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

BY: KUSH THAKER. (kthaker442@gmail.com)

Step 0: Identifying Operating system:

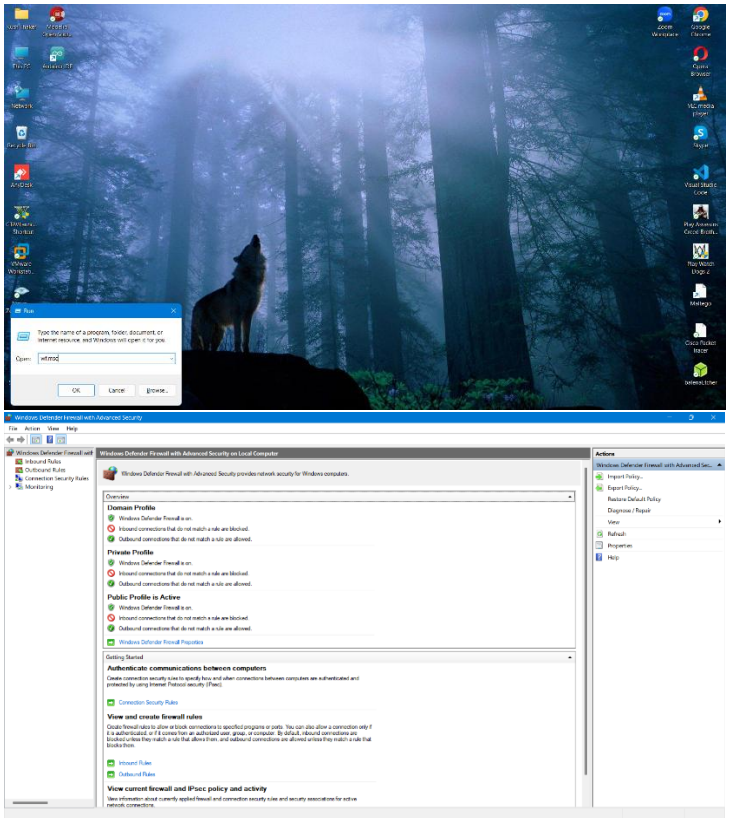
Here I am going use my Primary PC, which is Windows 11 (Phoenix).

Step 1: Open firewall configuration tool (Windows Firewall or terminal for UFW).

To open the Windows Firewall configuration tool, I:

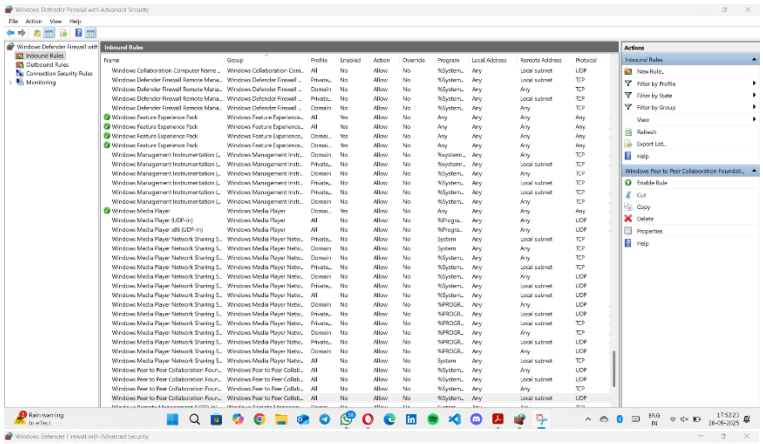
- Pressed **Win + R**
- Typed: wf.msc
- Pressed **Enter**

