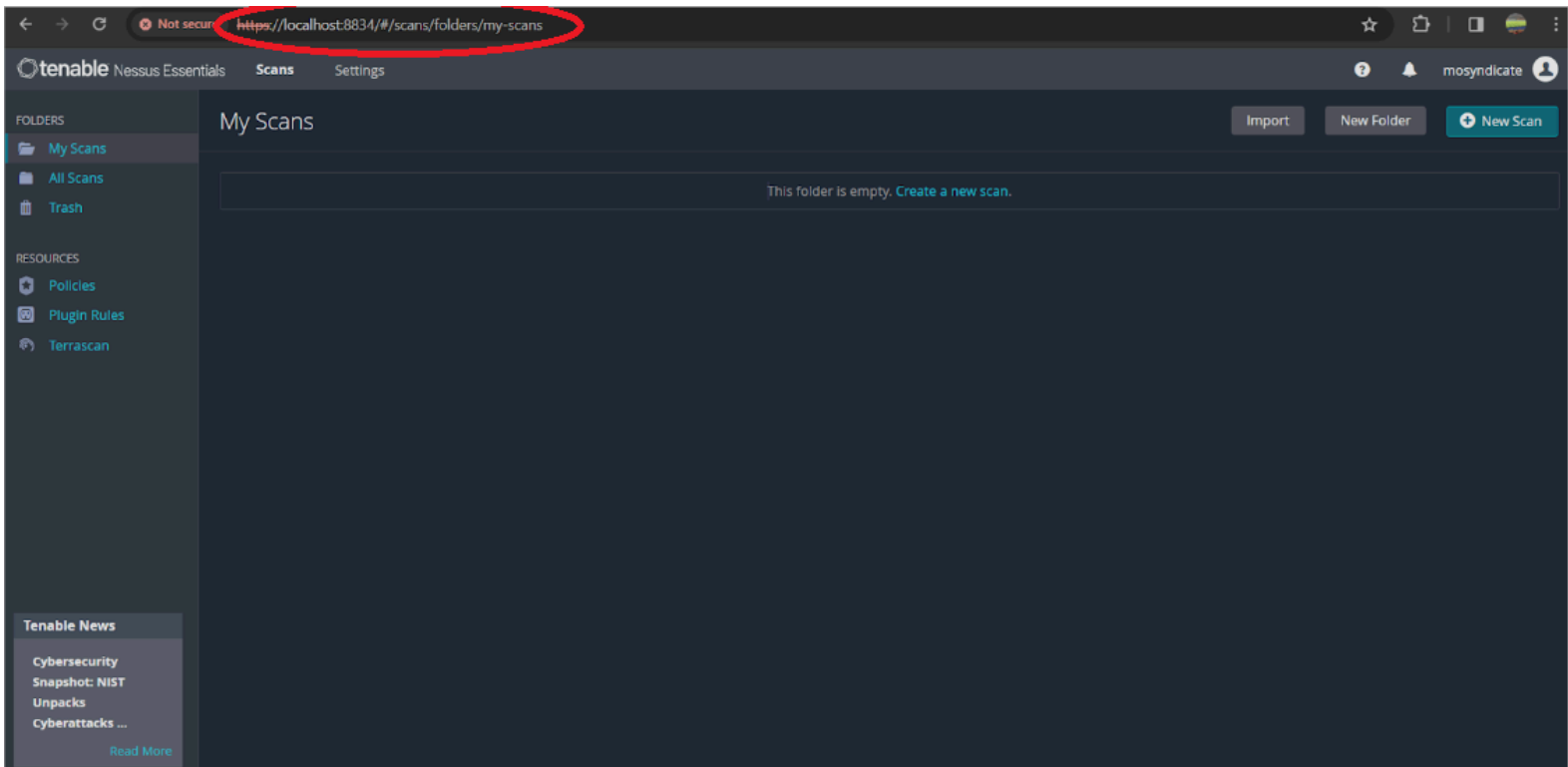


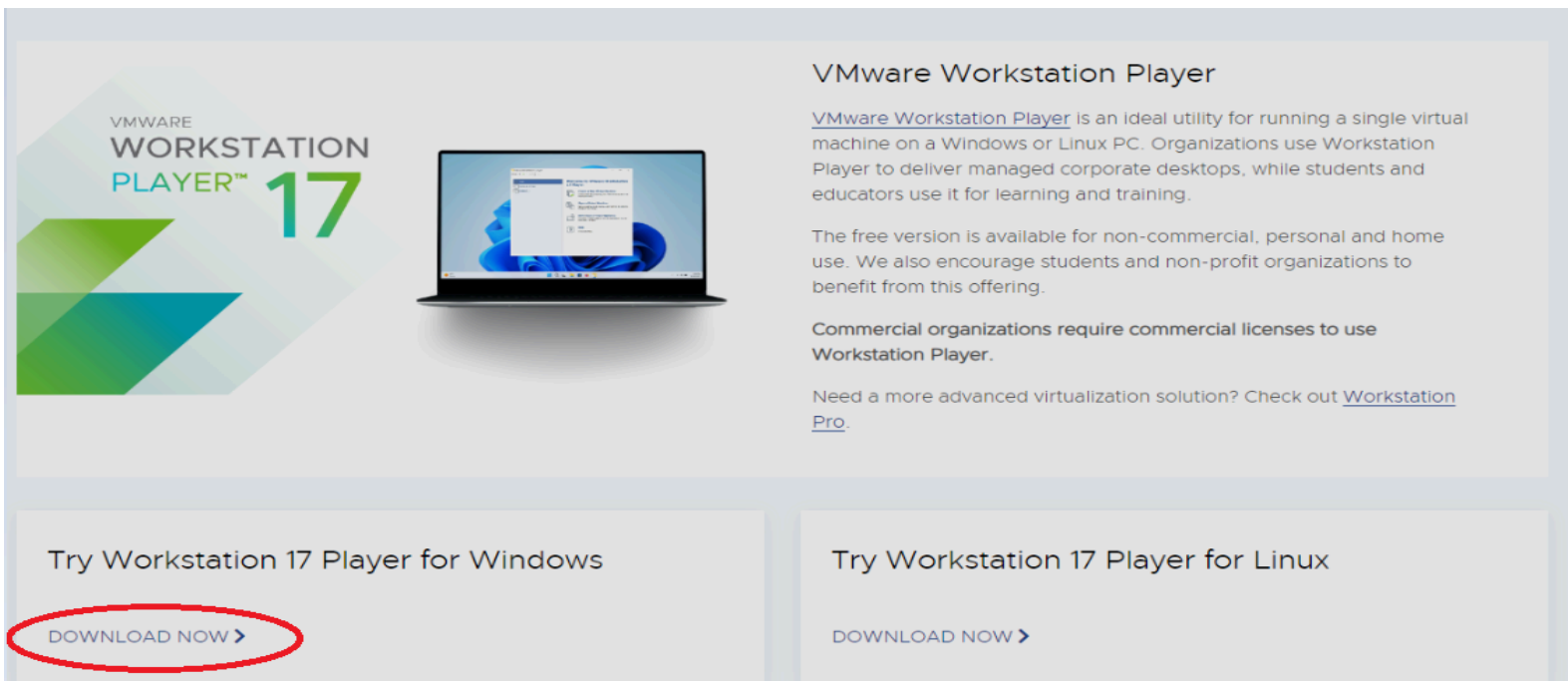
Nessus Vulnerability Project

- To do this project, you will need:
 - Nessus Essential
 - VMWare Workstation 17 Player (Any VM will suffice)
 - Microsoft ISO File
- Download Nessus Essentials:
- After downloading Nessus, you can access it by going to “https://localhost:8834”



- Download VMWare Workstation 17 Player:
- Visit the VMWare website and download VMWare Workstation 17 Player or any alternative VM.
- Navigate to:
<https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html>

- Click on "DOWNLOAD NOW" to initiate the download.



The screenshot shows the VMware Workstation Player download page. On the left, there is a logo for VMware Workstation Player 17 and an image of a laptop displaying the software interface. On the right, the text describes the software as an ideal utility for running a single virtual machine on a Windows or Linux PC. It mentions that the free version is available for non-commercial, personal, and home use, and that commercial organizations require commercial licenses. At the bottom, there are two buttons: "Try Workstation 17 Player for Windows" and "Try Workstation 17 Player for Linux". The "DOWNLOAD NOW" link under the Windows button is circled in red.

VMware
WORKSTATION
PLAYER™ 17

VMware Workstation Player is an ideal utility for running a single virtual machine on a Windows or Linux PC. Organizations use Workstation Player to deliver managed corporate desktops, while students and educators use it for learning and training.

The free version is available for non-commercial, personal and home use. We also encourage students and non-profit organizations to benefit from this offering.

Commercial organizations require commercial licenses to use Workstation Player.

Need a more advanced virtualization solution? Check out [Workstation Pro](#).

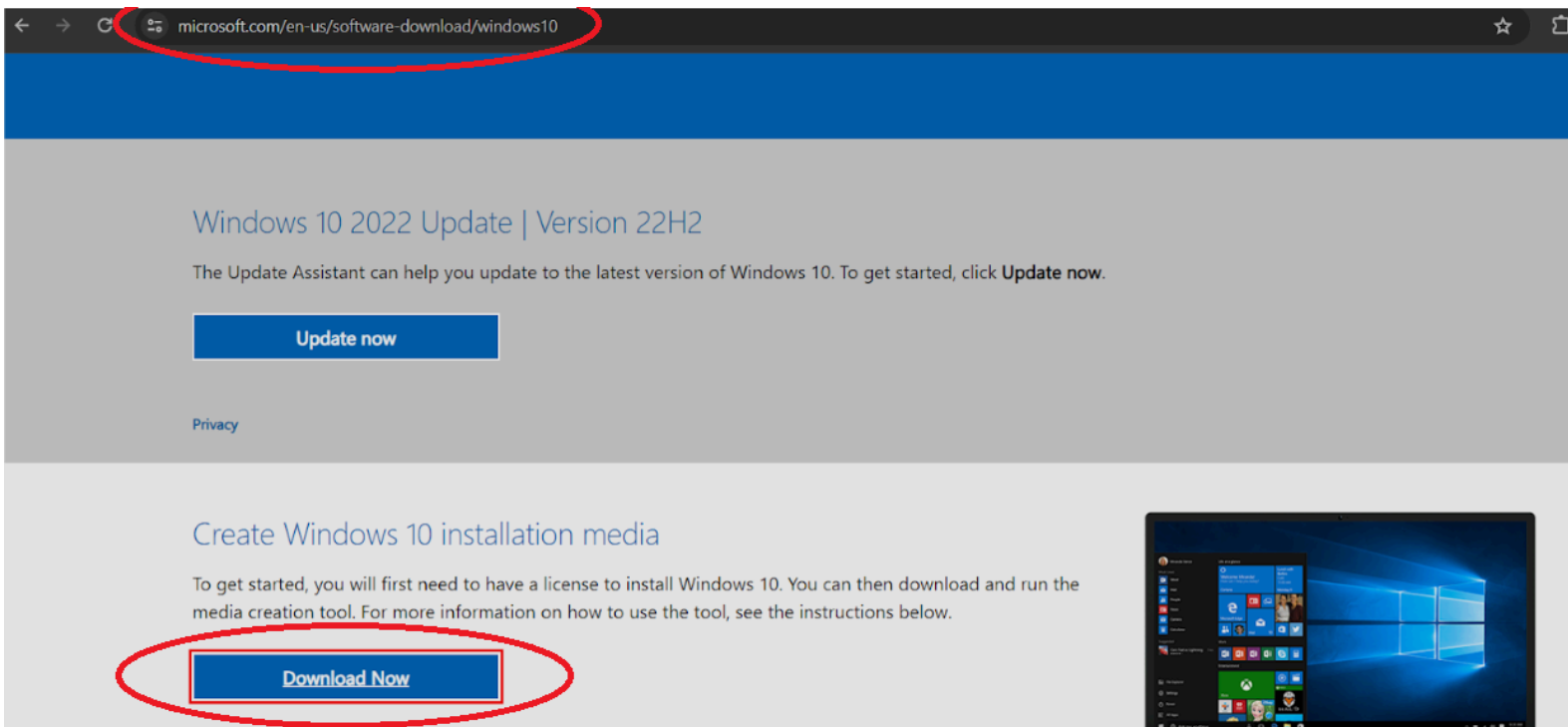
Try Workstation 17 Player for Windows

DOWNLOAD NOW >

Try Workstation 17 Player for Linux

DOWNLOAD NOW >

- Obtain a Windows 10 installation media by downloading the ISO file from the Microsoft website.
- Navigate to:
<https://www.microsoft.com/en-us/software-download/windows10>
- Click on "Download Now" to proceed.



