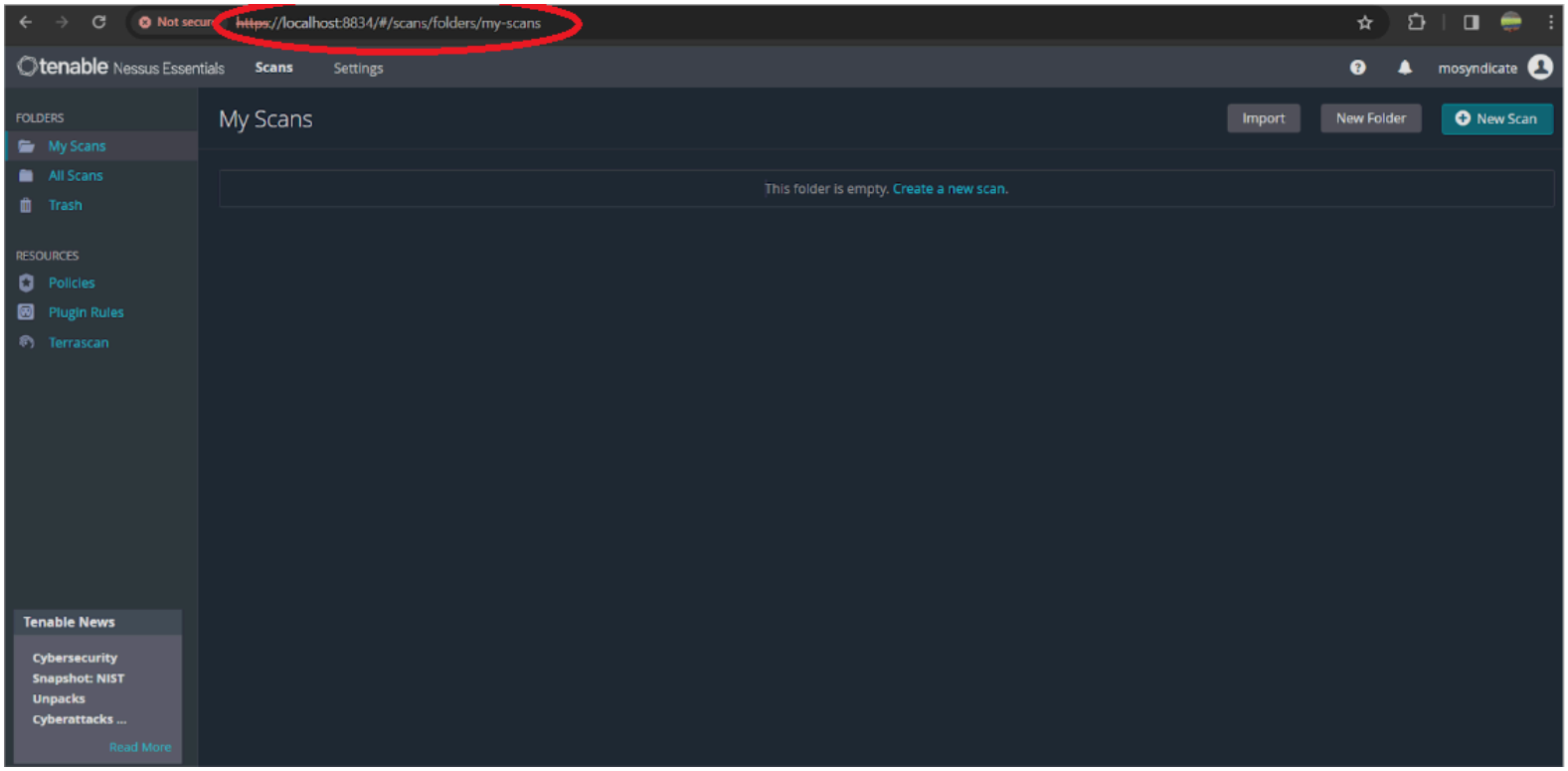
Vulnerability Testing With Nessus

- To do this project, you will need:
  - Nessus Essential
  - VMWare Workstation 17 Player (Any VM will suffice)
  - Microsoft ISO File

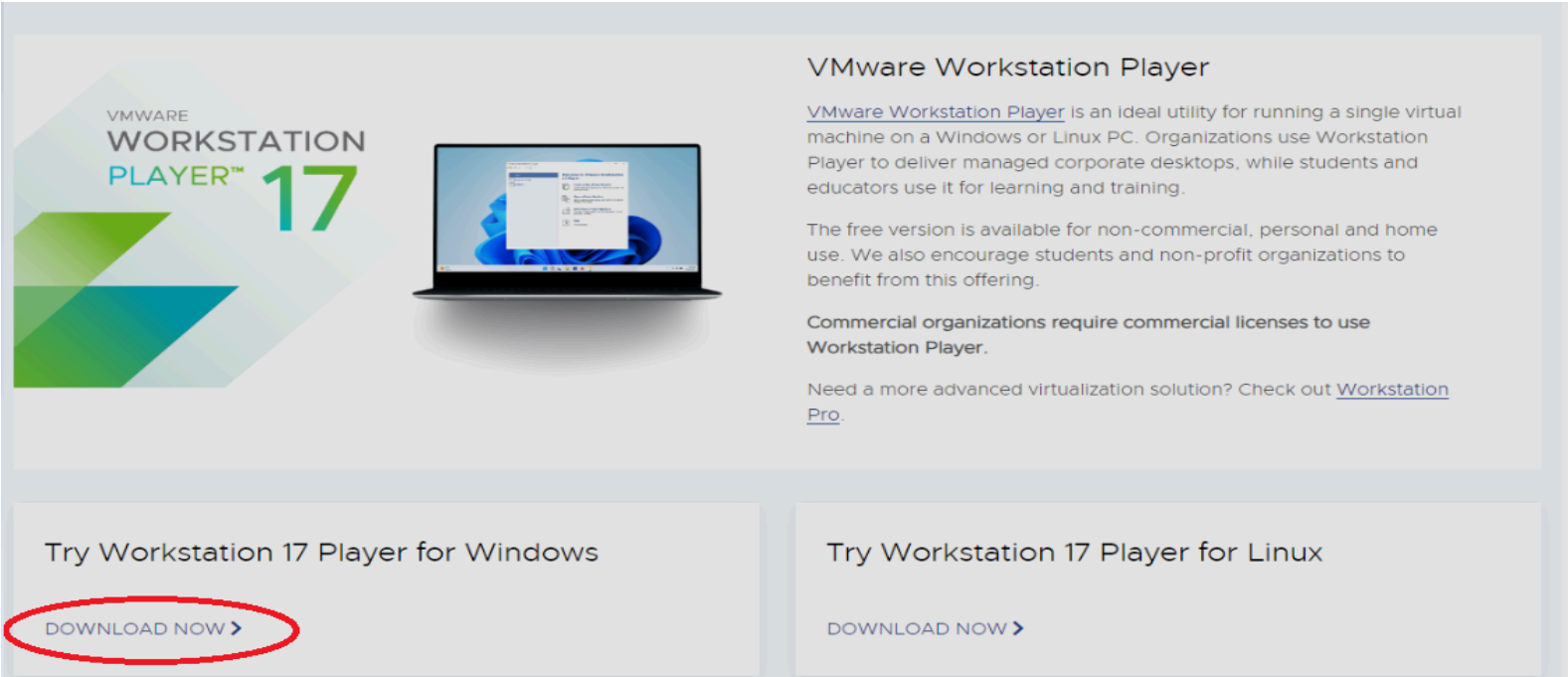
- Download Nessus Essentials:
- After downloading Nessus, you can access it by going to “https://localhost:8834”



