Vulnerability Management with OpenVAS

Executive Summary

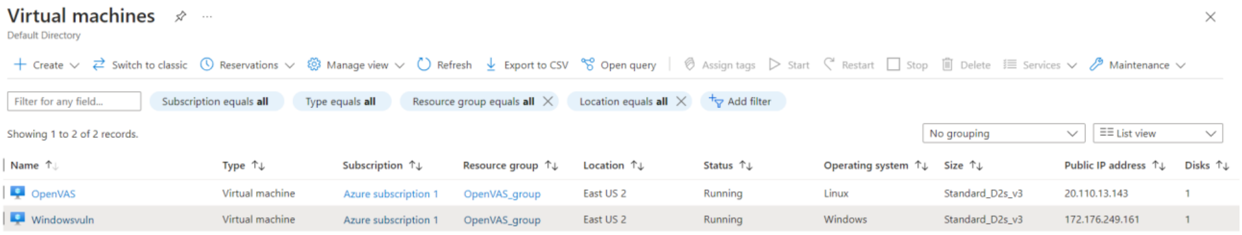
The objective of this project was to demonstrate the importance of patching regularly. In this project, a secure Azure network was established with an OpenVAS Vulnerability Management Scanner virtual machine (VM). I orchestrated a vulnerable Windows 10 VM, intentionally configured with outdated software and disabled security controls. Unauthenticated and credentialed vulnerability scans were conducted using OpenVAS, and the scan results were analyzed to highlight differences between the two approaches. Identified vulnerabilities were promptly remediated and verified through subsequent scans.

Requirements

- Azure account
- Windows 10 VM
- OpenVAS VM

Procedure

I configured both Windows 10 and OpenVAS VM on Azure cloud as shown in screenshot 1.



Subscription equals **all** | Type equals **all** | Resource group equals **all** | Location equals **all**

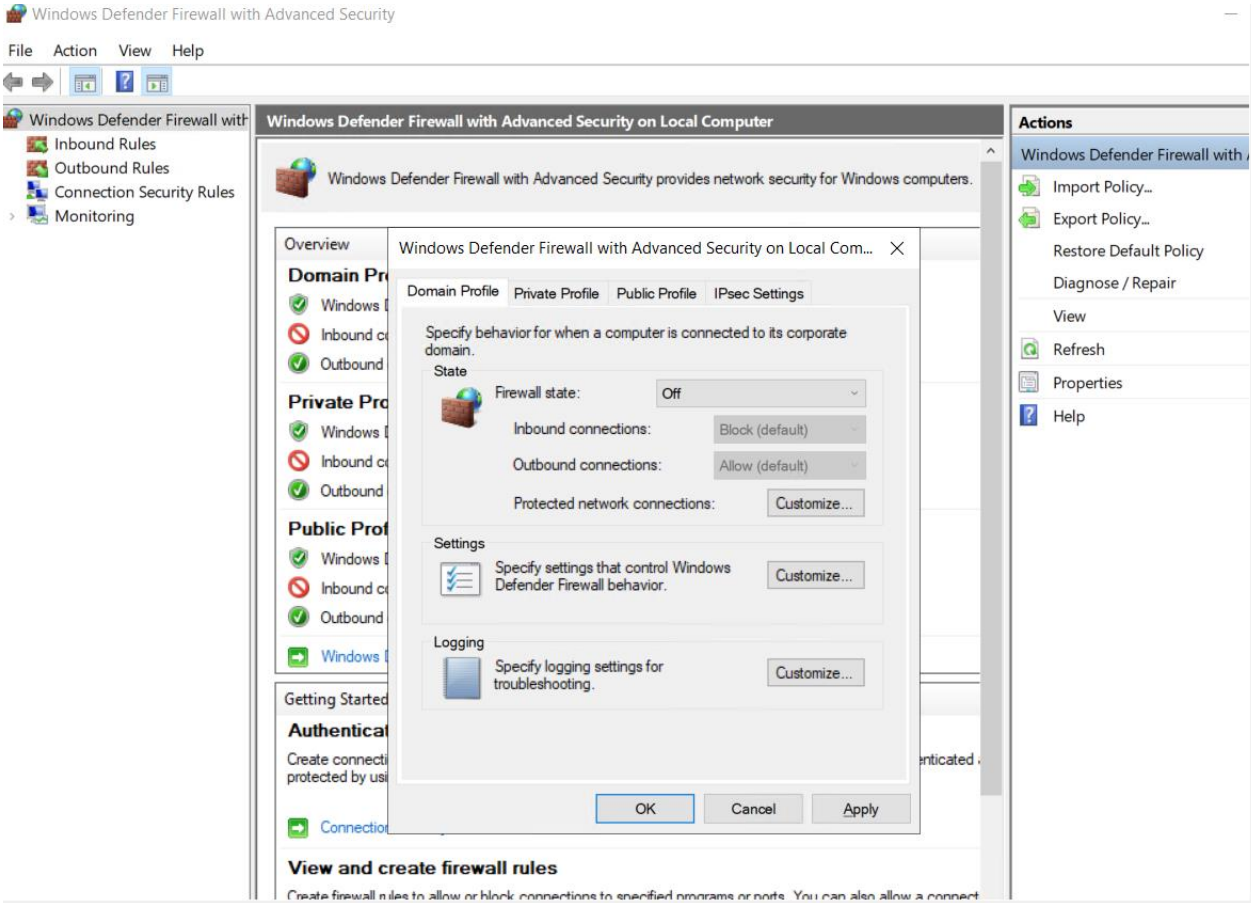
Showing 1 to 2 of 2 records.

