

# Vulnerability Assessment using Nessus

## 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 unauthorized access or compromise the security of the system.

Furthermore, a detailed report is generated by the Nessus tool of the identified vulnerabilities and further analyzed 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 prioritize and address the discovered vulnerabilities.

## PROJECT REQUIREMENTS:

1. VMware Workstation Player
2. Windows 10 OS
3. Nessus Essentials tool

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

## TEST CASES

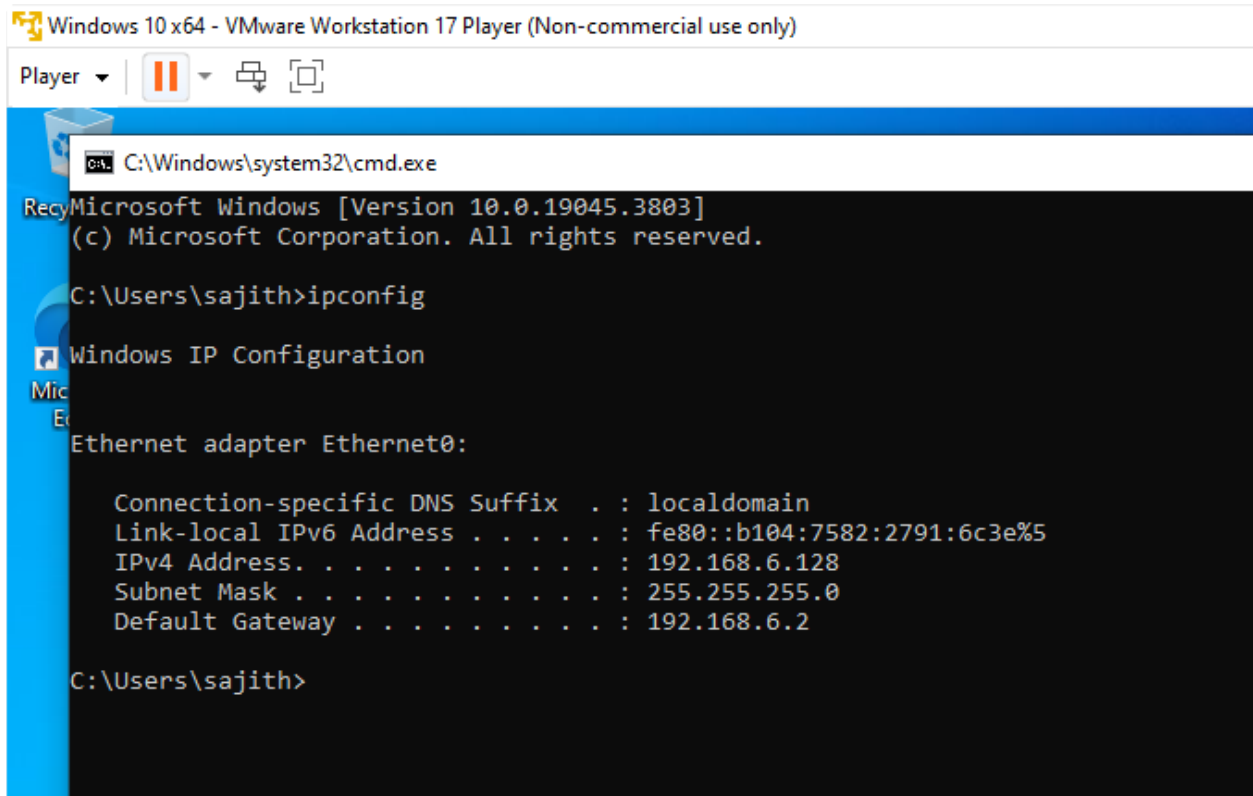
Following test cases were performed for the project.

### **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.

**Step 1:** Accessing the IP address of the Windows 10 OS installed on VMware using **ipconfig** command in the command prompt.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sajith>ipconfig

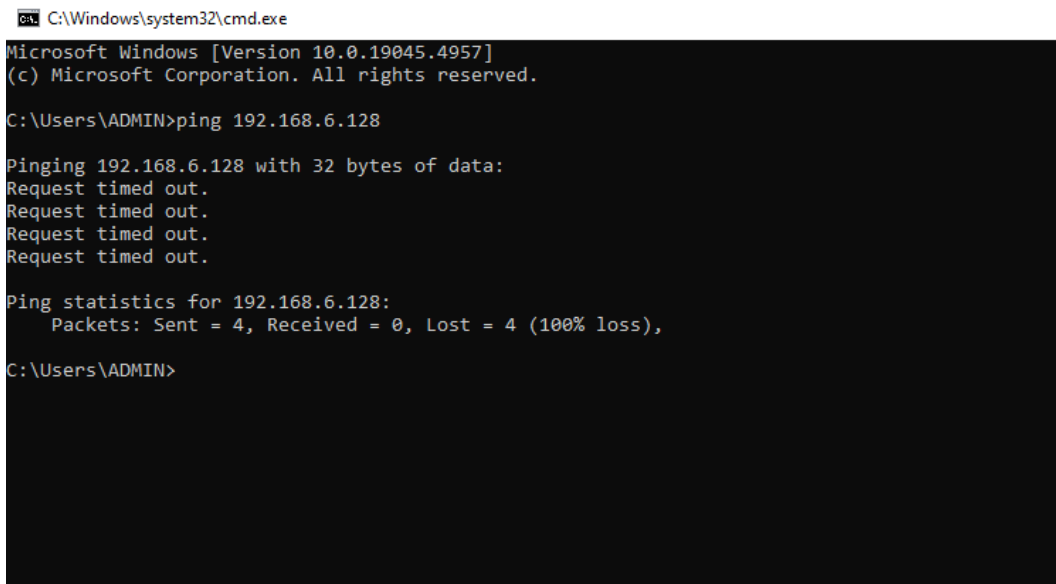
Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::b104:7582:2791:6c3e%5
    IPv4 Address. . . . . : 192.168.6.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.6.2

