

# Vulnerability Management with Nessus

By  
Seenuvasan

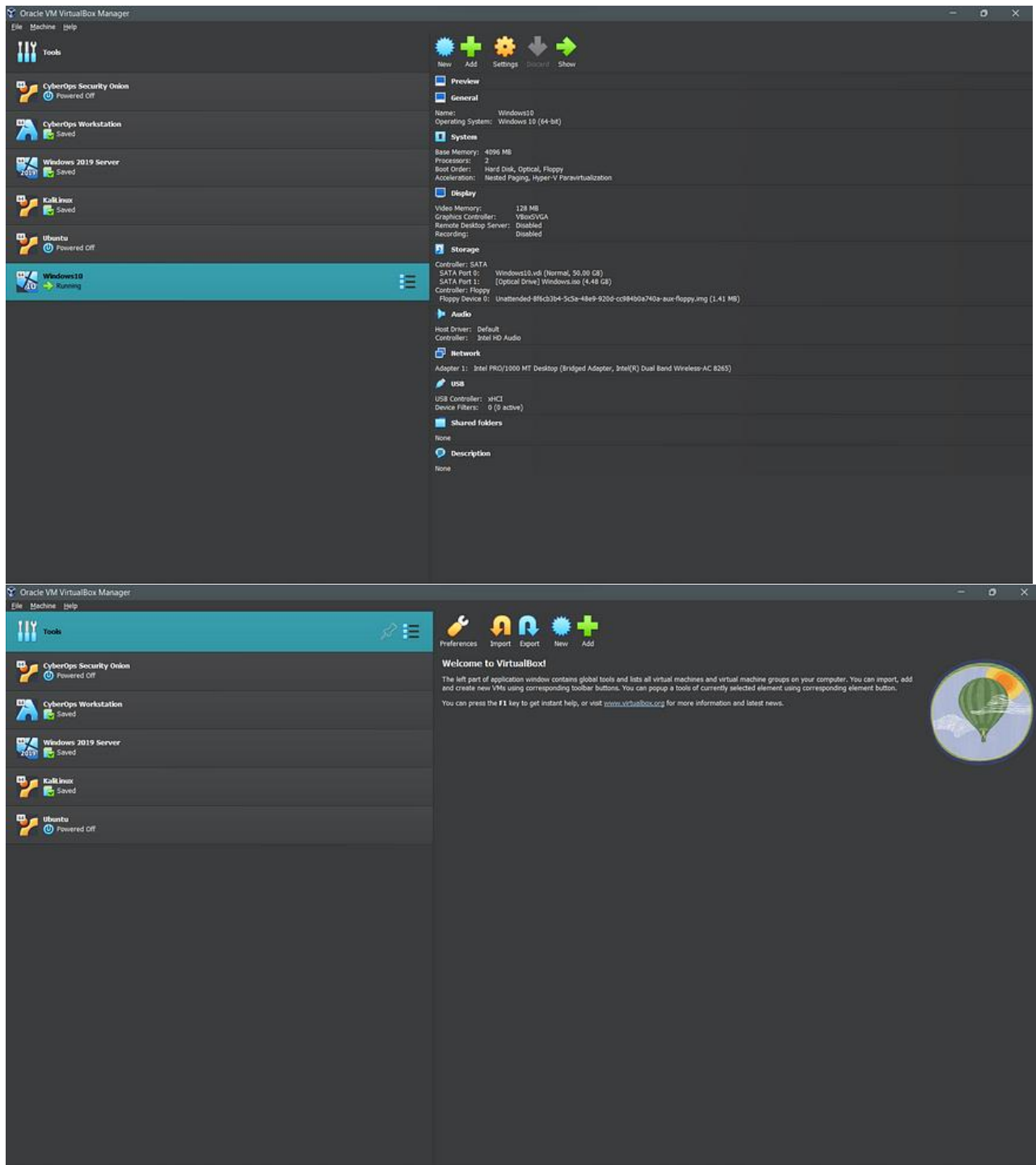
## **Setting up the virtual box**

In this home lab, I'll be making use of Oracle VirtualBox, Windows 10 Virtual machine and Nessus Tenable as the tools of choice.

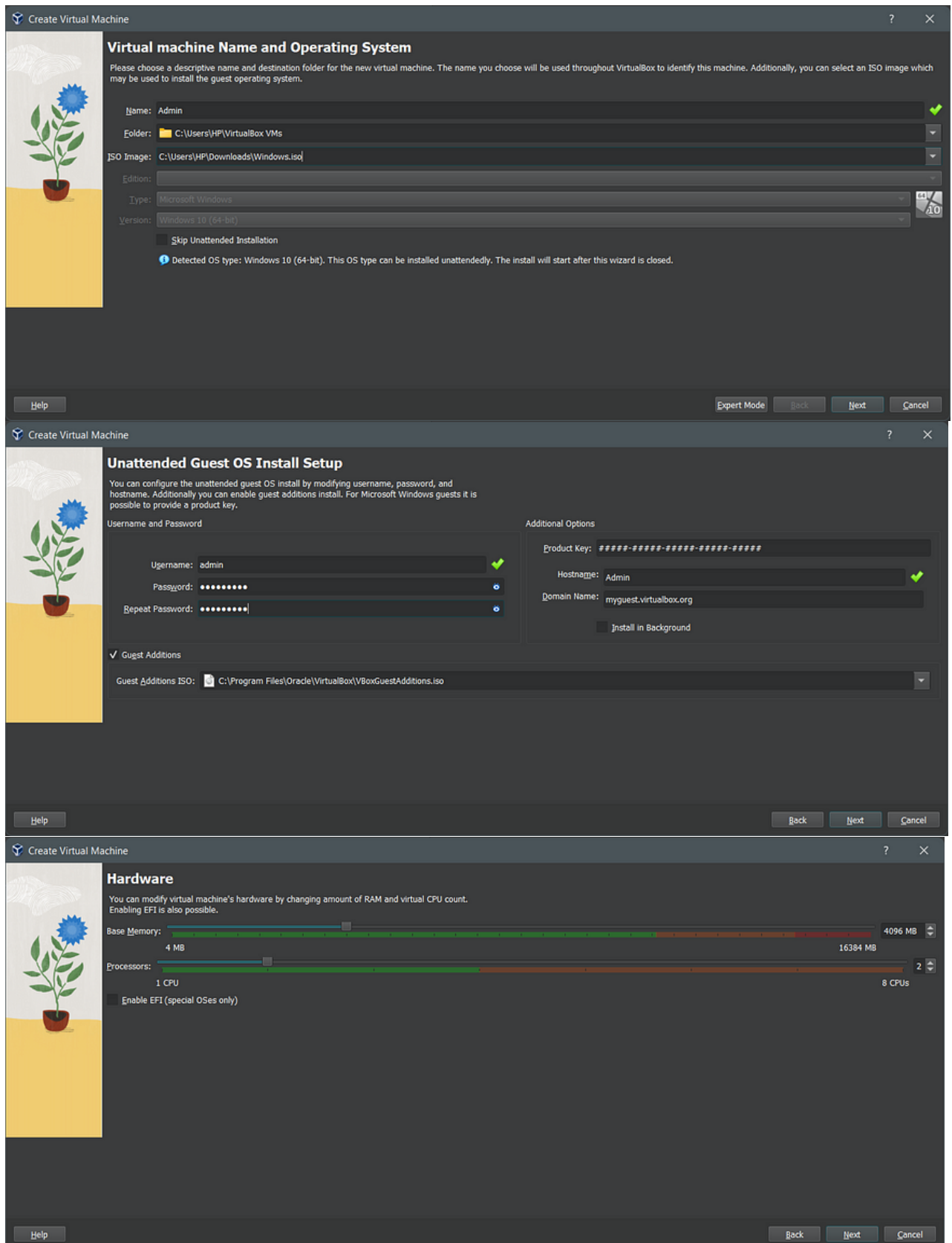
1. Oracle VirtualBox: For this exercise, VirtualBox will act as the hypervisor. To put it simply for those unfamiliar with technical terms, a hypervisor is software that enables the creation and operation of virtual machines (VMs). It allows a single host computer to accommodate multiple guest VMs by efficiently sharing its resources, such as memory and processing power.
2. Windows 10 Virtual Machine: For this exercise, my target virtual machine would be running on Windows 10.
3. Nessus Tenable: Nessus, a powerful vulnerability scanning tool, will be my primary tool for conducting the scan. With its extensive capabilities, Nessus can scan all network-connected devices, including printers and other Internet-of-Things (IoT) devices, to identify known vulnerabilities.

Now, let's delve into the realm of vulnerability management.

