Implementing a Vulnerability Scanning Solution

Nessus Vulnerability Scanning: Securing Systems Assessment

---

1. Executive Summary

The purpose of this vulnerability scan is to simulate and assess the security posture of a single Windows system on a network using Tenable Nessus and propose remediation strategies. The scan was conducted within a virtual lab environment. A single Windows 10 virtual machine (VM) served as the target for vulnerability scanning.

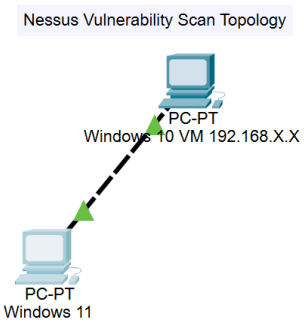
---

2. Environment Setup

- System Details:
    - The target environment consisted of a single VM running Windows 10. The VM was configured as a representative endpoint to simulate a real-world system for vulnerability scanning. It included standard software installations and basic configurations to emulate a typical user environment. The Windows machine was configured with vulnerabilities, including a deactivated firewall, and uninstalled and disabled Windows updates.

- **Nessus Installation:**
    - Nessus was installed on the host machine running the Windows 11 operating system to conduct vulnerability scans on the target virtual Windows 10 environment.

- **Network Topology:**



---

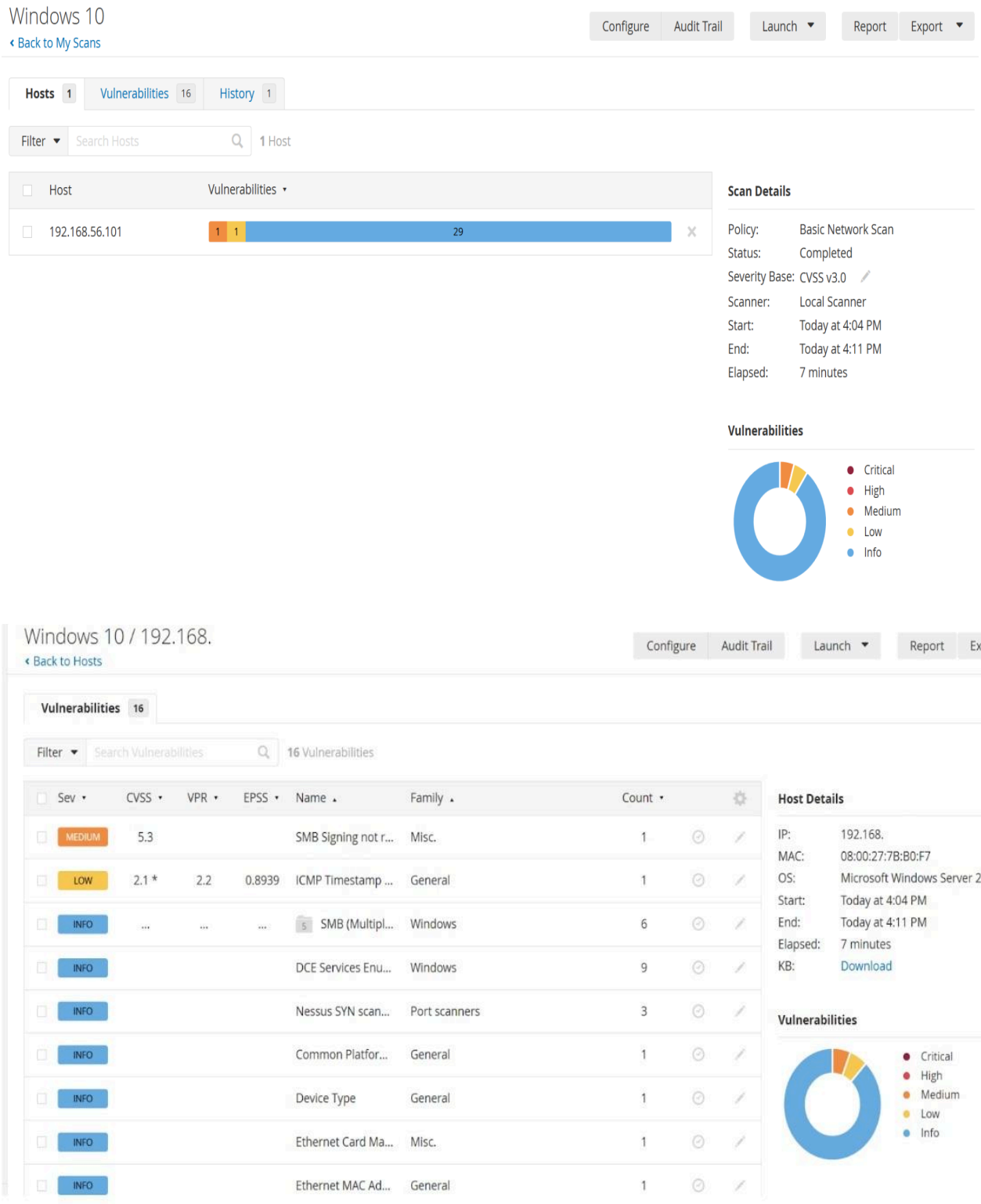
3. Scanning Process

- **Types of Scans:**
    - Non-Credentialed Scan
    - One-time scheduled scan of common ports
    - Basic network scan
    - Scan type set to default settings
    - Advanced setting set to default
    - No added plug-ins
- **Target Selection:**
    - 192.168.X.X
- **Execution:**
    - The scan was saved and after configuration, the “Launch” button was hit to begin the scanning process. The scan was launched on 1/10/25 at 16:14.

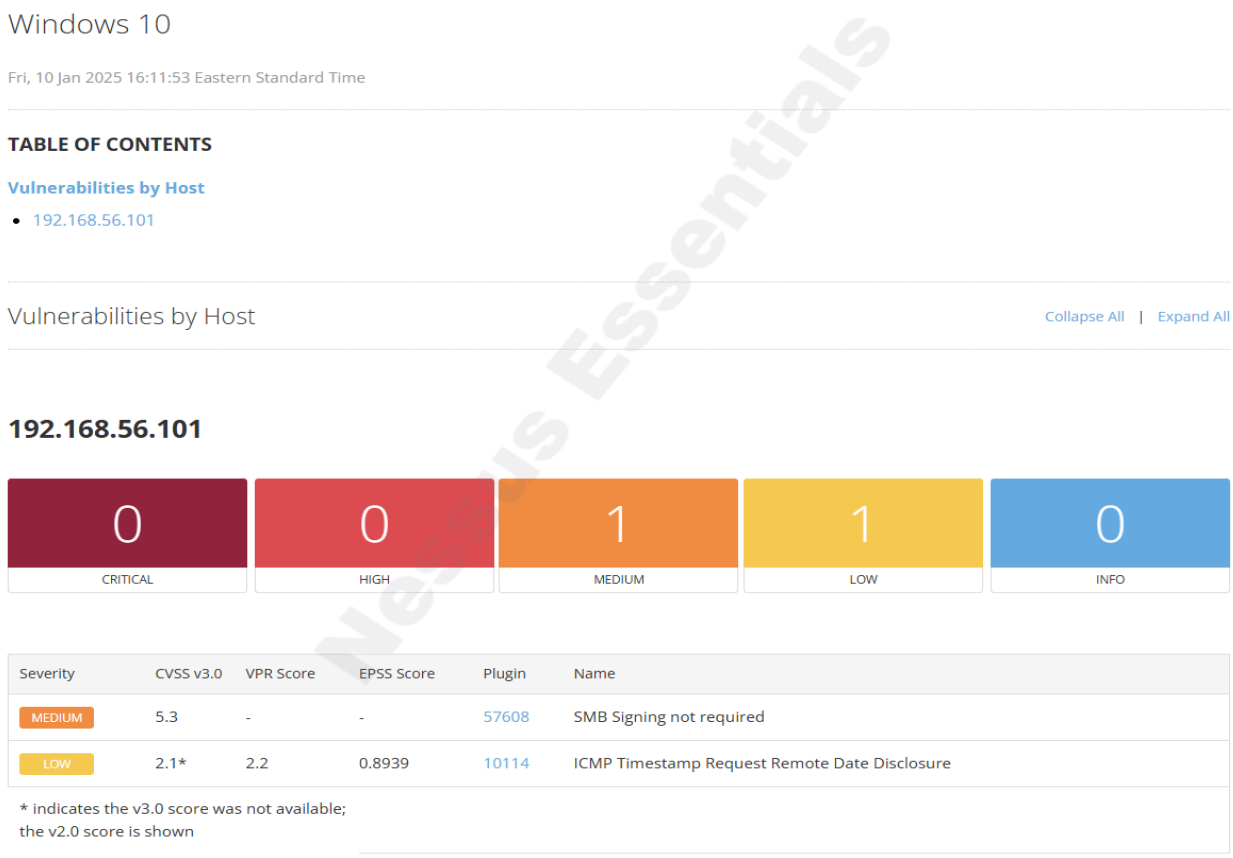
---

4. Findings Overview

The following sections present an overview of the vulnerabilities found during the scan, categorized by risk level.


