Intern

Imam Ashraf
Email: ashrafimam121@gmail.com
Date: 27-06-2025

Task 4

Setup and Use a Firewall on Windows

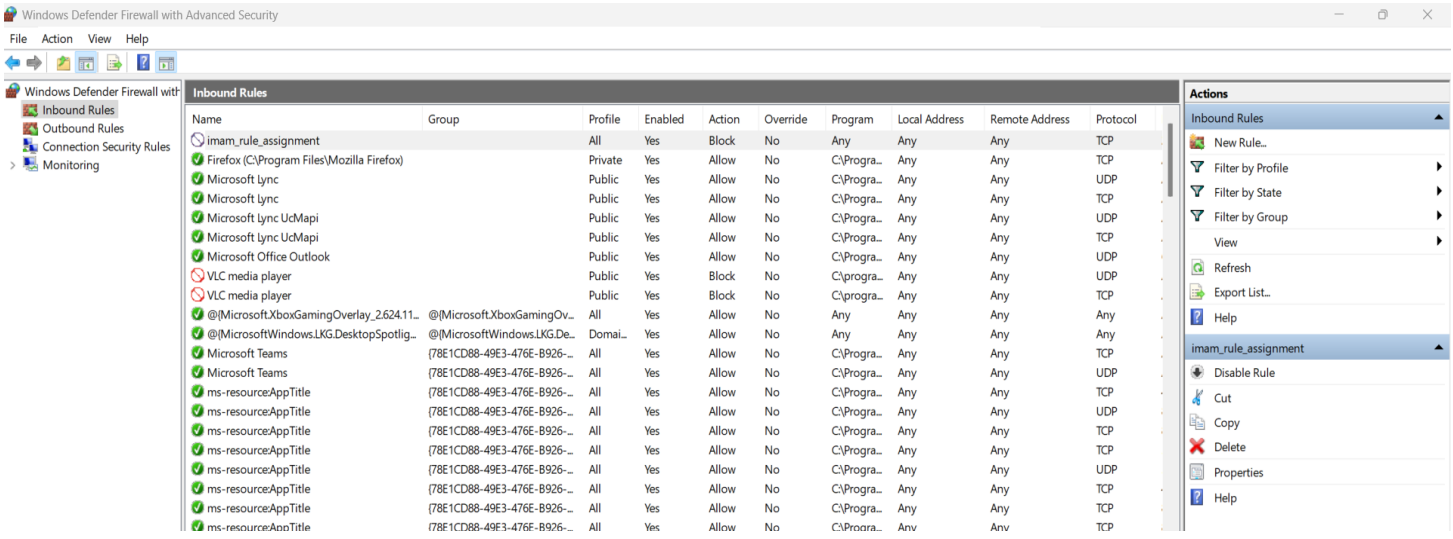
📌 Objective:

To configure and test a custom inbound rule on Windows Firewall to block all incoming traffic on TCP port 23 (used by Telnet protocol), demonstrating basic firewall configuration and traffic filtering.

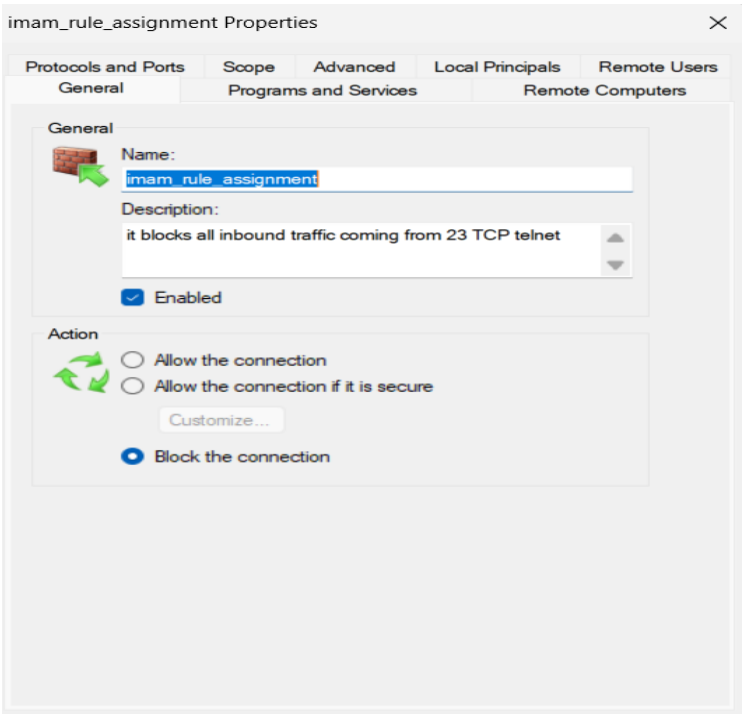
🛠 Steps Performed:

🔴 1. Block Inbound Traffic on Telnet (Port 23)

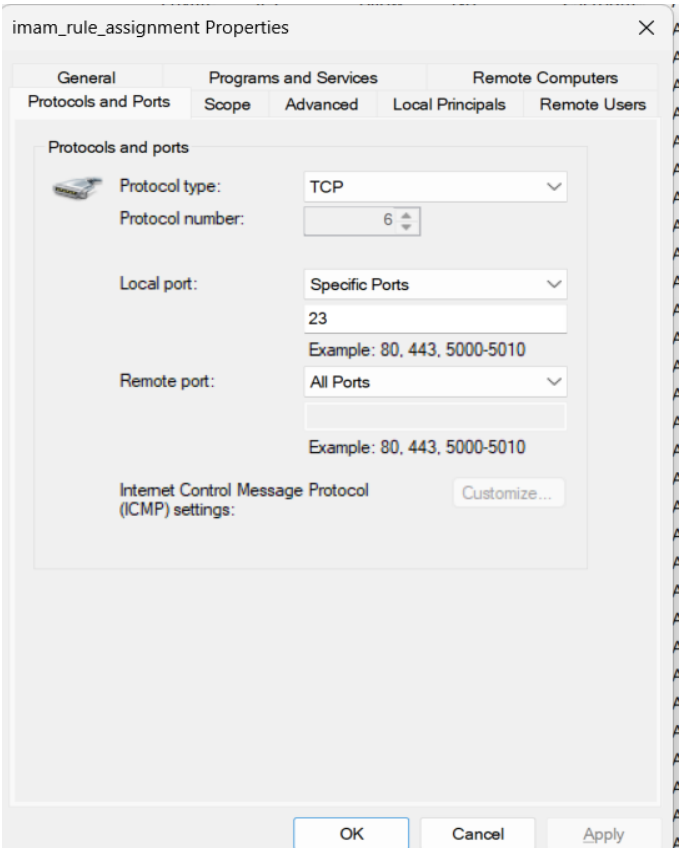
1. **Opened Windows Defender Firewall with Advanced Security**
    - Navigated to:
      Control Panel → System and Security → Windows Defender Firewall → Advanced Settings
2. **Created a New Inbound Rule**



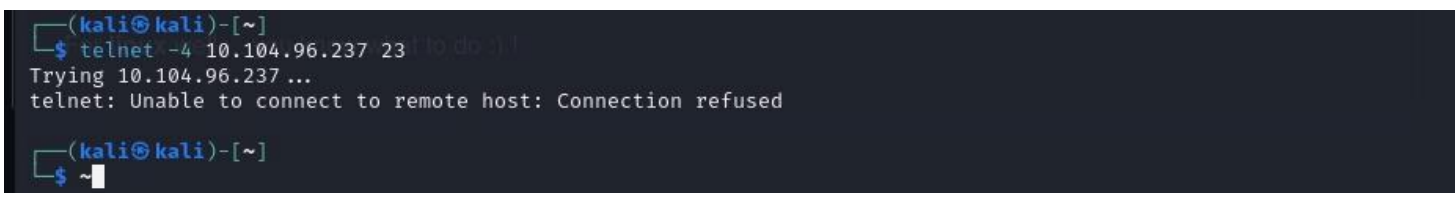
    - Action: Block the connection
    - Protocol: TCP
    - Local Port: 23
    - Name: imam_rule_assignment



- Description: *"It blocks all inbound traffic coming from 23 TCP telnet"*



- Enabled the rule immediately.



3. **Verified the Rule**
    - The newly created rule is visible in the “Inbound Rules” list with Block action and status Enabled.
    - Verified under the rule properties that the protocol is **TCP**, and the **local port is set to 23**.
4. **Screenshot Evidence**
    - **Screenshot 1:** Rule listed in Windows Firewall (imam_rule_assignment shown as Block)
    - **Screenshot 2:** General Properties with description and action selected
    - **Screenshot 3:** Protocol and Ports tab showing TCP port 23

🔍 Rule Purpose:

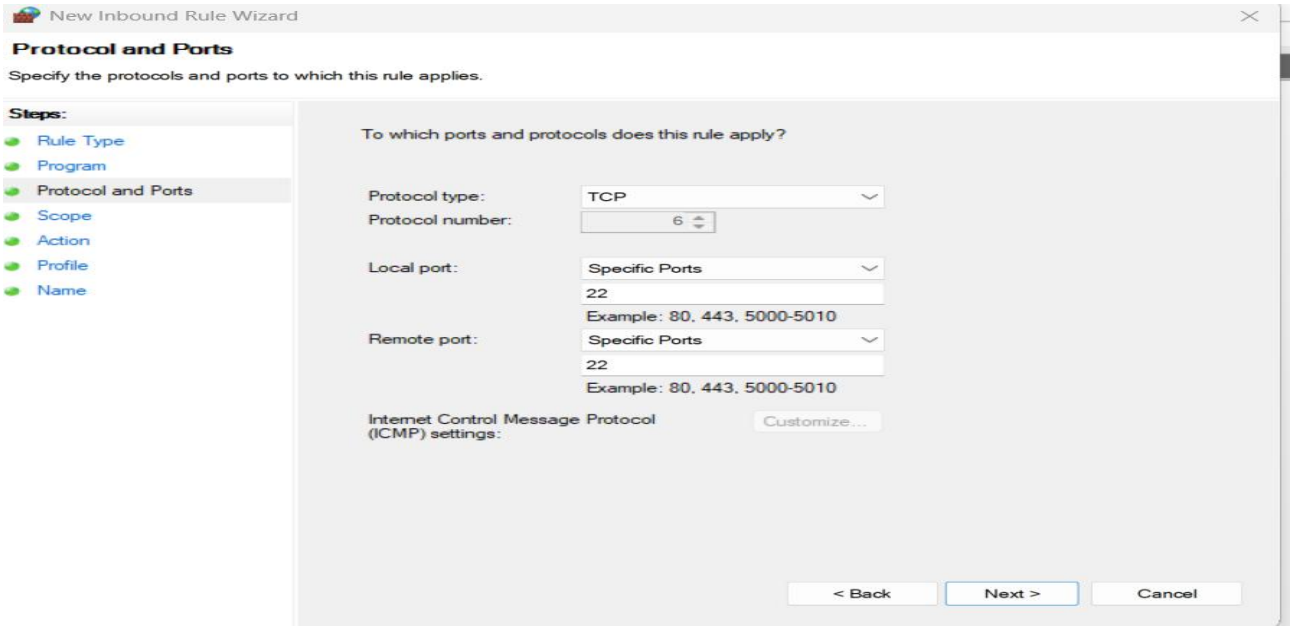
Port 23 is commonly used by **Telnet**, a protocol known to transmit data (including passwords) in plaintext. Blocking this port enhances security by:

- Preventing unauthorized remote access via Telnet
- Reducing vulnerability exposure on outdated services

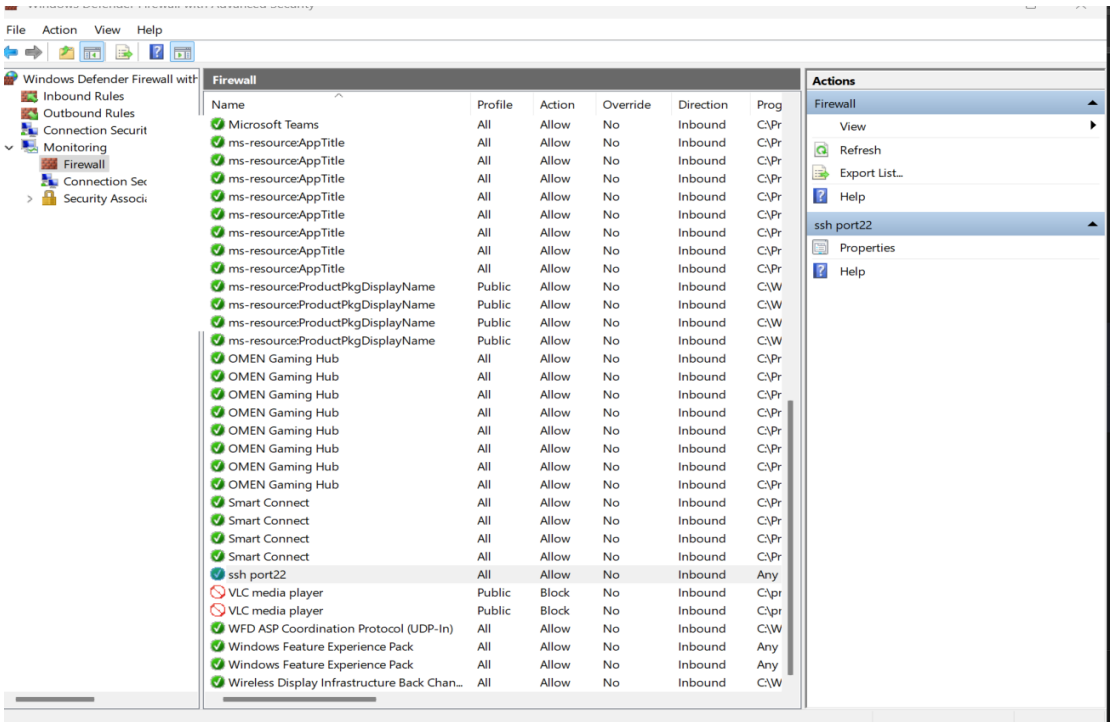
🟢 2. Allow Inbound Traffic on SSH (Port 22)

