Vulnerability Assessment Scan Report on a Windows Endpoint Using Nessus

IP Address: 192.168.0.8

Prepared By: Dennis Gilbert

Date: March 7, 2025

Table Of Content

Introduction

Purpose:

This vulnerability scan was conducted to assess the security posture of a Windows machine. The objective was to identify vulnerabilities, misconfigurations, and potential security risks that could be exploited by attackers.

Scope:

- **Target System:** Windows
- **IP Address of Target:** 192.168.0.8
- **Scanning Tool**: Nessus
- **ScanType:** Basic Network Scan
- **Scan Date**; March 15, 2025

Methodology

- Preparation:
  - Ensured the Windows VM was powered on and accessible from the Kali machine.
  - Configured Nessus scanner settings, selecting appropriate scan policies.
  - Verified network connectivity between Kali and the Windows VM.

- Scan Execution:
  - Launched Nessus and created a new scan.
  - Configured the target IP address and selected scan policies.
  - Initiated the scan and monitored its progress.

- Data Collection:
  - Collected scan results, including detected vulnerabilities, severity levels, and suggested mitigation.
  - Verified scan completion.

Reconnaissance

Tool Used

Nessus

- Purpose: Helps to identify security weaknesses, misconfigurations, and compliance issues.

Findings

Summary of Vulnerabilities

Severity Level	**Count**
Critical	**0**
High	**0**
Medium	**1**
Low	**2**
Informational	**19**

Medium & Low-Risk Vulnerabilities

- **Vulnerability**: SMB Signing not required
    - Description: 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.
    - Severity: Medium
    - CVE ID: CVE-2016-2115
    - Affected Components: SMB Servers, Samba, & Windows Server
    - Risk Impact: Risk of having a man-in-the-middle attack against the SMB server
    - Recommendation: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.

- **Vulnerability**: Server Message Block (SMB) Protocol Version 1 Enabled
  - Description: The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.
  - Severity: low
  - CVE ID: CVE-2017-0271
  - Affected Components: Windows SMB Server and Client & Samba (Open Source SMB Implementation)
  - Risk Impact: data breaches, operational downtime, and potential regulatory non-compliance due to unauthorized access and the spread of malware
  - Recommendation: Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

- **Vulnerability**: ICMP Timestamp Request Remote Date Disclosure
  - Description: 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.
  - Severity: Low
  - CVE ID: CVE-1999 - 0524
  - Affected Components: ICMP timestamp requests (type 13) and responses (type 14)

- Risk Impact: May help attackers to defeat time based authentications schemes
- Recommendation: Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Remediation Plan

Action Item	Priority
Enable 'Microsoft network server: Digitally sign communications (always)' policy on Windows host to enforce message signing.	Medium
Disable SMBv1 per Microsoft KB2696547 instructions. Block TCP port 445 and TCP/UDP ports 137, 138, 139 on all network boundary devices.	Low
Filter ICMP timestamp requests (Type 13) and block outgoing ICMP timestamp replies (Type 14) at network boundary devices.	Low

Conclusion

This Nessus scan identified 3 vulnerabilities in the Windows VM, including 1 high-severity issues and 2 low -severity issues. Immediate action is required to mitigate the highest-risk vulnerabilities, particularly those that allow remote code execution or privilege escalation. Regular scans and security patching are recommended to maintain a secure environment.