Vulnerability Assessment Using Nessus Essentials

(Home-Lab Project)

Author: Prasad Kadu

Date: 04-03-2024

INTRODUCTION

A Vulnerability Assessment (VA) is a systematic process used to detect and evaluate security weakness within a system, network, or application. It involves the identification and classification of potential vulnerabilities that could be exploited by an adversary to compromise the confidentiality, integrity or availability (CIA) of the targeted system. The testing process involves various techniques, both automated and manual, to discover as many vulnerabilities as possible within a specific timeframe. The severity of these vulnerabilities is then assessed and categorized based on their potential impact on the security posture of the system.

VA helps organisations in identifying and addressing potential vulnerabilities in their software application as well as their supporting infrastructure (network). By regularly conducting VA, it helps to minimize the risk of cyber-threats and protect their systems from potential compromise.

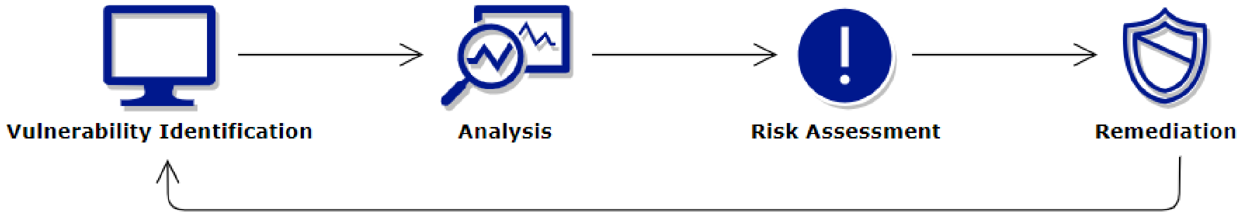
The primary objectives of a VA include:

1. Identifying Vulnerabilities
   The first objective is to systematically identify vulnerabilities within a system, network or applications. These vulnerabilities can range from critical design flaws, which may compromise the security of the entire system, to simple misconfigurations that leave certain aspects of the system vulnerable to exploitation.

2. Documenting Vulnerabilities
   Once the vulnerabilities are identified, they need to be documented in detail which serves as a record of the findings, providing developers and other relevant teams with clear information about the nature and severity of each vulnerability. Furthermore, it helps the developers in the reproduction of findings and to understand how the vulnerabilities were discovered.

3. Create Remediation Guidance
   Subsequently after vulnerabilities are identified and documented, the next step is to develop strategy guidance for remediation. The guidance typically includes recommendations and best practices for addressing each vulnerability for instance, applying software patches, updating software applications, reconfiguring settings, or implementing additional security controls. The goal is to provide developers with actionable steps they can take to fix the vulnerabilities within a timeframe and strengthen the security posture of the system. Remediation guidance can be prioritising recommendations based on the severity and potential impact of each vulnerability to allocate resources effectively to address the most critical issues first.

VULNERABILITY ASSESSMENT PROCESS



(Fig. 1 - Stages of VA Process)

There are four stages (see Fig. 1) involved in VA process including –

1. **Vulnerability Identification (Testing)**

   The first objective is to systematically identify vulnerabilities within a system, network or applications. These vulnerabilities can range from critical design flaws, which may compromise the security of the entire system, to simple misconfigurations that leave certain aspects of the system vulnerable to exploitation.

   This step can be performed through variety of methods including automated tools (e.g. Nessus) to scan the application or system for known vulnerabilities. Additionally, this can be performed manually (using NMAP also known as Network Mapper, where the analyst needs more control and flexibility over scanning process) that automated tools may miss. To support these efforts, analysts use a variety of sources, including vulnerability databases, vendor announcements, asset management systems, and threat intelligence feeds. These resources give useful information about new threats and known vulnerabilities that may affect the system's security posture.

2. **Vulnerability Assessment**

   After identifying vulnerabilities, the next step is to investigate their underlying causes. This involves determining the specific components or sections of the system that are responsible for each vulnerability along with clarifying why they offer a security risk. For instance, a vulnerability could result from using an outdated version of a software library.

   By identifying the root causes of vulnerabilities, effective strategies for remediation can be developed. In the case of the outdated software library, the solution might involve updating the library to a more secure version.

3. **Risk Assessment**

   Once vulnerabilities are identified and analysed, it's essential to prioritize them based on their potential impact on the system's security. This step involves assigning a rank or severity score to each vulnerability (for instance, “CRITICAL”, “HIGH”, “MEDIUM”, “LOW”, “INFORMATIONAL”).

   Factors that can be considered when assessing the risk posed by a vulnerability:

   - Which systems are affected by the vulnerability.

- What sensitive data could be compromised.
- The criticality of the affected business functions.
- How easy it is for an attacker to exploit the vulnerability.
- The severity of potential attacks.
- The extent of damage that could result from exploitation.

By evaluating these factors, security analysts can focus their efforts on addressing the most critical vulnerabilities first, ensuring that resources are allocated effectively to mitigate the greatest risks to the system's security.

4. **Remediation**
   The final step is to take action to fix and mitigate any discovered vulnerabilities. This frequently means collaboration across security, development, and operations teams. Collectively, they develop and implement solutions to close security gaps and lower the system's vulnerability to possible threats.

   Remediation efforts may include implementing new security measures, updating configurations, or developing and deploying patches to address specific vulnerabilities. These measures aim to strengthen the system's defences and reduce the likelihood of successful attacks.

Moreover, along with the four stages it also important to **document** the identified vulnerabilities in detail which serves as a record of the findings, providing developers and other relevant teams with clear information about the nature and severity of each vulnerability. Furthermore, it helps the developers in the reproduction of findings and to understand how the vulnerabilities were discovered.

PROJECT PURPOSE

The primary goal of this project is to conduct a thorough vulnerability assessment using Nessus Essentials tool of a vulnerable Windows 10 OS hosted using VMware to identify potential security weakness and vulnerabilities within the system, including missing updates, misconfigurations, and other exploitable flaws that could be exploited by the malicious attacker to gain unauthorised access or compromise the security of the system.

Furthermore, a detailed report is generated by the Nessus tool of the identified vulnerabilities and further analysed to assess their severity and potential impact on the overall security posture of the hosted vulnerable Windows 10 OS. The generated report serves as a valuable resource to prioritise and address the discovered vulnerabilities.

PROJECT REQUIREMENTS

1. VMware Workstation Player
   It provides a secure and isolated environment for conducting experiments and tests. By installing, it allows users to setup virtual machines to simulate a variety of operating environments while maintaining the security and integrity of the underlying system. The use of VMware ensures that any potential risks or consequences or consequences originating from vulnerability assessment activities are contained within virtual environment.

2. Windows 10 OS
   Setting up a vulnerable Windows 10 OS in VMware allows to simulate a real-world environment and will serve as the target machine where the vulnerabilities are identified and assessed. Additionally, to evaluate the security posture of a Windows-based OS.

3. Nessus Essentials tool
   Installing and configuring Nessus which is an open-source tool on local machine to perform vulnerability assessment is an important component of the project. Nessus is a remote security scanning tool which scans a computer and raises an alert if it discovers any weakness that malicious hackers could use to gain any computer connected to a network. Moreover, Nessus provides patching assistance to mitigate the detected vulnerabilities.

   Note – For the project, I downloaded the trial of Nessus which allows to perform operations up to 16 host.

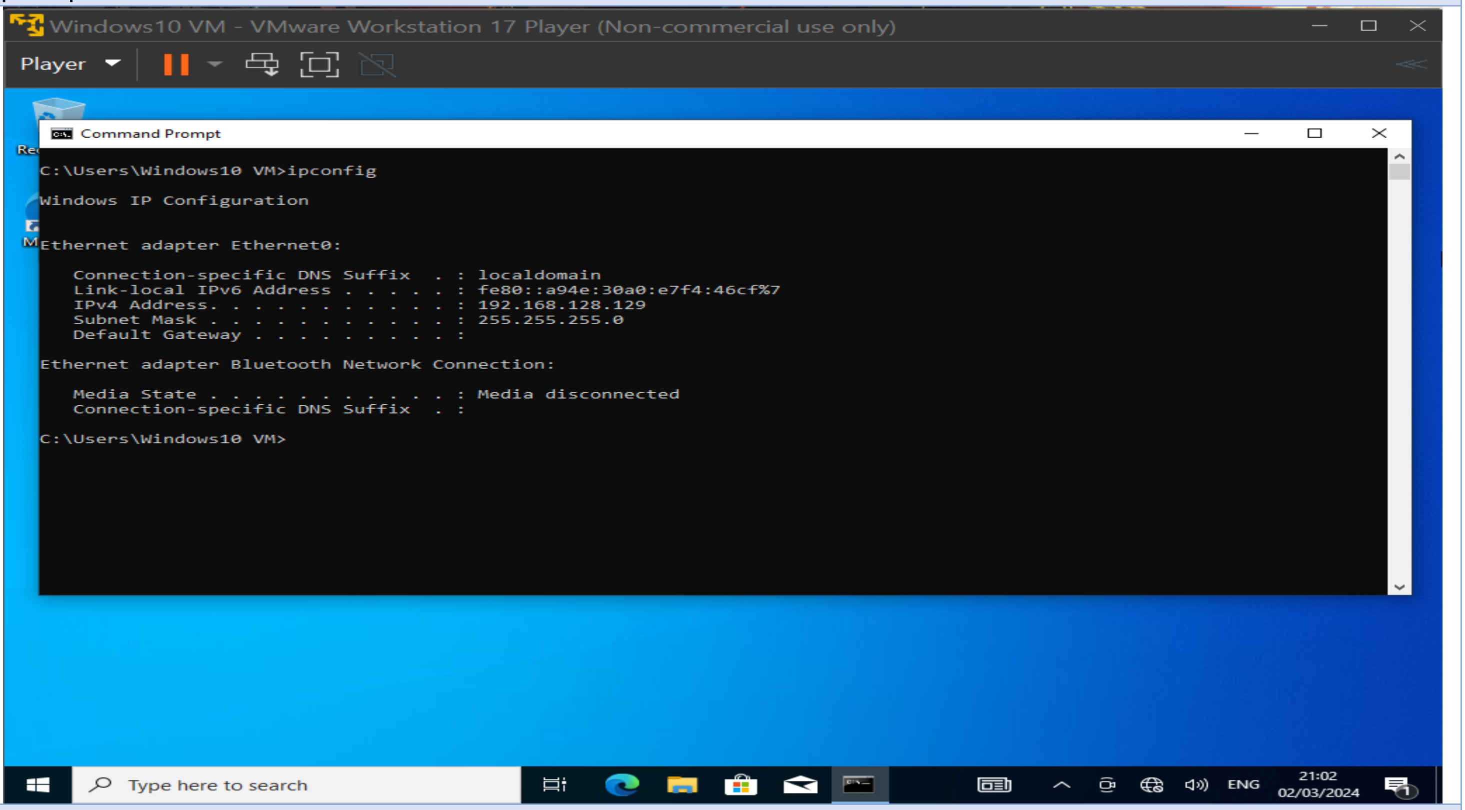
TEST CASES

Following test cases were performed for the project.

A. Checking The Network Connectivity Between Local Machine and Windows 10 VM Using Ping Command

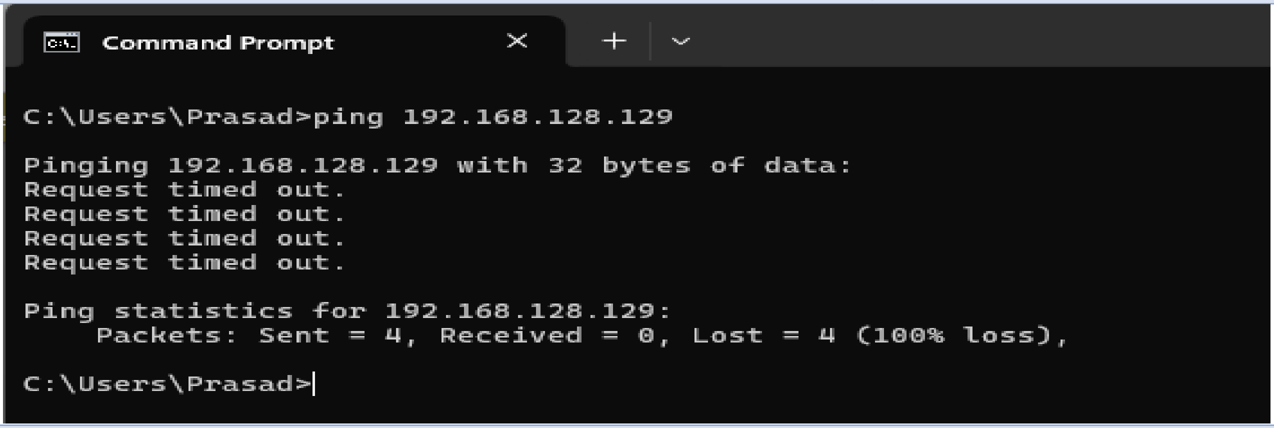
Expected Result (ER)	The ping requests are expected to be successful after the Windows Defender Firewall is disabled, indicating uninterrupted connectivity between the local machine and the Windows VM.

