# Vulnerability Scan Report

**Scan Type:** Basic Network Scan

**Scanner Used:** Tenable Nessus Essentials

**Scan Target:** 127.0.0.1 (localhost)

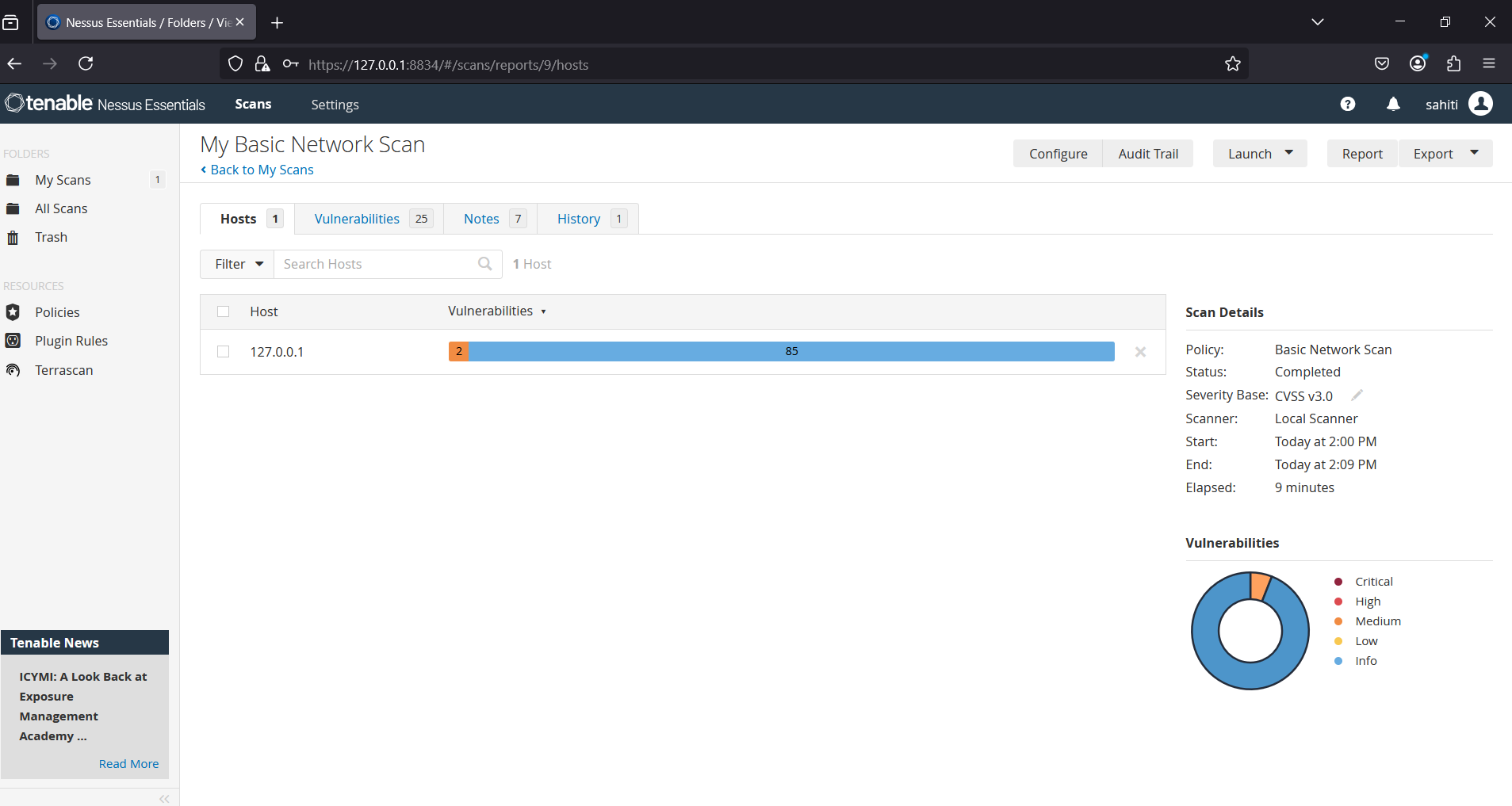