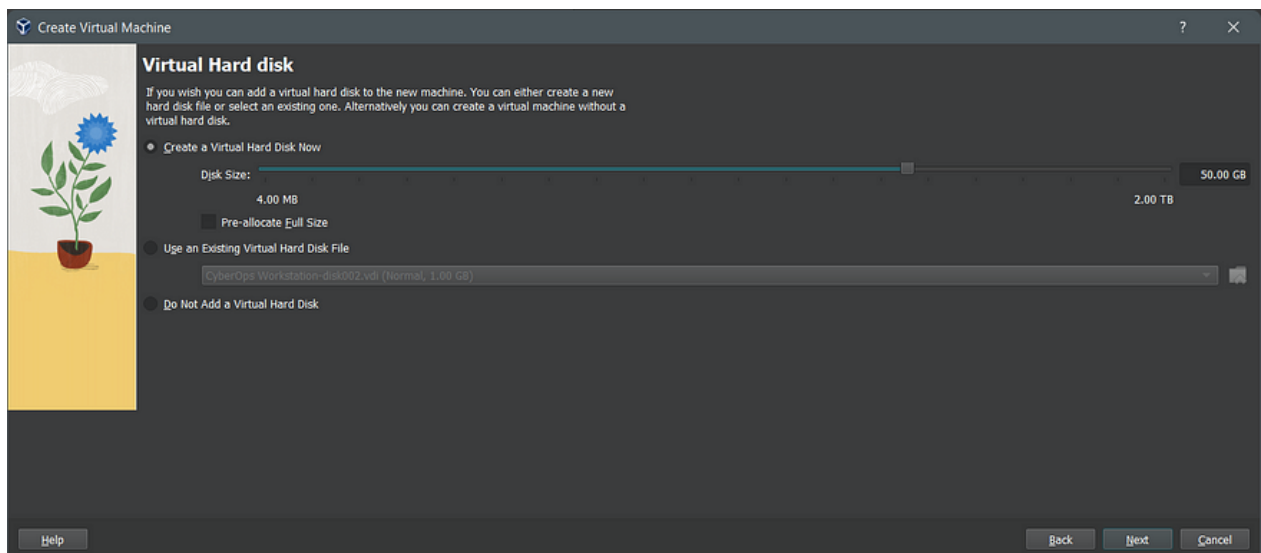
First tool I am going to make use of is VirtualBox. I already have my Virtualbox installed, but incase you want to follow along. If you wish to follow along, start by launching VirtualBox and installing a virtual machine, which will be your target for this exercise.



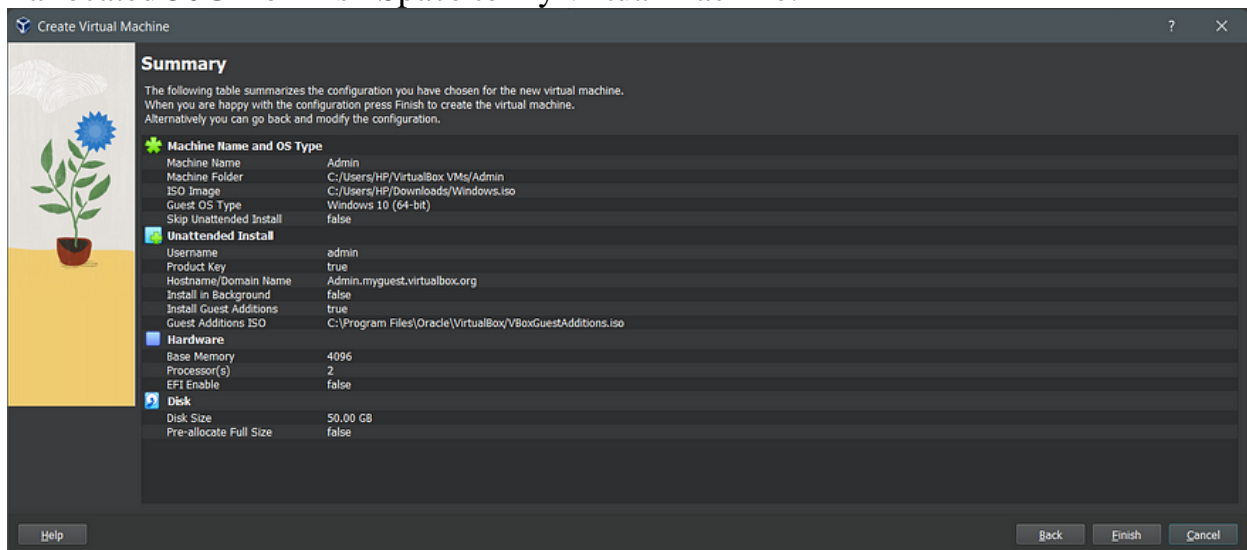
proceed with the installation of your virtual machine.



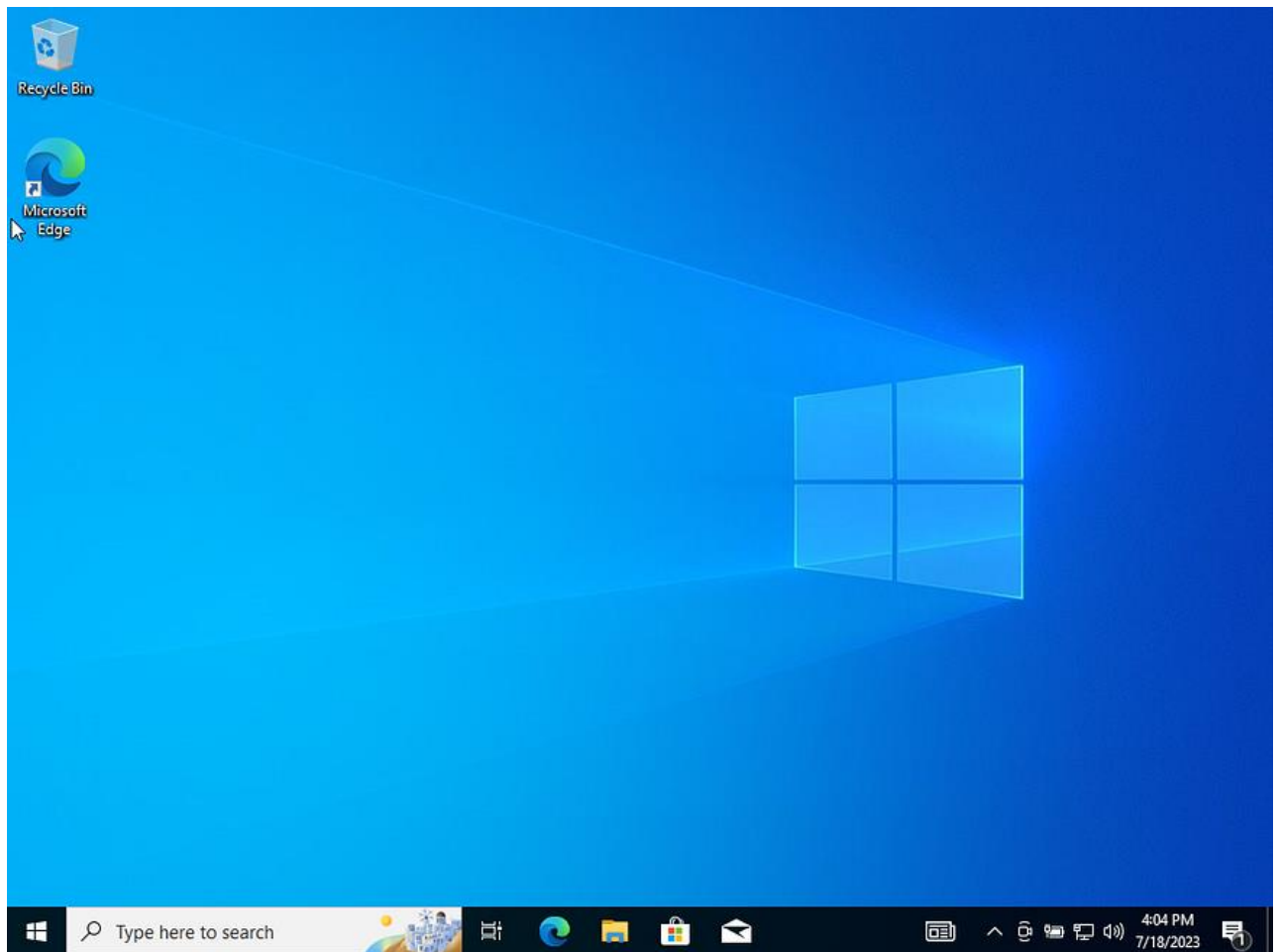
I allocated 4GB of RAM to my virtual machine.



I allocated 50GB of Disk Space to my virtual machine.

