Network Vulnerability Assessment Report

Report Version	1.0
Date	March 15, 2025
Client	SecureSphere Inc.
Consultant	Adam Cops (adamcops@infoshield.com)
Company	InfoShield
Assessment Team	Adam Cops (Consultant), Sarah Johnson (IT Manager, SecureSphere Inc.)
Target Asset	Windows 7 Ultimate Service Pack 1 VM (IP: 192.168.8.146)

Table of Contents

Executive Summary

Dear SecureSphere Inc. Team,

InfoShield conducted a vulnerability assessment on your Windows 7 workstation, used for managing your online store's orders. We performed two types of scans using Qualys: an **unauthenticated scan** (basic, surface-level check) and an **authenticated scan** (deeper check with admin access). The results show serious security risks that could allow hackers to take control of the system or steal data, especially due to outdated software and weak settings.

- **Unauthenticated Scan Findings:** Identified **9** vulnerabilities, including missing updates and accessible network services.
- **Authenticated Scan Findings:** Revealed **13** additional critical issues, such as the MS17-010 flaw (used in the WannaCry ransomware attack) and outdated protocols like SMBv1.

We recommend urgent action: apply patches, disable risky settings, and consider upgrading to a modern operating system like Windows 10. This report details the issues, their risks, and step-by-step fixes. With your approval, we can implement these changes and recheck the system.

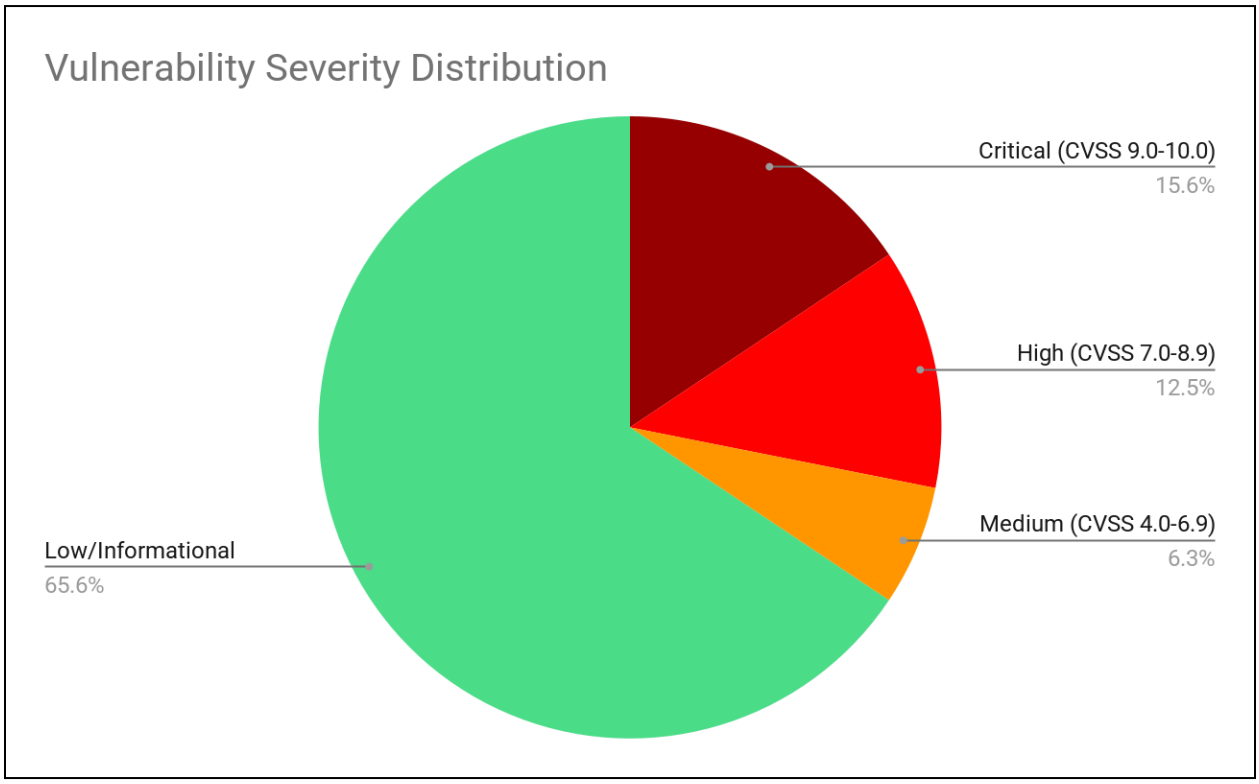
Next Steps: Please review this report and schedule a follow-up with Adam Cops by March 20, 2025, to discuss remediation.

