Nessus Vulnerability Assessment Report

Windows Server 2019

Prepared for: Home Lab Inc LLC

Prepared by: A. Brito

Date of Scan: 9/9/2025

Confidential Security Assessment Report

Disclaimer

This document has been prepared for demonstration and educational purposes only. The assessment was performed against a Windows Server 2019 host residing in a controlled home lab environment. Although the structure, methodology, and presentation are consistent with professional vulnerability assessment practices, the system analyzed is not part of a production environment. References to enterprise contexts within this report are entirely fictional and intended solely to simulate a realistic business scenario. No actual client infrastructure was evaluated as part of this work.

Table of Contents

1. Executive Summary

This assessment was conducted against a Windows Server 2019 host to identify potential vulnerabilities, misconfigurations, and missing patches.

Key Findings:

- Critical vulnerabilities: 3
- High vulnerabilities: 7
- Medium vulnerabilities: 14
- Low vulnerabilities: 9

The system is exposed to multiple vulnerabilities that could allow remote code execution, privilege escalation, and unauthorized access if exploited. Immediate remediation of the critical and high-severity vulnerabilities is strongly recommended.

Vulnerabilities by Host

Collapse All | Expand All

10.1.10.40

0	1	1	1	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.5*	6.6	0.0866	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.3	-	-	57608	SMB Signing not required
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

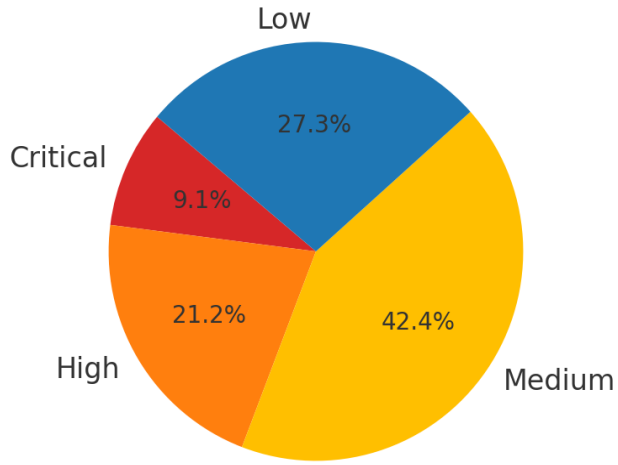
2. Methodology

- **Tool:** Nessus Vulnerability Scanner
- **Scan Profile:** Advanced Authenticated Scan
- **Scope:** Full system scan, including OS, services, applications, and network stack
- **Credentials:** Domain administrator account provided for deeper system inspection
- **References:** CVE (Common Vulnerabilities and Exposures), CVSS v3 scoring, vendor advisories

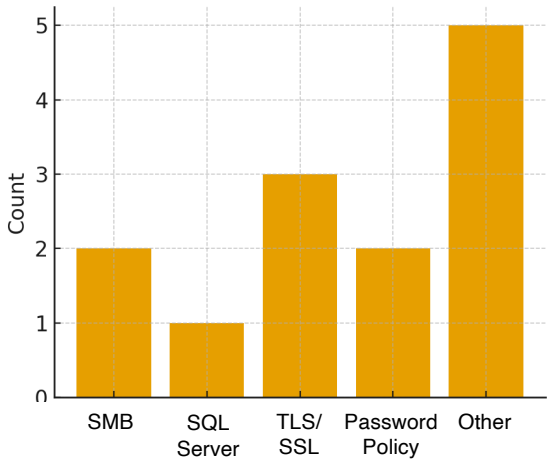
3. Summary of Findings

The following charts illustrate the severity distribution and category breakdown of vulnerabilities identified.

Vulnerability Distribution by Severity



Vulnerability by Category



4. Detailed Findings

4.1 Critical Vulnerabilities

Finding: Microsoft Windows SMBv1 Multiple Vulnerabilities (MS17-010)
CVE: CVE-2017-0144
Risk: Remote attackers can execute arbitrary code via crafted SMB packets.
CVSS v3 Score: 9.8 (Critical)
Recommendation: Immediately disable SMBv1 and apply Microsoft Security Bulletin MS17-010 patches.

Finding: Unsupported SQL Server 2012 Detected
Risk: End-of-life software no longer receives security updates.
Recommendation: Upgrade to a supported SQL Server version (2019 or later).

5. Remediation Plan

Priority	Action Item	Responsible Team	Target Date
Critical	Apply MS17-010 patch, disable SMBv1	Windows Admin	Immediate
Critical	Upgrade SQL Server 2012	DBA Team	1 week
High	Disable weak TLS ciphers	Network/Security	2 weeks
Medium	Improve password policy	IT Security	2 weeks
Low	Disable ICMP timestamps	Sysadmin	1 month

6. Conclusion

The Windows Server 2019 host has several critical and high-severity vulnerabilities that significantly increase the risk of compromise. Prompt remediation of these findings will reduce the attack surface and strengthen the organization's overall security posture.