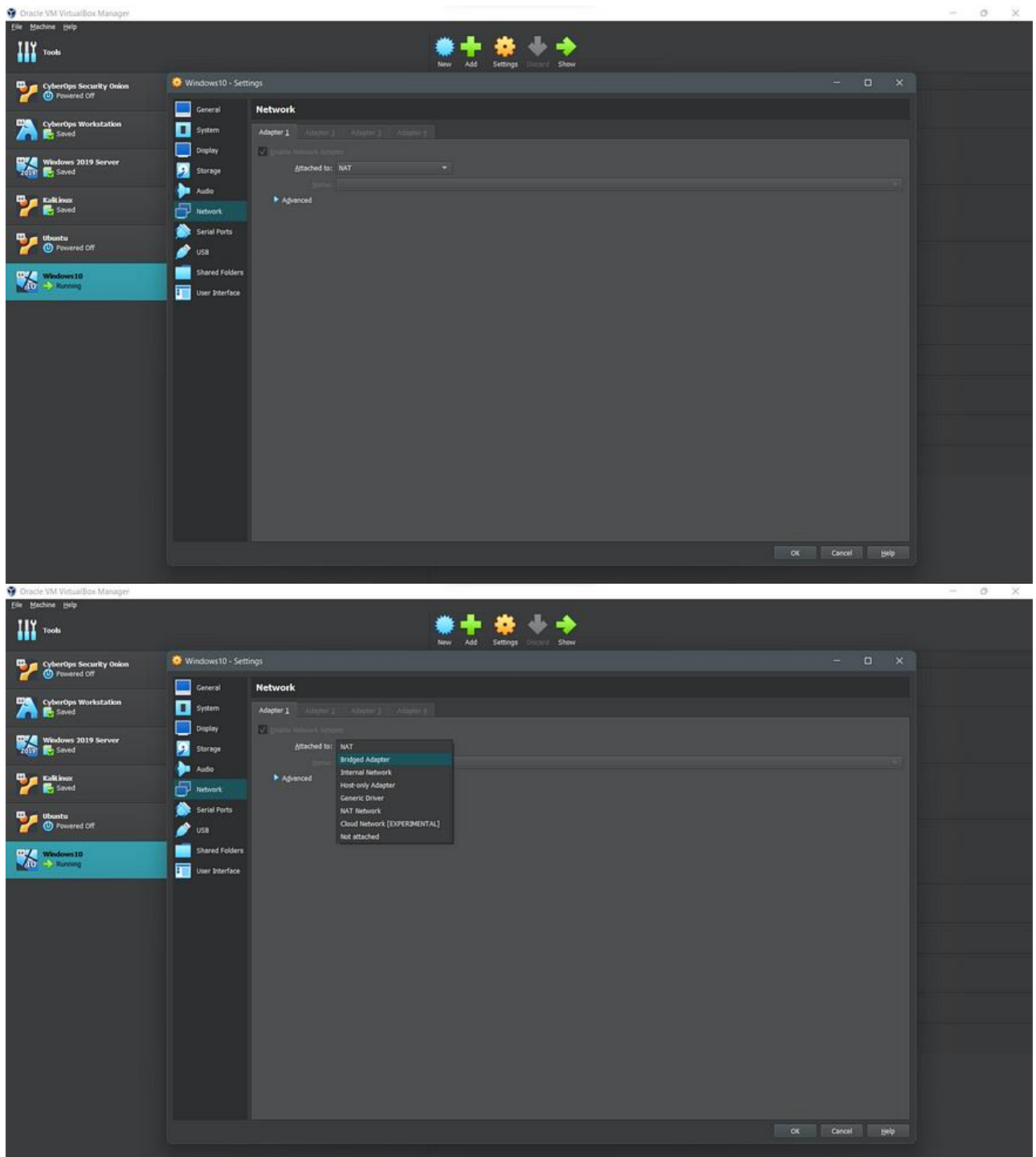


Since I already have my virtual machine installed, there is no need for me to click on “Finish.” However, if you are following along, please click “Finish” to initiate the installation of the Windows operating system.

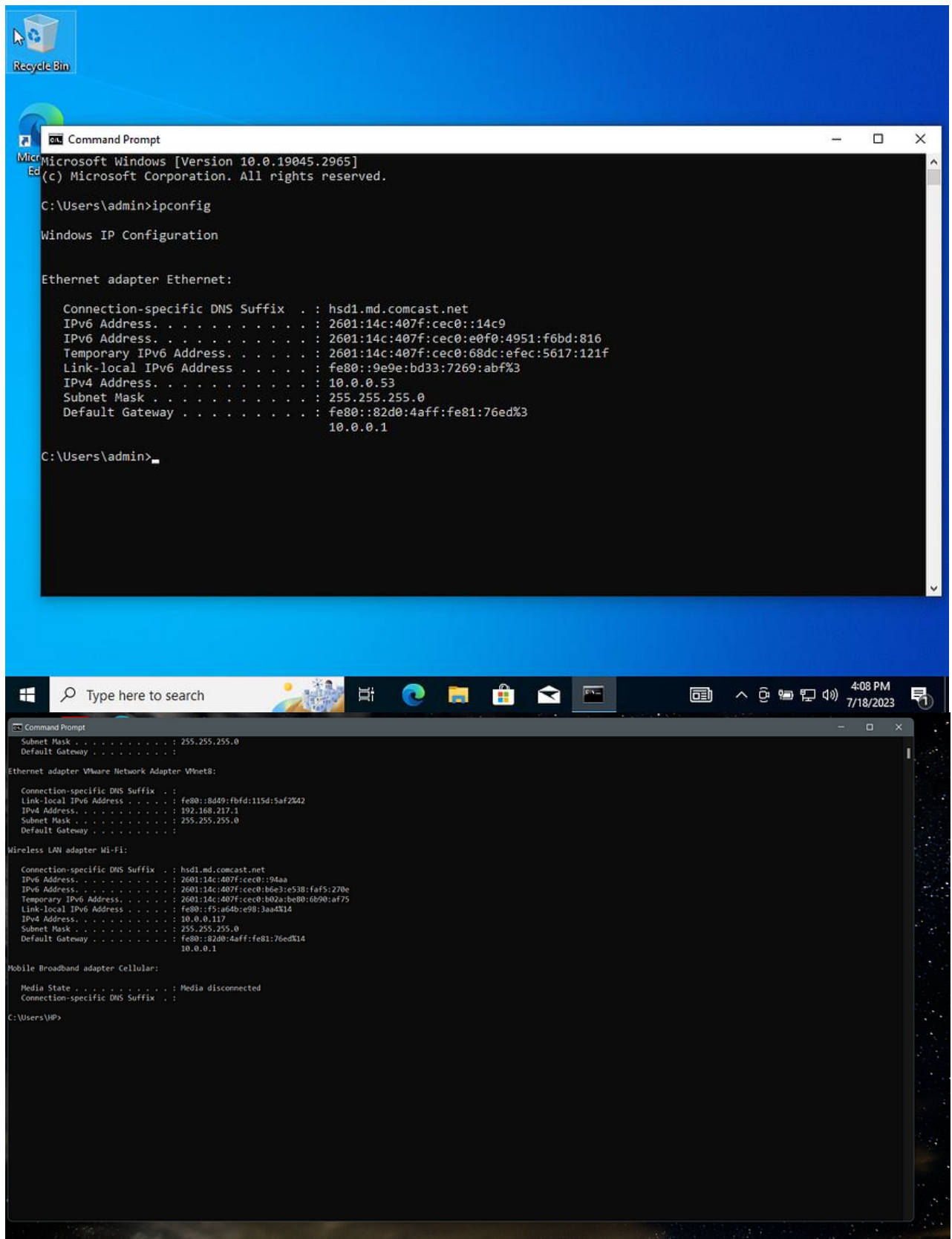


Launched my virtual machine

Next, I will modify the network adapter settings to “Bridged.” This adjustment is crucial as it ensures that my virtual machine is on the same network as my host machine, enabling seamless accessibility for my Nessus implementation. To make this change, I will access the VirtualBox Manager, select my virtual machine, and navigate to the Network settings.



I have successfully bridged my virtual machine network adapter with that of my local host. To verify this configuration, I will compare the IP address of my virtual machine with that of my local host.

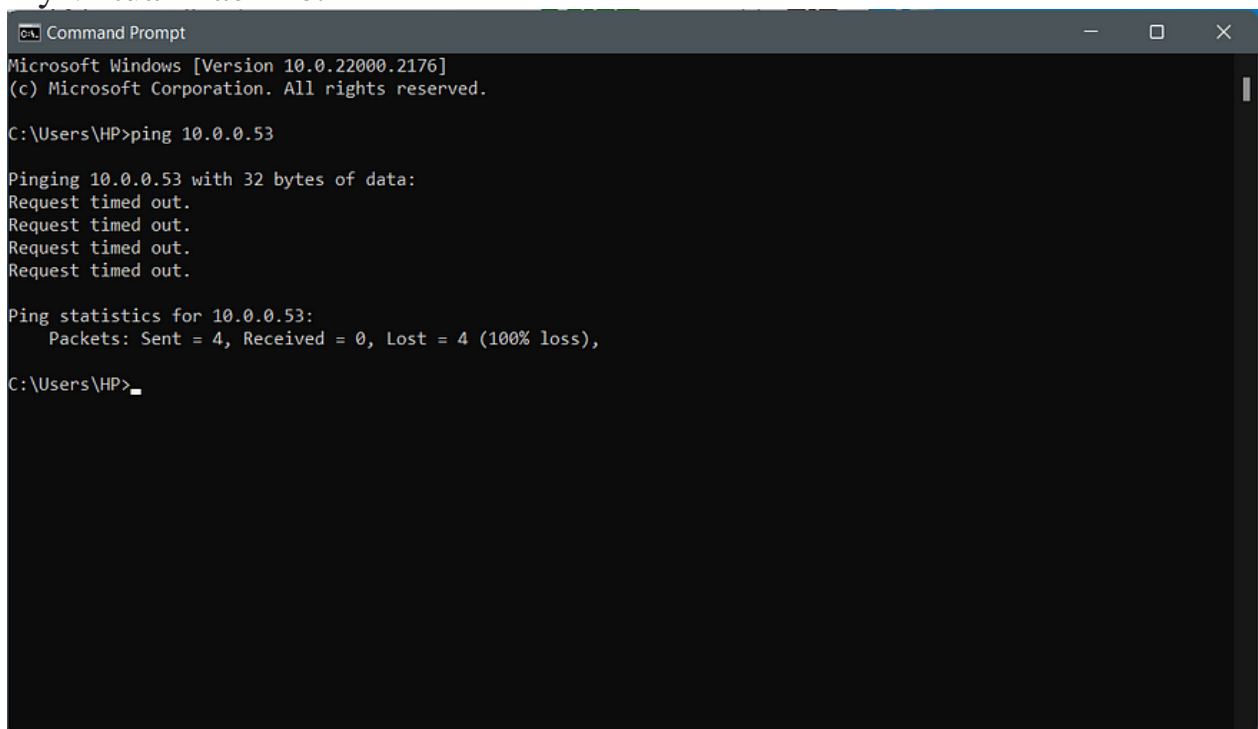


IP Configuration of my host machine.



With an IPv4 address of 10.0.0.53 assigned to my virtual machine and an IPv4 address of 10.0.0.117 assigned to my local host, it is evident that both machines are on the same network. This proves that my Nessus implementation can effectively reach and interact with my virtual machine.

