**Firewall Configuration Practical**

**Introduction**

A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predefined security rules. On Windows, the **Windows Defender Firewall with Advanced Security** is commonly used. It helps block unauthorized access while permitting legitimate communication.

In this practical, we configure and test basic firewall rules to block and allow specific traffic using Windows commands.

**Tools Used**

* **Windows Operating System** (with Windows Defender Firewall)
* **PowerShell / Command Prompt** (to execute firewall commands)
* **Telnet Client** (for testing blocked/allowed ports)

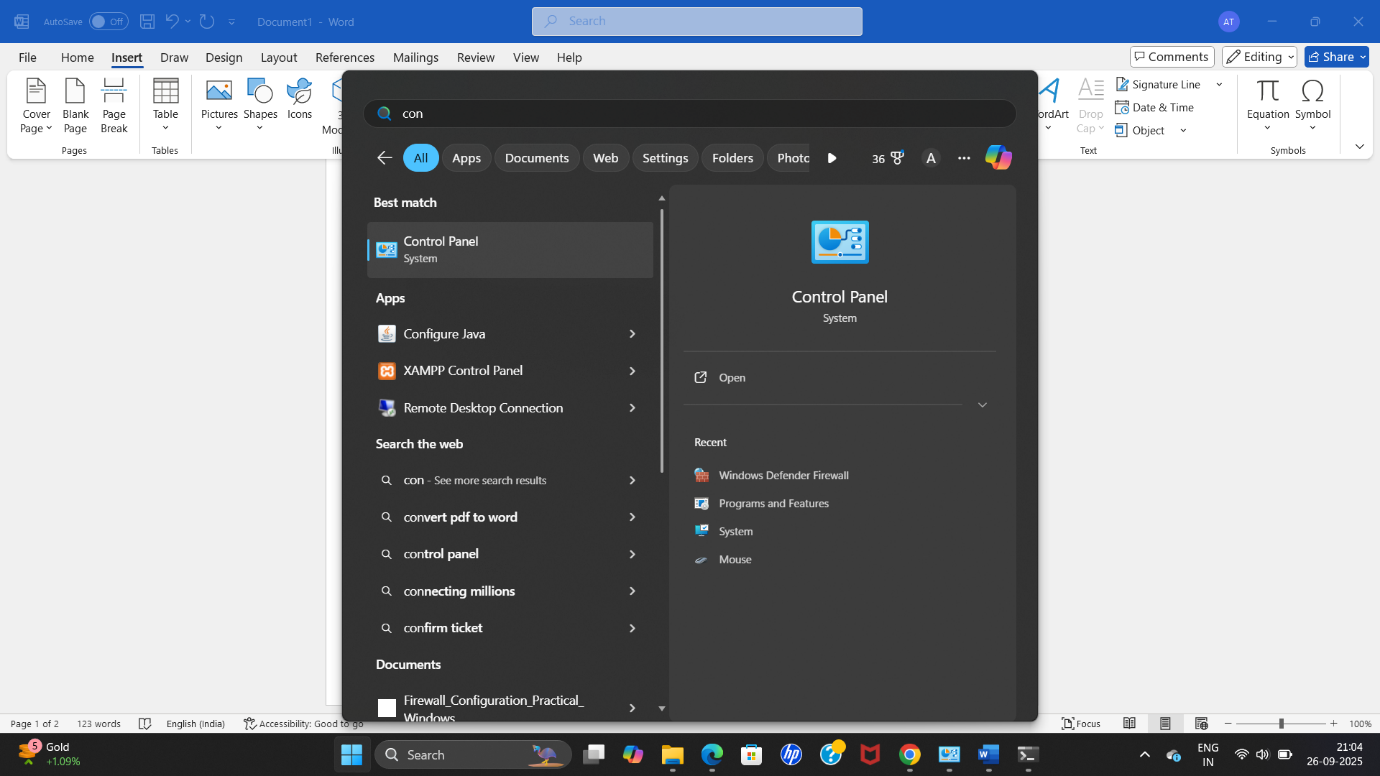
**Objective**

Configure and test basic firewall rules to allow or block traffic.