No.	Steps Description
1.	Accessing the IP address of the Windows 10 OS installed on VMware using **ipconfig command** in the command prompt


Windows10 VM - VMware Workstation 17 Player (Non-commercial use only)
Player
Command Prompt
Type here to search
ENG
21:02
02/03/2024

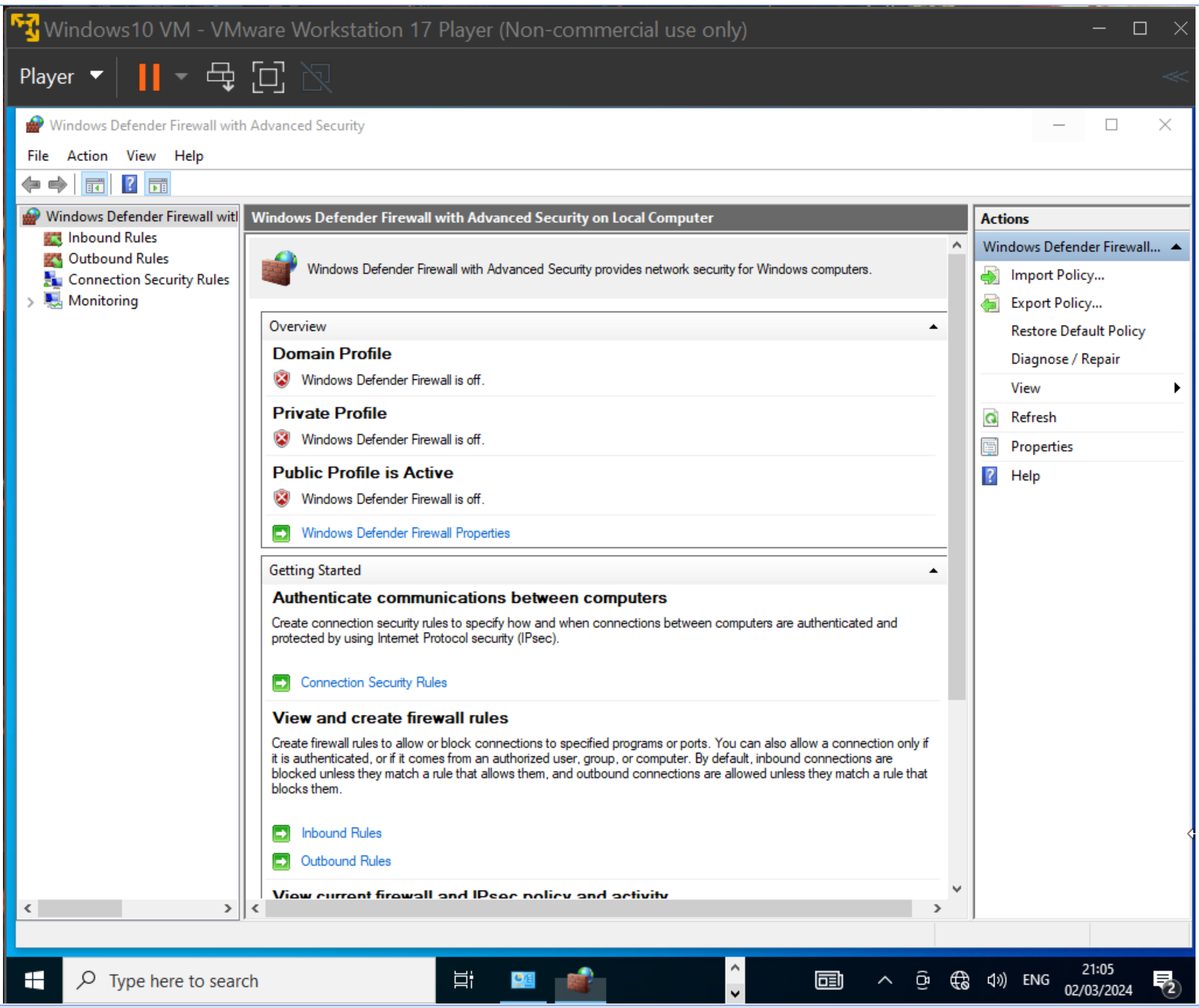
```
C:\Users\Windows10 VM>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a94e:30a0:e7f4:46cf%7
   IPv4 Address. . . . . . . . . . . : 192.168.128.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Windows10 VM>
```

No.	Steps Description
2.	Performing a ping test from the local machine to the Windows VM to verify initial connectivity. (As the Windows Defender Firewall was enabled in the Windows VM, the ping request would initially fail)



```
C:\Users\Prasad>ping 192.168.128.129

Pinging 192.168.128.129 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.128.129:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Prasad>
```

No.	Steps Description
3.	Disabling the Windows Defender Firewall on the Windows VM.



Windows10 VM - VMware Workstation 17 Player (Non-commercial use only)

Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security on Local Computer

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

Overview

Domain Profile

Windows Defender Firewall is off.

Private Profile

Windows Defender Firewall is off.

Public Profile is Active

Windows Defender Firewall is off.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

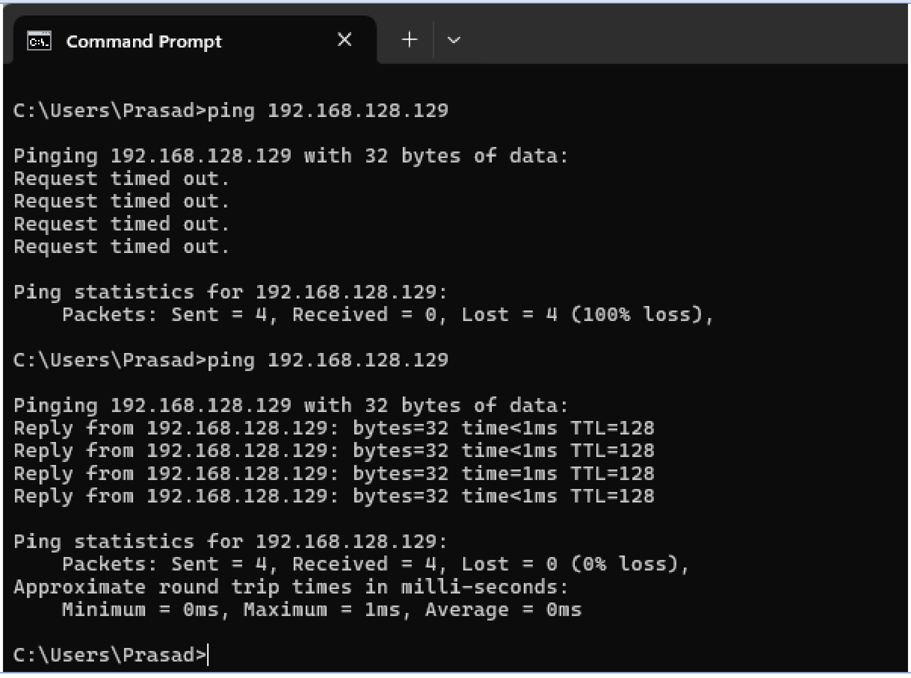
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

4. Repeating the ping test from the local machine to the Windows VM IP Address.
(Now, the ping request are successful which ensure a successful network connectivity)

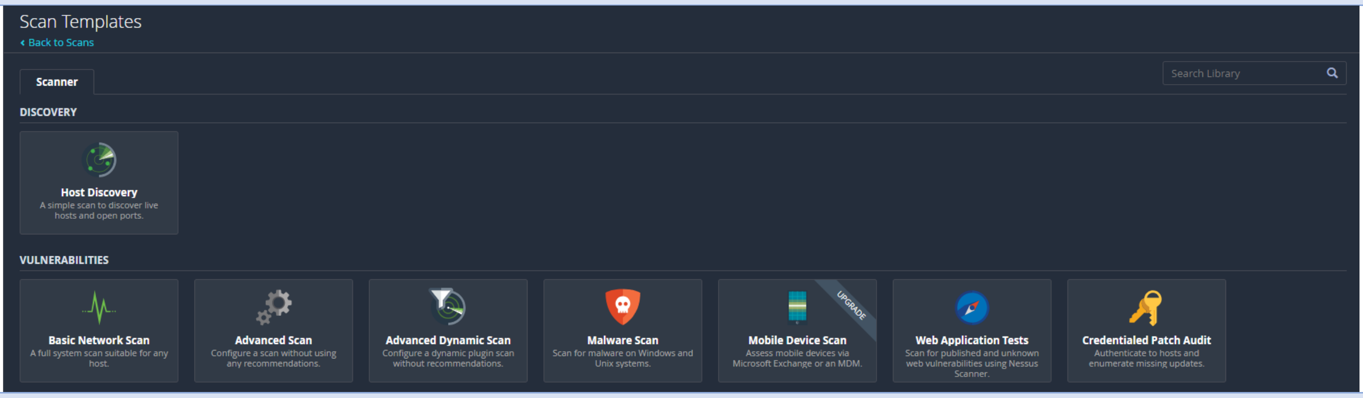
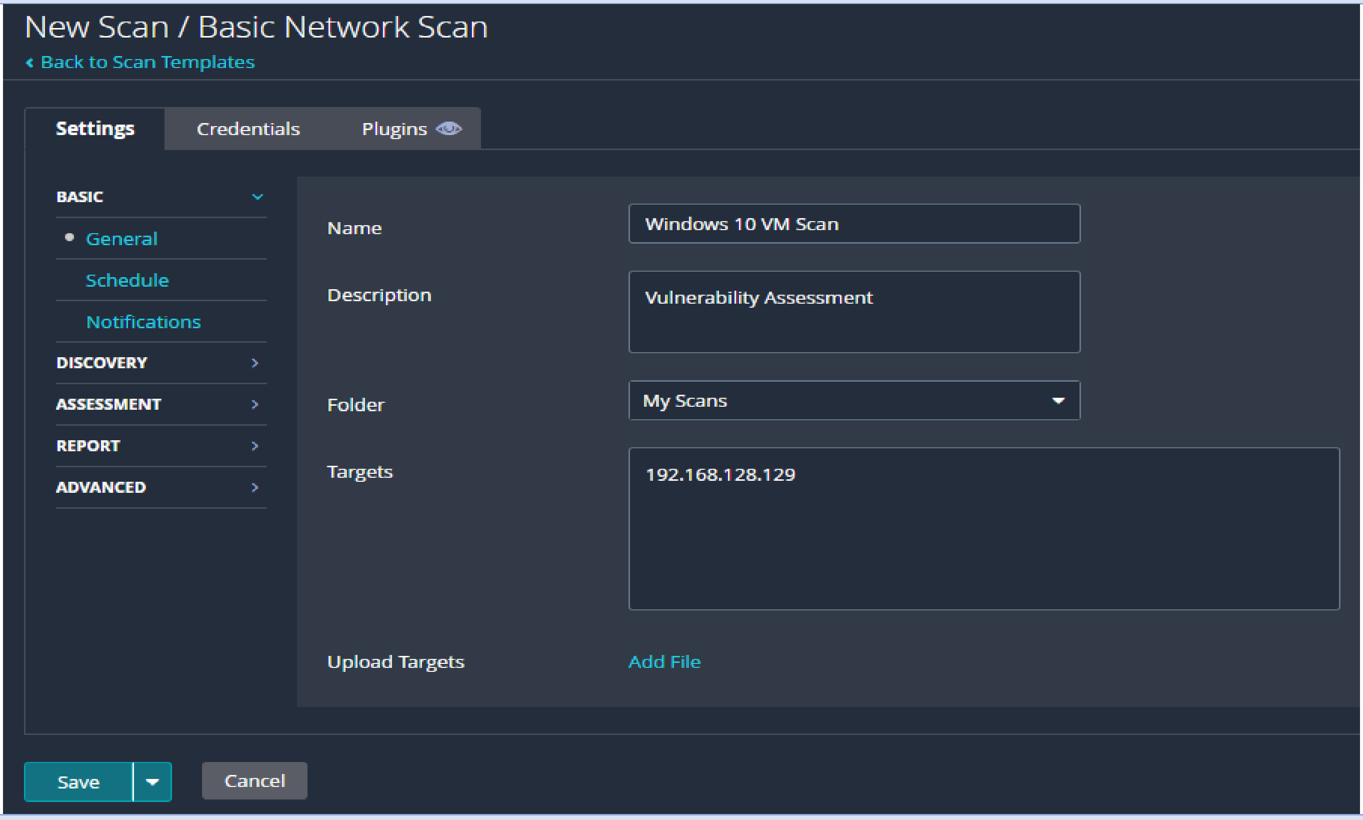