I will then test the connectivity between my local host and my virtual machine. To do this, I will initiate a ping command from my local host to my virtual machine.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text:

```
Microsoft Windows [Version 10.0.22000.2176]
(c) Microsoft Corporation. All rights reserved.

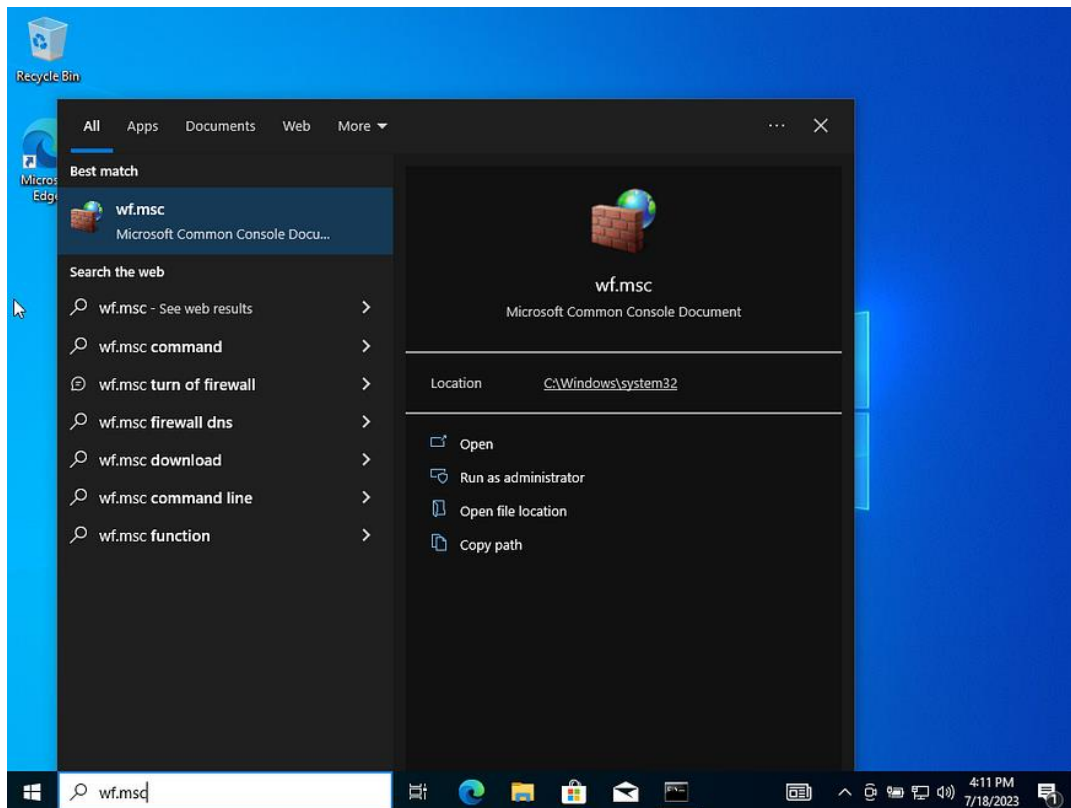
C:\Users\HP>ping 10.0.0.53

Pinging 10.0.0.53 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

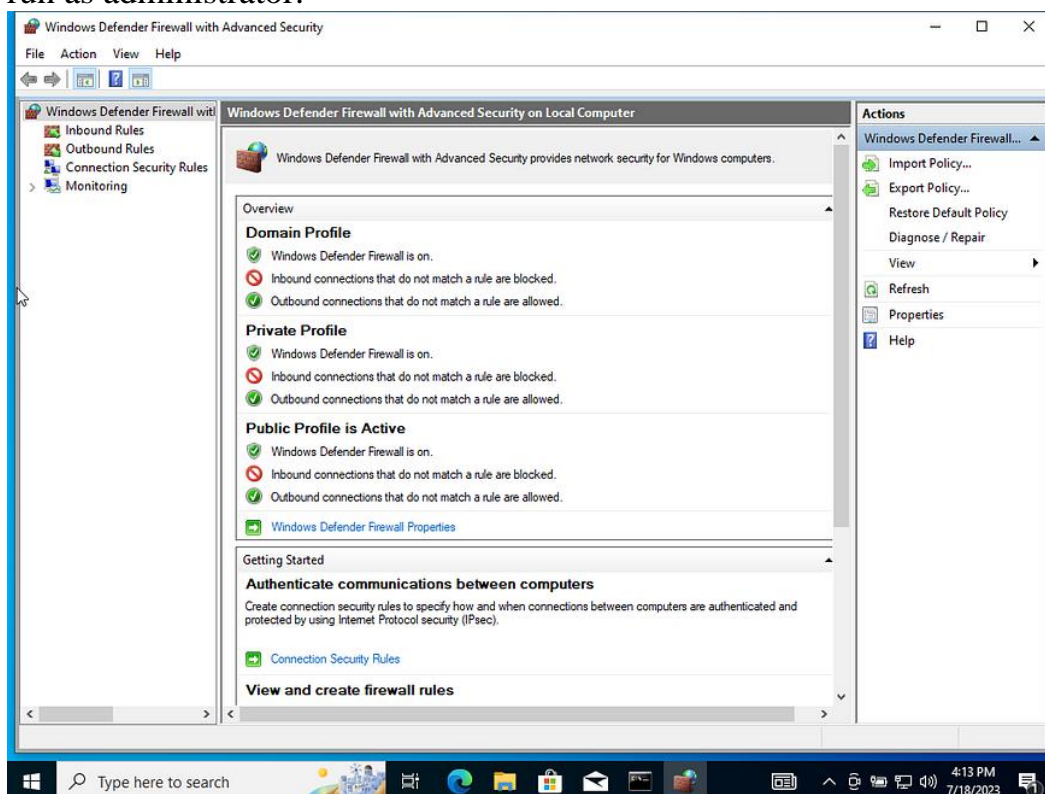
Ping statistics for 10.0.0.53:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\HP>
```

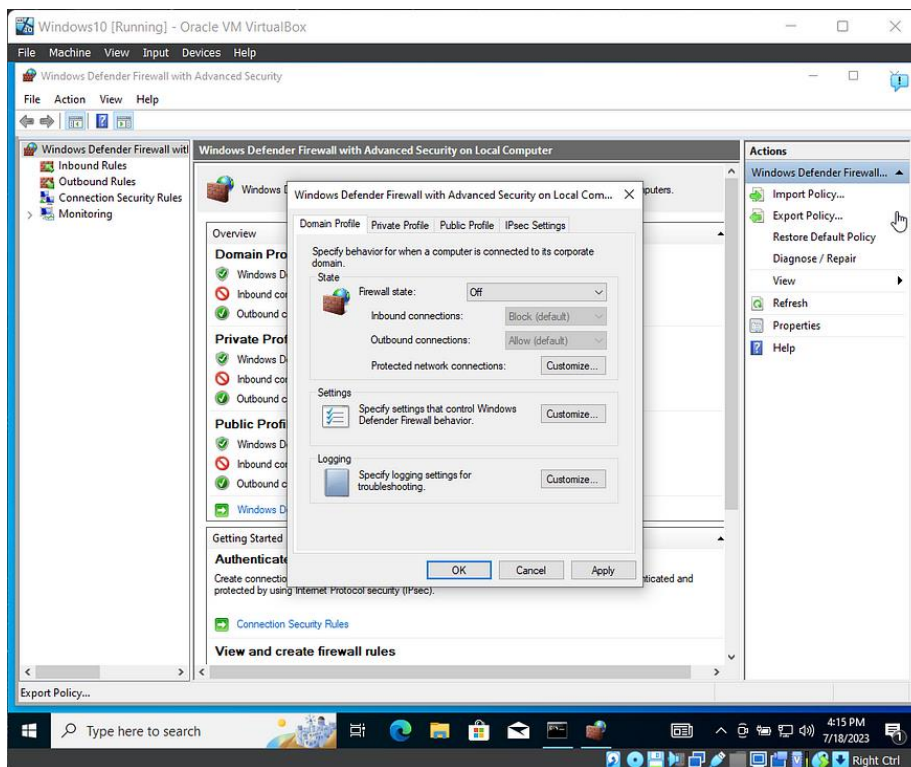
Unfortunately, the ping attempt between my local host and the virtual machine was unsuccessful due to a firewall rule running on my virtual machine. To rectify this issue and enable successful pinging, I will need to make adjustments to the firewall settings on the virtual machine.



