TASK 4: SETUP A FIREWALL AND USE IT

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 4:

Setting up a Firewall in Windows

Index

Objective

Configure and test basic firewall rules to allow or block traffic

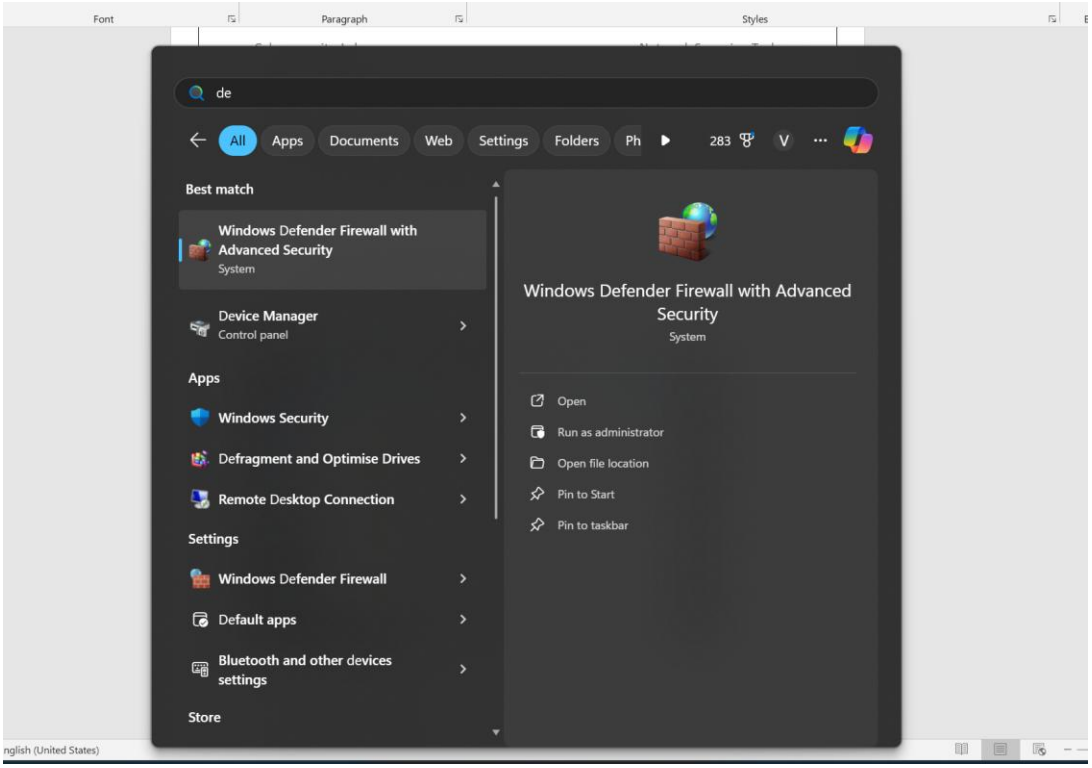
Tools Used

- Windows Firewall

Steps Performed:

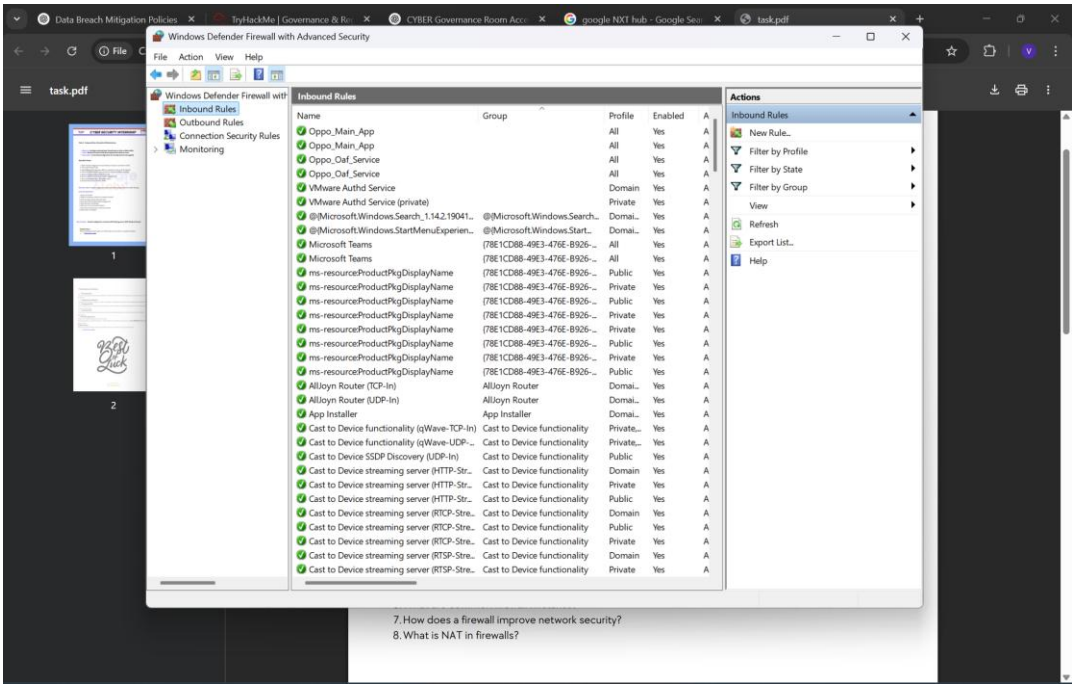
1. Open Firewall configuration tool in windows.

Search for **"Windows Defender Firewall with Advanced Security"** in Start Menu.



2. List Current Inbound Rules.

Click on **"Inbound Rules"** to view current rules.

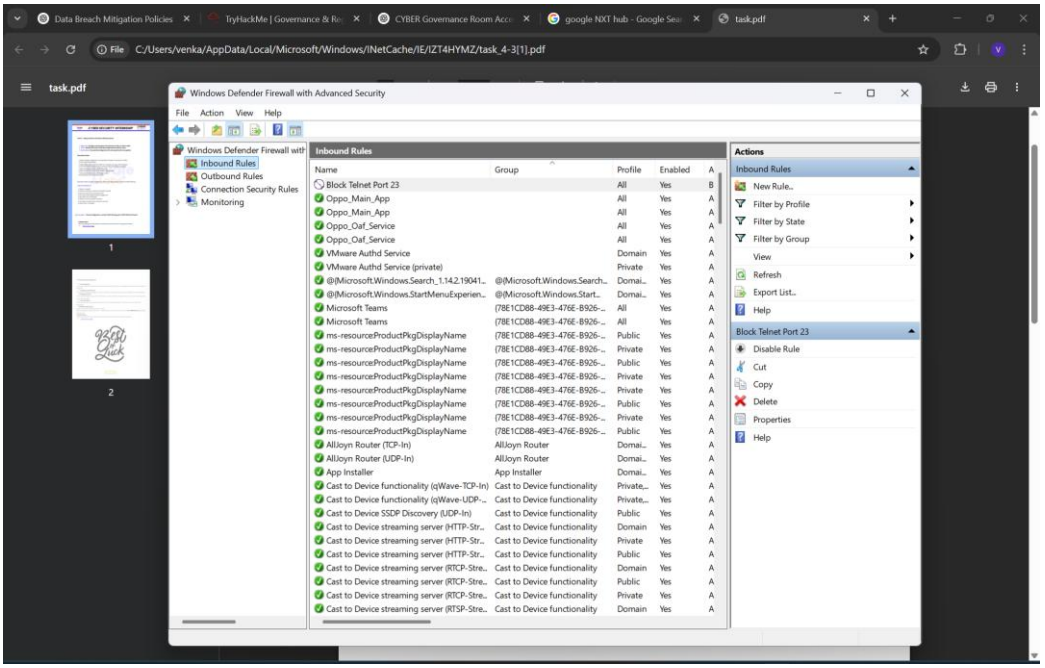


3. Block Port 23(Telnet):

Click **New Rule > Port > TCP > 23 > Block the connection**.