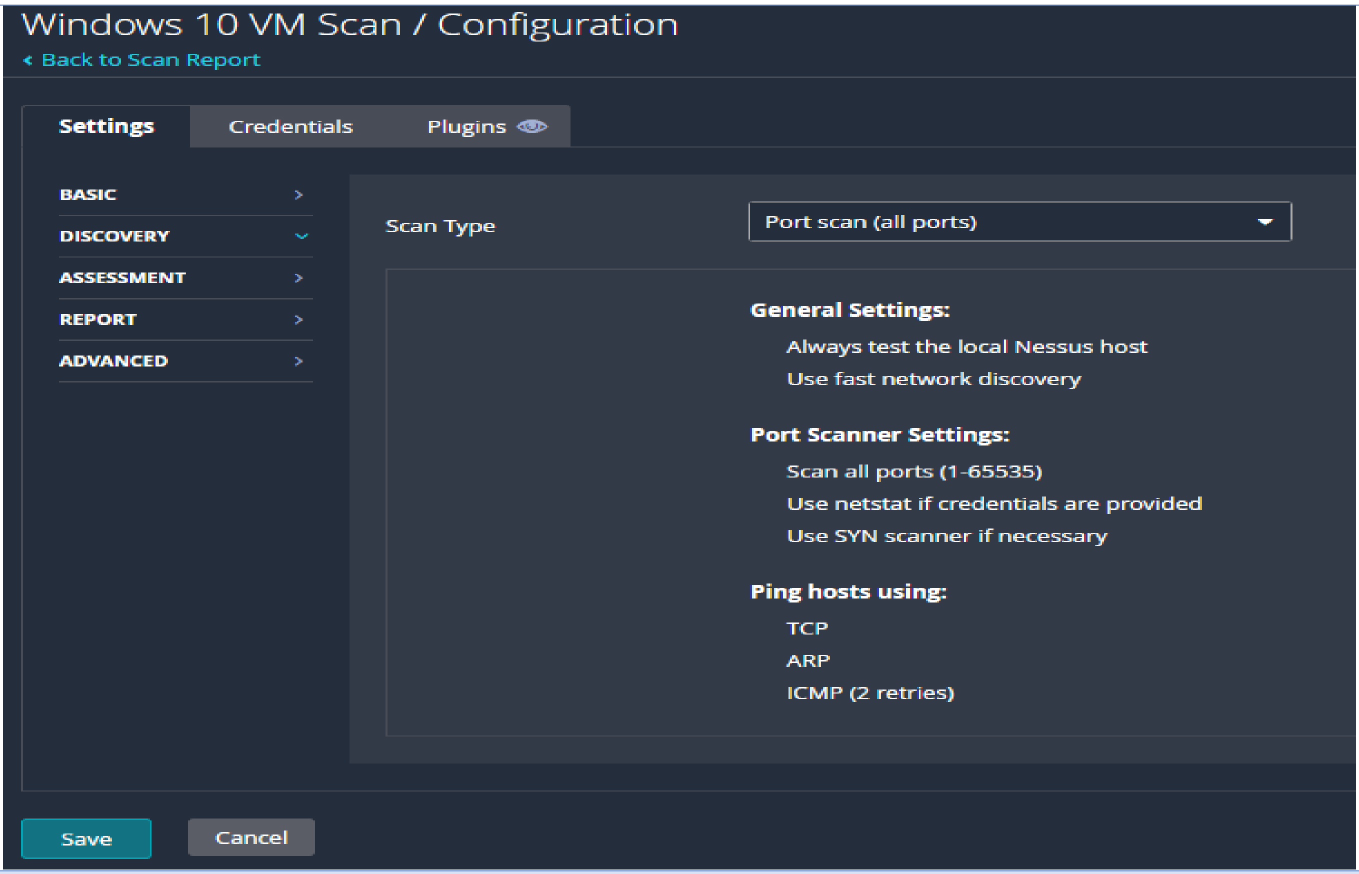
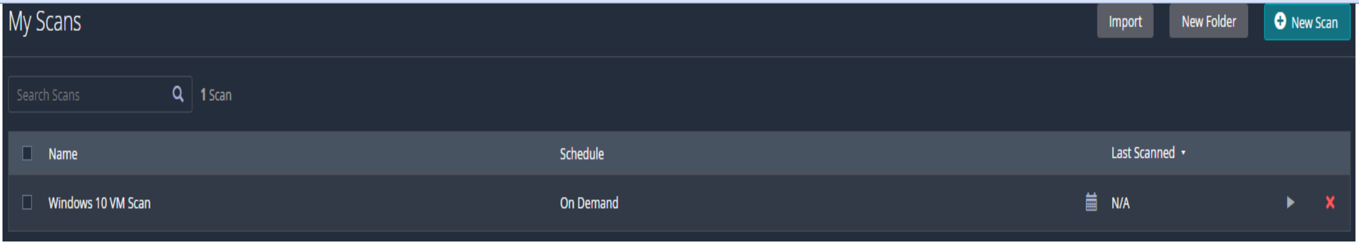
Command Prompt

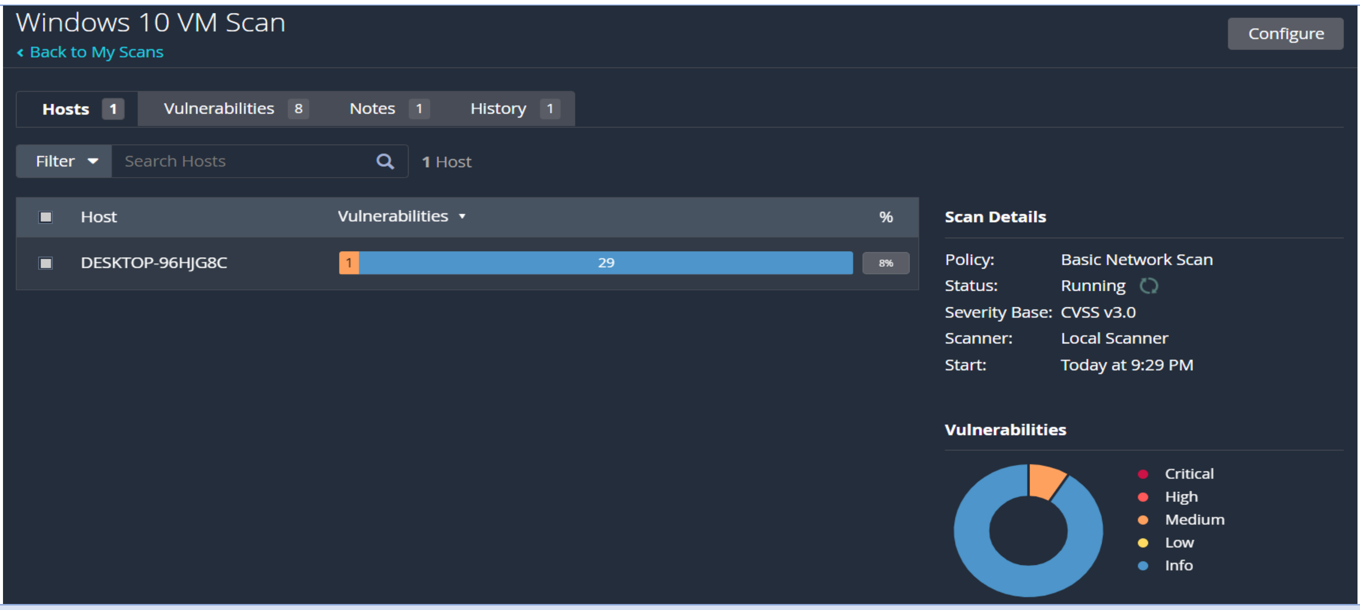
```
C:\Users\Prasad>ping 192.168.128.129

Pinging 192.168.128.129 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.128.129:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Prasad>ping 192.168.128.129

Pinging 192.168.128.129 with 32 bytes of data:
Reply from 192.168.128.129: bytes=32 time<1ms TTL=128
Reply from 192.168.128.129: bytes=32 time<1ms TTL=128
Reply from 192.168.128.129: bytes=32 time=1ms TTL=128
Reply from 192.168.128.129: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.128.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Prasad>
```

B. Accessing and Initiating The Basic Network Scan For The Identified Targeted Host

Expected Result (ER)	The Basic Network Scan is expected to be successful to identify the target machine (i.e. Windows VM) without any errors and complete the assessment by identifying the vulnerabilities and generate results.

No.	Steps Description
1.	Create a New Scan and select the “Basic Network Scan” feature which is a full system scan suitable for the hosted Windows 10 VM
	 Scan Templates ‹ Back to Scans Scanner Search Library DISCOVERY Host Discovery: A simple scan to discover live hosts and open ports. VULNERABILITIES Basic Network Scan: A full system scan suitable for any host. Advanced Scan: Configure a scan without using any recommendations. Advanced Dynamic Scan: Configure a dynamic plugin scan without recommendations. Malware Scan: Scan for malware on Windows and Unix systems. Mobile Device Scan: Assess mobile devices via Microsoft Exchange or an MDM. (UPGRADE) Web Application Tests: Scan for published and unknown web vulnerabilities using Nessus Scanner. Credentialed Patch Audit: Authenticate to hosts and enumerate missing updates.
2.	Enter relevant details, ensuring the IP address (i.e.192.168.128.129) of the targeted Windows 10 VM is specified in the Target field.
	 New Scan / Basic Network Scan ‹ Back to Scan Templates Settings · Credentials · Plugins BASIC: General, Schedule, Notifications DISCOVERY ASSESSMENT REPORT ADVANCED Name: Windows 10 VM Scan Description: Vulnerability Assessment Folder: My Scans Targets: 192.168.128.129 Upload Targets: Add File Save · Cancel
3.	Under Discovery section, select Scan Type as **“Port scan (all ports)”**

	 Windows 10 VM Scan / Configuration ‹ Back to Scan Report Settings · Credentials · Plugins BASIC › DISCOVERY ⌄ ASSESSMENT › REPORT › ADVANCED › Scan Type: Port scan (all ports) **General Settings:** Always test the local Nessus host Use fast network discovery **Port Scanner Settings:** Scan all ports (1-65535) Use netstat if credentials are provided Use SYN scanner if necessary **Ping hosts using:** TCP ARP ICMP (2 retries) Save · Cancel
4.	Now, access My Scan folder to locate the newly configured scan. Initiate the scanning process and wait until the vulnerability assessment is completed by verifying the status as "Completed". (The Basic Network Scan for the targeted Windows 10 VM will be successfully initiated without any errors and the assessment process progresses smoothly to completion by identifying the vulnerabilities of the targeted system)
	 My Scans Import · New Folder · New Scan Search Scans · 1 Scan □ Name · Schedule · Last Scanned □ Windows 10 VM Scan · On Demand · N/A ---



