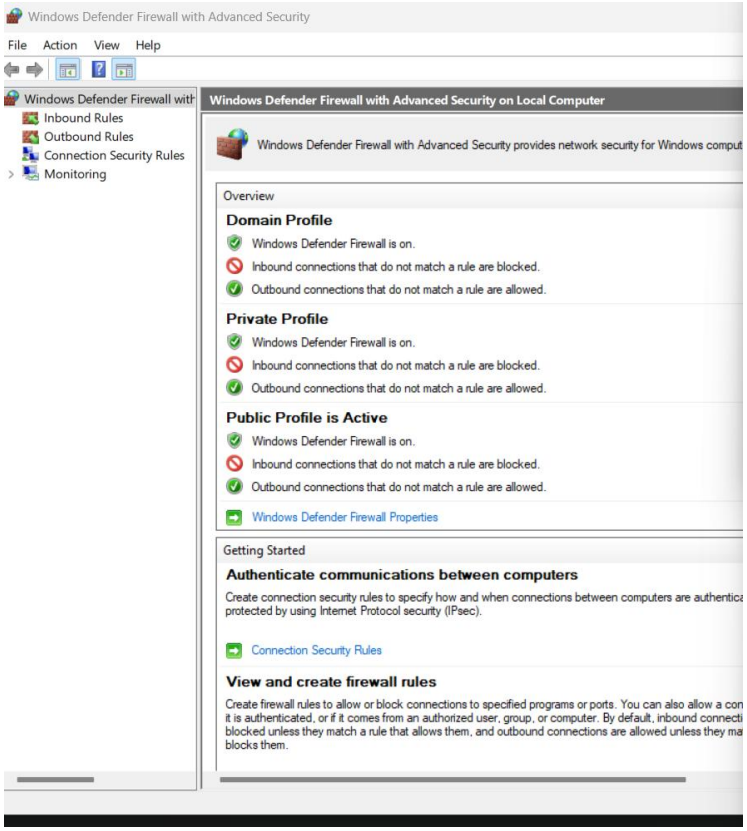
TASK 4

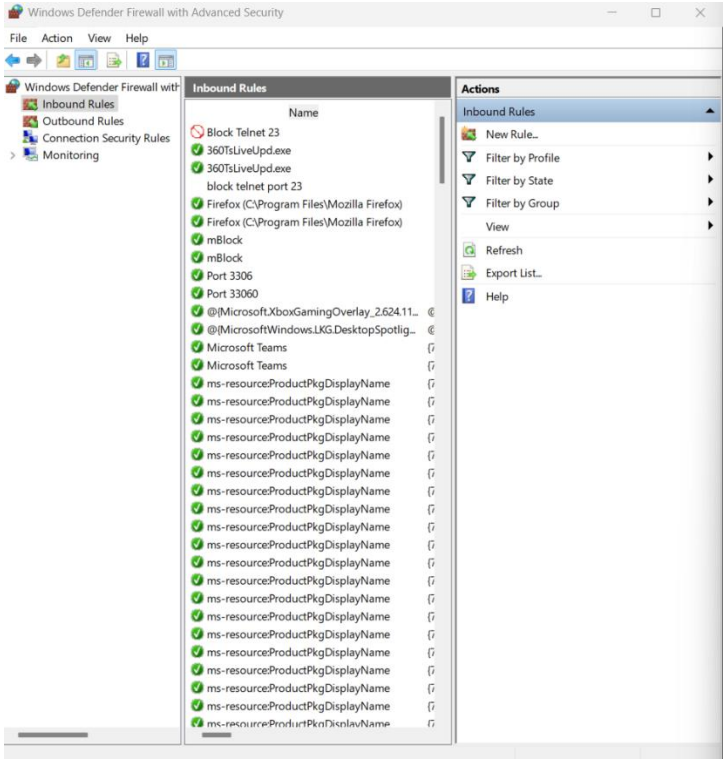
Explain the steps you followed to configure and test a firewall on Windows, including how you created a rule to block inbound traffic on a specific port, how you verified that it was blocked (e.g., using Telnet or Nmap), and how you restored the firewall to its original state. Also, briefly describe how a firewall filters traffic

Step 1 Open Firewall Configuration Tool :

