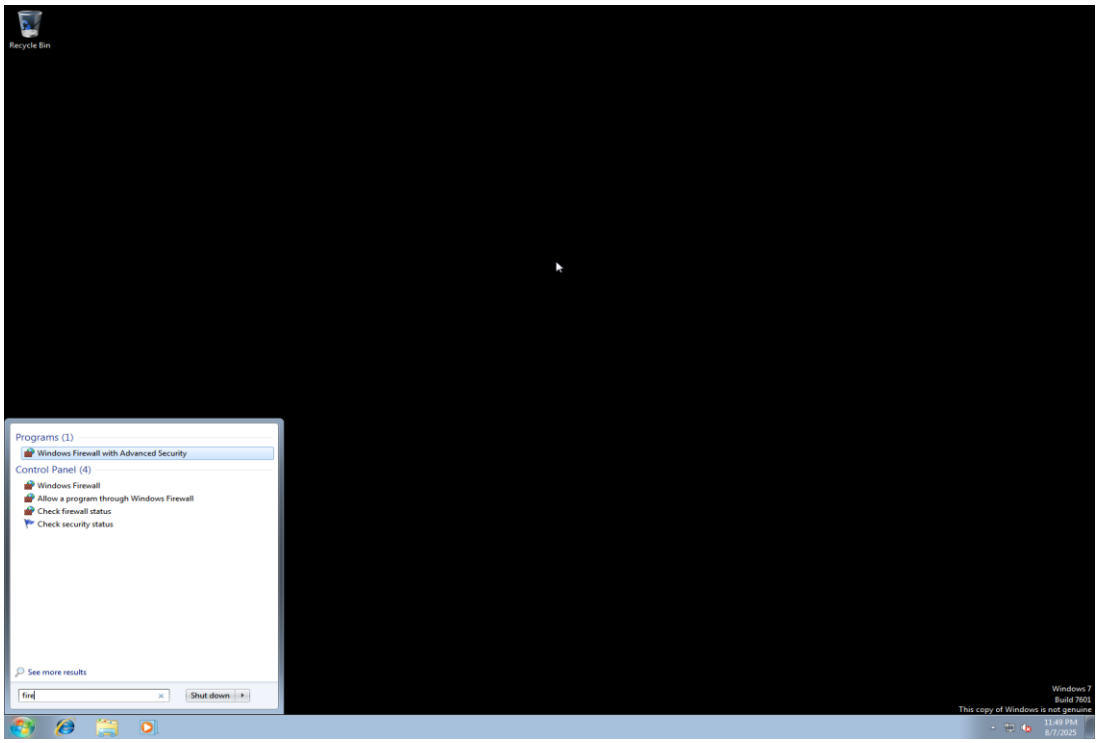
Setup and Use a Firewall on Windows/Linux