Windows 10 VM Scan

‹ Back to My Scans

Configure

Hosts 1 | Vulnerabilities 8 | Notes 1 | History 1

Filter ▾ | Search Hosts | 1 Host

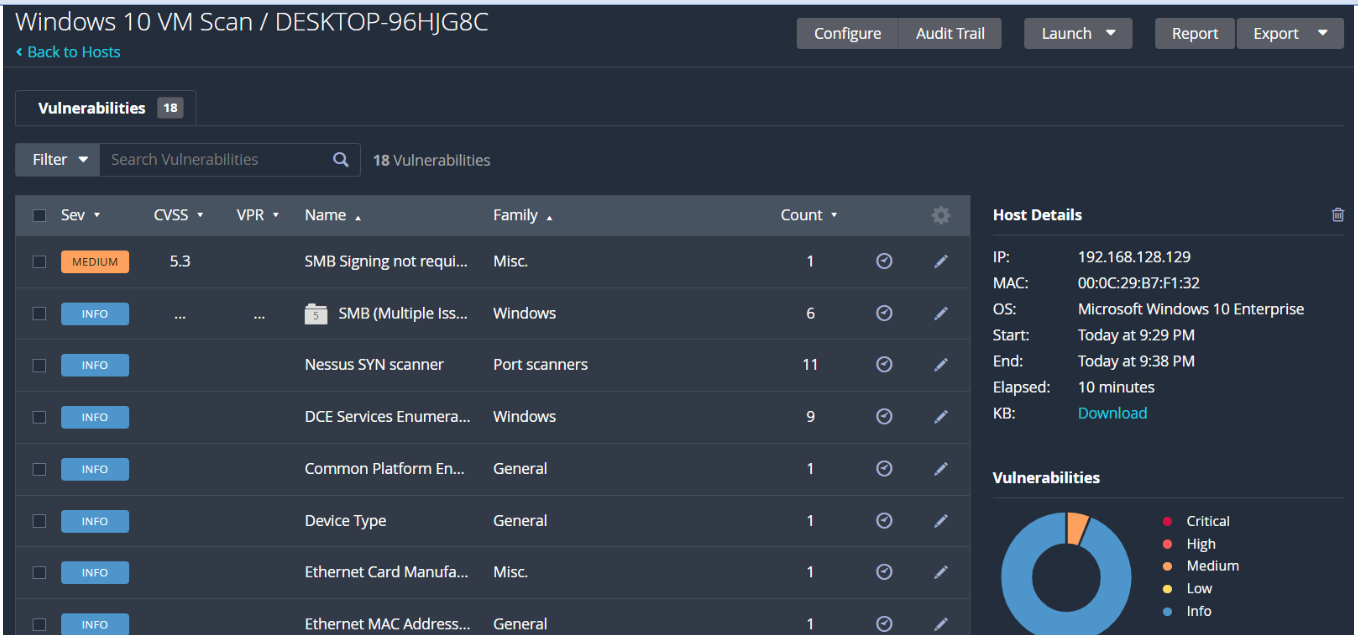
□	Host	Vulnerabilities ▾	%
□	DESKTOP-96HJG8C	1 29	8%

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:29 PM

Vulnerabilities

5. Once the scan is completed successfully (i.e. status changes from “Running” to “Completed”, the total number of vulnerabilities found will be displayed along with their severity levels. Download the Report to analyse the results in detail.



Windows 10 VM Scan / DESKTOP-96HJG8C

‹ Back to Hosts

Configure | Audit Trail | Launch ▾ | Report | Export ▾

Vulnerabilities 18

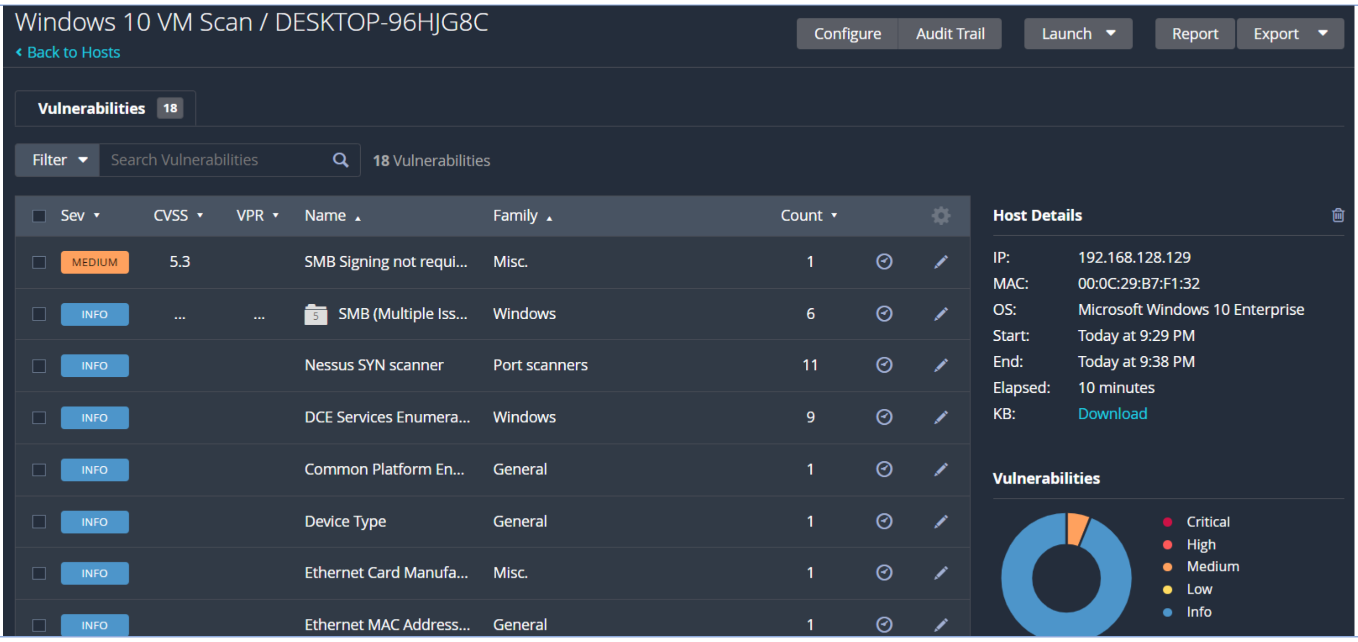
Filter ▾ | Search Vulnerabilities | 18 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
□	MEDIUM	5.3		SMB Signing not requi...	Misc.	1
□	INFO	...	...	5 SMB (Multiple Iss...	Windows	6
□	INFO			Nessus SYN scanner	Port scanners	11
□	INFO			DCE Services Enumera...	Windows	9
□	INFO			Common Platform En...	General	1
□	INFO			Device Type	General	1
□	INFO			Ethernet Card Manufa...	Misc.	1
□	INFO			Ethernet MAC Address...	General	1

Host Details

IP:	192.168.128.129
MAC:	00:0C:29:B7:F1:32
OS:	Microsoft Windows 10 Enterprise
Start:	Today at 9:29 PM
End:	Today at 9:38 PM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities



Windows 10 VM Scan / DESKTOP-96HJG8C

‹ Back to Hosts

Vulnerabilities 18

18 Vulnerabilities

	Sev	CVSS	VPR	Name	Family	Count
□	MEDIUM	5.3		SMB Signing not requi...	Misc.	1
□	INFO	...	...	5 SMB (Multiple Iss...	Windows	6
□	INFO			Nessus SYN scanner	Port scanners	11
□	INFO			DCE Services Enumera...	Windows	9
□	INFO			Common Platform En...	General	1
□	INFO			Device Type	General	1
□	INFO			Ethernet Card Manufa...	Misc.	1
□	INFO			Ethernet MAC Address...	General	1

Host Details

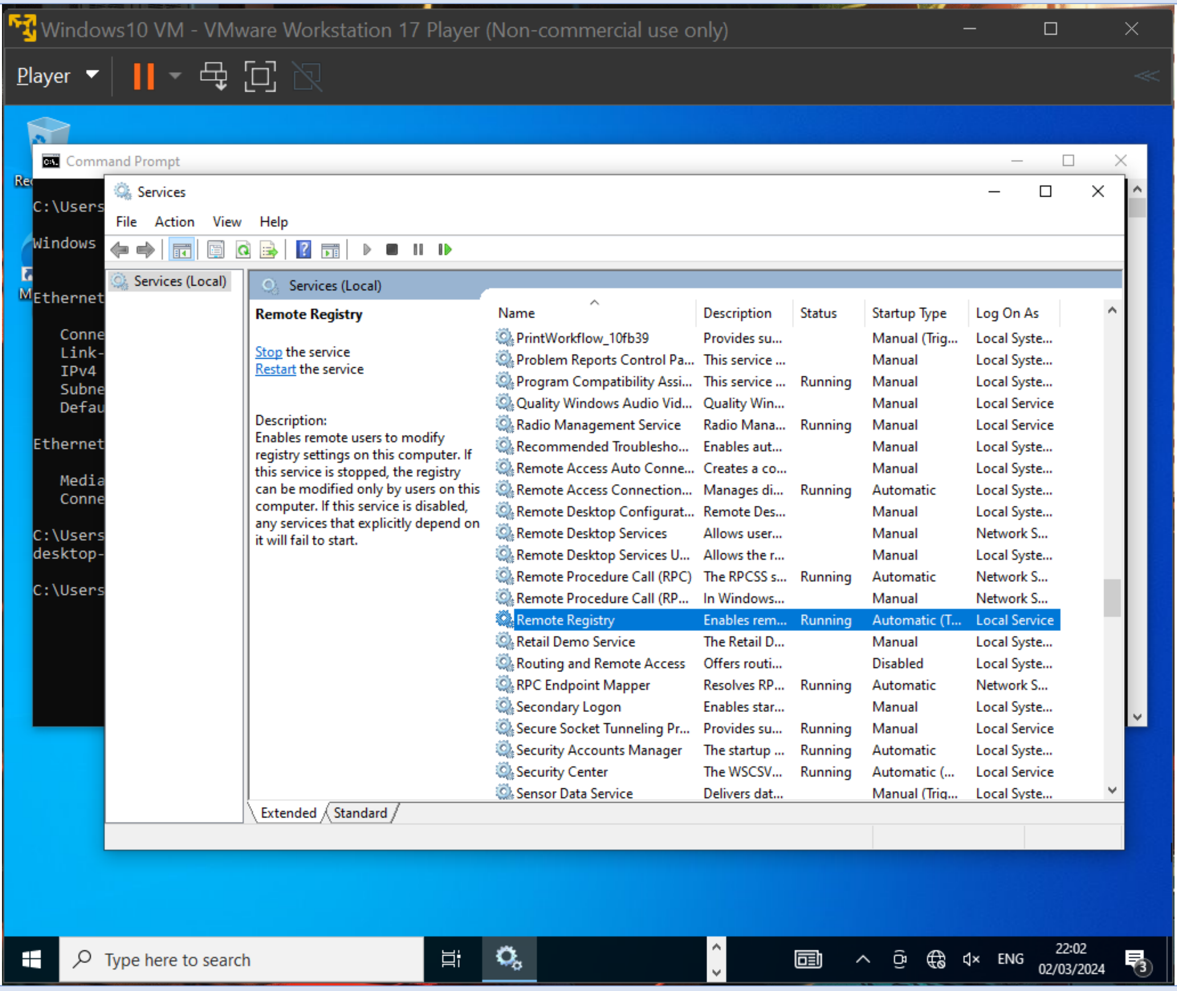
IP:	192.168.128.129
MAC:	00:0C:29:B7:F1:32
OS:	Microsoft Windows 10 Enterprise
Start:	Today at 9:29 PM
End:	Today at 9:38 PM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities

C. Utilising And Configuring Windows Credentials To Perform In-depth VA On Windows 10 VM

Expected Result (ER)	Using the Credentials feature by giving valid username and password of the targeted machine to perform in-depth vulnerability assessment on the Windows 10 VM is successfully conducted by utilising appropriate settings and configuration to enable remote access and authentication.