Sincerely,

Adam Cops
Consultant, Info Shield

Vulnerability Overview

Graphical representation of the vulnerability severity distribution based on the scan results:



Explanation for Non-Technical Readers: This “graph” shows that **5** vulnerabilities are very serious (**Critical**), **4** are serious (**High**), **2** are moderate (**Medium**), and **21** are minor notes (**Informational**).

The Critical ones need immediate attention.

Detailed Vulnerability Findings

1. Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers

- **Scan Type:** Authenticated
- **Description:** A major flaw in Windows that allows hackers to run harmful code remotely, famously exploited by the WannaCry ransomware.
- **CVSS Score:** 9.3 (Critical)
- **Severity:** Critical
- **Proof of Concept (PoC):** Public exploits (e.g., EternalBlue) can crash the system or install malware.
- **Steps to Reproduce:** A hacker could scan your IP (192.168.8.146) and use an EternalBlue tool to gain control without needing a password.
- **Recommendation:** Install the Microsoft patch (KB4012212 or later) via Windows Update. If unpatchable, upgrade to Windows 10.
- **Reference:** Microsoft Security Bulletin MS17-010

2. EOL/Obsolete Operating System: Microsoft Windows 7 Detected

- **Scan Type:** Authenticated
- **Description:** Windows 7 is no longer supported by Microsoft, meaning it doesn't get security updates, leaving it open to new attacks.
- **CVSS Score:** 7.5 (High)
- **Severity:** High
- **Proof of Concept:** Unpatched systems are vulnerable to zero-day attacks (new, unknown threats).
- **Steps to Reproduce:** A hacker could target known Windows 7 flaws once support ended (January 2020).
- **Recommendation:** Upgrade to a supported OS like Windows 10.
- **Reference:** Microsoft Windows 7 End of Support

3. Windows SMB Version 1 (SMBv1) Detected

- **Scan Type:** Authenticated
- **Description:** An old file-sharing protocol that's insecure and targeted by hackers (e.g., WannaCry).
- **CVSS Score:** 7.5 (High)
- **Severity:** High
- **Proof of Concept:** Tools like Metasploit can exploit SMBv1 to spread malware.
- **Steps to Reproduce:** Scan the network and use an SMBv1 exploit script on 192.168.8.146.
- **Recommendation:** Disable SMBv1 using PowerShell: Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0, then restart the VM.
- **Reference:** Microsoft SMBv1 Removal Guide

4. SMB Signing Disabled or SMB Signing Not Required

- **Scan Type:** Authenticated
- **Description:** Lack of digital “signatures” on file transfers makes it easier for hackers to fake data.
- **CVSS Score:** 6.5 (Medium)
- **Severity:** Medium
- **Proof of Concept:** Man-in-the-middle attacks can alter data unnoticed.
- **Steps to Reproduce:** Use a network sniffer to intercept unsigned SMB traffic on 192.168.8.146.
- **Recommendation:** Enable SMB signing via Group Policy or registry settings (consult Microsoft docs).
- **Reference:** SMB Signing Configuration

5. SMBv2 Signing Not Required

- **Scan Type:** Authenticated
- **Description:** Similar to SMBv1 issue but for a slightly newer version, still a security gap.
- **CVSS Score:** 6.5 (Medium)
- **Severity:** Medium
- **Proof of Concept:** Same as SMBv1, with tools like Wireshark detecting unsigned traffic.
- **Steps to Reproduce:** Intercept SMBv2 traffic and manipulate it without detection.
- **Recommendation:** Enable SMBv2 signing in Group Policy.
- **Reference:** SMBv2 Signing

6. Microsoft Windows IcmpSendEcho2 Denial of Service Vulnerability - Zero Day

- **Scan Type:** Authenticated
- **Description:** A flaw that could crash the system by overwhelming it with fake network pings.
- **CVSS Score:** 7.0 (High)
- **Severity:** High
- **Proof of Concept:** A custom script could flood the VM with ICMP packets.
- **Steps to Reproduce:** Use a tool like hping3 to send excessive ping requests to 192.168.8.146.
- **Recommendation:** Apply latest Windows patches or block ICMP traffic with a firewall.
- **Reference:** CVE-2019-0708