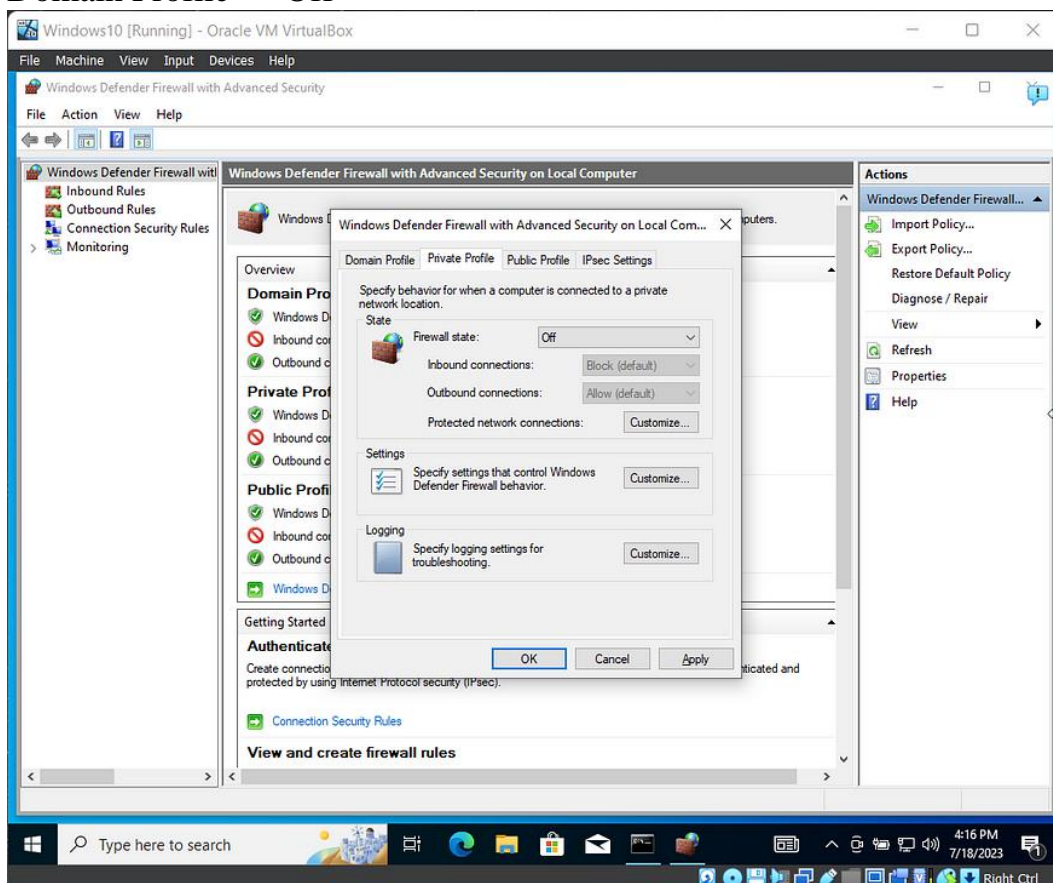
run as administrator.



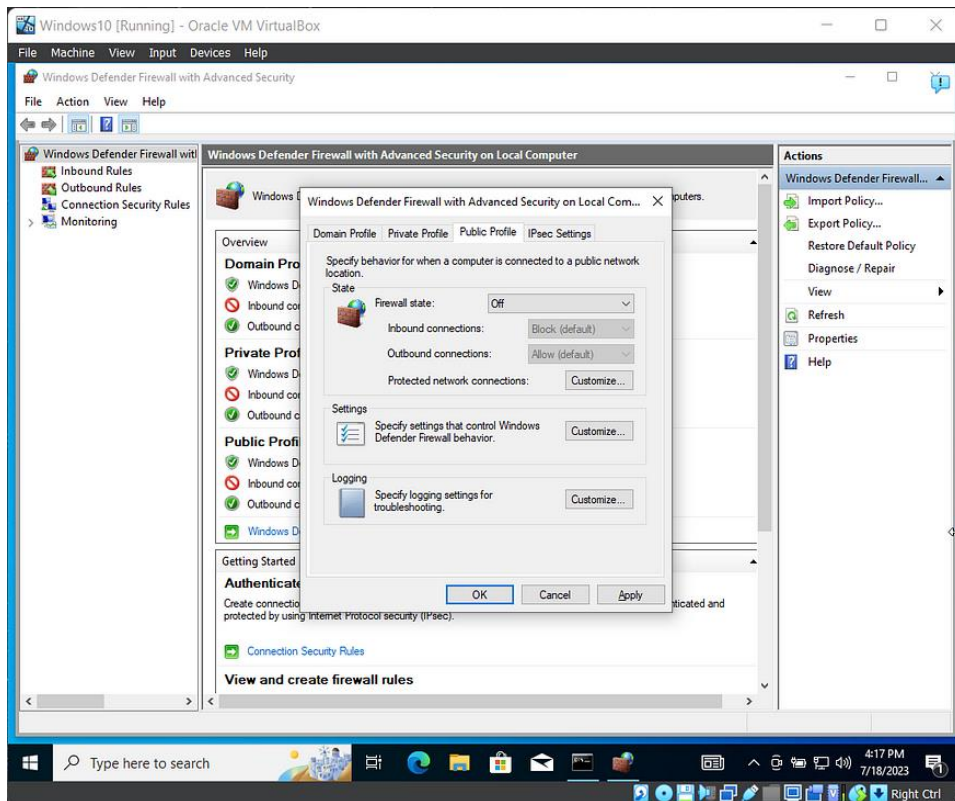
click Windows Defender Firewall Properties



Domain Profile — Off



Private Profile — Off



Public profile — Off

Now that I have successfully disabled the firewall rules that were blocking the ping request, I will proceed to ping my virtual machine once again.

**Note:** Disabling firewall rules is not recommended. If you are working with a virtual machine that contains no confidential data, then you can proceed to follow along. Otherwise, exercise caution and avoid disabling firewall rules on systems containing sensitive information. Make sure to switch the firewall rules back on after the scan has been completed.

```
Microsoft Windows [Version 10.0.22000.2176]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ping 10.0.0.53

Pinging 10.0.0.53 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.53:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\HP>ping 10.0.0.53

Pinging 10.0.0.53 with 32 bytes of data:
Reply from 10.0.0.53: bytes=32 time<1ms TTL=128
Reply from 10.0.0.53: bytes=32 time=1ms TTL=128
Reply from 10.0.0.53: bytes=32 time=1ms TTL=128
Reply from 10.0.0.53: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\HP>
```

Ping successful.

## Scanning with Nessus

Now, the next step is to open Nessus and initiate a basic network scan, specifically a non-credencial scan. Since I already have Nessus installed, I will open the application.



Nessus portal asking for my credentials.

nessus

Essentials

ScansSettings

1

2

1

FilterSearch Hosts1 Host

Host

Vulnerabilities

10.0.0.53

25

My PC Policy

ConfigureAudit TrailLaunchReportExport

Policy: My PC Policy

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:59 PM

End: Today at 6:06 PM

Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

My PC Policy / 10.0.0.53

ConfigureAudit TrailLaunchReportExport

Vulnerabilities12

FilterSearch Vulnerabilities12 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
INFO	...	...	SMB (Mul...	Windows	6	
INFO			DCE Services E...	Plugin ID: 45590	9	
INFO			Common Platf...	General	1	
INFO			Device Type	General	1	
INFO			Ethernet MAC ...	General	1	
INFO			Host Fully Qua...	General	1	
INFO			Nessus Scan I...	Settings	1	
INFO			OS Identificati...	General	1	
INFO			OS Security Pa...	Settings	1	

IP: 10.0.0.53

MAC: 48:F1:7F:4F:4E:D0

08:00:27:AB:DA:9D

OS: Windows

Start: Today at 5:59 PM

End: Today at 6:06 PM

Elapsed: 7 minutes

KB: Download

Vulnerabilities

Critical

High

Medium

Low

Info

Tenable News

Stored Cross-Site Scripting in Craft CMS

Read More

nessus

Essentials

ScansSettings

1

2

1

FilterSearch Hosts1 Host

Host

Vulnerabilities

10.0.0.53

25

My PC Policy

ConfigureAudit TrailLaunchReportExport

Policy: My PC Policy

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:59 PM

End: Today at 6:06 PM

Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Tenable News

Stored Cross-Site Scripting in Craft CMS

Read More

My PC Policy / 10.0.0.53

ConfigureAudit TrailLaunchReportExport

Vulnerabilities12

FilterSearch Vulnerabilities12 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
INFO	...	...	SMB (Mul...	Windows	6	
INFO			DCE Services E...	Plugin ID: 45590	9	
INFO			Common Platf...	General	1	
INFO			Device Type	General	1	
INFO			Ethernet MAC ...	General	1	
INFO			Host Fully Qua...	General	1	
INFO			Nessus Scan I...	Settings	1	
INFO			OS Identificati...	General	1	
INFO			OS Security Pa...	Settings	1	

IP: 10.0.0.53

MAC: 48:F1:7F:4F:4E:D0

08:00:27:AB:DA:9D

OS: Windows

Start: Today at 5:59 PM

End: Today at 6:06 PM

Elapsed: 7 minutes

KB: Download

Vulnerabilities

Critical

High

Medium

Low

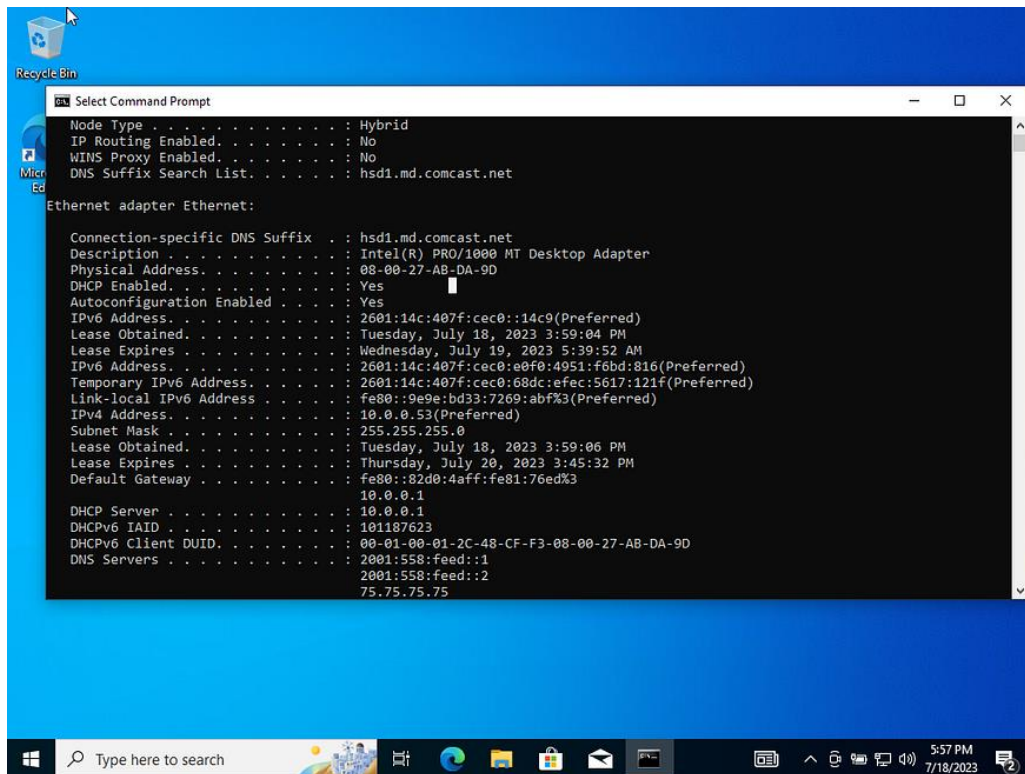
Info

Tenable News

Cross-Site Scripting in Microsoft Teams via Dynami...