No grouping

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
OpenVAS	Virtual machine	Azure subscription 1	OpenVAS_group	East US 2	Running	Linux	Standard_D2s_v3	20.110.13.143	1
Windowsvuln	Virtual machine	Azure subscription 1	OpenVAS_group	East US 2	Running	Windows	Standard_D2s_v3	172.176.249.161	1

Screenshot 1: Completed configuration of OpenVAS and Windowsvuln VMs

After that I made an SSH connection from a Linux machine to OpenVAS VM which returned the website link for web interface of OpenVAS machine. After that I connected to windows VM with the help of remote desktop connection from my local machine. This was connected to an Azure VM. After I logged into windows, I turned off all the firewalls as shown in screenshot 2.



Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Specify settings that control Windows Defender Firewall behavior.

Specify logging settings for troubleshooting.

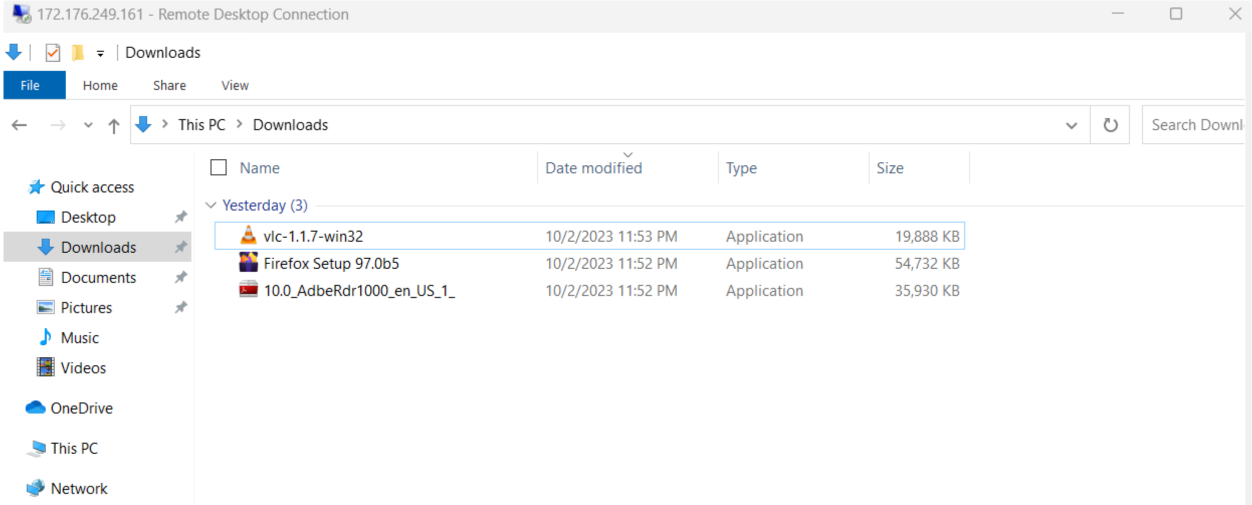
Create connecti… protected by usi… …nticated …

