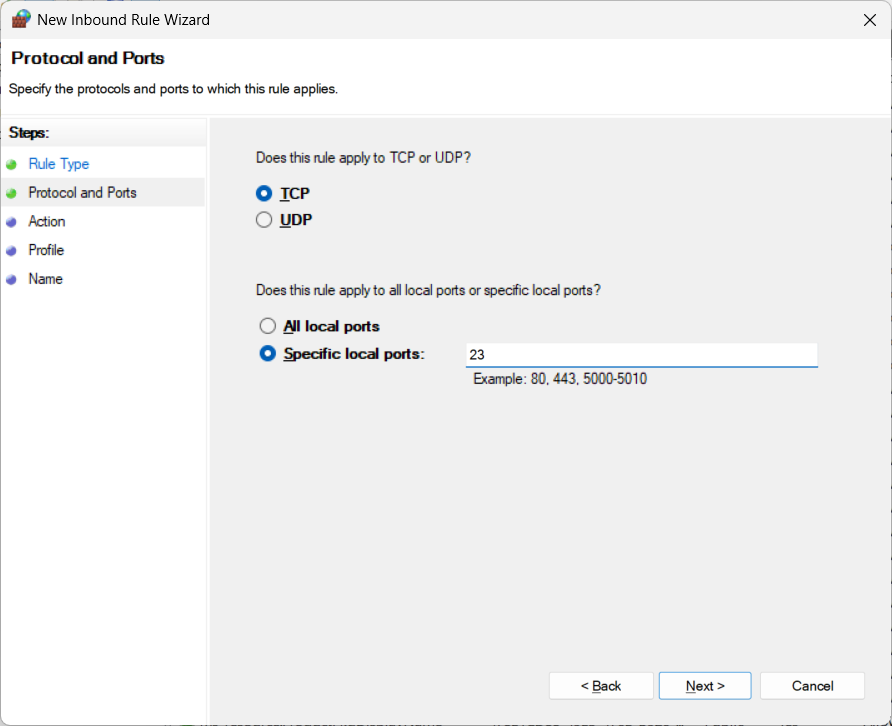
Apply to Domain, Private, and Public → Click Next

Name the rule: Block Telnet Port 23 → Click Finish

📸 *Screenshot: Rule creation wizard*

A screenshot of a computer

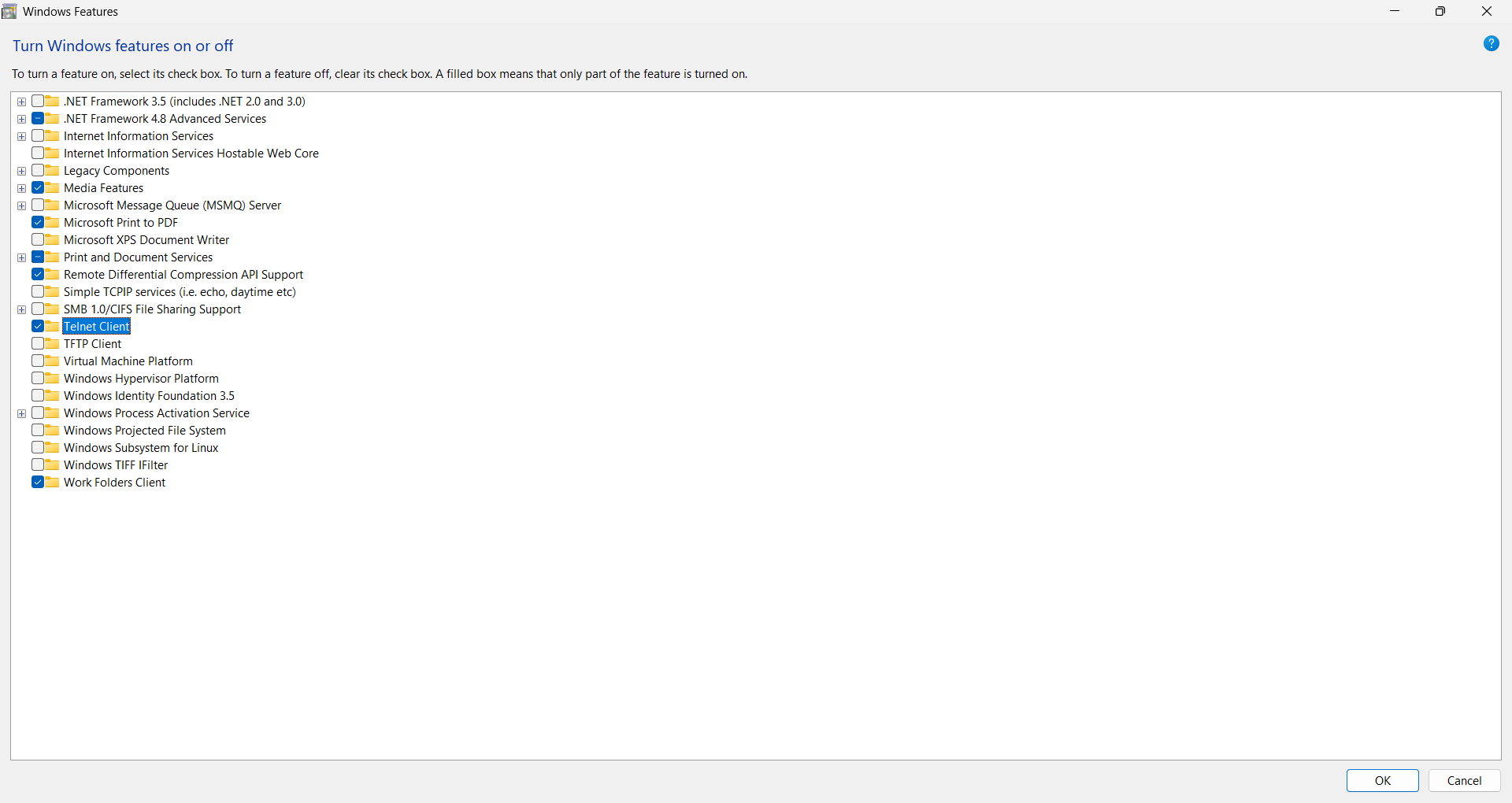
AI-generated content may be incorrect.



**Step 3: Enable Telnet Client**

* Press Windows + R, type optionalfeatures, and hit Enter.
* In **Windows Features**, check **Telnet Client** → Click **OK**

📸 *Screenshot: Telnet Client enabled*



**Step 4: Test the Rule**

* Open Command Prompt
* Run: telnet localhost 23
* Expected result: Connect failed

📸 *Screenshot: Telnet connection failure*

A screen shot of a computer

AI-generated content may be incorrect.

**Step 5: Delete the Rule**

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

📸 *Screenshot: Rule deletion confirmation*

**📚 Slide 6: What I Learned**

* How firewalls filter traffic based on ports and protocols
* Importance of blocking insecure services like Telnet
* Hands-on experience with rule creation and testing
* Professional documentation and troubleshooting
* Interview-ready knowledge on firewall concepts

**✅ Slide 10: Conclusion**

* Successfully configured and tested firewall rules
* Demonstrated secure system practices
* Gained practical cybersecurity skills
* Ready for future tasks and interviews