Vulnerability Management with Nessus

By
Seenuvasan

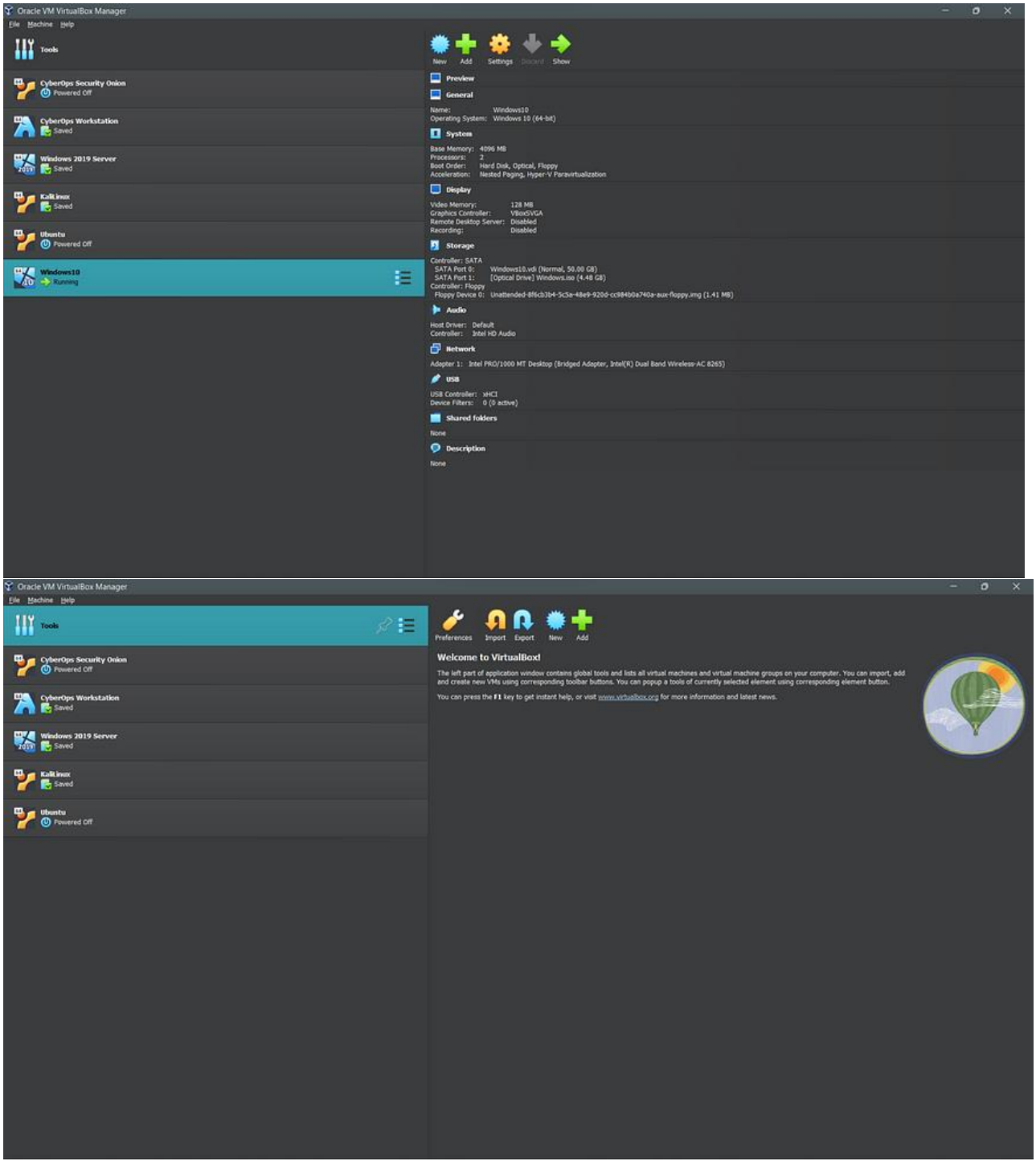
Setting up the virtual box

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

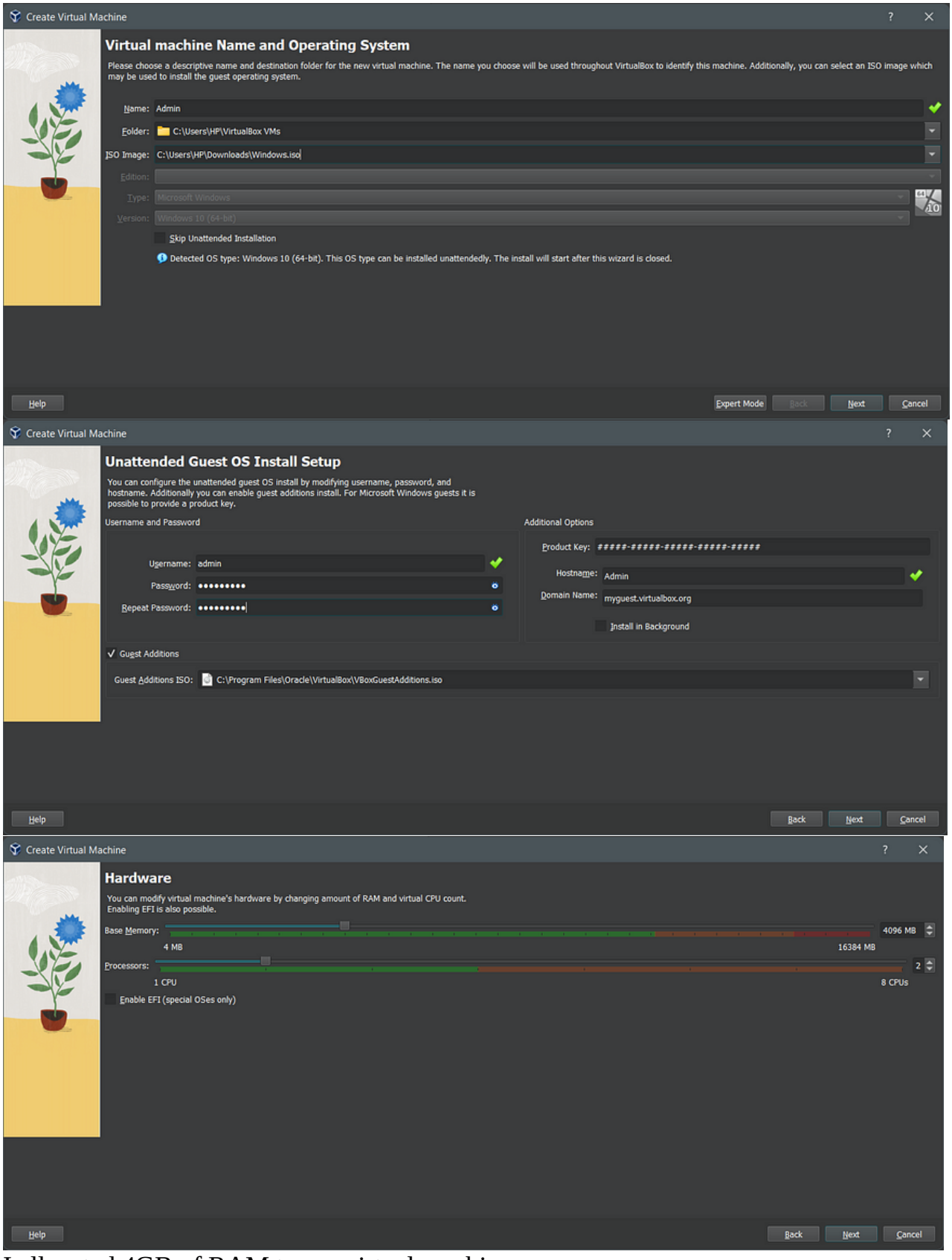
1. Oracle VirtualBox: For this exercise, VirtualBox will act as the hypervisor. To put it simply for those unfamiliar with technical terms, a hypervisor is software that enables the creation and operation of virtual machines (VMs). It allows a single host computer to accommodate multiple guest VMs by 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.

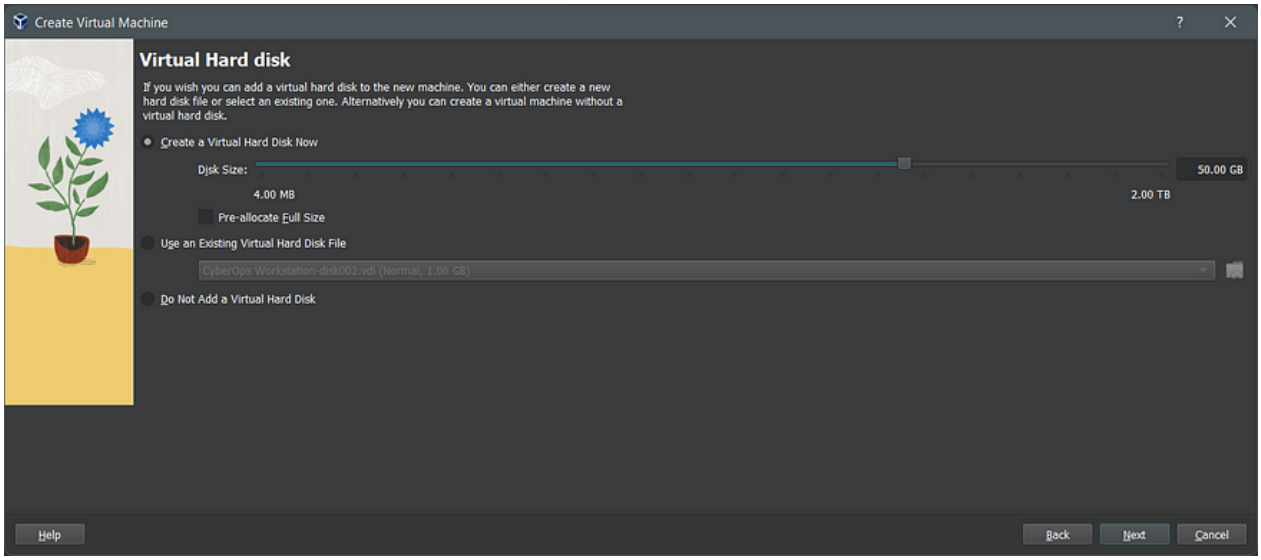
First tool I am going to make use of is VirtualBox. I already have my Virtualbox installed, but incase you want to follow along.If you wish to follow along, start by launching VirtualBox and installing a virtual machine, which will be your target for this exercise.



