

Overview / Case Summary / Executive Summary

Overview

This project involved setting up, testing, and securing remote SSH access on a Windows system. The work included installing the OpenSSH Server, enabling logging to track SSH activity, and creating a firewall rule to block SSH connections from a specific IP address. The objective was to understand how SSH operates on Windows, how to monitor it through system logs, and how to control access using host-based security tools.

Case Summary

The project began with installing the OpenSSH Server feature through PowerShell and verifying that the service was running correctly. Once the service was active, the system was confirmed to be listening on port 22. Event Viewer was then used to validate SSH logging, where the OpenSSH “server listening” event (Event ID 4) and successful logon events in the Security log were visible, confirming that logging was functioning.

A custom inbound firewall rule was then created in Windows Defender Firewall to block SSH traffic from a specific IP address. The IP was added under the Scope tab, and the rule was confirmed to be enabled and configured to block connections. The rule was tested by attempting to SSH into the Windows machine from a Linux Mint VM using the correct username and IP address. The connection timed out repeatedly, demonstrating that the firewall successfully blocked SSH traffic from the specified IP.

Although advanced packet-level auditing could not be enabled on the system, all required configuration, logging, and validation steps were completed successfully.

Executive Summary

This project demonstrated the full process of configuring and securing SSH on a Windows system. OpenSSH Server was installed and confirmed to be running, SSH logging was enabled and verified in Event Viewer, and a targeted firewall rule was implemented to block unauthorized SSH access. Testing from a Linux Mint VM confirmed that the firewall rule effectively denied the connection. The project provided hands-on experience with Windows service configuration, log analysis, and host-based firewall security—key skills for systems administration and cybersecurity.