From Vulnerability Detection to Remediation: A Hands-On Approach with Nessus Essentials

Author: Harshitkumar R. Panwala

Date: July 24, 2024

Introduction

Purpose

This report provides a comprehensive overview of a vulnerability management project conducted on a Windows 10 virtual machine ("Win10-Vulnerable") hosted on Azure. The assessment was performed using Nessus Essentials to identify, evaluate, and remediate vulnerabilities. This document is intended for technical teams and management to understand the current security posture and the steps taken to mitigate identified risks.

Audience

The primary audience includes cybersecurity professionals, system administrators, and management stakeholders involved in IT security and risk management.

What is Vulnerability Management?

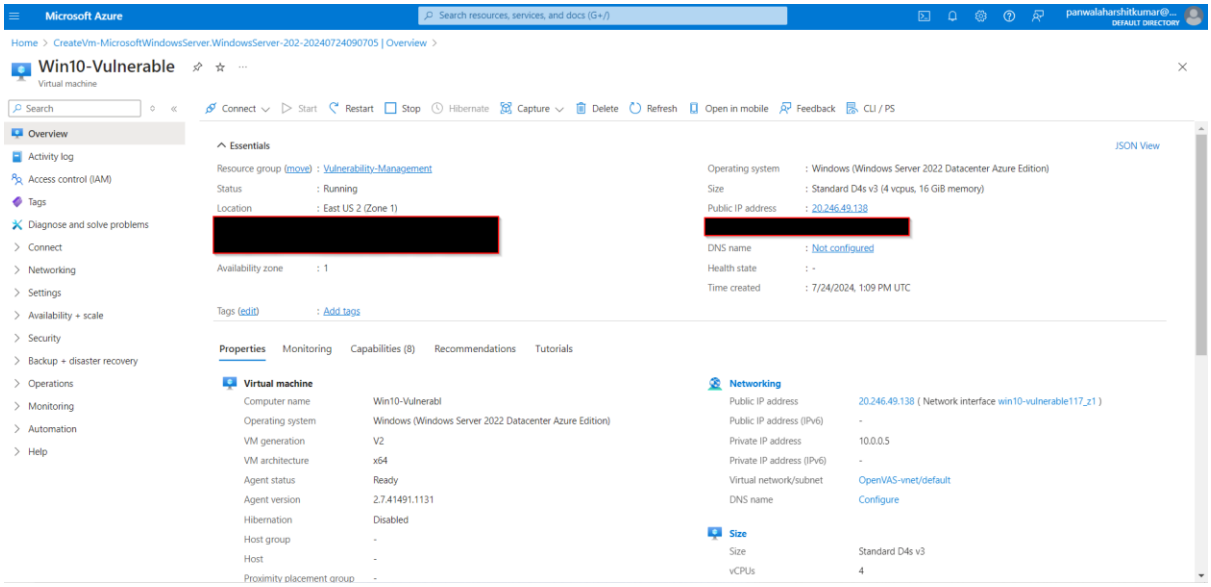
Vulnerability management is a critical process in cybersecurity that involves identifying, evaluating, treating, and reporting security vulnerabilities in systems and software. It ensures that security flaws are addressed proactively to prevent exploitation by malicious actors. This process includes regular scans, patch management, and configuration reviews.

Project Activities

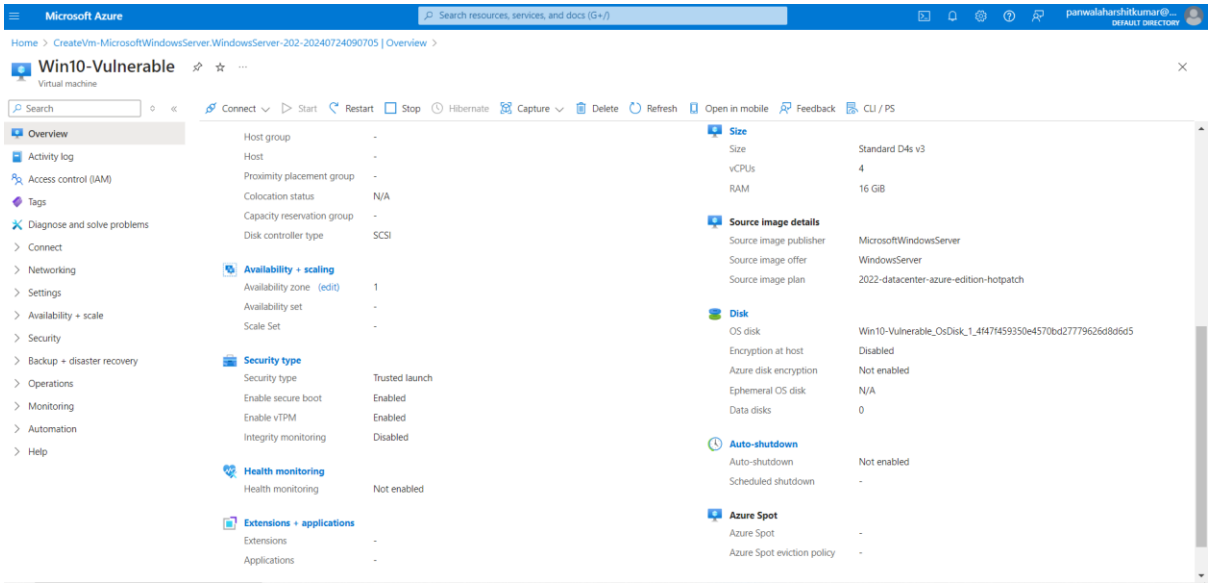
1. Setup Virtual Machine

Two VMs were set up on Azure:

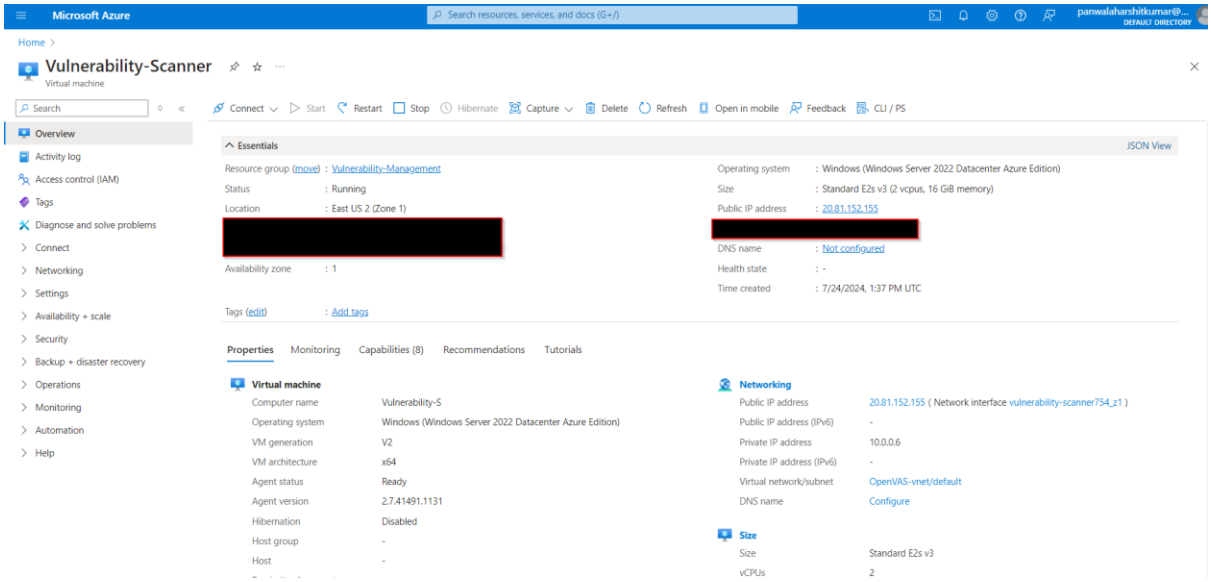
- **Win10-Vulnerable**: Target VM for vulnerability scanning.
- **Vulnerability-Scanner**: Host for Nessus Essentials.