The screenshot shows the Microsoft website for downloading Windows 10. The URL in the browser's address bar is circled in red. The page has a blue header and a grey main content area. It features a section for the "Windows 10 2022 Update | Version 22H2" with an "Update now" button. Below this, there is a "Privacy" link. The bottom section is titled "Create Windows 10 installation media" and includes instructions on how to get started. A "Download Now" button is circled in red. To the right of the text, there is an image of a Windows 10 desktop.

← → ↻ 🔍 microsoft.com/en-us/software-download/windows10 ☆ 📁

Windows 10 2022 Update | Version 22H2

The Update Assistant can help you update to the latest version of Windows 10. To get started, click **Update now**.

Update now

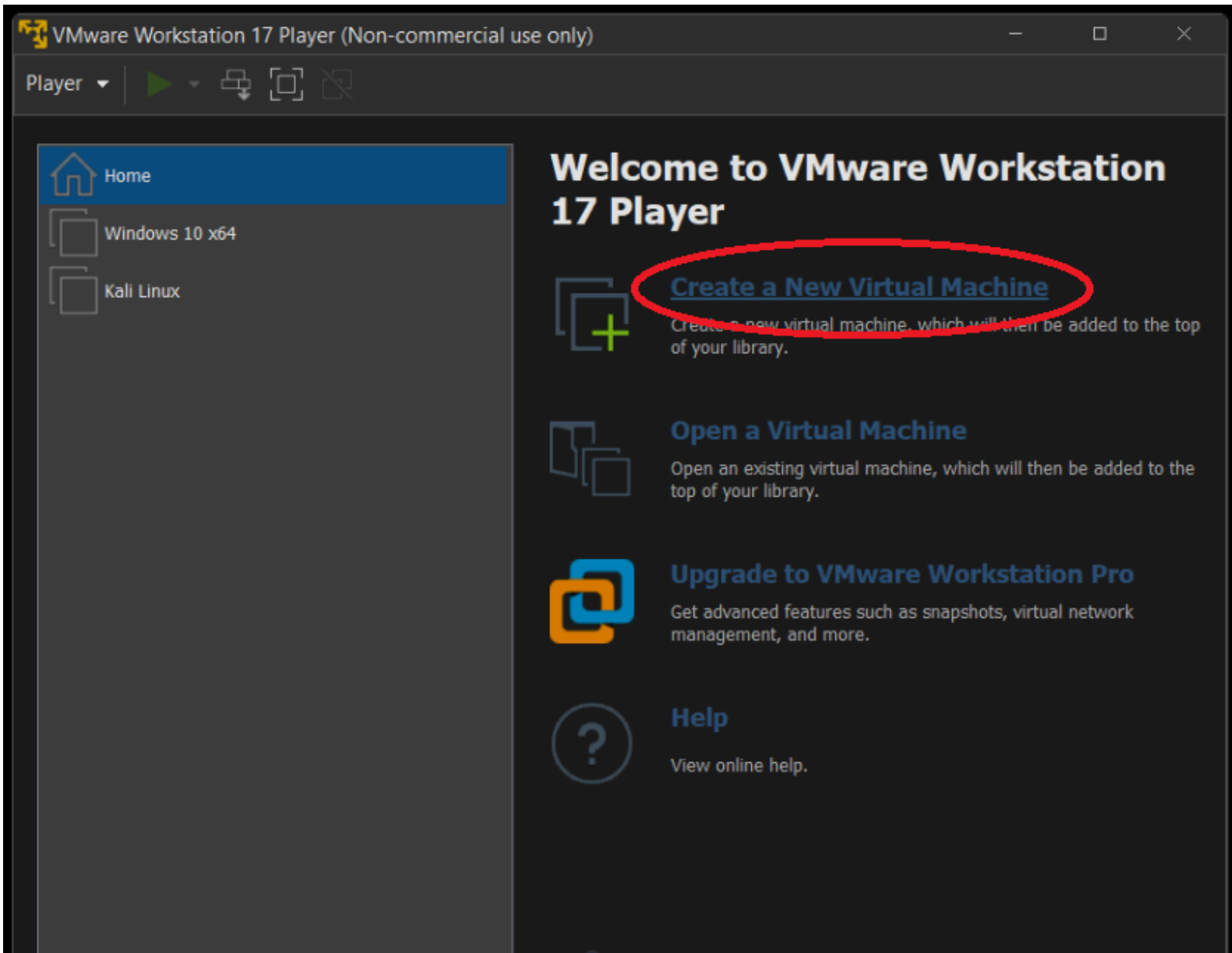
Privacy

Create Windows 10 installation media

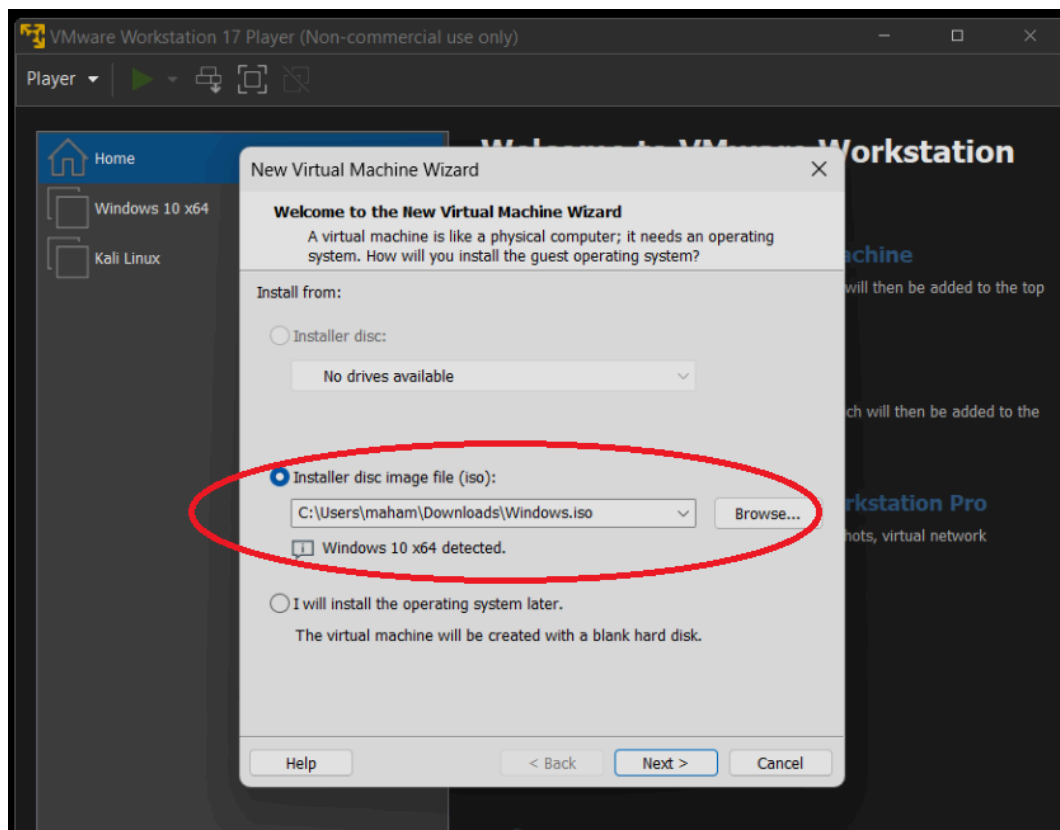
To get started, you will first need to have a license to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.

Download Now

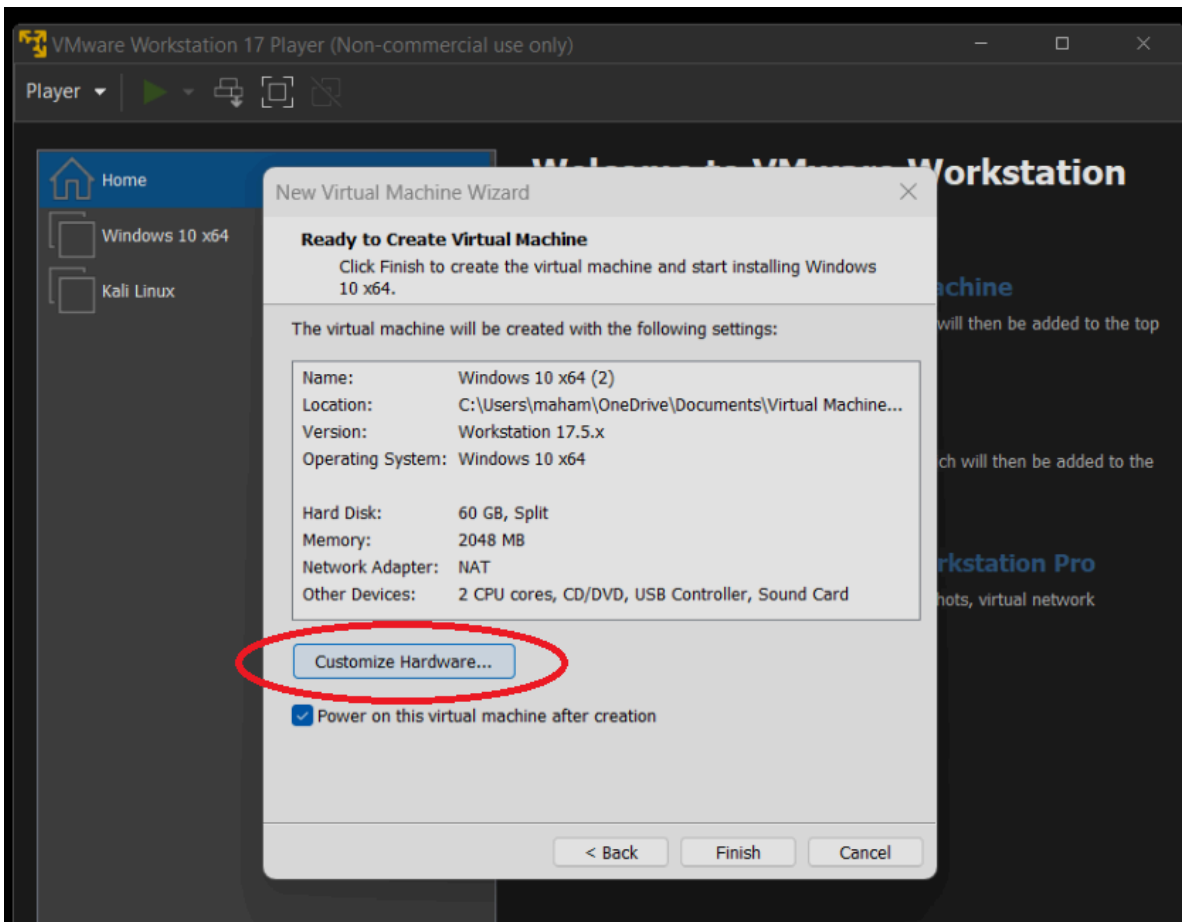
- Launch VMWare Player after downloading both VMWare Player and the Windows ISO file. Select “Create a New Virtual Machine”.