Step 1: Open Firewall Configuration Tool



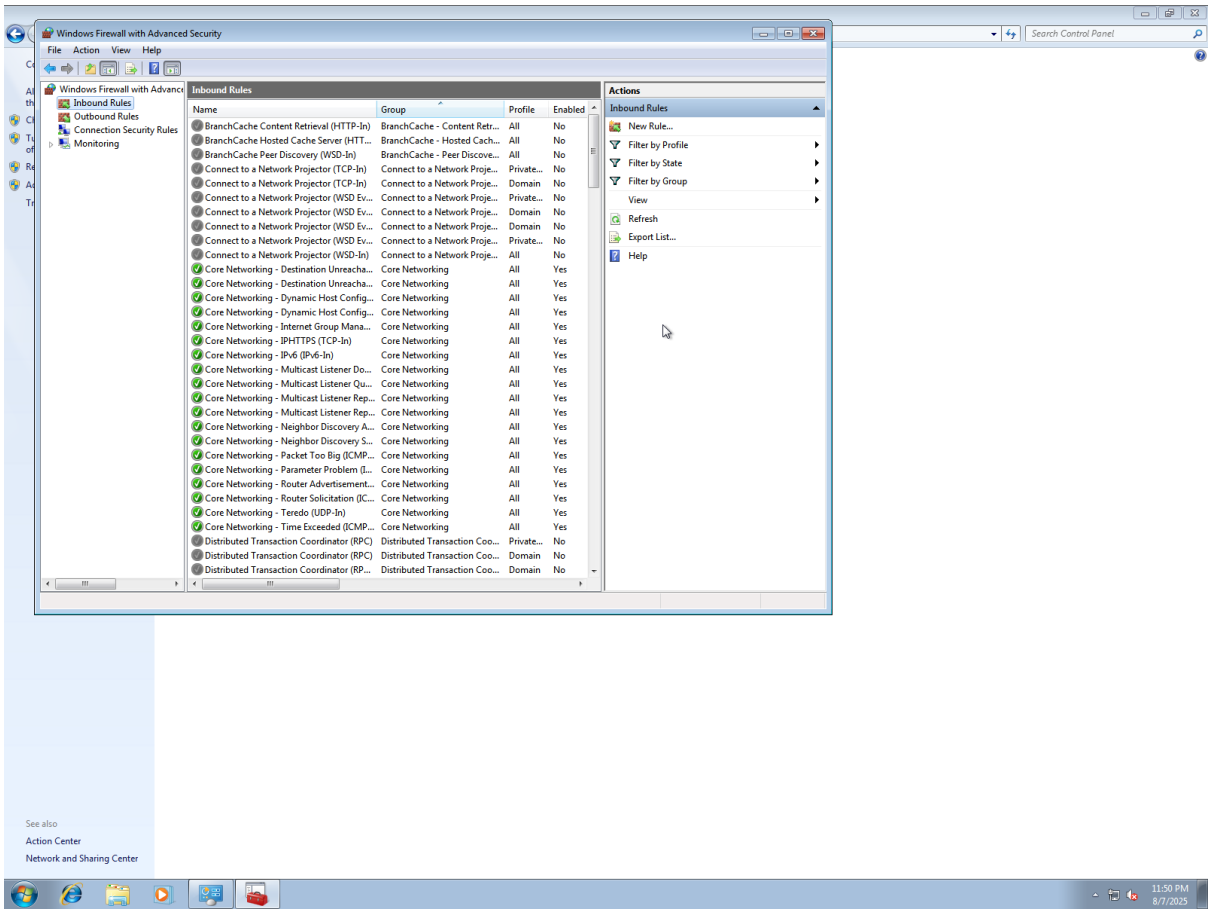
Access Windows Firewall:

- Click **Start** > Search Type> **Windows Firewall**.
- Click **Advanced settings** on the left to open **Windows Firewall with Advanced Security**.

Alternative Access:

- Press **Win + R**, type wf.msc, and press **Enter**.