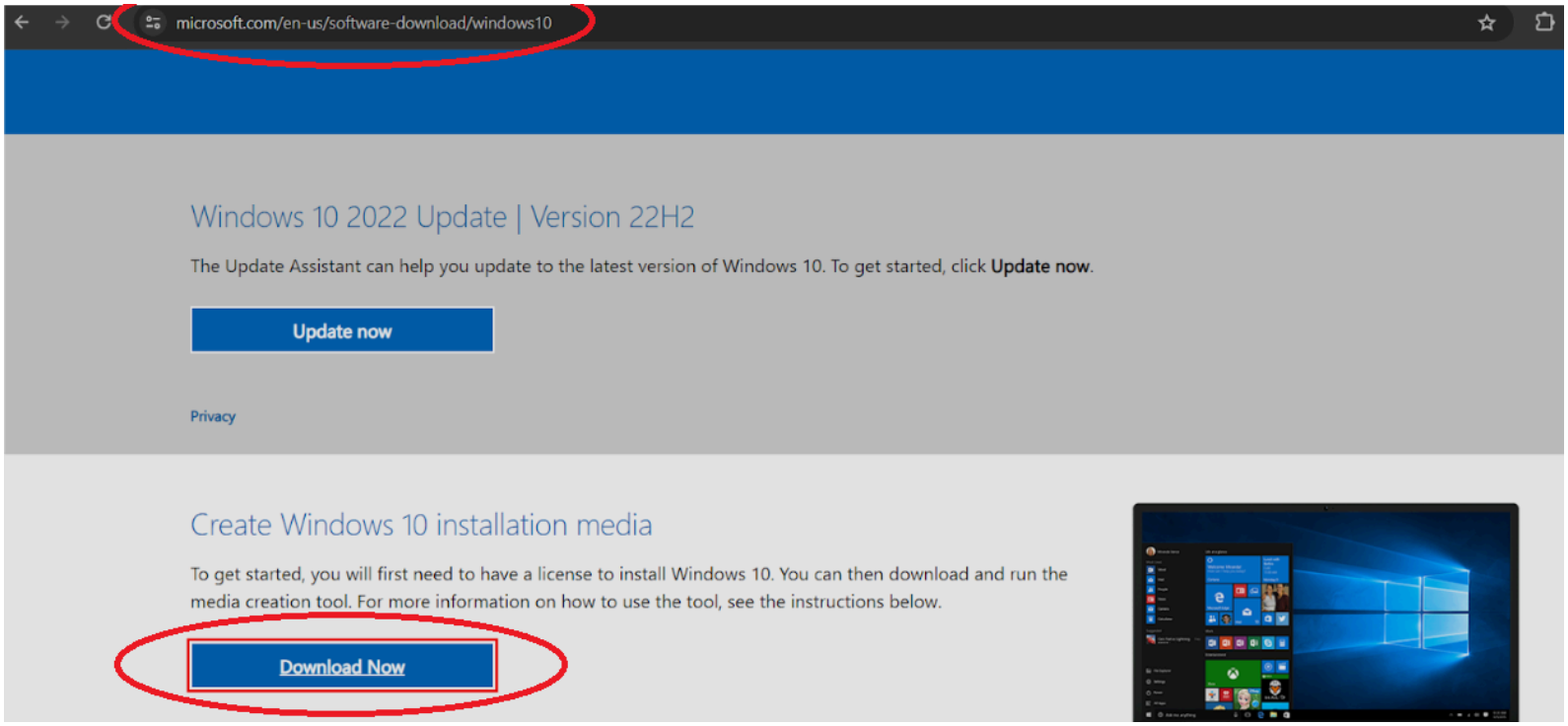
- Download VMWare Workstation 17 Player:
- Visit the VMWare website and download VMWare Workstation 17 Player or any alternative VM.
- Navigate to:

https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

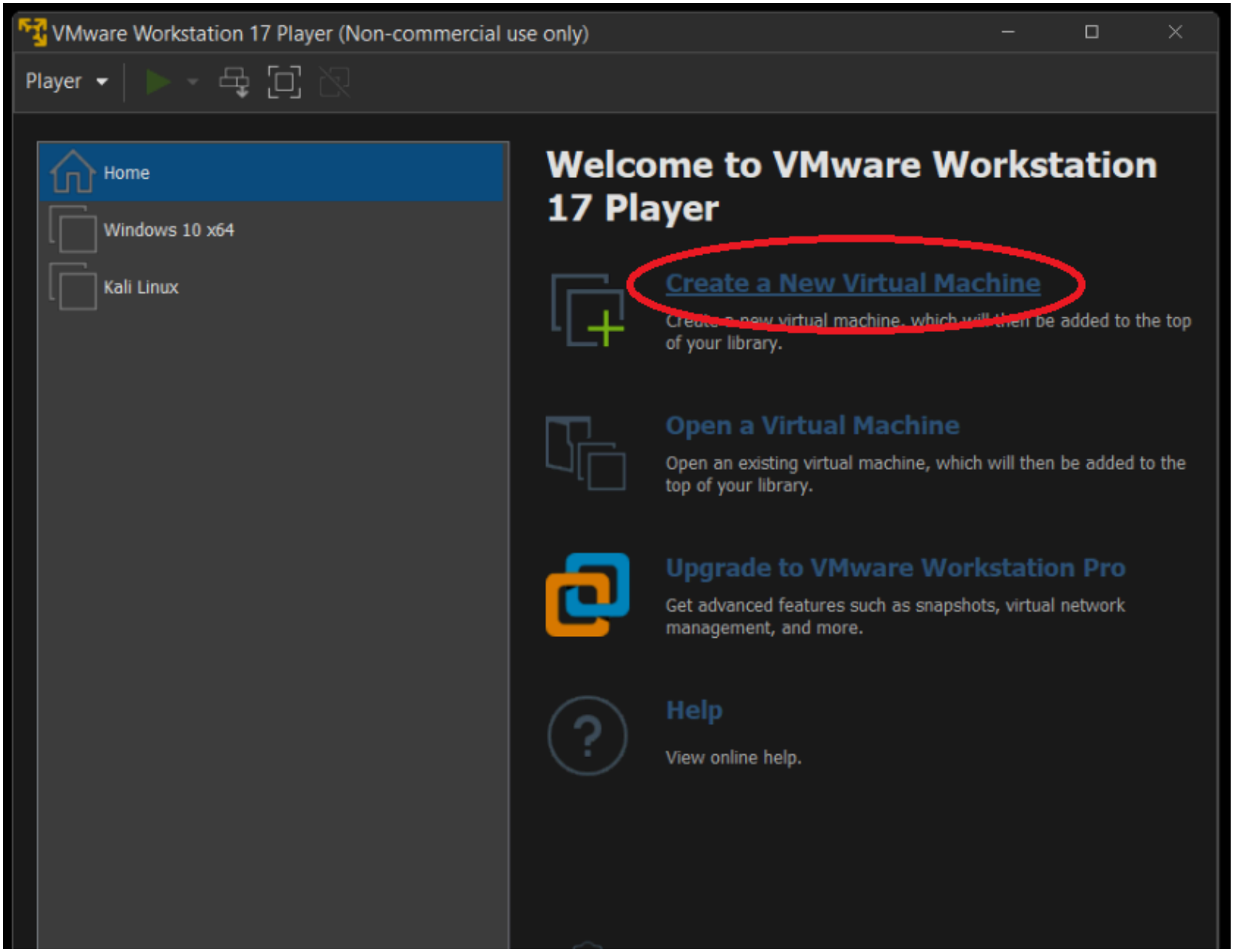
- Click on "DOWNLOAD NOW" to initiate the download.