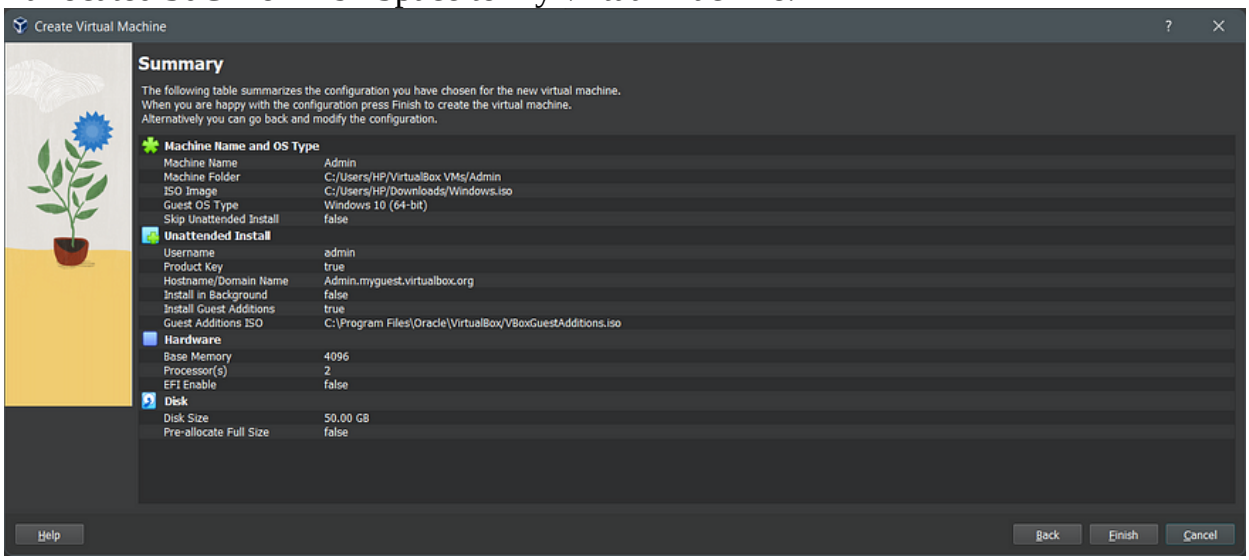
proceed with the installation of your virtual machine.



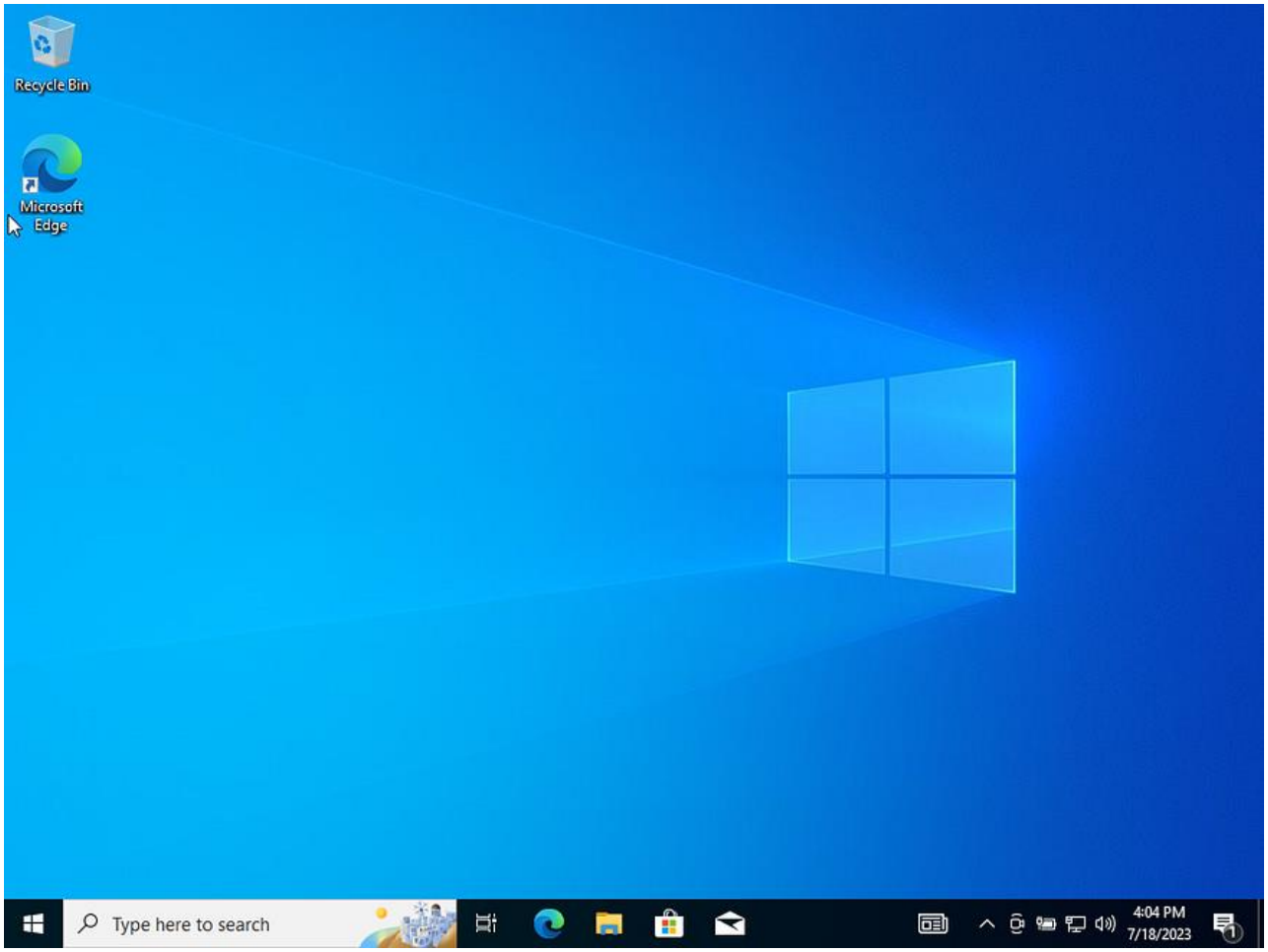
I allocated 4GB of RAM to my virtual machine.



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

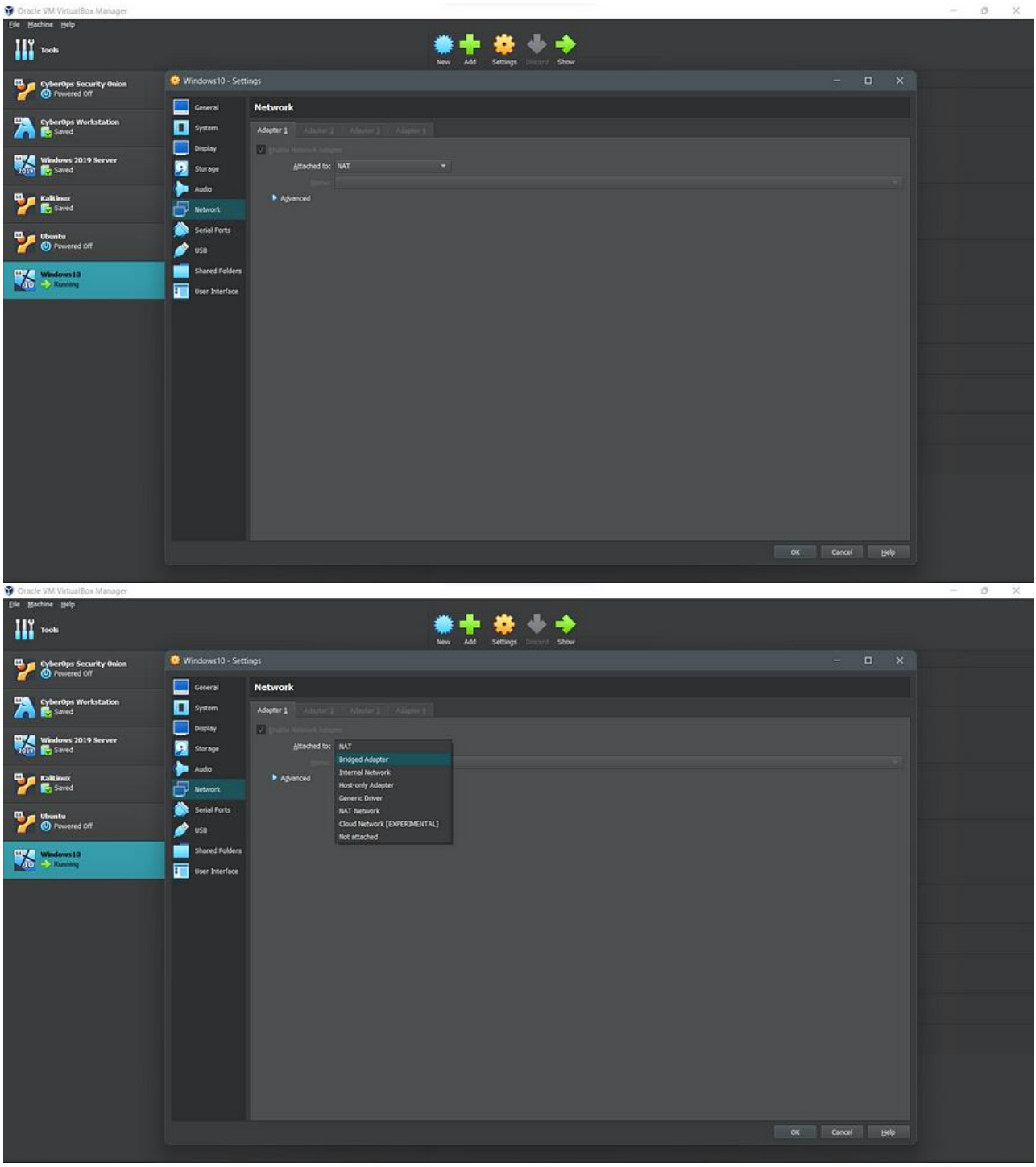


Since I already have my virtual machine installed, there is no need for me to click on “Finish.” However, if you are following along, please click “Finish” to initiate the installation of the Windows operating system.