Read More





The MAC Address and IPv4 Address of my virtual machine align with the addresses displayed in the scan results, affirming that my virtual machine was indeed successfully scanned.

Next, I will provide Nessus with my Virtual Machine credentials, so a more advanced and accurate vulnerability scan can be carried out, which is known as credentialed scan.

nessusEssentials

ScansSettings

1

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Tenable Cyber Watch: NAIAC Submits First Report to...

Read More

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Windows 10 Basic Scan

Description

Folder

My Scans

Targets

10.0.0.53

Upload Targets

Add File

Save

Cancel

nessusEssentials

ScansSettings

1

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

CVE-2023-3595, CVE-2023-3596: Rockwell Automation ...

Read More

Credentialed VM Policy

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts

Vulnerabilities

Remediations

History

Filter

Search Hosts

1 Host

Host

Vulnerabilities

10.0.0.53

145

162

Scan Details

Policy: Credentialed VM Policy

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 6:40 PM

End: Today at 6:51 PM

Elapsed: 11 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

## credentialed scan result

nessusEssentials

ScansSettings

1

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Stored Cross-Site Scripting in Craft CMS

Read More

Credentialed VM Policy / 10.0.0.53

[Back to Hosts](#)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

40

Filter

Search Vulnerabilities

40 Vulnerabilities

Sev

CVSS

VPR

Name

Count

MIXED

...

...

Microsoft... Windows : Microsoft Bulletins

5

MIXED

...

...

Microsoft... Windows

3

HIGH

8.1

6.7

Security Upda... Windows : Microsoft Bulletins

1

MIXED

...

...

Microsoft... Windows

89

MEDIUM

5.3

...

SMB Signing n... Misc.

1

LOW

3.3

2.2

Windows Snip... Windows

1

INFO

...

...

SMB (Mul... Windows

17

INFO

...

...

Windows... Windows

3

INFO

...

...

Microsoft... Windows

2

Host Details

IP: 10.0.0.53

MAC: 48:F1:7F:4F:4E:D0

OS: Microsoft Windows 10 Pro Build 19045

Start: Today at 6:40 PM

End: Today at 6:51 PM

Elapsed: 11 minutes

KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info



## Credentialed scan result

By providing Nessus with my virtual machine credentials, it has been able to uncover additional vulnerabilities. Providing Nessus with my virtual machine credentials is important in enabling it to reach certain depths that would have otherwise been inaccessible without these credentials.

The comparison between the scan results (Credential scan) and my previous scan (Non-credential scan) highlights the remarkable accuracy that credential scans offer over non-credential scans.

### **Credentialed Scan Result:**

**Critical — 3 (1.62%)**

**High — 14 (7.57%)**

**Medium — 5 (2.70%)**

**Low — 1 (0.54%)**

**Info — 162 (87.57%)**

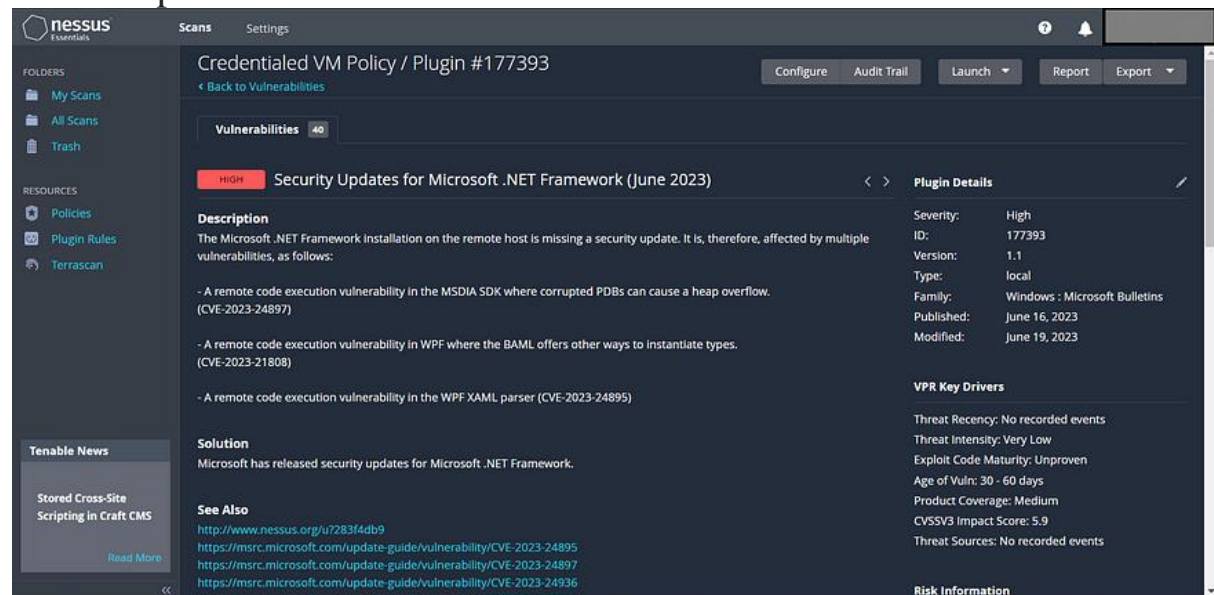
### **Non-Credentialed Scan Result**

**Info — 25 (100%)**

In a typical scan result, you can expect to find detailed information about the specific vulnerability, including its severity level, suggested

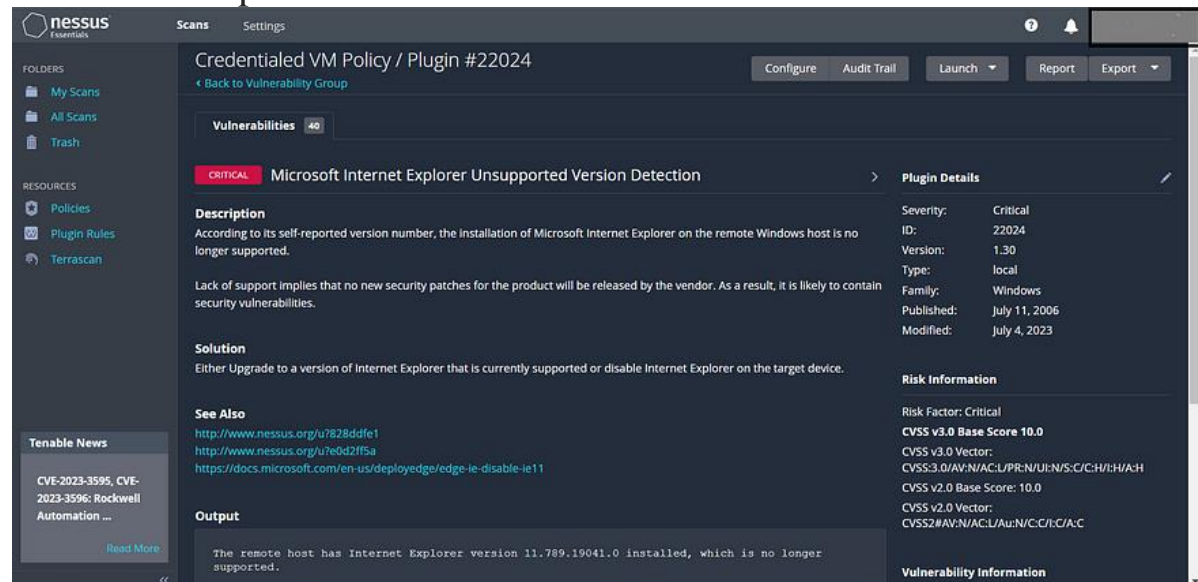
remediation steps, and other pertinent details relating to the identified vulnerability.

An example can be seen below



The screenshot displays the Nessus Essentials interface. The left sidebar shows the navigation menu with folders like 'My Scans', 'All Scans', and 'Trash', and resources like 'Policies', 'Plugin Rules', and 'Terrascan'. The main content area is titled 'Credentialed VM Policy / Plugin #177393'. It shows a 'Vulnerabilities' count of 40. The selected vulnerability is 'Security Updates for Microsoft .NET Framework (June 2023)' with a 'HIGH' severity. The description states that the Microsoft .NET Framework installation is missing a security update, affecting multiple vulnerabilities. The solution is to install the security updates released by Microsoft. The 'See Also' section provides links to Nessus.org and Microsoft update guides. The 'Plugin Details' section on the right lists attributes: Severity: High, ID: 177393, Version: 1.1, Type: local, Family: Windows : Microsoft Bulletins, Published: June 16, 2023, and Modified: June 19, 2023. The 'Risk Information' section shows threat recency, intensity, and maturity.