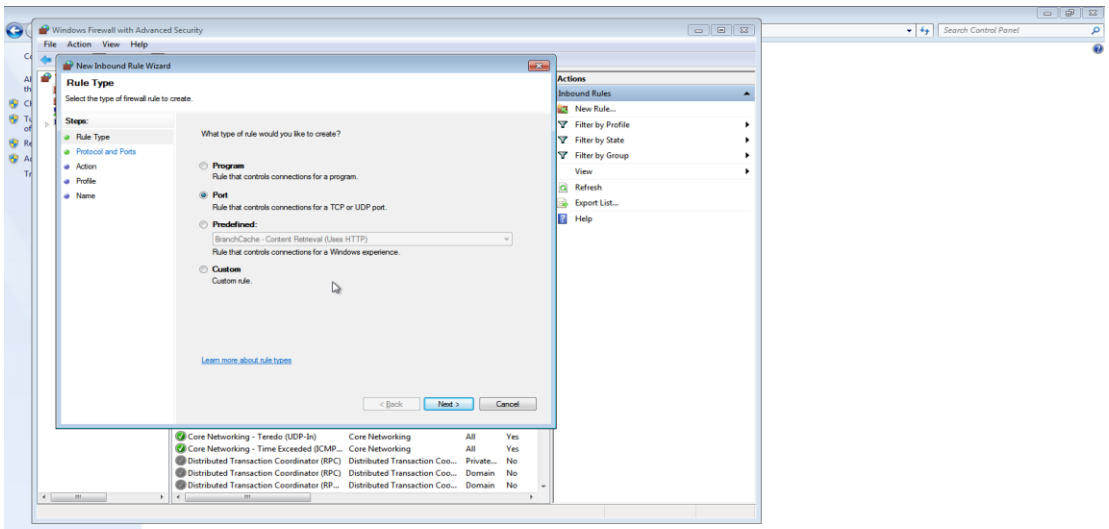
Step 2 : List Current Firewall Rules

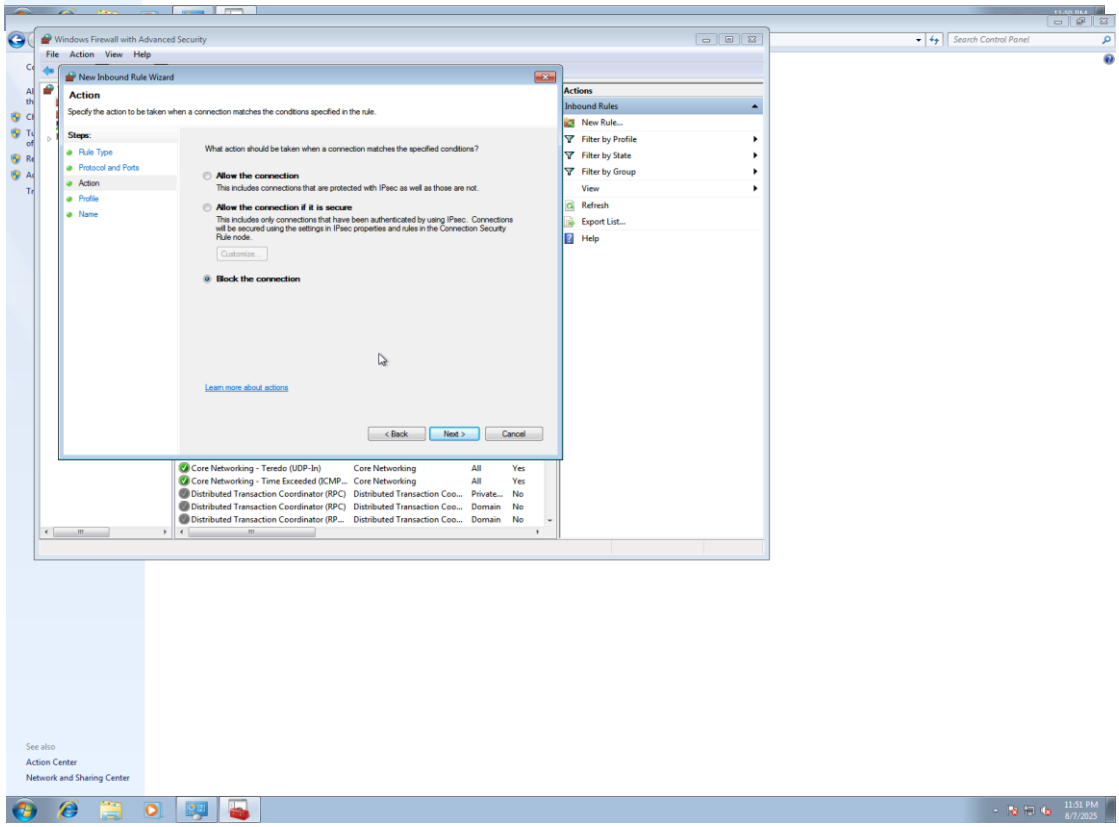


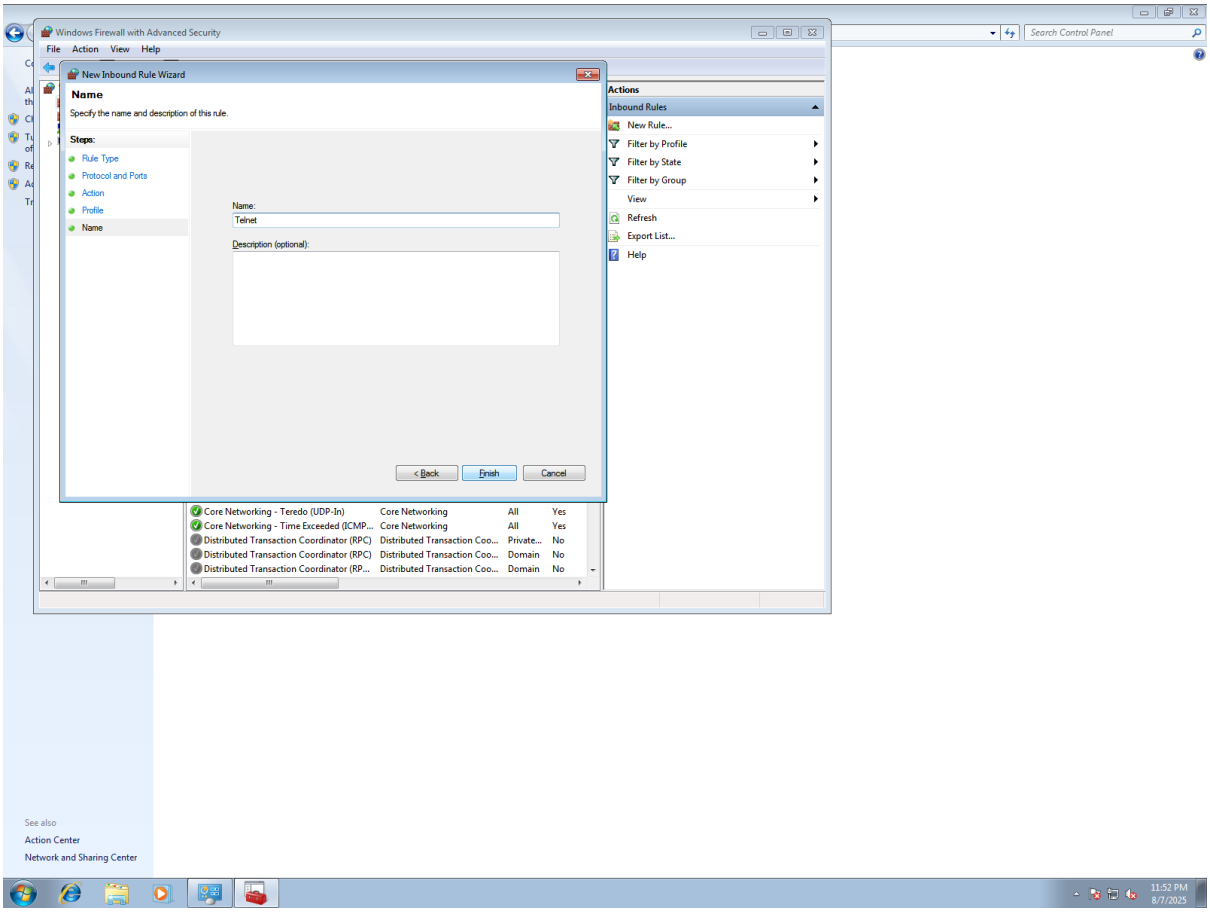
In **Windows Firewall with Advanced Security**:

- Click **Inbound Rules** or **Outbound Rules** in the left pane to view existing rules.
- Scroll through the list to see enabled rules, ports, and protocols.