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connect

Screenshot 2: Firewalls removed in windowsvuln

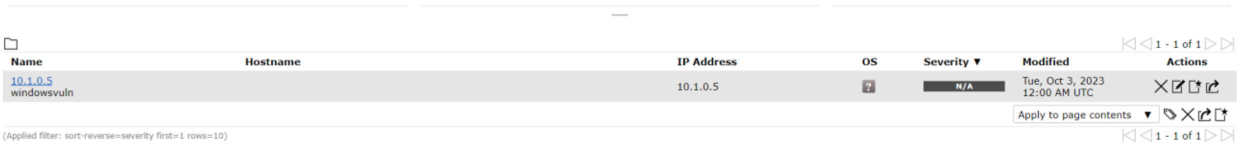
In the next step, I downloaded some old versions of VLC, Firefox, and Adobe software as shown in the screenshot 3 and installed all of them.


172.176.249.161 - Remote Desktop Connection

Name	Date modified	Type	Size
vlc-1.1.7-win32	10/2/2023 11:53 PM	Application	19,888 KB
Firefox Setup 97.0b5	10/2/2023 11:52 PM	Application	54,732 KB
10.0_AdbeRdr1000_en_US_1_	10/2/2023 11:52 PM	Application	35,930 KB

Screenshot 3: Completed configuration of OpenVAS and Windowsvuln VMs

In the next step, I have created a new target and added windows vuln private IP as shown below.

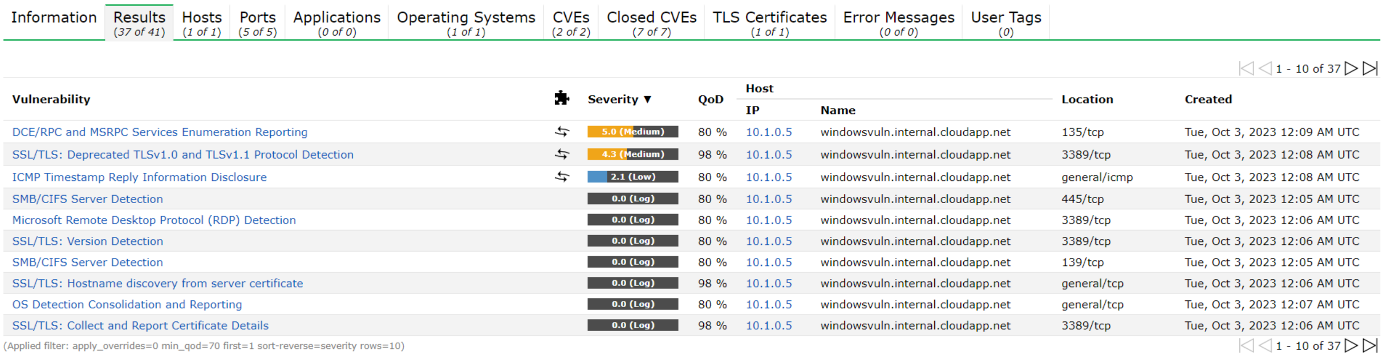


Name	Hostname	IP Address	OS	Severity ▼	Modified	Actions
10.1.0.5 windowsvuln		10.1.0.5	?	N/A	Tue, Oct 3, 2023 12:00 AM UTC	

(Applied filter: sort-reverse=severity first=1 rows=10)

Screenshot 4: windowsvuln added as target in OpenVAS.

