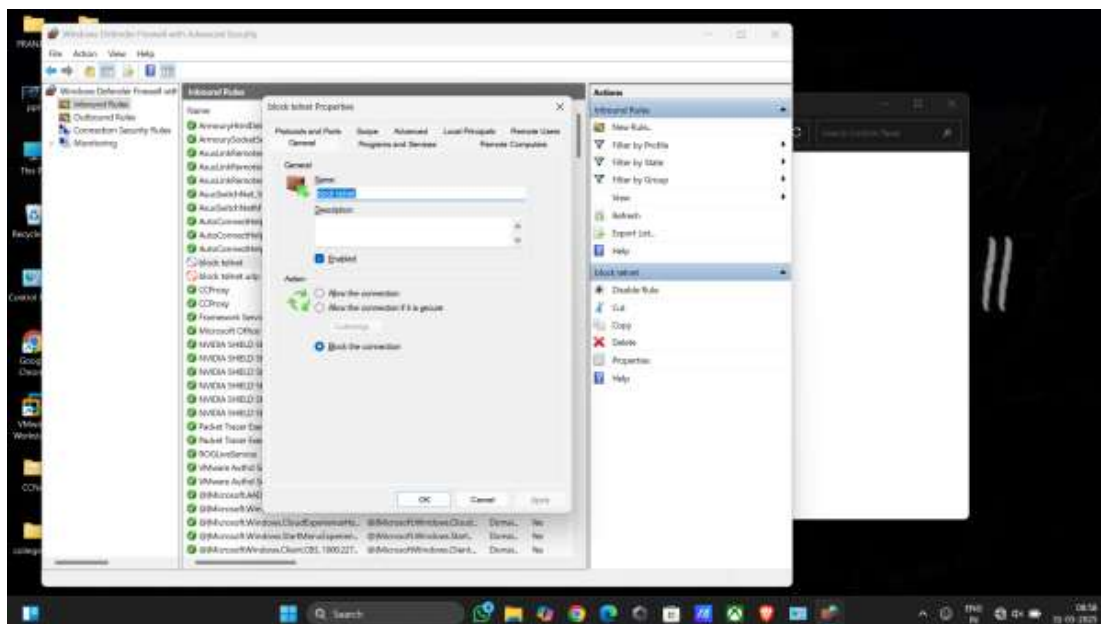


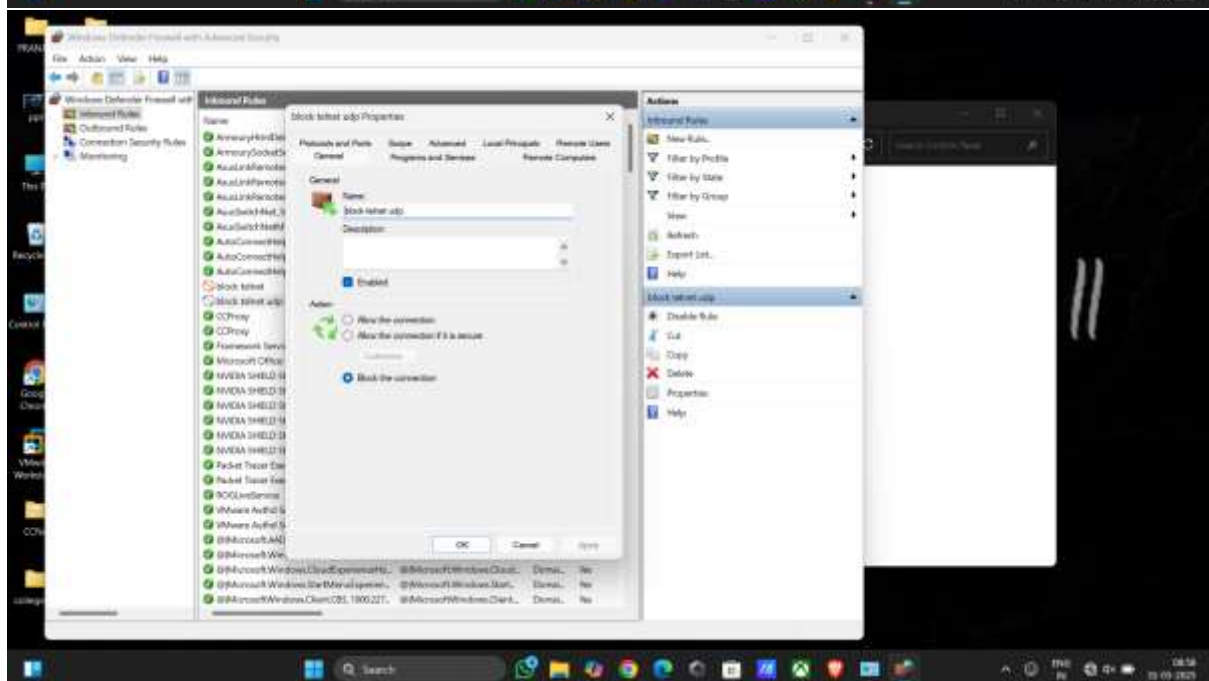
