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. Environmet & Setup

Component	Details
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

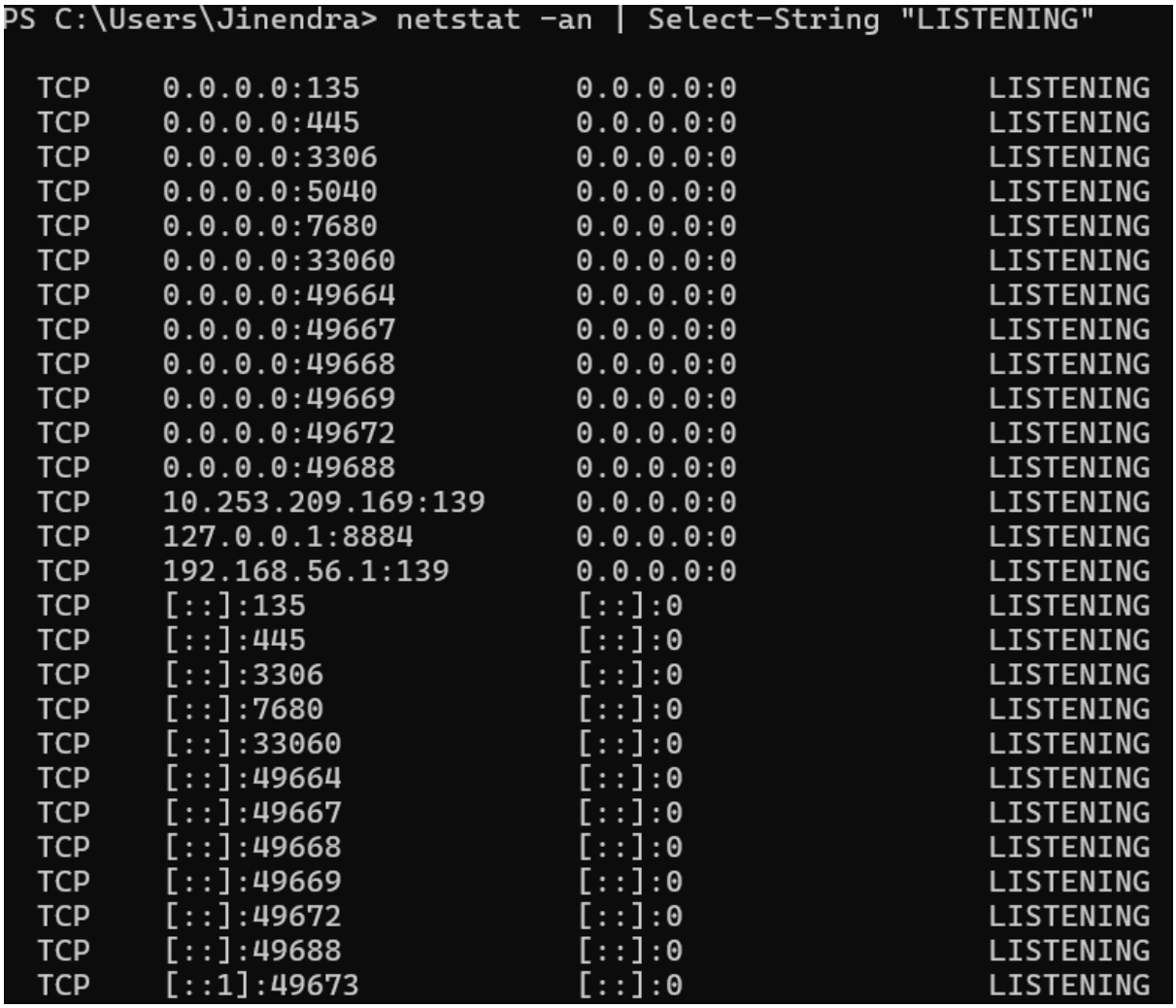
3. **Methodology & Execution**

Step 1: Check Active Listening Ports

- **Command Used**:

netstat -an | Select-String "LISTENING"

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



Step 2: Activate Telnet Listener on Port 23

- **PowerShell Commands**:

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

??

