Windows Firewall Inbound Rules Test Report

Internship : Elevate Labs

Submitted by S.Abhishek

Objective

This exercise demonstrates the use of Windows Firewall inbound rules to manage network traffic, specifically by blocking Telnet (port 23) and testing its behavior using Windows PowerShell.

Background Concepts

What is Telnet?

Telnet is a network protocol that enables users to connect to and control remote computers over a TCP/IP network, such as the internet or a local area network (LAN). It creates a virtual terminal connection, allowing text-based interactions with a remote device. Telnet operates using plain text transmission, making it less secure than modern alternatives like SSH (Secure Shell). It is typically used for network device management, testing services, and troubleshooting.

What is PowerShell?

PowerShell is Microsoft’s advanced command-line shell and scripting language built on the .NET framework. It is designed for system administration, automation of tasks, configuration management, and network diagnostics. PowerShell supports both interactive commands (cmdlets) and scripting, providing administrators with powerful tools to automate complex tasks and perform remoting, system monitoring, and troubleshooting.

What are Inbound Firewall Rules?

Inbound firewall rules control all incoming traffic to a device or network. These rules are critical for network security as they filter and restrict access to internal resources, protect against malware and hacking attempts, and regulate which ports/services are accessible from external sources. Common use-cases include allowing secure connections like HTTPS and blocking potentially insecure or unneeded protocols such as Telnet.

Methodology

Navigated to the Windows Firewall interface and reviewed existing inbound rules.

Created custom rules:

Allowed incoming SSH traffic (Port 22)

Blocked incoming Telnet traffic (Port 23)

Checked the enabled/disabled status for these rules.

Used PowerShell to test TCP connectivity to Telnet port (23) on localhost.

Observations

Inbound Rules Configuration

The inbound rules panel lists several predefined and custom firewall rules for multiple applications and services.

The custom rule for "Block Telnet 23" is clearly visible and enabled, which should prevent connections over port 23.

PowerShell Test Result

Command executed:

Test-NetConnection -ComputerName 127.0.0.1 -Port 23

Outcome:

TCP connection attempt to port 23 failed (TcpTestSucceeded: False), confirming the firewall rule is working.

Network path was reachable (PingSucceeded: True) but traffic was blocked at the specified port. A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Analysis

The test validates that inbound traffic can be managed effectively using firewall rules, enhancing system security.

Blocking Telnet (an insecure protocol) prevents unauthorized access, while allowing other traffic (e.g., SSH) supports secure remote management.

PowerShell streamlines testing and troubleshooting of firewall configurations.

Conclusion

This experiment demonstrates how Windows Firewall inbound rules can be configured to restrict network access for certain protocols. Blocking Telnet improves security by preventing unencrypted remote sessions, and PowerShell provides a simple way to verify rule enforcement.