🔧 Rule Configuration Steps

1. Opened **Windows Defender Firewall with Advanced Security**
    - Path: Control Panel → System and Security → Windows Defender Firewall → Advanced Settings
2. Clicked on **Inbound Rules → New Rule...**



3. Selected the following:
    - **Rule Type:** Port
    - **Protocol:** TCP
    - **Local Port:** 22
    - **Remote Port:** 22
    - **Action:** Allow the connection
    - **Profile:** All (Domain, Private, Public)
    - **Name:** ssh port22
    - **Description:** *(Optional)*
4. Clicked **Finish** to apply the rule.



✅ Rule Verification

- The rule named ssh port22 appears in the **Inbound Rules** list with the **Allow** action.
- Confirms the system accepts SSH traffic securely over **TCP port 22**.

🔍 Purpose of Allowing Port 22 (SSH)

SSH (Secure Shell) is a secure protocol that provides encrypted remote access to systems.

Allowing SSH:

- Enables safe remote management of systems
- Supports secure file transfer (SFTP/SCP)

- Ensures encrypted communication, reducing security risks

By allowing port 22 and blocking insecure ports like 23 (Telnet), we enhance both **security** and **usability**.

Outcome:

- Learned to create, configure, and apply Windows Firewall rules
- Understood how to block specific ports for enhanced security
- Gained hands-on experience with traffic filtering

1. What is a firewall?

A **firewall** is a security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
In my task, **Windows Defender Firewall** was used to block **inbound traffic on port 23 (Telnet)**, which is a potential security risk.

2. Difference between stateful and stateless firewall?

- **Stateful Firewall:** Tracks the state of active connections and makes decisions based on the context of traffic (e.g., whether it's part of an existing connection).
- **Stateless Firewall:** Evaluates each packet individually without knowing its connection state.

Windows Defender Firewall is stateful, meaning your rule to block traffic on port 23 only applies to unsolicited inbound requests, not replies to trusted outbound requests.

3. What are inbound and outbound rules?

- **Inbound Rule:** Controls traffic **coming into** your device.
- **Outbound Rule:** Controls traffic **going out** of your device.

In my task, you created an **inbound rule** (imam_rule_assignment) to **block TCP traffic on port 23**, preventing remote systems from initiating Telnet connections to your machine.

4. How does UFW simplify firewall management?

(UFW is not used here but for Linux systems)

UFW (Uncomplicated Firewall) simplifies Linux firewall configuration by providing easy command-line tools. For example:

sudo ufw deny 23/tcp

sudo ufw allow 22/tcp

This removes the complexity of dealing directly with iptables.

- **5. Why block port 23 (Telnet)?**

Port 23 is used by **Telnet**, an insecure protocol that transmits data in **plaintext**, including usernames and passwords.
Your screenshot shows a rule specifically targeting TCP **port 23** with the action to **block the connection**, which protects the system from remote Telnet-based attacks.

- **6. What are common firewall mistakes?**

  - **Leaving default ports open**, like Telnet (23), RDP (3389), etc.
  - **Allowing unnecessary inbound rules**
  - **Not enabling the firewall**
  - **Misconfigured profiles (Public vs Private)**

My configuration correctly blocks port 23 on **all profiles**, avoiding these mistakes.

- **7. How does a firewall improve network security?**

A firewall:

- Blocks **unauthorized access**
- Controls **what services are exposed** to the network
- Prevents **exploitation of known vulnerable ports**

By blocking port 23, your firewall **prevents legacy Telnet access**, which could otherwise be exploited.

- **8. What is NAT in firewalls?**

NAT (Network Address Translation) allows a firewall/router to modify IP address information in packets to enable multiple devices on a LAN to share a single public IP address.

Though not directly visible in your Windows Firewall configuration, **NAT is typically used in routers**, and firewalls work alongside it to **filter traffic** after translation.