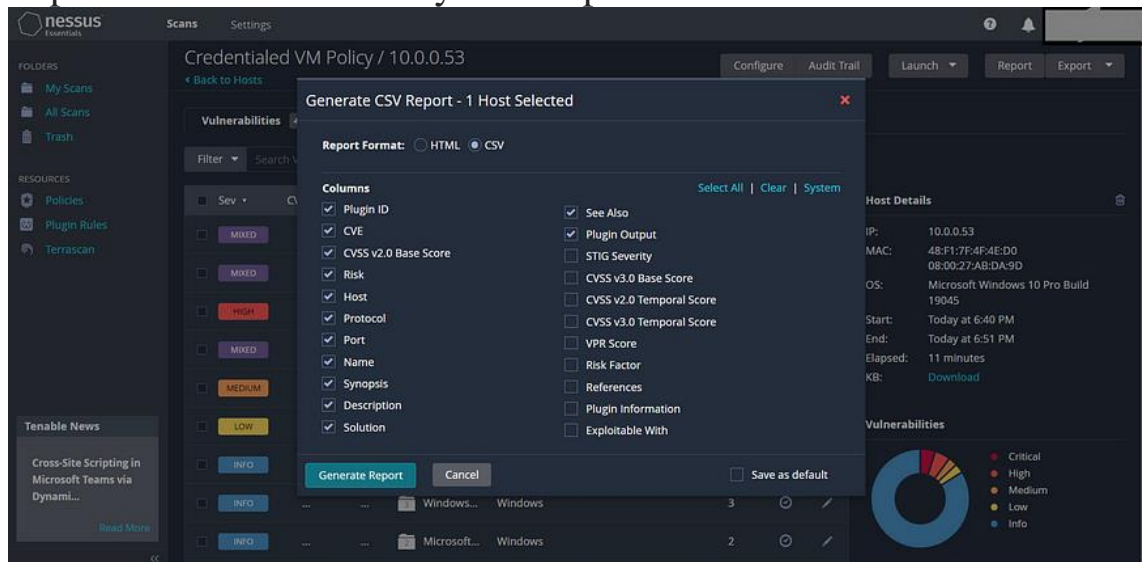
Another example



The screenshot displays the Nessus Essentials interface for a different vulnerability. The left sidebar is the same. The main content area is titled 'Credentialed VM Policy / Plugin #22024'. It shows a 'Vulnerabilities' count of 40. The selected vulnerability is 'Microsoft Internet Explorer Unsupported Version Detection' with a 'CRITICAL' severity. The description states that the installation of Microsoft Internet Explorer on the remote Windows host is no longer supported. The solution is to upgrade to a supported version or disable Internet Explorer. The 'See Also' section provides links to Nessus.org and Microsoft deployment guides. The 'Plugin Details' section on the right lists attributes: Severity: Critical, ID: 22024, Version: 1.30, Type: local, Family: Windows, Published: July 11, 2006, and Modified: July 4, 2023. The 'Risk Information' section shows a risk factor of Critical, a CVSS v3.0 Base Score of 10.0, and a CVSS v2.0 Base Score of 10.0. The 'Output' section shows the remote host has Internet Explorer version 11.789.19041.0 installed, which is no longer supported.

Vulnerability scan results can be exported either as HTML or CSV files. The primary purpose of exporting these scan results is to simplify the process of documentation and share the findings with the relevant parties

accountable for remediation. This streamlined approach enhances communication and ensures that necessary actions are taken to address and improve the overall security landscape.



A typical exported csv vulnerability scan result would look like this

	A	B	C	D	E	F	G	H	I	J	K	L	M
	Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
1	10150		None	10.0.0.53	udp	137	Windows NetBIOS / SMB Remote Host Info	It was possible to obtain the network name	The remote host is	n/a			The following 3
2	10287		None	10.0.0.53	udp	0	Traceroute Information	It was possible to obtain traceroute information	Makes a traceroute	n/a			For your
3	10394		None	10.0.0.53	tcp	445	Microsoft Windows SMB Log In Possible	It was possible to log into the remote host	The remote host is	n/a		<a href="http://www.nessus.com">http://www.nessus.com</a>	- The SMB tests will
4	10395		None	10.0.0.53	tcp	445	Microsoft Windows SMB Shares Enumeration	It is possible to enumerate remote network	By connecting to	n/a			
5	10396		None	10.0.0.53	tcp	445	Microsoft Windows SMB Shares Access	It is possible to access a network share	The remote has	To restrict access			
6	10400		None	10.0.0.53	tcp	445	Microsoft Windows SMB Registry Remotely	Access the remote Windows Registry	It was possible to	n/a			
7	10456		None	10.0.0.53	tcp	445	Microsoft Windows SMB Service Enumeration	It is possible to enumerate remote services	This plugin	To prevent the listing			
8	10736		None	10.0.0.53	tcp	135	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
9	10736		None	10.0.0.53	tcp	445	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
10	10736		None	10.0.0.53	tcp	49664	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
11	10736		None	10.0.0.53	tcp	49665	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
12	10736		None	10.0.0.53	tcp	49666	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
13	10736		None	10.0.0.53	tcp	49667	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
14	10736		None	10.0.0.53	tcp	49668	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
15	10736		None	10.0.0.53	tcp	49669	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
16	10736		None	10.0.0.53	tcp	49670	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
17	10736		None	10.0.0.53	tcp	49671	DCE Services Enumeration	A DCE/RPC service is running on the remote	By sending a	n/a			
18	10785		None	10.0.0.53	tcp	445	Microsoft Windows SMB NativeLanManager	It was possible to obtain information about	Nessus was able to	n/a			Nessus was able to
19	10859		None	10.0.0.53	tcp	445	Microsoft Windows SMB LsaQueryInformation	It is possible to obtain the host SID for the remote	By emulating the	You can prevent	<a href="http://technet.microsoft.com">http://technet.microsoft.com</a>		
20	10902		None	10.0.0.53	tcp	445	Microsoft Windows 'Administrators' Group	There is at least one user in the 'Administrators' group	Using the supplied	Verify that each member of the group should			
21	11011		None	10.0.0.53	tcp	139	Microsoft Windows SMB Service Detection	A file / print sharing service is listening on the remote	The remote	n/a			
22	11011		None	10.0.0.53	tcp	445	Microsoft Windows SMB Service Detection	A file / print sharing service is listening on the remote	The remote	n/a			
23	11457		None	10.0.0.53	tcp	445	Microsoft Windows SMB Registry : Winlogon	User credentials are stored in memory	The registry key	Consult Microsoft documentation	<a href="http://www.nessus.com">http://www.nessus.com</a>		
24	11777		None	10.0.0.53	tcp	445	Microsoft Windows SMB Share Hosting Poss	The remote host may contain material	This plugin displays	Delete the files infringing copyright			
25	11936		None	10.0.0.53	tcp	0	OS Identification	It is possible to guess the remote operating system	Using a	n/a			
26	12053		None	10.0.0.53	tcp	0	Host Fully Qualified Domain Name (FQDN)	It was possible to resolve the name of the remote host	Nessus was able to	n/a			
27	16193		None	10.0.0.53	tcp	445	Antivirus Software Check	An antivirus application is installed on the remote host	An antivirus	n/a		<a href="http://www.nessus.com">http://www.nessus.com</a>	The following
28	17651		None	10.0.0.53	tcp	445	Microsoft Windows SMB : Obtain the Password	It is possible to retrieve the remote host's password	Using the supplied	n/a			Information about
29	19506		None	10.0.0.53	tcp	0	Nessus Scan Information	This plugin displays information about the Nessus scan	This plugin	n/a			

They can be filtered based on various metrics. The most used metric used in filtering vulnerability scan results is the risk or Severity metric.



This is an example:

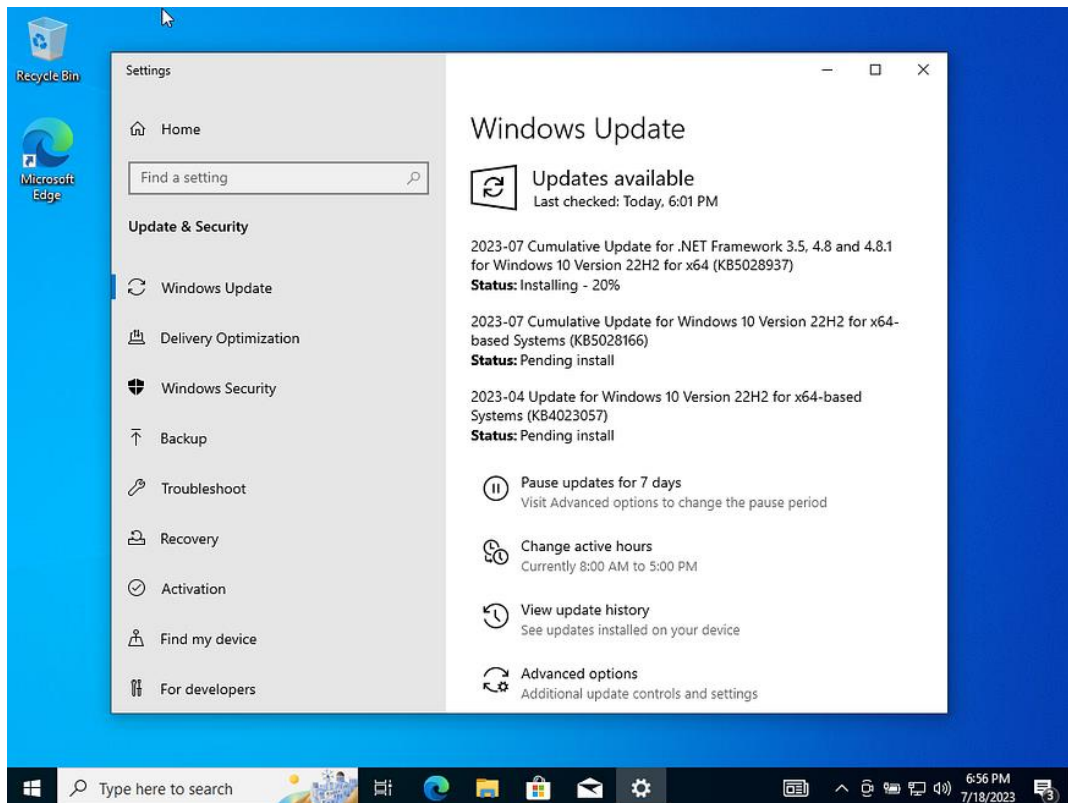
Plugin ID	CVE	CVSS v2	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
137				10.0.0.53	udp		Windows NetBIOS / SMB Remote Host Information	It was possible to obtain the network name of the remote host.	The remote host is n/a	n/a		The following 3
0				10.0.0.53	udp		Traceroute Information	It was possible to obtain traceroute information from the remote host.	Makes a traceroute n/a	n/a		For your
445				10.0.0.53	tcp		Microsoft Windows SMB Log In Possible	It was possible to log into the remote host.	The remote host is n/a	n/a	<a href="http://www.nessus.org">http://www.nessus.org</a>	The SMB tests will
445				10.0.0.53	tcp		Microsoft Windows SMB Shares Enumeration	It is possible to enumerate remote network shares by connecting to the remote host.	The remote host is n/a	To restrict access		
445				10.0.0.53	tcp		Microsoft Windows SMB Shares Access	It is possible to access a network share.	The remote host is n/a	To prevent the listing		
445				10.0.0.53	tcp		Microsoft Windows SMB Registry Remotely Access	Access the remote Windows Registry.	It was possible to n/a	n/a		
445				10.0.0.53	tcp		Microsoft Windows SMB Service Enumeration	It is possible to enumerate remote services.	This plugin n/a	n/a		
135				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
445				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49664				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49665				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49666				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49667				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49668				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49669				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
49671				10.0.0.53	tcp		DCE Services Enumeration	A DCE/RPC service is running on the remote host.	By sending a n/a	n/a		
445				10.0.0.53	tcp		Microsoft Windows SMB Native LanManager	It was possible to obtain information about the remote host's LAN Manager status.	Nessus was able to n/a	Nessus was able to		
445				10.0.0.53	tcp		Microsoft Windows SMB LsaQueryInformation	It was possible to obtain the host SID for the remote host by emulating the LAN Manager protocol.	You can prevent n/a	<a href="http://technet.microsoft.com">http://technet.microsoft.com</a>		
445				10.0.0.53	tcp		Microsoft Windows Administrators' Group L	There is at least one user in the 'Administrators' group on the remote host.	Using the supplied n/a	Verify that each member of the group should have the following information about		
139				10.0.0.53	tcp		Microsoft Windows SMB Service Detection	A file / print sharing service is listening on the remote host.	The remote host is n/a	n/a		
445				10.0.0.53	tcp		Microsoft Windows SMB Service Detection	A file / print sharing service is listening on the remote host.	The remote host is n/a	n/a		
445				10.0.0.53	tcp		Microsoft Windows SMB Registry : Winlogon	User credentials are stored in memory.	The registry key n/a	Consult Microsoft documentation: <a href="http://www.nessus.org">http://www.nessus.org</a>		
445				10.0.0.53	tcp		Microsoft Windows SMB Share Hosting Poss	The remote host may contain material that is not intended to be shared.	This plugin displays n/a	Delete the files infringing copyright.		
0				10.0.0.53	tcp		OS Identification	It is possible to guess the remote operating system.	Using a n/a	n/a		
0				10.0.0.53	tcp		Host Fully Qualified Domain Name (FQDN) Resolution	It was possible to resolve the name of the remote host.	Nessus was able to n/a	n/a		
445				10.0.0.53	tcp		Antivirus Software Check	An antivirus application is installed on the remote host.	The remote host is n/a	<a href="http://www.nessus.org">http://www.nessus.org</a>		
445				10.0.0.53	tcp		Microsoft Windows SMB : Obtains the Password	It is possible to retrieve the remote host's password.	Using the supplied n/a	n/a		
0				10.0.0.53	tcp		Nessus Scan Information	This plugin displays information about the Nessus scan.	The remote host is n/a	n/a		
445				10.0.0.53	tcp		Microsoft Windows Installed Software Enumeration	It is possible to enumerate installed software on the remote host.	This plugin lists n/a	Remove any n/a	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Microsoft Internet Explorer Unsupported Versions	The remote host contains an unsupported version of Internet Explorer.	According to its n/a	Either Upgrade to a n/a	<a href="http://www.nessus.org">http://www.nessus.org</a>	

Plugin ID	CVE	CVSS v2	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
140596	CVE-2020-140596	6.9	High	10.0.0.53	tcp		Microsoft Windows WebP Image Extension L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
141430	CVE-2020-141430	9.3	High	10.0.0.53	tcp		Microsoft 3D Viewer Base3D Code Execution	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Microsoft 3D Viewer app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
141430	CVE-2020-141430	9.3	High	10.0.0.53	tcp		Microsoft 3D Viewer Base3D Code Execution	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Microsoft 3D Viewer app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft Windows VP9 Video Extensions L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows 'VP9' app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft Windows Web Media Extensions L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft 3D Viewer Multiple Vulnerabilities	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows '3D' app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft 3D Viewer Multiple Vulnerabilities	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows '3D' app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft Windows VP9 Video Extensions L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows 'VP9' app installed on the remote host.	Upgrade to app version <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft 3D Viewer Multiple Vulnerabilities	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the version of the app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft 3D Viewer Multiple Vulnerabilities	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the version of the app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft Windows VP9 Video Extensions L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows 'VP9' app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft Windows HEIF Image Extensions L	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows 'HEIF' app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft Paint 3D Code Execution (March 2)	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
445				10.0.0.53	tcp		WinVerifyTrust Signature Validation CVE-201	The remote Windows host is potentially misconfigured.	The remote host is n/a	Add and enable n/a	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
445				10.0.0.53	tcp		Security Updates for Microsoft .NET Framework	The Microsoft .NET Framework installation on the remote host is outdated.	The Microsoft .NET Framework installation on the remote host.	Microsoft has released <a href="http://www.nessus.org">http://www.nessus.org</a>	<a href="http://www.nessus.org">http://www.nessus.org</a>	
0				10.0.0.53	tcp		Microsoft Paint 3D Code Execution (July 202)	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	
0				10.0.0.53	tcp		Microsoft Paint 3D Code Execution (July 202)	The Windows app installed on the remote host is vulnerable to a buffer overflow.	In the Windows app installed on the remote host.	Upgrade to app version <a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>	

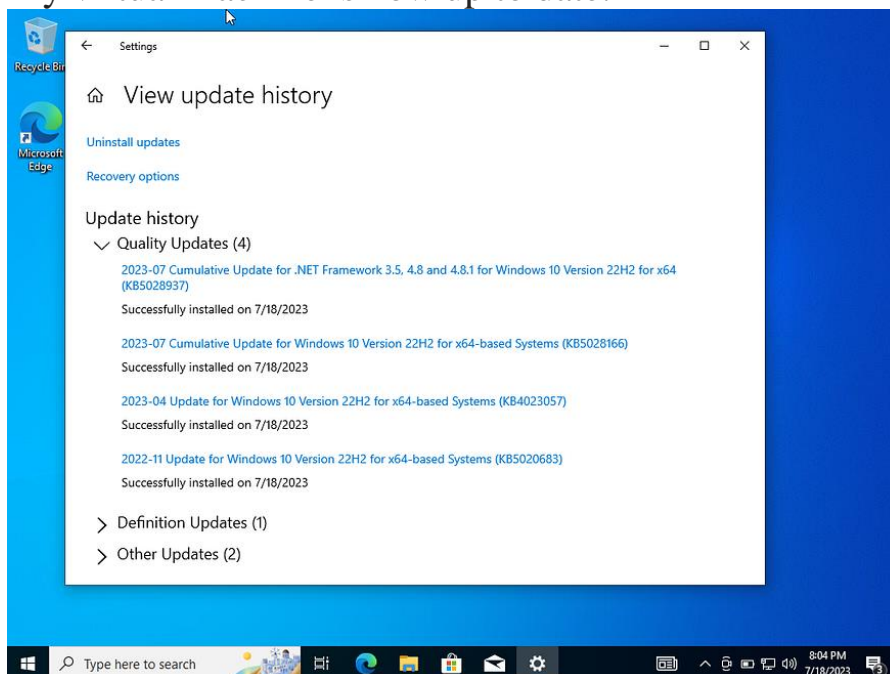
Filtered result based on High Risk.





Updating my virtual machine.

My virtual machine is now up to date.





## **conclusion**

After completing the update process for my virtual machine, its security has significantly improved. This reaffirms the vital importance of keeping operating systems and applications up to date on a regular basis. These updates frequently include essential security bug fixes that play a vital role in safeguarding your system against potential vulnerabilities and threats.