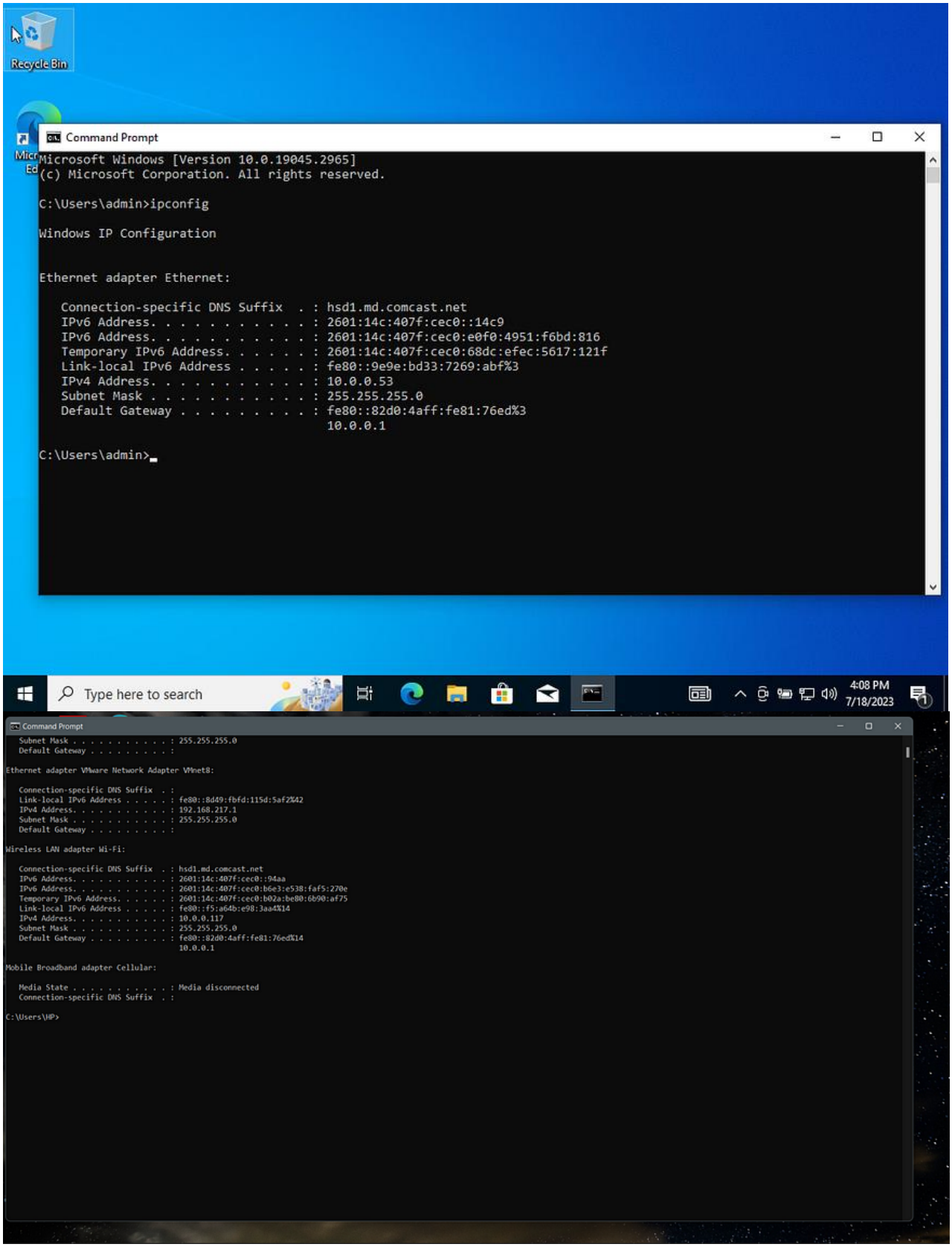


Launched my virtual machine

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.



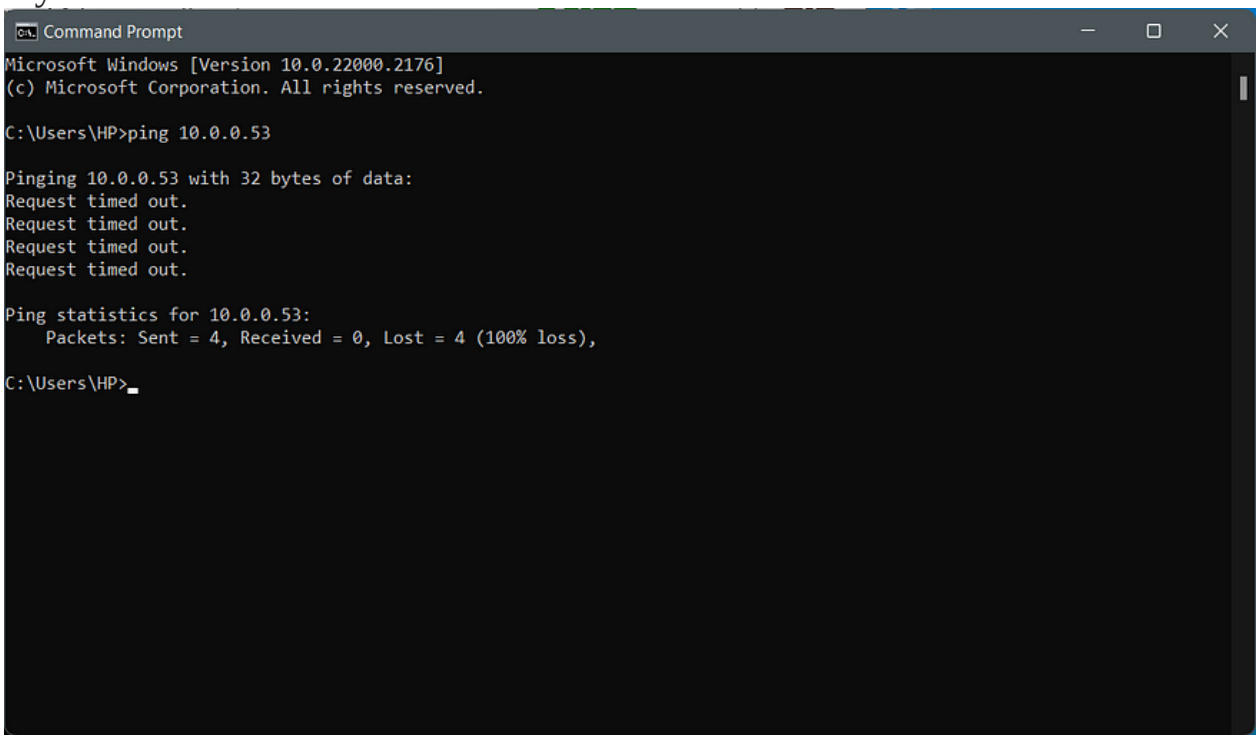
I have successfully bridged my virtual machine network adapter with that of my local host. To verify this configuration, I will compare the IP address of my virtual machine with that of my local host.



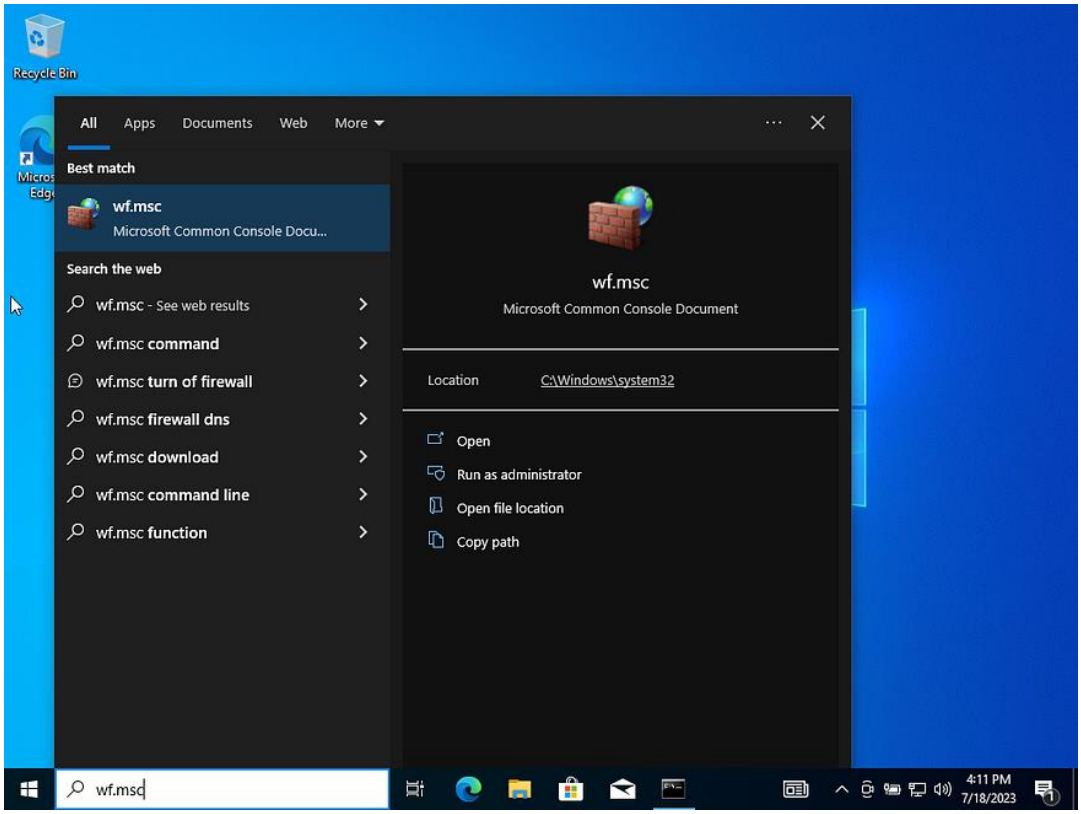
IP Configuration of my host machine.

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.

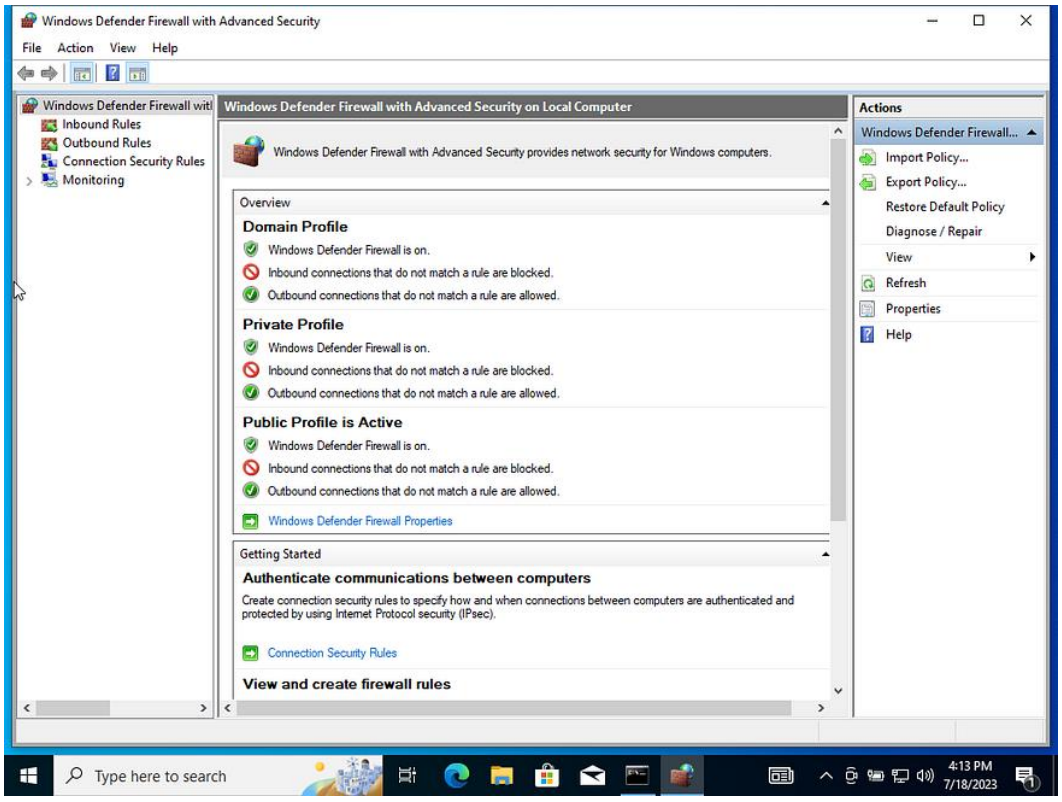
I will then test the connectivity between my local host and my virtual machine. To do this, I will initiate a ping command from my local host to my virtual machine.



