## **CONFIGURING AND TESTING FIREWALL RULES IN WINDOWS**

***OBJECTIVE:***

To configure windows firewall to block inbound traffic on telnet port(23), test it using Nmap, and verify the rule’s effect.

***STEPS PERFORMED:***

**-**Opened Windows defender firewall:Advanced security

- Listed all the inbound rules

-Blocked the Inbound traffic on port 23(Telent):

New rule->Port-> TCP, Destination Port ->Block the connection->named the block->finish

-Tested the rule using Nmap:

Target- localhost

Command- nmap -p 23 localhost

-Removed the test block

***RESULTS:***

With the block : Port state service : 23/tcp filtered telnet

Removed block : Port state service : 23/tcp closed telnet

***SUMMARY***

A firewall filters network traffic by controlling which connections are allowed or blocked based on a set of predefined rules.

It examines data packets entering or leaving the system and checks details such as the **IP address, port number, protocol, and direction (inbound or outbound)**.

If a packet matches an **allow rule**, it is permitted through; if it matches a **block rule**, it is dropped.  
This helps protect the computer from unauthorized access, malware, and network attacks while still allowing safe communication.