No.	**Steps Description**
1.	Access the Services configuration of the Windows 10 VM and enable the Remote Registry service to allow remote access. (This will allow the Nessus to perform in-depth scanning to discovery and identify more critical and high vulnerabilities which can be exploited by the attacker)



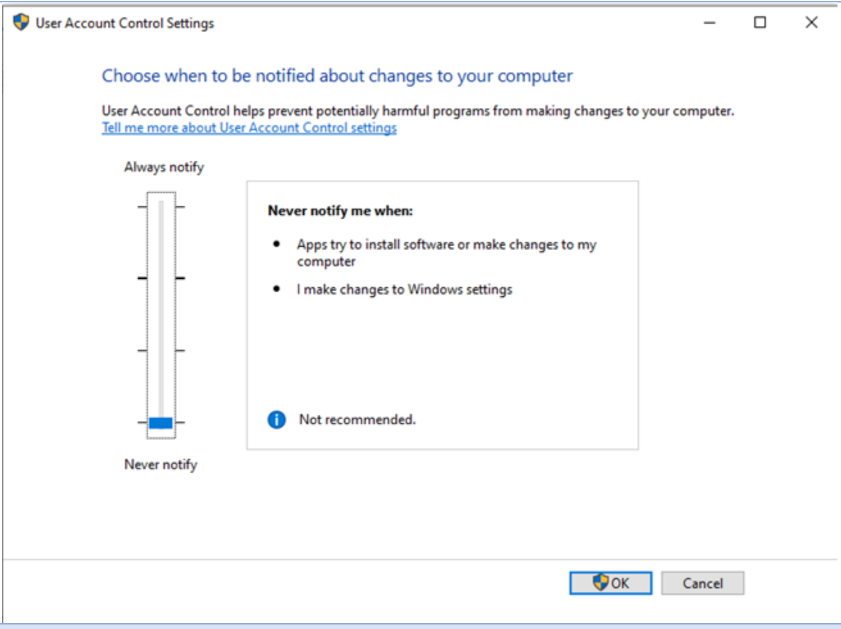
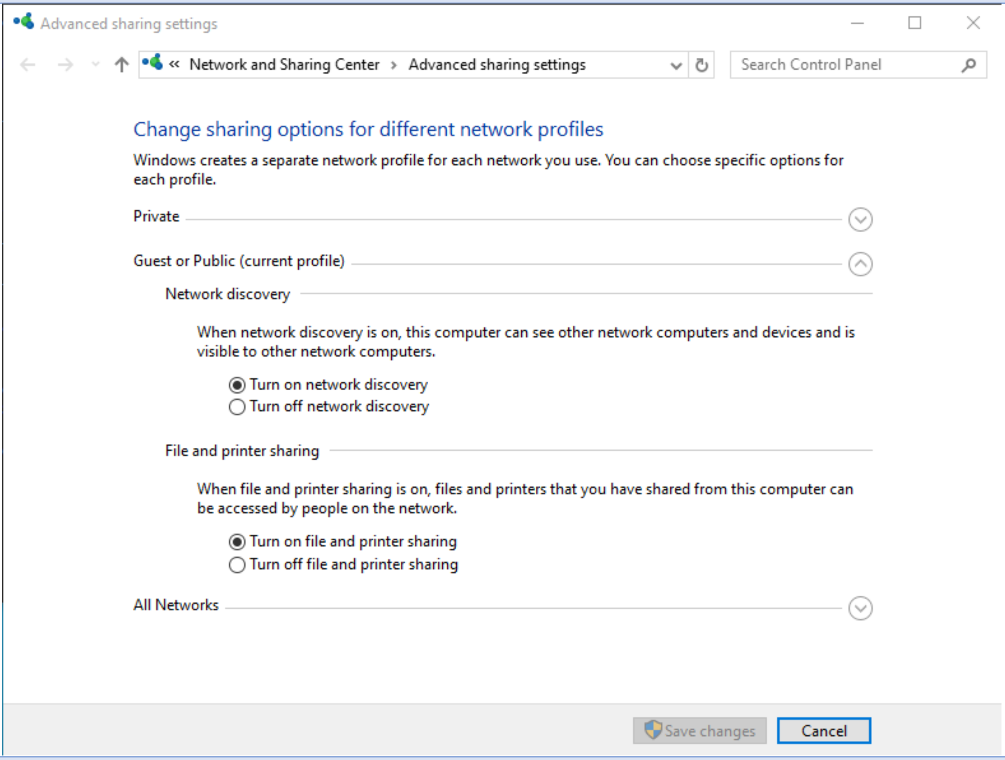
Remote Registry

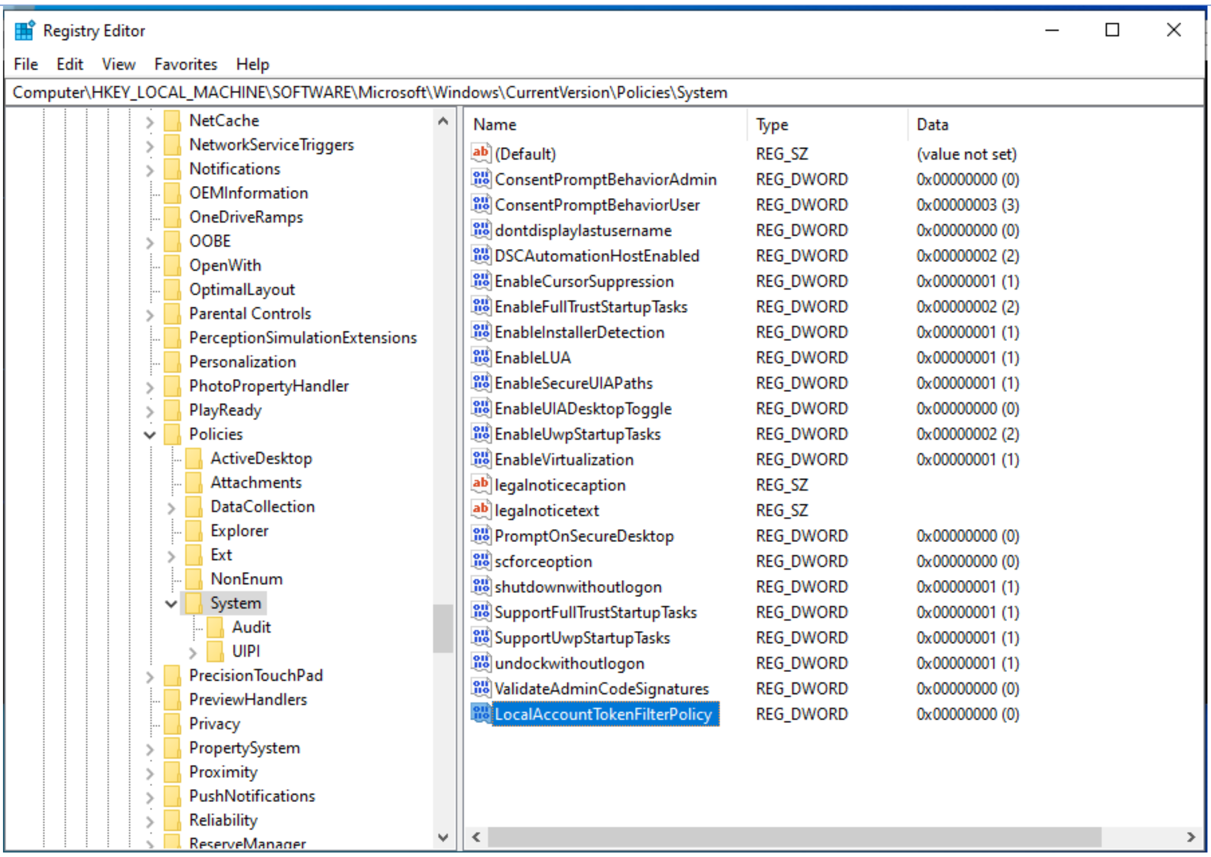
Stop the service
Restart the service

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
PrintWorkflow_10fb39	Provides su...		Manual (Trig...	Local Syste...
Problem Reports Control Pa...	This service ...		Manual	Local Syste...
Program Compatibility Assi...	This service ...	Running	Manual	Local Syste...
Quality Windows Audio Vid...	Quality Win...		Manual	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troublesho...	Enables aut...		Manual	Local Syste...
Remote Access Auto Conne...	Creates a co...		Manual	Local Syste...
Remote Access Connection...	Manages di...	Running	Automatic	Local Syste...
Remote Desktop Configurat...	Remote Des...		Manual	Local Syste...
Remote Desktop Services	Allows user...		Manual	Network S...
Remote Desktop Services U...	Allows the r...		Manual	Local Syste...
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network S...
Remote Procedure Call (RP...	In Windows...		Manual	Network S...
Remote Registry	Enables rem...	Running	Automatic (T...	Local Service
Retail Demo Service	The Retail D...		Manual	Local Syste...
Routing and Remote Access	Offers routi...		Disabled	Local Syste...
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides su...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Security Center	The WSCSV...	Running	Automatic (...	Local Service
Sensor Data Service	Delivers dat...		Manual (Trig...	Local Syste...

2.	Modify the User Account Control to “Never Notify” under User Account Control Settings in Windows 10 VM (This will ensure uninterrupted scanning by preventing the OS from prompting for user consent when the changes are made to the Windows 10 VM)

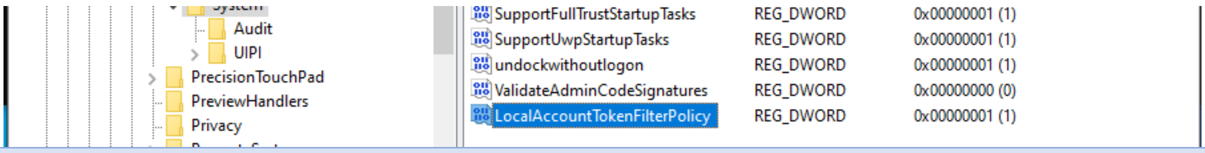
	 User Account Control Settings Choose when to be notified about changes to your computer User Account Control helps prevent potentially harmful programs from making changes to your computer. Tell me more about User Account Control settings Always notify **Never notify me when:** - Apps try to install software or make changes to my computer - I make changes to Windows settings Not recommended. Never notify OK Cancel
3.	Ensure that Network discovery and File and printer sharing are enabled on the Windows 10 VM. (This allows Nessus to interact with the targeted machine remotely)
	 Advanced sharing settings « Network and Sharing Center › Advanced sharing settings Search Control Panel Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private Guest or Public (current profile) Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. ● Turn on network discovery ○ Turn off network discovery File and printer sharing When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network. ● Turn on file and printer sharing ○ Turn off file and printer sharing All Networks Save changes Cancel
4.	Using the Registry Editor, create a new DWORD registry (given the specified path) and assign the value as 1. After successful creation, restart the Windows 10 VM. (Creating a new registry will allow the non-administrator account (Nessus) to perform the scan on the Windows 10 VM)



Registry Editor

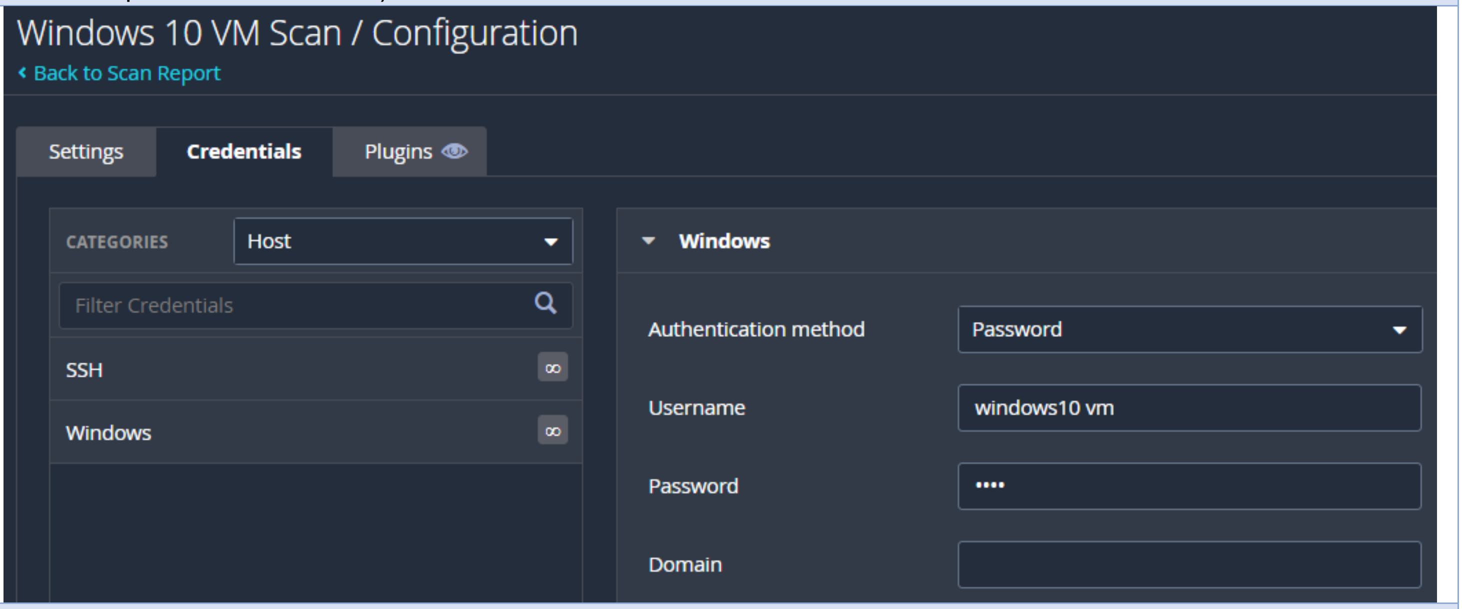
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000000 (0)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
dontdisplaylastusername	REG_DWORD	0x00000000 (0)
DSCAutomationHostEnabled	REG_DWORD	0x00000002 (2)
EnableCursorSuppression	REG_DWORD	0x00000001 (1)
EnableFullTrustStartupTasks	REG_DWORD	0x00000002 (2)
EnableInstallerDetection	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)
EnableUIADesktopToggle	REG_DWORD	0x00000000 (0)
EnableUwpStartupTasks	REG_DWORD	0x00000002 (2)
EnableVirtualization	REG_DWORD	0x00000001 (1)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecureDesktop	REG_DWORD	0x00000000 (0)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
SupportFullTrustStartupTasks	REG_DWORD	0x00000001 (1)
SupportUwpStartupTasks	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000000 (0)