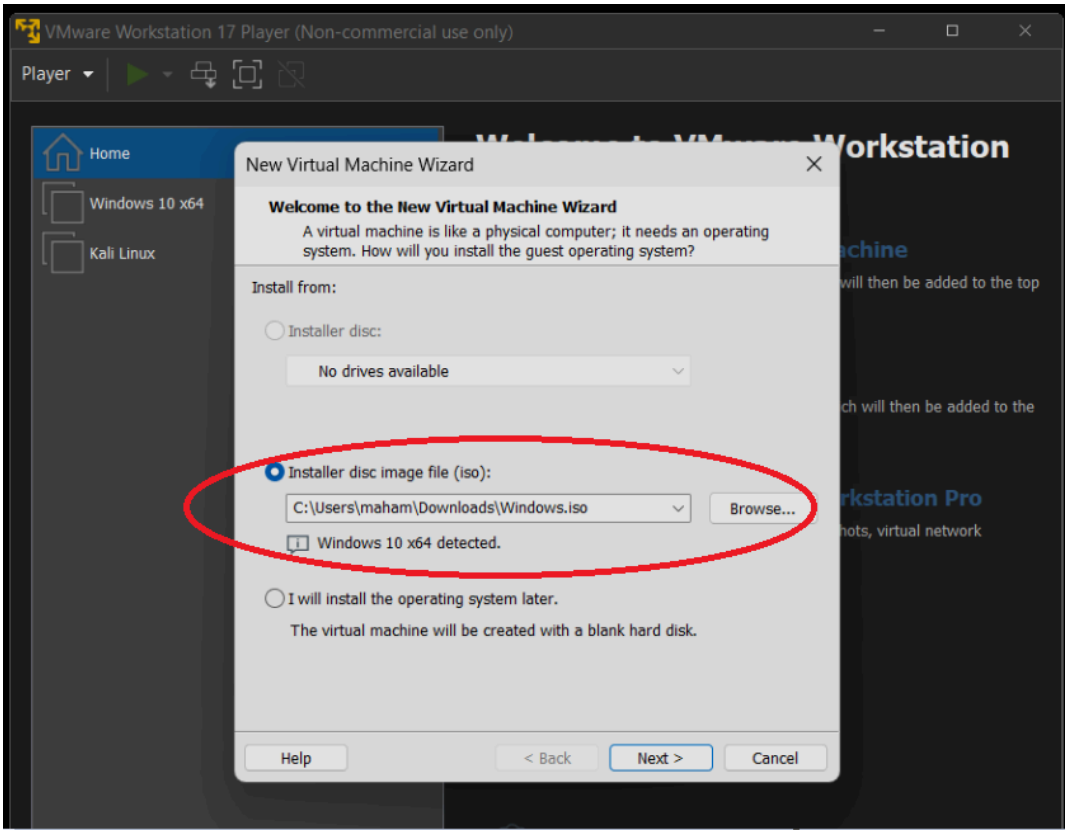
- Obtain a Windows 10 installation media by downloading the ISO file from the Microsoft website.
- Navigate to: https://www.microsoft.com/en-us/software-download/windows10
- Click on "Download Now" to proceed.