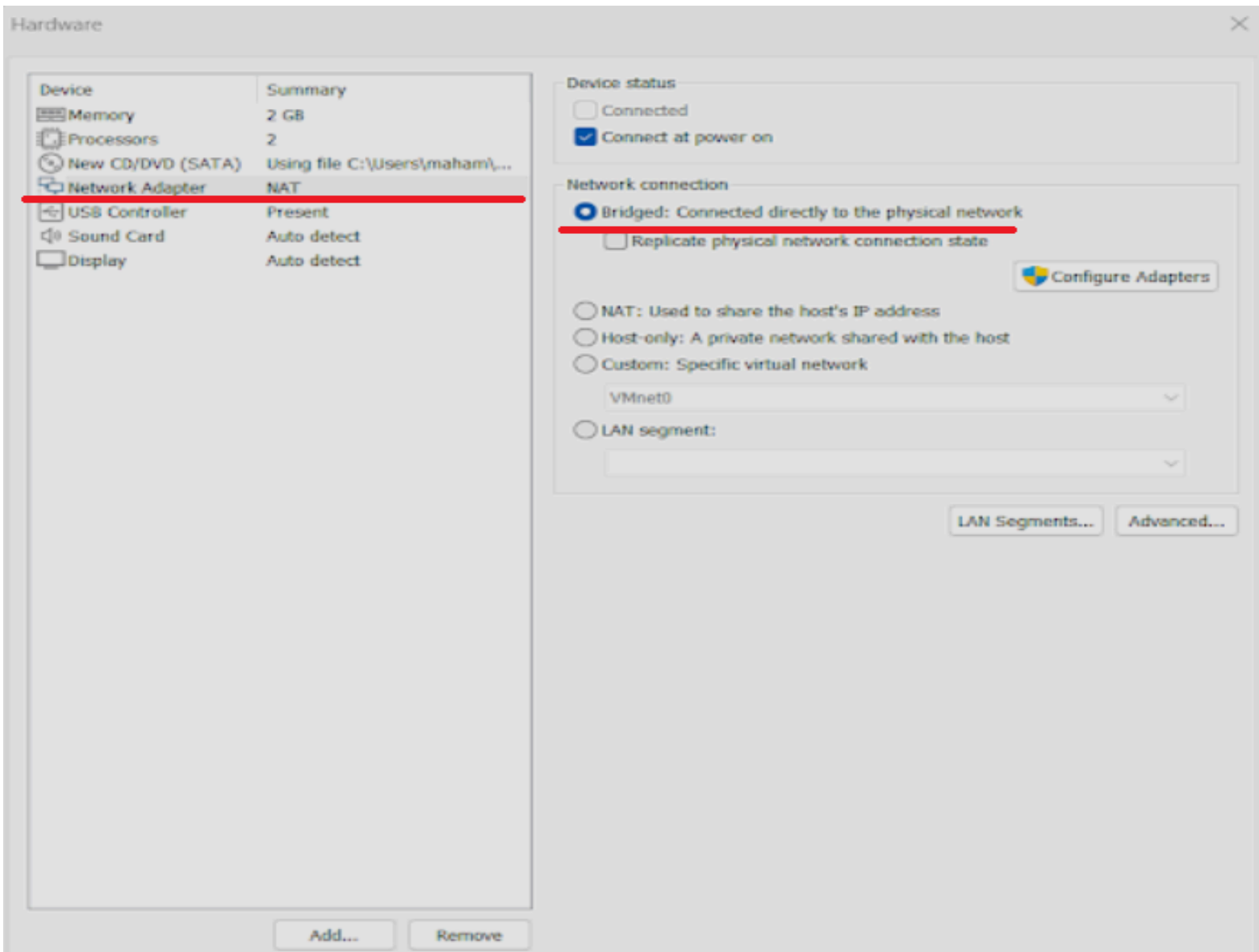
- You will need to select the middle radio button to use to ISO file.
- After browsing to where you downloaded the ISO file, you click “Next”.



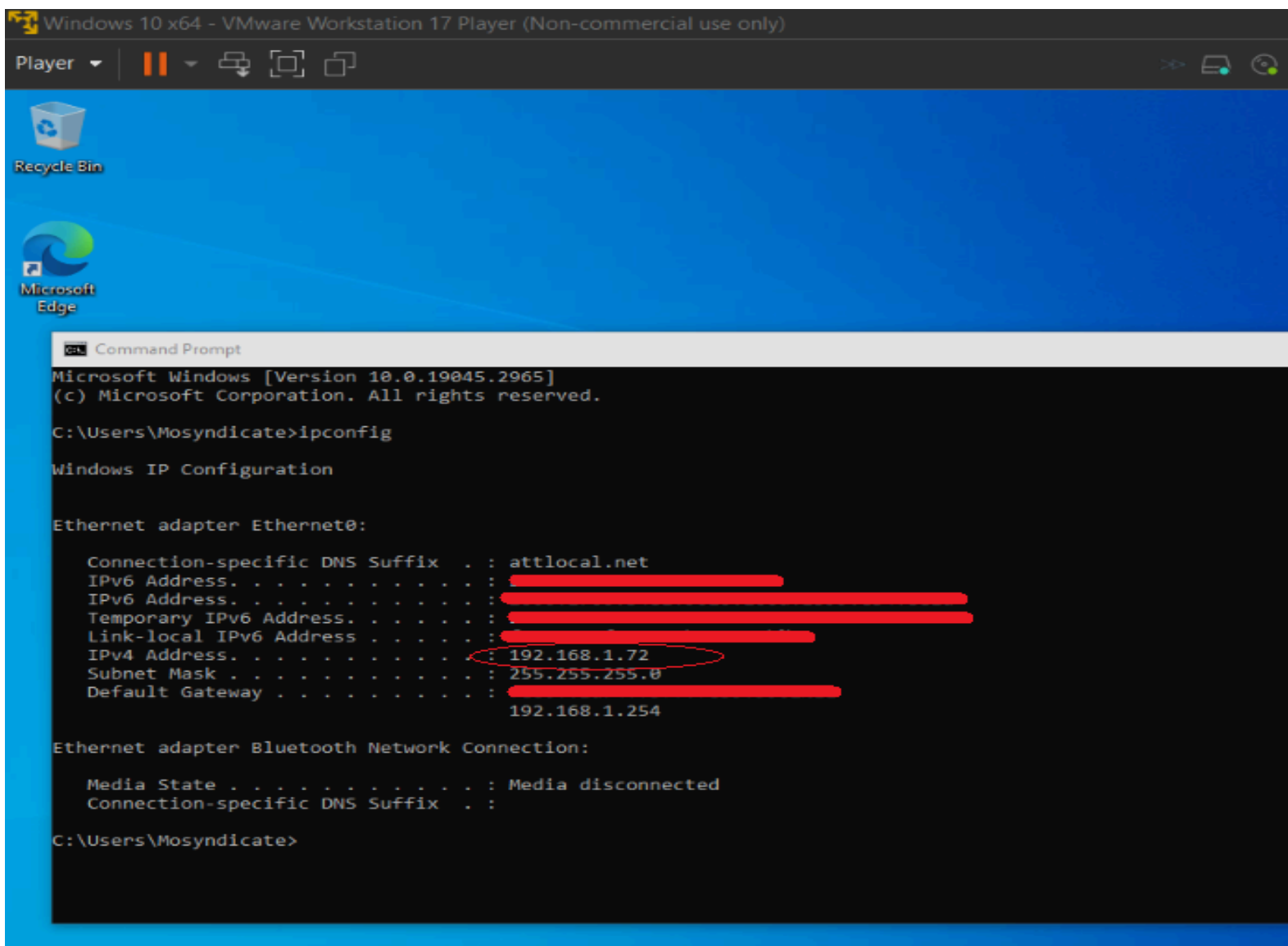
- It is important at this part you select “Customize Hardware”



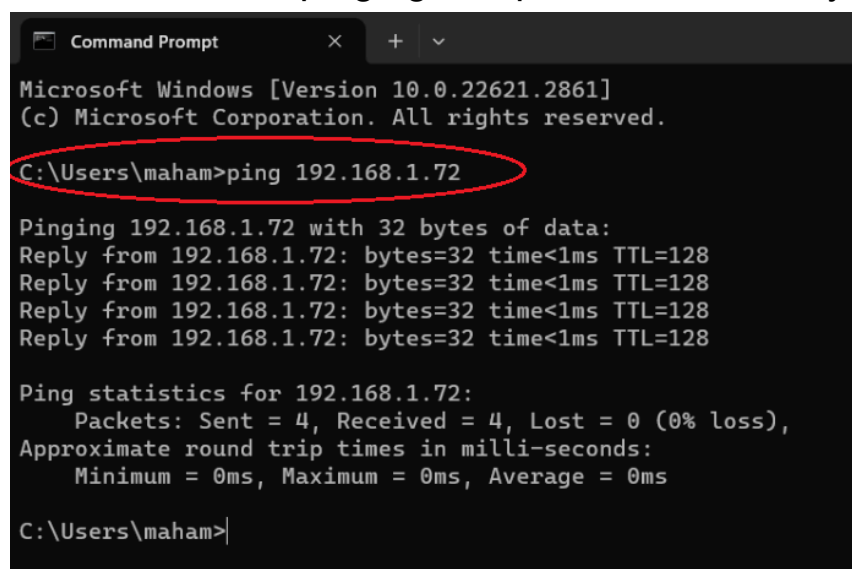
- On the ‘Network Adapter’ tab you will need to select the “Bridged” radio button
- This will allow the virtual machine to share the same network with your physical Workstation.



- After launching the virtual machine, confirm network connectivity by pinging your physical workstation from the virtual machine or vice versa. Adjust firewall settings if necessary to enable successful pinging.
- In the screenshot, I am getting the IP address of the virtual computer.

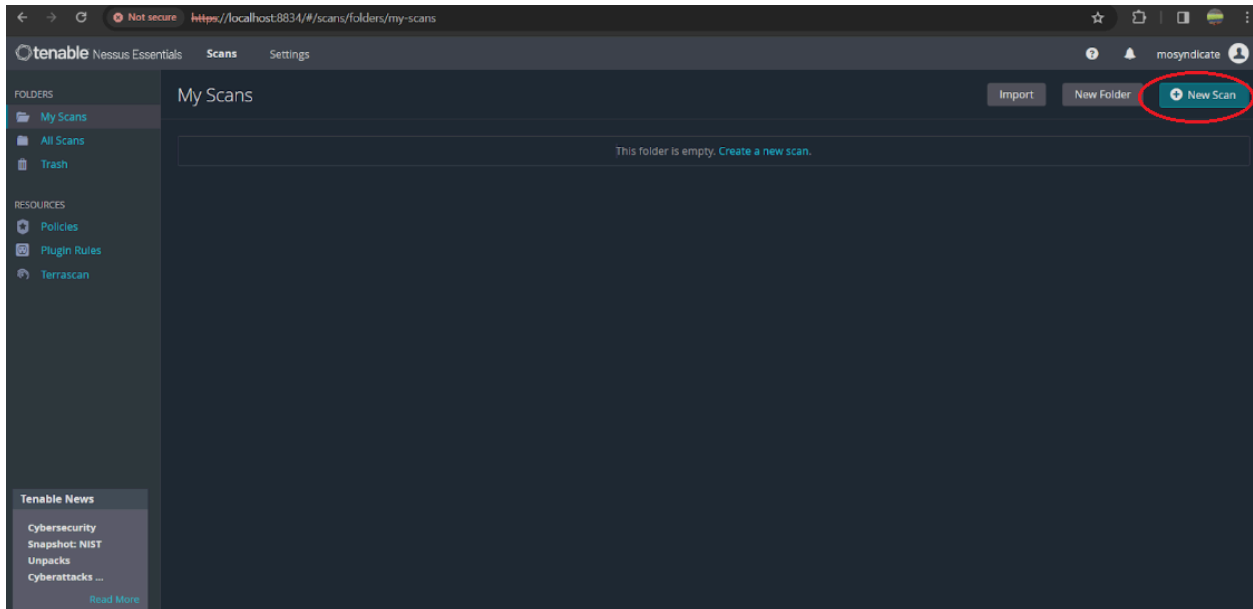


- Here, I am pinging the ip address from my workstation.