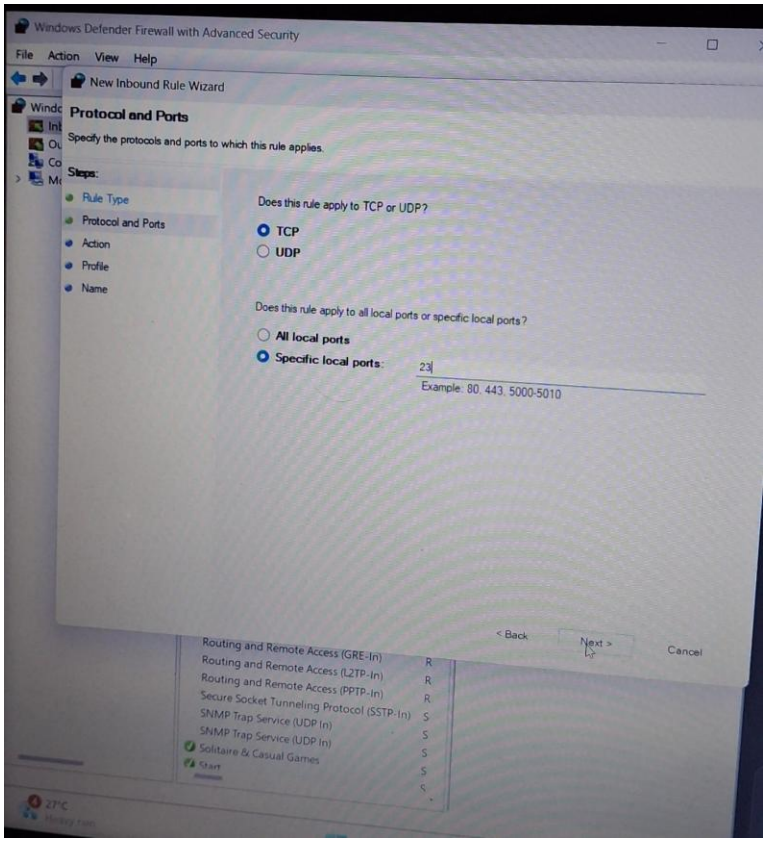
1. **Windows Defender Firewall with Advanced Security**

