

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.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20240724090705 | Overview >

Win10-Vulnerable

Virtual machine

Search

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Essentials

Resource group (move) : [Vulnerability-Management](#)

Status : Running

Location : East US 2 (Zone 1)

Availability zone : 1

Tags (edit) : [Add tags](#)

Operating system : Windows (Windows Server 2022 Datacenter Azure Edition)

Size : Standard D4s v3 (4 vcpus, 16 GiB memory)

Public IP address : [20.246.49.138](#)

DNS name : [Not configured](#)

Health state : -

Time created : 7/24/2024, 1:09 PM UTC

JSON View

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	Win10-Vulnerabl
Operating system	Windows (Windows Server 2022 Datacenter Azure Edition)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1131
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-

Networking

Public IP address	20.246.49.138 (Network interface win10-vulnerable117_z1)
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	OpenVAS-vnet/default
DNS name	Configure

Size

Size	Standard D4s v3
vCPUs	4

Win10-Vulnerable VM (1)

Microsoft Azure

Search resources, services, and docs (G+/)

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20240724090705 | Overview >

Win10-Vulnerable

Virtual machine

Search

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Host group -

Host -

Proximity placement group -

Colocation status N/A

Capacity reservation group -

Disk controller type SCSI

Availability + scaling

Availability zone (edit)	1
Availability set	-
Scale Set	-

Security type

Security type	Trusted launch
Enable secure boot	Enabled
Enable vTPM	Enabled
Integrity monitoring	Disabled

Health monitoring

Health monitoring	Not enabled
-------------------	-------------

Extensions + applications

Extensions	-
Applications	-

Size

Size	Standard D4s v3
vCPUs	4
RAM	16 GiB

Source image details

Source image publisher	MicrosoftWindowsServer
Source image offer	WindowsServer
Source image plan	2022-datacenter-azure-edition-hotpatch

Disk

OS disk	Win10-Vulnerable_OsDisk_1_4f47459350e4570bd2779626d8d6d5
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