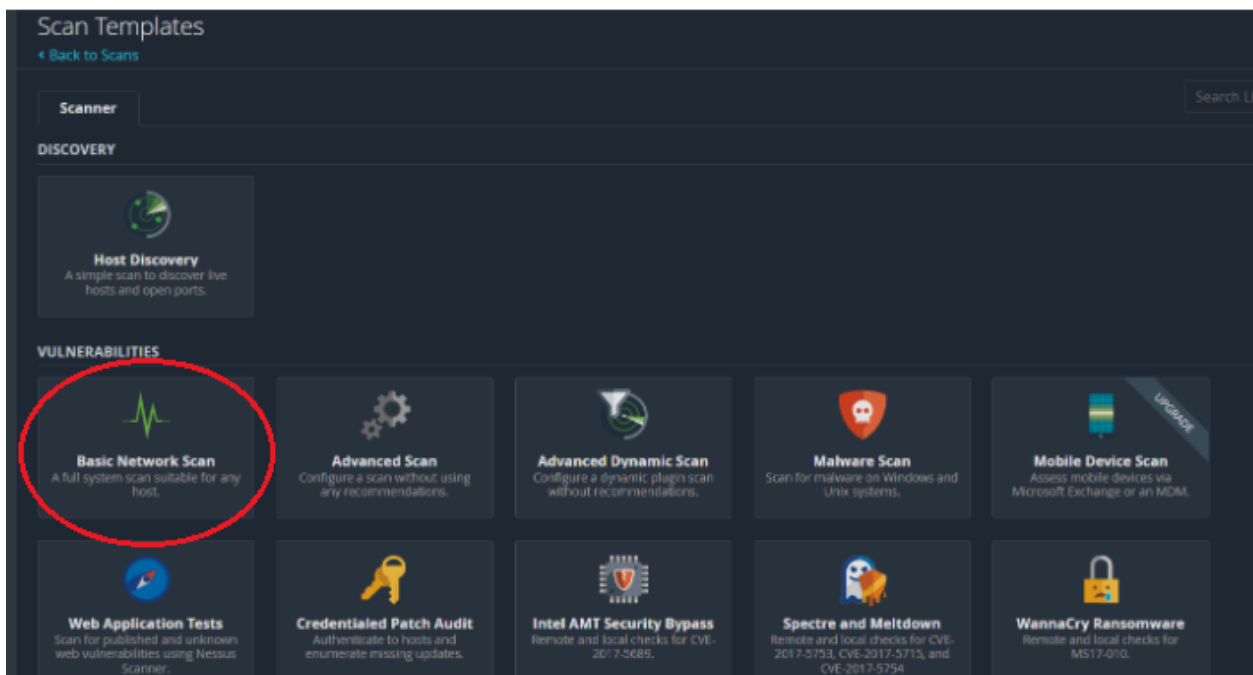


- If the ping is not complete, you may need to disable the firewall on your junk virtual lab VM
- Go to Start menu > wf.msc > Windows Defender Firewall Properties; turn off the Domain Profile, Public Profile and IPsec settings
- Then, trying the ping again. If successful, you may continue with the next step.

-
- Return back to Nessus on your workstation
 - Select “New Scan”



- Select “Basic Network Scan”



- Input the IP address of the virtual machine and input a name and a description of your choice

New Scan / Basic Network Scan
[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Windows 10 VM Single Host

Description:

Folder: My Scans

Targets: 192.168.1.72

Upload Targets Add File

Save Cancel

- If you would like to scan all port and not just common ports, go to the “Discovery” drop down (Scanning all ports will take longer than just the common ports)
- After that, you will need to save it

New Scan / Basic Network Scan
[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC >

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Scan Type: Port scan (all ports)

General Settings:

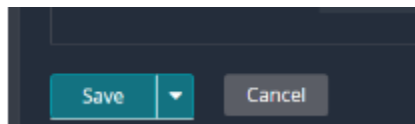
- Always test the local Nessus host
- Use fast network discovery

Port Scanner Settings:

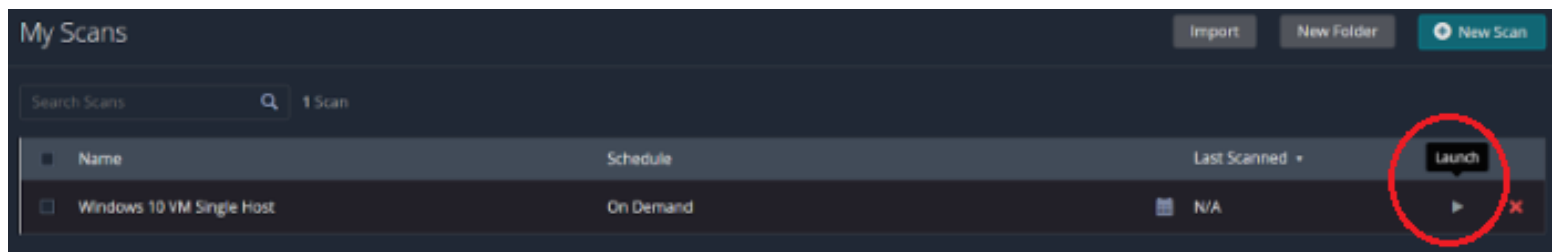
- Scan all ports (1-65535)
- Use netstat if credentials are provided
- Use SYN scanner if necessary

Ping hosts using:

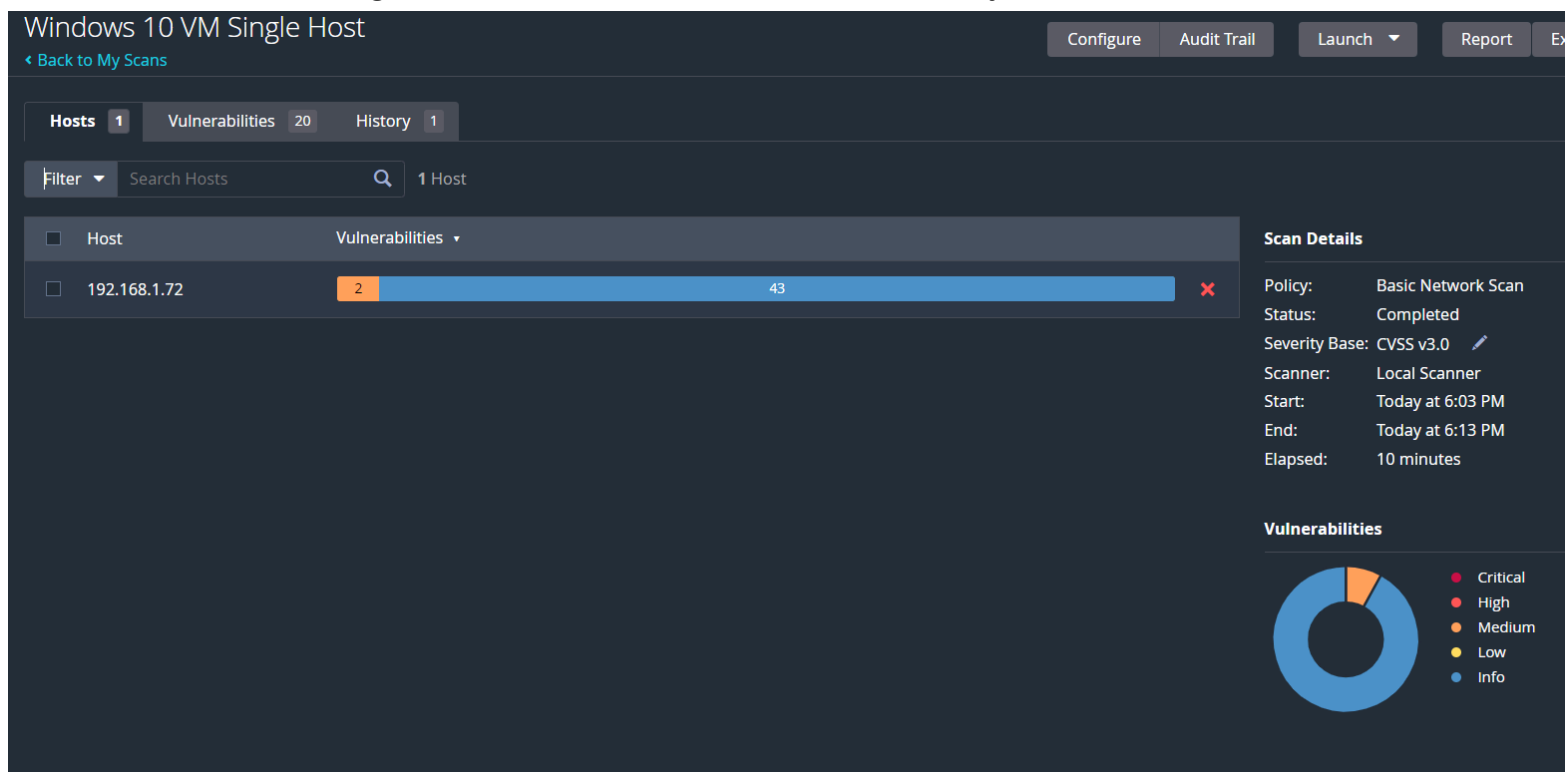
- TCP
- ARP
- ICMP (2 retries)



- This will display on your screen after saving it
- Select “launch” to start the scan, this may take some time



- After the scan is complete, review the results and available remediation options. Note any vulnerabilities identified, their severity, and CVSS scores.
- There are a total of 20 vulnerabilities and 2 medium level vulnerabilities. The highest CVSS score for a vulnerability is 6.5



Nessus EssentialsScansSettings

Vulnerabilities20

FilterSearch Vulnerabilities20 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
MEDIUM	6.5	4.9	IP Forwarding Enabled	Firewalls	1	
MEDIUM	5.3		SMB Signing not required	Misc.	1	
INFO	SMB (Multiple Issues)	Windows	6	
INFO			Nessus SYN scanner	Port scanners	13	
INFO			DCE Services Enumeration	Windows	9	
INFO			Common Platform Enumeration (CPE)	General	1	
INFO			Device Type	General	1	
INFO			Ethernet Card Manufacturer Detection	Misc.	1	
INFO			Ethernet MAC Addresses	General	1	
INFO			Host Fully Qualified Domain Name (FQD...	General	1	
INFO			ICMP Timestamp Request Remote Data D	General	1	

Host Details

IP: 192.168.1.72
MAC: 98:43:FA:4F:1A:D2
00:0C:29:B6:B9:08
OS: Microsoft Windows
Start: Today at 6:03 PM
End: Today at 6:13 PM
Elapsed: 10 minutes
KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

entialsScansSettings

Windows 10 VM Single Host / Plugin #50686

ConfigureAudit TrailLaunchReportExport

Vulnerabilities20

MEDIUMIP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Plugin Details

Severity: Medium
ID: 50686
Version: 1.16
Type: remote
Family: Firewalls
Published: November 23, 2010
Modified: October 17, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 3.7
Threat Sources: No recorded events

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Risk Information

Vulnerability Priority Rating (VPR): 4.9

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:

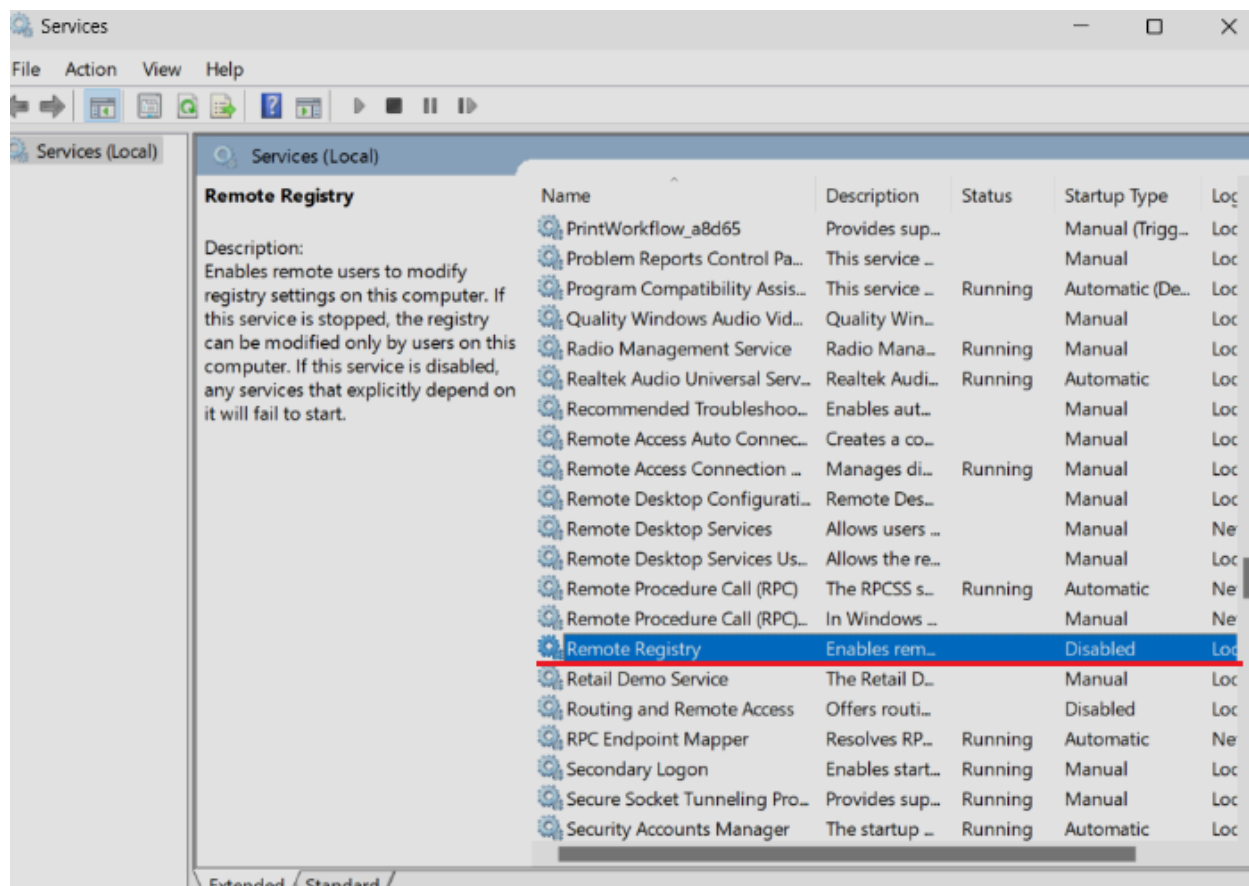
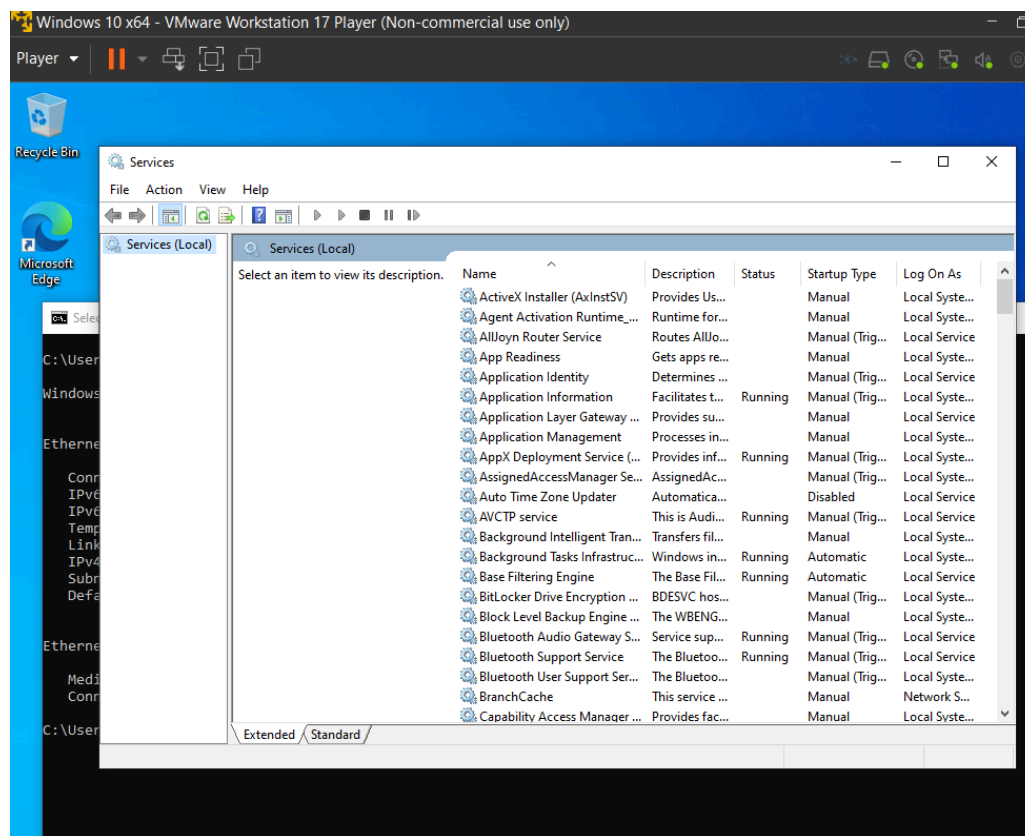
CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

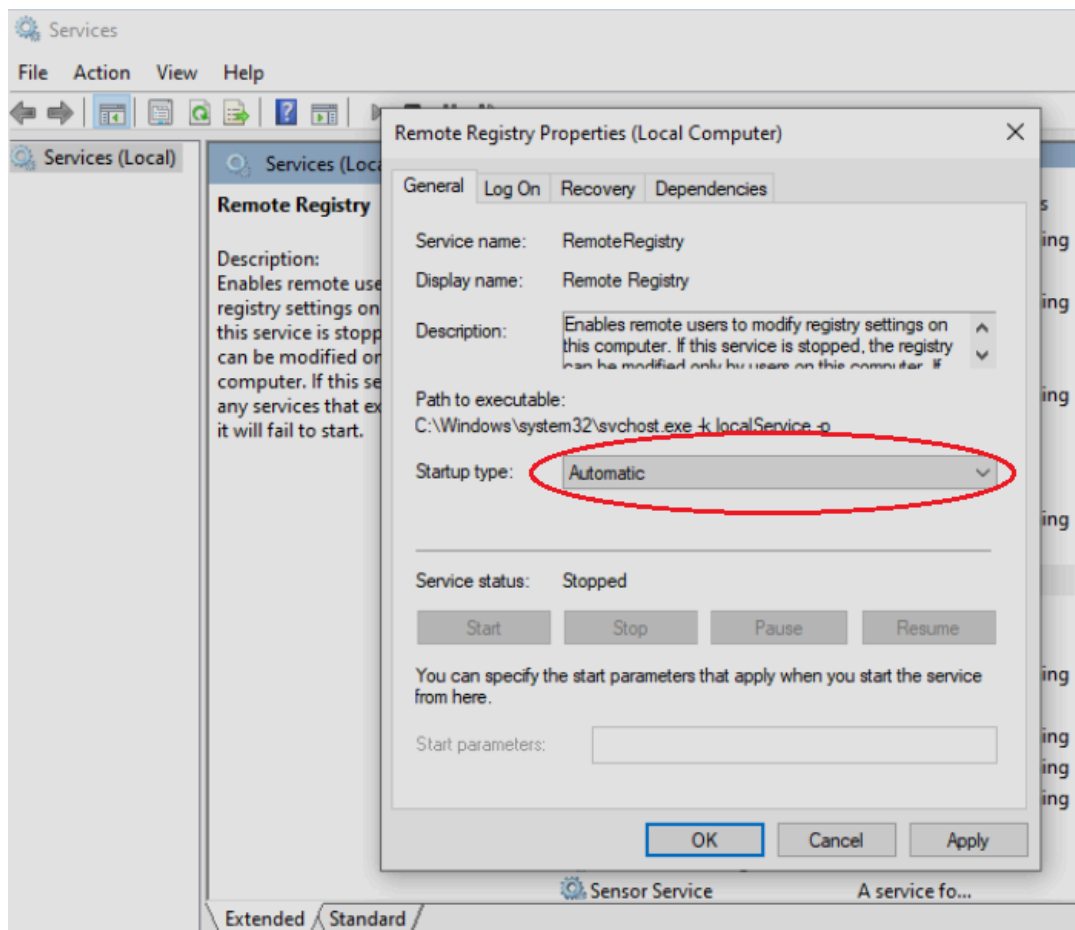
CVSS v2.0 Base Score: 5.8

CVSS v2.0 Vector:

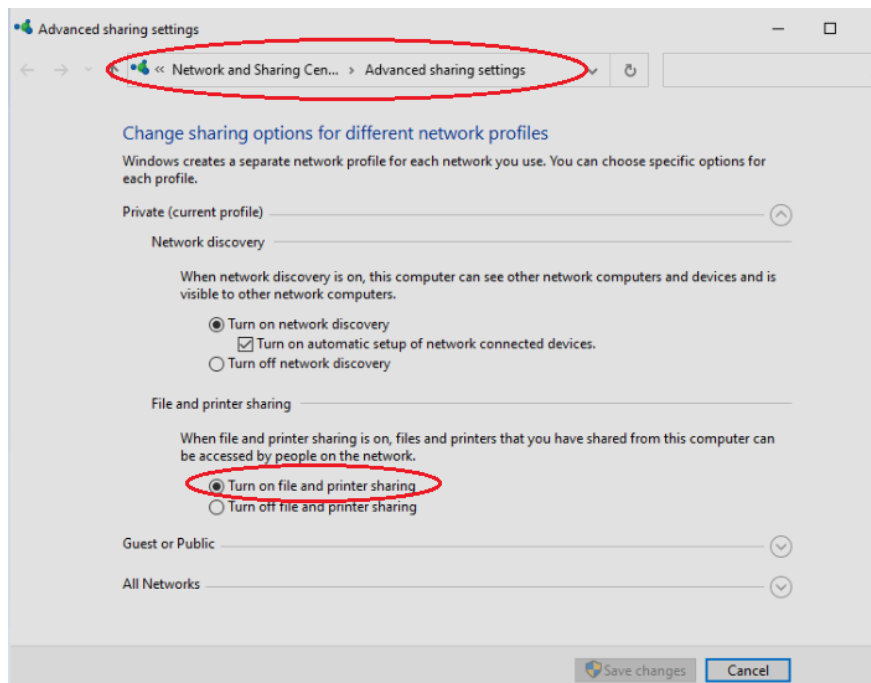
CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P

-
- Create a credential scan to see what more vulnerabilities are there
 - Return back the to VM and open “Services”
 - Enable “Remote Registry”, it will originally be disabled. The “startup type” should be automatic
 - This allows Nessus to connect to the registry