SupportFullTrustStartupTasks	REG_DWORD	0x00000001 (1)
SupportUwpStartupTasks	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000001 (1)

5. Reconfigure the scan settings to include Windows 10 VM credentials (both username and password) under Credentials setting.
(This will allow Nessus to authenticate with the hosted Windows 10 VM during vulnerability assessment enabling access to protected resources)



Windows 10 VM Scan / Configuration

CATEGORIES: Host

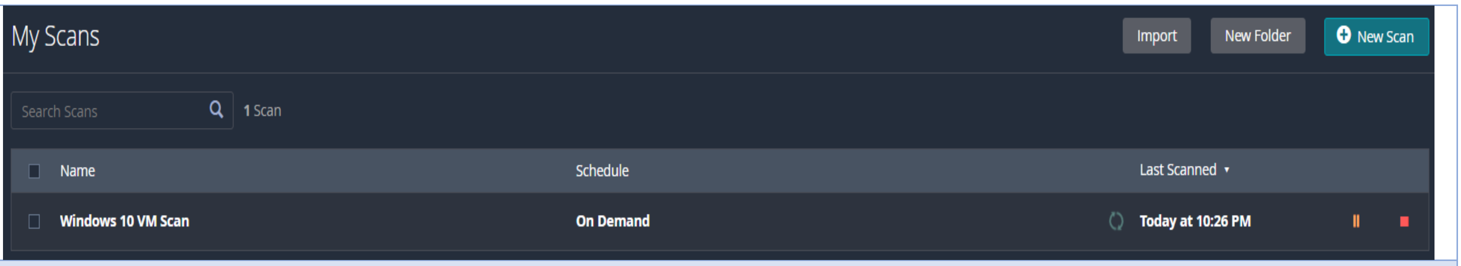
Authentication method: Password

Username: windows10 vm

Password: ••••

Domain:

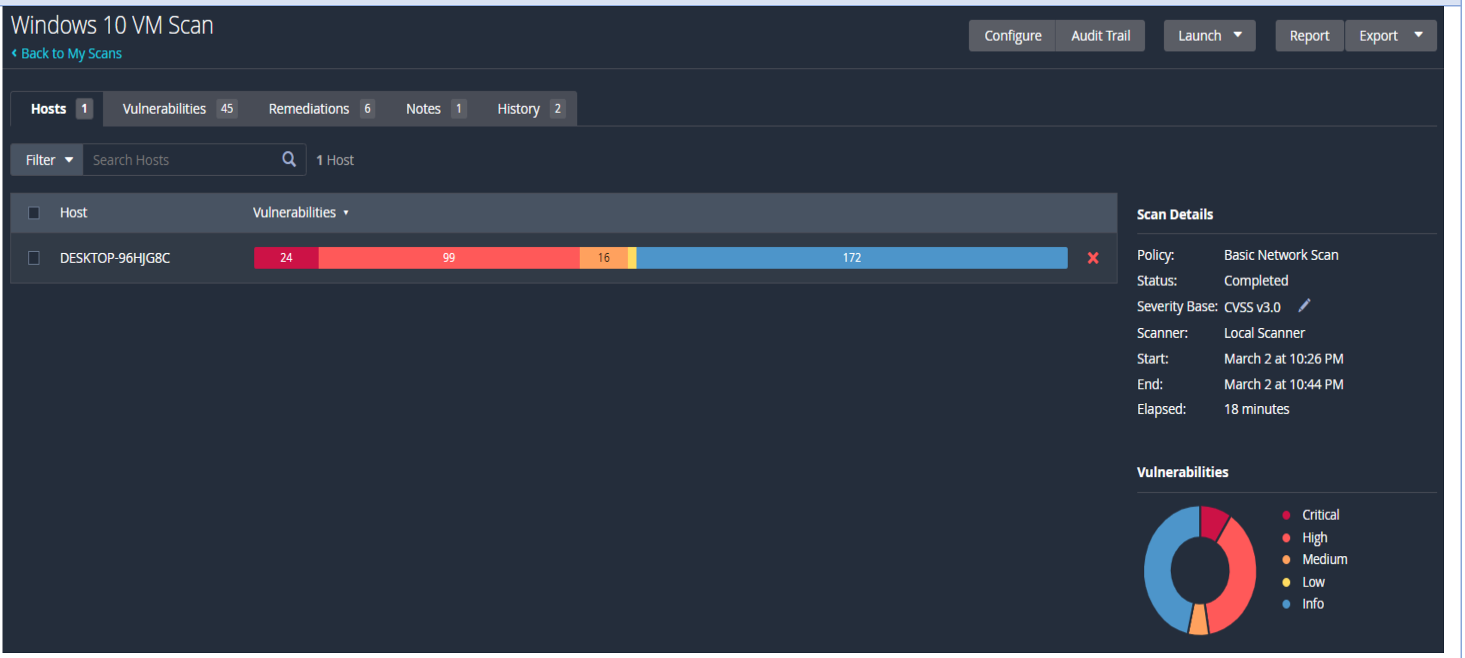
6. Rerun the Vulnerability Scan



1 Scan

Name	Schedule	Last Scanned
Windows 10 VM Scan	On Demand	Today at 10:26 PM

7. Once the scan is completed successfully (i.e. status changes from "Running" to "Completed", the total number of vulnerabilities found will be displayed along with their severity levels. Download the Report to analyse the results in detail.



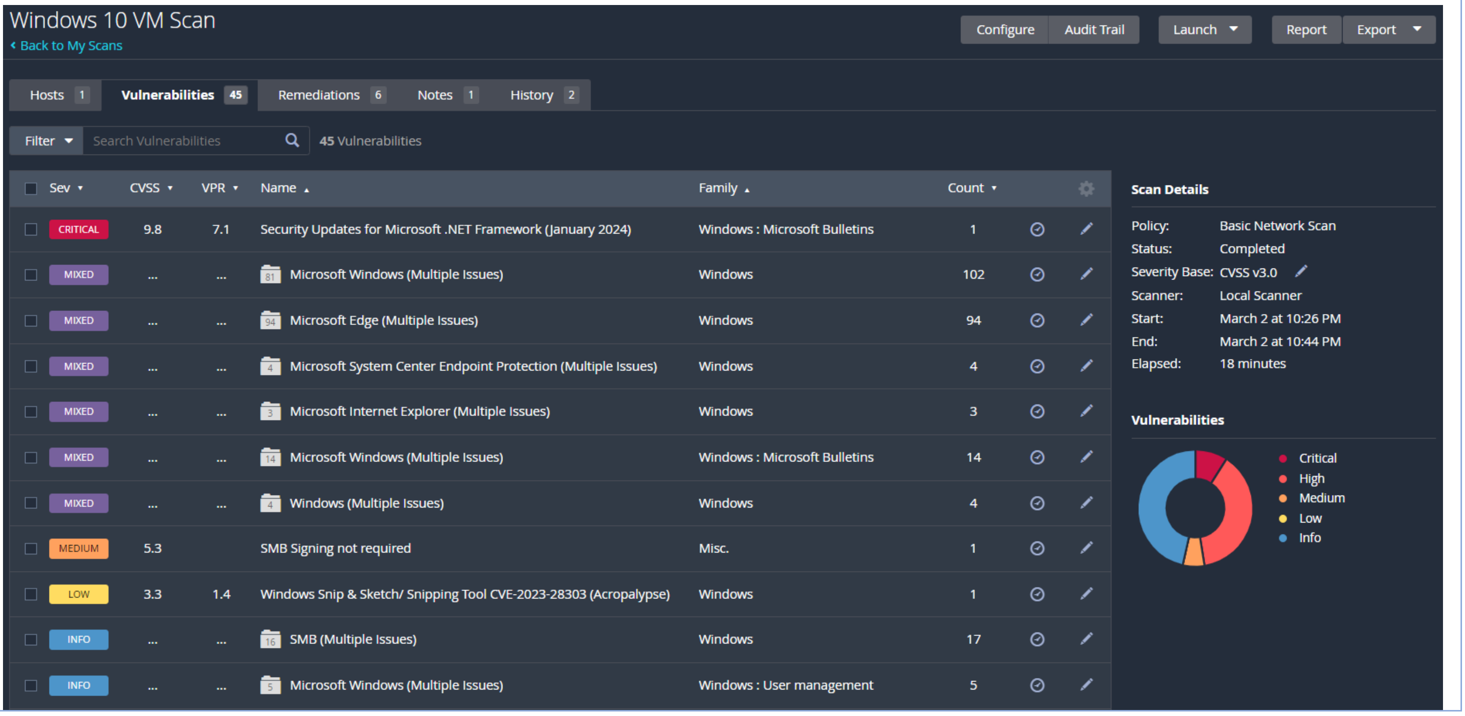
1 Host

Host	Vulnerabilities
DESKTOP-96HJG8C	24 99 16 172

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: March 2 at 10:26 PM
End: March 2 at 10:44 PM
Elapsed: 18 minutes

Vulnerabilities



45 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8	7.1	Security Updates for Microsoft .NET Framework (January 2024)	Windows : Microsoft Bulletins	1
MIXED	...	...	81 Microsoft Windows (Multiple Issues)	Windows	102
MIXED	...	...	94 Microsoft Edge (Multiple Issues)	Windows	94
MIXED	...	...	4 Microsoft System Center Endpoint Protection (Multiple Issues)	Windows	4
MIXED	...	...	3 Microsoft Internet Explorer (Multiple Issues)	Windows	3
MIXED	...	...	14 Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	14
MIXED	...	...	4 Windows (Multiple Issues)	Windows	4
MEDIUM	5.3		SMB Signing not required	Misc.	1
LOW	3.3	1.4	Windows Snip & Sketch/ Snipping Tool CVE-2023-28303 (Acropalypse)	Windows	1
INFO	...	...	16 SMB (Multiple Issues)	Windows	17
INFO	...	...	5 Microsoft Windows (Multiple Issues)	Windows : User management	5