**Scan Date:** May 29 , 2025

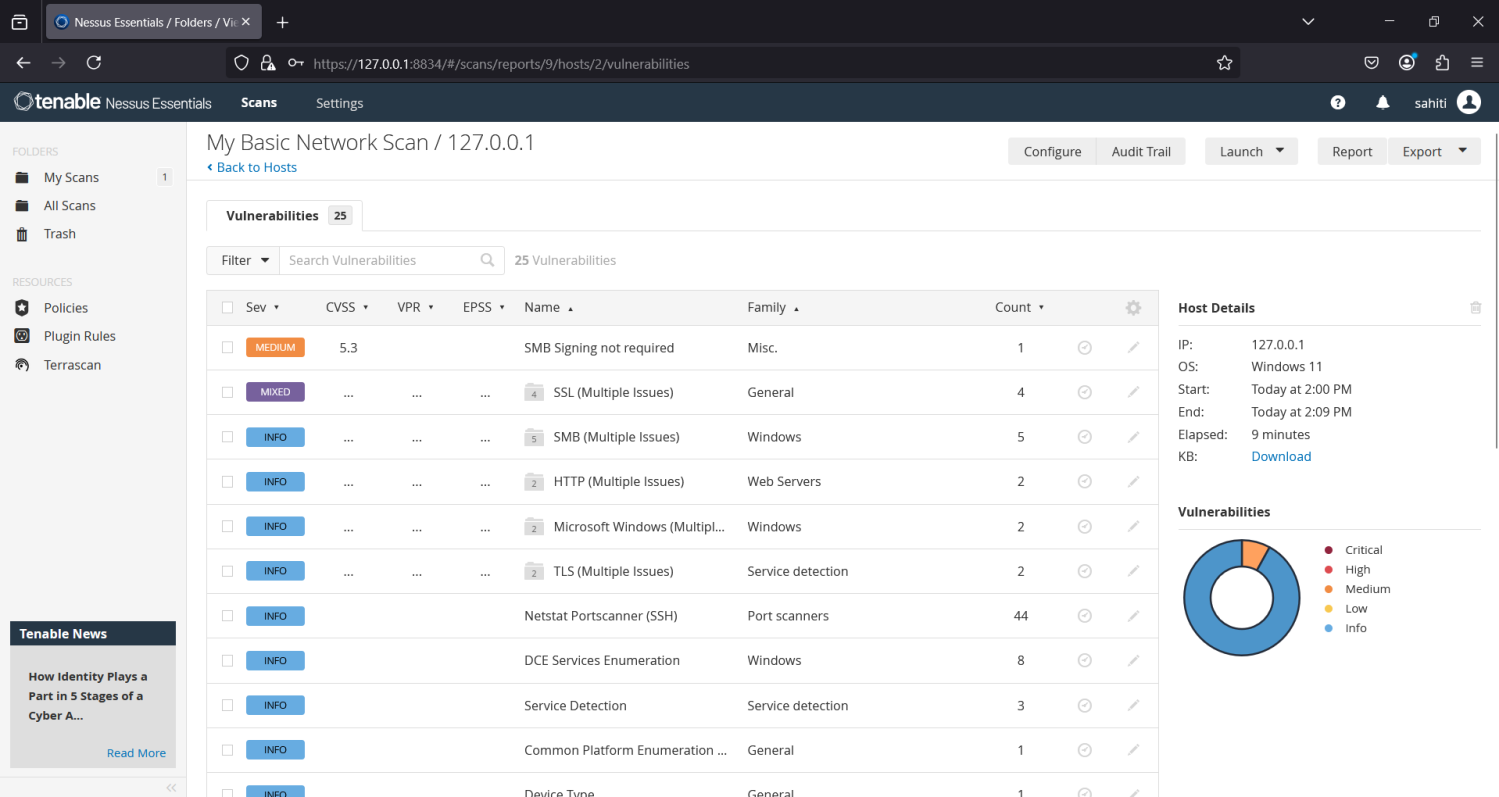
**Scan Duration:** ~9 minutes

## Objective

To perform a basic vulnerability scan using Nessus Essentials and identify potential security issues on the local machine.