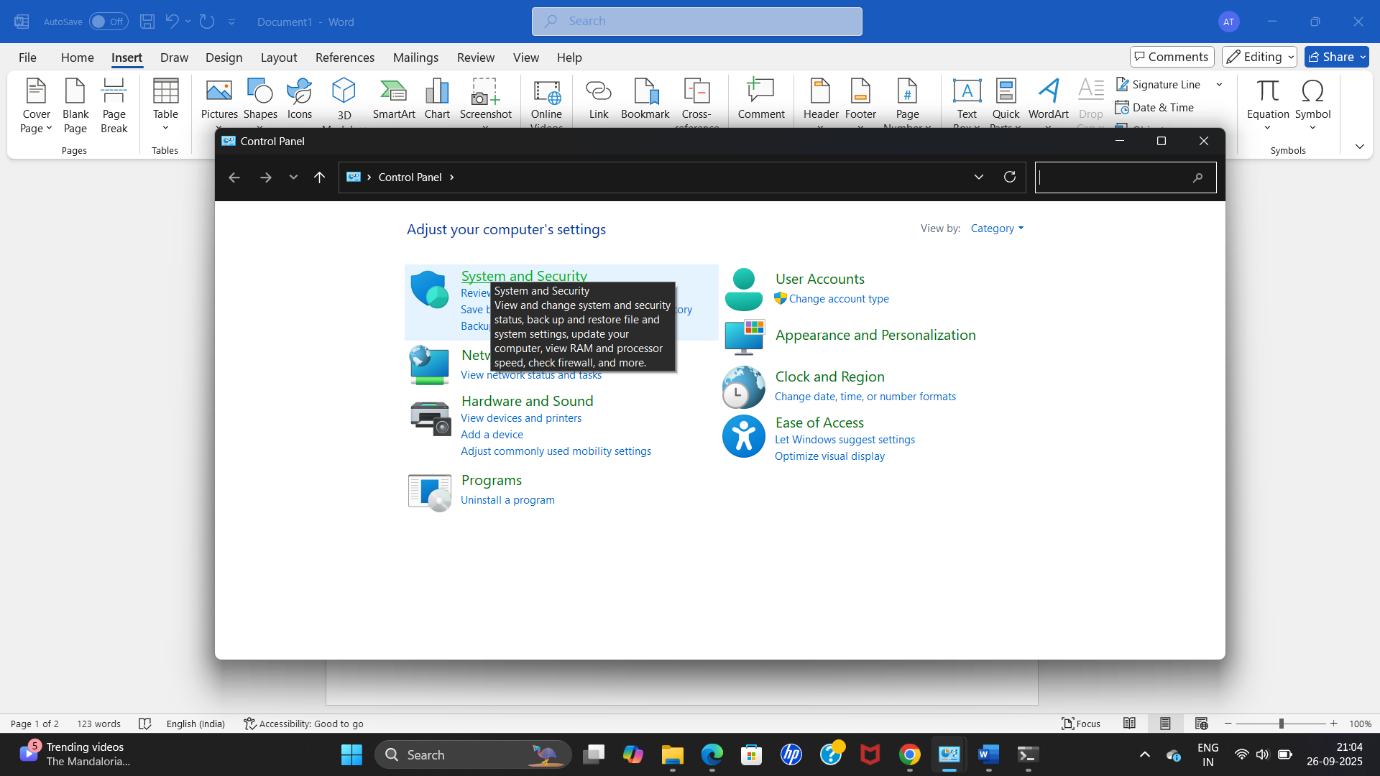
**Steps**

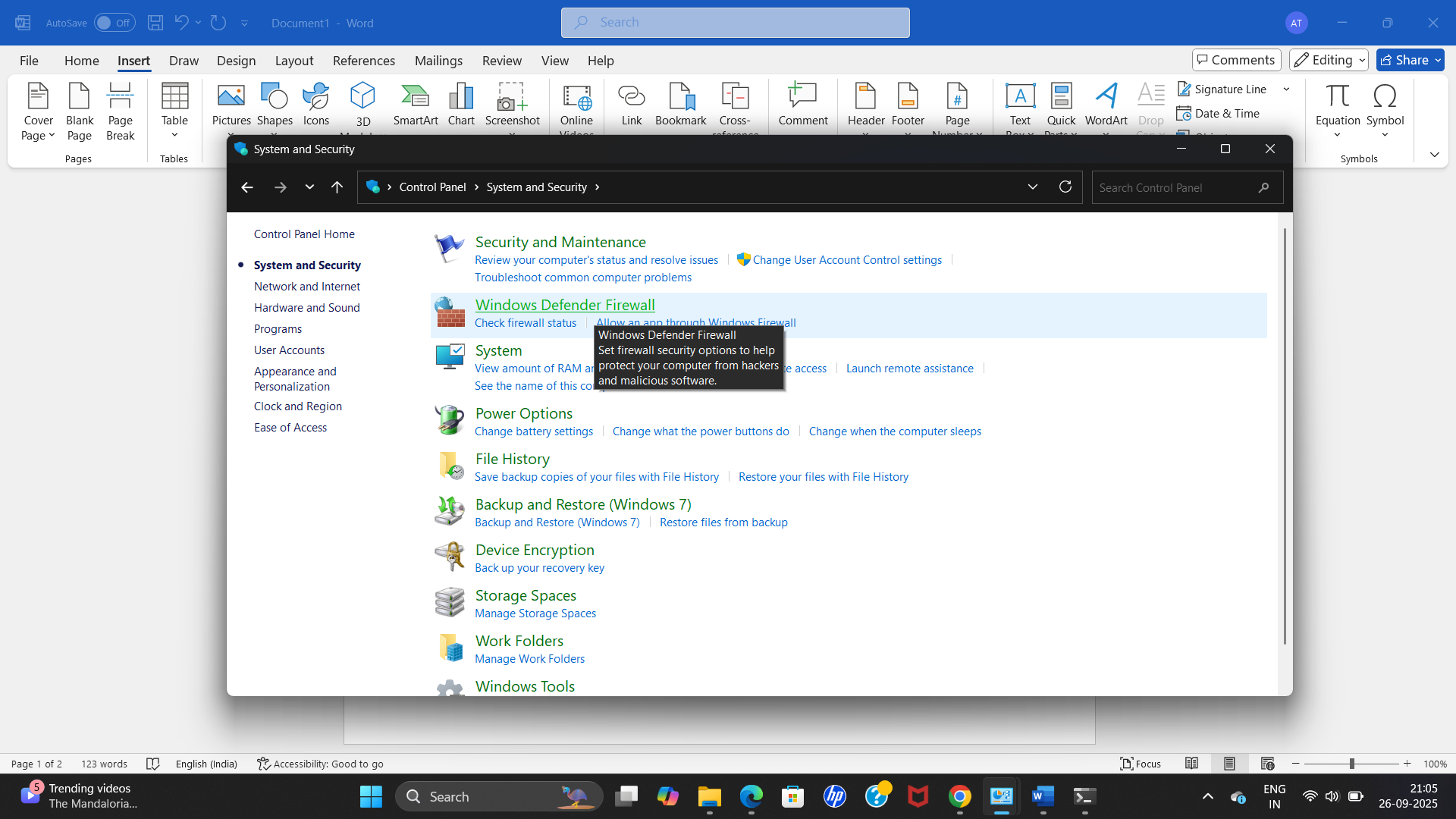
**1. Open Firewall Configuration Tool**

On windows, open control panel as below