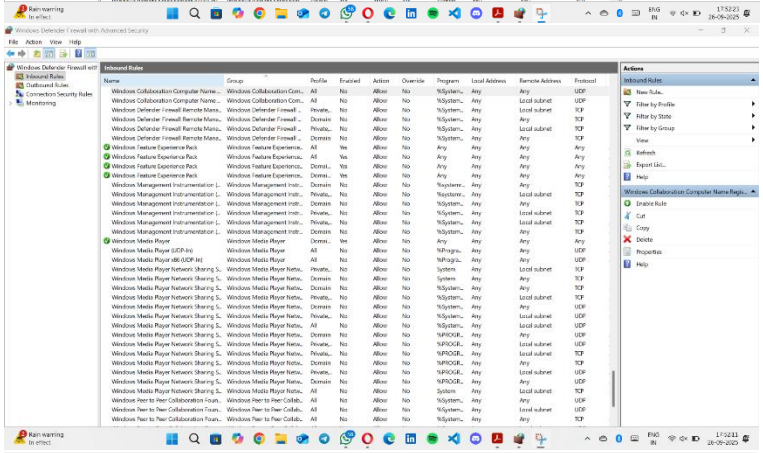
This launched *Windows Defender Firewall with Advanced Security*. From the left panel, I clicked **Inbound Rules** to view all existing firewall rules. On the right-hand side, I saw the option to add a **New Rule**. Pasted bellow

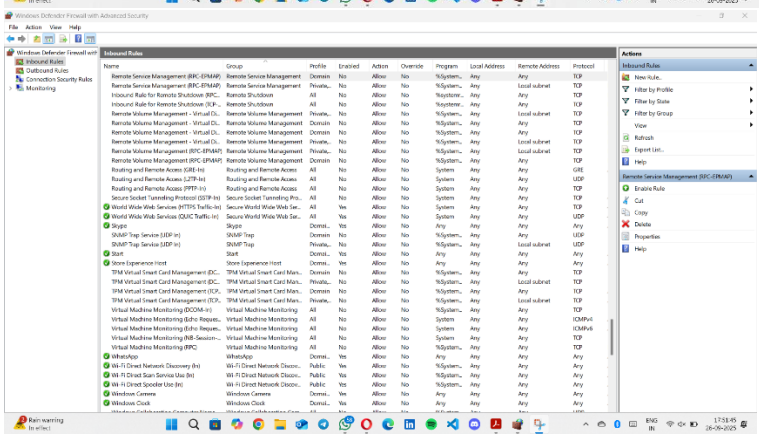


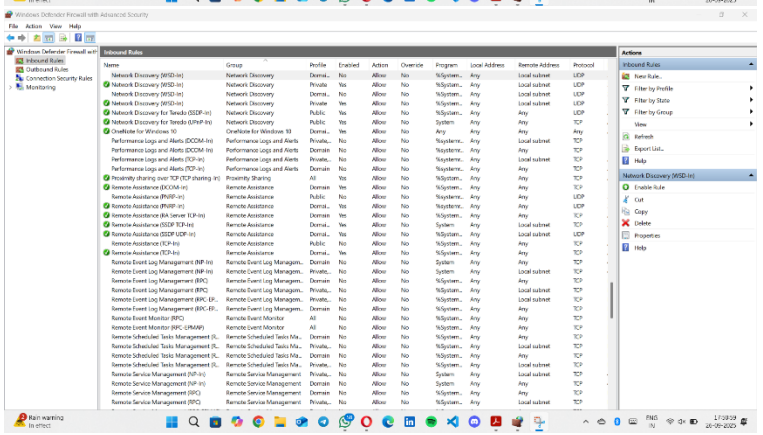
Step 2: List current firewall rules.