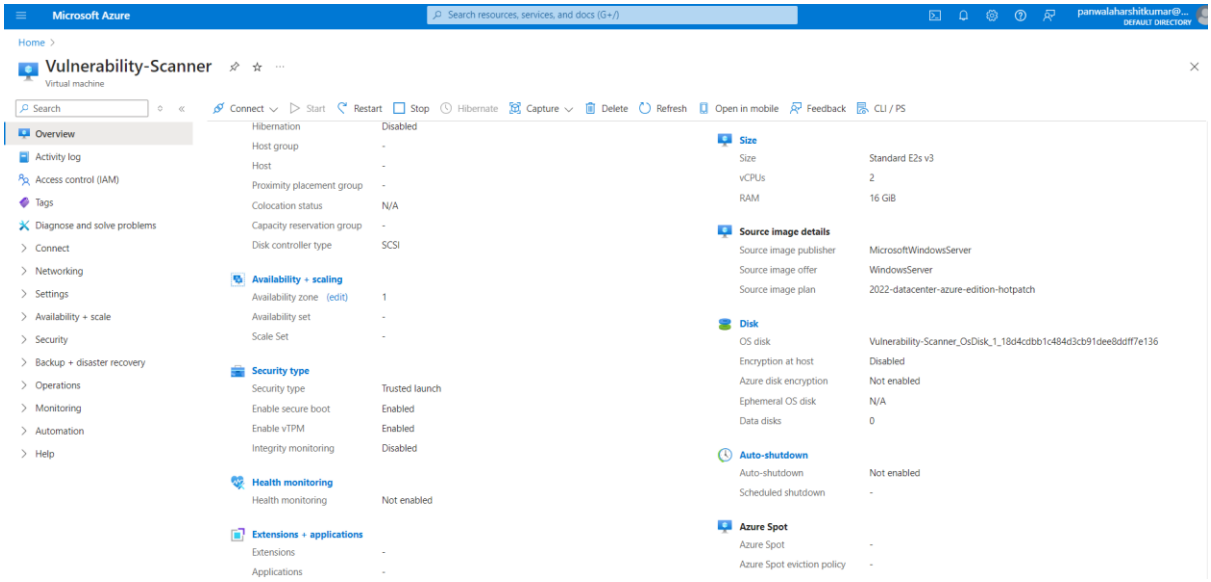
Win10-Vulnerable VM (1)



Win10-Vulnerable VM (2)



Vulnerability-Scanner VM (1)



Vulnerability-Scanner VM (2)

2. Download and Install Nessus Essentials

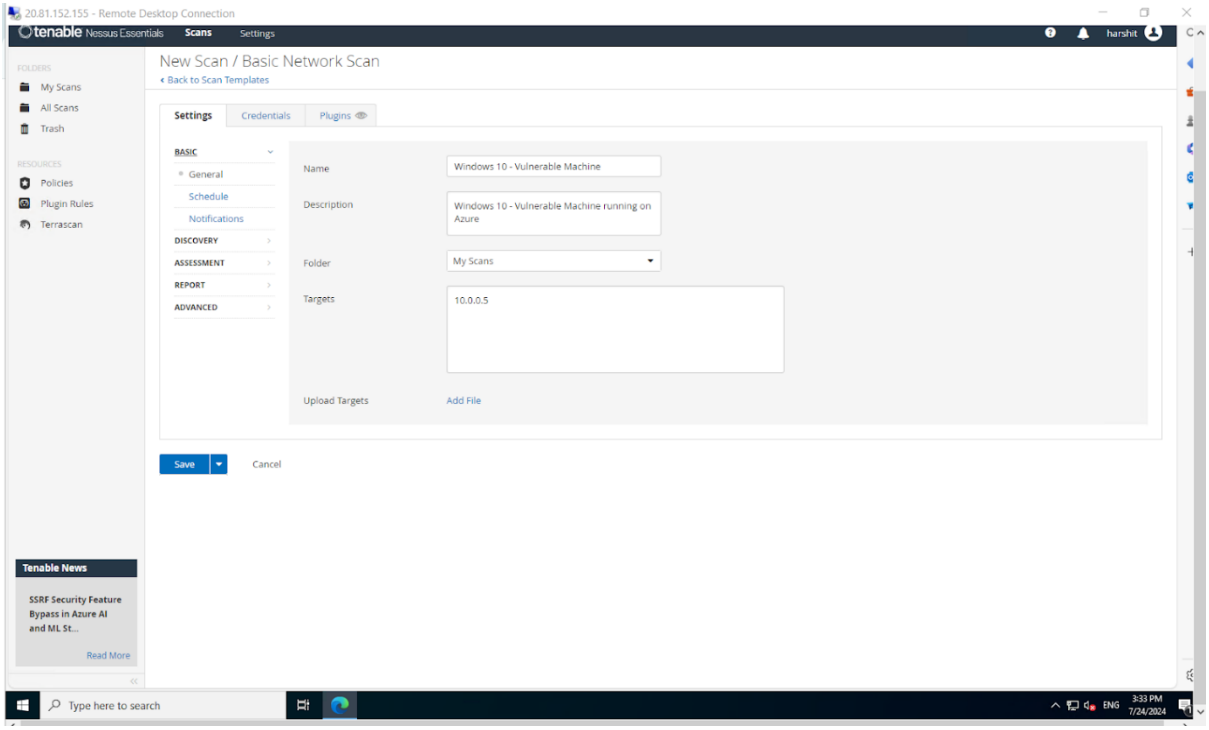
Nessus Essentials, a widely used vulnerability assessment tool, was installed on the "Vulnerability-Scanner" VM. This tool was selected for its comprehensive scanning capabilities and ease of use in detecting vulnerabilities across various systems. The Nessus web interface was accessed at https://localhost:8834/#/.

3. Ensure Connectivity with VM

Connectivity between the "Vulnerability-Scanner" and "Win10-Vulnerable" VMs was verified, ensuring that the scanner could reach the target VM over the network for scanning.