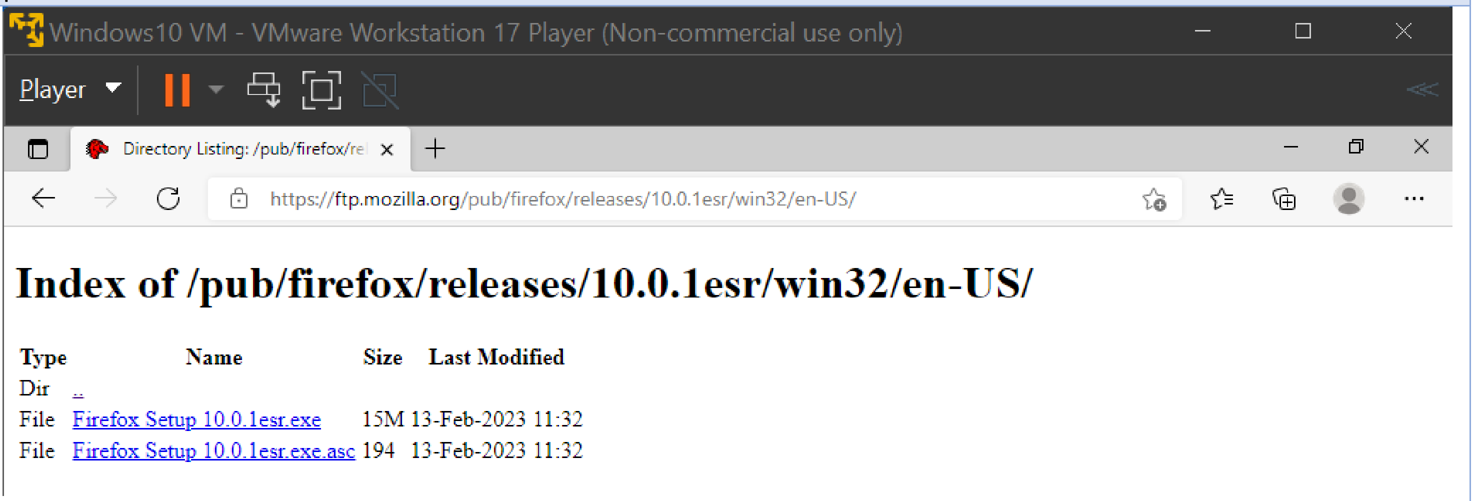
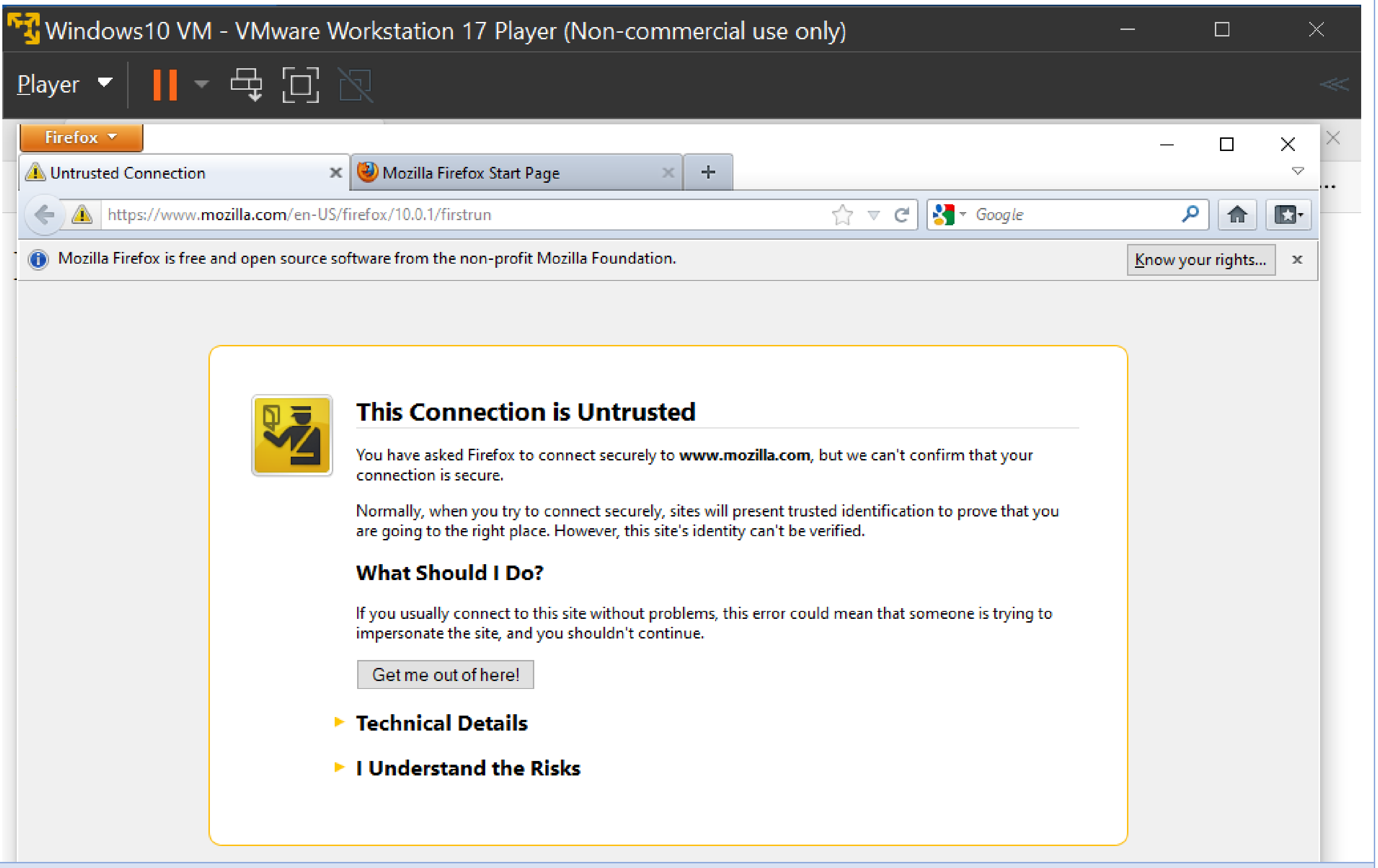
Scan Details

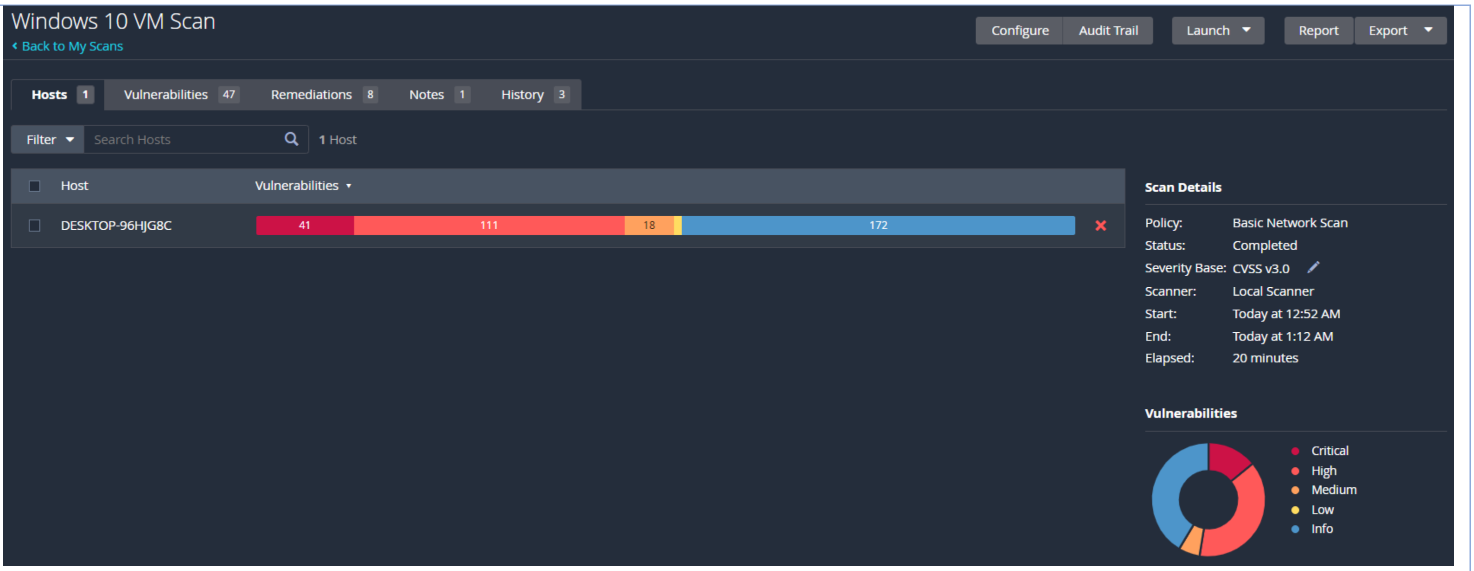
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: March 2 at 10:26 PM
End: March 2 at 10:44 PM
Elapsed: 18 minutes

Vulnerabilities

D. Installing Old Version of Firefox On The Targeted Windows 10 VM

Expected Result (ER)	Firefox out dated version is successfully installed on the hosted machine and Nessus identifies the presence of the outdated Firefox version during vulnerability assessment.

No.	Steps Description
1.	Download and install the outdated Firefox version on the Windows 10 VM according to standard installation procedures and rerun the Nessus scan.
	 Windows10 VM - VMware Workstation 17 Player (Non-commercial use only) Player Directory Listing: /pub/firefox/re https://ftp.mozilla.org/pub/firefox/releases/10.0.1esr/win32/en-US/ Index of /pub/firefox/releases/10.0.1esr/win32/en-US/ Type Name Size Last Modified Dir .. File Firefox Setup 10.0.1esr.exe 15M 13-Feb-2023 11:32 File Firefox Setup 10.0.1esr.exe.asc 194 13-Feb-2023 11:32 ---  Windows10 VM - VMware Workstation 17 Player (Non-commercial use only) Player Firefox Untrusted Connection Mozilla Firefox Start Page Google Know your rights... Get me out of here! https://www.mozilla.com/en-US/firefox/10.0.1/firstrun Mozilla Firefox is free and open source software from the non-profit Mozilla Foundation. This Connection is Untrusted You have asked Firefox to connect securely to **www.mozilla.com**, but we can't confirm that your connection is secure. Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified. What Should I Do? If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. ▸ Technical Details ▸ I Understand the Risks
2.	Once the scan is completed successfully (i.e. status changes from "Running" to "Completed", the total number of vulnerabilities found will be displayed along with their severity levels. Download the Report to analyse the results in detail.



Windows 10 VM Scan

‹ Back to My Scans

1 Host

Host	Vulnerabilities
DESKTOP-96HJG8C	41 111 18 172

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:52 AM
End:	Today at 1:12 AM
Elapsed:	20 minutes

Vulnerabilities

Windows 10 VM Scan

‹ Back to My Scans

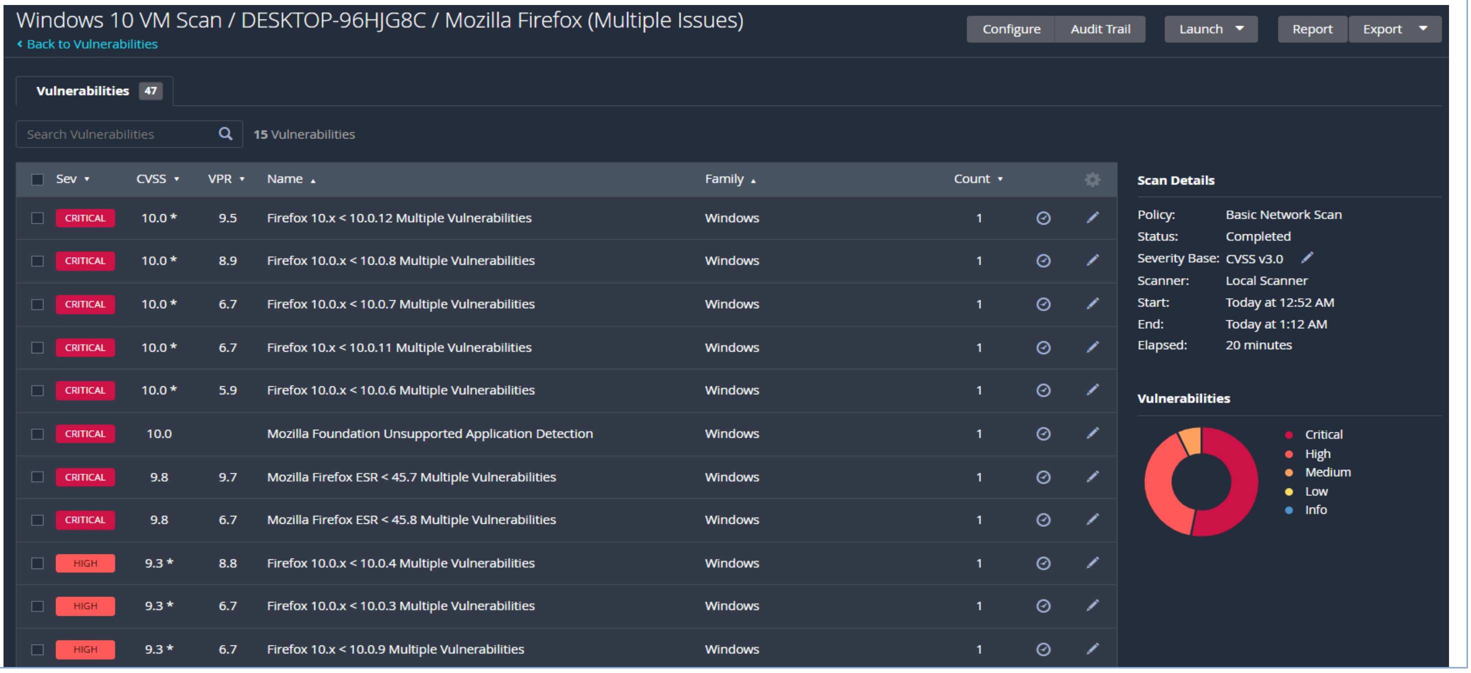
1 Host

Host	Vulnerabilities
DESKTOP-96HJG8C	41 111 18 172

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:52 AM
End:	Today at 1:12 AM
Elapsed:	20 minutes