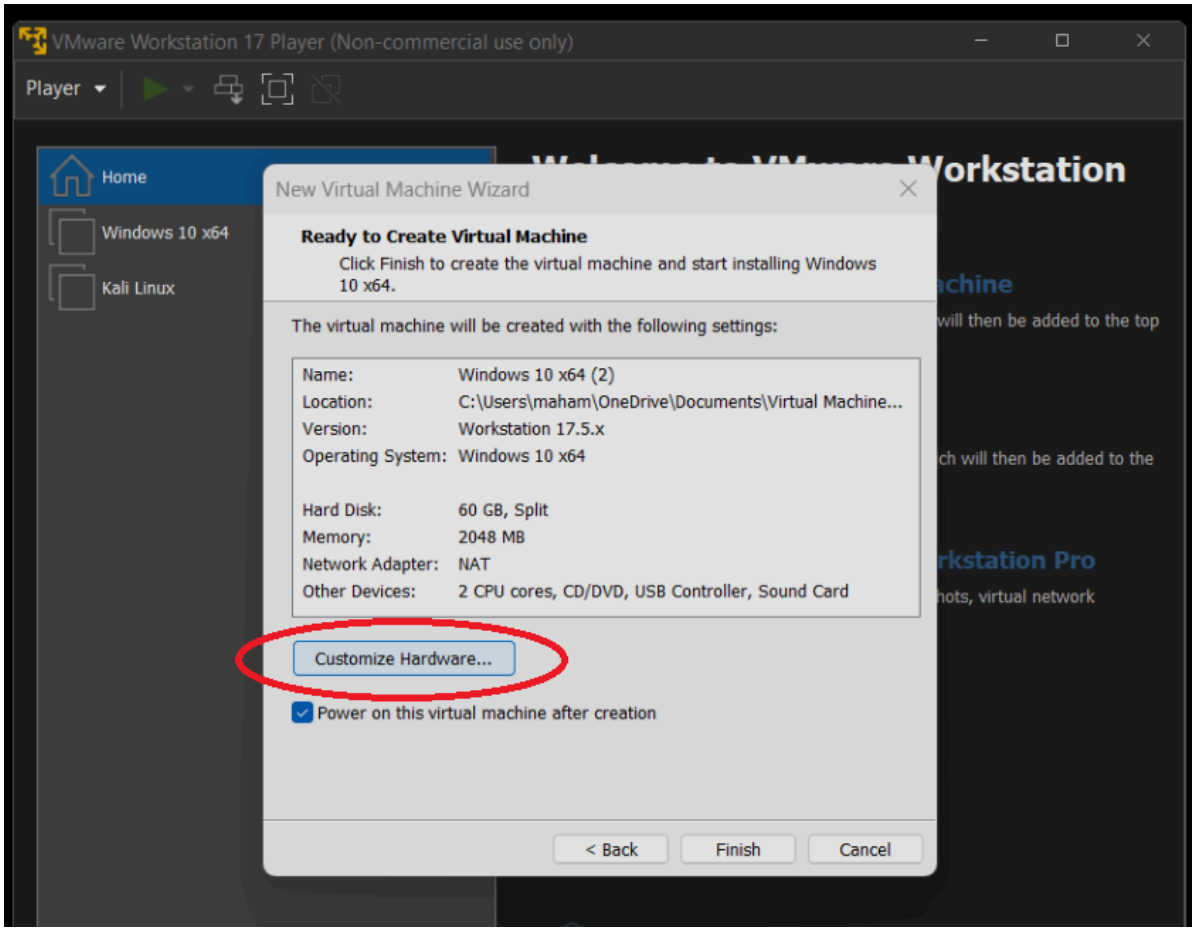
- Launch VMWare Player after downloading both VMWare Player and the Windows ISO file. Select “Create a New Virtual Machine”.



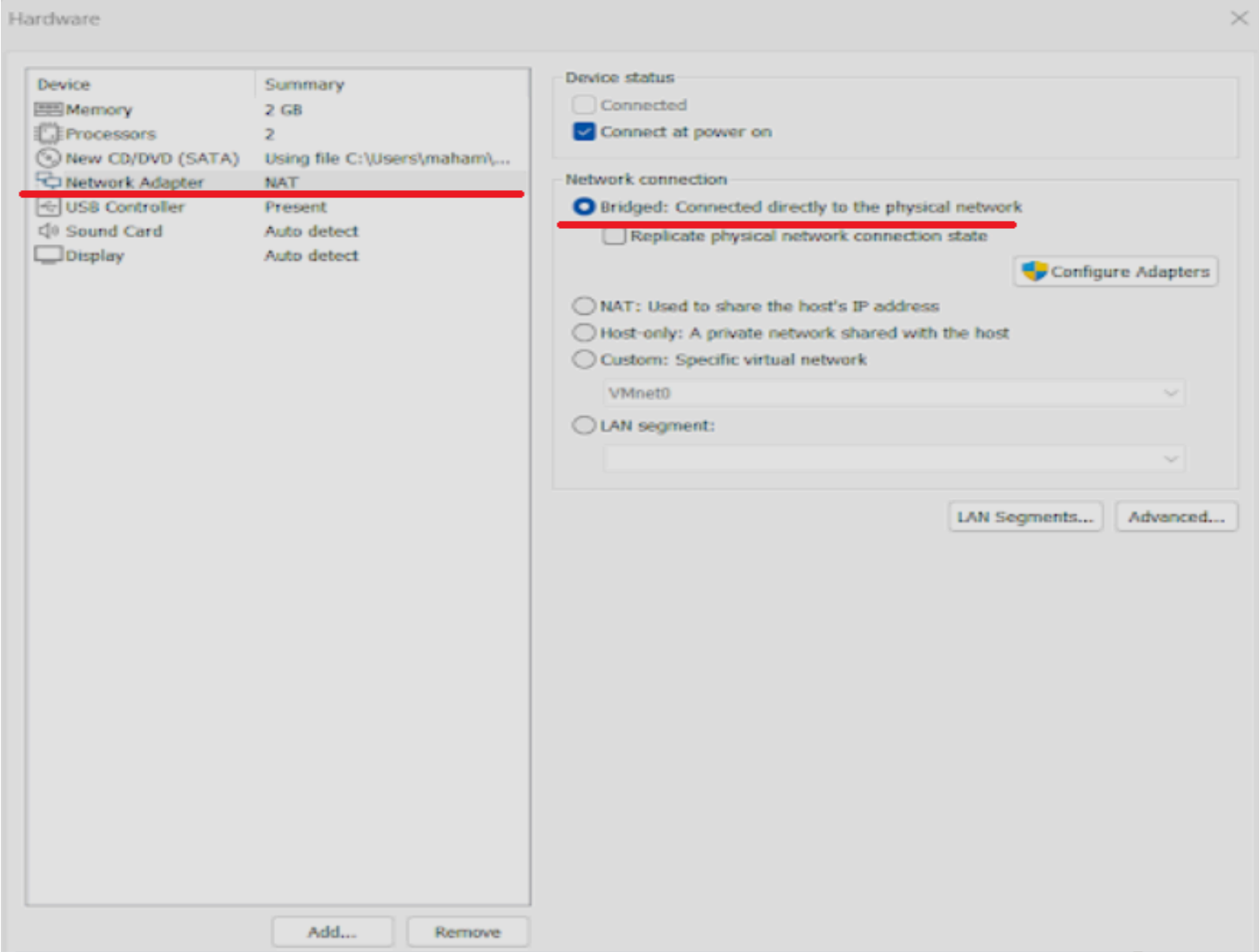
- You will need to select the middle radio button to use to ISO file.
- After browsing to where you downloaded the ISO file, you click “Next”.



- 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.

Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)

Player

Recycle Bin

Microsoft Edge

Command Prompt

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mosyndicate>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : attlocal.net
   IPv6 Address. . . . . . . . . . . : [redacted]
   IPv6 Address. . . . . . . . . . . : [redacted]
   Temporary IPv6 Address. . . . . . : [redacted]
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.1.72
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : [redacted]
                                       192.168.1.254

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\Mosyndicate>
```

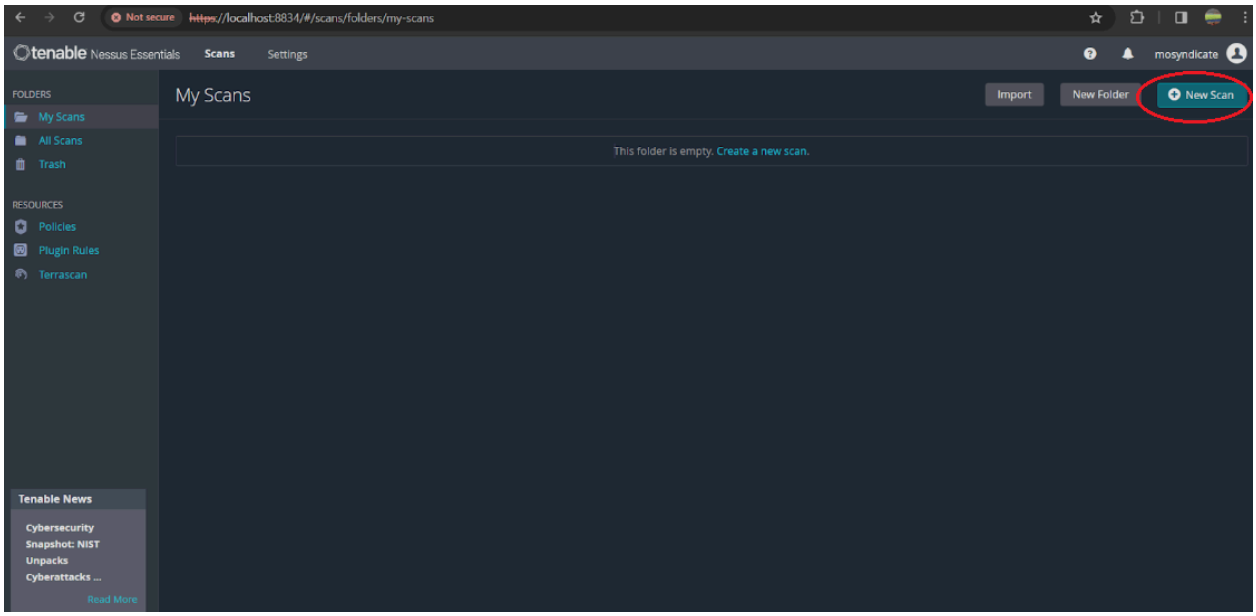
- Here, I am pinging the ip address from my workstation.

Command Prompt

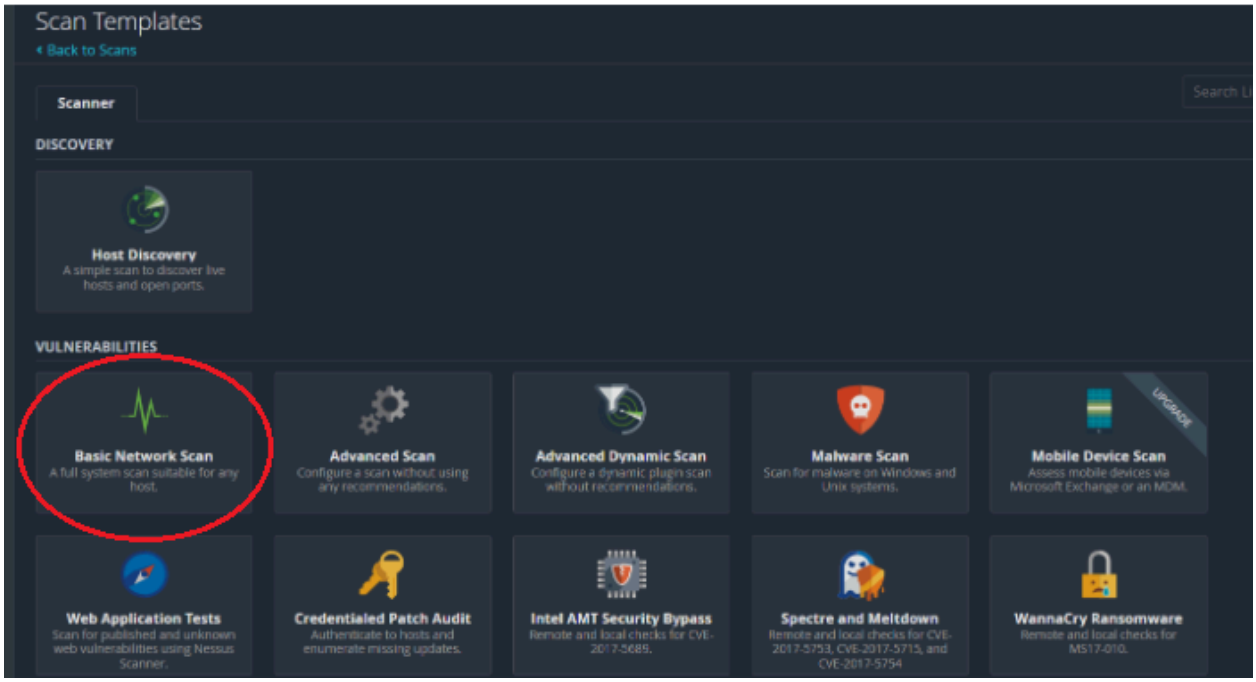
```
Microsoft Windows [Version 10.0.22621.2861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\maham>ping 192.168.1.72

