

# Firewall Rule Validation Report – Port 23 (Telnet)

## 1. Executive Summary

- **Objective:** To validate the effectiveness of a custom inbound firewall rule that blocks TCP traffic on port 23.
- **Environment:** Windows 11 host with Kali Linux VM (bridge mode)
- **Tools Used:** PowerShell, netstat, Windows Defender Firewall, Telnet
- **Outcome:** The firewall successfully blocked inbound Telnet traffic on port 23 when the rule was active.

## 2. Environment & Setup

<u>Component</u>	<u>Details</u>
Host OS	Windows 11
Guest OS	Kali linux ( Bridge adapter mode)
Test Port	Port 23 (Telnet)
Listener Setup	Powershell Tcp listener
Firewall Tool	Windows defender firewall

### 3. Methodology & Execution

#### Step 1: Check Active Listening Ports

- **Command Used:**

```
netstat -an | Select-String "LISTENING"
```

- **Result:** No service was listening on port 23.

PS C:\Users\Jinendra> netstat -an   Select-String "LISTENING"			
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:33060	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49688	0.0.0.0:0	LISTENING
TCP	10.253.209.169:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8884	0.0.0.0:0	LISTENING
TCP	192.168.56.1:139	0.0.0.0:0	LISTENING
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:3306	[::]:0	LISTENING
TCP	[::]:7680	[::]:0	LISTENING
TCP	[::]:33060	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49667	[::]:0	LISTENING
TCP	[::]:49668	[::]:0	LISTENING
TCP	[::]:49669	[::]:0	LISTENING
TCP	[::]:49672	[::]:0	LISTENING
TCP	[::]:49688	[::]:0	LISTENING
TCP	[::1]:49673	[::]:0	LISTENING

## Step 2: Activate Telnet Listener on Port 23

- **PowerShell Commands:**

```
$listener =  
[System.Net.Sockets.TcpListener]::new([System.Net.IPA  
ddress]::Any, 23) $listener.Start()
```

??

- **Purpose:** Simulate a service listening on port 23.

## Step 3: Confirm Port 23 is Listening

- **Command Used:**

```
netstat -an | Select-String ":23"
```

- **Result:** Port 23 is now active and listening.

```
PS C:\Users\Jinendra> $listener = [System.Net.Sockets.TcpListener]::new([System.Net.IPA  
ddress]::Any, 23)  
PS C:\Users\Jinendra> $listener.Start()  
PS C:\Users\Jinendra>  
PS C:\Users\Jinendra> netstat -an | Select-String ":23"  
  
TCP      0.0.0.0:23          0.0.0.0:0          LISTENING  
  
PS C:\Users\Jinendra> |
```