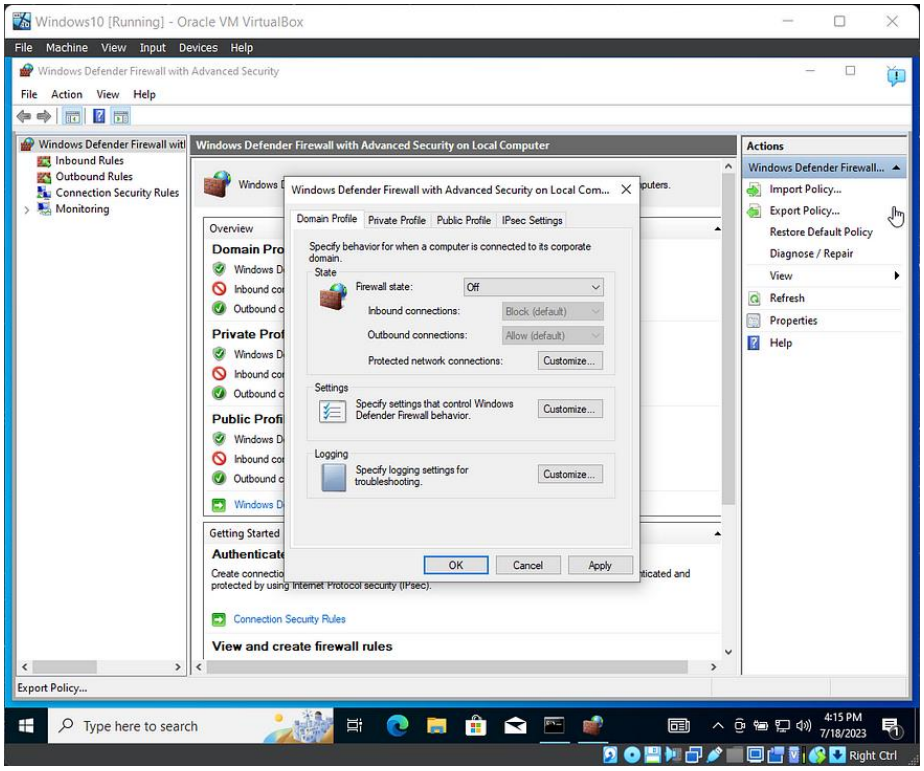
Unfortunately, the ping attempt between my local host and the virtual machine was unsuccessful due to a firewall rule running on my virtual machine. To rectify this issue and enable successful pinging, I will need to make adjustments to the firewall settings on the virtual machine.



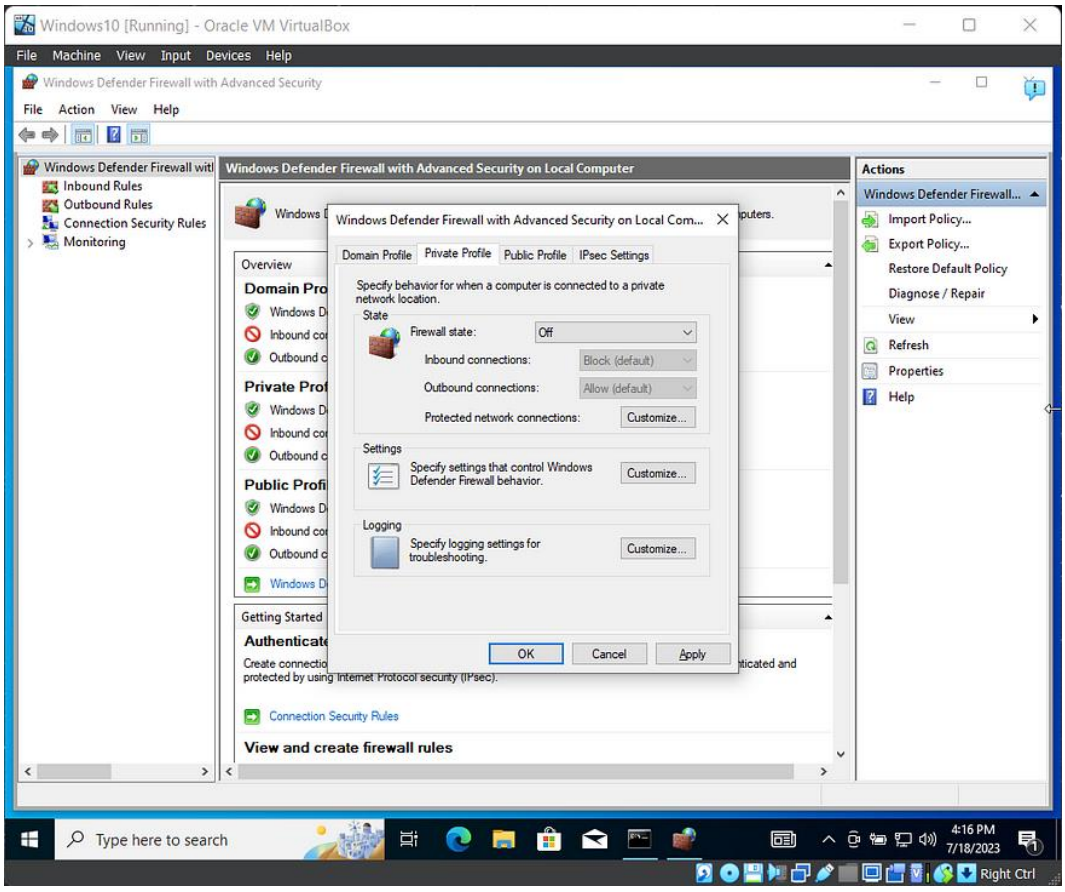
run as administrator.



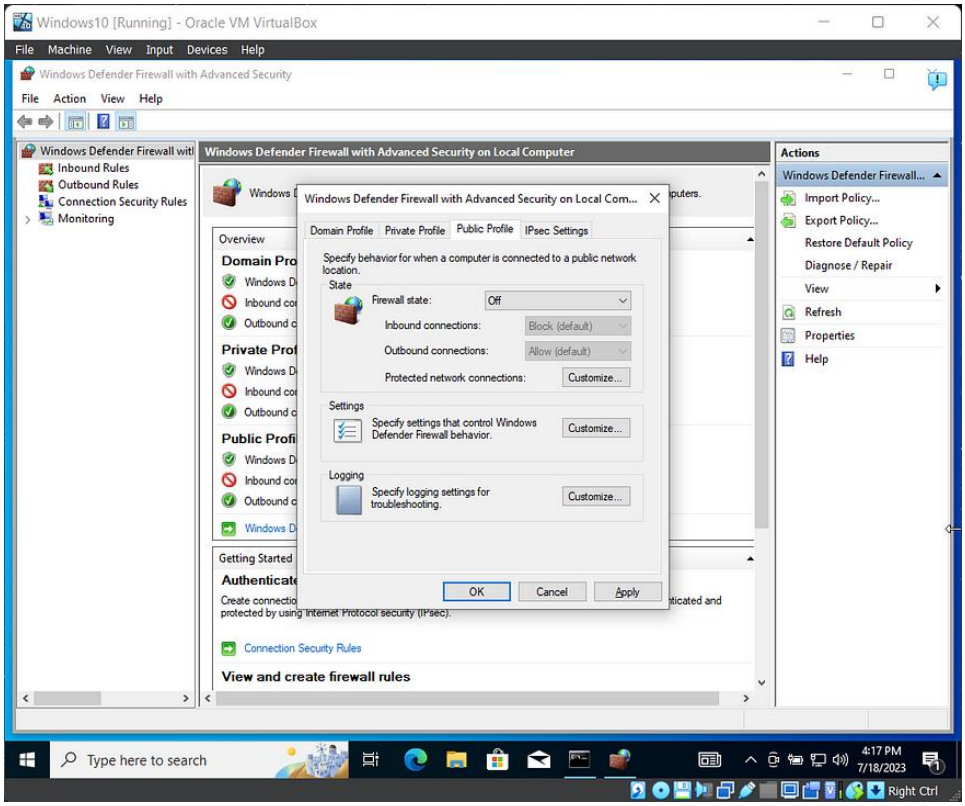
click Windows Defender Firewall Properties



Domain Profile — Off



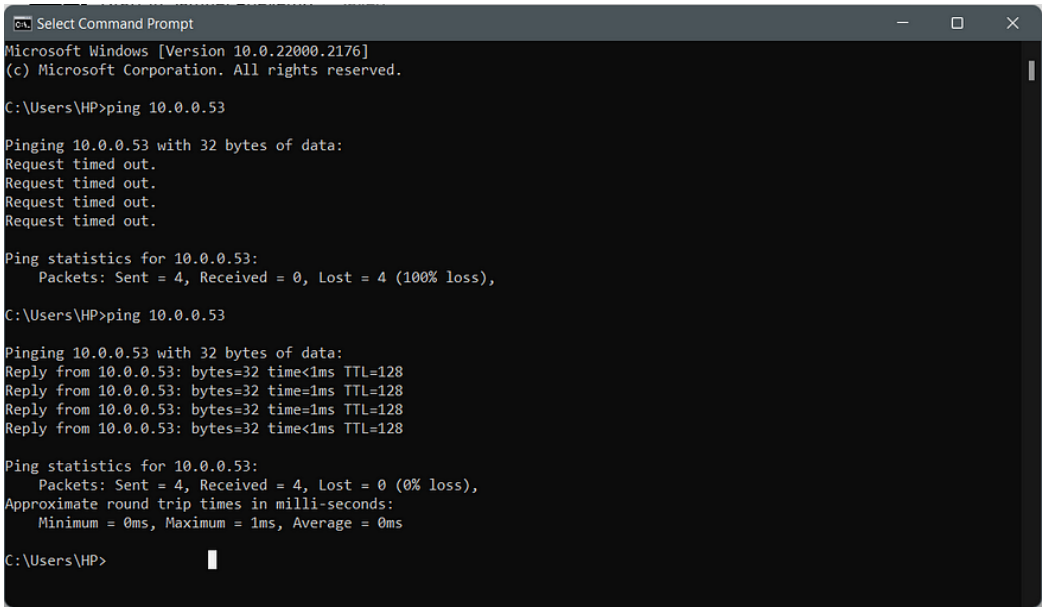
Private Profile — Off



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.