C:\Users\sajith>
```

**Step 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:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4957]
(c) Microsoft Corporation. All rights reserved.

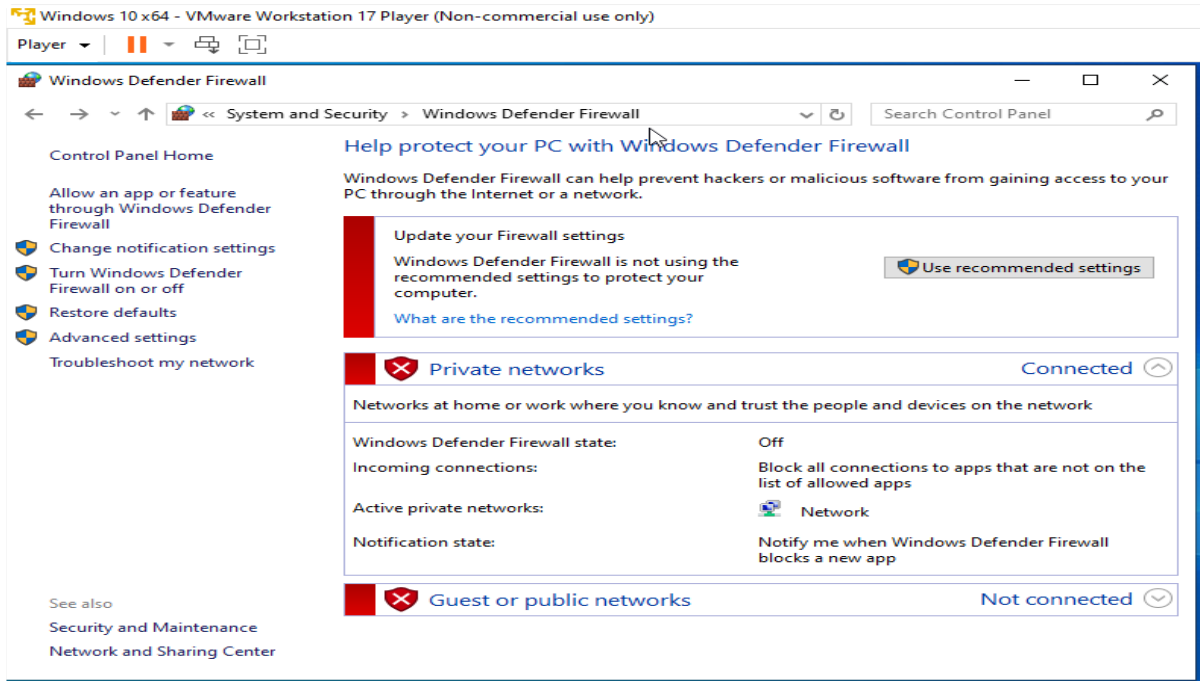
C:\Users\ADMIN>ping 192.168.6.128

Pinging 192.168.6.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.6.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ADMIN>
```

### Step 3: Disabling the Windows Defender Firewall on the Windows VM.



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

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4957]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>ping 192.168.6.128

Pinging 192.168.6.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.6.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ADMIN>ping 192.168.6.128

Pinging 192.168.6.128 with 32 bytes of data:
Reply from 192.168.6.128: bytes=32 time<1ms TTL=128
Reply from 192.168.6.128: bytes=32 time<1ms TTL=128
Reply from 192.168.6.128: bytes=32 time<1ms TTL=128
Reply from 192.168.6.128: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.6.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