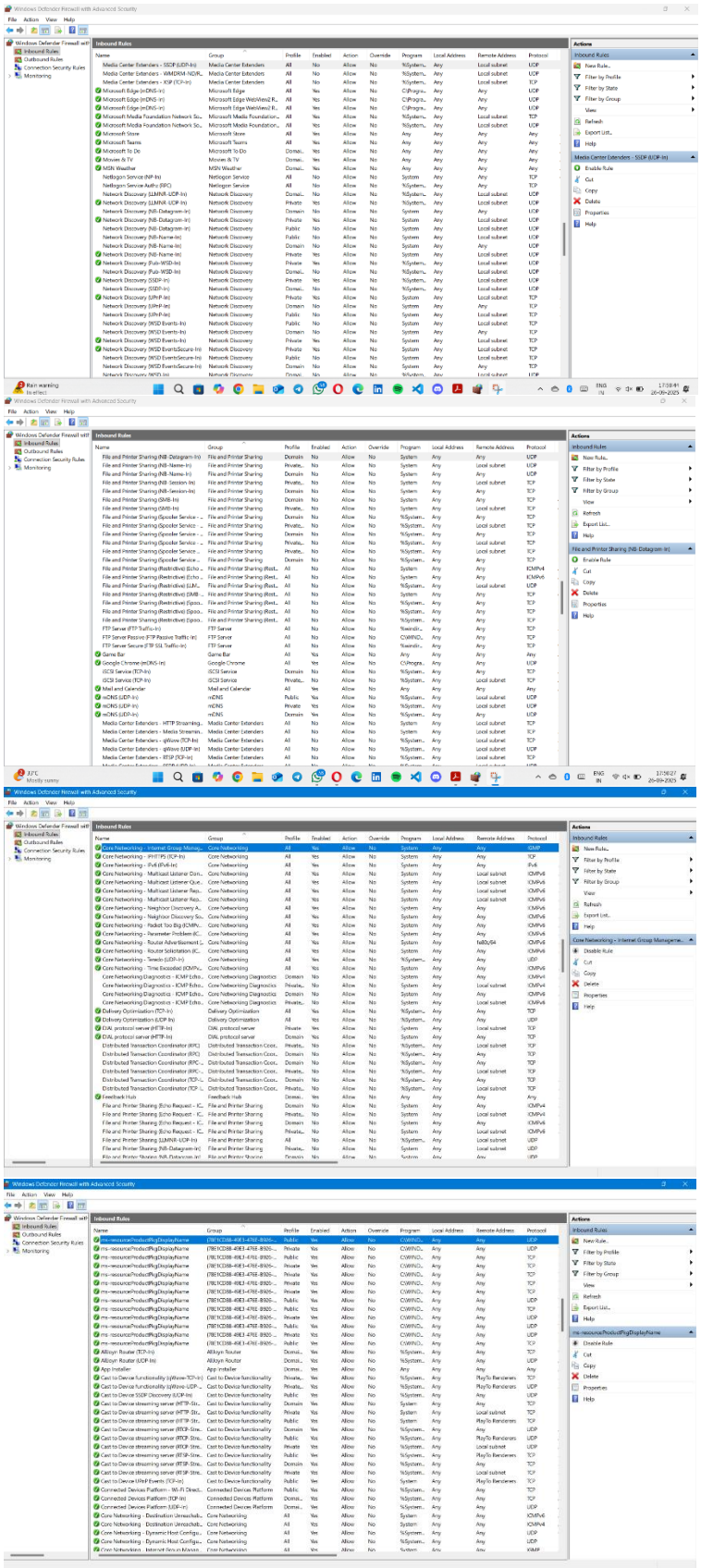
Inside the Firewall Manager, I navigated to **Inbound Rules**. This section displayed a long list of pre-configured rules that manage the traffic for different applications and services. I reviewed these existing rules as a baseline before applying new custom rules. Pasted below