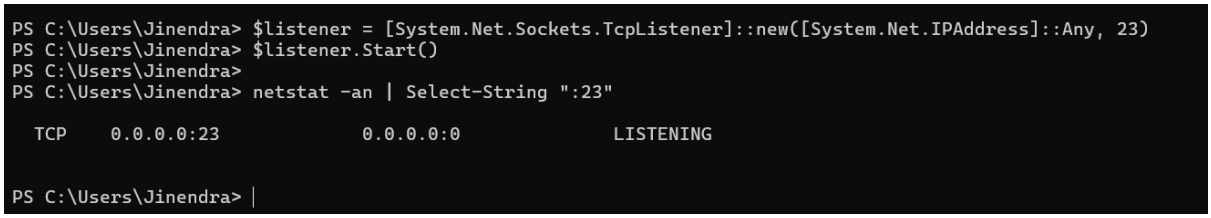
- **Purpose**: Simulate a service listening on port 23.

Step 3: Confirm Port 23 is Listening

- **Command Used**:

  netstat -an | Select-String ":23"

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



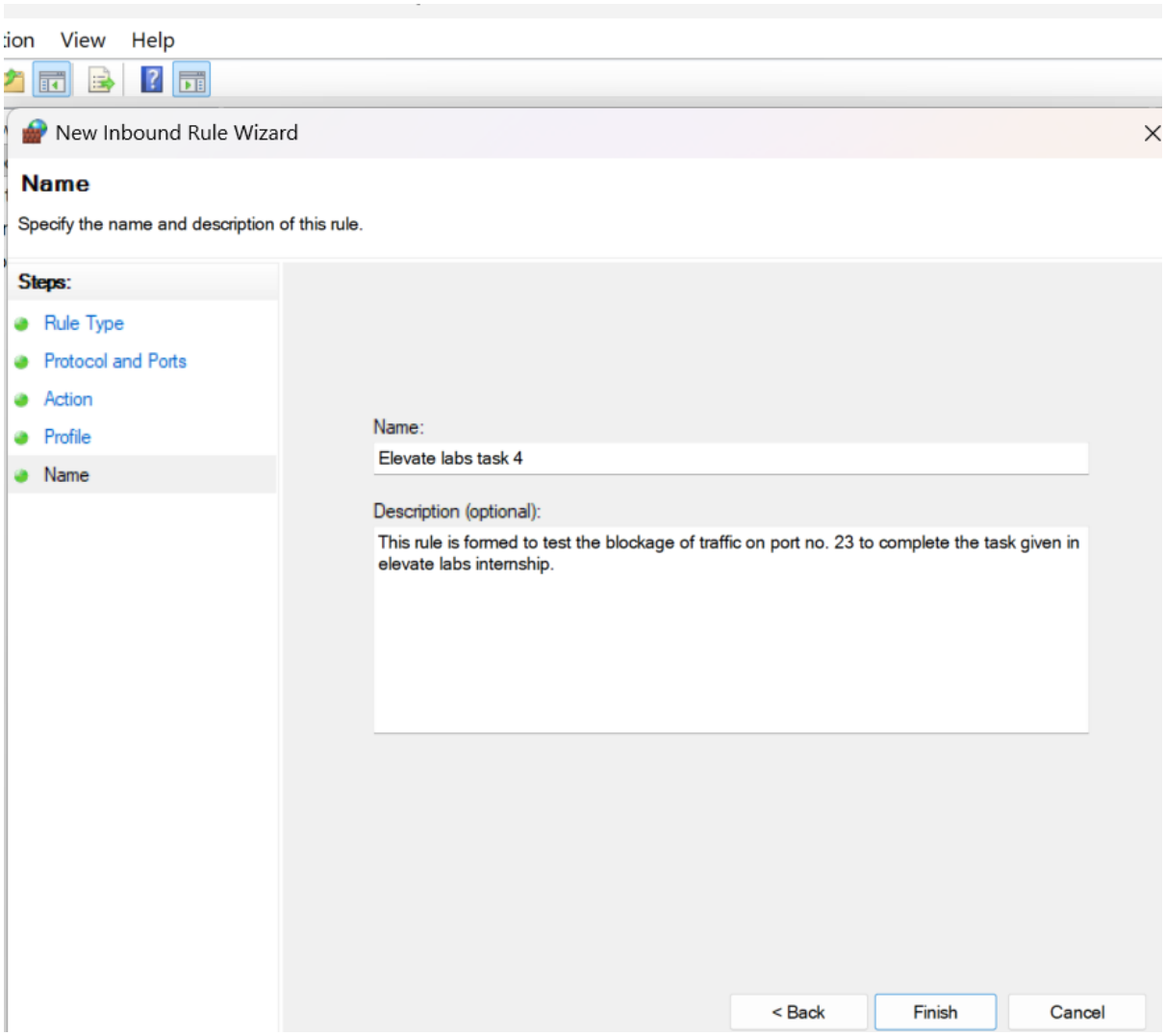
Step 4: Create Inbound Firewall Rule to Block Port 23