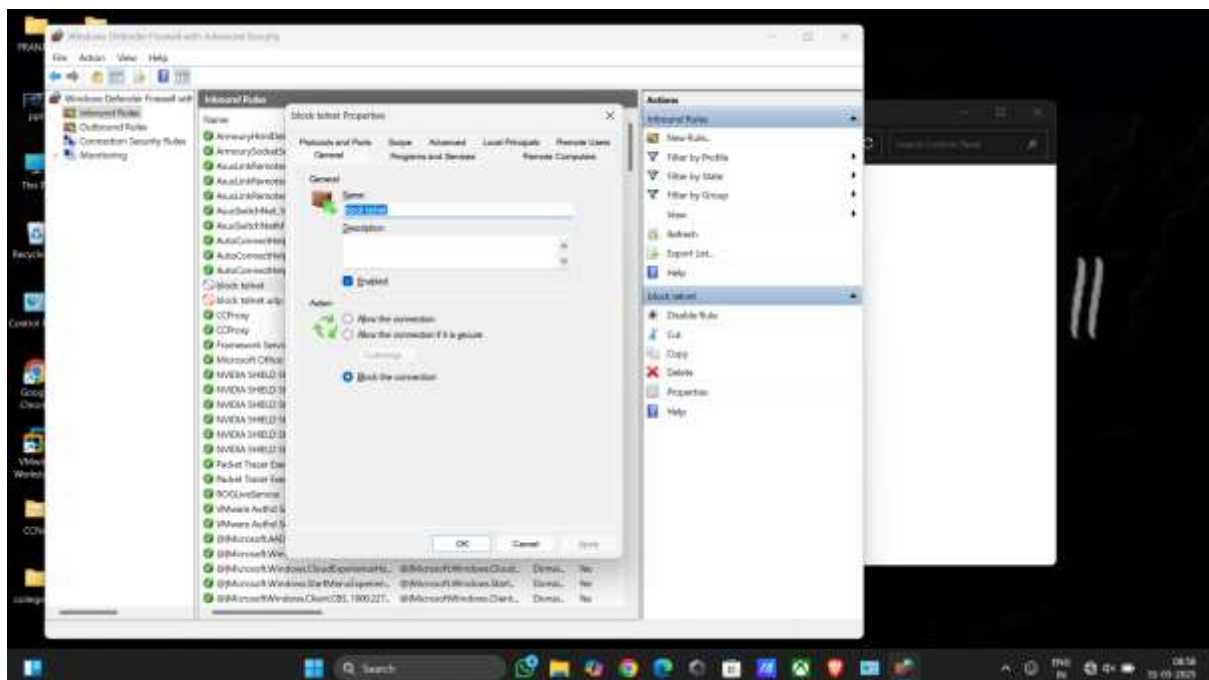
## Task 4 : Setup and Use a Firewall on Windows/Linux