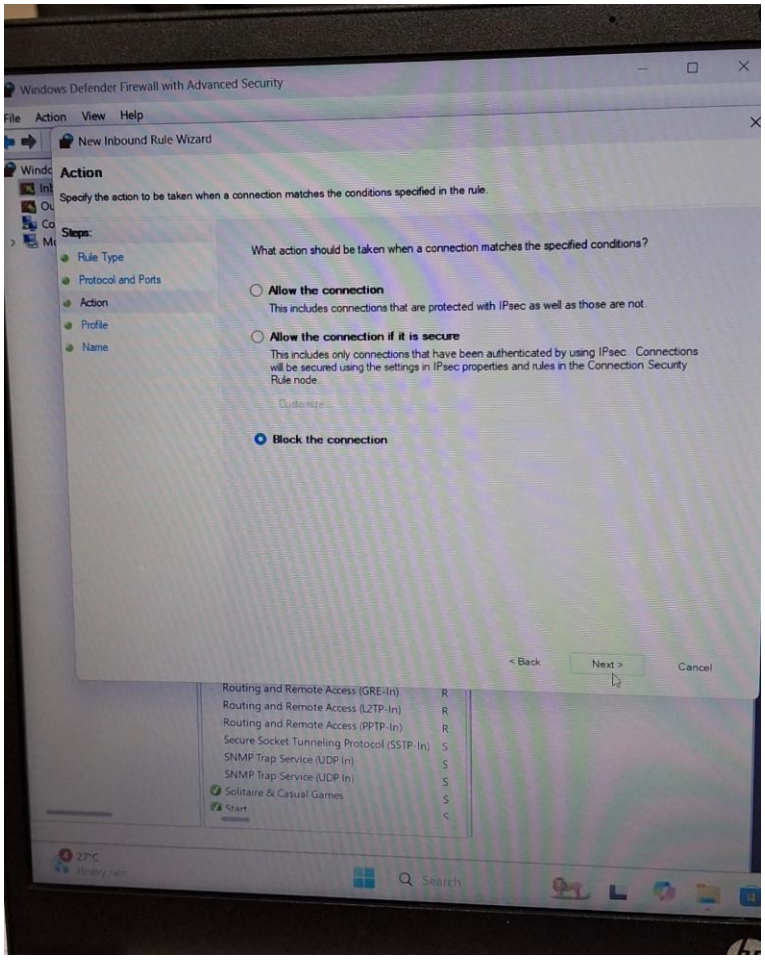


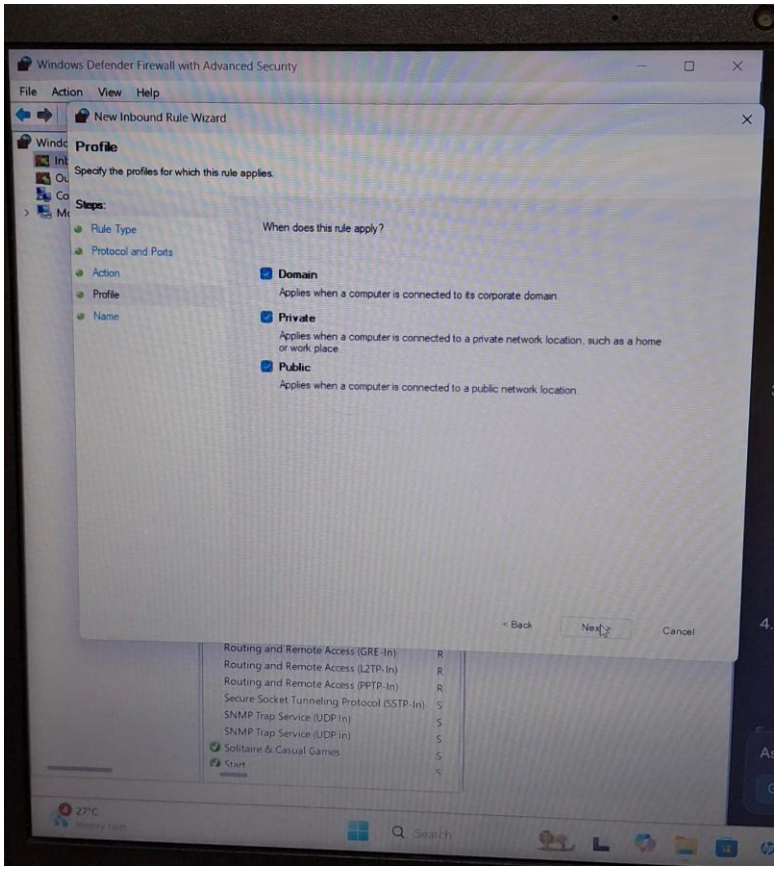
Step 2 List Current Firewall Rules:

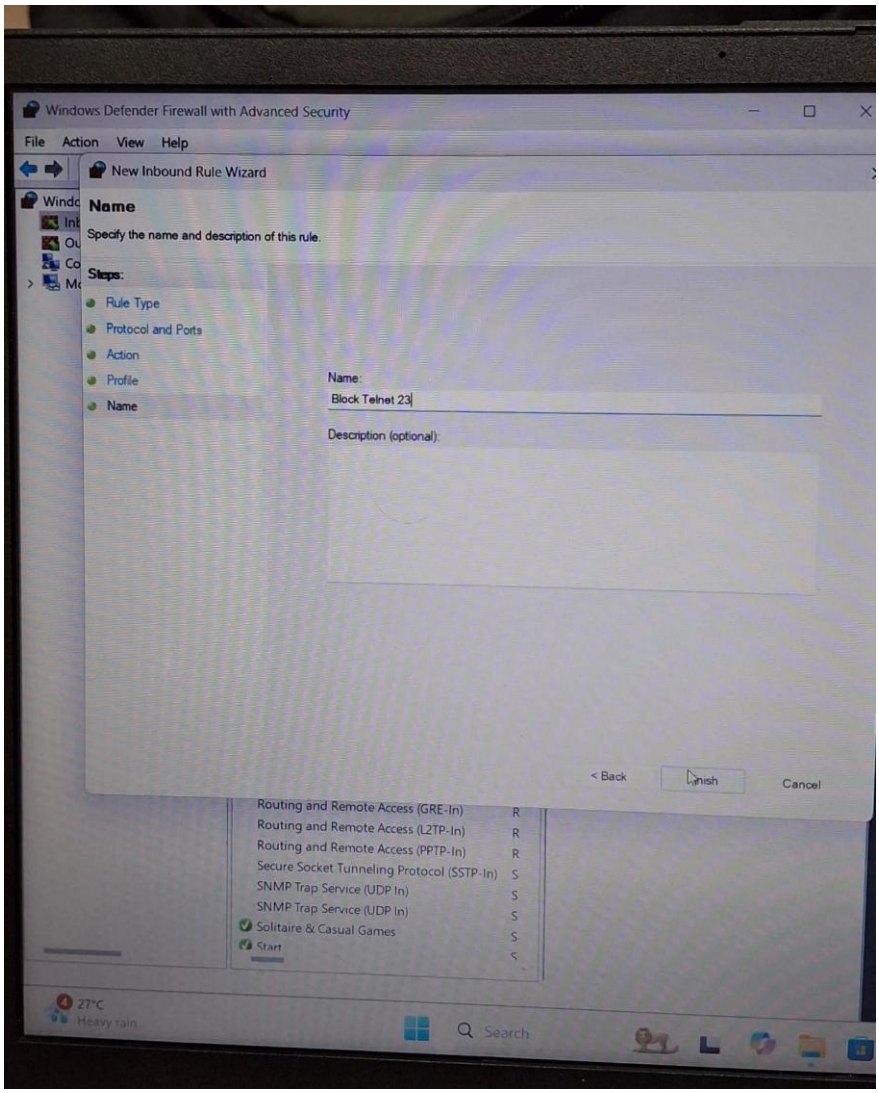


Step 3 Add a Rule to Block Inbound Traffic on a Specific Port (port 23 for Telnet):




Windows Defender Firewall with Advanced Security
File Action View Help
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
Routing and Remote Access (GRE-In)
Routing and Remote Access (L2TP-In)
Routing and Remote Access (PPTP-In)
Secure Socket Tunneling Protocol (SSTP-In)
SNMP Trap Service (UDP In)
SNMP Trap Service (UDP In)
Solitaire & Casual Games
Start
27°C
Search