4. Create a New Scan in Nessus

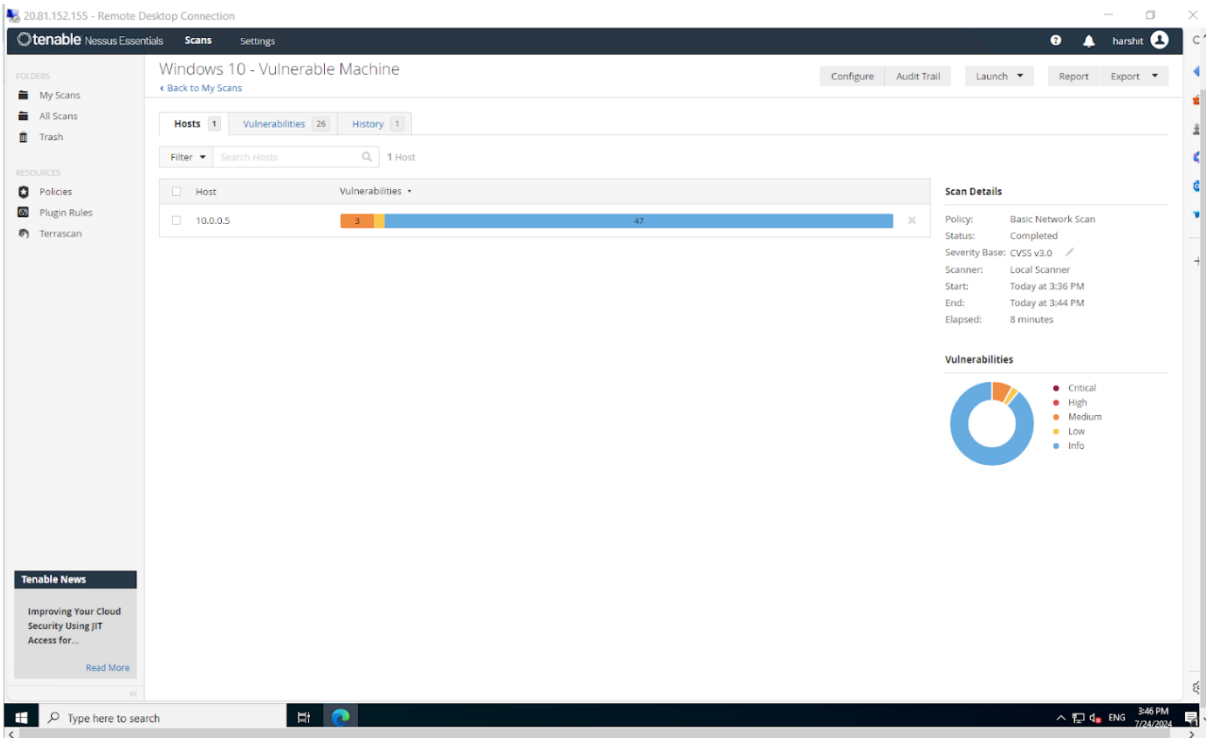
An uncredentialed scan was created and initiated in Nessus, targeting the IP address of the Win10-Vulnerable VM. This scan aimed to identify visible vulnerabilities without administrative access.



5. Inspecting the First Scan (No Credentials)

Findings:

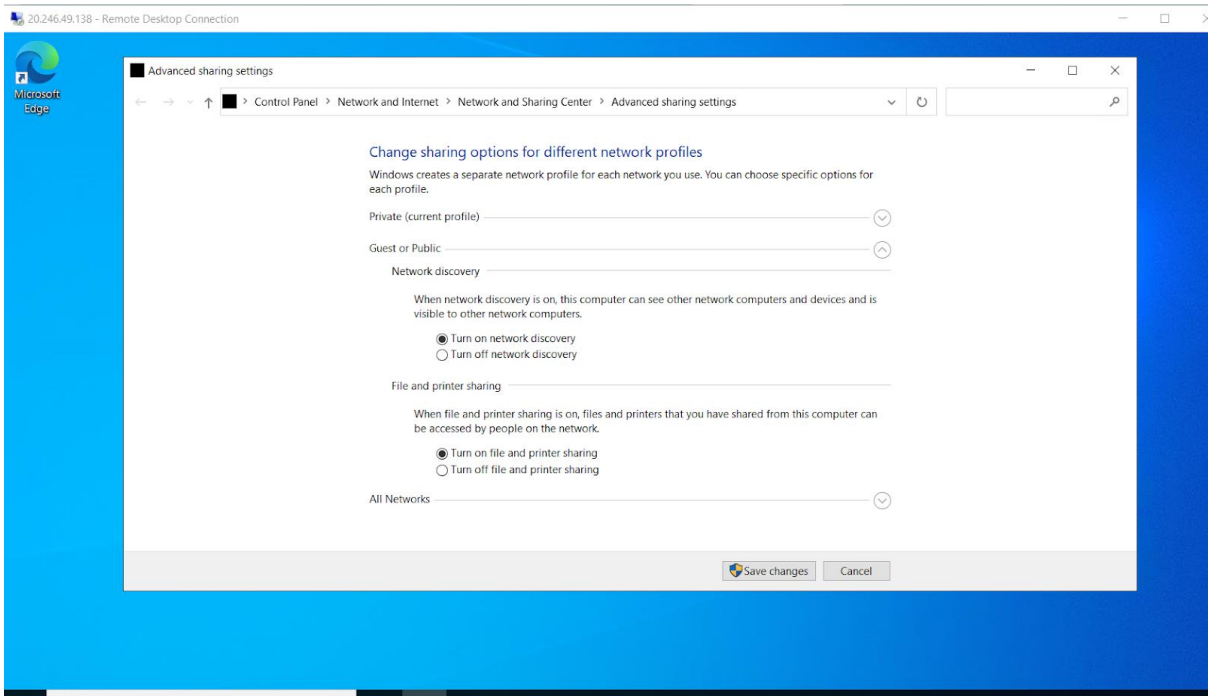
- Several vulnerabilities were detected, primarily related to network exposure and outdated software. However, the depth of the scan was limited due to the lack of administrative credentials.
- **Total Vulnerabilities Detected**: 4
- **Critical**: 0
- **High**: 0
- **Medium**: 3
- **Low**: 1
- **Info**: 47