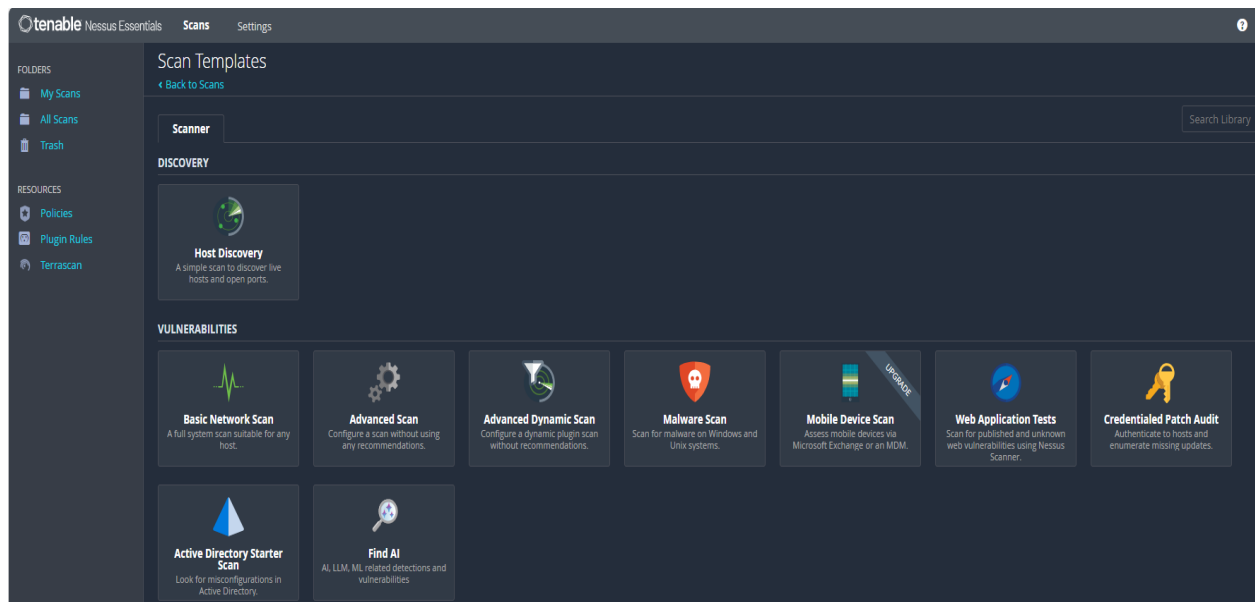
C:\Users\ADMIN>
```

## b) Accessing and Initiating The Basic Network Scan For The Identified Targeted Host.

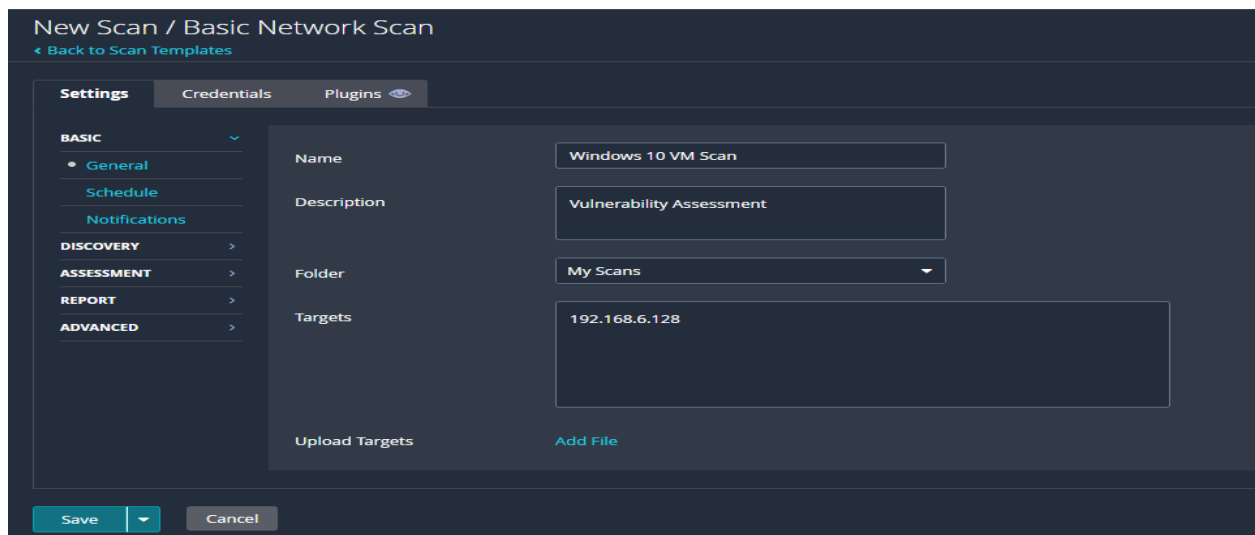
### Expected Result (ER):

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

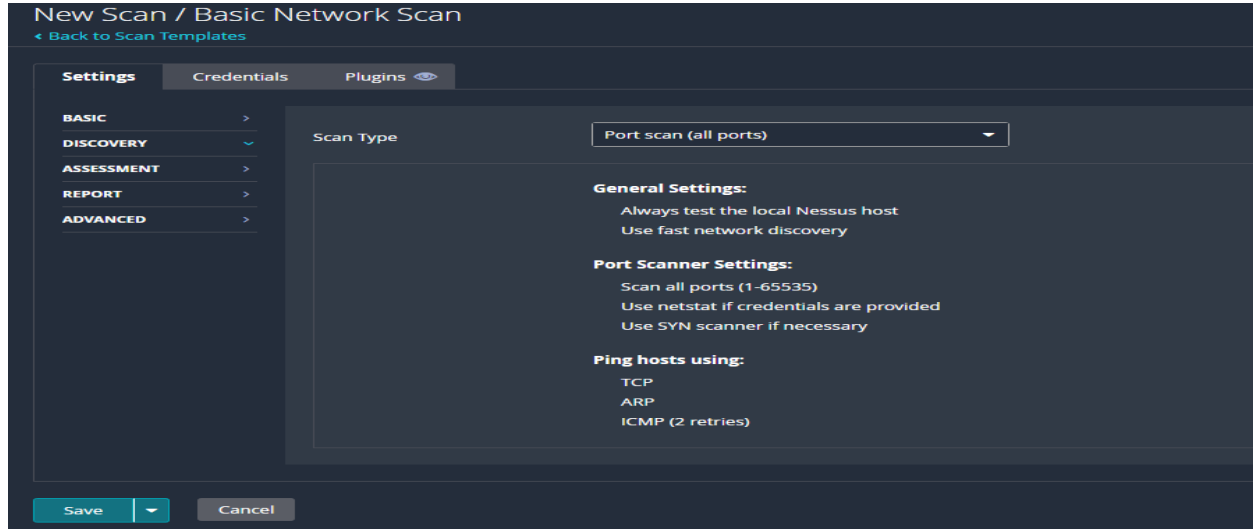
**Step 1:** Create a New Scan and select the “Basic Network Scan” feature which is a full system scan suitable for the hosted Windows 10 VM.



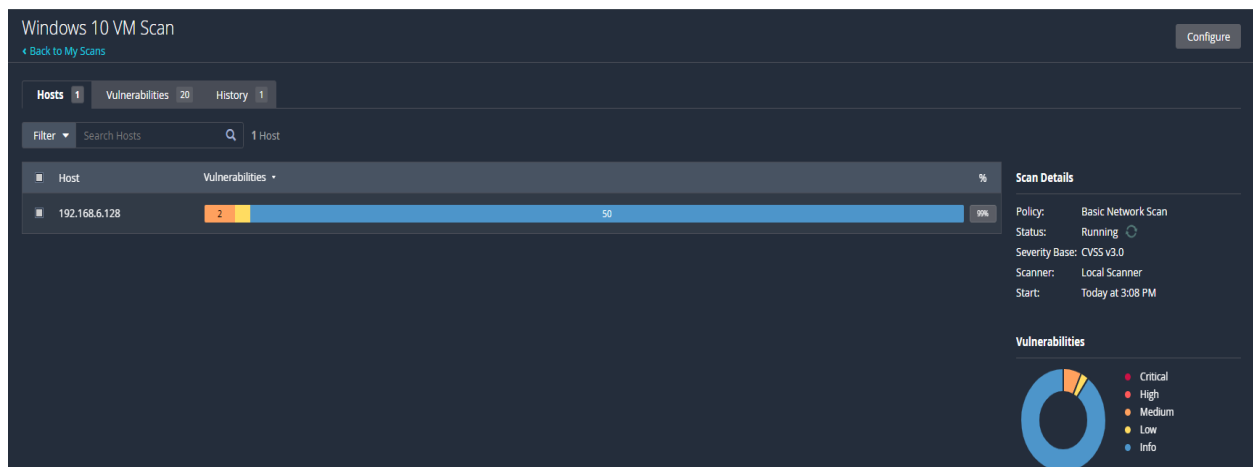
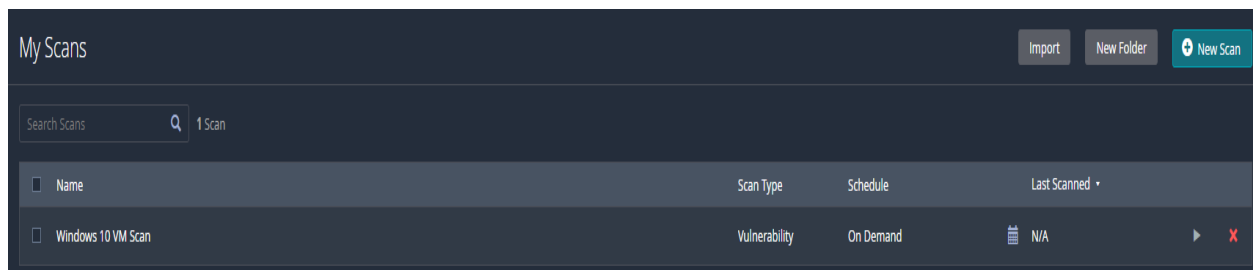
**Step 2:** Enter relevant details, ensuring the IP address (i.e.192.168.128.129) of the targeted Windows 10 VM is specified in the Target field.



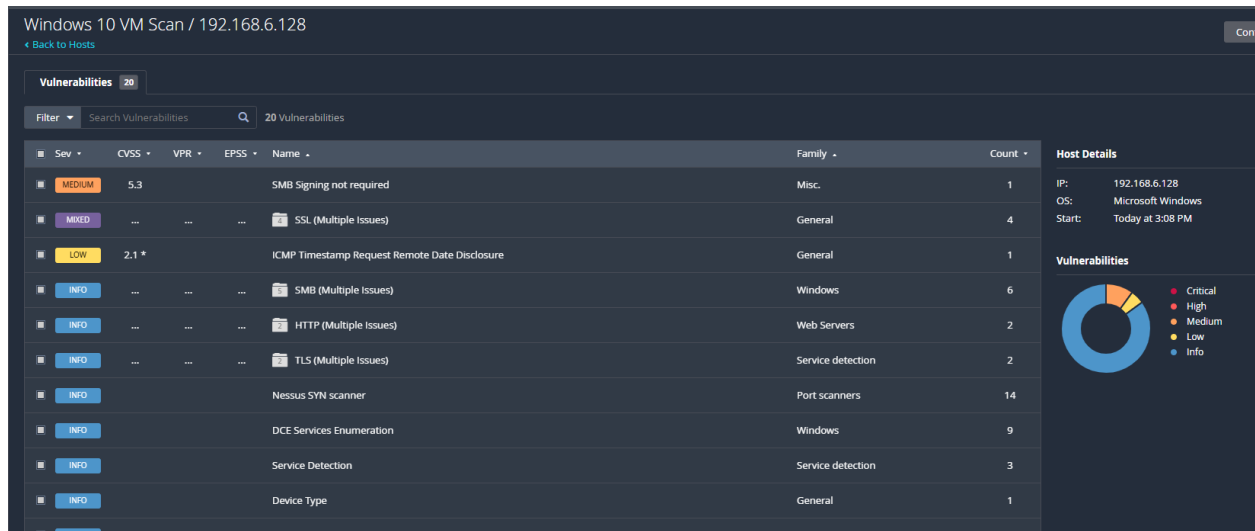
**Step 3:** Under Discovery section, select Scan Type as “Port scan (all ports)”.



**Step 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).



**Step 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 analyze the results in detail.



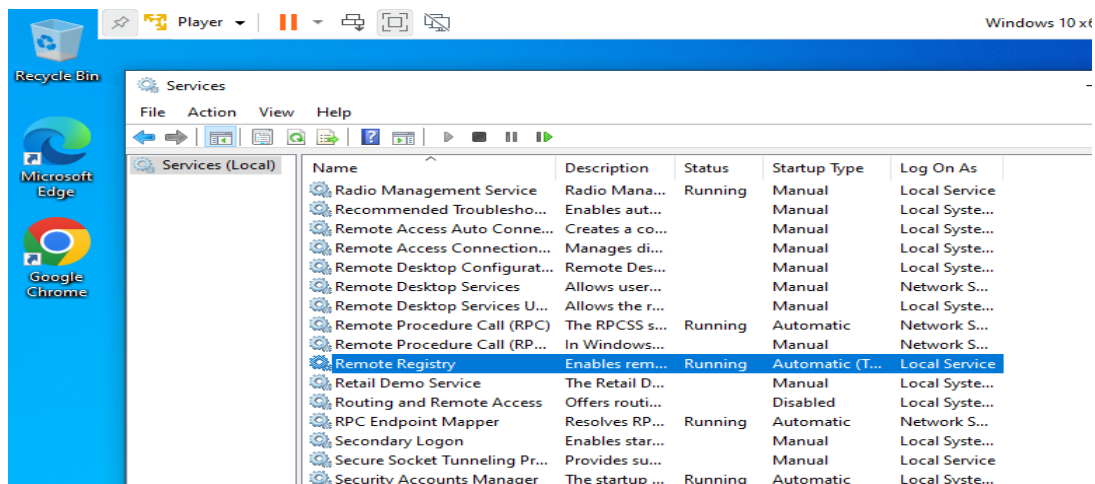
## c) Utilizing and Configuring Windows Credentials To Perform In-depth VA On Windows 10 VM

### Expected Result (ER):

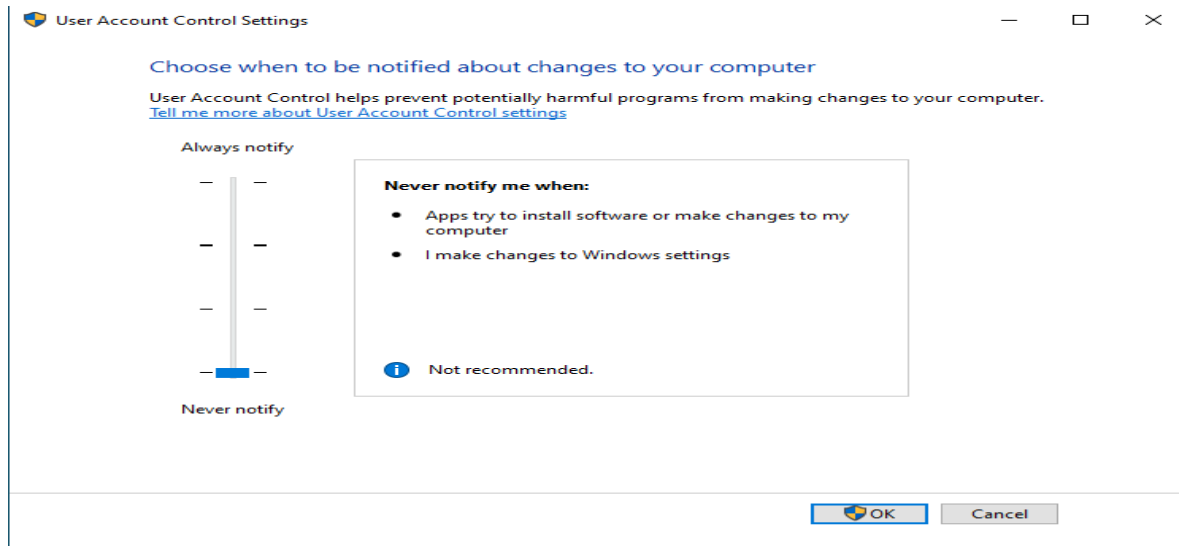