Then navigate to system and security and then windows defender firewall



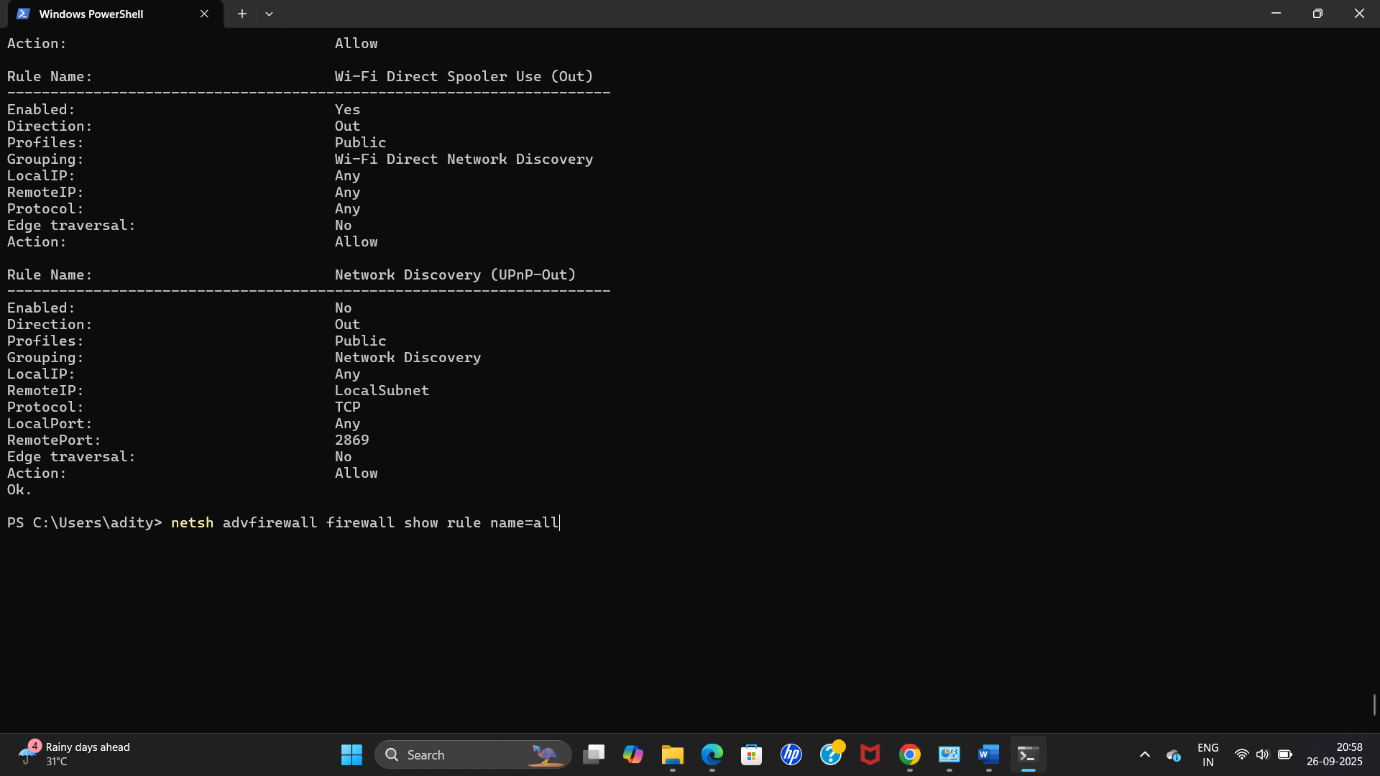


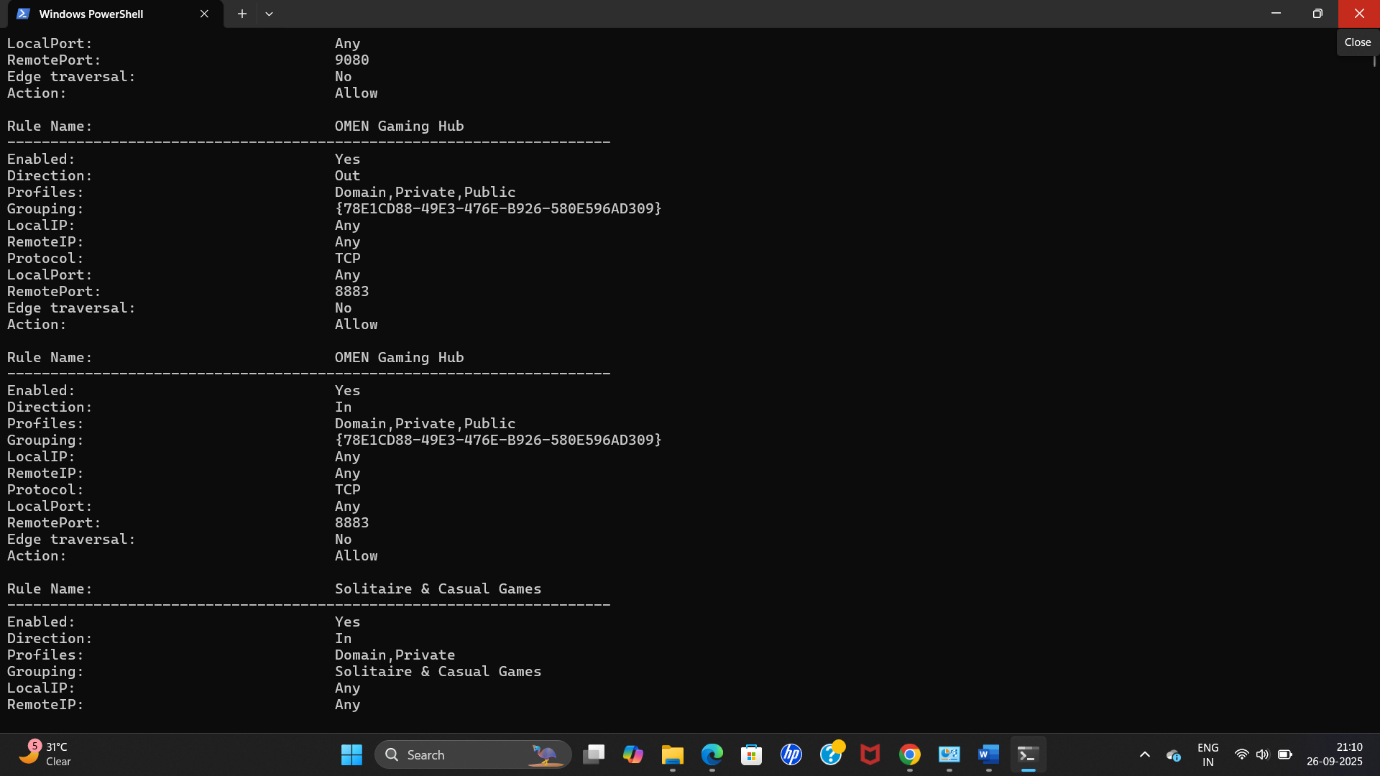
List Current Firewall Rules