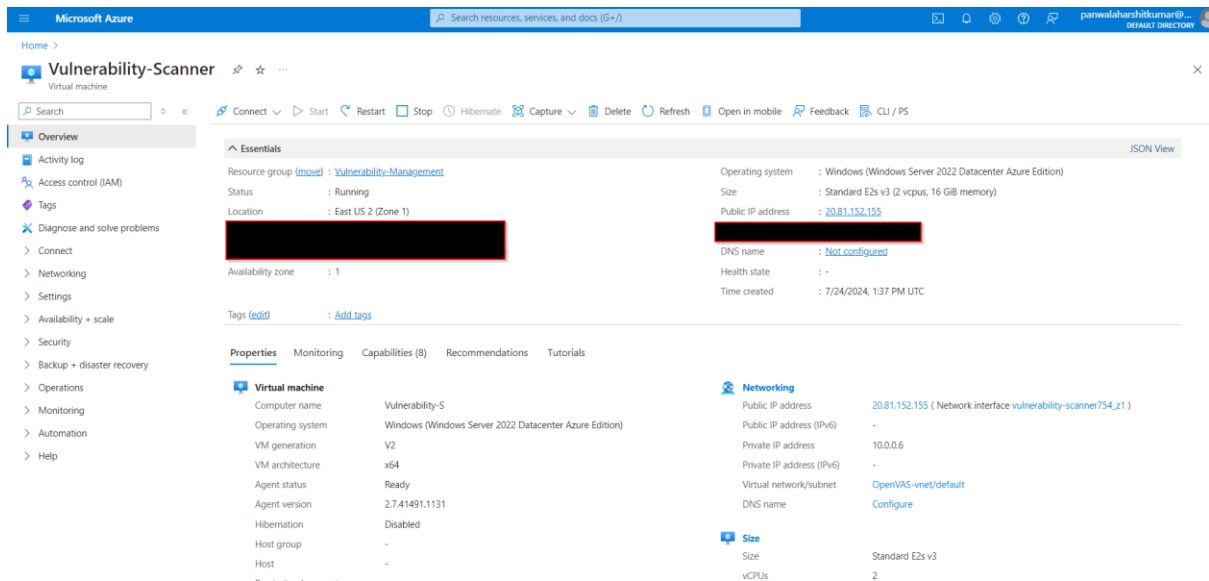
Auto-shutdown

Auto-shutdown	Not enabled
Scheduled shutdown	-

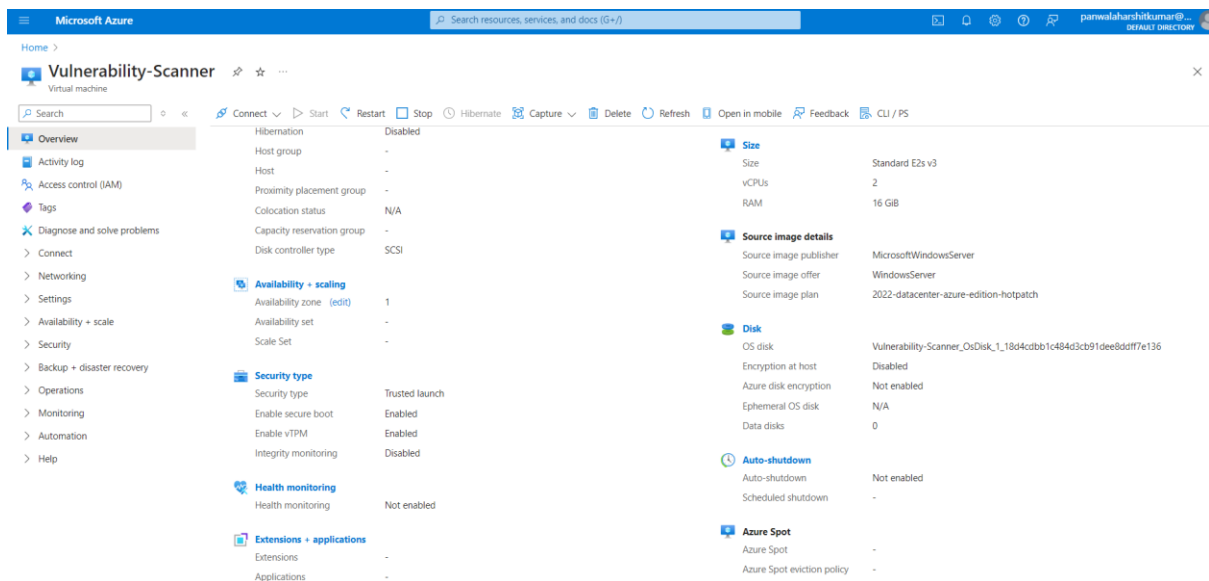
Azure Spot

Azure Spot	-
Azure Spot eviction policy	-

Win10-Vulnerable VM (2)



Vulnerability-Scanner VM (1)



Vulnerability-Scanner VM (2)

2. Download and Install Nessus Essentials

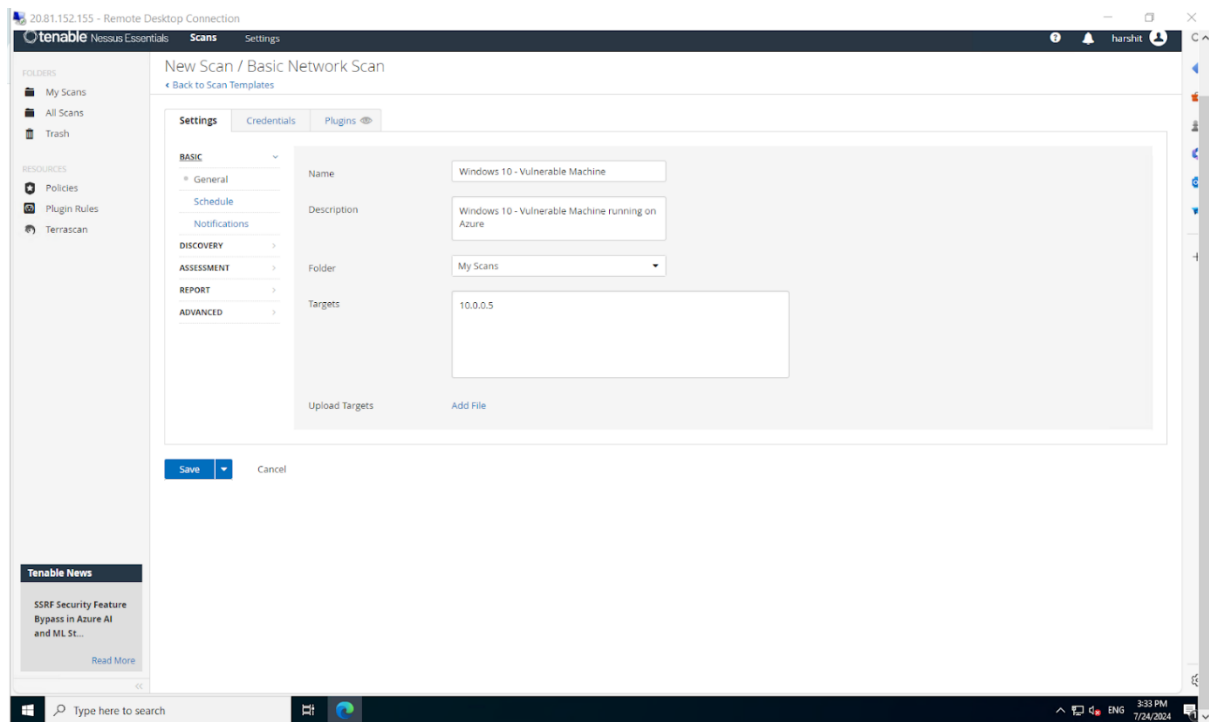
Nessus Essentials, a widely used vulnerability assessment tool, was installed on the "Vulnerability-Scanner" VM. This tool was selected for its comprehensive scanning capabilities and ease of use in detecting vulnerabilities across various systems. The Nessus web interface was accessed at <https://localhost:8834/#/>.