Using the Credentials feature by giving valid username and password of the targeted machine to perform in-depth vulnerability assessment on the Windows 10 VM is successfully conducted by utilizing appropriate settings and configuration to enable remote access and authentication.

**Step 1:** Access the Services configuration of the Windows 10 VM and enable the Remote Registry service to allow remote access.

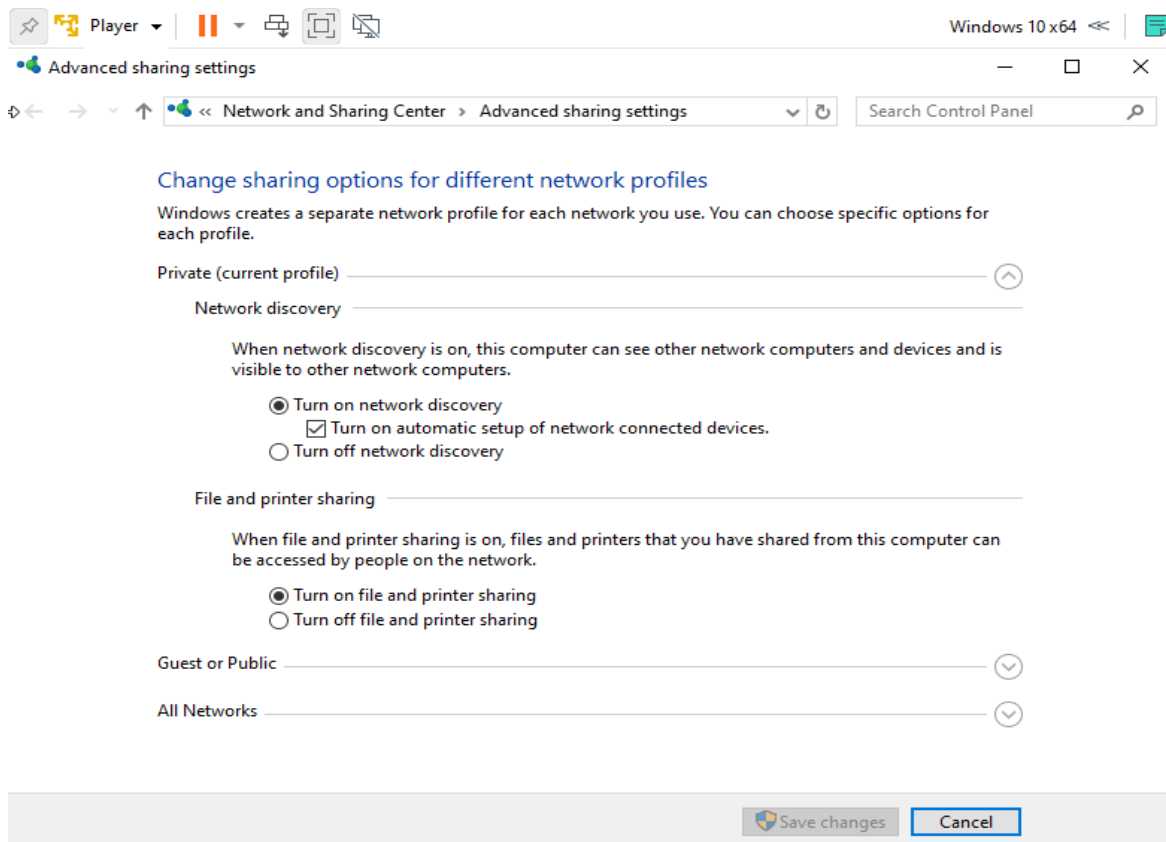
(This will allow the Nessus to perform in-depth scanning to discovery and identify more critical and high vulnerabilities which can be exploited by the attacker)



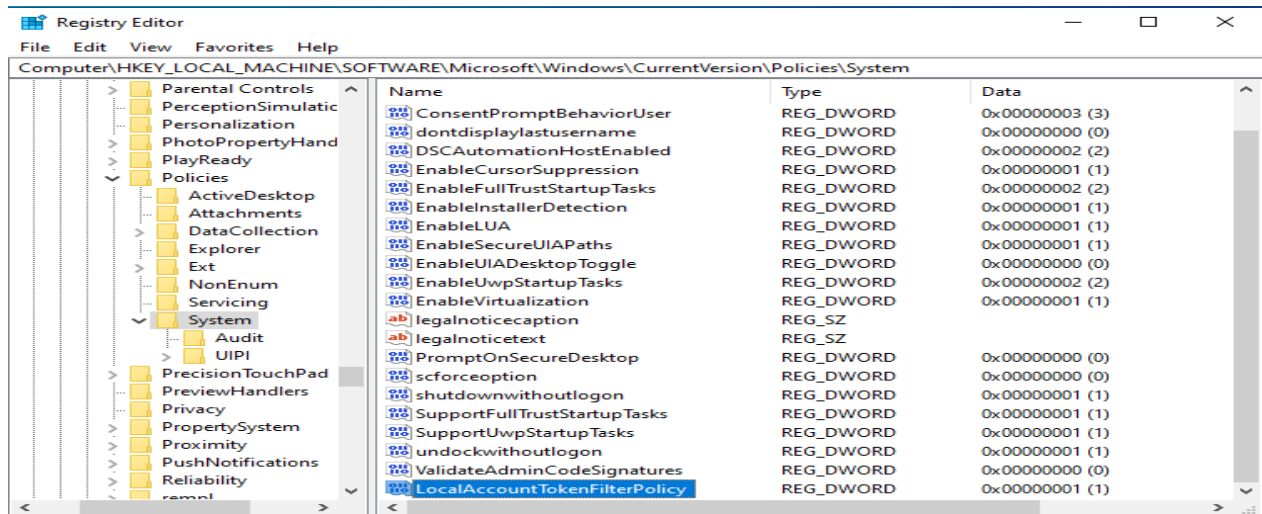
**Step 2:** Modify the User Account Control to “Never Notify” under User Account Control Settings in Windows 10 VM (This will ensure uninterrupted scanning by preventing the OS from prompting for user consent when the changes are made to the Windows 10 VM)



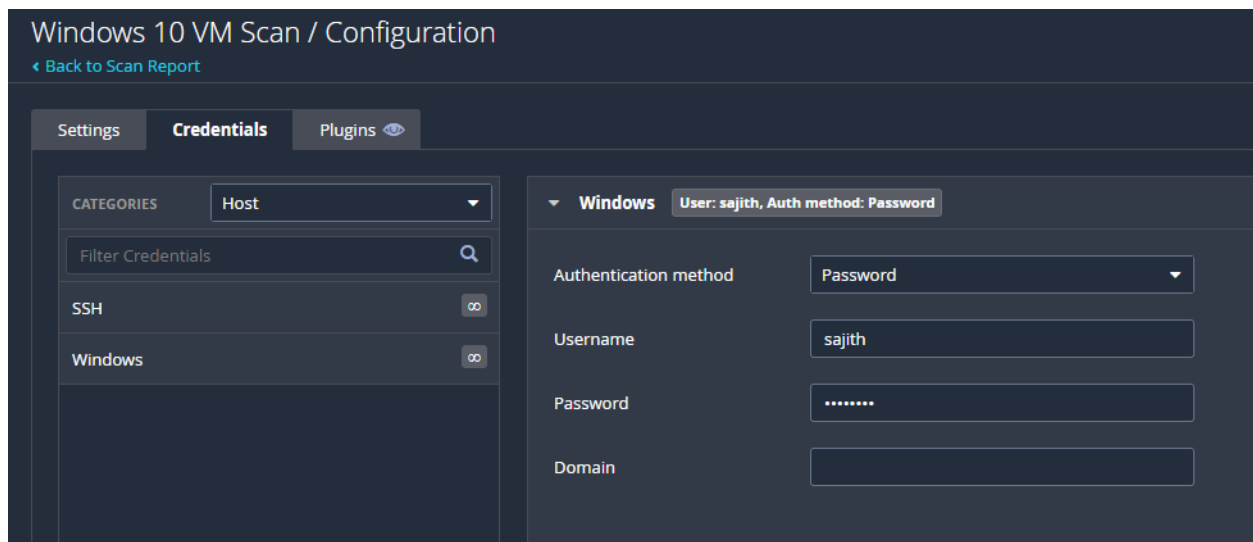
**Step 3:** Ensure that Network discovery and File and printer sharing are enabled on the Windows 10 VM.  
(This allows Nessus to interact with the targeted machine remotely)



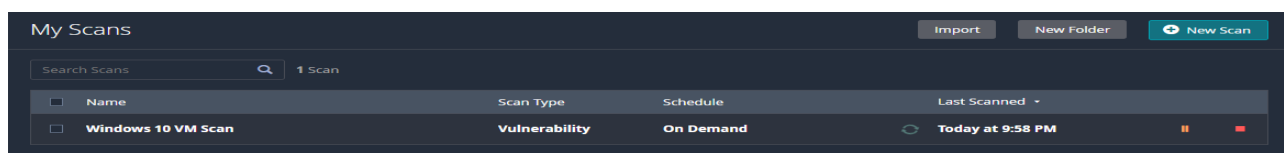