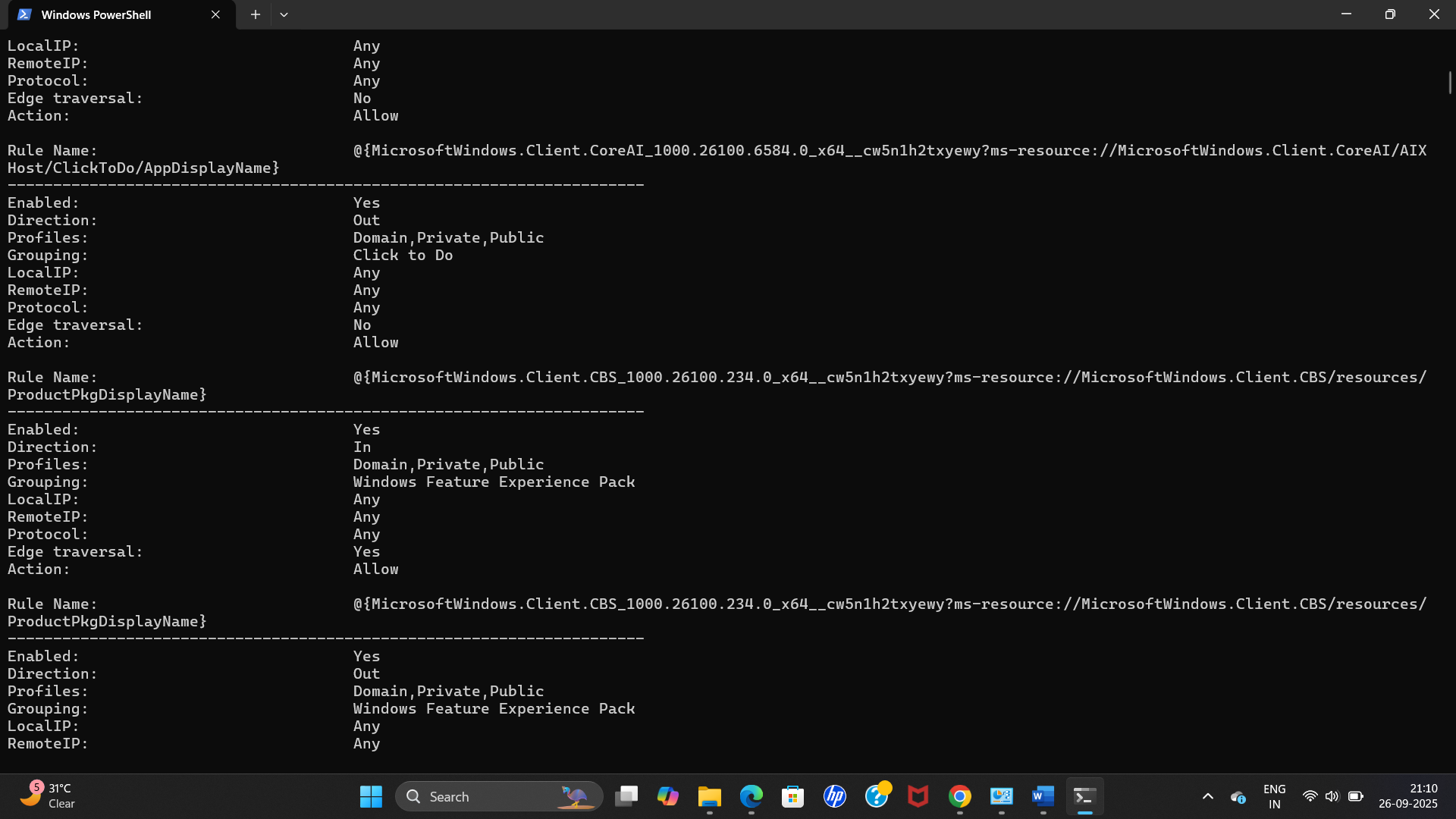
The command for listing current firewall rules is netsh advfirewall firewall show rule name=all where,

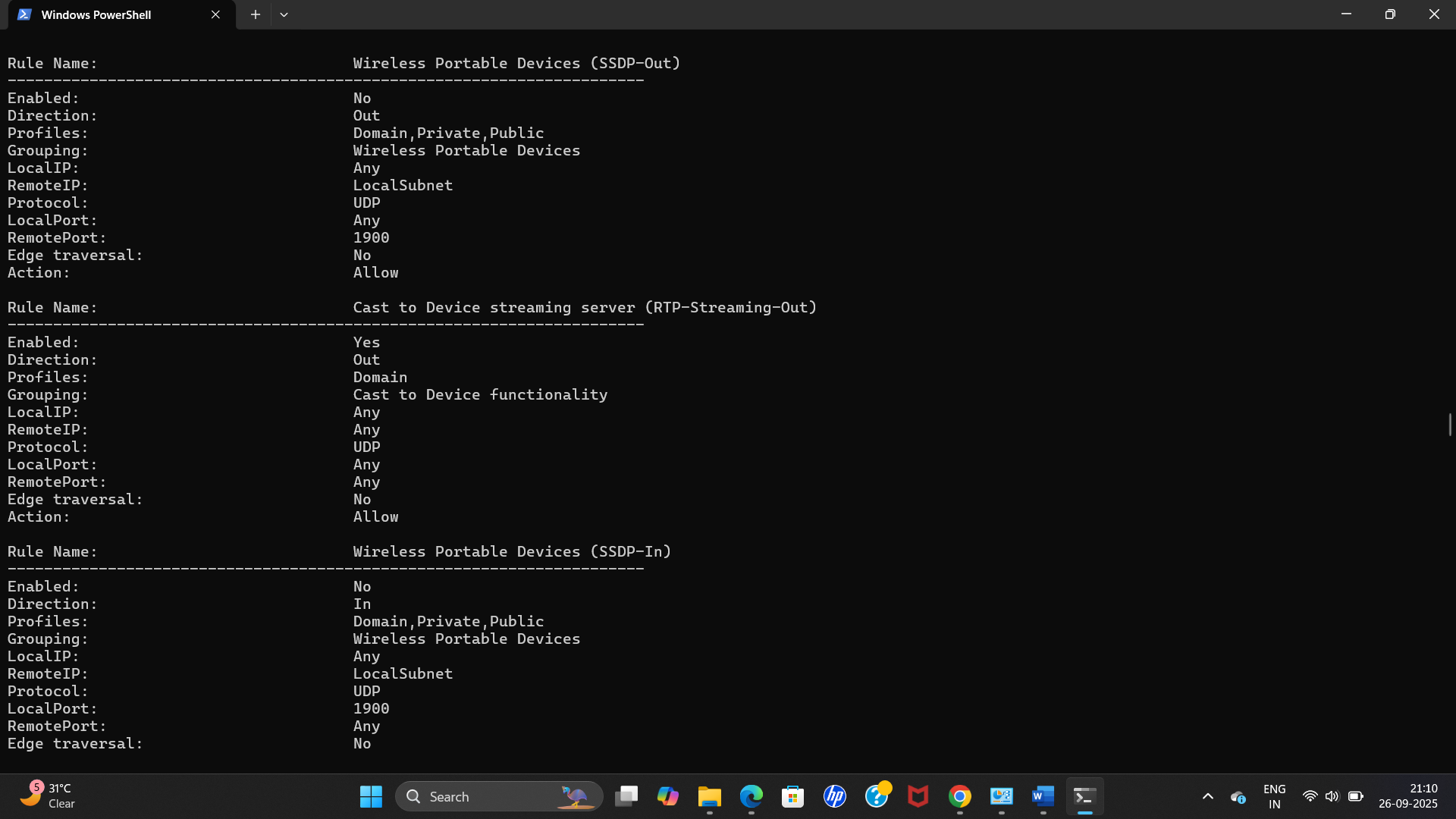
* netsh → Windows network configuration tool.
* advfirewall → Accesses advanced firewall settings.
* firewall show rule name=all → Displays all firewall rules currently applied.

