Executive Summary

Objective of the Audit

- The purpose of this audit was to assess the credentialed Vulnerability Scan of Nswell and identify any vulnerabilities that could pose risk to confidentiality, integrity and availability.

Summary of Findings

- **Total Vulnerability Detected**: 22

- **Critical Issues**: 2 Medium, Mixed 4, All Info

- **Key Risk Areas**: SMB sever breach, Plugin SSL related attempts, all though risk factor is none there are a lot of open ports, more than 22 ports.

- **Overall Security Rating**: Medium

Key Findings and Risk Analysis

Vulnerability	Severity	Impact	Recommendation
SMB Signing not required	Medium	System is at risk of remote attacker	Enforce message signing on the Microsoft network server
SSL Certificate cannot be trusted	Medium	any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server	Purchase or generate a proper SSL certificate for this service.
Plugin SSL attempts	Low	Attempts to extract and dump the X.509 certificates 22 times	Recommend classification with machine learn and algorithm from host and another ID. Transactions will be secured.

Recommendation & Next Steps

Critical Fixes

- Immediate action to enforce message signing on the Microsoft network server

- Purchase or generate a proper SSL certificate for this service immediately.

- Introduction of Classification of machine learning and generating algorithms during transactions process, to establish authentic transactions and communications between two ends.

- Fix the problem(s) so that OS Security Patch Assessment is possible.

Long Term Security Improvement

- Regular security audit every 3 months

- Train employees in cybersecurity and internet of things including machine learning best practices

- Implement hardening of network systems.

Conclusion

This IT Audit identified 22 vulnerabilities including medium issues which require immediate action. Addressing these risks will significantly improve the system security posture and reduce the likelihood of a cyber-attack.

- Final Risk Rating: Medium

- Next Audit: May 2025