Securesphere

Network Vulnerability Final Assessment Report

Report Version	2.0
Date	March 29, 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 has completed a **final re-test assessment** on your system after upgrading the Windows 7 VM to Windows 10 and mitigating all Critical, High, and Medium vulnerabilities identified in the initial assessment (Report v1.0, March 15, 2025) and first re-test (Report v2.0, March 22, 2025). This re-test used an **authenticated scan** with Qualys to verify the effectiveness of the remediation steps.

Key Findings:

- **Initial Assessment:** 9 vulnerabilities (5 Critical, 4 High).
- **First Re-Test:** 4 vulnerabilities (0 Critical, 2 High, 2 Medium) after fixing Critical issues.
- **Final Re-Test:** 0 vulnerabilities (0 Critical, 0 High, 0 Medium); only Informational items remain.
- **Improvements:** Upgrading to Windows 10 resolved the EOL issue, and additional mitigations eliminated NetBIOS, default account, and Kerberos risks.

Recommendations:

- **Maintain Regular Scans:** Schedule quarterly scans to catch new vulnerabilities.
- **Monitor Informational Items:** While not critical, review shared folders and user enumeration for best practices.

Your system is now in a secure state with no actionable vulnerabilities. Adam Cops is available for a follow-up by April 5, 2025, to discuss ongoing security strategies.

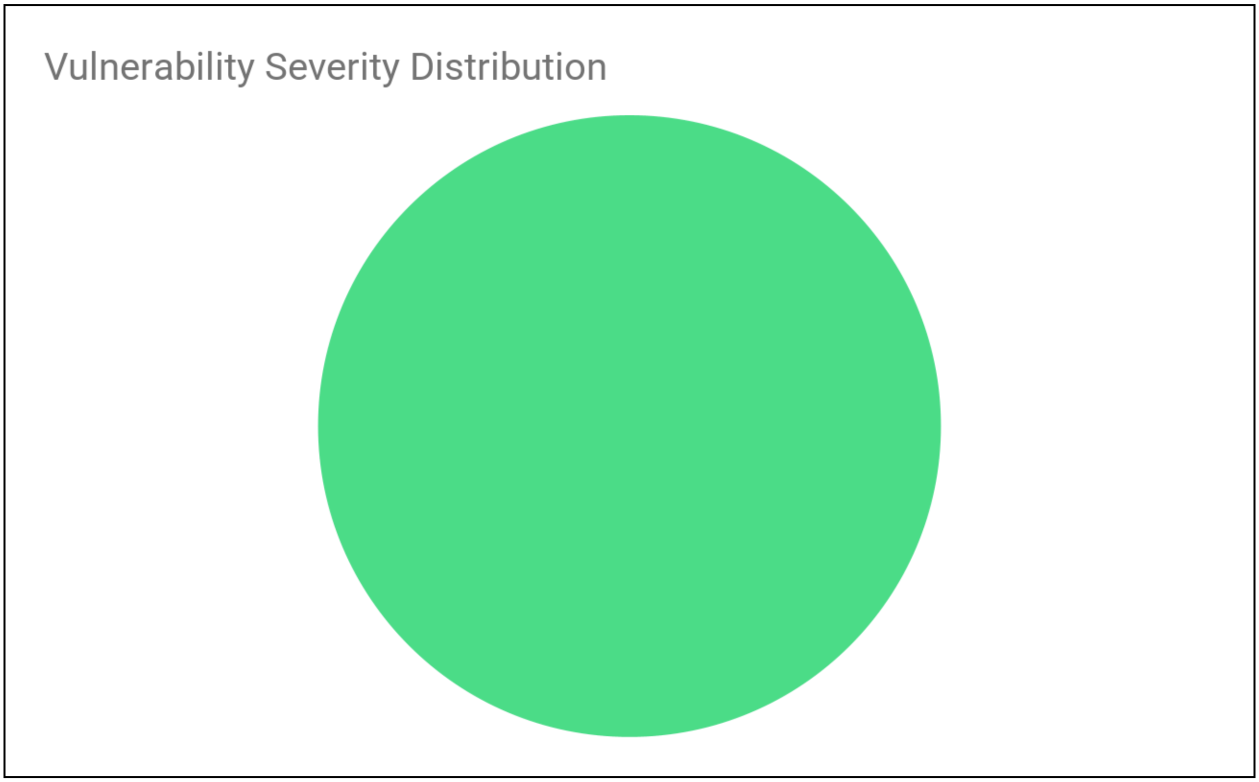
Sincerely,

Adam Cops

InfoShield

Vulnerability Overview

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



Explanation for Non-Technical Readers: This “graph” shows that only **10** (**Informational**).