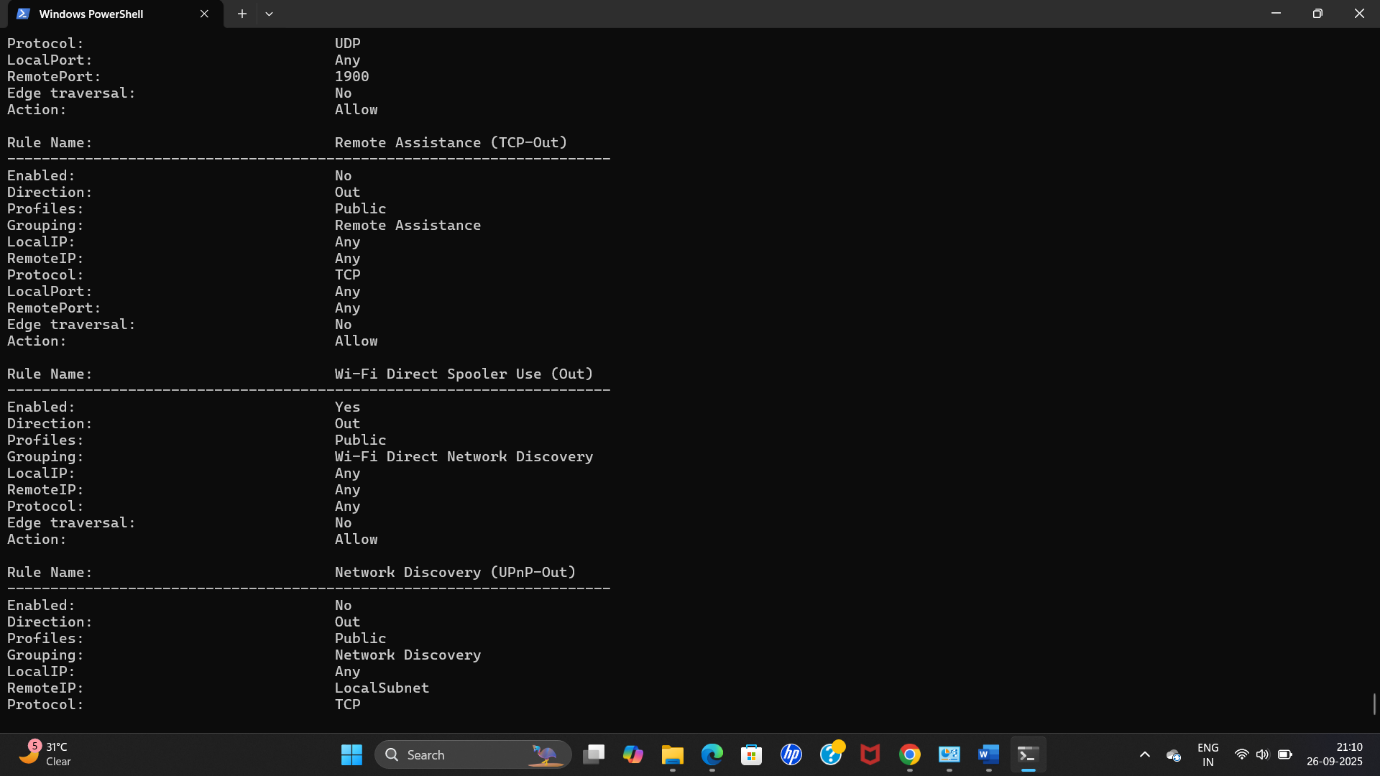
Lets the run the command in Microsoft powershell and analyze it