## Summary of Findings



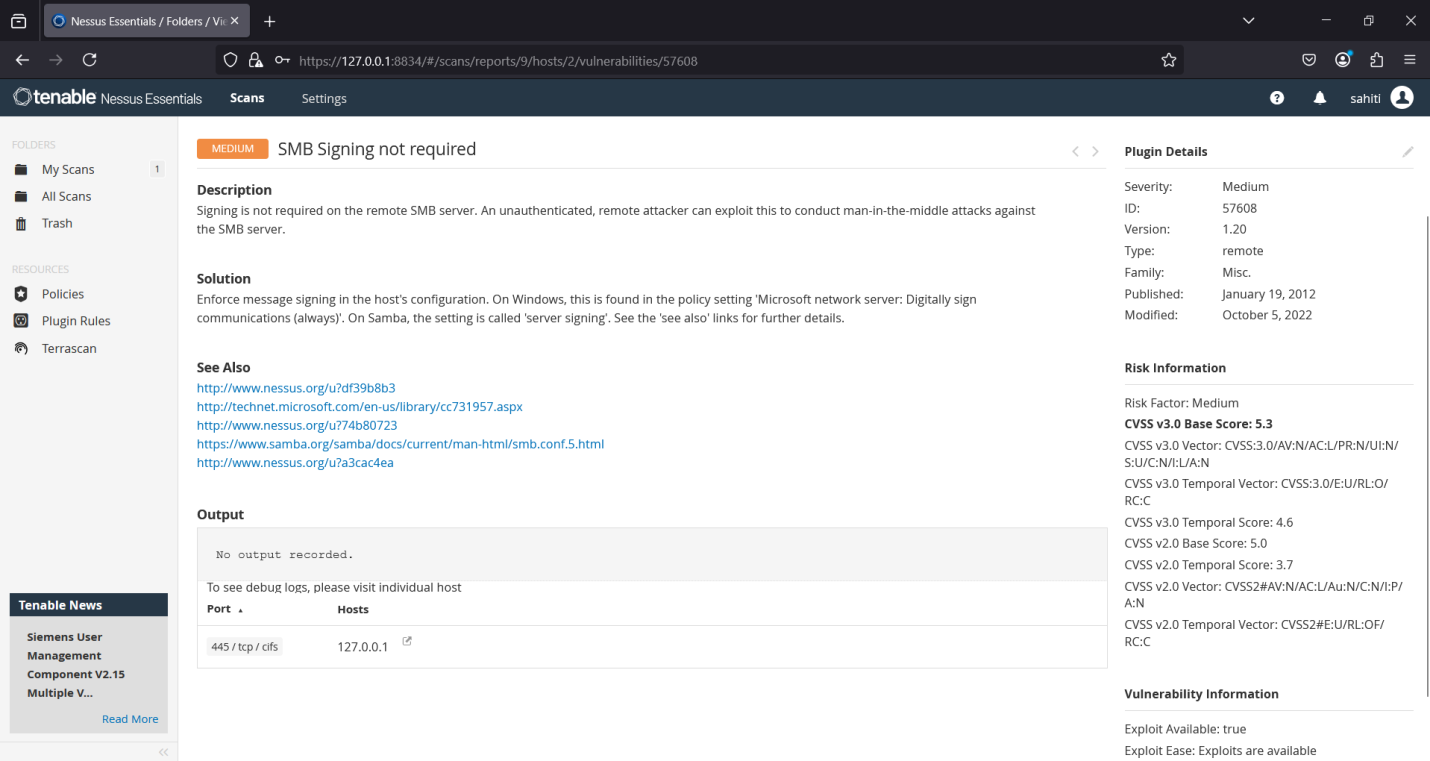


|  |  |
| --- | --- |
| **Severity** | **Number of Issues** |
| Critical | 0 |
| High | 0 |
| Medium | 2 |
| Low | 0 |
| Info | 85 |