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



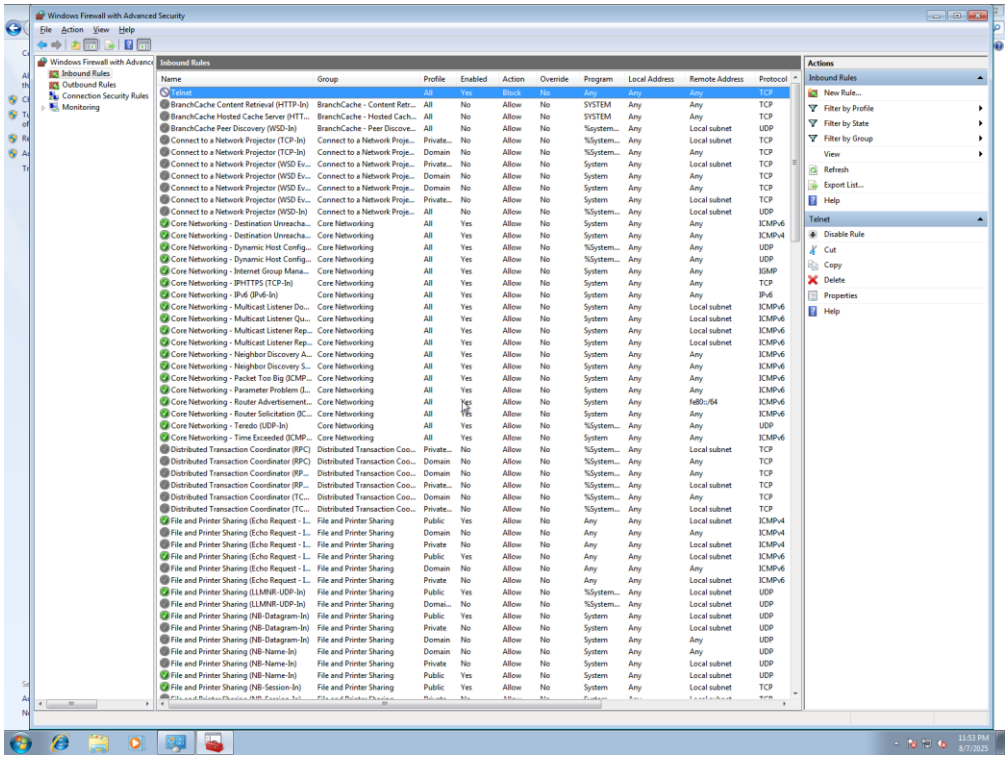


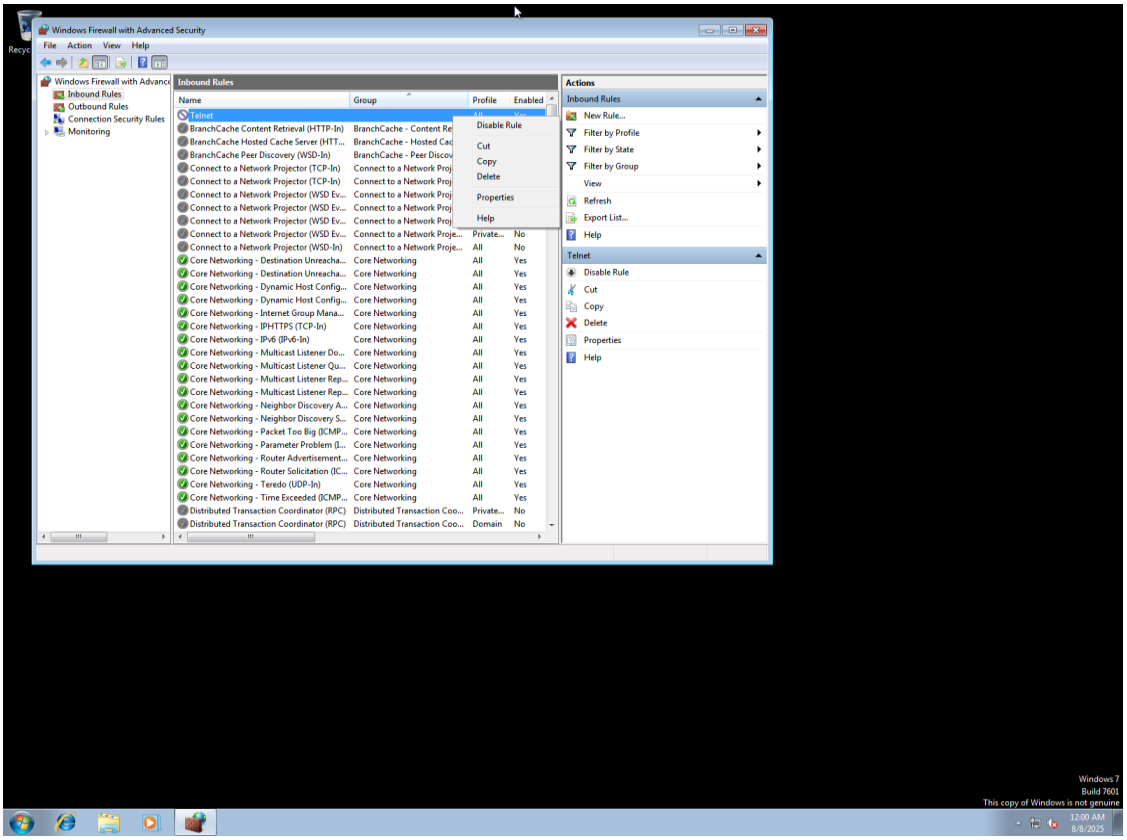


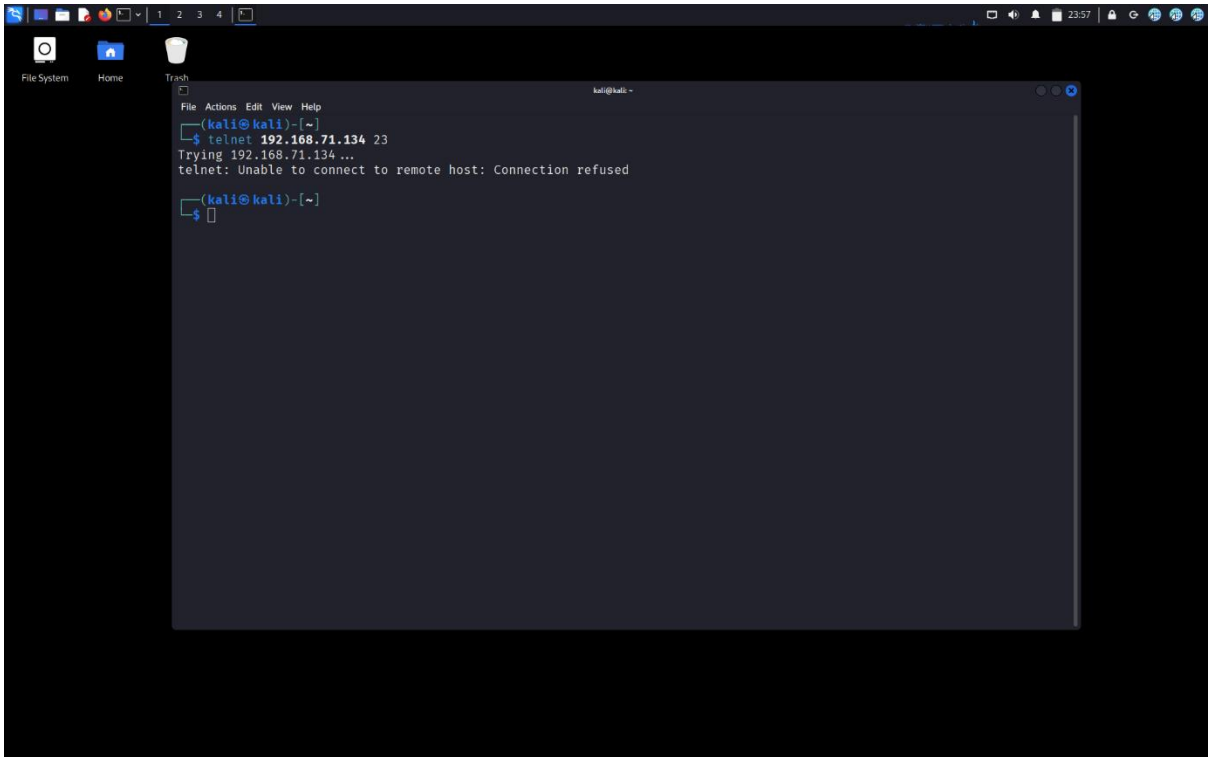
In **Windows Firewall with Advanced Security**:

- Click **Inbound Rules** > **New Rule** (right pane).
- Select **Port** > **Next**.
- Choose **TCP**, enter 23 in **Specific local ports** > **Next**.
- Select **Block the connection** > **Next**.
- Apply to all profiles (Domain, Private, Public) > **Next**.
- Name the rule (e.g., Block_Telnet_Port_23) > **Finish**.