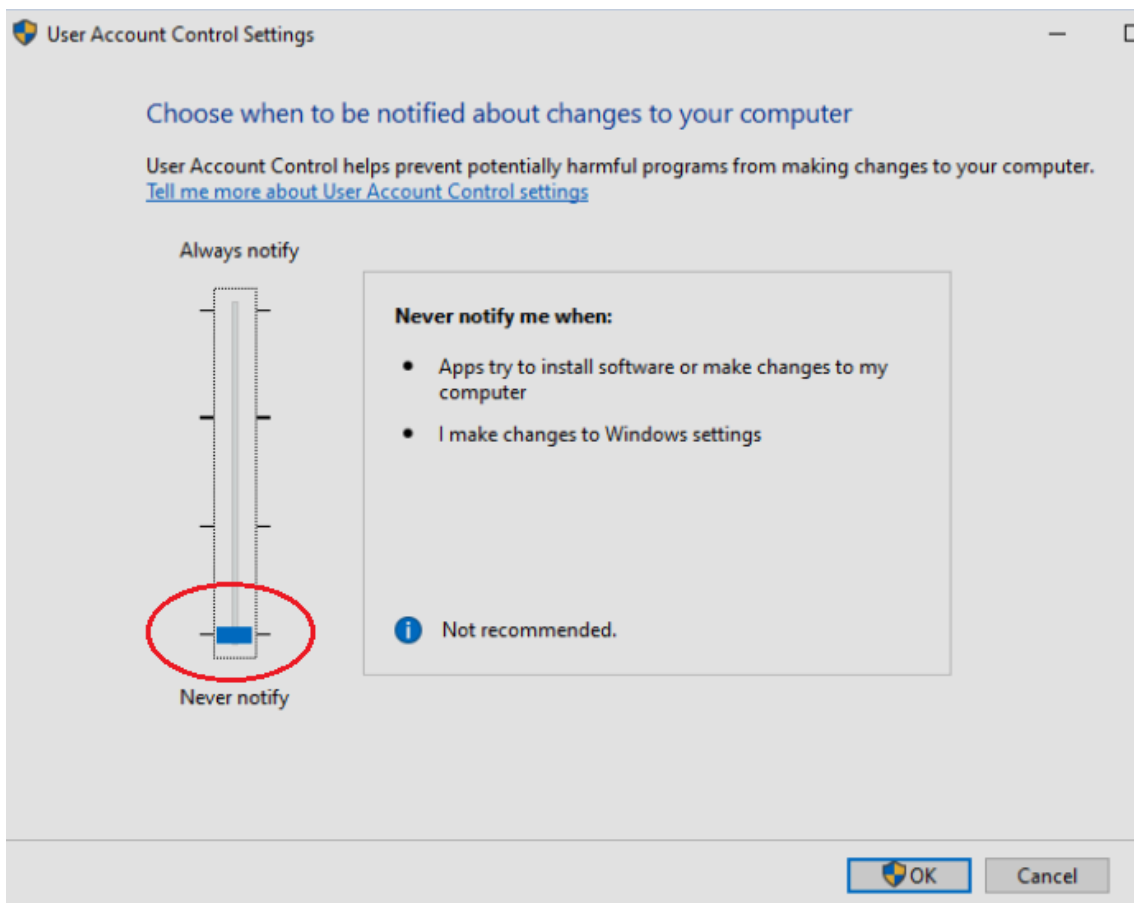
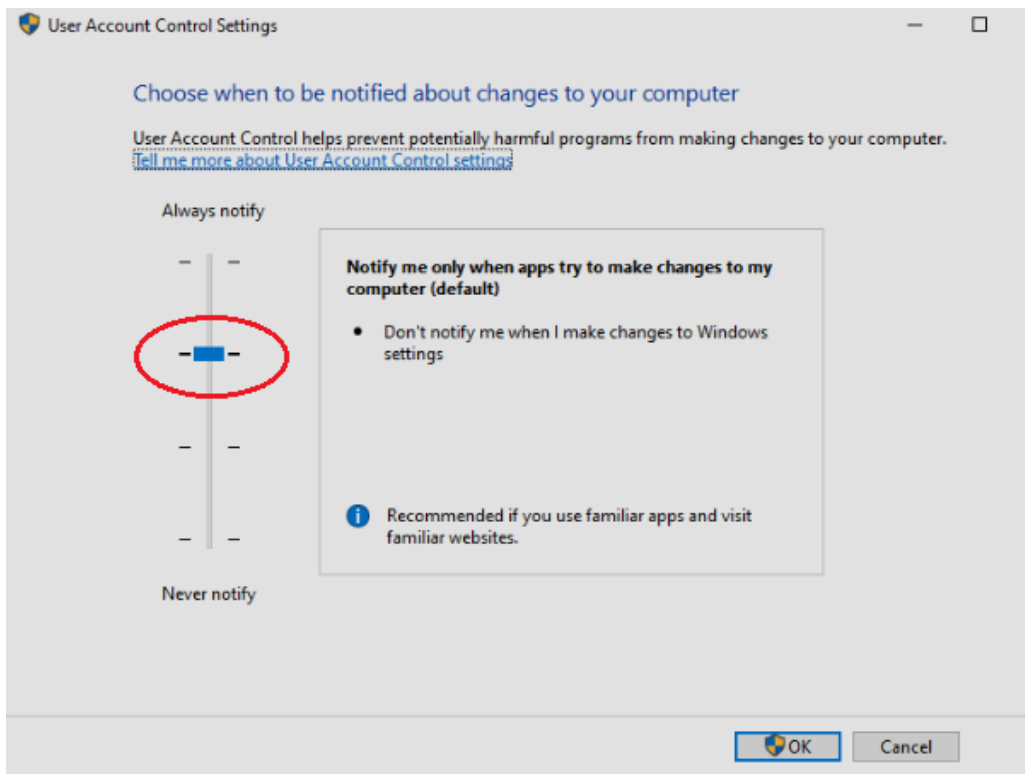




- Next, go to Control plane > Advanced sharing settings
- Make sure “Turn on file and printer sharing” radio button is selected



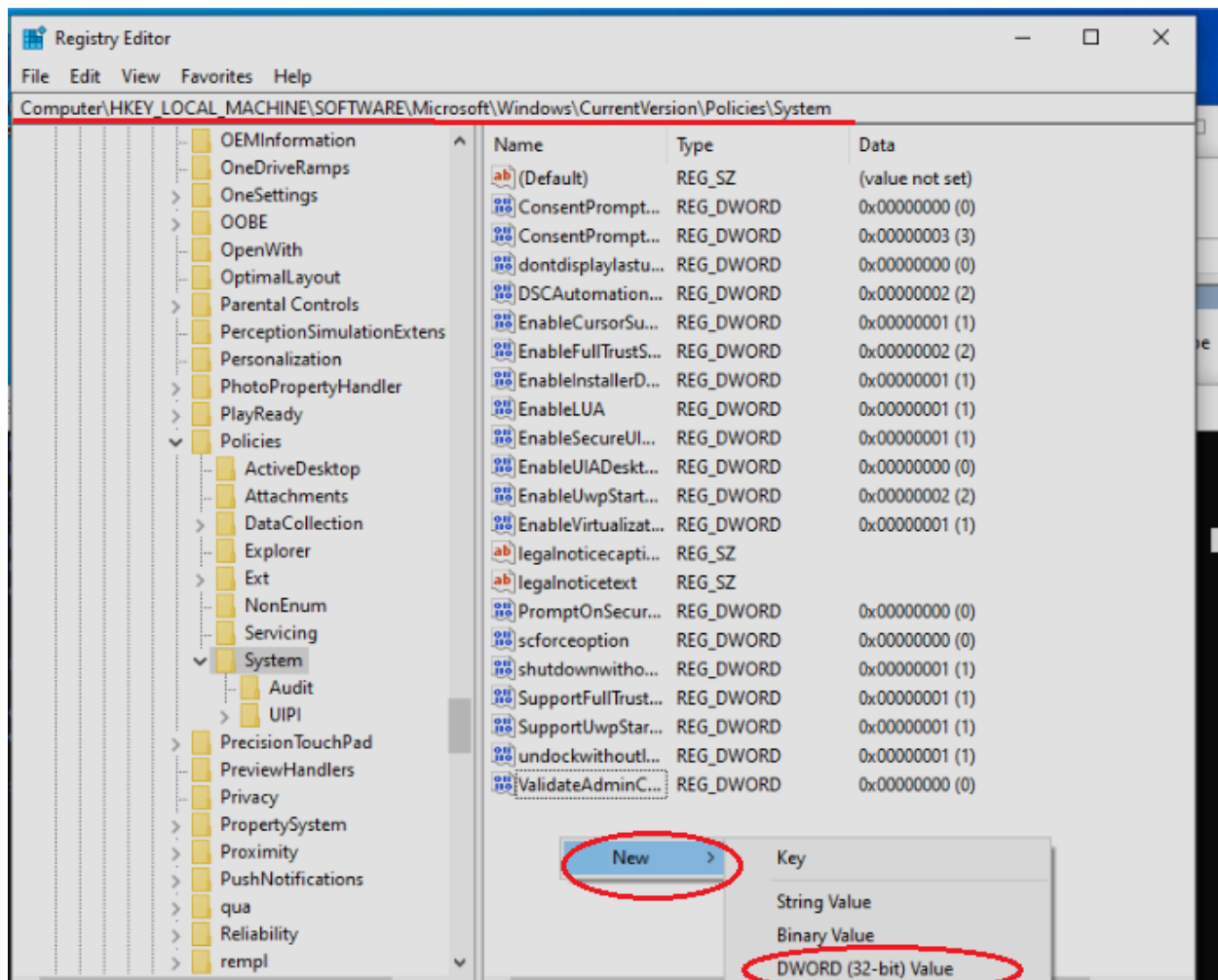
- Lastly, Adjust the “User Account Control Settings”



- Nessus recommends these steps for computers that are not on a domain, reminder although these steps are suggested, this does not mean you can perform this on any environment.
- Here is the documentation that suggests these modifications:
<https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm#Configure-a-Local-Account>

https://community.tenable.com/s/article/Scanning-with-non-default-Windows-Administrator-Account?language=en_US

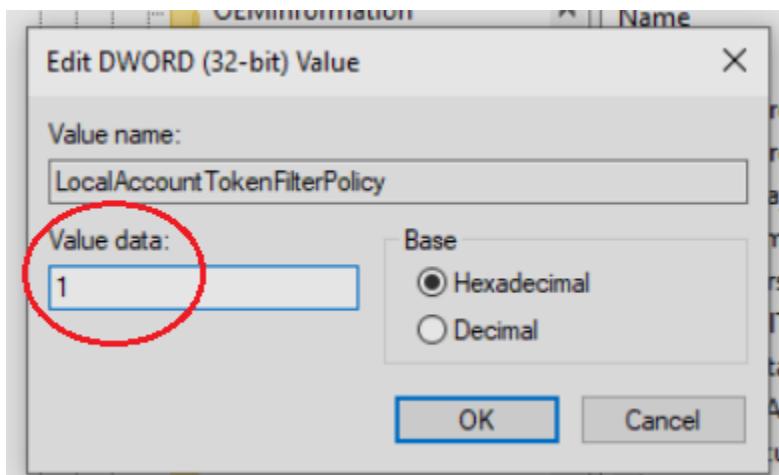
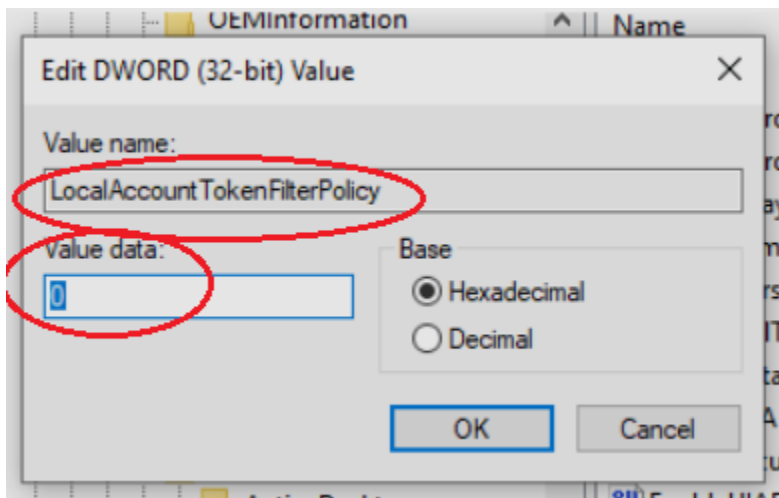
-
- Next step is to go to the Windows Registry
 - Navigate to this location to create a new “DWORD (32-bit) Value”