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

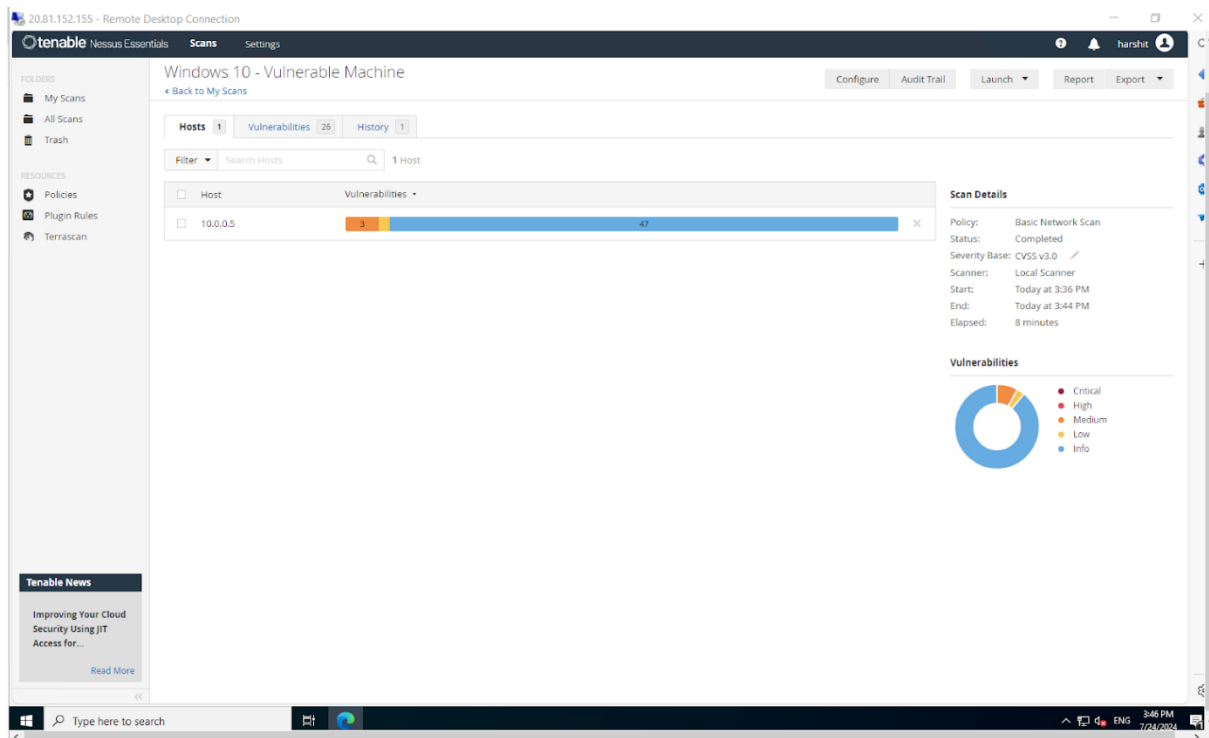
An uncredentialed scan was created and initiated in Nessus, targeting the IP address of the Win10-Vulnerable VM. This scan aimed to identify visible vulnerabilities without administrative access.



5. Inspecting the First Scan (No Credentials)

Findings:

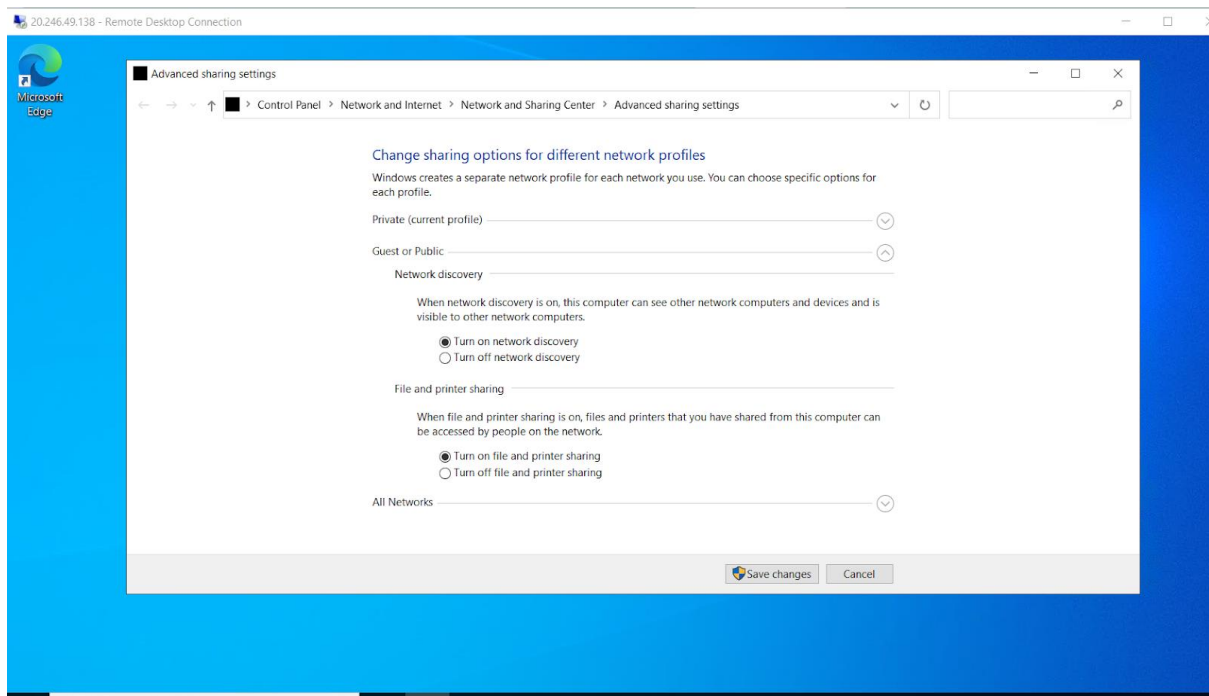
- Several vulnerabilities were detected, primarily related to network exposure and outdated software. However, the depth of the scan was limited due to the lack of administrative credentials.
- **Total Vulnerabilities Detected: 4**
- **Critical: 0**
- **High: 0**
- **Medium: 3**
- **Low: 1**
- **Info: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