After that, I scheduled a non-credentialed scan and it scanned for about 15 minutes and showed the following report as shown in screenshot 5

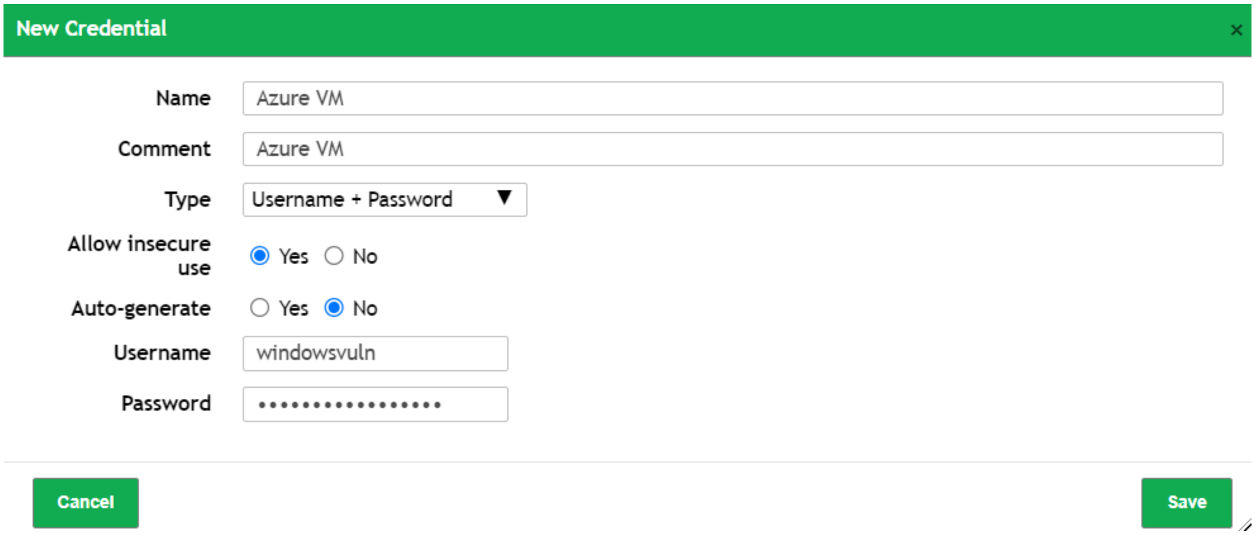


Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	135/tcp	Tue, Oct 3, 2023 12:09 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	10.1.0.5	windowsvuln.internal.cloudapp.net	3389/tcp	Tue, Oct 3, 2023 12:08 AM UTC
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/icmp	Tue, Oct 3, 2023 12:08 AM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	445/tcp	Tue, Oct 3, 2023 12:05 AM UTC
Microsoft Remote Desktop Protocol (RDP) Detection		0.0 (Log)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	3389/tcp	Tue, Oct 3, 2023 12:06 AM UTC
SSL/TLS: Version Detection		0.0 (Log)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	3389/tcp	Tue, Oct 3, 2023 12:06 AM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	139/tcp	Tue, Oct 3, 2023 12:05 AM UTC
SSL/TLS: Hostname discovery from server certificate		0.0 (Log)	98 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 12:06 AM UTC
OS Detection Consolidation and Reporting		0.0 (Log)	80 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 12:07 AM UTC
SSL/TLS: Collect and Report Certificate Details		0.0 (Log)	98 %	10.1.0.5	windowsvuln.internal.cloudapp.net	3389/tcp	Tue, Oct 3, 2023 12:06 AM UTC

(Applied filter: apply_overrides=0 min_qod=70 first=1 sort-reverse=severity rows=10)