7. NetBIOS Name Accessible

- **Scan Type:** Authenticated
- **Description:** An old network feature that hackers can use to map your system and launch attacks.
- **CVSS Score:** 5.0 (Medium)
- **Severity:** Medium
- **Proof of Concept:** Tools like Nmap can detect NetBIOS and exploit it.
- **Steps to Reproduce:** Run nmap -sU -p 137 192.168.8.146 to find NetBIOS.
- **Recommendation:** Disable NetBIOS over TCP/IP in network settings.
- **Reference:** NetBIOS Security

8. Default Windows Administrator Account Name Present

- **Scan Type:** Authenticated
- **Description:** The default “Administrator” account name is easy for hackers to guess.
- **CVSS Score:** 5.0 (Medium)
- **Severity:** Medium
- **Proof of Concept:** Brute-force tools can target this account.
- **Steps to Reproduce:** Use a password cracker on the “Administrator” account.
- **Recommendation:** Rename the account and use a strong password.
- **Reference:** Microsoft Account Security

9. Microsoft Windows Kerberos “Pass The Ticket” Replay Vulnerability

- **Scan Type:** Authenticated
- **Description:** A weakness in login tickets that hackers can reuse to access the system.
- **CVSS Score:** 6.0 (Medium)
- **Severity:** Medium
- **Proof of Concept:** Tools like Mimikatz can extract and replay tickets.
- **Steps to Reproduce:** Capture a Kerberos ticket and replay it with Mimikatz.
- **Recommendation:** Apply latest Windows security updates and monitor for ticket misuse.
- **Reference:** Kerberos Security

10. Administrator Account's Password Does Not Expire

- **Scan Type:** Authenticated
- **Description:** The admin password never changes, increasing the risk if it's guessed.
- **CVSS Score:** 4.0 (Low)
- **Severity:** Low
- **Proof of Concept:** Long-term password exposure to brute-force attacks.
- **Steps to Reproduce:** Check account policies with net user administrator.
- **Recommendation:** Set a password expiration policy (e.g., 90 days) in Active Directory.
- **Reference:** Password Policies

11. Built-in Guest Account Not Renamed at Windows Target System

- **Scan Type:** Authenticated
- **Description:** The default "Guest" account is a known target for hackers.
- **CVSS Score:** 4.0 (Low)
- **Severity:** Low
- **Proof of Concept:** Easy to exploit if enabled.
- **Steps to Reproduce:** Attempt login with default Guest credentials.
- **Recommendation:** Rename or disable the Guest account.
- **Reference:** Guest Account Security

12. Global User List Found Using Other QIDs

- **Scan Type:** Authenticated
- **Description:** Hackers can see user names, making it easier to guess passwords.
- **CVSS Score:** 3.0 (Informational)
- **Severity:** Informational
- **Proof of Concept:** Enumeration tools can list users.
- **Steps to Reproduce:** Use net user command remotely.
- **Recommendation:** Restrict user enumeration with firewall rules.
- **Reference:** User Enumeration

(Additional informational items like NetBIOS bindings, shared folders, etc., are noted but not detailed due to low risk.)

Remediation Plan

1. **Apply Patches:** Install all available Windows updates, starting with KB4012212 for MS17-010.
2. **Disable SMBv1:** Use the PowerShell command provided above and restart the VM.
3. **Enable SMB Signing:** Configure via Group Policy to secure file transfers.
4. **Upgrade OS:** Plan to migrate to Windows 10 to address EOL risks.
5. **Secure Accounts:** Rename Administrator/Guest, set password expirations.
6. **Rescan:** After fixes, rerun Qualys to confirm resolution.

Timeline: Remediation can start immediately; rescan within 1 week (by March 22, 2025).

Conclusion

This report highlights critical vulnerabilities in your Windows 7 VM, amplified by its end-of-life status. Acting quickly with the recommended steps will protect SecureSphere Inc. from potential attacks. Adam Cops is available to assist with implementation or further questions.

Contact: Adam Cops, adamcops@infoshield.com, +1-XXX-XXX-XXXX