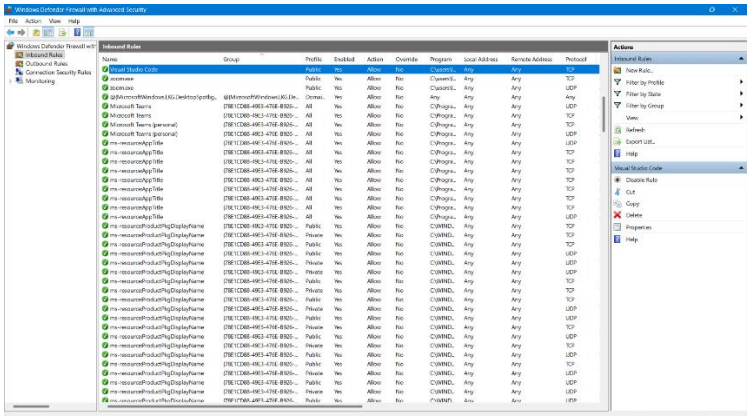


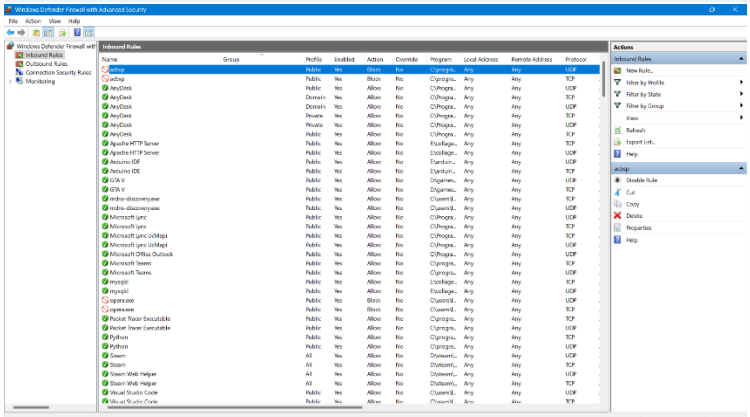


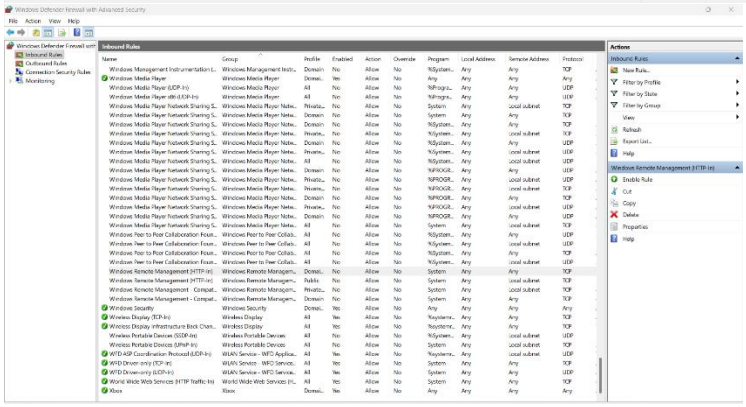












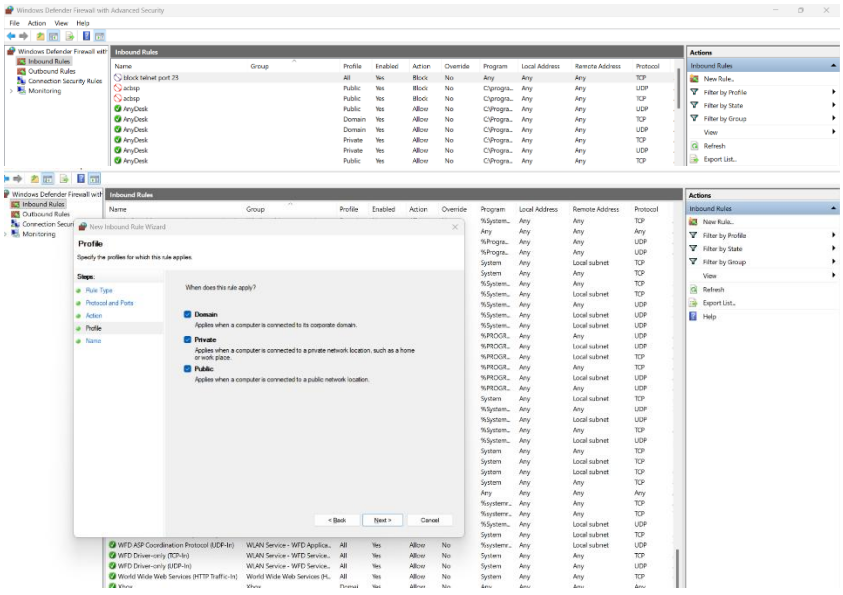
PTO.