**Step 4:** Using the Registry Editor, create a new DWORD registry (given the specified path) and assign the value as 1. After successful creation, restart the Windows 10 VM.  
(Creating a new registry will allow the non-administrator account (Nessus) to perform the scan on the Windows 10 VM)



**Step 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)

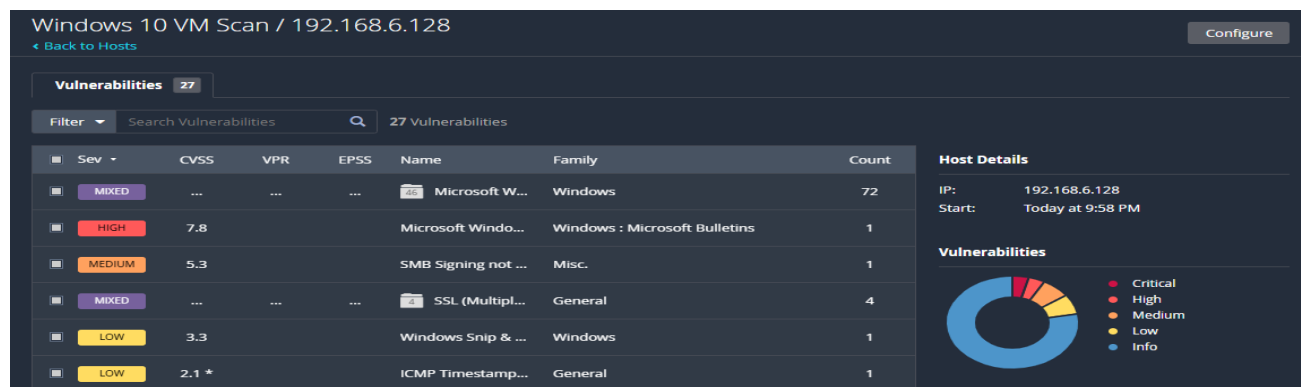
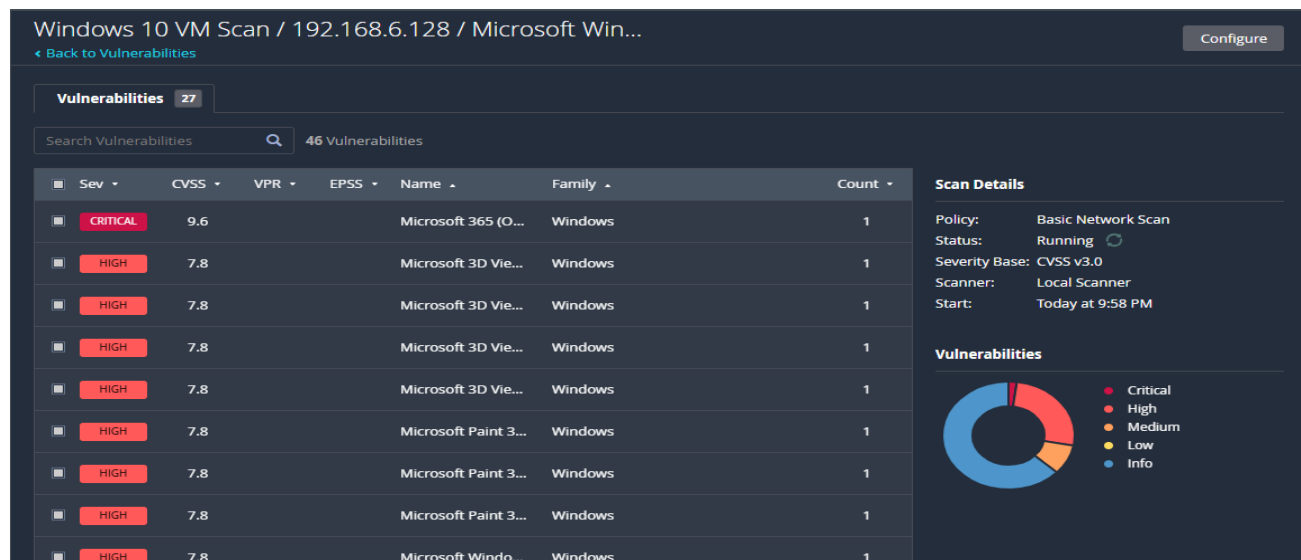
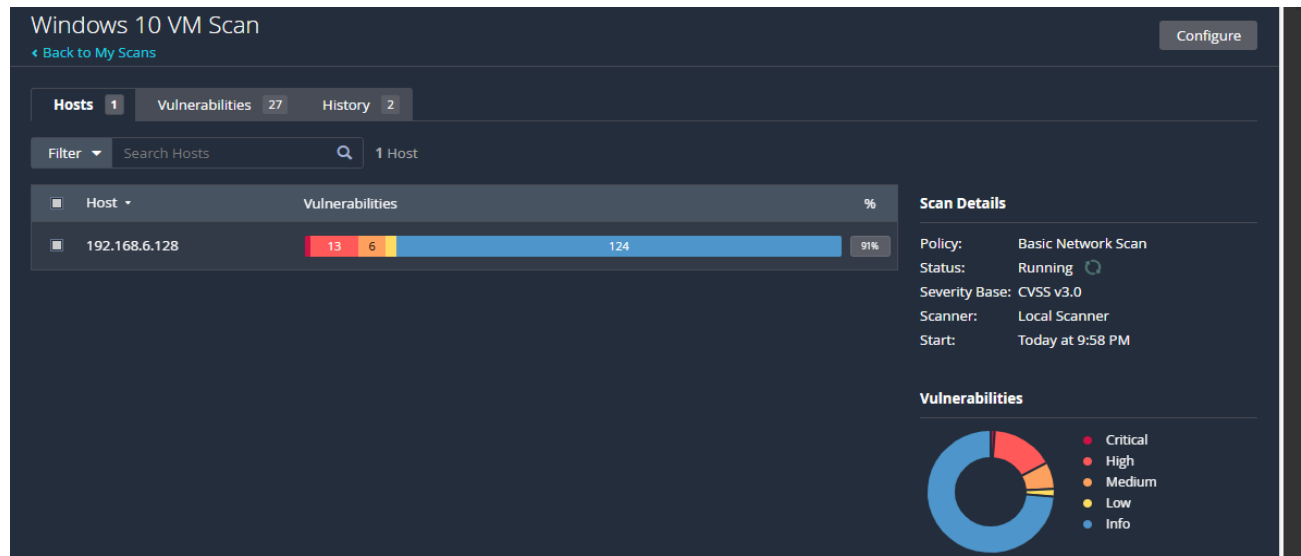


**Step 6:** Rerun the Vulnerability Scan





**Step 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 analyze the results in detail.

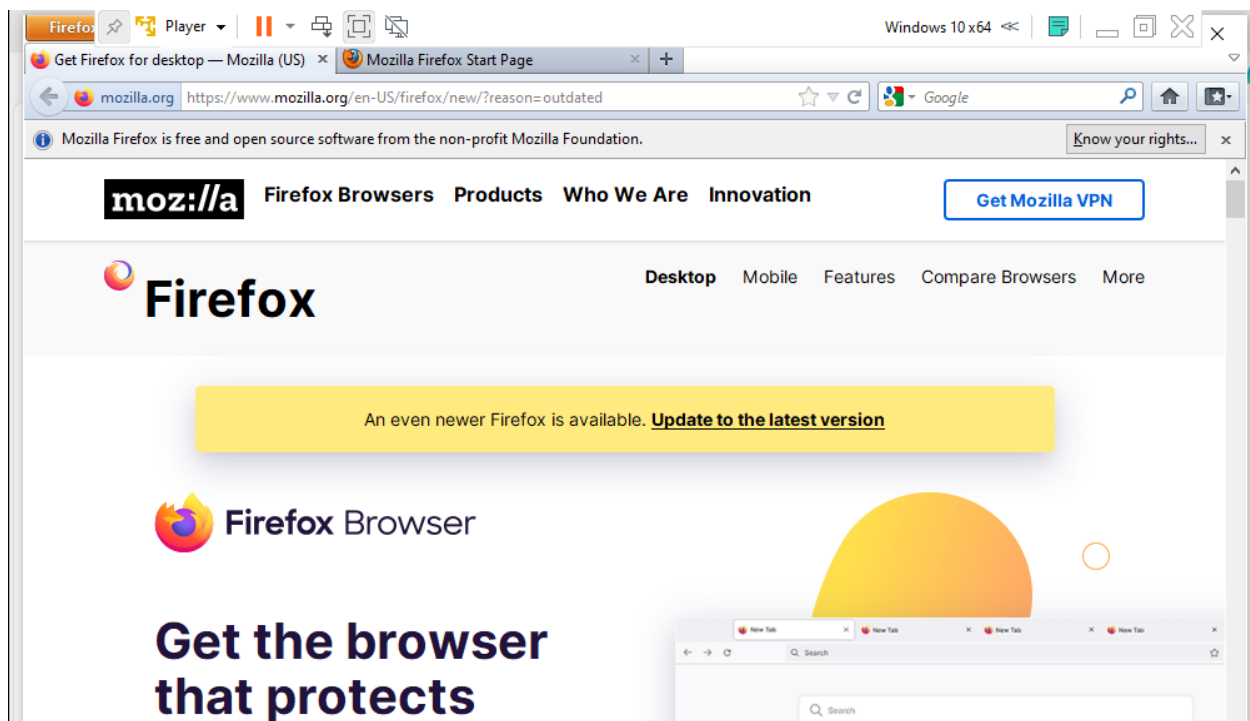


## d) Installing Old Version of Firefox On The Targeted Windows 10 VM

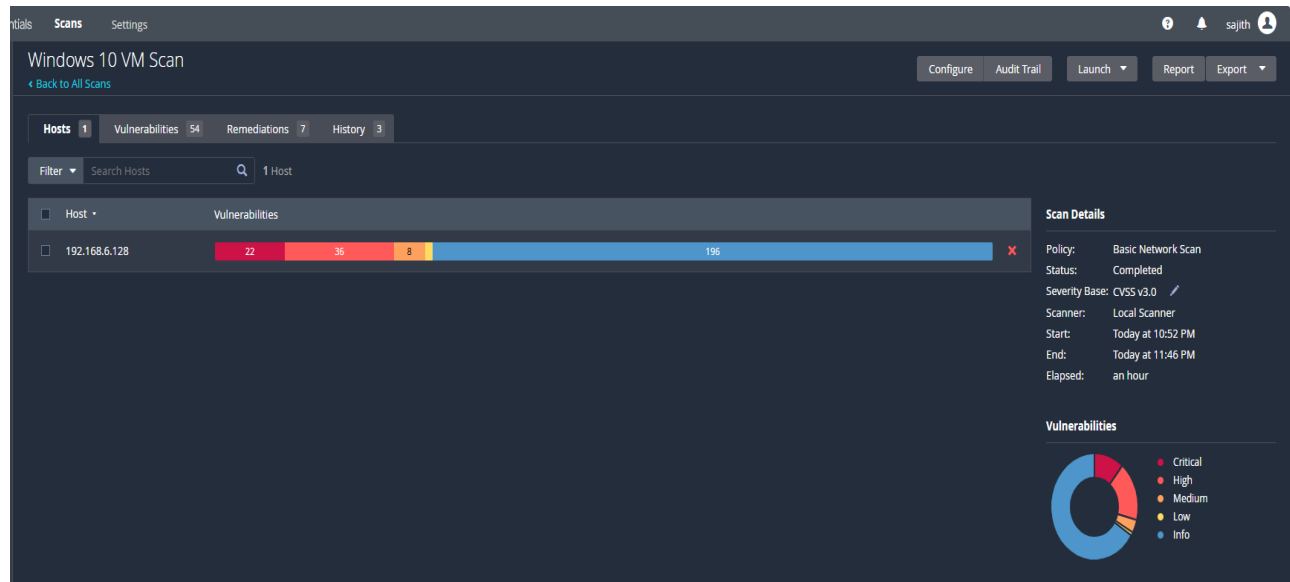
### Expected Result (ER):

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

**Step 1:** Download and install the outdated Firefox version on the Windows 10 VM according to standard installation procedures and rerun the Nessus scan.



**Step 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 analyze the results in detail.



Windows 10 VM Scan / 192.168.6.128 / Mozilla Firefox ESR (Multiple Issues)

Configure

Vulnerabilities 39