Vulnerabilities



Windows 10 VM Scan / DESKTOP-96HJG8C / Mozilla Firefox (Multiple Issues)

‹ Back to Vulnerabilities

15 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	9.5	Firefox 10.x < 10.0.12 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *	8.9	Firefox 10.0.x < 10.0.8 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *	6.7	Firefox 10.0.x < 10.0.7 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *	6.7	Firefox 10.x < 10.0.11 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *	5.9	Firefox 10.0.x < 10.0.6 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0		Mozilla Foundation Unsupported Application Detection	Windows	1
CRITICAL	9.8	9.7	Mozilla Firefox ESR < 45.7 Multiple Vulnerabilities	Windows	1
CRITICAL	9.8	6.7	Mozilla Firefox ESR < 45.8 Multiple Vulnerabilities	Windows	1
HIGH	9.3 *	8.8	Firefox 10.0.x < 10.0.4 Multiple Vulnerabilities	Windows	1
HIGH	9.3 *	6.7	Firefox 10.0.x < 10.0.3 Multiple Vulnerabilities	Windows	1
HIGH	9.3 *	6.7	Firefox 10.x < 10.0.9 Multiple Vulnerabilities	Windows	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:52 AM
End:	Today at 1:12 AM
Elapsed:	20 minutes

Vulnerabilities

VULNERABILITY ASSESSMENT RESULTS ANALYSIS

The analysis of the result for each test case is based on the report generated by Nessus after the successful completion of the assessment on the targeted machine.

TC #1 Checking The Network Connectivity Between Local Machine and Windows 10 VM Using Ping Command

The ping requests are expected to be successful after the Windows Defender Firewall is disabled, indicating uninterrupted connectivity between the local machine and the Windows VM.

This expected result is based on the assumption that the Windows Defender Firewall is the only barrier to successful network connectivity between the local machine and the Windows VM. Disabling the firewall should allow ICMP packets (ping requests) to pass through, resulting in successful ping responses between the two systems.

Once the firewall is disabled, the ping command should return successful responses, confirming that network connectivity between the local machine and the Windows VM has been established without interruption.

TC #2 Accessing and Initiating The Basic Network Scan For The Identified Targeted Host

Vulnerabilities Summary

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
DESKTOP-96HJG8C	18	0	0	1	0	17

Initially, a basic network scan was conducted on the targeted machine (Windows 10 OS) without providing any credentials. The scan provided information about numerous vulnerabilities of which one medium severity vulnerability related to SMB Signing not required and other detailing parameters of the machines.

Nessus categorised these vulnerabilities as either Critical, High, Medium, Low and Info (not necessarily a vulnerability but useful to be aware of). These categorizations are based on the Common Vulnerabilities and Exposures (CVE) catalogue system, maintained by MITRE corporation. Furthermore, each vulnerability was associated with a Common Vulnerabilities and Exposures (CVSS) score.

Moreover, it is important to address the vulnerabilities promptly to mitigate potential security risk associated with unauthorised access and tampering SMB communication that the hosted vulnerable VM can face.

Details of Identified Vulnerability

- **Vulnerability:** SMB Signing not required
- **Severity:** Medium
- **CVSS V3.0 score:** 5.3
- **Plugin Name/ID:** 57608
- **Vulnerability Priority Rating (VPR):** 4

Description

SMB (Server Message Block) is a network protocol used for providing shared access to files, printers, and other communication between nodes on a network. SMB Signing is a feature that digitally signs SMB packets, which helps prevent man-in-the-middle attacks. When SMB Signing is not required, it means that the system allows communication without enforcing the signing of SMB packets. This can potentially expose the system to security risks, as an attacker could intercept and modify SMB packets without detection. The medium severity indicates that while the vulnerability is not critical, it still poses a risk that should be addressed.

Recommendation/Solution

The recommendation is to enforce message signing in the host's configuration to mitigate the identified vulnerability related to SMB Signing not being required. On Windows, this can be achieved by configuring the policy setting 'Microsoft network server: Digitally sign communications (always)', ensuring that SMB packets are digitally signed, thus enhancing communication security. These measures reduce the risk of unauthorized access and tampering.

TC #3	Utilising And Configuring Windows Credentials To Perform In-depth VA On Windows 10 VM

Vulnerabilities Summary

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
DESKTOP-96HJG8C	260	24	99	16	1	120

After configuring credentials and re-running the scan on the targeted host, the result revealed a total 260 vulnerabilities. Among these, 24 were classified as critical posing immediate and severe risks to the system's security. Additionally, 99 vulnerabilities were categorized as high severity, indicating significant potential for exploitation and system compromise if left unaddressed. There were also 16 medium severity vulnerabilities detected, highlighting potential security weaknesses that could be exploited under certain conditions. Only one vulnerability was classified as low severity, suggesting a relatively lower risk but still requiring attention to mitigate potential impacts. Furthermore, the scan identified 120 informational findings, providing valuable insights into the system's configuration and software landscape for proactive security measures and maintenance.

For some identified vulnerabilities, Nessus provided remediation options that typically include recommendations.

Key findings from TC #3

1. Critical Vulnerabilities (Total 24)
   The critical vulnerabilities include multiple vulnerabilities found in Microsoft Edge (Chromium) versions below 111.0.1661.54 and 110.0.1587.78. These vulnerabilities could potentially lead to remote code execution or other severe security breaches. Additionally, critical vulnerabilities were discovered in Microsoft .NET Framework and Microsoft 365 (Office) App, potentially allowing attackers to execute arbitrary code on the affected system.

2. High Severity Vulnerabilities (Total: 99)
   The Microsoft Edge (Chromium) is identified as having numerous vulnerabilities across different versions, including versions below 100.0.1185.29, 101.0.1210.32, 107.0.1418.24, and many others. These vulnerabilities could potentially allow attackers to execute arbitrary

code or gain unauthorized access to systems. Furthermore, Windows 10 Version 21H2 / Windows 10 Version 22H2 (KB5034763) is affected by security flaws, which could lead to system compromise if exploited. Additionally, vulnerabilities in Microsoft applications such as 3D Viewer and Paint 3D, along with security issues in Windows Defender and related libraries, pose significant threats to system integrity and data confidentiality.

3. Medium Severity Vulnerabilities (Total: 16)
   Medium severity vulnerabilities involve a range of weaknesses, including security feature bypasses, spoofing attacks, and information disclosure. Specifically, Microsoft Edge (Chromium) versions below 104.0.1293.60 and 109.0.1518.61 are susceptible to vulnerabilities that could allow attackers to bypass security measures or disclose sensitive information. Additionally, issues in Microsoft OneNote and Windows Defender.

4. Low Severity Vulnerabilities (Total: 1)
   The Windows Snip & Sketch/Snipping Tool is affected by a low-level vulnerability identified as CVE-2023-28303, dubbed "Acropalypse." While the risk posed by this vulnerability is relatively low.

5. Info Severity Vulnerabilities (Total: 120)
   The scan result for info includes detecting ICMP Timestamp Requests for remote date disclosure, verifying the presence of antivirus software, examining application compatibility caches, retrieving BIOS information via WMI, enumerating computer manufacturer details, and confirming the presence of CURL on Windows systems. Additionally, it involves gathering data on network configuration such as Ethernet card manufacturer detection, MAC addresses, and IP assignment methods. Other findings entail detecting installed software like Microsoft .NET Framework, Internet Explorer, OneDrive, and Remote Desktop Connection, as well as assessing security-related aspects such as password policies, logged-on users, and SMB configurations. Furthermore, it involves identifying system components like the Windows registry settings, SMB shares, scripting host configurations, and time zone information.

TC #4 Installing Old Version of Firefox On The Targeted Windows 10 VM

Vulnerabilities Summary

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
DESKTOP-96HJG8C	291	41	111	18	1	120

Installing an old version of firebox browser and initiating the assessment revealed a significant result. A total of 291 vulnerabilities across various severity levels. Among these, there are 41 critical vulnerabilities, 111 high-severity vulnerabilities, 18 medium-severity vulnerabilities, 1 low-severity vulnerability, and 120 informational findings.

Key findings for TC #4

1. Critical Vulnerabilities (Total: 41)
   The critical vulnerabilities discovered in the system, with a severity rating of 9.6 to 10.0, present significant risks to its security. These vulnerabilities include multiple weaknesses found in widely used software such as Mozilla Firefox ESR and Microsoft Edge (Chromium).

They encompass various types of vulnerabilities, ranging from code execution to multiple vulnerabilities in different versions of the software. **Additionally, unsupported versions of Firefox, including versions 10.0.x, have critical vulnerabilities that could lead to system compromise if not addressed promptly.**

Furthermore, the presence of critical vulnerabilities in Microsoft's security products like Forefront Endpoint Protection and System Centre Endpoint Protection highlights potential weaknesses in the hosted Windows 10 VM.

2. High Severity Vulnerabilities (Total: 111)
   The high-risk vulnerabilities discovered in the hosted Windows 10 VM, with a severity rating of 8.8 to 9.3, pose significant threats to its security. These vulnerabilities encompass multiple weaknesses found in widely used software such as Mozilla Firefox ESR and Microsoft Edge (Chromium). They include various types of vulnerabilities, ranging from remote code execution to privilege escalation. Additionally, security updates and patches for Windows Defender and Forefront Endpoint.

3. Medium Severity Vulnerabilities (Total: 18)
   The medium-risk vulnerabilities identified in the system, with a severity rating ranging from 4.3 to 6.5, present moderate security concerns. These vulnerabilities include weaknesses found in Microsoft Edge (Chromium) versions, which could lead to various issues such as information disclosure, security feature bypass, and tampering. Additionally, vulnerabilities in Microsoft OneNote and Windows Defender require attention to prevent spoofing attacks and ensure adequate protection against threats. Furthermore, security updates for Windows Defender and extensions like the VP9 Video Extensions Library are essential to address potential security gaps and maintain system integrity.

4. Low Severity Vulnerabilities (Total: 1)
   Again, the Windows Snip & Sketch/Snipping Tool is affected by a low-level vulnerability identified as CVE-2023-28303, dubbed "Acropalypse." While the risk posed by this vulnerability is relatively low.

5. Info Severity Vulnerabilities (Total: 120)
   The "INFO" findings provide a comprehensive overview of various technical aspects of the system and network environment. These findings include details such as the presence of antivirus software, information about application compatibility cache, BIOS details obtained through Windows Management Instrumentation (WMI), and Common Platform Enumeration (CPE) data. Additionally, the findings cover details about computer manufacturer information, the presence of specific software like Curl on Windows systems, and information about Distributed Computing Environment (DCE) services. Furthermore, insights into user enumeration via WMI, detection of Ethernet card manufacturers, and resolution of host fully qualified domain names are included.

CONCLUSION

The vulnerability assessment results indicate essential details about the security vulnerabilities found in the targeted Windows 10 virtual machine. Using Nessus, the project discovered vulnerabilities ranging from critical to informational across many software components and system configurations using a series of test cases.

For the vulnerabilities based on the high CVSS score, Nessus highlighted immediate action is needed to fix serious vulnerabilities, including those involving SMB Signing, outdated software versions, and potential exploits in widely used apps such as Mozilla Firefox ESR and Microsoft Edge (Chromium).

REFERENCES

[1] VMWare Workstation 17 Player

https://www.vmware.com/content/vmware/vmware-published-sites/us/products/workstation-player/workstation-player-evaluation.html.html

[2] Windows 10 ISO File

https://www.microsoft.com/en-us/software-download/windows10

[3] Nessus Essentials

https://www.tenable.com/

[4] Microsoft Vulnerability Management

https://www.microsoft.com/en-gb/security/business/security-101/what-is-vulnerability-management#:~:text=FAQs-,Vulnerability%20management%20defined,from%20cyberattacks%20and%20data%20breaches.