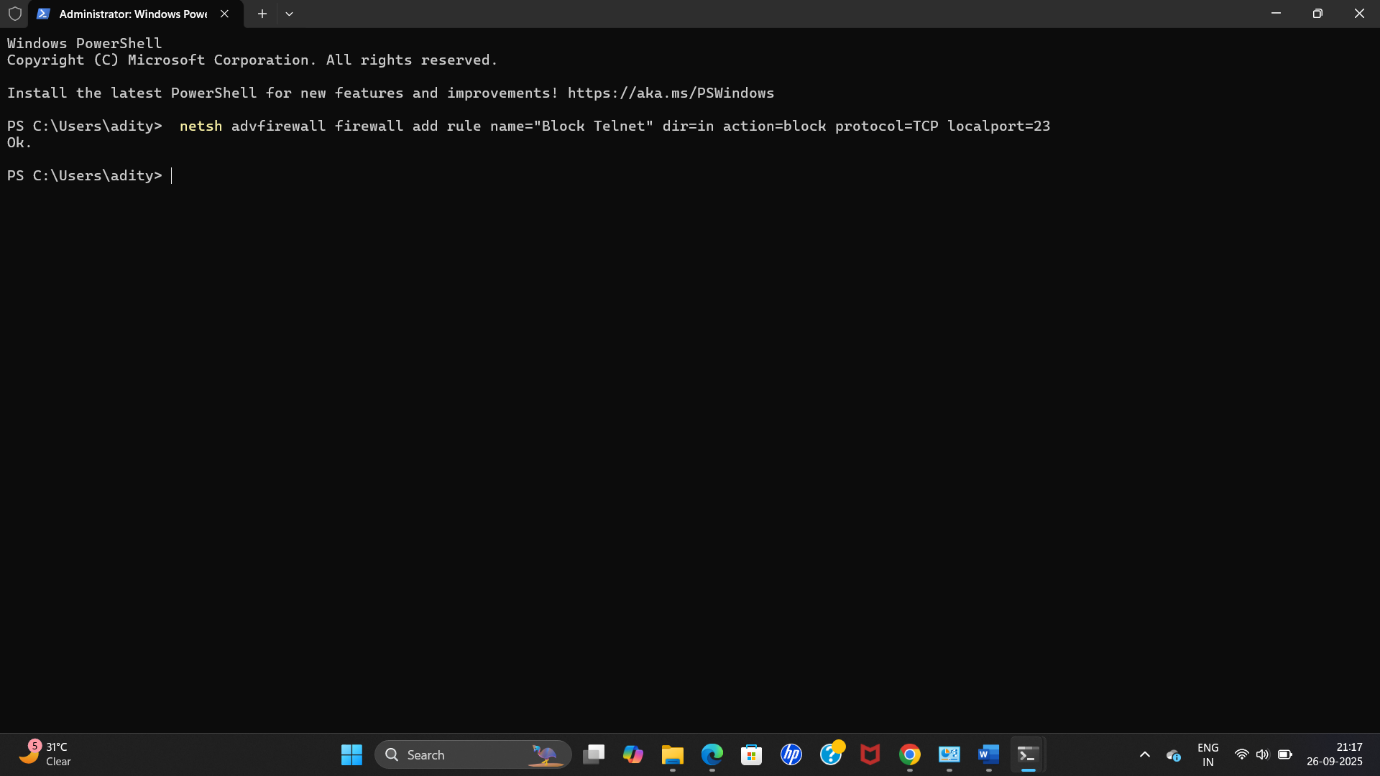
Add a Rule to Block Inbound Traffic on Port 23 (Telnet)

To block inbound traffic on port 23 of telnet we use the command

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

* add rule → Creates a new firewall rule.
* name="Block Telnet" → Rule name (used to identify it later).
* dir=in → Applies to **inbound traffic** (coming into the system).
* action=block → Blocks matching traffic.
* protocol=TCP → Restricts the rule to TCP traffic.
* localport=23 → Targets port **23** (Telnet service).