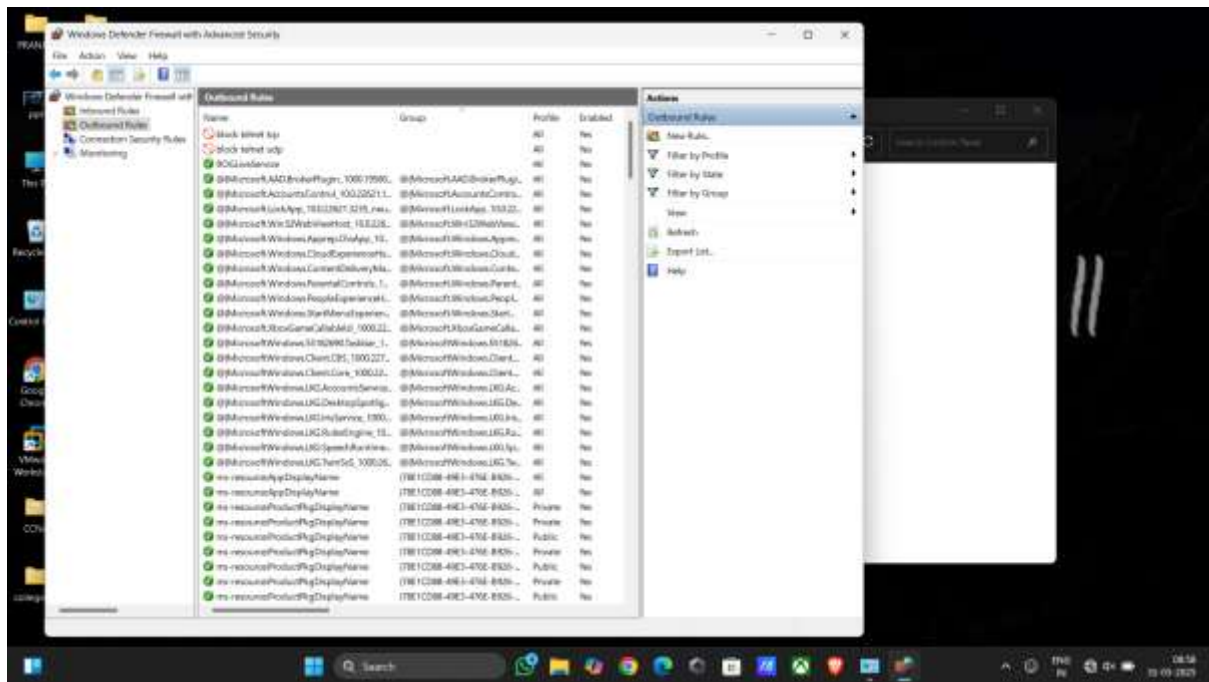
- **Objective:** Configure and test basic firewall rules to allow or block traffic.
- **Tools:** Windows Firewall
- **Steps :**

### 1. Creating the Firewall Rule to Block Telnet

- Opened "Windows Defender Firewall with Advanced Security"
- Navigated to "Inbound Rules".
- Selected "New Rule".
- Select rule type: "Port"
- Select "TCP" protocol and specified port "23"
- Select "Block the connection"
- Apply the rule to all profiles (Domain, Private, Public)
- Named the rule "Block Telnet"