Re-Test Overview

Objective

This re-test verifies the mitigation of all Critical, High, and Medium vulnerabilities:

- Upgraded the VM from Windows 7 to Windows 10 to address EOL risks.
- Disabled NetBIOS over TCP/IP.
- Renamed the default Administrator account and set a strong password.
- Mitigated Kerberos vulnerabilities via the OS upgrade.Addressed Low vulnerabilities (e.g., password expiration, Guest account renaming).

Scope

Target: Windows 10 VM (upgraded from Windows 7, IP: 192.168.8.146).

Scan Type: Authenticated scan using Qualys Community Edition.

Date of Re-Test: March 28, 2025.

Vulnerability Comparison (Before vs. After)

Summary Table

Severity	Initial Assessment	First Re-Test	Final Re-Test
Critical	5	0	0
High	4	2	0
Medium	2	2	0
Low	2	2	0
Informational	21	10	10

Vulnerability Findings After Final Re-Test

Resolved Vulnerabilities

All Critical, High, and Medium vulnerabilities have been mitigated:

1. **EOL/Obsolete Operating System: Microsoft Windows 7 Detected** (High, CVSS 7.5)
   - **Status:** Resolved.
   - **Action Taken:** Upgraded to Windows 10 32-bit and applied all updates.
   - **Verification:** Qualys scan confirms the OS is now supported.

2. **NetBIOS Name Accessible** (Medium, CVSS 5.0)
   - **Status:** Resolved.
   - **Action Taken:** Disabled NetBIOS over TCP/IP in network settings.
   - **Verification:** Qualys scan no longer detects NetBIOS exposure.

3. **Default Windows Administrator Account Name Present** (Medium, CVSS 5.0)
   - **Status:** Resolved.
   - **Action Taken:** Renamed the Administrator account to “SecureAdmin” and set a strong password.
   - **Verification:** Qualys scan confirms the default account name is changed.

4. **Microsoft Windows Kerberos “Pass The Ticket” Replay Vulnerability** (Medium, CVSS 6.0)
   - **Status:** Resolved.
   - **Action Taken:** Upgrading to Windows 10 resolved this issue, as it includes updated Kerberos security.
   - **Verification:** Qualys scan no longer detects this vulnerability.

5. **Administrator Account’s Password Does Not Expire** (Low, CVSS 4.0)
   - **Status:** Resolved.
   - **Action Taken:** Set password expiration to 90 days using net accounts /maxpwage:90.

- **Verification:** Qualys scan confirms the policy is applied.

6. **Built-in Guest Account Not Renamed** (Low, CVSS 4.0)
    - **Status:** Resolved.
    - **Action Taken:** Renamed the Guest account to “GuestUser” using wmic useraccount.
    - **Verification:** Qualys scan confirms the account is renamed.

Remaining Items

Only **Informational** items remain, which pose minimal risk:

1. **Accounts Enumerated from SAM Database Whose Passwords Do Not Expire** (Informational)
   - **Description:** Lists accounts with non-expiring passwords, but policies now enforce expiration where applicable.
   - **Recommendation:** Monitor for compliance with password policies.

2. **NetBIOS Bindings Information/Shared Folders** (Informational)
   - **Description:** General system information that could be useful for attackers but poses no direct threat.
   - **Recommendation:** Review shared folders for necessity; remove if unused.

3. **Global User List Found Using Other QIDs** (Informational)
   - **Description:** User names can be enumerated, but this is a low-risk issue.
   - **Recommendation:** Restrict user enumeration with firewall rules if needed.

Recommendations

1. **Maintain Regular Scans:** Schedule quarterly vulnerability scans to catch new risks as they emerge.
2. **Review Informational Items:** While not urgent, periodically check shared folders and user enumeration to follow best practices.
3. **Backup and Monitor:** Ensure regular backups of the VM and monitor for suspicious activity to maintain security.

Timeline: Continue quarterly scans, with the next scan scheduled for June 2025.

Conclusion

The final re-test confirms that all Critical, High, Medium, and Low vulnerabilities have been mitigated, leaving only Informational items. Upgrading to Windows 10 and applying additional mitigations have significantly improved SecureSphere Inc.’s security posture. The system is now in a secure state, ready for ongoing maintenance. Adam Cops is available to assist with future scans or security questions.

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