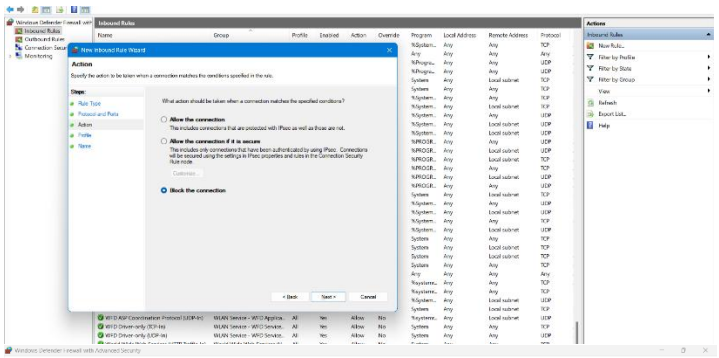
Step 3: Add a rule to block inbound traffic on a specific port.

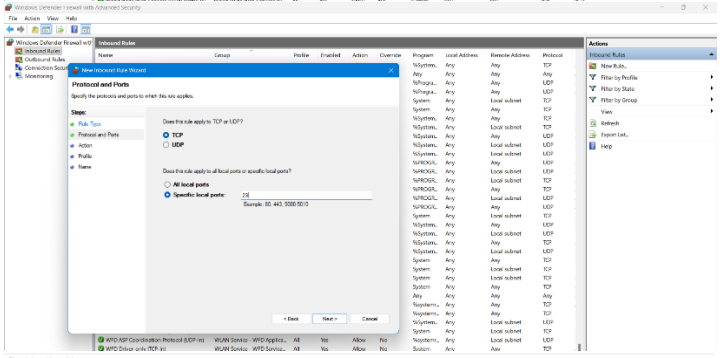
To block Telnet, I created a new inbound rule:

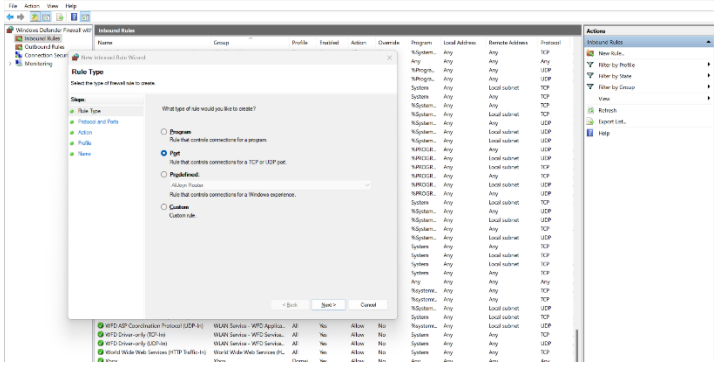
- Clicked **New Rule…** from the right panel
- Selected **Port** → clicked **Next**
- Chose **TCP**
- Entered **23** in “Specific local ports”
- Selected **Block the connection**
- Applied the rule to **Domain, Private, Public** profiles
- Named the rule: **Block Telnet (Port 23)**
- Clicked **Finish**

The rule appeared in the inbound rules list. As Demonstrated Below:




New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
25
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

Step 4: Testing the Rule.