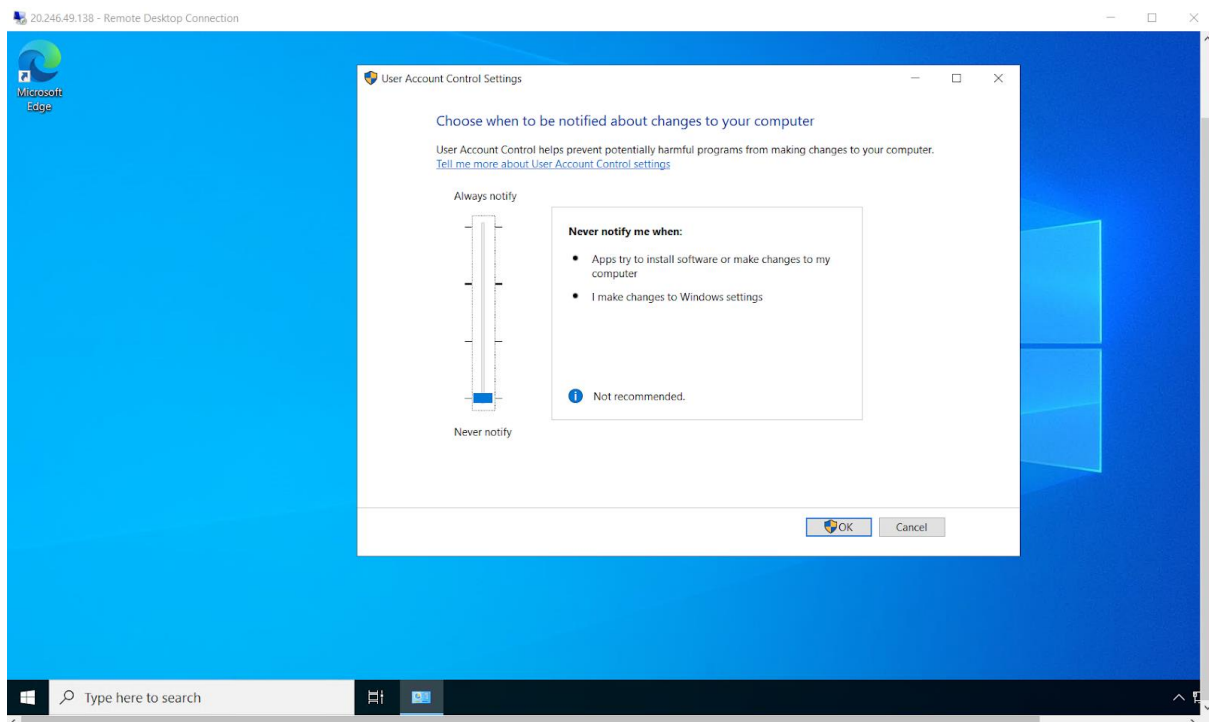
6. Configuring VM for Credentialed Scans