- **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

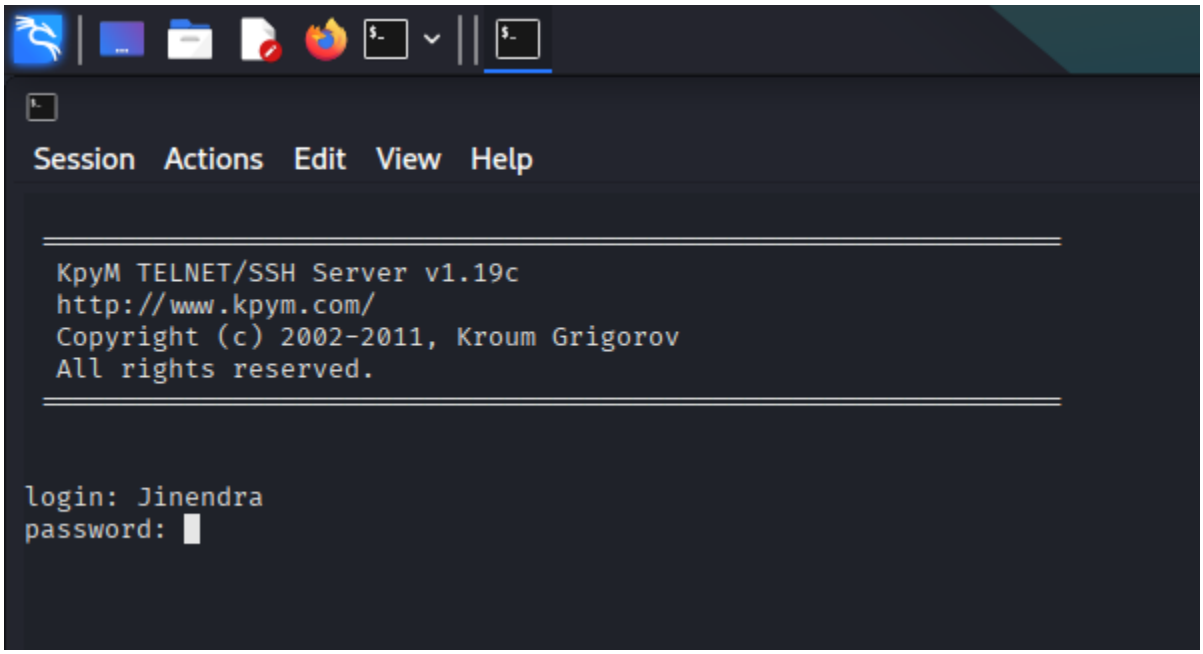


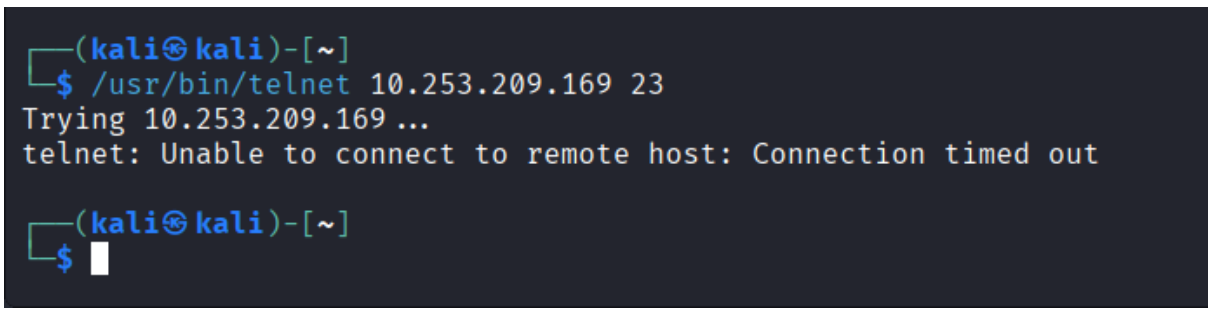
Step 5: Test Connectivity from Kali Linux

- **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)





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.