Test the rule by attempting to connect to port 23

Before testing, I enabled Telnet Client:

- Opened **Control Panel → Programs and Features → Turn Windows features on or off**
- Checked **Telnet Client**
- Clicked **OK**

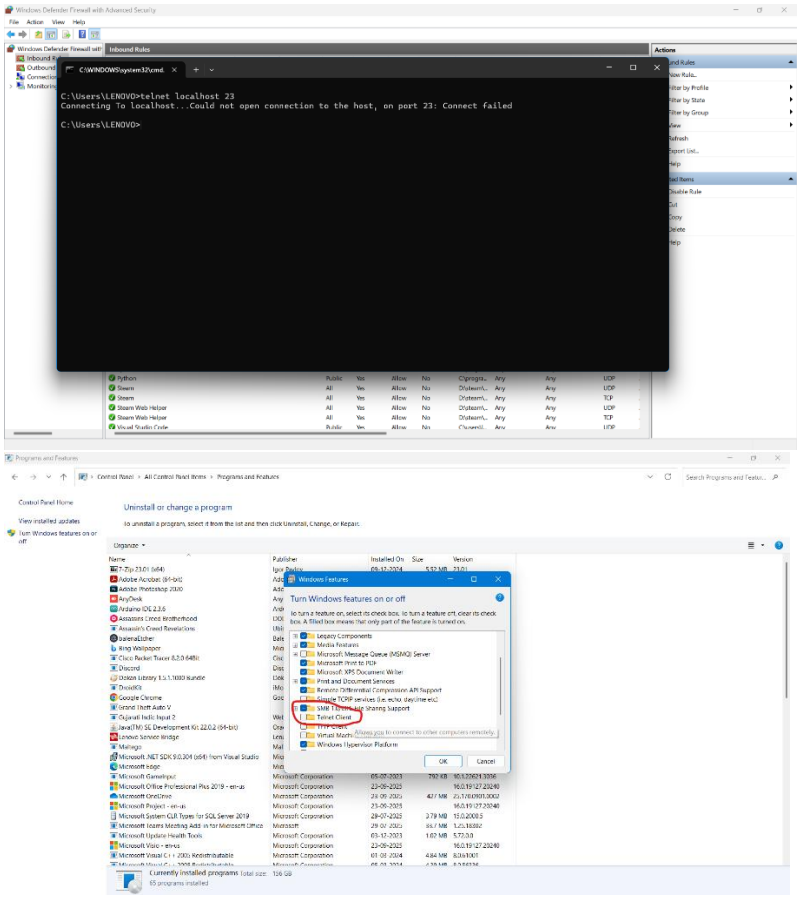
Then I tested the rule using Command Prompt:

- Ran the command:

  telnet localhost 23

The connection failed, proving the firewall rule was blocking inbound Telnet traffic on port 23.

As Demonstrated below.



Step 5: Remove the test block rule to restore original state

After confirming the rule worked, I removed it:

- Went back to **Inbound Rules**
- Located **Block Telnet (Port 23)**
- Right-clicked → **Delete**

This restored the firewall back to its original state.

Summary.

The main commands and GUI steps I used during this task were:

- **Win + R → wf.msc** (open Firewall Manager)
- **Inbound Rules → New Rule… → Port → TCP → 23 → Block the connection** (create Telnet block rule)
- **Control Panel → Programs and Features → Turn Windows features on or off → enable Telnet Client**
- **telnet localhost 23** (test Telnet connection)
- **Right-click rule → Delete** (remove custom firewall rule)

A firewall works by filtering traffic based on predefined rules.

- If a packet matches a **block rule**, it is denied.
- If a packet matches an **allow rule**, it is permitted.

In this task, I demonstrated this by blocking Telnet (port 23). The firewall successfully denied access when I attempted to connect using Telnet. Later, I deleted the rule, which restored the firewall to its original state. This practical test shows how firewalls provide protection by blocking unauthorized or insecure connections while still allowing safe communication.

REGARDS,

KUSH THAKER.