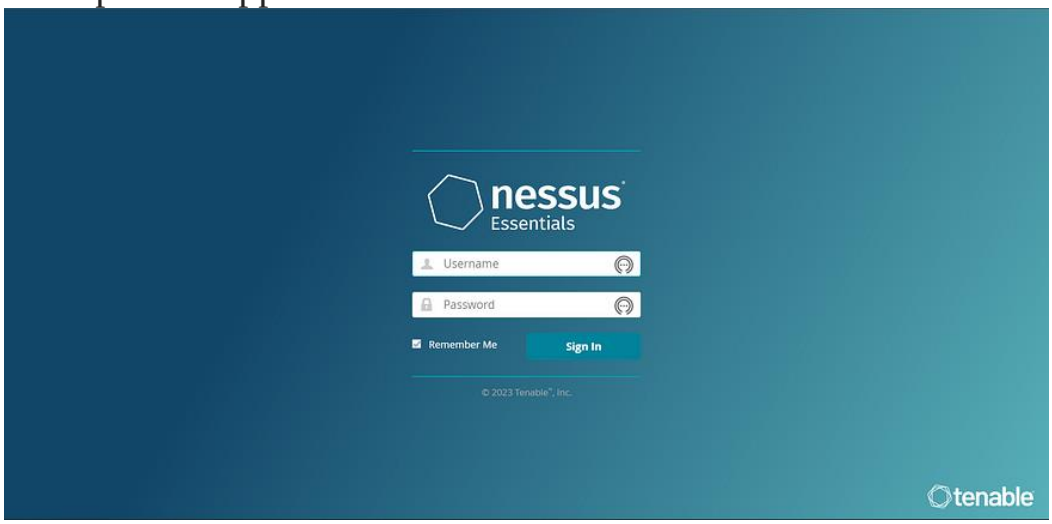
Note: Disabling firewall rules is not recommended. If you are working with a virtual machine that contains no confidential data, then you can proceed to follow along. Otherwise, exercise caution and avoid disabling firewall rules on systems containing sensitive information. Make sure to switch the firewall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



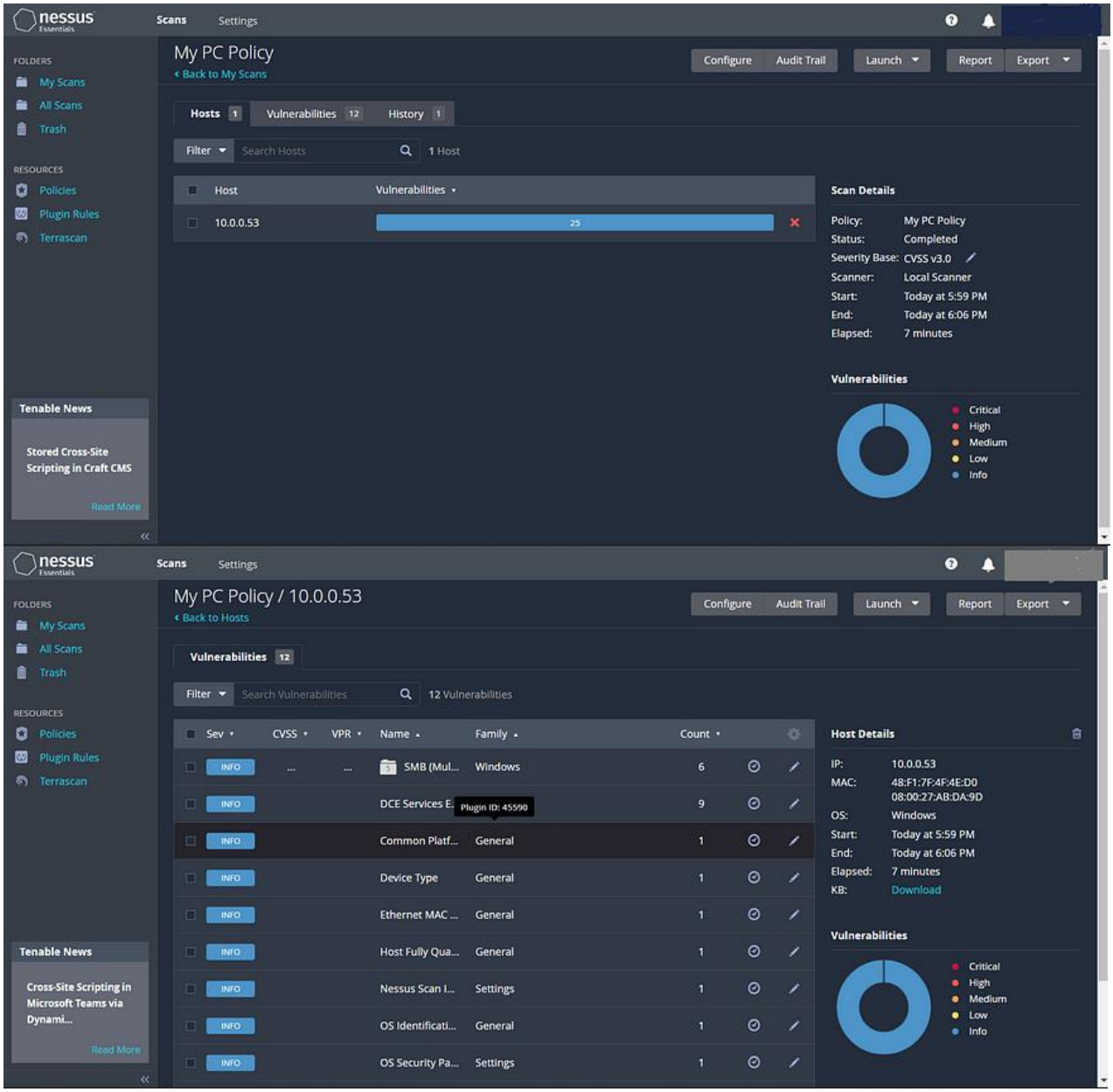
Ping successful.

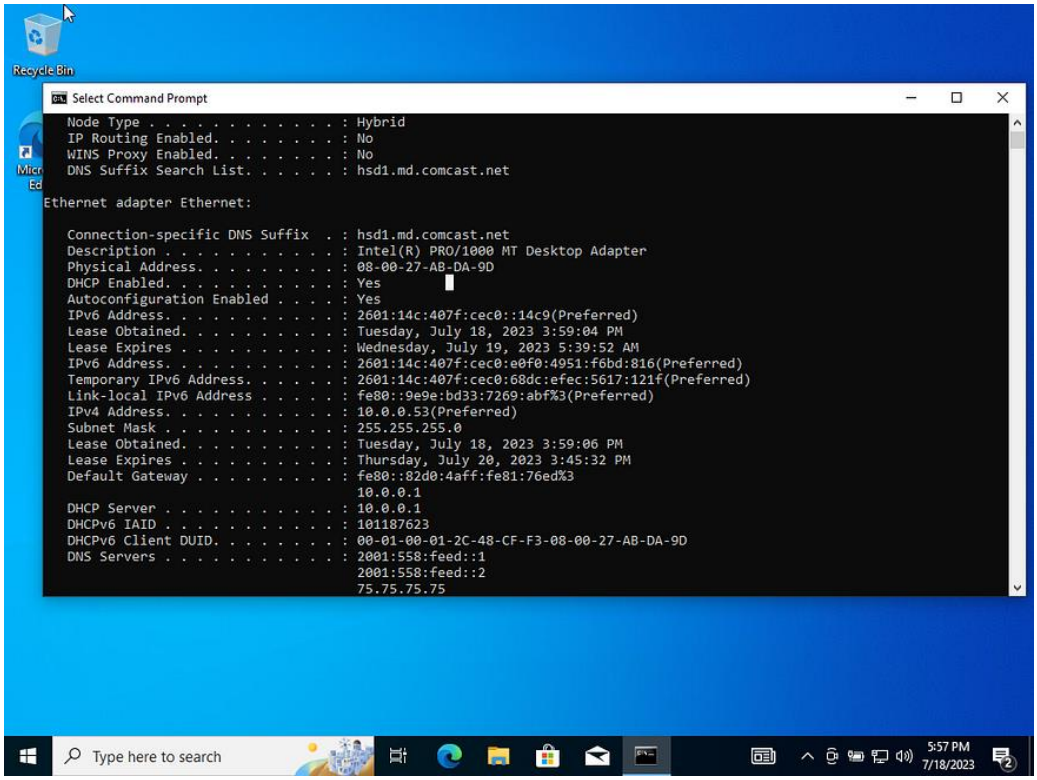
Scanning with Nessus

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



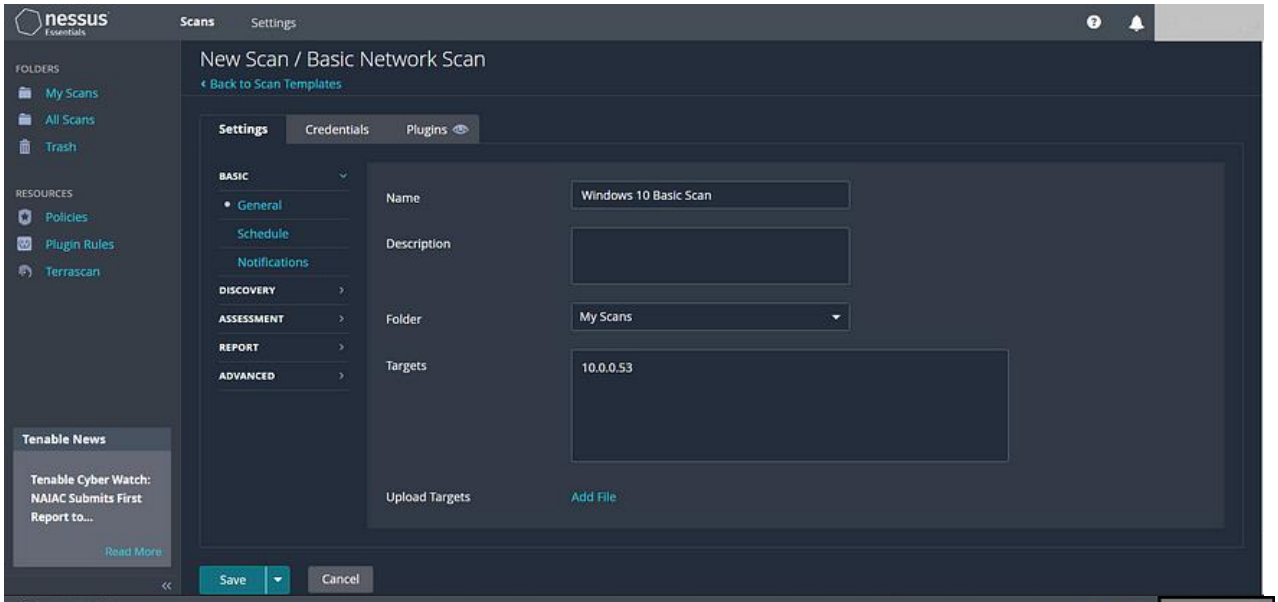
Nessus portal asking for my credentials.