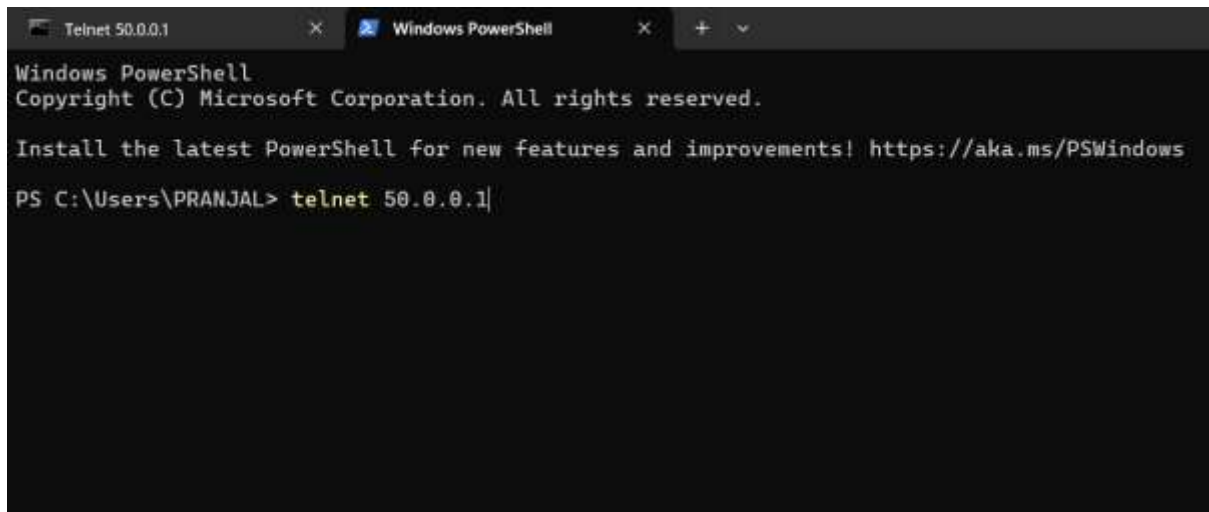


## 2. Testing the Firewall Rule


- Conducted two test cases to verify the firewall rule:

- **Test Case 1: Before Rule Implementation**

- Executed command: telnet 50.0.0.1



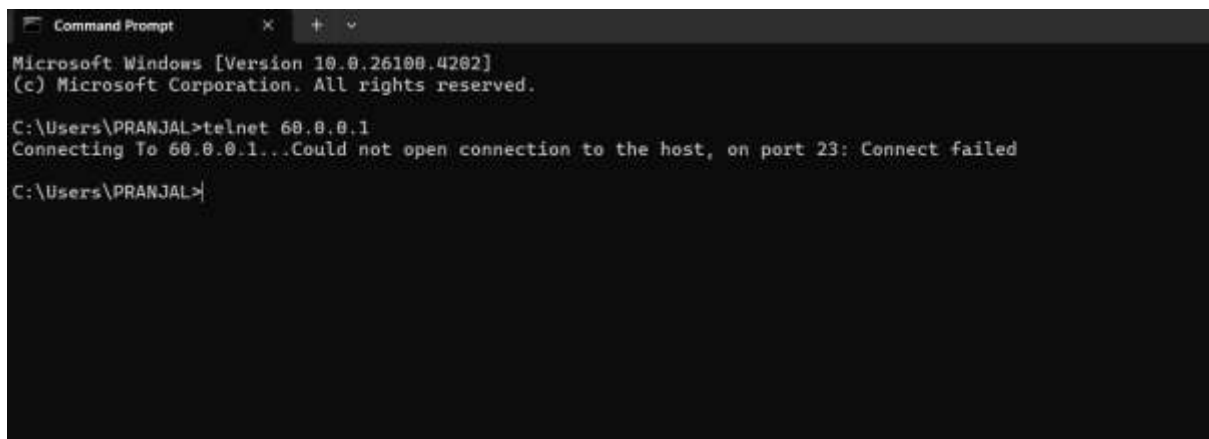
- **Result:** Successfully connected to Telnet server



A screenshot of a Telnet session. The window title is 'Telnet 50.0.0.1'. The text displayed is:   
\*=====   
Microsoft Telnet Server.   
\*=====   
C:\Users\Administrator>

- **Test Case 2: After Rule Implementation**

- Executed command: telnet 60.0.0.1
- **Result:** "Could not open connection to the host, on port 23: Connect failed".



A screenshot of a Windows Command Prompt window. The text displayed is:   
Microsoft Windows [Version 10.0.26100.4202]   
(c) Microsoft Corporation. All rights reserved.   
C:\Users\PRANJAL>telnet 60.0.0.1   
Connecting To 60.0.0.1...Could not open connection to the host, on port 23: Connect failed   
C:\Users\PRANJAL>

- This shows that the firewall rule is effectively blocking Telnet traffic

- **Key Observations**

- The firewall rule successfully blocked inbound Telnet connections while allowing other traffic to pass
- The blocking was immediate after rule creation, demonstrating real-time filtering
- The system provided clear feedback when connections were blocked