Step 4 : Test the Rule / Remote Test



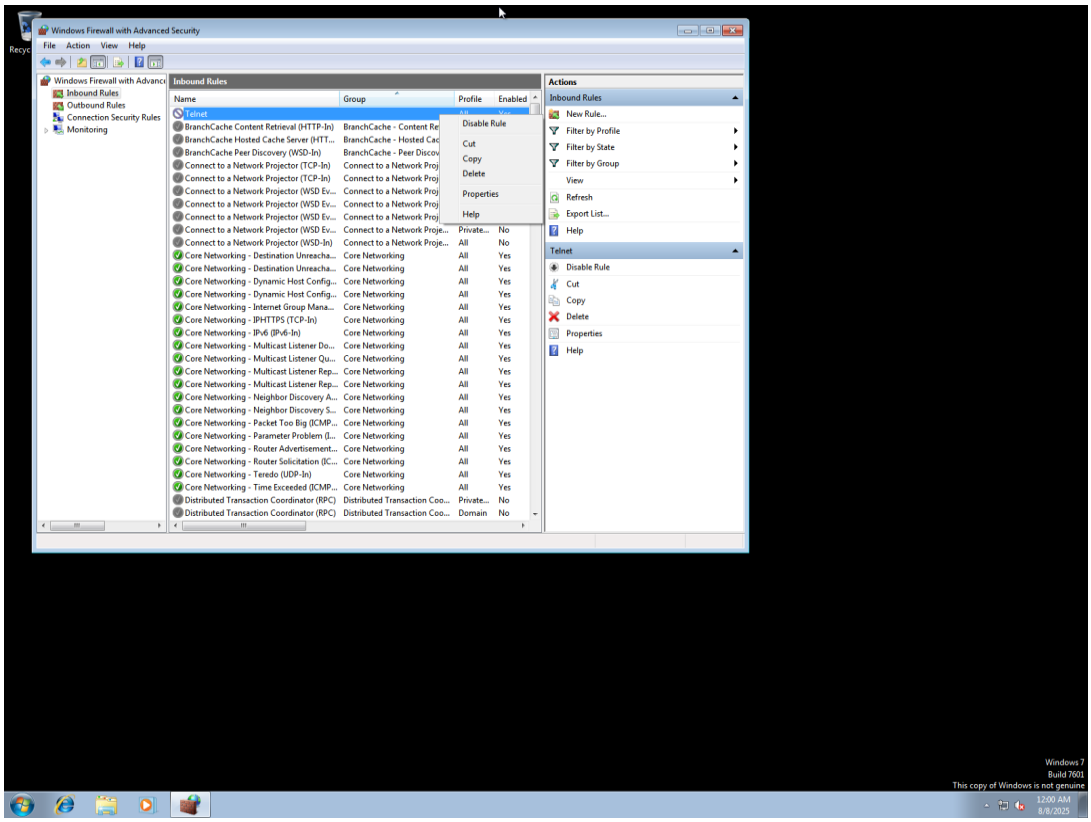




If another VM or system is available on the same VMware network:

- Run telnet <Windows7_IP> 23 from the other system (e.g., Kali Linux).
- Expected result: Connection refused.

Step 5 : Remove the Test Block Rule



In **Windows Firewall with Advanced Security**:

- Go to **Inbound Rules**.
- Find and right-click the Block_Telnet_Port_23 rule > **Delete**.
- Confirm deletion.

Step 6 : Conclusion

By Completing this Task provided hands-on experience in configuring and managing firewall rules on both Windows 7 and Kali Linux using Windows Firewall and UFW, respectively. By setting up rules to block insecure ports like Telnet (port 23) and allowing secure services like SSH (port 22), I gained practical skills in network traffic filtering and enhanced my understanding of firewall operations. This task highlighted the importance of firewalls in securing networks by controlling inbound and outbound traffic based on predefined rules. Documenting the process and testing the rules reinforced problem-solving abilities and the significance of precise configuration to prevent unauthorized access. The knowledge acquired, including the differences between stateful and stateless firewalls and common configuration pitfalls, will be valuable for building secure network environments in future cybersecurity tasks.