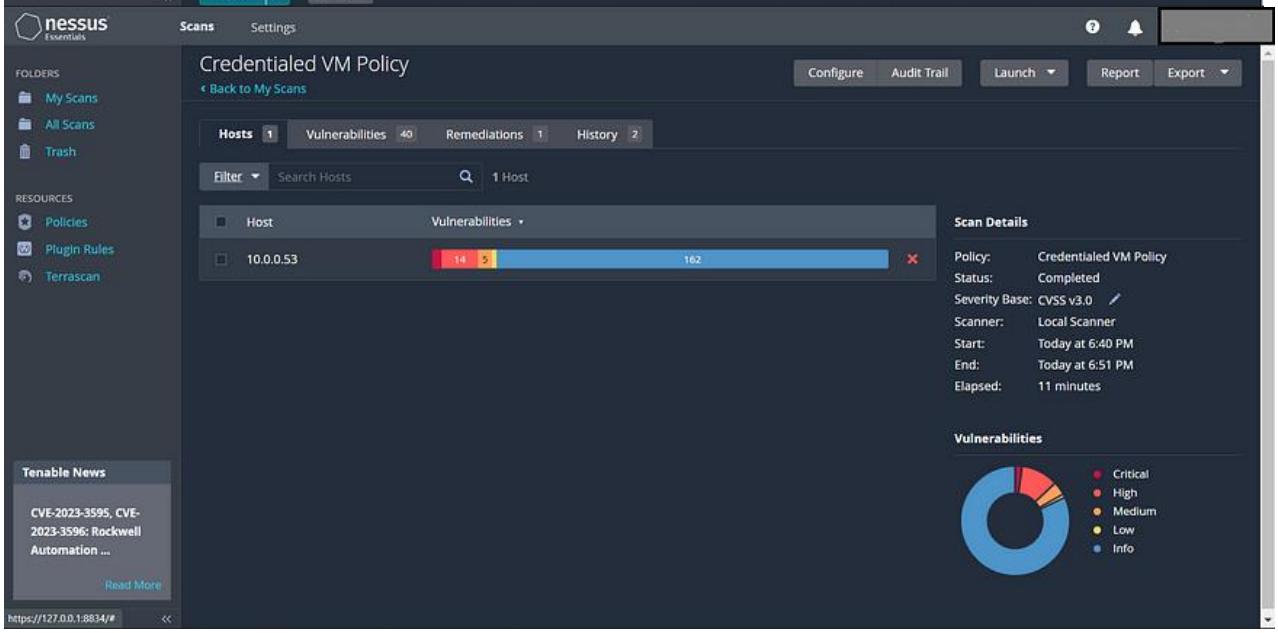

nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Stored Cross-Site Scripting in Craft CMS
Read More
My PC Policy
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 12
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.0.0.53
25
Scan Details
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
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cross-Site Scripting in Microsoft Teams via Dynami...
Read More
My PC Policy / 10.0.0.53
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 12
Filter
Search Vulnerabilities
12 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
INFO
SMB (Mul...
Windows
6
DCE Services E...
Plugin ID: 45590
9
Common Platf...
General
1
Device Type
General
1
Ethernet MAC ...
General
1
Host Fully Qua...
General
1
Nessus Scan I...
Settings
1
OS Identificati...
General
1
OS Security Pa...
Settings
1
Host Details
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



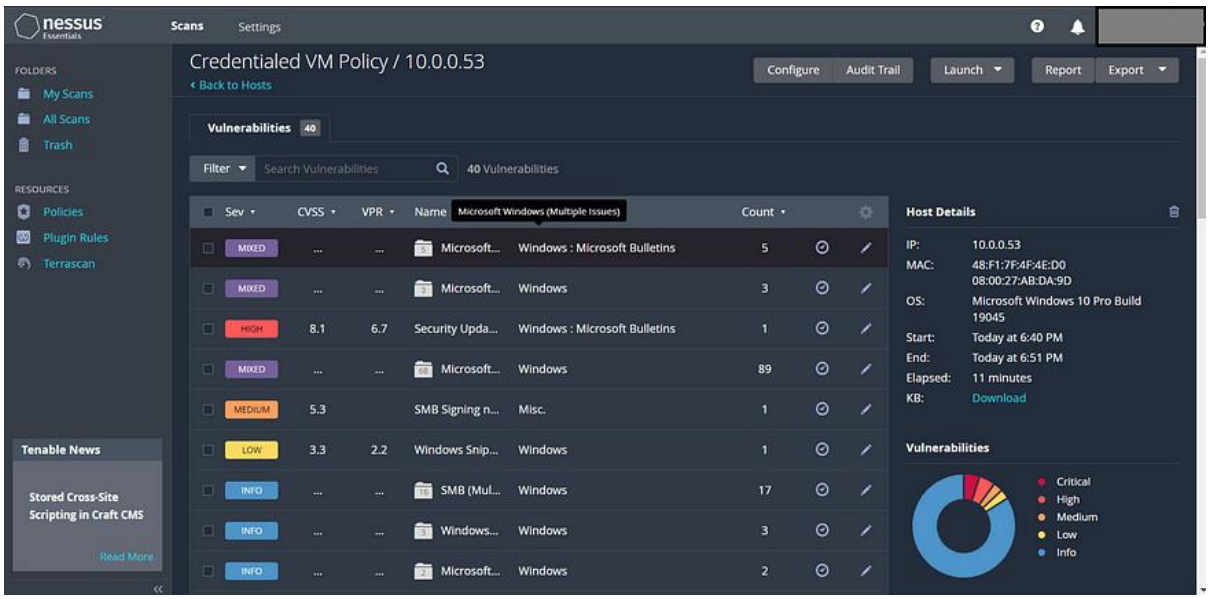
The MAC Address and IPv4 Address of my virtual machine align with the addresses displayed in the scan results, affirming that my virtual machine was indeed successfully scanned.

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.





credentialed scan result



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%)

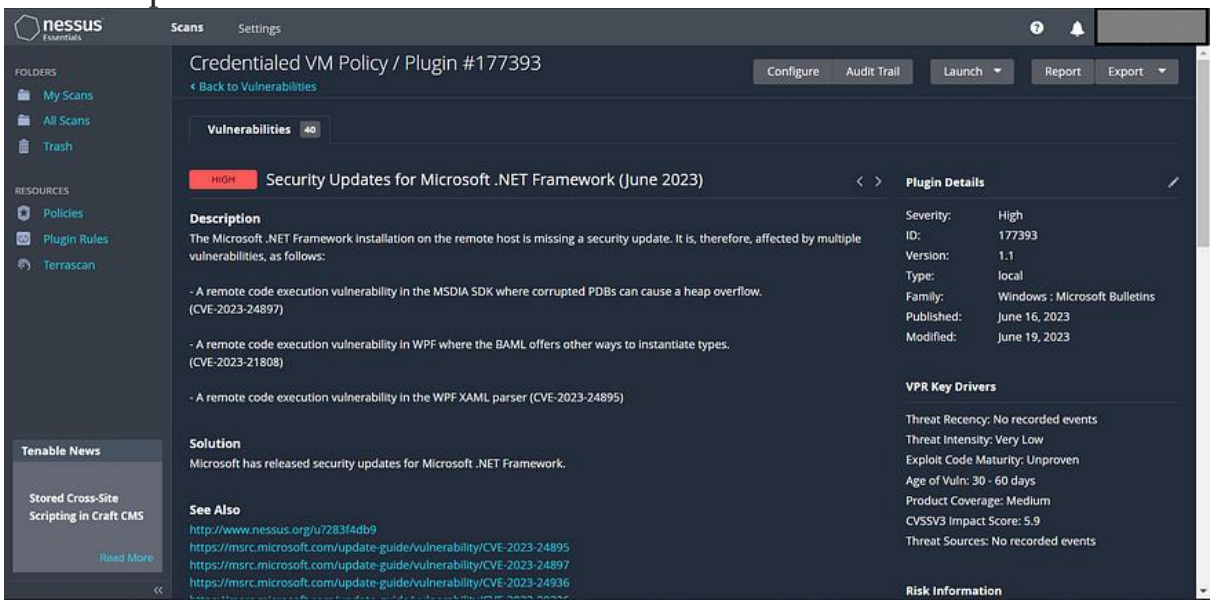
Non-Credentialed Scan Result

Info — 25 (100%)

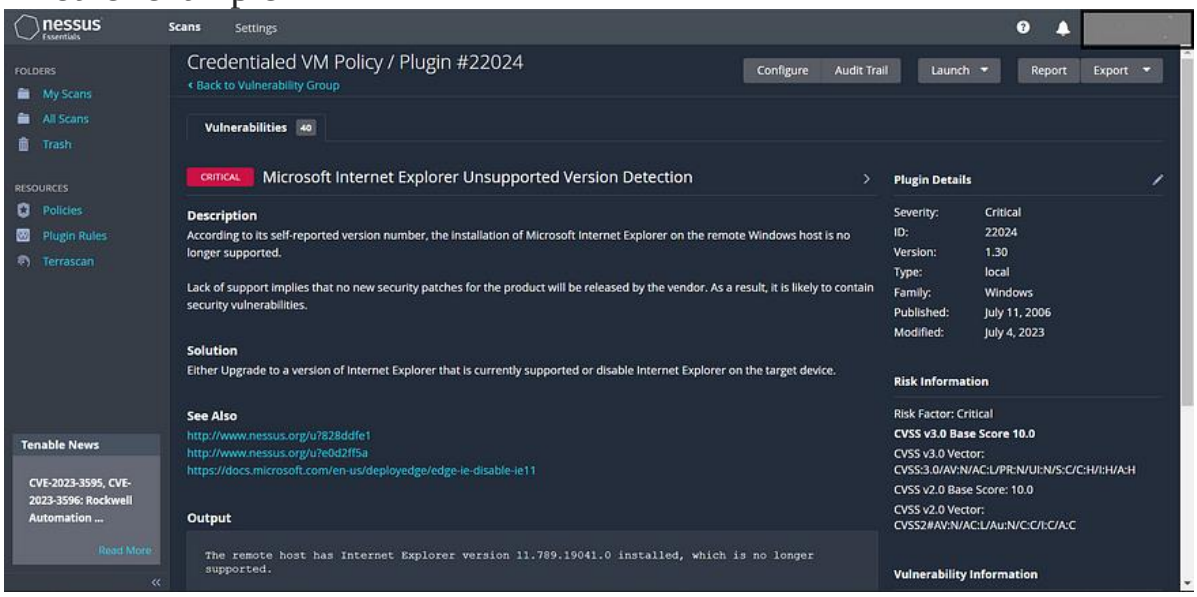
In a typical scan result, you can expect to find detailed information about the specific vulnerability, including its severity level, suggested