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

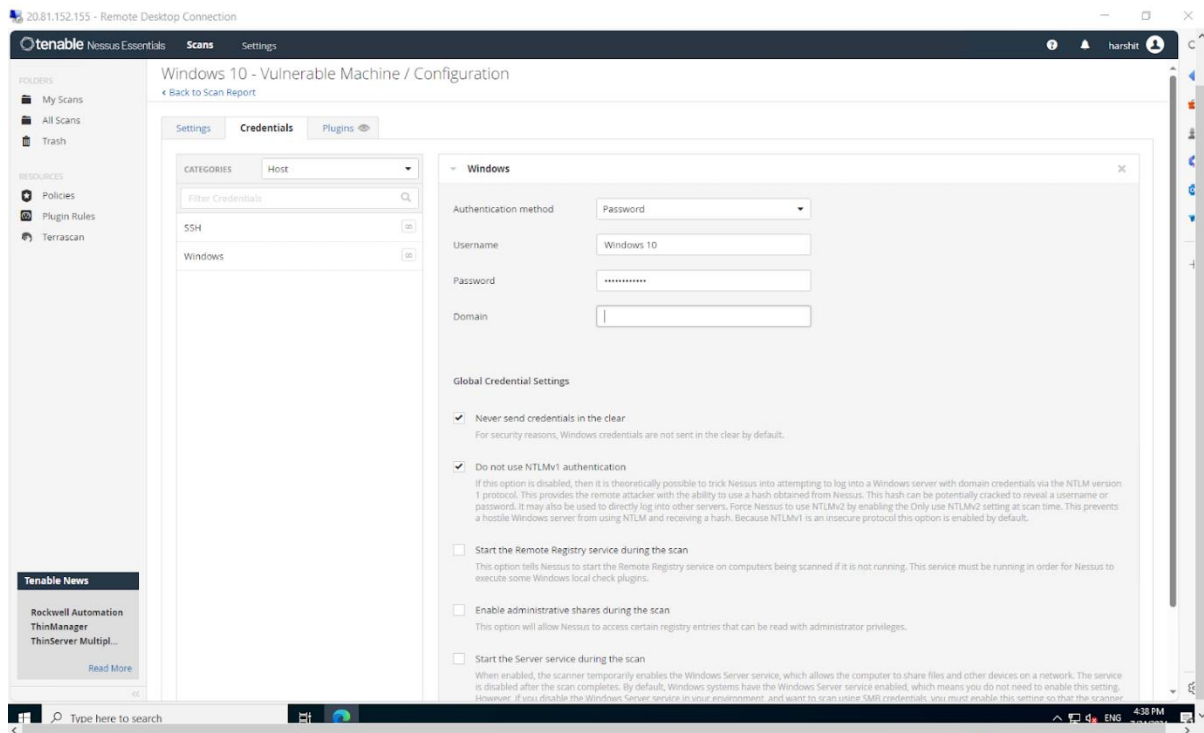


User Account Control

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**

Windows 10 - Vulnerable Machine / 10.0.0.5

Back to Hosts

Vulnerabilities 51

Filter Search Vulnerabilities 51 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
HIGH	7.8	8.9	WinVerifyTrust Signature Validation CVE-2013-3900 Mitiga...	Windows : Microsoft Bulletins	1
MEDIUM	5.3		SMB Signing not required	Misc.	1
MIXED			SSL (Multiple Issues)	General	6
LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO			Microsoft Windows (Multiple Issues)	Windows	83
INFO			SMB (Multiple Issues)	Windows	17
INFO			HTTP (Multiple Issues)	Web Servers	4
INFO			Microsoft Windows (Multiple Issues)	Windows : User management	4
INFO			Microsoft (Multiple Issues)	Windows	2
INFO			Microsoft Internet Explorer (Multiple Issues)	Windows	2
INFO			SMB (Multiple Issues)	Windows : User management	2
INFO			TLS (Multiple Issues)	General	2
INFO			Windows (Multiple Issues)	Windows	2
INFO			Netstat Portscanner (WMI)	Port scanners	28

Host Details

IP: 10.0.0.5
 DNS: win10-vulnerable.internal.cloudapp.net
 MAC: 60:45:BD:7E:19:30
 OS: Microsoft Windows Server 2022 Datacenter Azure Edition Build 20348
 Start: Today at 4:42 PM
 End: Today at 4:58 PM
 Elapsed: 16 minutes
 KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

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

Windows 10 - Vulnerable Machine / Plugin #166555

Back to Vulnerabilities

Hosts 1 Vulnerabilities 51 History 2

HIGH WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

Solution

Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

See Also

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900>
<https://www.nessus.org/u/9780b9d2>

Output

```

Nessus detected the following potentially insecure registry key configuration:
- Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry.
- Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry.
  
```

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / off	10.0.0.5

Plugin Details

Severity: High
 ID: 166555
 Version: 1.7
 Type: local
 Family: Windows : Microsoft Bulletins
 Published: October 26, 2022
 Modified: December 26, 2023

VPR Key Drivers

Threat Recency: No recorded events
 Threat Intensity: Very Low
 Exploit Code Maturity: High
 Age of Vuln: 730 days +
 Product Coverage: Very High
 CVSSV3 Impact Score: 5.9
 Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 8.9
 Risk Factor: High
CVSS v3.0 Base Score 7.8
 CVSS v3.0 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:U/A:H
 CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R:L/O:R/C:C
 CVSS v3.0 Temporal Score: 7.5
 CVSS v2.0 Base Score: 7.6
 CVSS v2.0 Temporal Score: 6.6

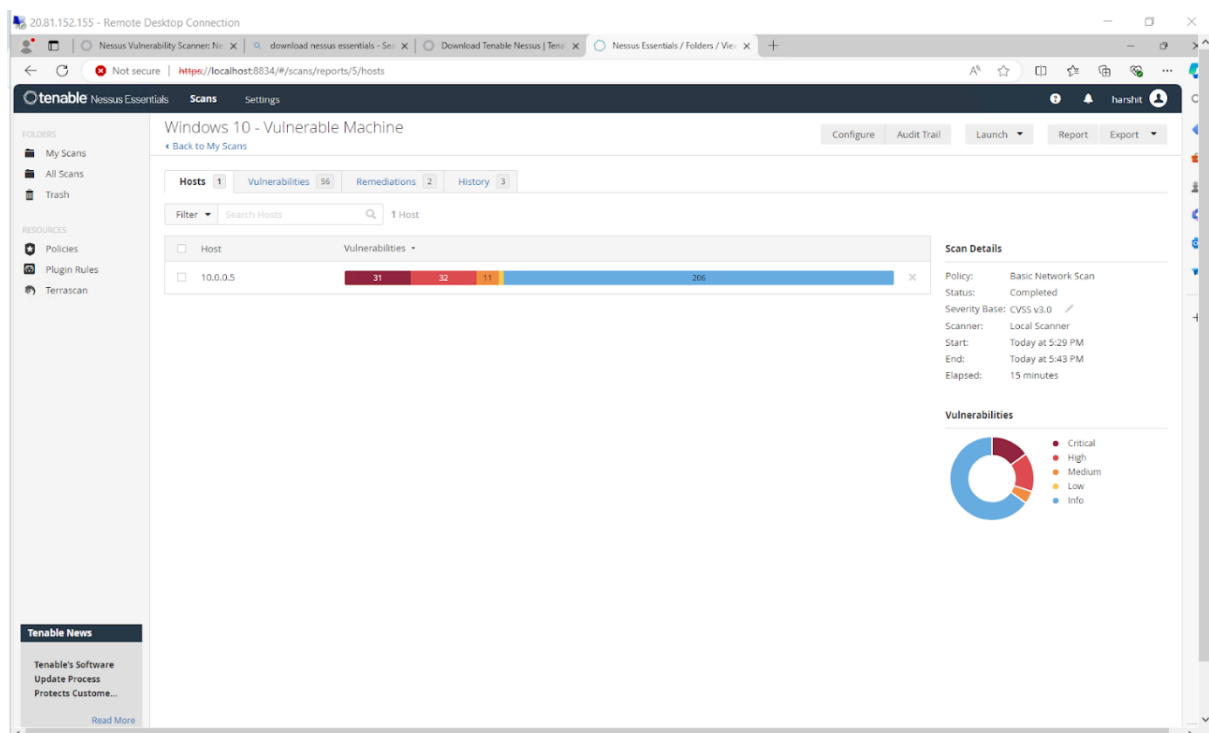
9. Installing Deprecated Firefox and VLC Media Player on Our VM