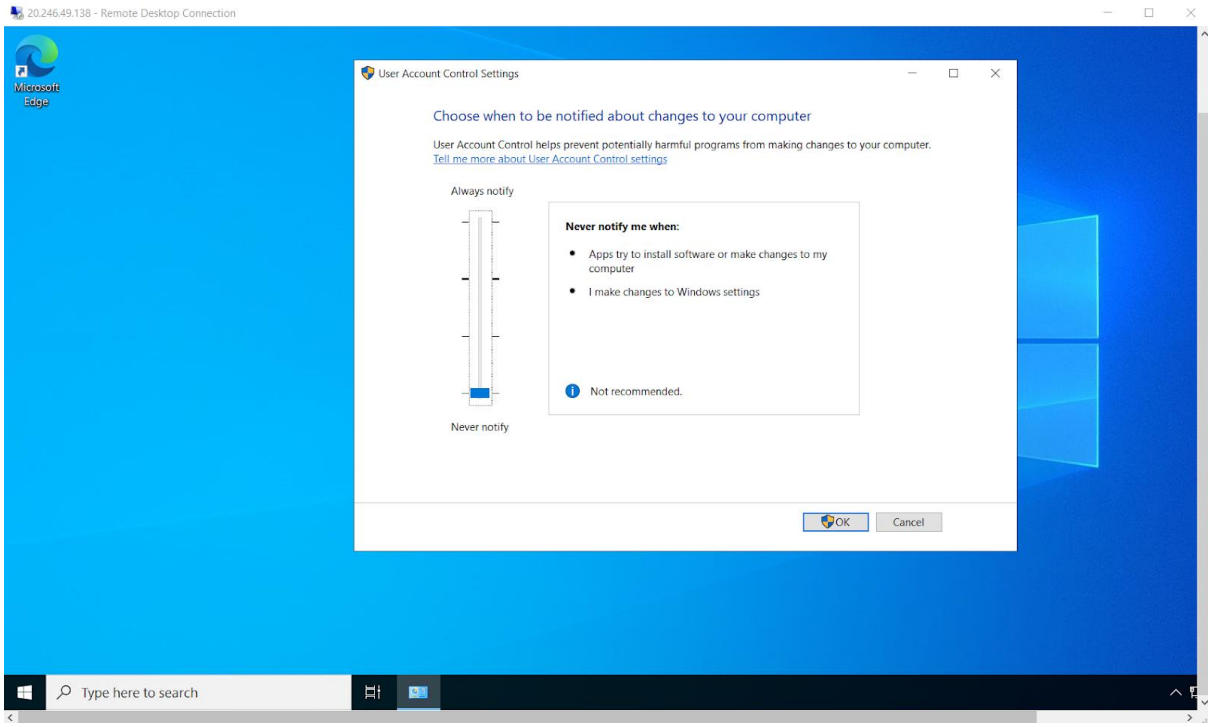
6. Configuring VM for Credentialed Scans

To facilitate a comprehensive scan, the following configurations were applied to the Win10-Vulnerable VM:

- **Remote Registry Service**: Enabled and set to automatic.
- **Network Discovery and File Sharing**: Enabled.
- **User Account Control (UAC)**: Set to "Never Notify."
- **Registry Modification**: Added `LocalAccountTokenFilterPolicy` DWORD with a value of 1.



Advanced sharing settings

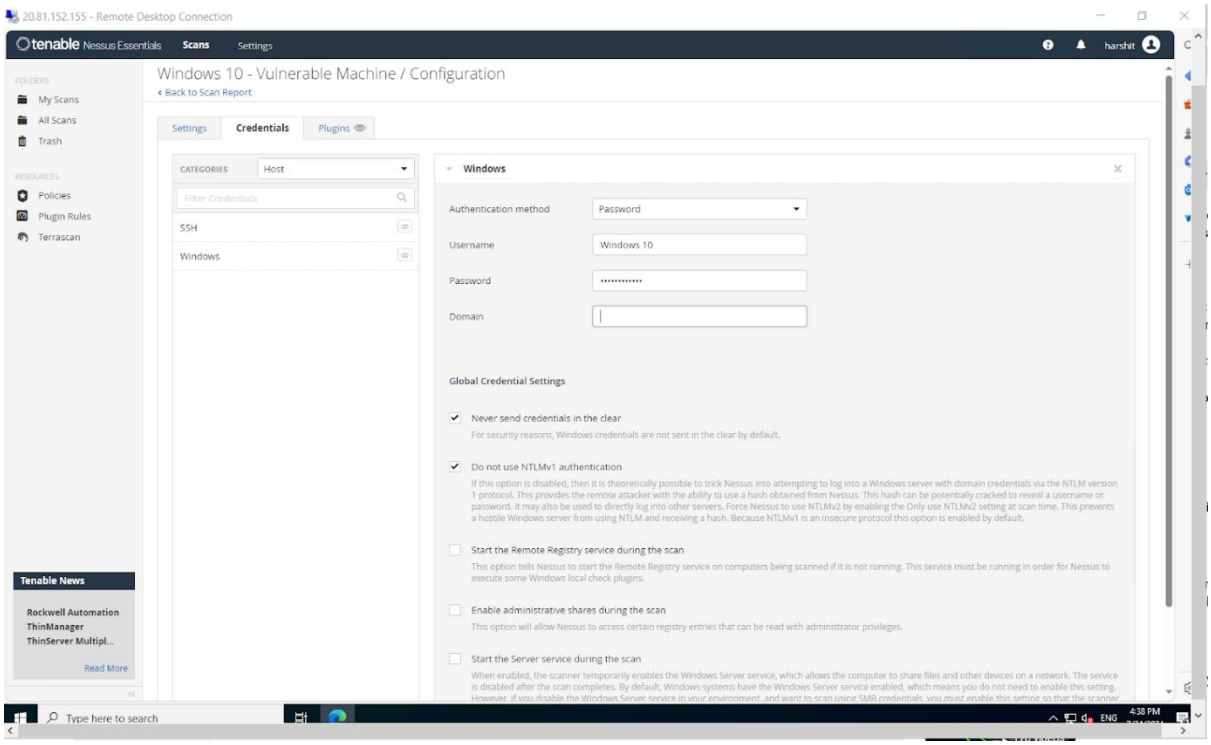


User Account Control

These changes allowed Nessus to perform deeper inspections, accessing system settings and configurations.