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

An example can be seen below

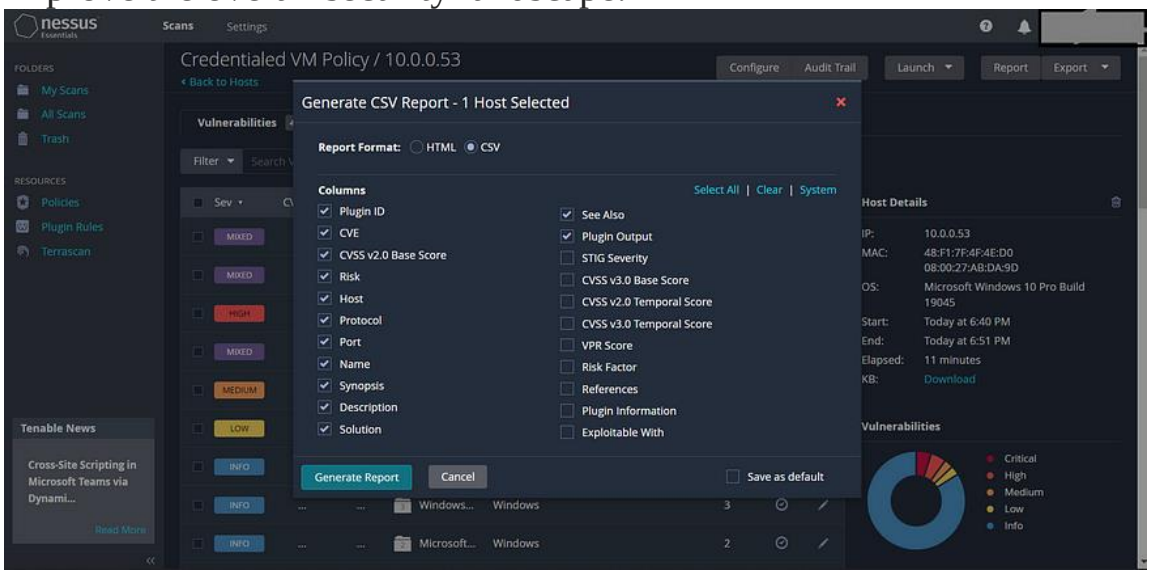


Another example

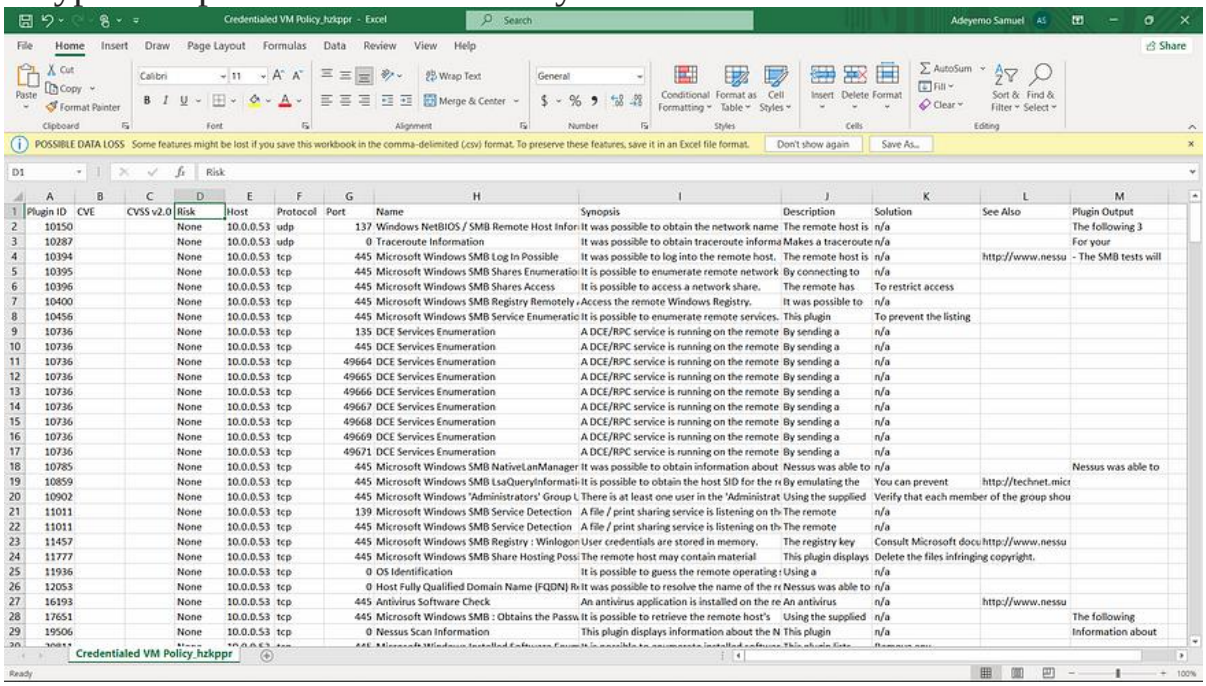


Vulnerability scan results can be exported either as HTML or CSV files. The primary purpose of exporting these scan results is to simplify the process of documentation and share the findings with the relevant parties

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



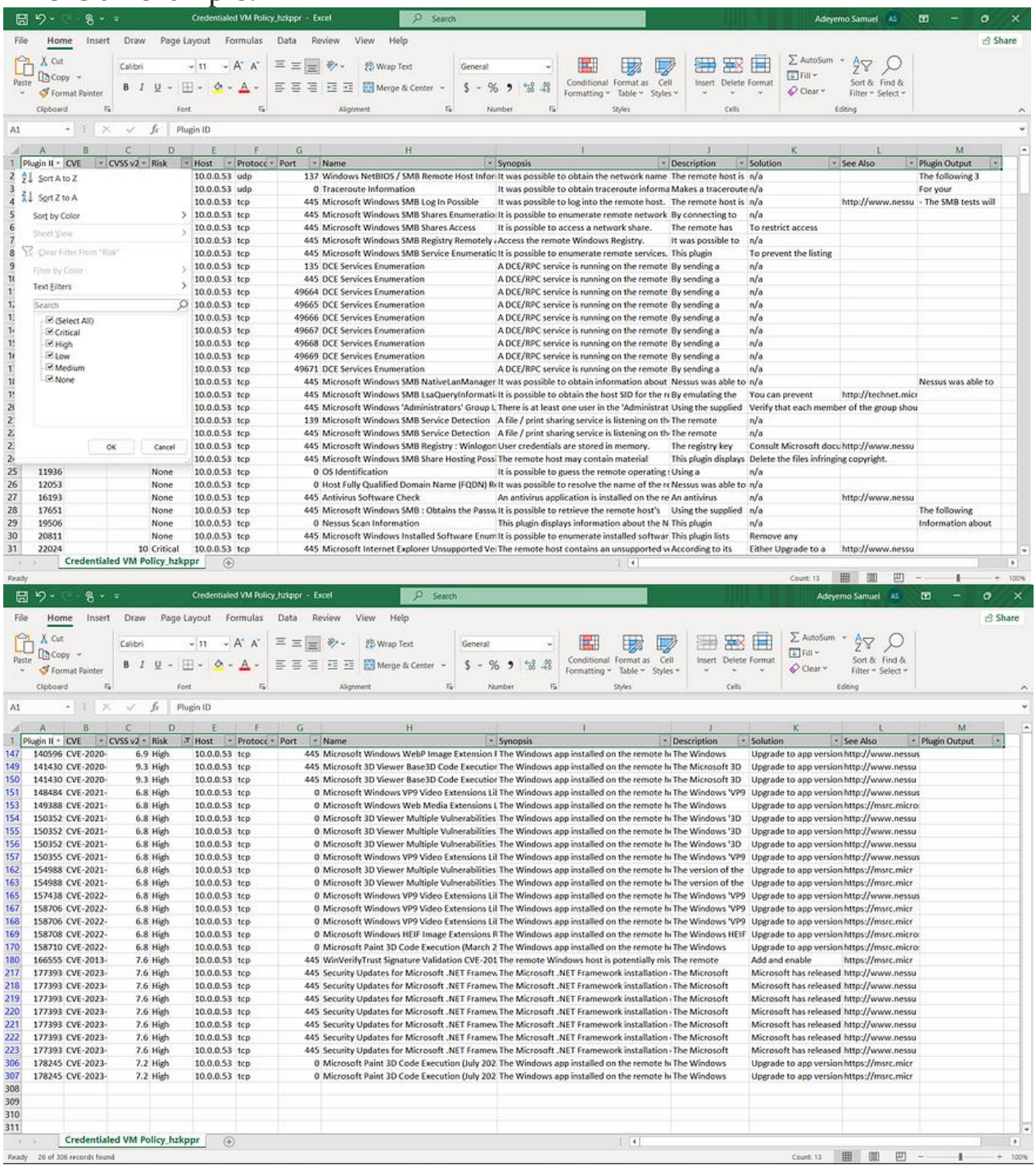
A typical exported csv vulnerability scan result would look like this