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**



20.81.152.155 - Remote Desktop Connection

Nessus Vulnerability Scanner: Nessus | download nessus essentials - Se: X | Download Tenable Nessus | Tena: X | Nessus Essentials / Folders / Vie: X

Not secure | https://localhost:8834/#/scans/reports/5/vulnerabilities/group/40362

tenable Nessus Essentials Scans Settings

Windows 10 - Vulnerable Machine / Mozilla Firefox (Multiple Issues)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 56 Remediations 2 History 3

Search Vulnerabilities 40 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Mozilla Foundation Unsupported Application Detection	Windows	1	
CRITICAL	9.8	9.4	Mozilla Firefox < 126.0	Windows	1	
CRITICAL	9.8	8.4	Mozilla Firefox < 128.0	Windows	1	
CRITICAL	9.8	7.7	Mozilla Firefox < 124.0.1	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 100.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 101.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 102.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 103.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 107.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 110.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 112.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 113.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 114.0	Windows	1	
CRITICAL	9.8	6.7	Mozilla Firefox < 116.0	Windows	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:29 PM
End: Today at 5:43 PM
Elapsed: 15 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Vulnerable Machine/Mozilla Firefox

20.81.152.155 - Remote Desktop Connection

Nessus Vulnerability Scanner: Nessus | download nessus essentials - Se: X | Download Tenable Nessus | Tena: X | Nessus Essentials / Folders / Vie: X

Not secure | https://localhost:8834/#/scans/reports/5/vulnerabilities/group/55024

tenable Nessus Essentials Scans Settings

Windows 10 - Vulnerable Machine / Videolan VLC Media Player (Multiple Issues)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 56 Remediations 2 History 3

Search Vulnerabilities 24 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0	6.7	VLC < 1.1.10 Multiple Vulnerabilities	Windows	1	
CRITICAL	10.0	6.7	VLC < 2.0.5 Multiple Vulnerabilities	Windows	1	
CRITICAL	9.8	6.7	VLC < 3.0.8 Multiple Vulnerabilities	Windows	1	
CRITICAL	9.8	6.7	VLC < 3.0.9 Multiple Vulnerabilities	Windows	1	
CRITICAL	9.8	6.7	VLC Media Player < 2.1.5 Multiple Vulnerabilities	Windows	1	
CRITICAL	9.8	6.0	VLC < 3.0.7 Multiple Vulnerabilities	Windows	1	
CRITICAL	9.8	5.9	VLC Media Player < 2.2.7 Overflow Condition	Windows	1	
CRITICAL	9.1	6.0	VLC < 3.0.5 Denial of Service and/or Infoleak Vulnerability	Windows	1	
HIGH	9.3 *	7.4	VLC Media Player < 1.1.8 Multiple Buffer Overflows	Windows	1	
HIGH	9.3 *	7.4	VLC Media Player < 2.0.1 Multiple Vulnerabilities	Windows	1	
HIGH	9.3 *	5.9	VLC get_chunk_header Function Tivo File Remote Code Ex...	Windows	1	
HIGH	9.3 *	5.9	VLC Media Player < 1.1.9 Multiple Vulnerabilities	Windows	1	
HIGH	9.3 *	5.9	VLC Media Player 0.5.0 to 1.1.10 Multiple Buffer Overflows	Windows	1	
HIGH	8.8	6.7	VLC < 2.2.9 Type Conversion Vulnerability	Windows	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:29 PM
End: Today at 5:43 PM
Elapsed: 15 minutes