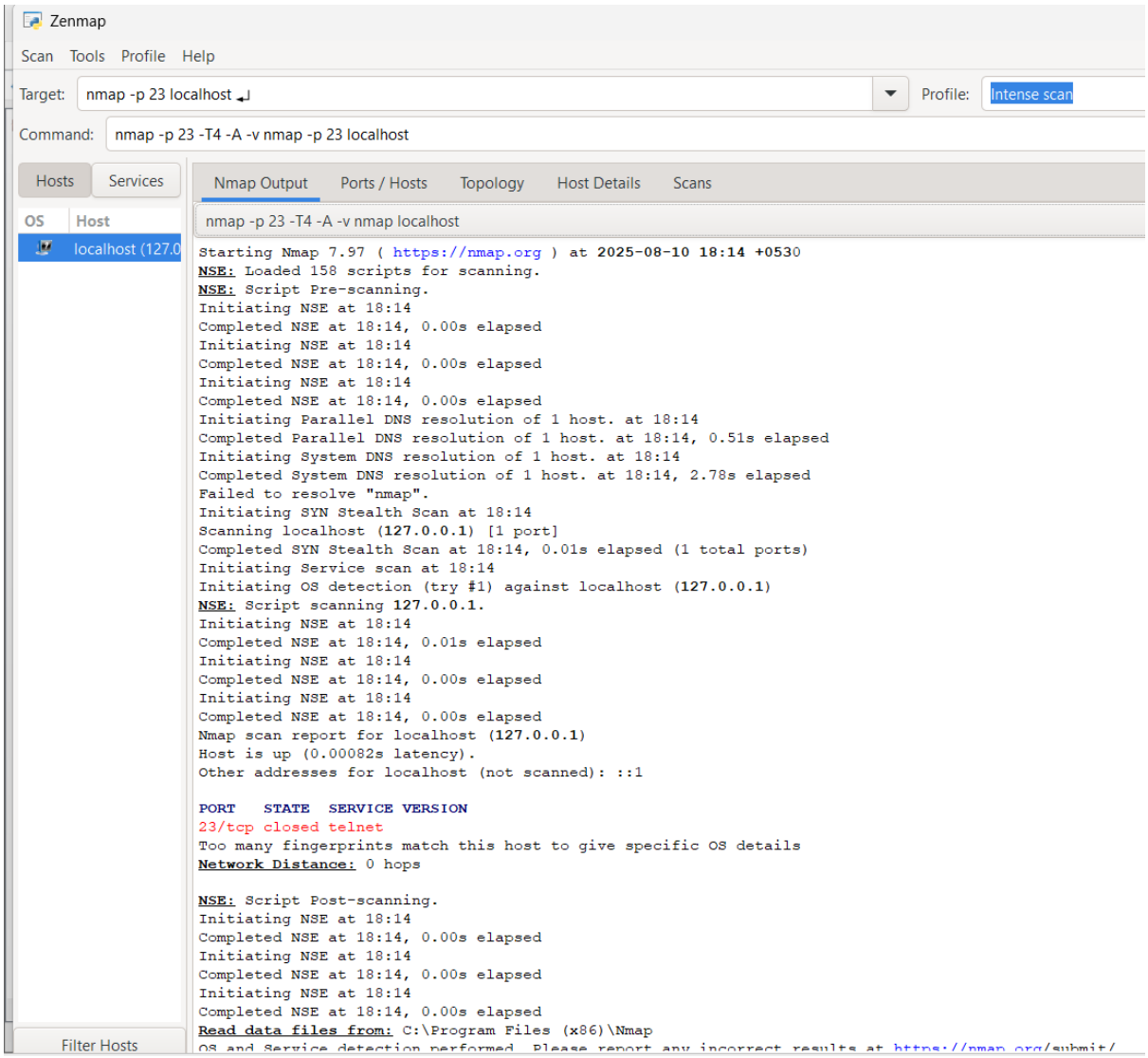

Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel
Routing and Remote Access (GRE-In)
Routing and Remote Access (L2TP-In)
Routing and Remote Access (PPTP-In)
Secure Socket Tunneling Protocol (SSTP-In)
SNMP Trap Service (UDP In)
SNMP Trap Service (UDP In)
Solitaire & Casual Games
Start
27°C
Search

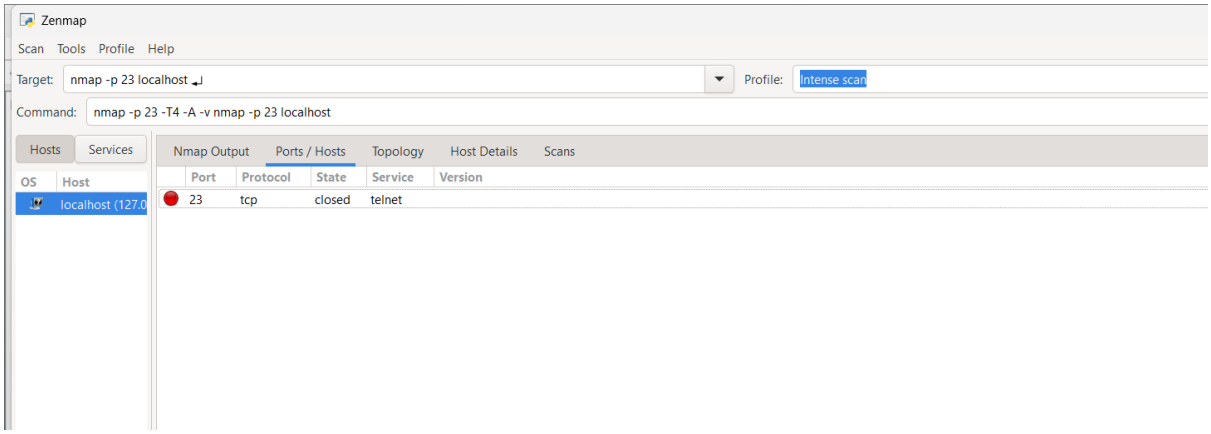


- "Inbound Rules" → "New Rule" (on the right-hand side).
- Choose Port, then click Next.
- Select TCP, specify the port number "23", then click Next.
- Choose Block the connection, then click Next.
- Select when this rule applies (Domain, Private, Public), typically all three, then Next.
- Name the rule something like "Block Telnet Port 23," then Finish

Step 5 Test the Rule:

I'm using nmap to check the 23 port is working or not





It's showing the port is blocked

Summary:

In this task, I successfully configured and tested basic firewall rules on a Windows system. I created an inbound rule to block Telnet traffic on port 23, verified the block using Telnet and Nmap, and then removed the rule to restore the firewall to its original state. This practical exercise demonstrated how a firewall can filter network traffic based on predefined rules, allowing or denying connections by criteria such as port number and protocol. The activity reinforced my understanding of how firewalls protect systems from unwanted or potentially harmful network access