- Name the DWORD: LocalAccountTokenFilterPolicy

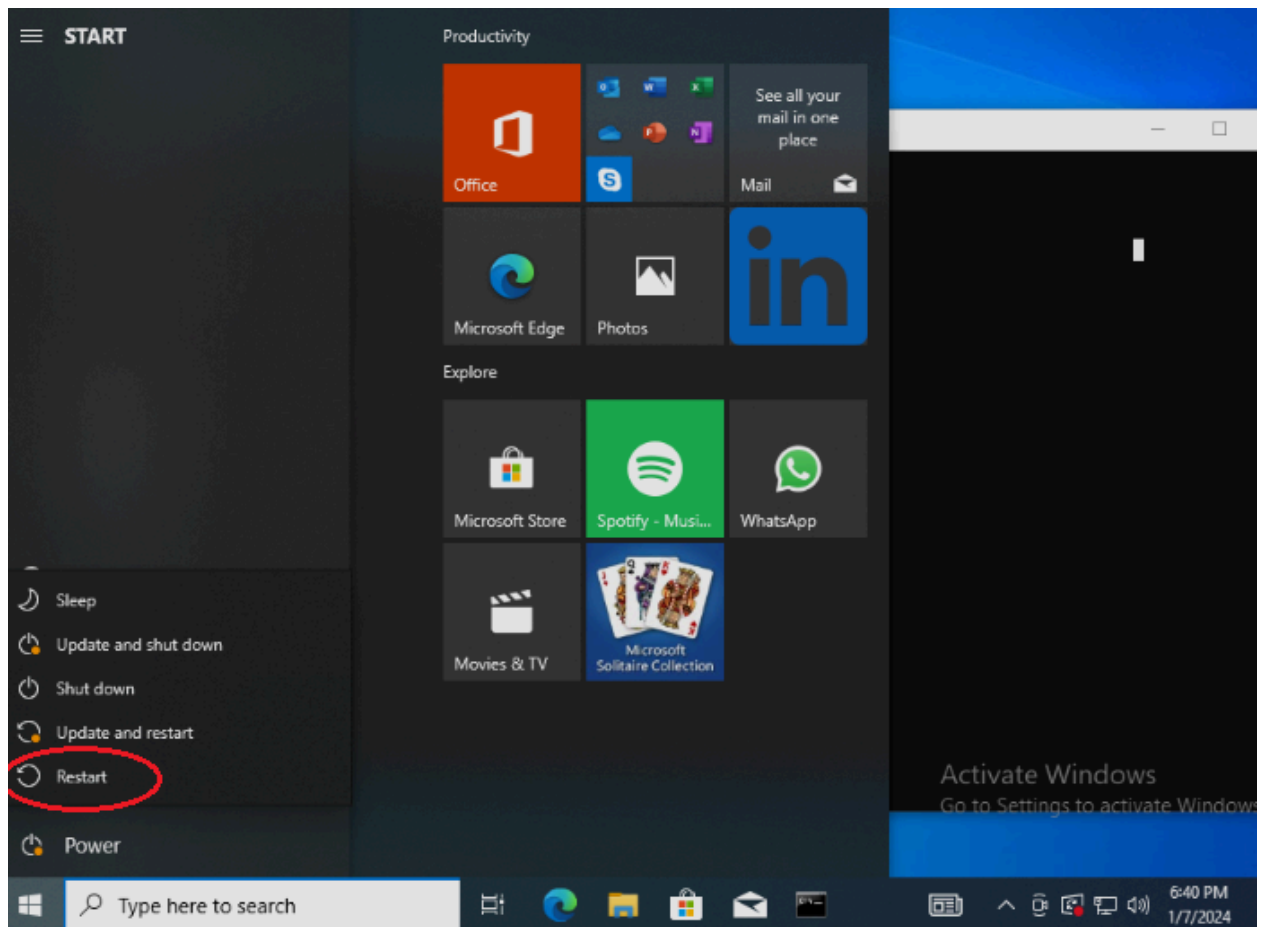
shutdownwitho...	REG_DWORD	0x00000001 (1)
SupportFullTrust...	REG_DWORD	0x00000001 (1)
SupportUwpStar...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)
LocalAccountTokenFilterPolicy		0x00000000 (0)

- Modify the DWORD to have a Value data of “1”



SupportFullTrust...	REG_DWORD	0x00000001 (1)
SupportUwpStar...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)
LocalAccountTo...	REG_DWORD	0x00000001 (1)

- Now, Restart your VM



-
- On your physical workstation, go to Nessus to create a new scan (credential)
 - Ensure that the IP address remains unchanged after the restart. If it has changed, you will be using the new IP address for the scan.

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Windows 10 VM Single Host - Credential

Description:

Folder: My Scans

Targets: 192.168.1.72

Upload Targets Add File

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings **Credentials** Plugins

CATEGORIES: Host

Filter Credentials

SSH

Windows

Windows

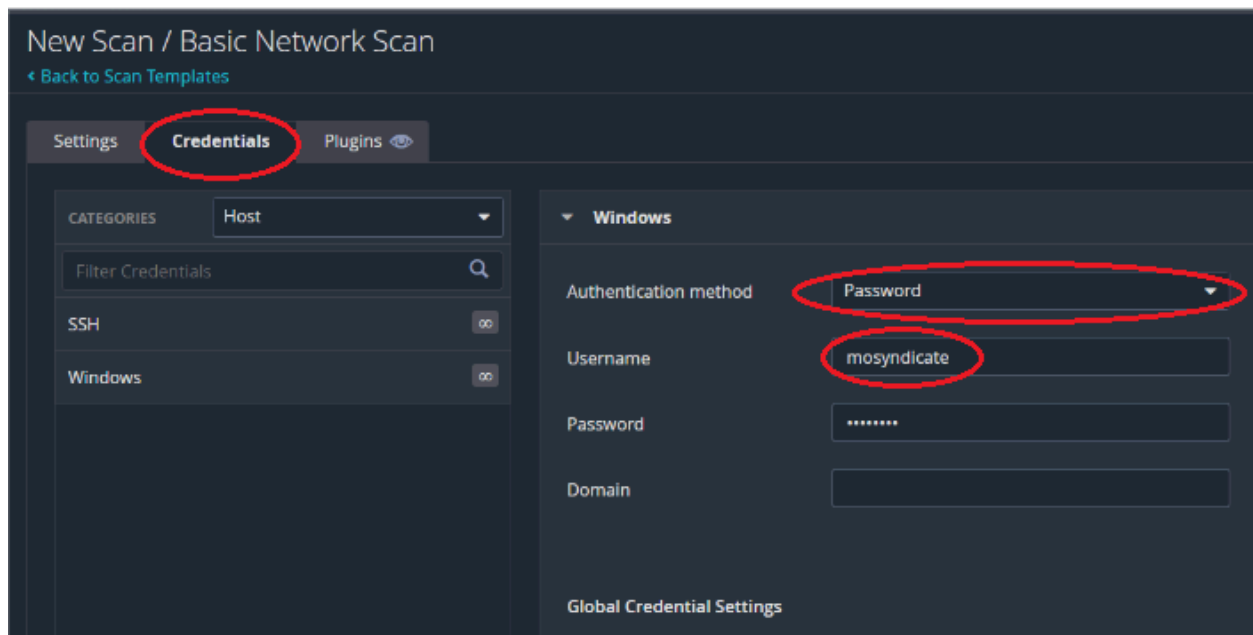
Authentication method: Password

Username: administrator REQUIRED

Password: REQUIRED

Domain:

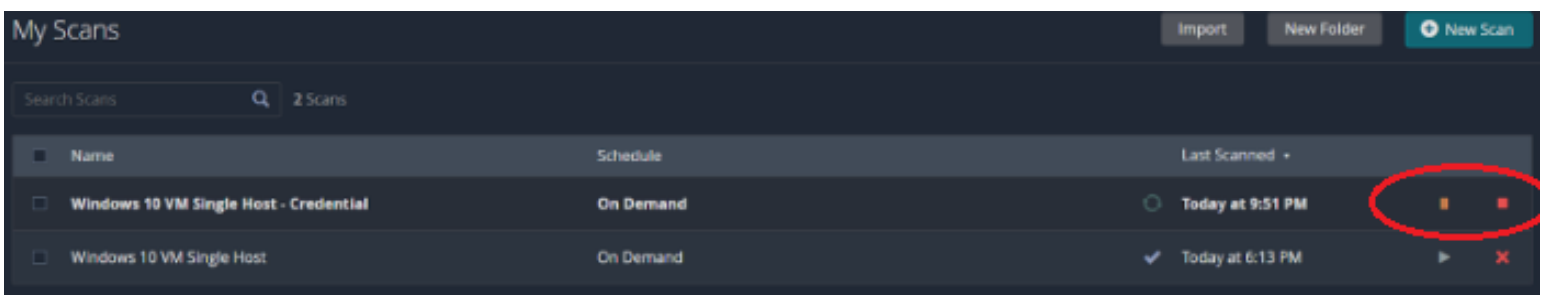
- Fill in the username and password for the VM



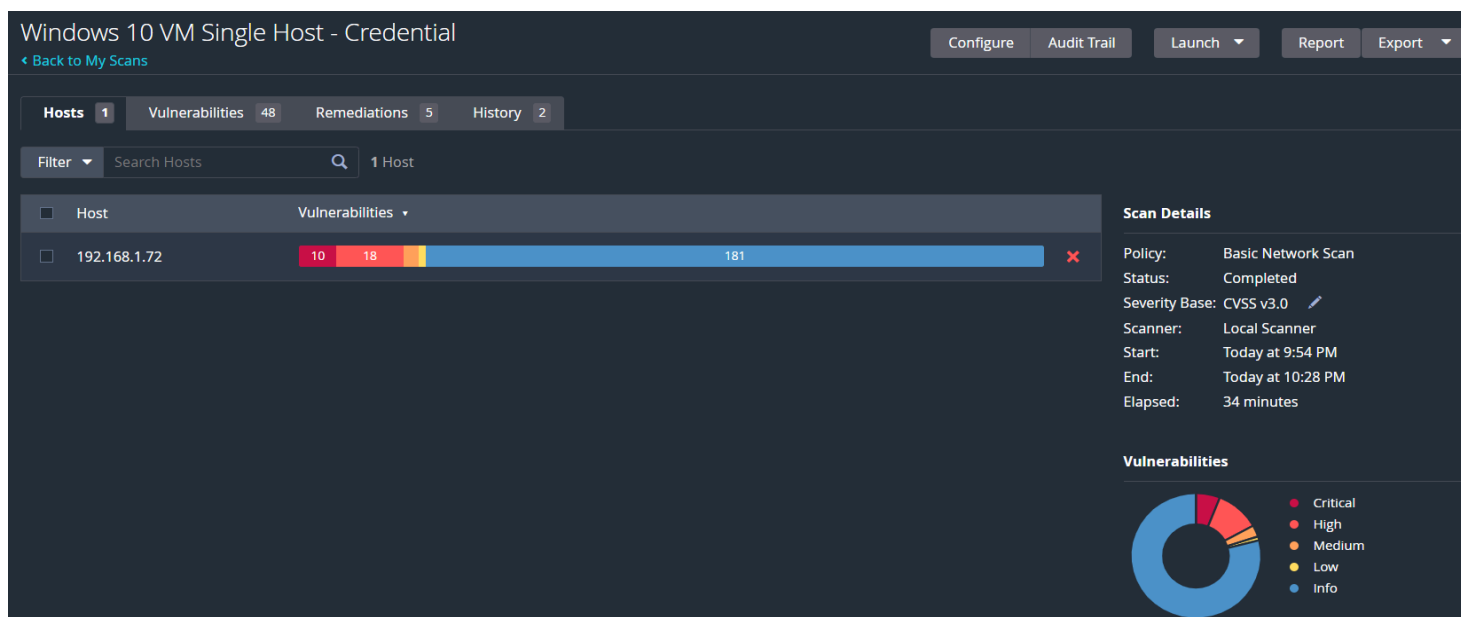
- If you do not know your username, return back to the command prompt and type in “whoami”

```
C:\Users\Mosyndicate>whoami
desktop-d8uutk8\mosyndicate
C:\Users\Mosyndicate>
```

- Once the new scan is complete, review the results which may reveal an increased number of vulnerabilities.



- After adding a credentialed scan, the vulnerabilities have jumped to 48 total. The highest being a critical with a CVSS of 9.5.