Vulnerabilities

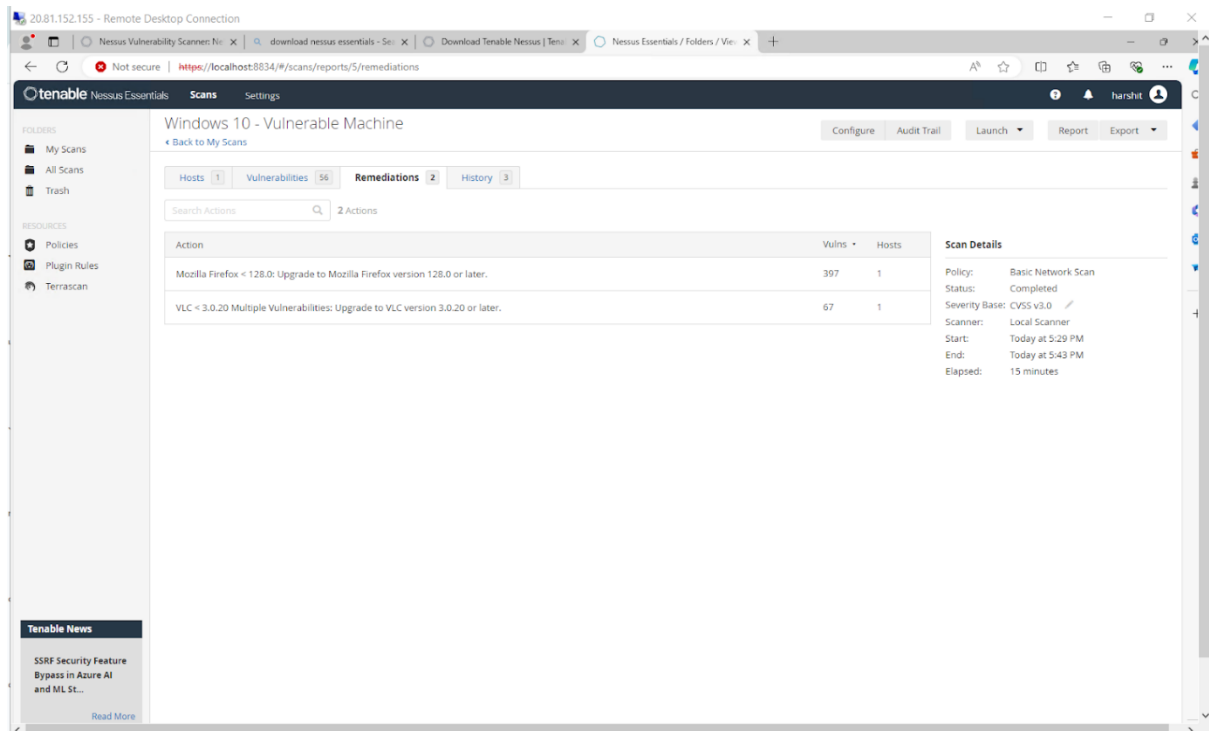
Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Vulnerable Machine/VLC Media Player

11. Remediating Some Vulnerabilities

Key remediation actions included:

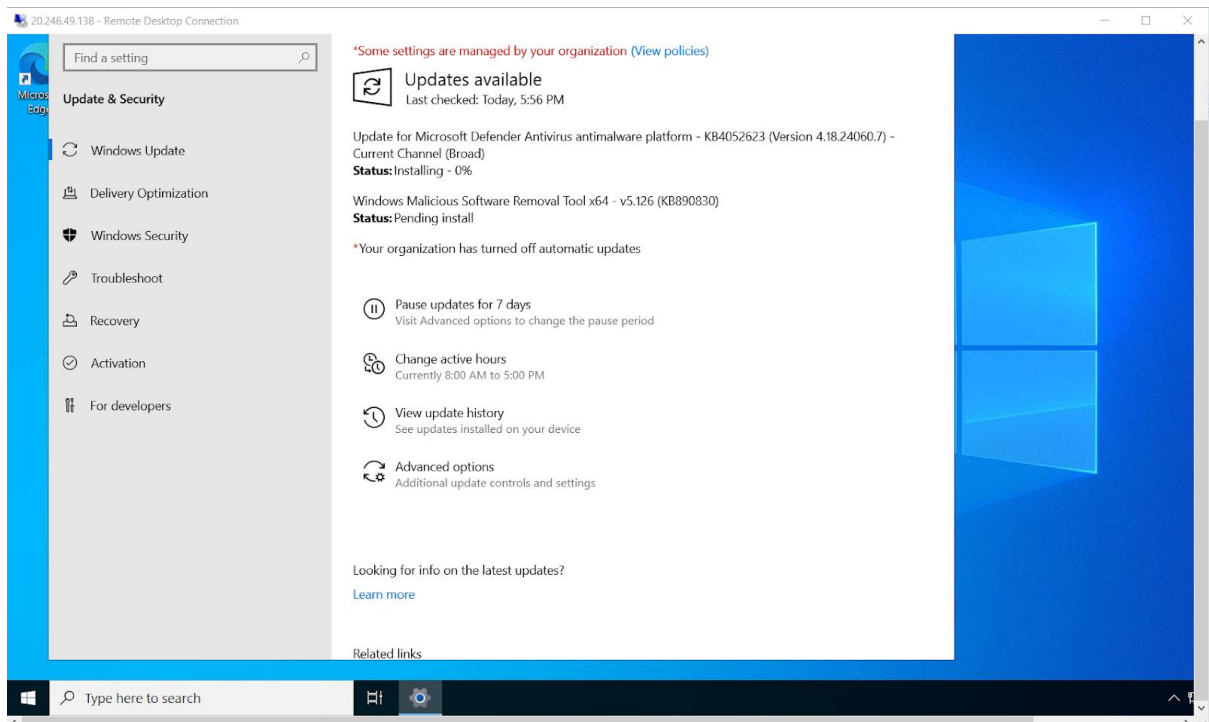
- **Uninstalling Deprecated Software:** Firefox, VLC Media Player, and other outdated applications were removed.
- **System Updates:** Applied all available security patches and updates to the operating system and remaining software.