Search Vulnerabilities 16 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			Firefox ESR < 17.0.10 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *			Firefox ESR < 38.2 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *			Firefox ESR < 38.2.1 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0 *			Firefox ESR < 38.5 Multiple Vulnerabilities	Windows	1
CRITICAL	10.0			Mozilla Firefox ESR < 60.5	Windows	1
CRITICAL	9.8			Firefox ESR < 38.6 Multiple Vulnerabilities	Windows	1
CRITICAL	9.8			Firefox ESR < 38.7 Multiple Vulnerabilities	Windows	1
CRITICAL	9.8			Mozilla Firefox ESR < 60.4 Multiple Vulnerabilities	Windows	1
CRITICAL	9.8			Mozilla Firefox ESR < 68.6 Multiple Vulnerabilities	Windows	1
HIGH	8.8			Firefox ESR < 38.6.1 Multiple Graphite 2 Library RCE	Windows	1
HIGH	8.8			Firefox ESR < 38.8 Multiple Vulnerabilities	Windows	1
HIGH	8.8			Mozilla Firefox ESR < 60.5.1	Windows	1
HIGH	7.5 *			Firefox ESR < 17.0.11 Null_Cipher Code Execution	Windows	1
HIGH	7.5 *			Firefox ESR < 38.3 Multiple Vulnerabilities	Windows	1
HIGH	7.5 *			Firefox ESR < 38.4 Multiple Vulnerabilities	Windows	1

Scan Details

Policy: Basic Network Scan  
Status: Running  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 10:52 PM

Vulnerabilities

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