7. First Scan with Credentials

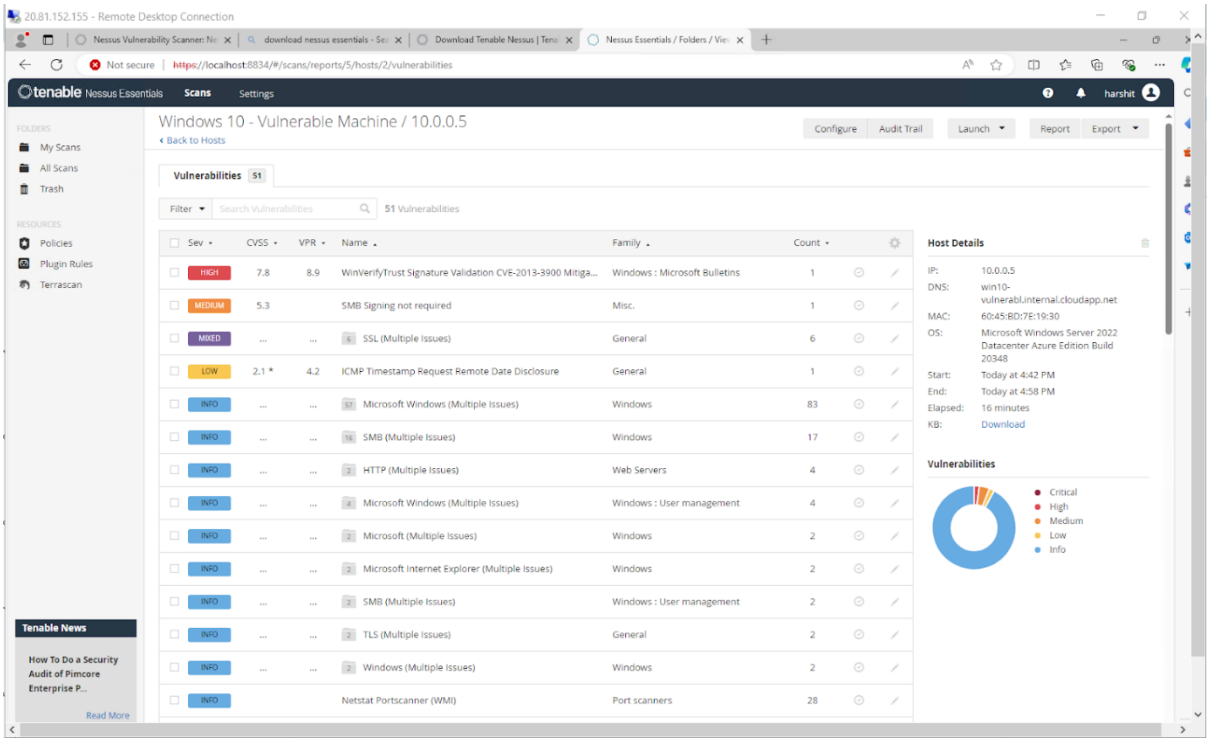
A credentialed scan was initiated using administrative credentials. This scan provided a more detailed view of the system's vulnerabilities, including those related to installed software and system configurations.



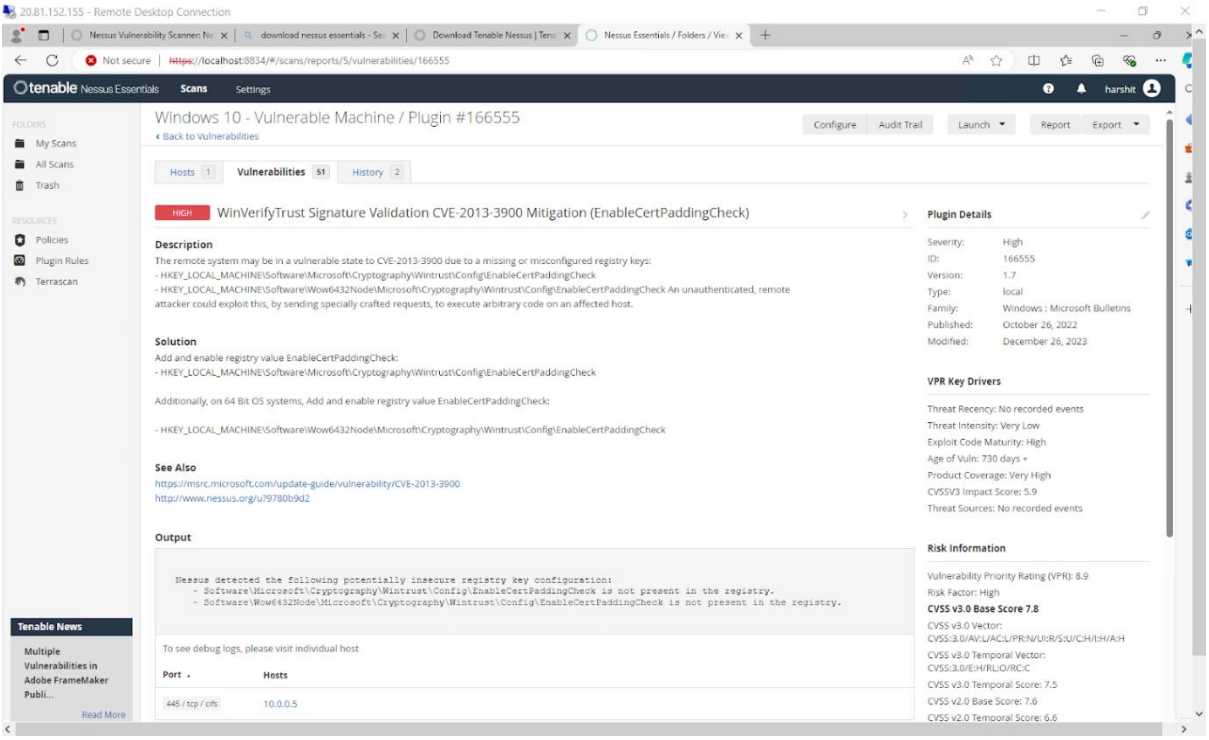
8. Inspecting First Scan with Credentials Results

Findings:

- **Total Vulnerabilities Detected**: 5
- **Critical**: 0
- **High**: 1
- **Medium**: 3
- **Low**: 1
- **Info**: 198



Significant vulnerabilities included outdated software versions, insecure system settings, and exposure to potential exploits.



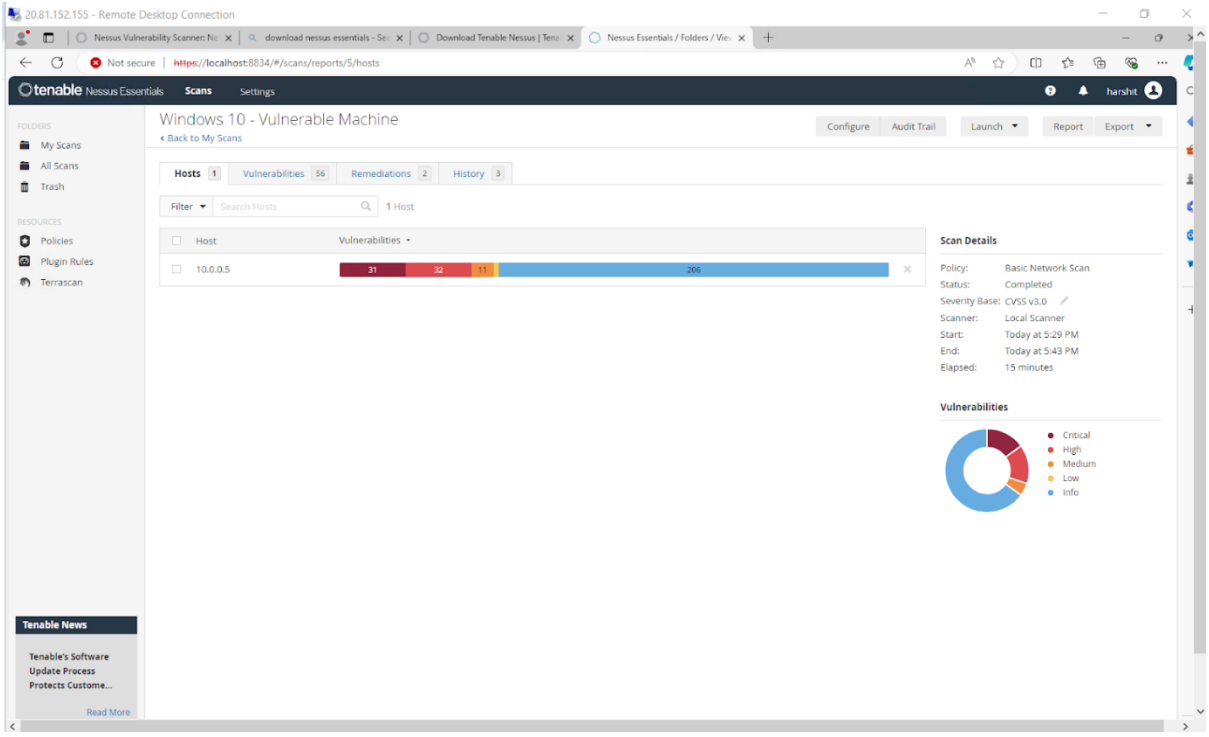
9. Installing Deprecated Firefox and VLC Media Player on Our VM