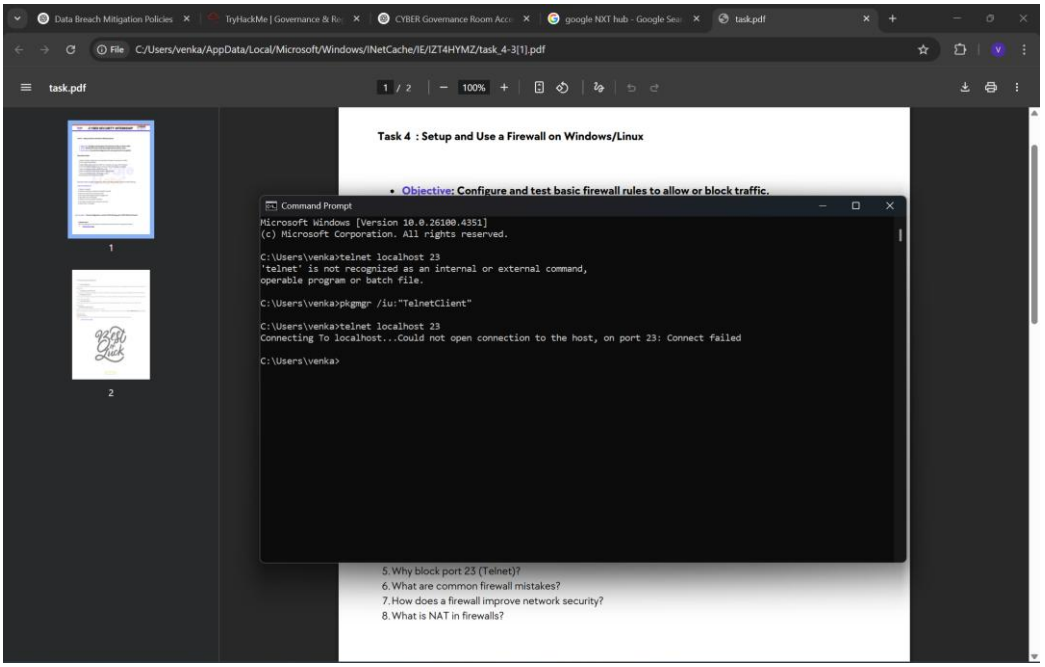
Apply to **Domain, Private, Public** profiles.

Name it: **Block Telnet Port 23**.



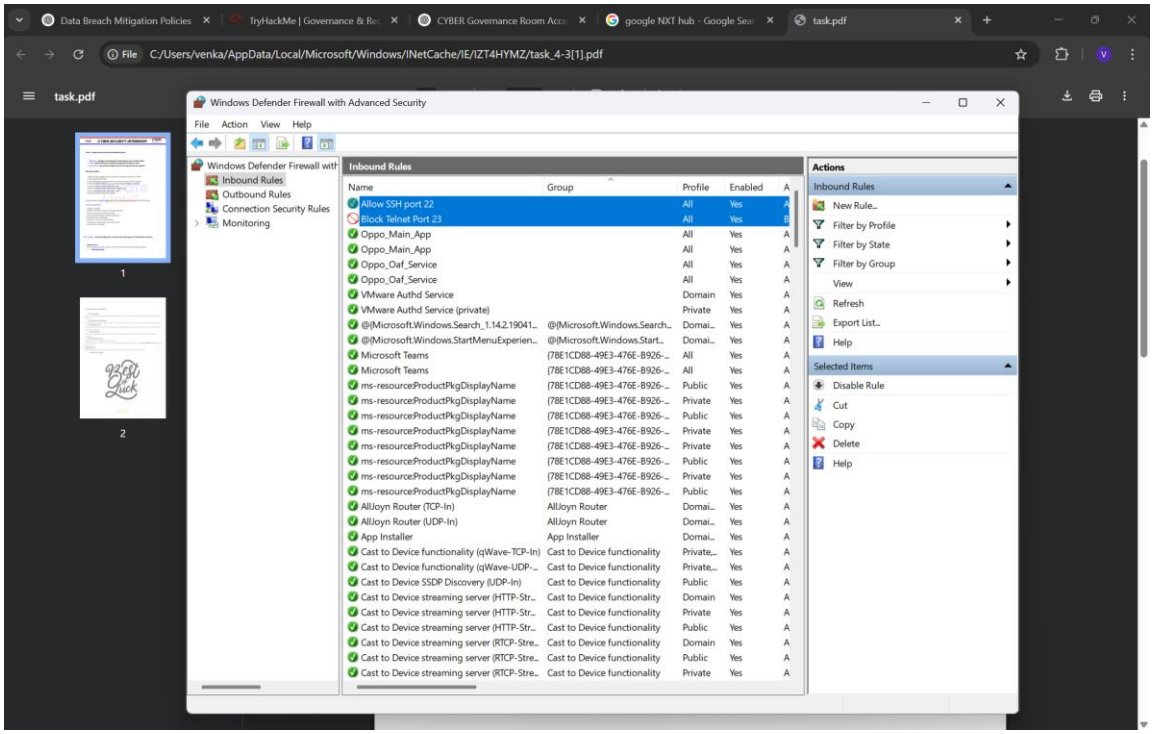
4. Test the Rule:

Open Command Prompt



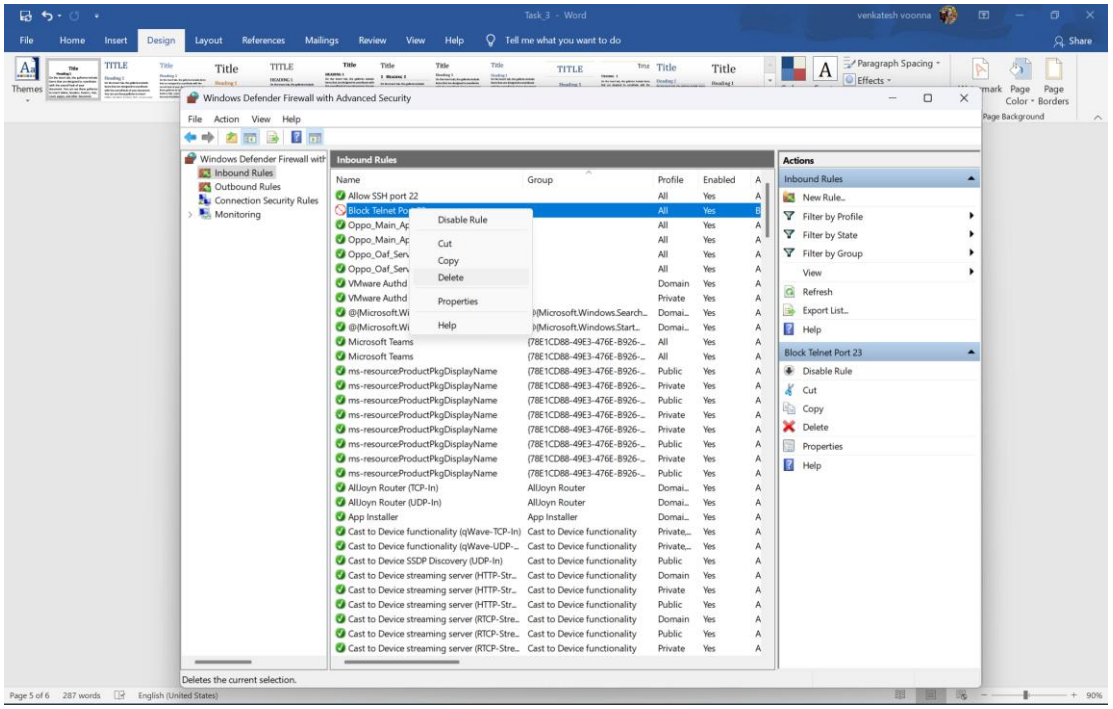
5. Allow Port 22(SSH):

Follow the Same Steps as above nut make the following Changes:
Port: 22
Action: Allow the connection
Name: Allow SSH port 22



Remove Telnet Block Rule:

Right-click the **Block Telnet Port 23** rule **> Delete.**



Conclusion:

In this task, we successfully configured basic firewall rules on both Windows and Linux systems to control network traffic. By blocking port 23 (Telnet), we demonstrated how firewalls can prevent unwanted or insecure connections. We also allowed port 22 (SSH) to ensure secure remote access. Testing and reviewing these rules helped reinforce the importance of firewalls in protecting systems from unauthorized access and attacks. This practical exercise highlights how firewall configurations serve as a crucial first line of defense in a layered security strategy.