Lets run the command and see if it works,



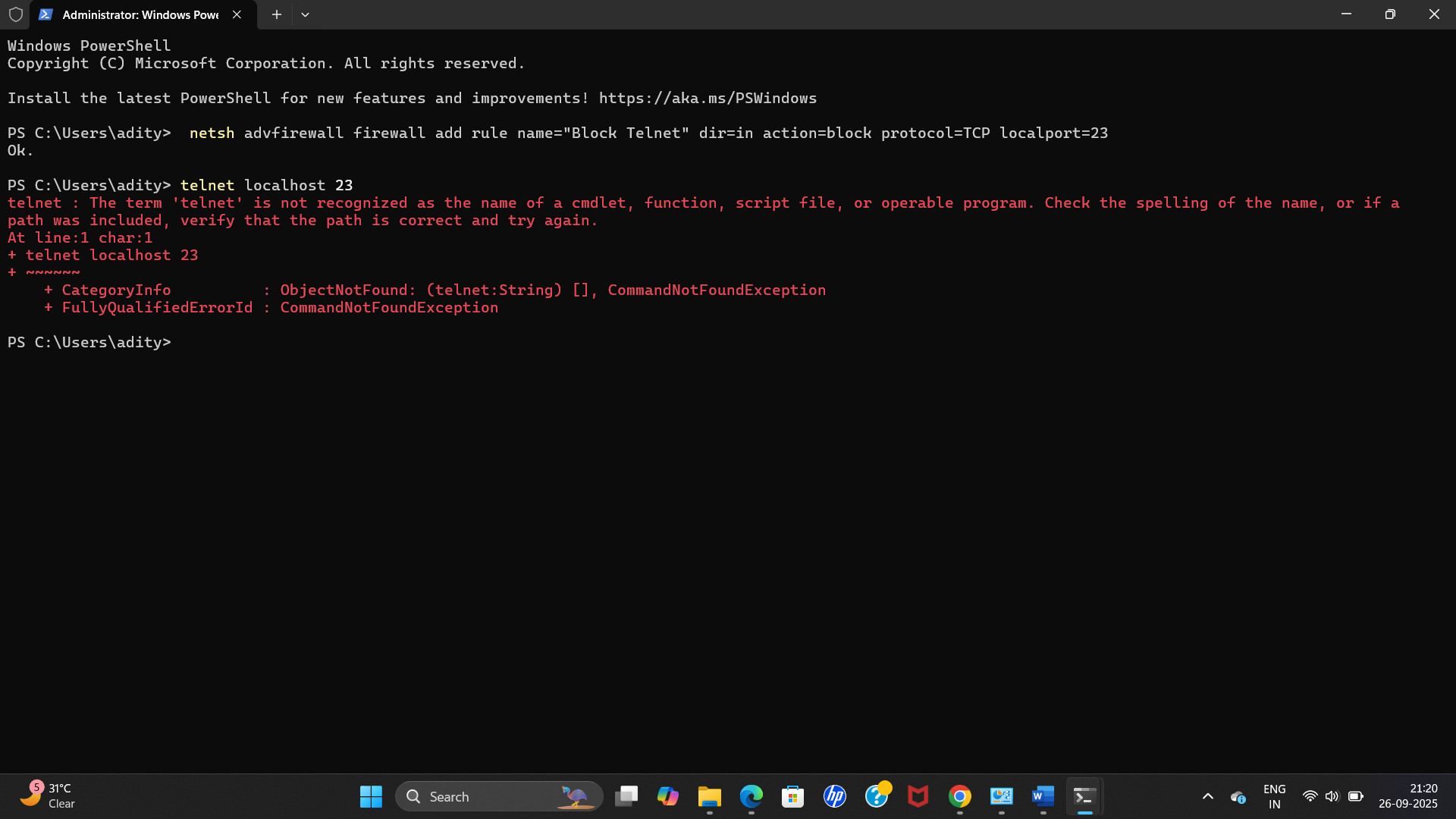
The result which came back as ok, means it has updated its security protocols, now to check if it works, we use the command telnet localhost 23 where,

 telnet → Tool to test connectivity to a specific port.

 localhost → Refers to the local system (127.0.0.1).

 23 → The port being tested.

Lets check the programme while running it

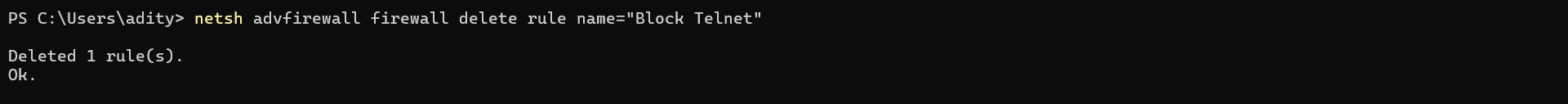


The rule is successfully applied as its showing error while trying to run the port 23 of telnet.

Now to Remove the Test Block Rule we use the command netsh advfirewall firewall delete rule name="Block Telnet" where,

 delete rule → Removes an existing firewall rule.

 name="Block Telnet" → Identifies the rule to be deleted.



**Conclusion / Summary**

A firewall acts as a **security barrier** between trusted and untrusted networks. It works by filtering traffic based on rules defined by the administrator.

In this practical:

* We listed existing rules.
* Added a rule to block inbound Telnet traffic (port 23).
* Verified the block using Telnet testing.
* Deleted the rule to restore the original configuration.

This demonstrates how firewall rules can be applied to **control specific ports/services**, ensuring that only **authorized and safe communication** is allowed. Firewalls are an essential defense mechanism to protect systems from unauthorized access and potential attacks.