## Top Medium Vulnerabilities

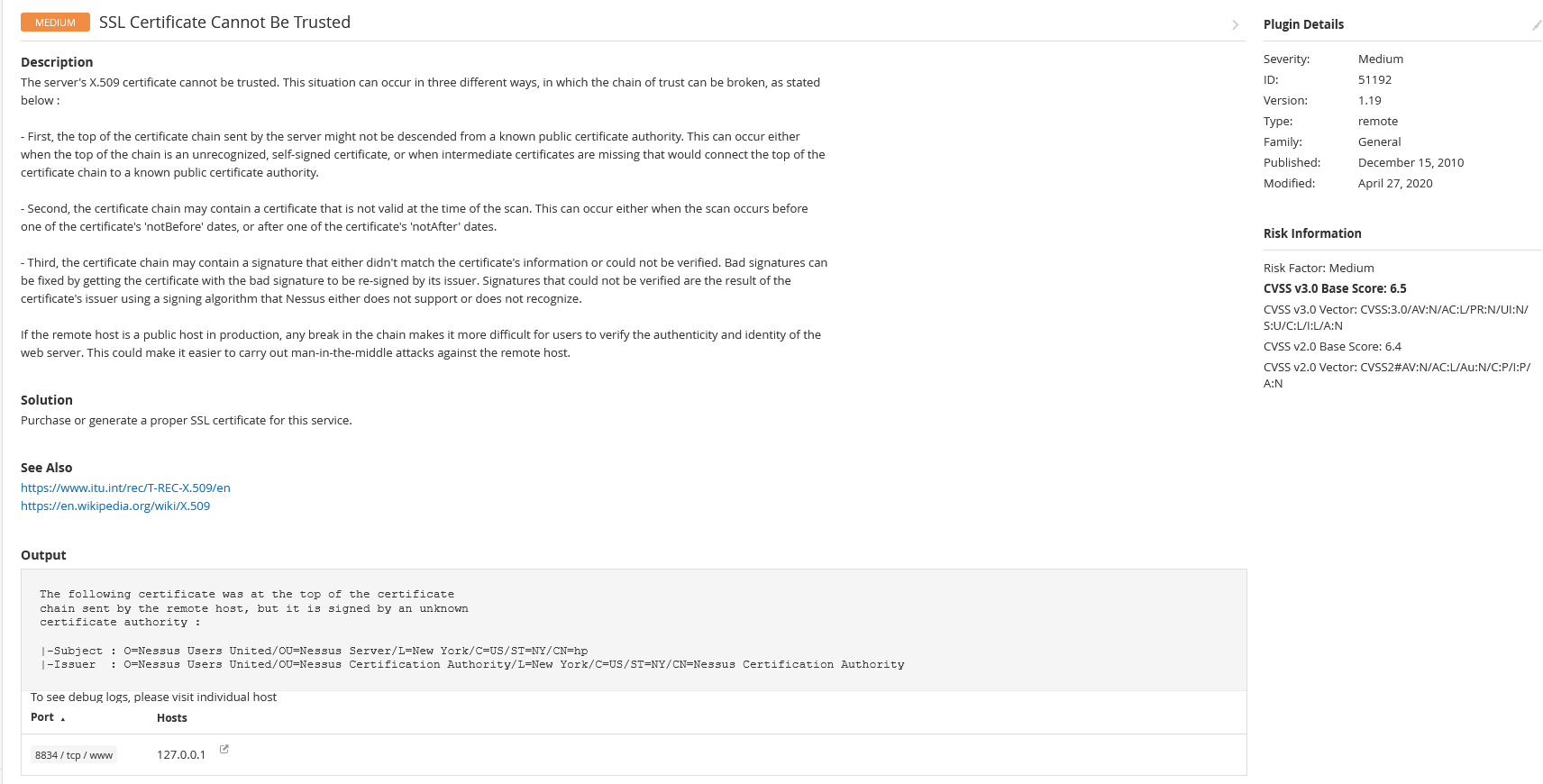
1. SSL Self- Signed Certificate

* The SSL certificate used is self-signed
* Impact: May not be trusted by clients, enabling Man-In-The-Middle attacks
* Solution: Replace with a certificate from a trusted certificate authority (CA)
* CVSS: 5.3



1. SSL Certificate cannot be trusted

* The SSL certificate cannot be verified by a trusted CA
* Impact: Insecure HTTPS communication
* Solution: Install a valid certificate signed by a recognized by CA
* CVSS: 6.5



## Fixes and Mitigation steps

* Replace all self-signed and untrusted certificates with valid CA-signed ones
* Regularly update system packages and apply security patches
* Schedule periodic vulnerability scans to monitor new risks