Screenshot 5: Non-credentialed scan of windowsvuln

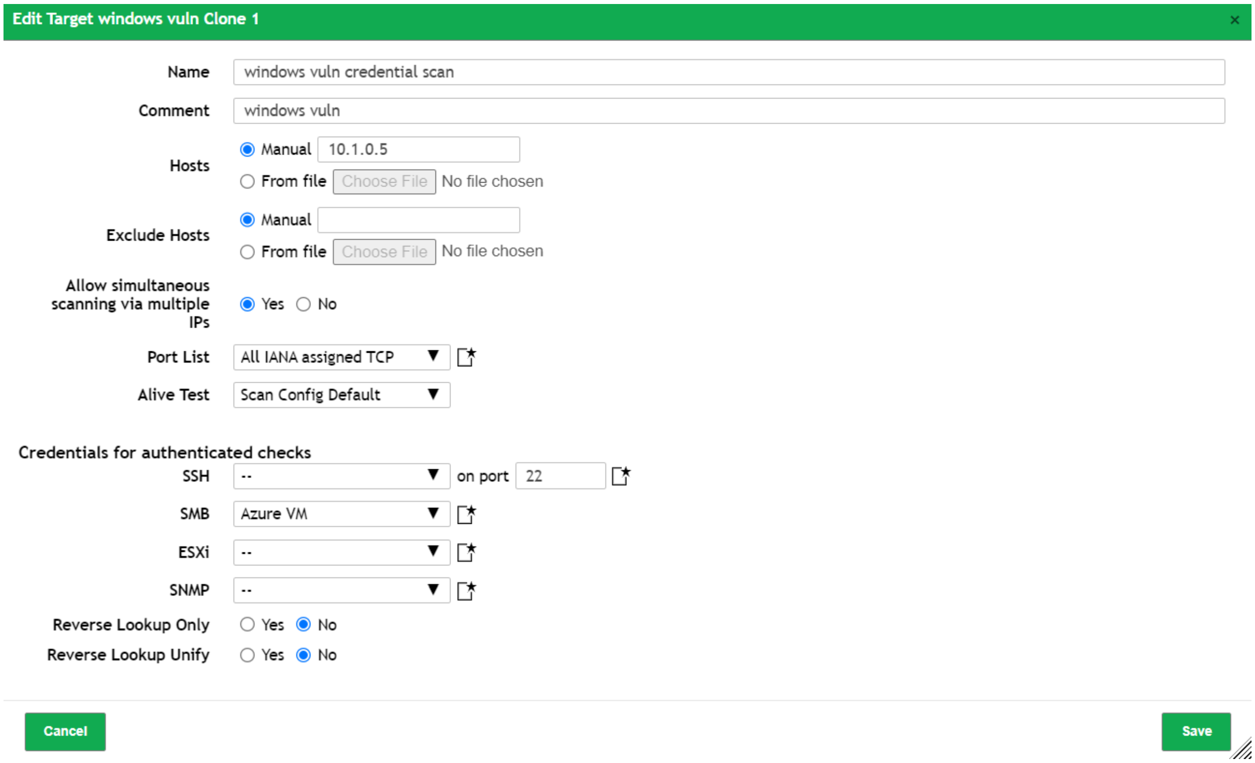
The report of the non-credentialed scan showed the details of the vulnerabilities including severity, CVE, OS of the host. The next step was to make configuration changes to perform a credentialed scan on windows 10 vulnerable machine. For that, I have disabled user account control, enabled remote registry and added the LocalAccountTokenFilterPolicy in SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System key and set it to 1.That completed configuration of windowsvuln VM. After that I configured the OpenVAS for performing credential scan. For that, I selected the credentials tab and entered the details as shown in the screenshot 6.



Name	Azure VM
Comment	Azure VM
Type	Username + Password ▼
Allow insecure use	● Yes ○ No
Auto-generate	○ Yes ● No
Username	windowsvuln
Password	•••••••••••••••••

Screenshot 6: Setup for credentialed scan.

After that I cloned the target file and scan file that I configured earlier for the non-credentialed scan, to perform a credentialed scan as shown in the screenshot .7