Windows 10 VM Single Host - Credential / 192.168.1.72

Configure Audit Trail Launch Report Exp

Vulnerabilities 48

Filter Search Vulnerabilities 48 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8	9.2	Curl 7.69 < 8.4.0 Heap Buffer Overflow	Misc.	2
MIXED	Microsoft Windows (Multiple Issues)	Windows	91
MIXED	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	10
MIXED	Microsoft .NET Framework (Multiple ...)	Windows : Microsoft Bulletins	4
MIXED	Microsoft Internet Explorer (Multiple...)	Windows	3
MIXED	Haxx Curl (Multiple Issues)	Windows	3
MIXED	VMware Tools (Multiple Issues)	Windows	2
MEDIUM	6.5	4.9	IP Forwarding Enabled	Firewalls	1
MEDIUM	5.3		SMB Signing not required	Misc.	1
LOW	3.3	1.4	Windows Snip & Sketch/ Snipping Tool CV...	Windows	1

Host Details

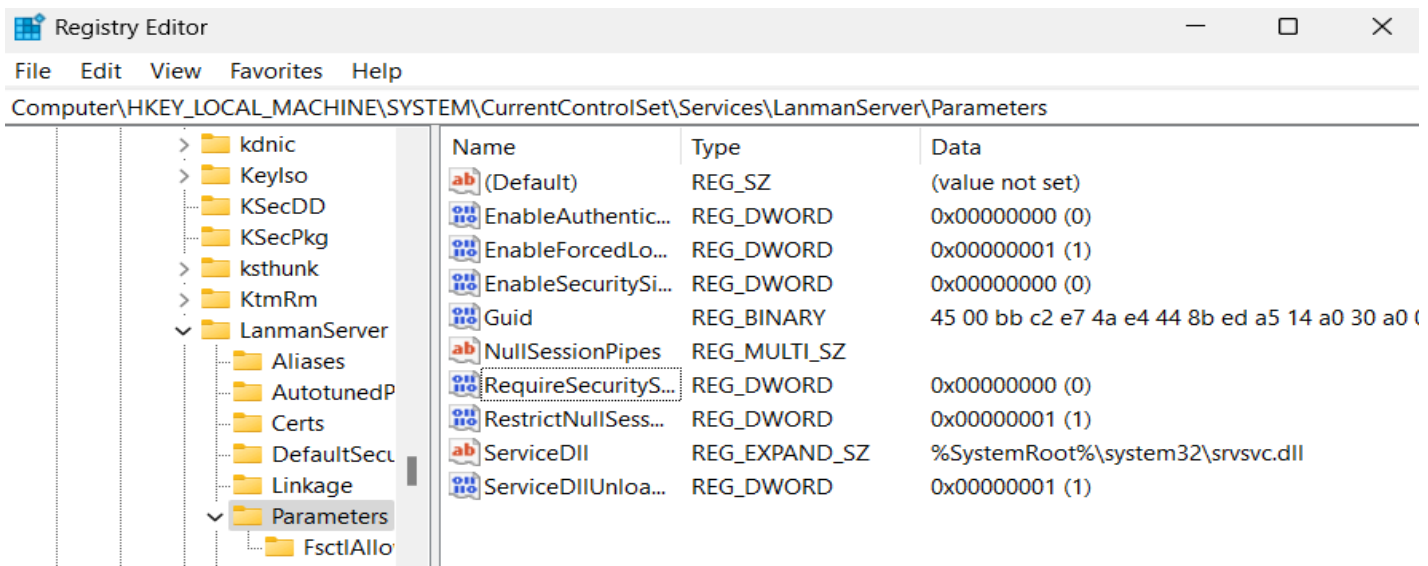
IP: 192.168.1.72
 MAC: 98:43:FA:4F:1A:D2
 OS: Microsoft Windows 10 Pro Bu 19045
 Start: Today at 9:54 PM
 End: Today at 10:28 PM
 Elapsed: 34 minutes
 KB: [Download](#)

Vulnerabilities

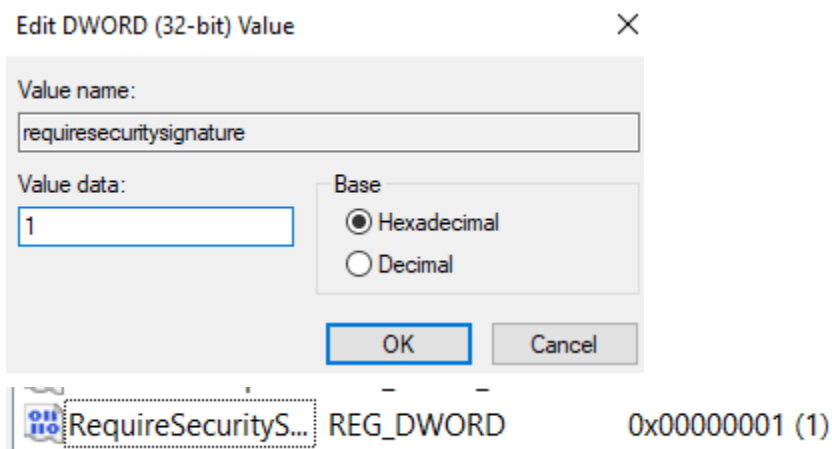
- From here I will download some legacy applications and make the system even more insecure. And then the challenge is to remediate all the vulnerabilities to the best of our ability.

- From here, your goal is to remediate all the issues presented on Nessus. You will need to use the scan details, solutions mentioned in the remediation tab and researching about the CVEs. This is a challenge, you can delete this specific virtual machine after when you are done or use it as your personal sandbox.

- Here, we will try to remove this vulnerability



- First we will need to navigate to the Registry Editor



- Edit the Data Value “RequireSecuritySignature” in the Registry Editor from a 0 to a 1

MEDIUM5.3SMB Signing not requiredMisc.1

Windows 10 VM Single Host - Credential / Plugin #57608

< Back to Vulnerabilities

Hosts1Vulnerabilities47Remediations2History7

MEDIUMSMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

<http://www.nessus.org/u?df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?74b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.1.72

- This is where I found the link to remediate the issue. Looking to the “See Also” links of the urls has lead me to the microsoft page to help me get rid of this issue

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing>

- Here is the resolution for the fix that I used

Policy locations for SMB signing

The policies for SMB signing are located in **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.

- Microsoft network client: Digitally sign communications (always)**
Registry key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters`
Registry value: **RequireSecuritySignature**
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)
- Microsoft network client: Digitally sign communications (if server agrees)**
Registry key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters`
Registry value: **EnableSecuritySignature**
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)
- Microsoft network server: Digitally sign communications (always)**
Registry key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters`
Registry value: **RequireSecuritySignature**
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)
- Microsoft network server: Digitally sign communications (if client agrees)**
Registry key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters`
Registry value: **EnableSecuritySignature**
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)

Note In these policies, "always" indicates that SMB signing is required, and "if server agrees" or "if client agrees" indicates that SMB signing is enabled.

Additional resources

Documentation

[Microsoft network client Digitally sign communications \(always\) - Windows Security](#)

Best practices and security considerations for the Microsoft network client Digitally sign communications (always) security policy setting.

[Network access Restrict anonymous access to Named Pipes and Shares - Windows Security](#)

Best practices, security considerations, and more for the security policy setting, Network access Restrict anonymous access to Named Pipes and Shares.

Understanding "RequireSecuritySignature" and "EnableSecuritySignature"

The **EnableSecuritySignature** registry setting for SMB2+ client and SMB2+ server is ignored. Therefore, this setting does nothing unless you're using SMB1. SMB 2.02 and later signing is controlled solely by being required or not. This setting is used when either the server or client requires SMB signing. Only if both have signing set to 0 will signing not occur.

Expand table

-	Server – RequireSecuritySignature=1	Server – RequireSecuritySignature=0
Client – RequireSecuritySignature=1	Signed	Signed
Client – RequireSecuritySignature=0	Signed	Not signed

Reference

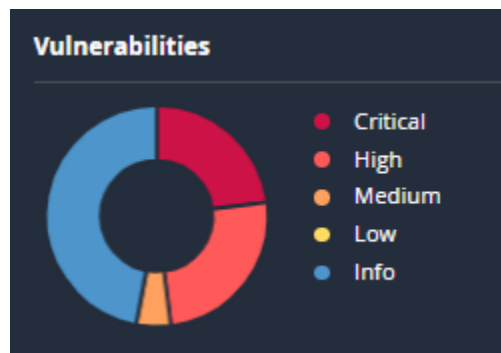
[Configure SMB Signing with Confidence](#)

[How to Defend Users from Interception Attacks via SMB Client Defense](#)

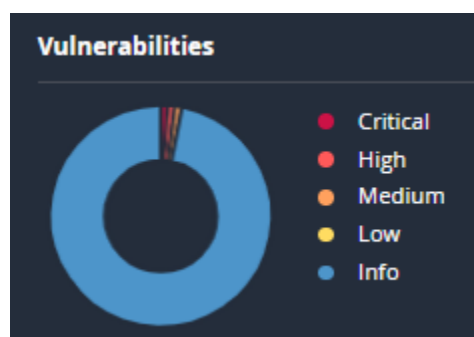
[SMB 2 and SMB 3 security in Windows 10: the anatomy of signing and cryptographic keys](#)

[SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions](#)

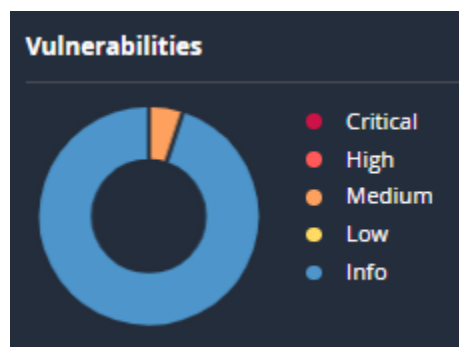
[Netdom computename](#)



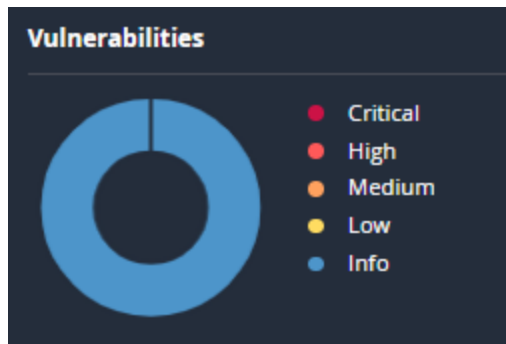
- Results after the first credentialed scan



- Results after remediating and doing a few more scans to see the progress of my remediation efforts
- This is the results from my home lab workstation:



- Before



- After
- Regular maintenance and remediation efforts are essential for maintaining security in your home lab workstation or in the workplace. Embrace the challenge of securing your environment, knowing that vigilance and ongoing efforts are crucial in the realm of cybersecurity. Good luck!

Nessus Vulnerability Project: Strengthening Cybersecurity

In today's digital landscape, where cyber threats loom large, the importance of vulnerability testing and remediation cannot be overstated. Whether in a home lab workstation setup or within the confines of a workplace environment, regular maintenance and remediation efforts stand as pillars of defense against malicious actors seeking to exploit weaknesses in systems and networks.

At the heart of vulnerability assessment lies tools like Nessus, a potent asset in the arsenal of cybersecurity professionals. Nessus, with its robust features and comprehensive scanning capabilities, empowers users to identify vulnerabilities within their systems, allowing for proactive measures to be taken before potential threats escalate into breaches. Its

user-friendly interface and extensive database of vulnerabilities make it an indispensable tool in the quest for fortified security.

However, Nessus is but one piece of the puzzle in the broader landscape of vulnerability management. Other vulnerability scanners offer complementary features and strengths, each bringing its own unique advantages to the table. From open-source solutions like OpenVAS to commercial offerings such as Qualys, the diversity of vulnerability scanning tools caters to varying needs and preferences, ensuring that organizations can select the most suitable toolset to fortify their defenses.

Yet, the acquisition of sophisticated tools alone does not guarantee impregnable security. The true essence of cybersecurity lies in fostering a culture of vigilance and awareness. Security consciousness must permeate every facet of an organization, from top-level management to frontline employees. Regular training programs, simulated phishing exercises, and ongoing education initiatives serve to arm individuals with the knowledge and skills needed to thwart evolving threats effectively.

Moreover, the journey towards cybersecurity excellence is not a one-time endeavor but an ongoing commitment. Just as threats evolve, so too must our defenses. Regular vulnerability assessments, supplemented by thorough remediation efforts, form the cornerstone of a proactive security posture. By diligently addressing vulnerabilities as they arise and staying abreast of emerging threats, organizations can stay one step ahead of adversaries, safeguarding their assets and preserving the trust of their stakeholders.

In the context of a home lab workstation, the same principles apply with equal relevance. Whether you're a cybersecurity enthusiast honing your skills or an IT professional testing new configurations, maintaining a secure environment is paramount. Embrace the challenge of

securing your digital domain, recognizing that every vulnerability addressed is a victory won in the ongoing battle for cybersecurity supremacy.

In closing, let us remember that cybersecurity is not merely a technical endeavor but a collective responsibility. By working together, sharing knowledge, and remaining vigilant, we can build a safer digital ecosystem for all. So, as you embark on your vulnerability testing and remediation journey, know that your efforts are not in vain. Share this project to anyone you think will benefit from it or would enjoy taking a look, thank you. Your dedication to securing your environment contributes to a safer and more resilient cyber world.