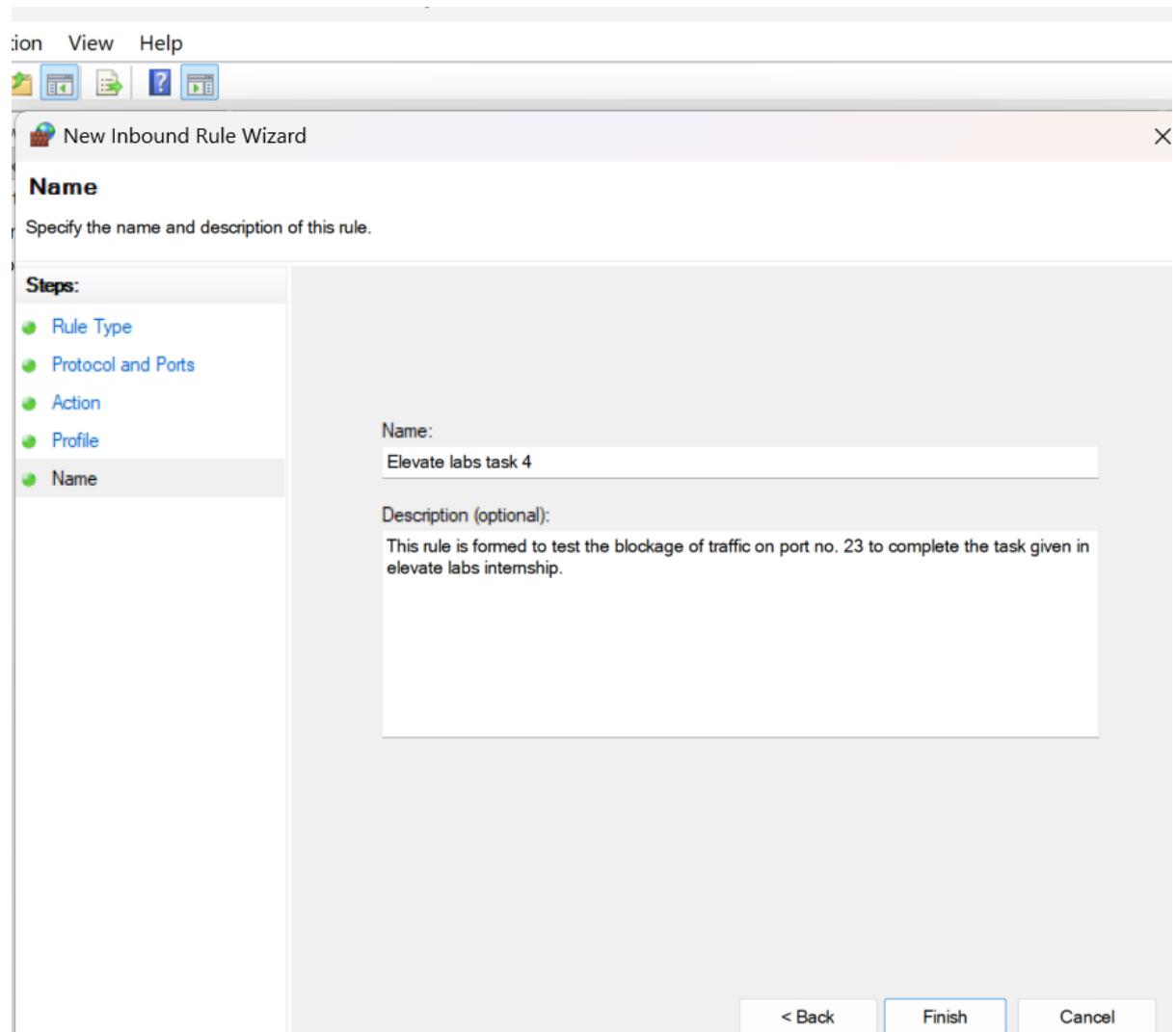
## Step 4: Create Inbound Firewall Rule to Block Port 23

- **Steps:**

1. Open Firewall & network protection → Advanced settings
2. Navigate to **Inbound Rules** → **New Rule**

### 3. Configure:

- **Rule Type:** Port
- **Protocol:** TCP
- **Port:** 23
- **Action:** Block the connection
- **Profile:** Domain, Private, Public
- **Name:** Elevate labs task 4