Windows 10
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 16
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.56.101
1 1 29
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:04 PM
End: Today at 4:11 PM
Elapsed: 7 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Windows 10 / 192.168.
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 16
Filter
Search Vulnerabilities
16 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MEDIUM 5.3 SMB Signing not r... Misc. 1
LOW 2.1 * 2.2 0.8939 ICMP Timestamp ... General 1
INFO ... ... SMB (Multipl... Windows 6
INFO DCE Services Enu... Windows 9
INFO Nessus SYN scan... Port scanners 3
INFO Common Platfor... General 1
INFO Device Type General 1
INFO Ethernet Card Ma... Misc. 1
INFO Ethernet MAC Ad... General 1
Host Details
IP: 192.168.
MAC: 08:00:27:7B:B0:F7
OS: Microsoft Windows Server 2019
Start: Today at 4:04 PM
End: Today at 4:11 PM
Elapsed: 7 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

5. Results Analysis



Windows 10

Fri, 10 Jan 2025 16:11:53 Eastern Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.56.101

Vulnerabilities by Host — Collapse All | Expand All

192.168.56.101

0	0	1	1	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	5.3	-	-	57608	SMB Signing not required
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

Medium-Risk Vulnerability

A distinct vulnerability was classified as medium severity. These issues may expose details that could aid attackers in planning additional intrusions. Although they should be addressed promptly, they do not require the same level of urgency as higher-priority vulnerabilities.

NAME	DESCRIPTION	SOLUTION	COUNT	SCORE
Windows 10 / Plugin #57608 57608 - SMB Signing not required Vulnerability	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba,	1	CVSS v3.0 Base Score: 5.3 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:

		the setting is called 'server signing'. See the 'see also' links for further details.		N/S:U/C:N/I:L/A:N

Affected Device: Windows 10 Virtual Machine (VM) System

Authentication is not required on the remote SMB server, which allows an unauthenticated, remote attacker to exploit this vulnerability and carry out man-in-the-middle attacks against the SMB server.

This vulnerability allows for unauthenticated, remote exploitation but would require the attacker to be within range of the SMB service. While this could lead to interception or manipulation of SMB traffic, the impact is relatively moderate, and remediation steps can reduce the risk significantly.

Low-Risk Vulnerability

A distinct vulnerability was classified as low severity. These issues pose minimal risk but may still provide limited information that could be useful to attackers under specific circumstances. While they should be addressed eventually, they do not demand immediate attention and can be resolved as part of routine maintenance.

NAME	DESCRIPTION	SOLUTION	COUNT	SCORE
Windows 10 / Plugin #10114 10114 - ICMP Timestamp Request Remote Date Disclosure Vulnerability	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).	1	CVSS v2.0 Base Score: 2.1 CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N

Affected Device: Windows 10 Virtual Machine (VM) System

ICMP Timestamp Request Remote Date Disclosure CVE-1999-0524

Exposure of Sensitive Information to an Unauthorized Actor. The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine. This may allow an attacker to access the system's internal clock information.

---

6. Recommendations

This report's recommendations are based on findings from the uncredentialed scan audit. While vulnerability scans are one approach to assessing network security, they do not fully capture the overall security landscape. To achieve a comprehensive evaluation, additional steps may be necessary.

Prioritization:

Vulnerability remediation recommendations are prioritized from the most critical in severity to the least.

Mitigation Actions:

- Enforce message signing in the host's configuration settings. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
- Configure the firewall to filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

---

7. Challenges Faced

There were no significant technical or operational challenges encountered during the vulnerability assessment.

---

7. Conclusion

Scanning was non-intensive, therefor the scanning process had a minimal impact on system performance and operations. It successfully identified vulnerabilities across the system, providing valuable insights into potential risks and security weaknesses. Although no major issues arose during the scan, the discovery of multiple vulnerabilities—especially low-severity ones—highlighted areas that could benefit from better configurations or updates. Overall, the scan helped strengthen the security posture by identifying areas for improvement without causing disruptions to normal system operations.

---

8. Appendices

CVE-1999-0524 - Vulnerability Overview
CVE-1999-0524 - NVD
Provides the National Vulnerability Database (NVD) record for CVE-1999-0524, detailing its impact and recommended mitigations.

Microsoft Security Configuration Guide
TechNet - Security Policies for SMB
Offers guidelines on securing Server Message Block (SMB) protocols to mitigate potential threats.

Microsoft Server Message Block Signing Overview
Overview of SMB Signing
A guide on the importance of SMB signing in preventing man-in-the-middle attacks and securing file sharing.

Nessus Documentation on Vulnerabilities
Nessus Vulnerability Report - 74B80723
Contains information regarding another identified vulnerability, with advice on patching and securing the network.

Nessus Documentation on Vulnerabilities
Nessus Vulnerability Report - A3CAC4EA
Another relevant vulnerability report, detailing a specific weakness and necessary mitigation actions.

Nessus Documentation on Vulnerabilities
Nessus Vulnerability Report - DF39B8B3
Provides detailed information on the identified vulnerability and recommended remediation steps.

Samba Configuration and Security
Samba SMB Configuration Manual
Detailed documentation on configuring Samba settings to enhance security in SMB services.