Edit Target windows vuln Clone 1

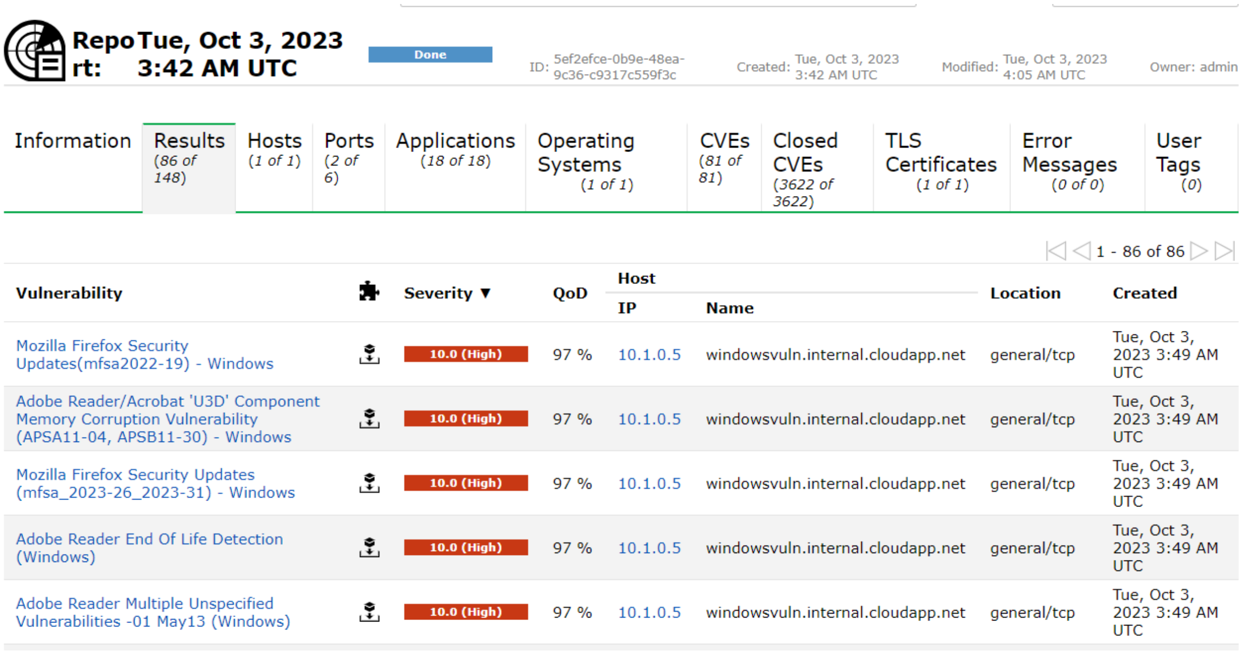
Name	windows vuln credential scan
Comment	windows vuln
Hosts	● Manual 10.1.0.5 ○ From file Choose File No file chosen
Exclude Hosts	● Manual ○ From file Choose File No file chosen
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All IANA assigned TCP
Alive Test	Scan Config Default

Credentials for authenticated checks

SSH	-- on port 22
SMB	Azure VM
ESXi	--
SNMP	--
Reverse Lookup Only	○ Yes ● No
Reverse Lookup Unify	○ Yes ● No

Screenshot 7: target configuration for credentialed vulnerability scan.

It took a while to complete the credentialed scan and the results of the scan were shown in screenshot 8.



Repo Tue, Oct 3, 2023
rt: 3:42 AM UTC

Done

ID: 5ef2efce-0b9e-48ea-9c36-c9317c559f3c Created: Tue, Oct 3, 2023 3:42 AM UTC Modified: Tue, Oct 3, 2023 4:05 AM UTC Owner: admin