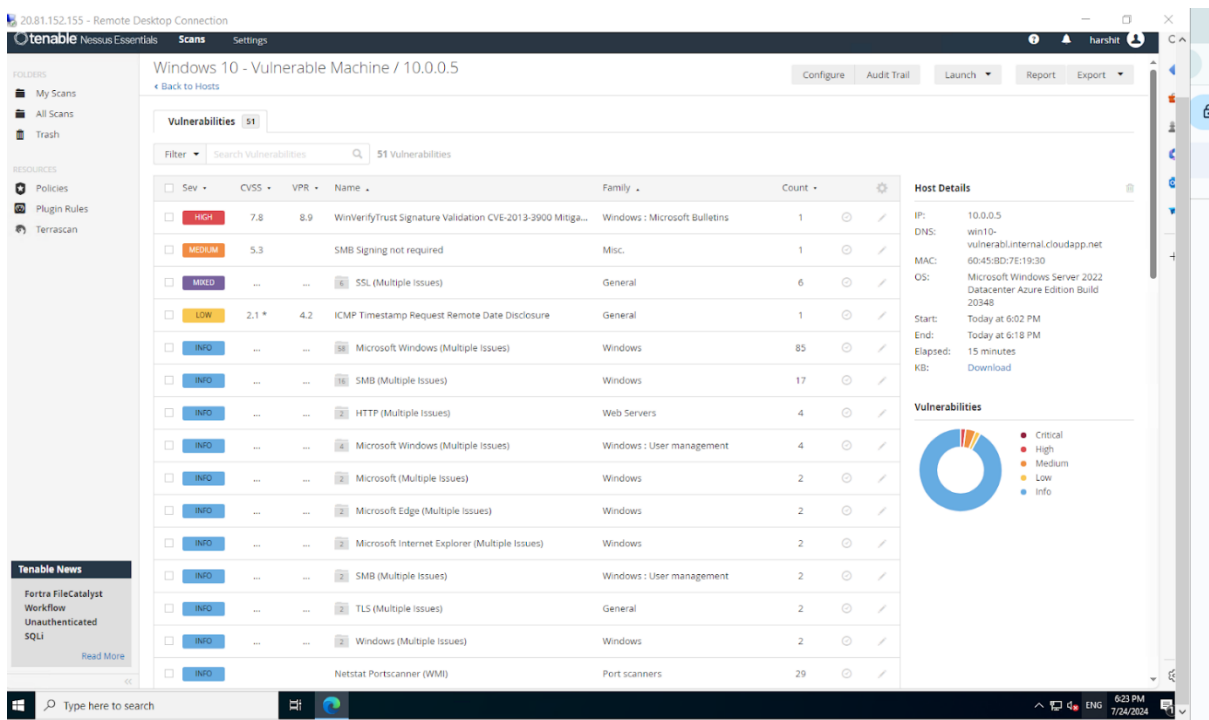
12. Inspect Scan Results After Remediating Some Vulnerabilities

Findings:

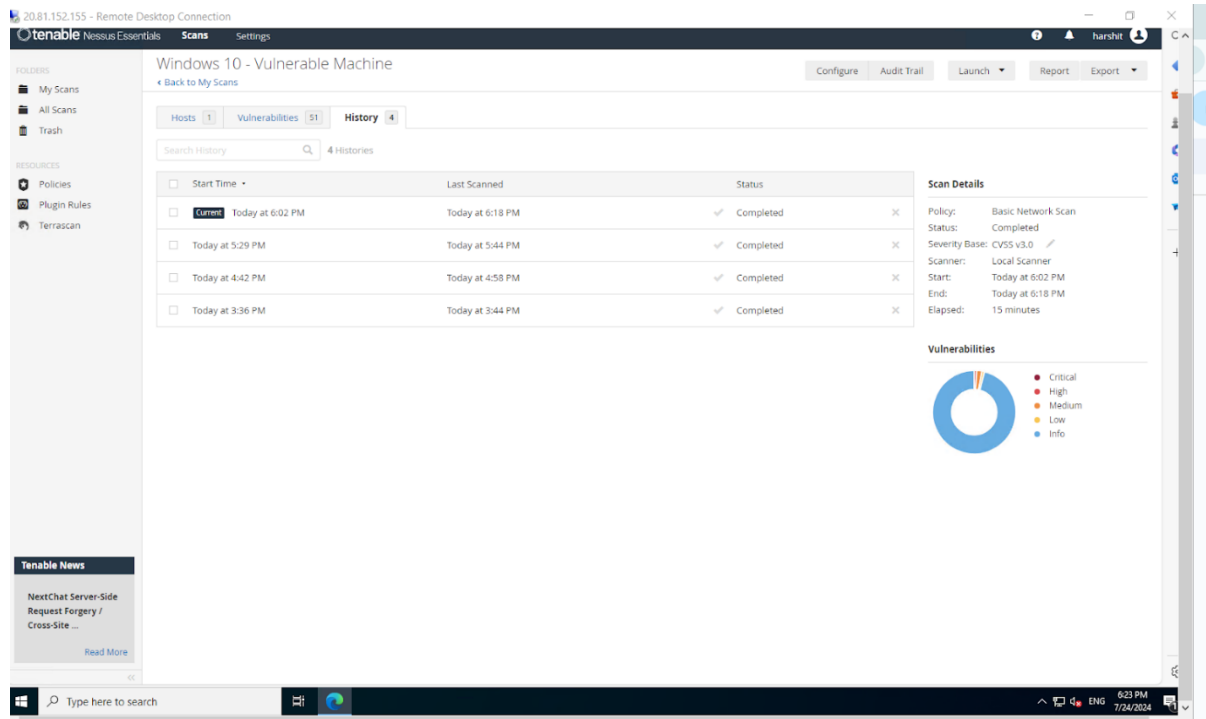
- **Reduction in Critical and High Severity Vulnerabilities:** The number of critical and high vulnerabilities significantly decreased, indicating successful remediation.
- **Total Vulnerabilities Detected: 5**
- **Critical: 0**
- **High: 1**
- **Medium: 3**
- **Low: 1**
- **Info: 202**



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.