## 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.

### Test Case 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.

### Test Case 2:

#### ❖ **Accessing and Initiating The Basic Network Scan For The Identified Targeted Host.**

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
192.168.6.128	20	0	0	1	1	18

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 categorized these vulnerabilities as 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 unauthorized 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.

### Test Case 3:

- ❖ **Utilizing And Configuring Windows Credentials To Perform In-depth VA On Windows 10 VM**

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
192.168.6.128	151	1	13	6	7	124

After configuring credentials and re-running the scan on the targeted host, the result revealed a total 151 vulnerabilities. Among these, 1 is classified as critical posing immediate and severe

risks to the system's security. Additionally, 13 vulnerabilities were categorized as high severity, indicating significant potential for exploitation and system compromise if left unaddressed. There were also 6 medium severity vulnerabilities detected, highlighting potential security weaknesses that could be exploited under certain conditions. There are 6 vulnerability was classified as low severity, suggesting a relatively lower risk but still requiring attention to mitigate potential impacts. Furthermore, the scan identified 124 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 Test Case 3:**

#### **1. Critical Vulnerabilities (Total 1)**

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: 13)**

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: 6)**

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: 7)

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: 124)

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.

#### Test Case 4:

##### ❖ Installing Old Version of Firefox On the Targeted Windows 10 VM

Hostname	Total Vulnerabilities	Critical	High	Medium	Low	Info
192.168.6.128	264	22	36	8	2	196

#### Key findings from Test Case 4:

##### 1. Critical Vulnerabilities (Total 22)

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: 36)**

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: 8)**

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.

## **4. Low Severity Vulnerabilities (Total: 2)**

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: 196)**

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.

## **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).