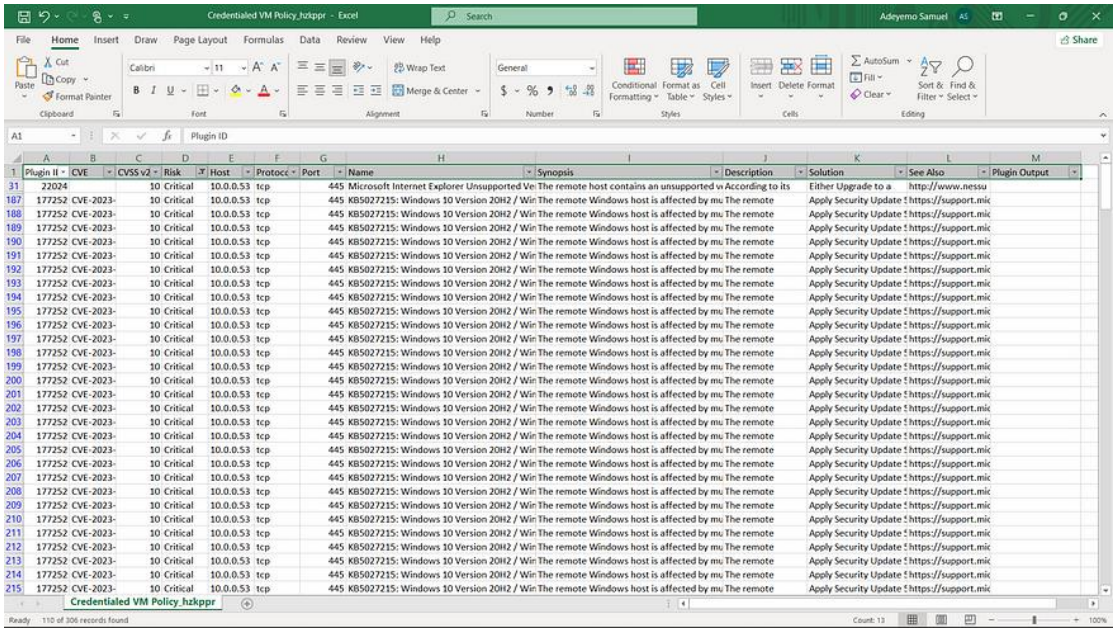
Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
10150			None	10.0.0.53	udp	137	Windows NetBIOS / SMB Remote Host Infor	It was possible to obtain the network name	The remote host is	n/a		The following 3
10287			None	10.0.0.53	udp	0	Traceroute Information	It was possible to obtain traceroute informa	Makes a traceroute	n/a		For your
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	http://www.nessu	- The SMB tests will
10395			None	10.0.0.53	tcp	445	Microsoft Windows SMB Shares Enumeratio	It is possible to enumerate remote network	By connecting to	n/a		
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		
10400			None	10.0.0.53	tcp	445	Microsoft Windows SMB Registry Remotely	Access the remote Windows Registry.	It was possible to	n/a		
10456			None	10.0.0.53	tcp	445	Microsoft Windows SMB Service Enumeratio	It is possible to enumerate remote services.	This plugin	To prevent the listing		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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
10859			None	10.0.0.53	tcp	445	Microsoft Windows SMB LsaQueryInformati	It is possible to obtain the host SID for the r	By emulating the	You can prevent	http://technet.micr	
10902			None	10.0.0.53	tcp	445	Microsoft Windows 'Administrators' Group U	There is at least one user in the 'Administrat	Using the supplied	Verify that each member of the group shou		
11011			None	10.0.0.53	tcp	139	Microsoft Windows SMB Service Detection	A file / print sharing service is listening on th	The remote	n/a		
11011			None	10.0.0.53	tcp	445	Microsoft Windows SMB Service Detection	A file / print sharing service is listening on th	The remote	n/a		
11457			None	10.0.0.53	tcp	445	Microsoft Windows SMB Registry : Winlogon	User credentials are stored in memory.	The registry key	Consult Microsoft docu	http://www.nessu	
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.		
11936			None	10.0.0.53	tcp	0	OS Identification	It is possible to guess the remote operating	Using a	n/a		
12053			None	10.0.0.53	tcp	0	Host Fully Qualified Domain Name (FQDN) Re	It was possible to resolve the name of the re	Nessus was able to	n/a		
16193			None	10.0.0.53	tcp	445	Antivirus Software Check	An antivirus application is installed on the re	An antivirus	n/a	http://www.nessu	
17651			None	10.0.0.53	tcp	445	Microsoft Windows SMB : Obtains the Passw	It is possible to retrieve the remote host's	Using the supplied	n/a		The following
19506			None	10.0.0.53	tcp	0	Nessus Scan Information	This plugin displays information about the N	This plugin	n/a		Information about

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:



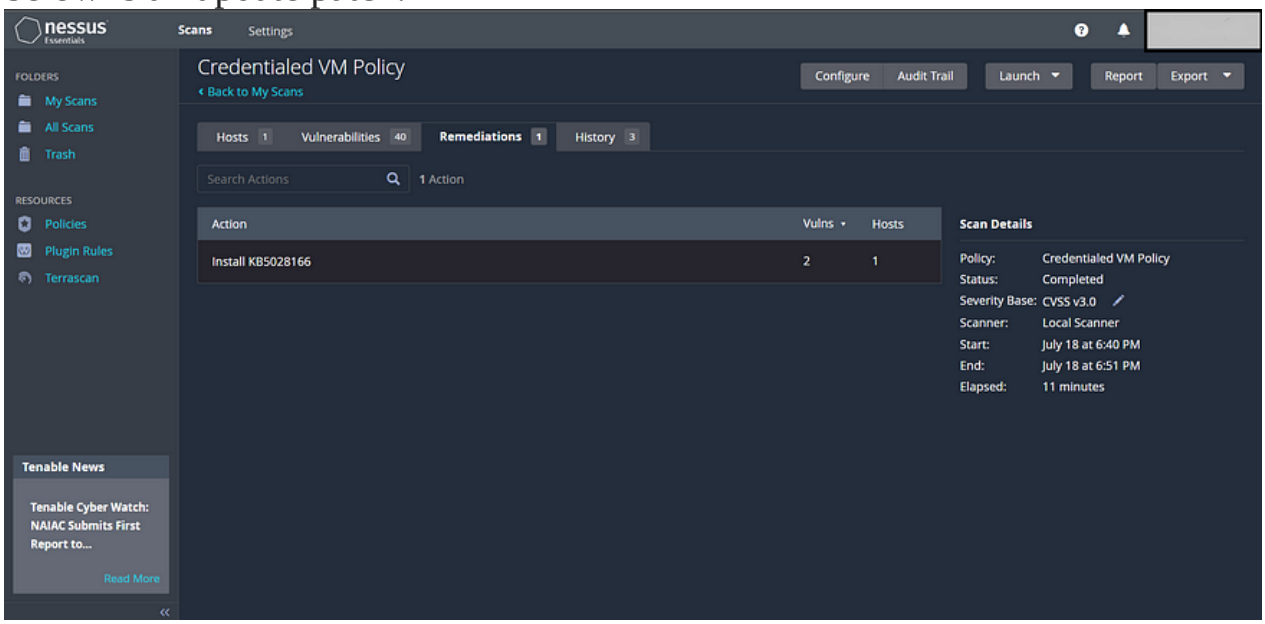
Filtered result based on High Risk.

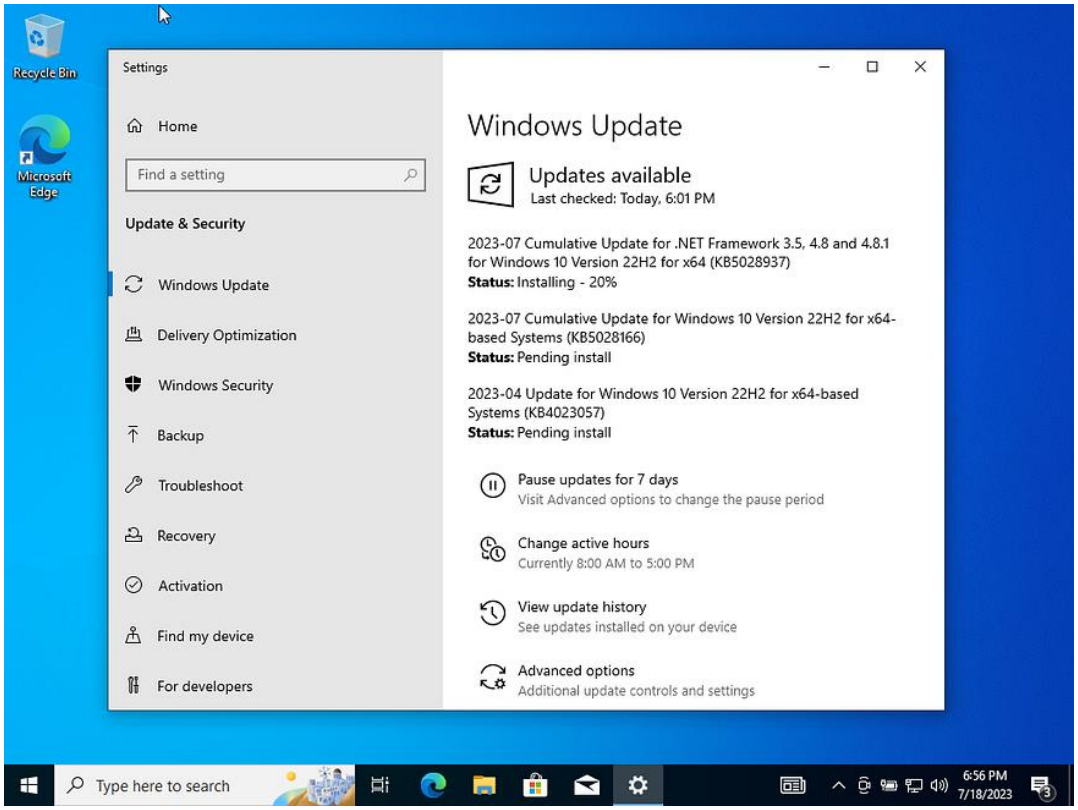


Filtered result based on critical risk

In addition to filtering vulnerability scan results based on various metrics, such as risk (severity), another option is filtering based on the host. However, since this particular scan was conducted on a single host, there is no need to apply host-based filtering in this case.

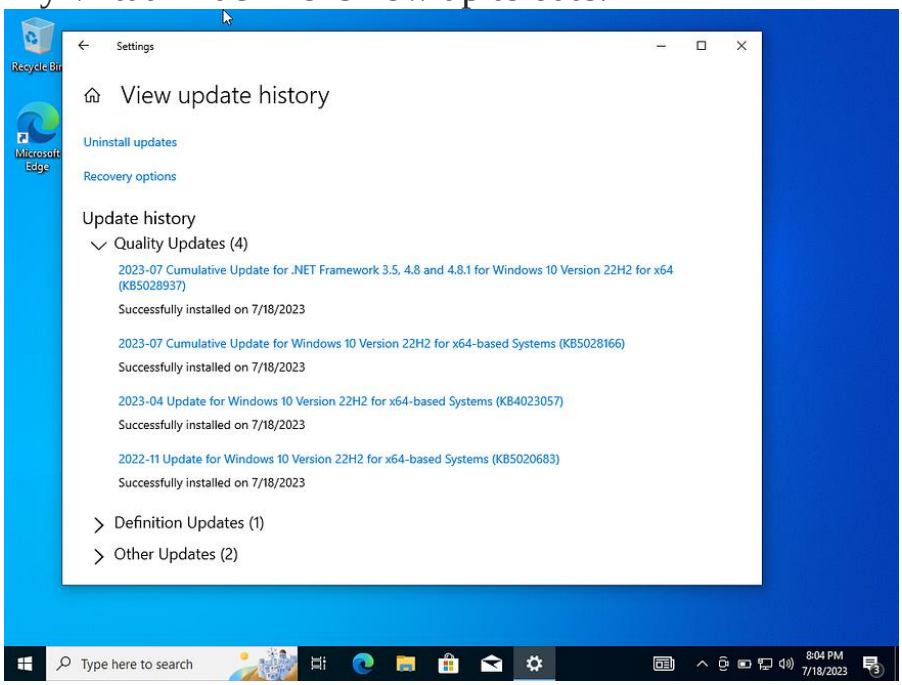
To address these vulnerabilities, a recommended remediation step is to update the operating system of my virtual machine. “KB5028166” as seen below is an update patch.





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.