Cybersecurity Vulnerability Assessment Report

Project Title: Authenticated & Unauthenticated Vulnerability Scans on Windows 11 VM in Azure

Name: CyberSolex

GitHub: https://github.com/Jaysolex/CyberSolex

Date: May 23, 2025

Tools Used: Microsoft Azure, Tenable Nessus Essentials

Techniques: Vulnerability Scanning, Risk Assessment, Hardening Planning

1. Project Overview

As part of a hands-on cybersecurity portfolio project using Josh Madakor's lab framework, I created a Windows 11 virtual machine in Microsoft Azure and conducted both unauthenticated and authenticated scans using Tenable Nessus. The goal was to simulate attacker reconnaissance vs. internal asset visibility to identify and prioritize security risks.

2. Lab Environment

- Platform: Microsoft Azure
- VM: Windows 11 Pro Build 26100
- Scanner: Tenable Nessus Essentials
- Network: Default NSG allowing RDP
- Credentialed Access: Enabled via labuser account

3. Scan Summary

Scan Type	Critical	High	Medium	Low	Info	Total
Unauthenticated	0	0	4	1	31	36
Authenticated	0	2	4	1	133	140

4. Key Findings (Authenticated Scan)

High Severity:

- CVE-2024-20670 - Microsoft Outlook NTLM Hash Leak: Apply KB5002574.

- Winlogon Cached Passwords: Set CachedLogonsCount = 0 in the registry.

Medium Severity:

- Self-Signed SSL Certificate on RDP: Replace with a valid certificate.

- TLS 1.1 Detected: Disable TLS 1.0/1.1, enforce 1.2 or 1.3.

- SMB Shares Wide Access: Limit access to trusted users or restrict externally.

5. Security Insights Gained

- Compared external vs internal exposure by using both scan types.

- Enumerated users, network configs, services, and installed packages.

- Simulated attacker and insider scenarios.

6. Skills Demonstrated

- Vulnerability Scanning (Nessus Essentials)

- Windows Hardening Techniques

- Azure VM Deployment & NSG Configuration

- Registry & Group Policy Review

- Report Analysis and Prioritization

- Credentialed vs Uncredentialed Threat Modeling

7. Remediation Plan

- Apply patches (e.g., Outlook, .NET rollups)

- Restrict and secure RDP

- Replace self-signed certs

- Limit SMB access

- Enforce TLS 1.2/1.3

- Disable cached credentials