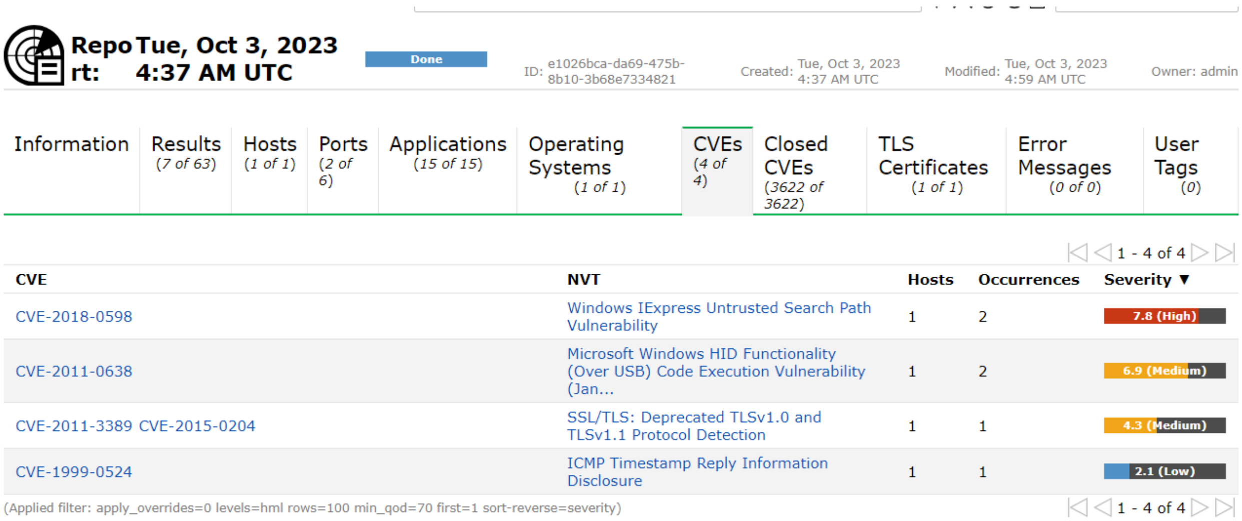
Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(86 of 148)	(1 of 1)	(2 of 6)	(18 of 18)	(1 of 1)	(81 of 81)	(3622 of 3622)	(1 of 1)	(0 of 0)	(0)

1 - 86 of 86

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Mozilla Firefox Security Updates(mfsa2022-19) - Windows		10.0 (High)	97 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 3:49 AM UTC
Adobe Reader/Acrobat 'U3D' Component Memory Corruption Vulnerability (APSA11-04, APSB11-30) - Windows		10.0 (High)	97 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 3:49 AM UTC
Mozilla Firefox Security Updates (mfsa_2023-26_2023-31) - Windows		10.0 (High)	97 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 3:49 AM UTC
Adobe Reader End Of Life Detection (Windows)		10.0 (High)	97 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 3:49 AM UTC
Adobe Reader Multiple Unspecified Vulnerabilities -01 May13 (Windows)		10.0 (High)	97 %	10.1.0.5	windowsvuln.internal.cloudapp.net	general/tcp	Tue, Oct 3, 2023 3:49 AM UTC

Screenshot 8: OpenVAS credentialed scan result for windowsvuln.

OpenVAS completed the credentialed scan and showed a lot more vulnerabilities unlike in the non-credentialed vulnerability scan. Most of the vulnerabilities were because of the outdated sofwares like firefox, Adobe, VLC media player. In the next step to remove the vulnerabilities, I updated all the outdated softwares and did the credentialed scan again with same configurations. The results of the credentialed scan are shown in screenshot 9.



Repo Tue, Oct 3, 2023
rt: 4:37 AM UTC

Done

ID: e1026bca-da69-475b-8b10-3b68e7334821 Created: Tue, Oct 3, 2023 4:37 AM UTC Modified: Tue, Oct 3, 2023 4:59 AM UTC Owner: admin

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(7 of 63)	(1 of 1)	(2 of 6)	(15 of 15)	(1 of 1)	(4 of 4)	(3622 of 3622)	(1 of 1)	(0 of 0)	(0)

1 - 4 of 4

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2018-0598	Windows IExpress Untrusted Search Path Vulnerability	1	2	7.8 (High)
CVE-2011-0638	Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan…	1	2	6.9 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) 1 - 4 of 4

Screenshot 9: OpenVAS credentialed scan results after updating outdated softwares.

As shown in screenshot 9, there were 2 CVEs, 2018-0598, 2011-0638 that were of high severity vulnerabilities left. To mitigate these vulnerabilities I updated the older system and reset the changes and did the credentialed scan again. This reduced the number of vulnerabilities even more.

Conclusion

This concluded the demonstration of how OpenVAS helped in identification of vulnerabilities and mitigating them and also the importance of patching software whenever available. Zero day attacks could come at any time and one of the effective ways is staying up to date with the patches. This could be done with vulnerability management effectively.