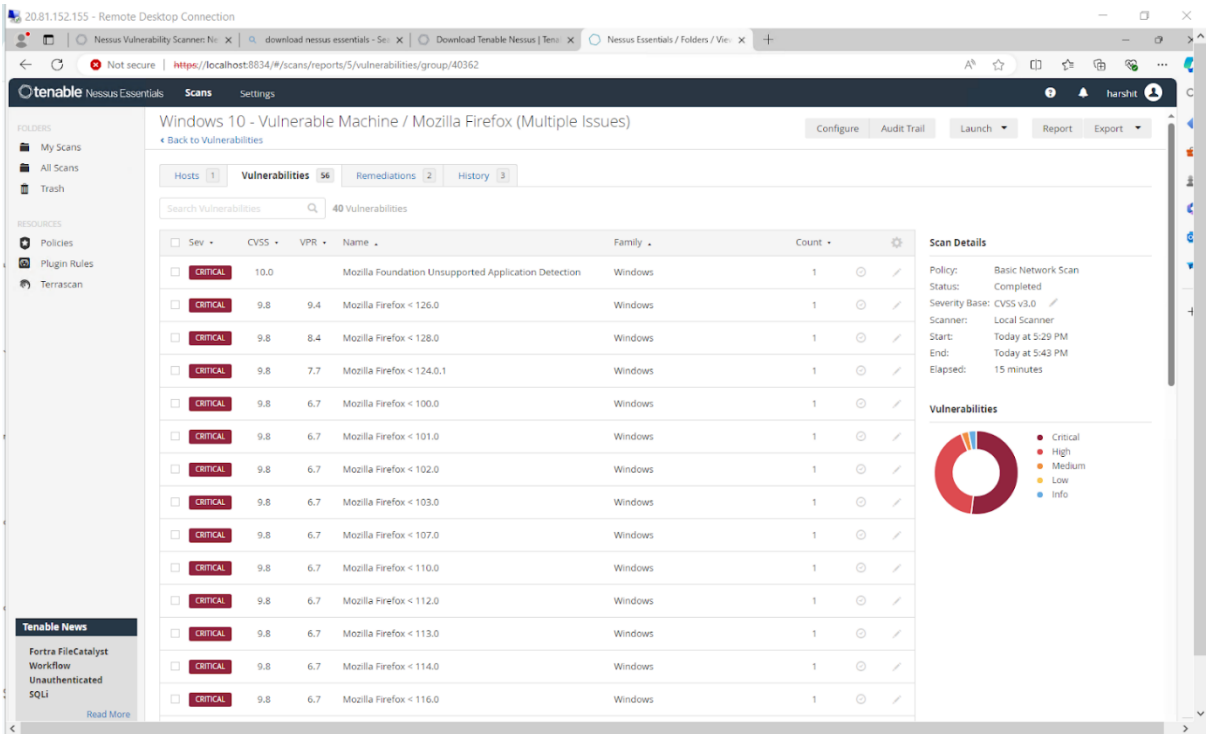
To test the vulnerability detection capabilities, outdated versions of Mozilla Firefox and VLC Media Player were installed on the Win10-Vulnerable VM. These software products are known for having critical security vulnerabilities due to their unsupported status.

10. Inspect Scan Results After Installing Deprecated Firefox and VLC Media Player

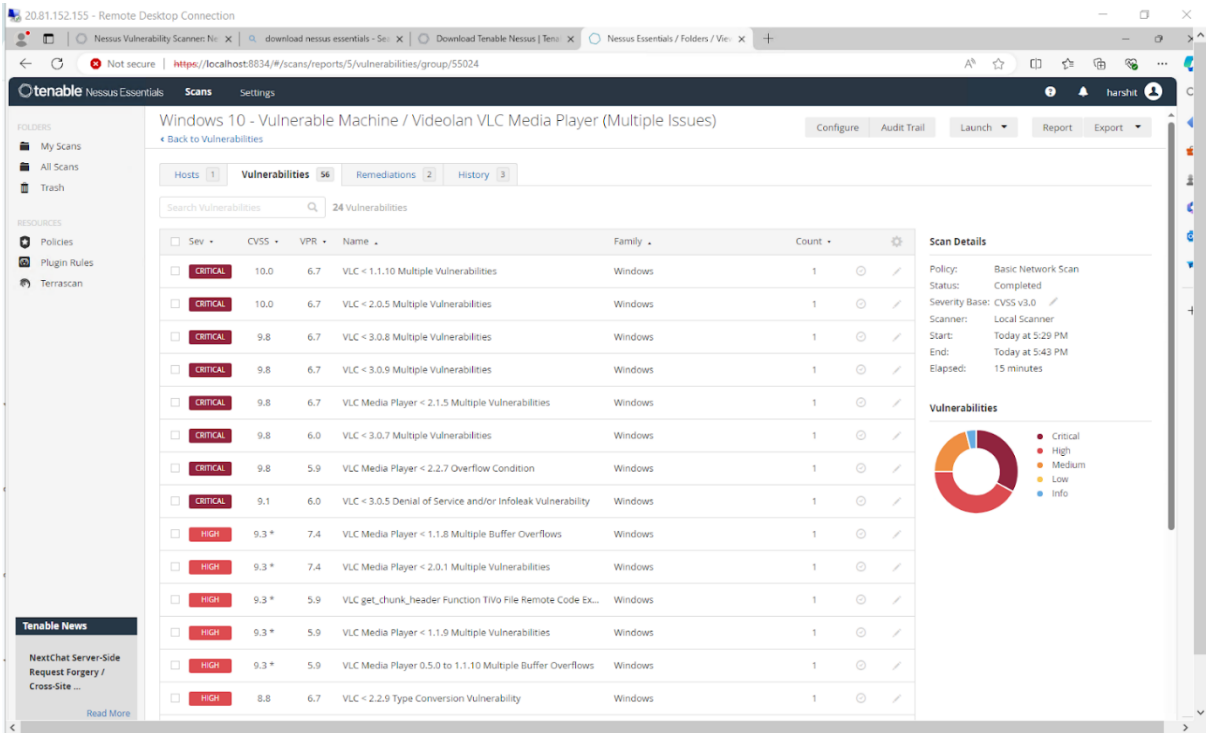
Findings:

- **Increased Number of Vulnerabilities**: Notable increase in critical and high severity vulnerabilities due to the introduction of deprecated software.
- **Total Vulnerabilities Detected**: 75
- **Critical**: 31
- **High**: 32
- **Medium**: 11
- **Low**: 1
- **Info**: 206





Vulnerable Machine/Mozilla Firefox

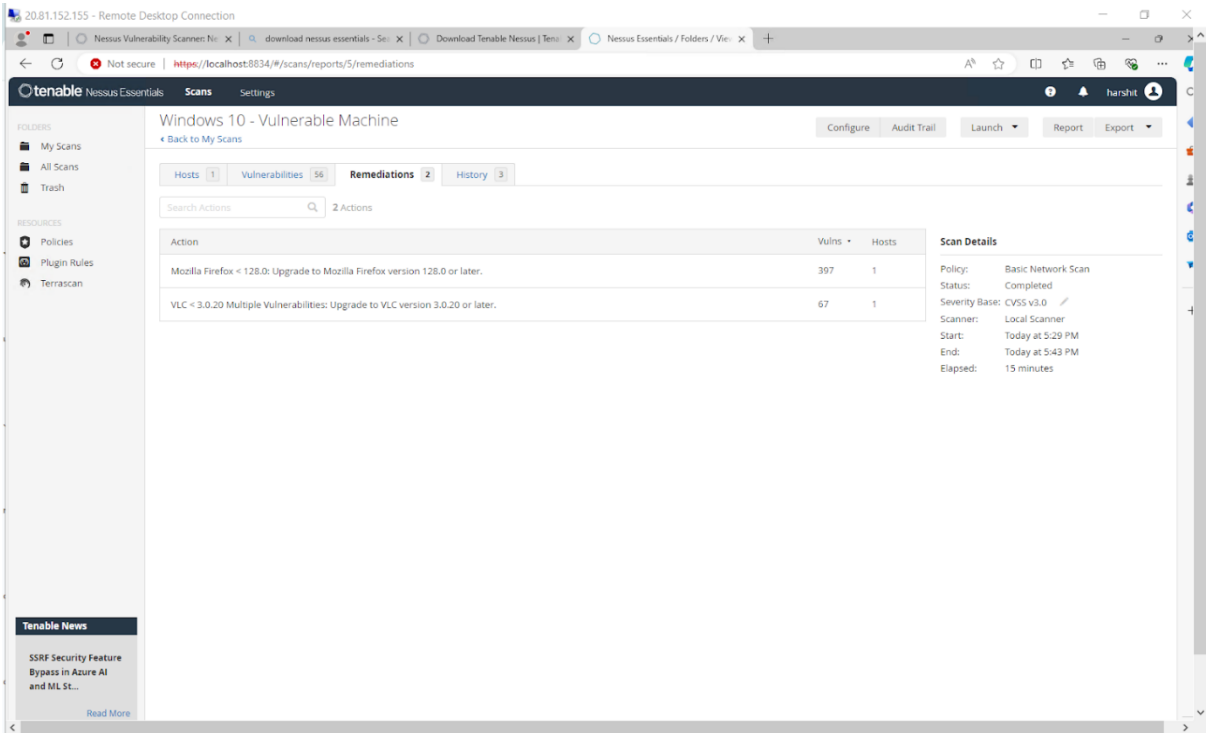


Vulnerable Machine/VLC Media Player

11. Remediating Some Vulnerabilities

Key remediation actions included:

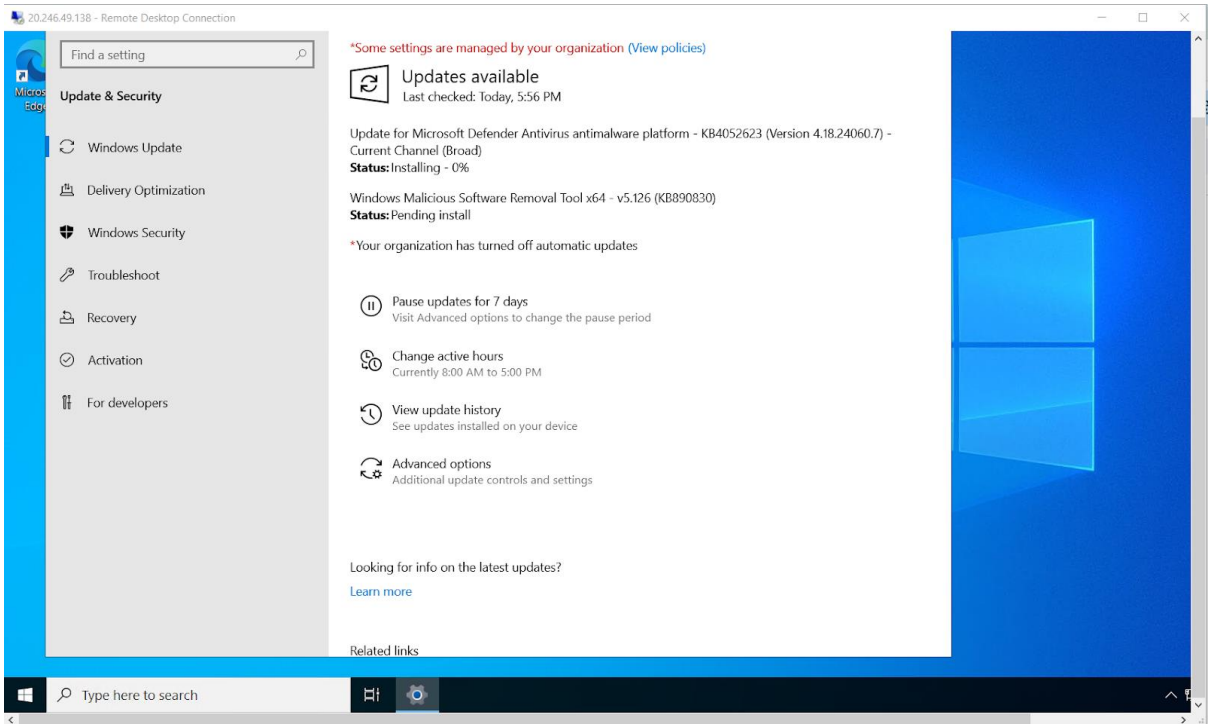
- **Uninstalling Deprecated Software**: Firefox, VLC Media Player, and other outdated applications were removed.
- **System Updates**: Applied all available security patches and updates to the operating system and remaining software.