Pinging 192.168.1.72 with 32 bytes of data:
Reply from 192.168.1.72: bytes=32 time<1ms TTL=128
Reply from 192.168.1.72: bytes=32 time<1ms TTL=128
Reply from 192.168.1.72: bytes=32 time<1ms TTL=128
Reply from 192.168.1.72: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\maham>
```

- 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.

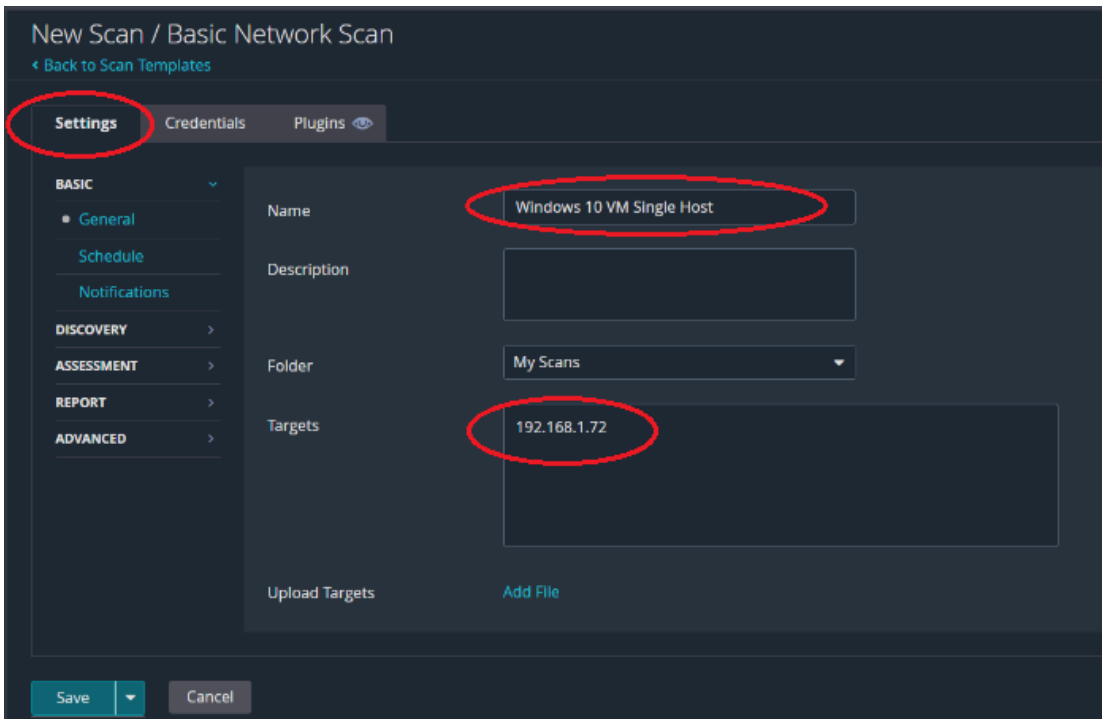
- Return back to Nessus on your workstation
- Select “New Scan”



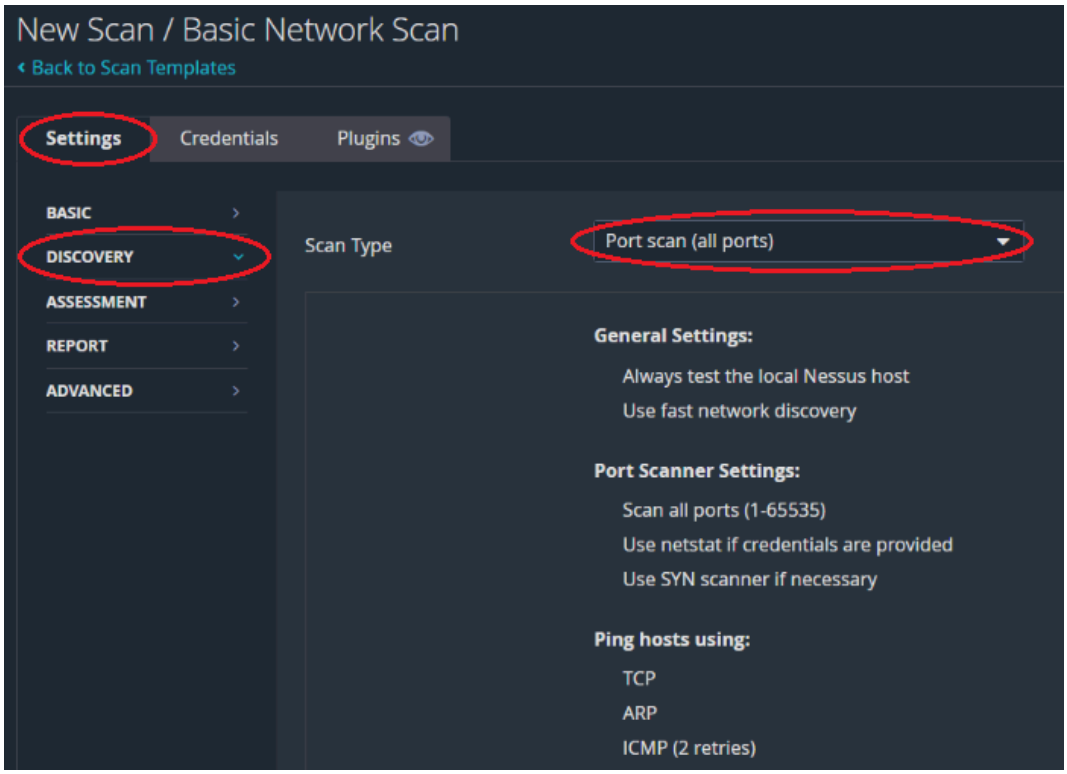
- Select “Basic Network Scan

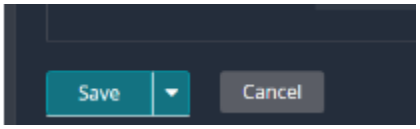


- Input the IP address of the virtual machine and input a name and a description of your choice