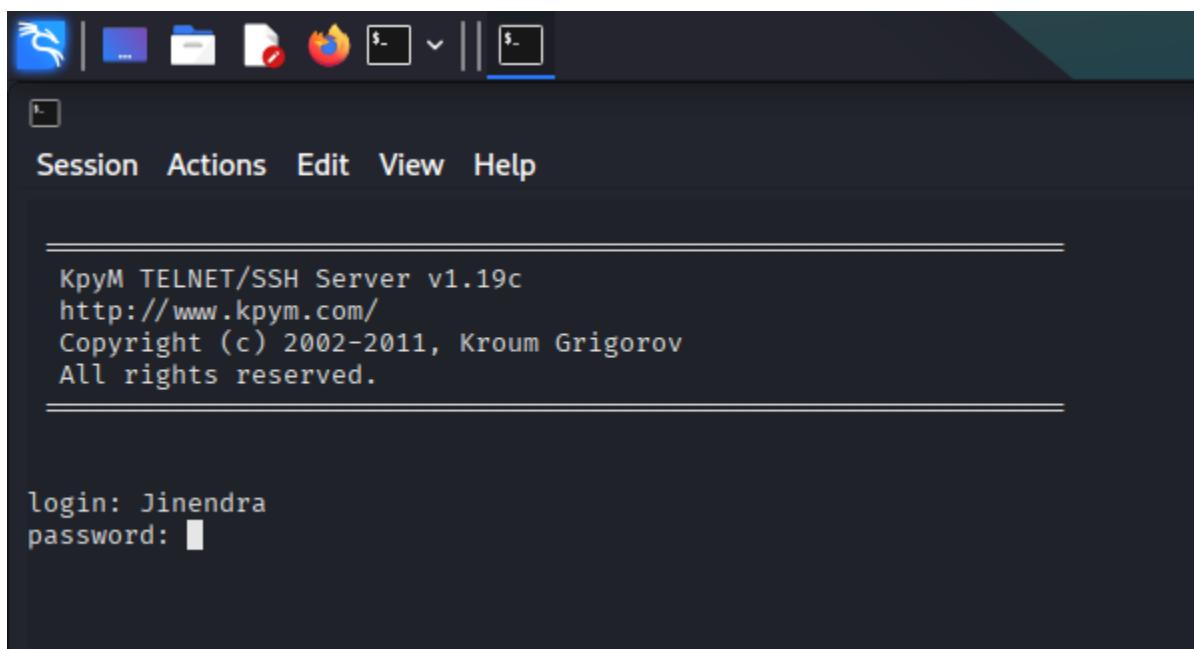


## Step 5: Test Connectivity from Kali Linux

- **Setup:** Kali VM on bridge adapter (same subnet)
- **Command Used:**

telnet <host ip> 23

- **Result:**
- Before rule: Connection successful
- After rule: Connection blocked (no response)

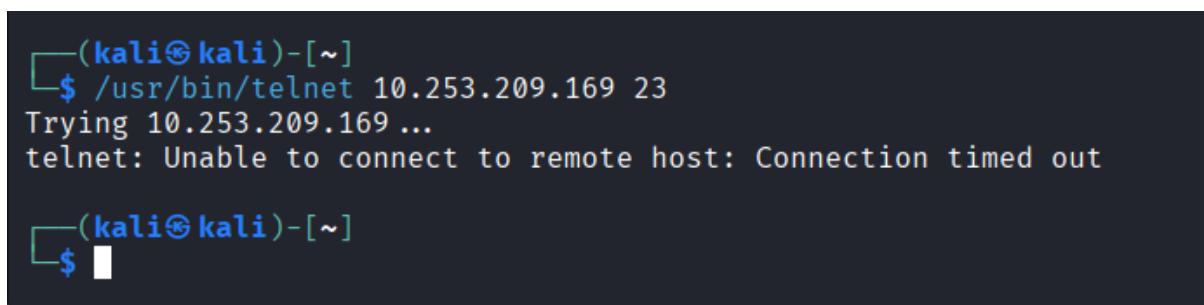


The screenshot shows a Kali Linux desktop environment. At the top is a dark blue header bar with various icons. Below it is a menu bar with "Session", "Actions", "Edit", "View", and "Help". The main window is a terminal session titled "Session 1". It displays the following text:

```
KpyM TELNET/SSH Server v1.19c
http://www.kpym.com/
Copyright (c) 2002-2011, Kroum Grigorov
All rights reserved.
```

Below this, the terminal prompt shows:

```
login: Jinendra
password: [REDACTED]
```



The screenshot shows a terminal window on Kali Linux. The command entered was:

```
$ /usr/bin/telnet 10.253.209.169 23
```

The output shows the attempt to connect to the host at 10.253.209.169 on port 23, but it fails with the message:

```
Trying 10.253.209.169 ...
telnet: Unable to connect to remote host: Connection timed out
```

## Step 6: Cleanup – Delete the Rule

- **Action:** Removed the Elevate labs task 4 rule from Inbound Rules
- **Result:** Port 23 is accessible again

## 4. Conclusion

- The firewall rule effectively blocked inbound traffic on port 23.
- The test confirmed the rule's enforcement using a real listener and external VM.
- The environment was restored to its original state post-validation.