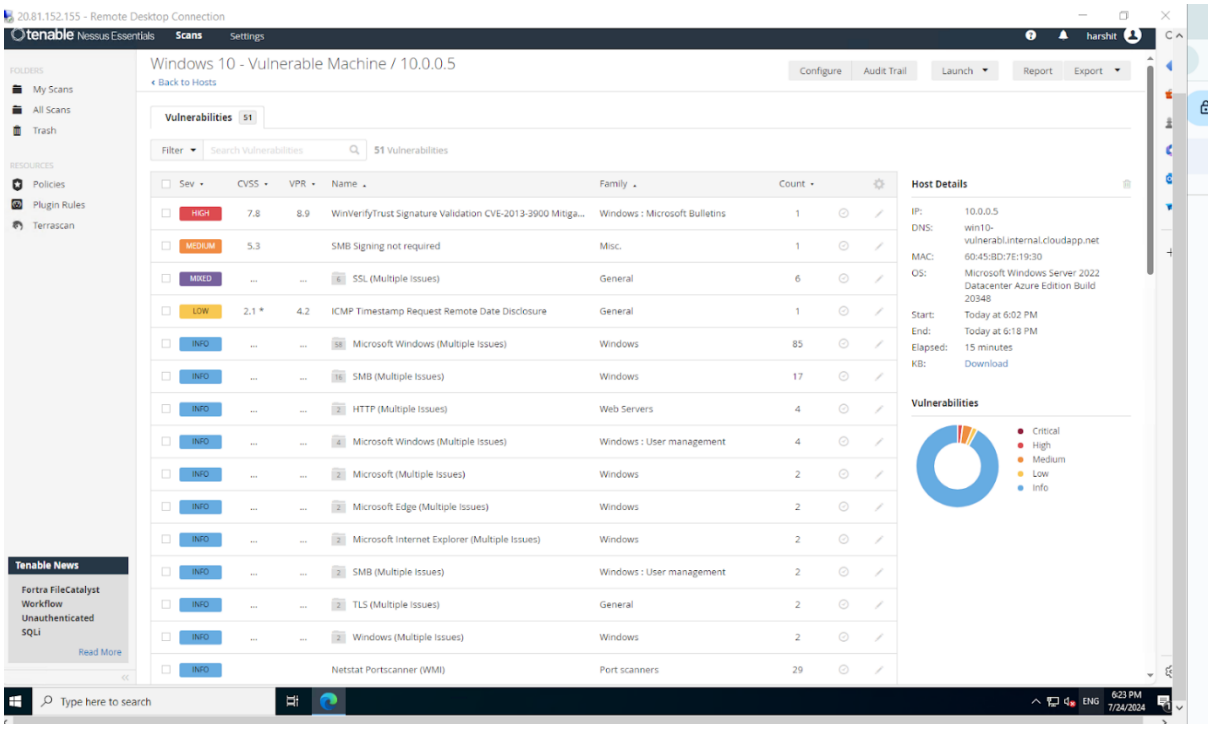
12. Inspect Scan Results After Remediating Some Vulnerabilities

Findings:

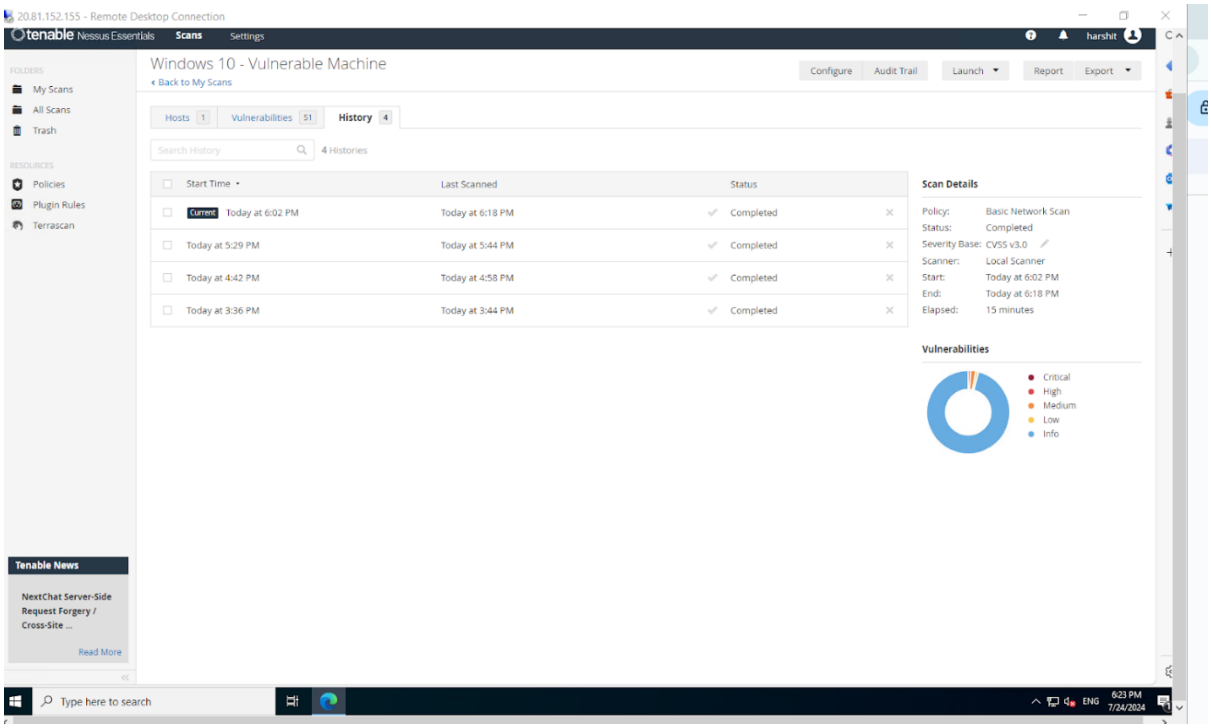
- **Reduction in Critical and High Severity Vulnerabilities**: The number of critical and high vulnerabilities significantly decreased, indicating successful remediation.
- **Total Vulnerabilities Detected**: 5
- **Critical**: 0
- **High**: 1
- **Medium**: 3
- **Low**: 1
- **Info**: 202



Updates



Final Scan Results (1)



Final Scan Results (2)

13. Other Thoughts on Enterprise Vulnerability Management

- **Continuous Monitoring**: Regular scans and updates are crucial for maintaining a secure environment.
- **Policy and Compliance**: Adherence to security policies and compliance standards is essential for safeguarding against threats.
- **User Training and Awareness**: Educating users on security best practices helps in reducing the risk of human error and enhancing overall security posture.

Challenges Faced

Throughout this project, I encountered a few hurdles that required creative solutions:

1. **Installation Issues**: I initially faced persistent problems while trying to install Nessus Essentials on my host machine. Despite multiple attempts, errors related to user creation kept cropping up, making it clear that something was amiss.
2. **Transition to Azure**: To resolve these issues, I decided to move the project to Azure. This shift was not only a practical solution but also provided a valuable learning experience. Working with Azure offered me a deeper understanding of cloud-based environments and management, which proved beneficial.

Ultimately, using Azure helped smooth out the project's execution and allowed me to handle the vulnerability assessment process more efficiently. This experience turned a challenging situation into an opportunity for growth and skill enhancement.

Conclusion

The vulnerability management project on the Win10-Vulnerable VM has highlighted key areas of improvement and resulted in a more secure system environment. Ongoing vigilance, including regular updates and continuous monitoring, is essential for maintaining security and protecting against emerging threats.