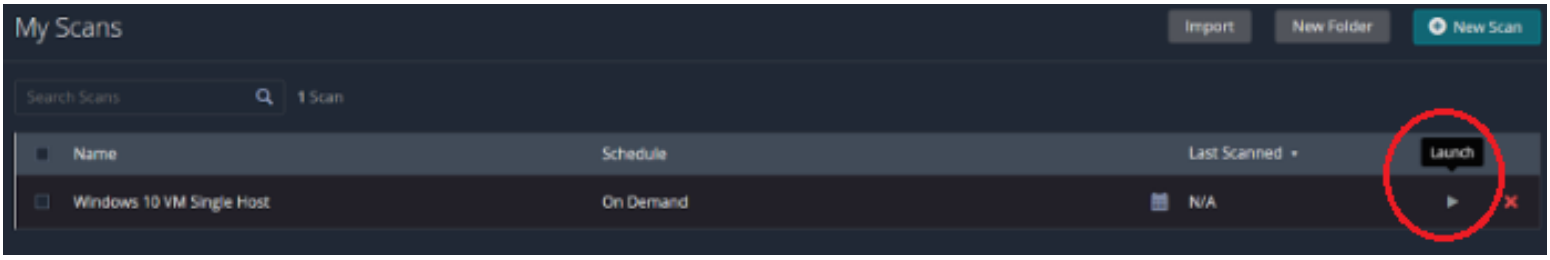


- If you would like to scan all port and not just common ports, go to the "Discovery" drop down (Scanning all ports will take longer than just the common ports)
- After that, you will need to save it

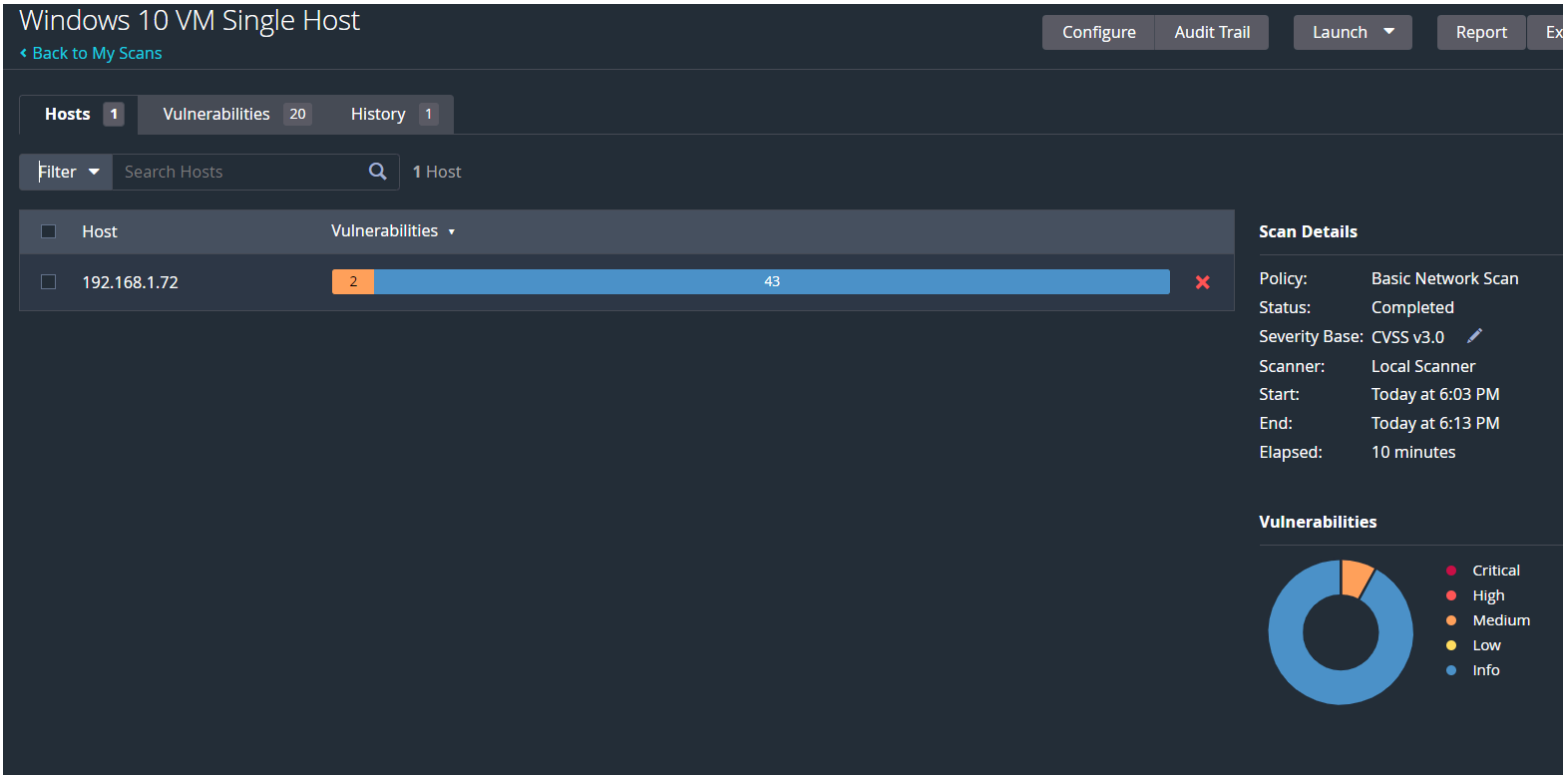




- This will display on your screen after saving it
- Select “launch” to start the scan, this may take some time



- 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 Essentials | Scans | Settings

Vulnerabilities 20

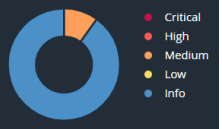
Filter | Search Vulnerabilities | 20 Vulnerabilities

