# Firewall Rule Configuration Report by TANMAY PRADHAN

# 1. Objective

To configure and test a basic firewall rule to block inbound traffic on port 23 (Telnet) and then remove the rule to restore original state using Windows Firewall.

# 2. Tools Used

- Windows 11  
- Command Prompt (Run as Administrator)  
- Telnet Client

# 3. Firewall Rule Configuration Steps

Step 1: Open Command Prompt as Administrator

Step 2: Add a rule to block Telnet traffic (port 23):

netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23

Step 3: Test the rule using Telnet:

telnet 127.0.0.1 23

Step 4: If the rule is working, connection will be blocked (connection failed message).

Step 5: Remove the rule to restore original state:

netsh advfirewall firewall delete rule name="Block Telnet"

# 4. Output & Verification

Include screenshots of:

- Adding the rule in Command Prompt

- Testing with Telnet showing 'connection failed'

- Deleting the rule

# 5. Summary

This exercise demonstrated how to block a specific port using Windows Firewall, verify it using Telnet, and then remove the rule to return to the default firewall state. It helped understand the basic working of host-based firewalls and how traffic is filtered based on rules.

# 6. How a Firewall Filters Traffic

* A firewall inspects every incoming and outgoing packet and evaluates it against its rule set.
* If a packet matches a rule, the firewall performs the specified action—typically ALLOW or BLOCK.
* Stateful inspection enables the firewall to track the state of a connection (NEW, ESTABLISHED, RELATED) and make context‑aware decisions.
* Rules can filter traffic based on direction (inbound/outbound), protocol (TCP/UDP/ICMP), port numbers, and source/destination IP addresses.
* A default‑deny policy ensures that any traffic not explicitly allowed is automatically blocked, enhancing security.