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 Date 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



entials | Scans | Settings | mosyndi

Windows 10 VM Single Host / Plugin #50686

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Expor

Vulnerabilities 20

MEDIUM **IP 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

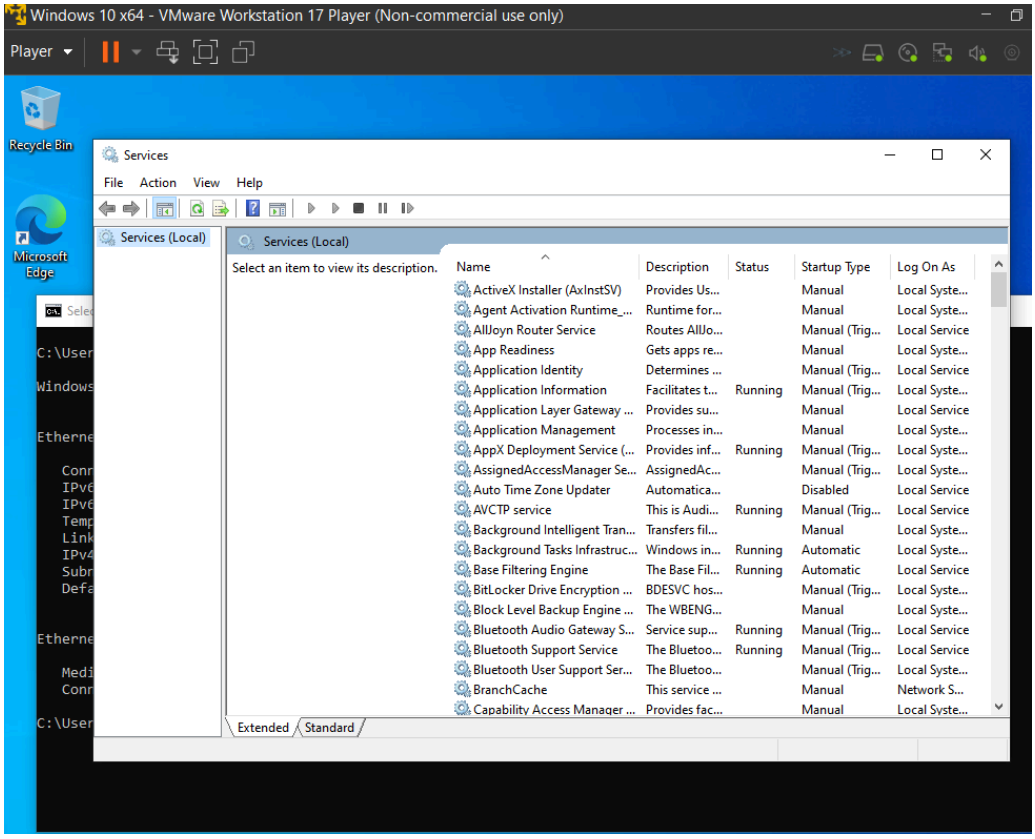
CVSS v3.0 Base Score 6.5

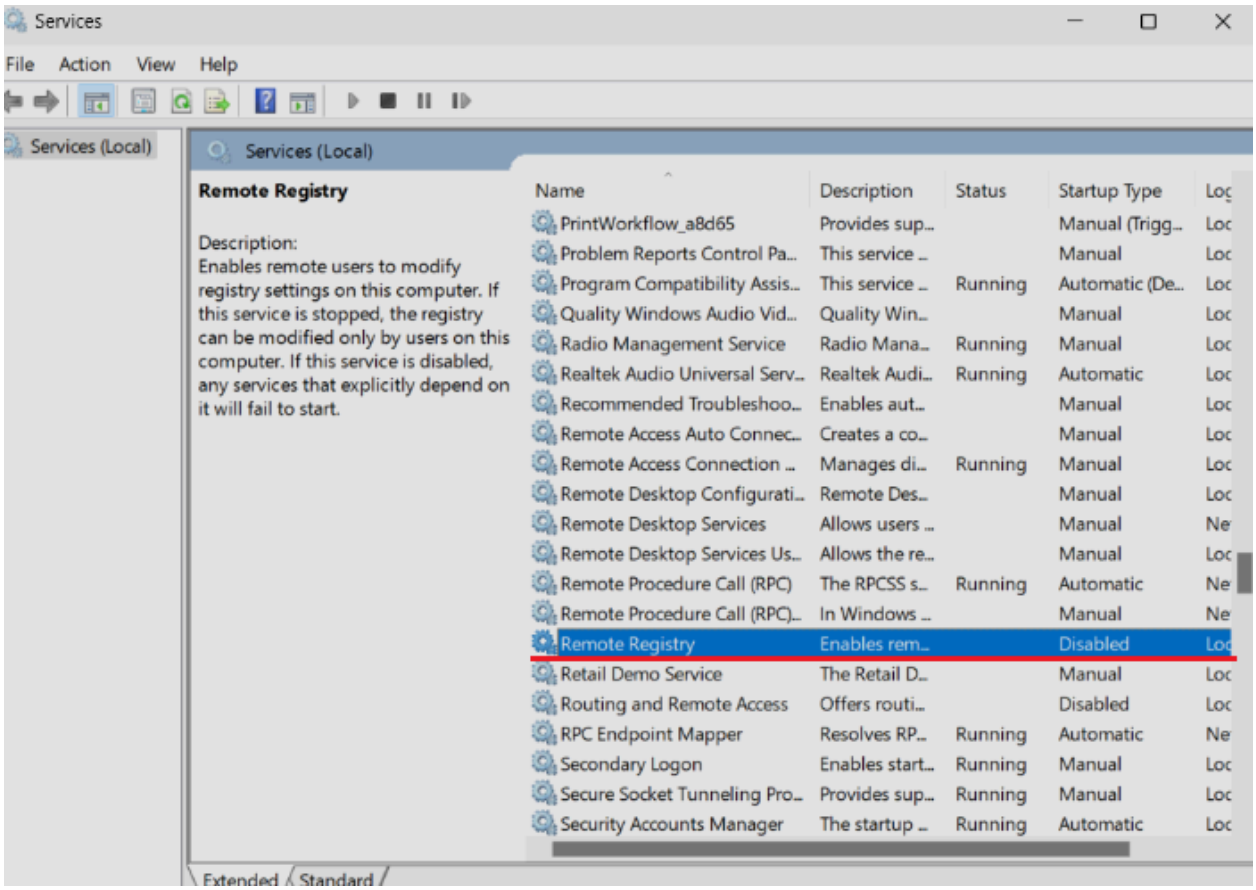
CVSS v3.0 Vector:
CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

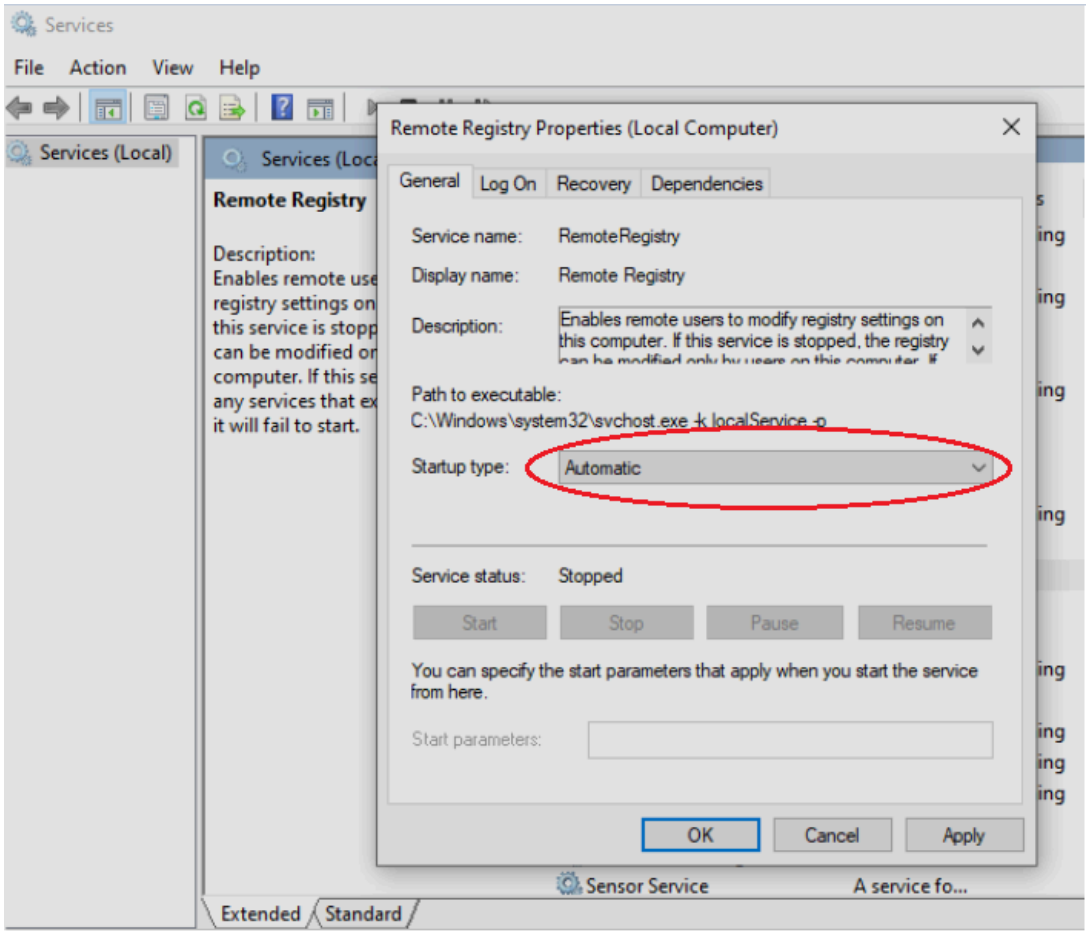
CVSS v2.0 Base Score: 5.8

CVSS v2.0 Vector:
CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P

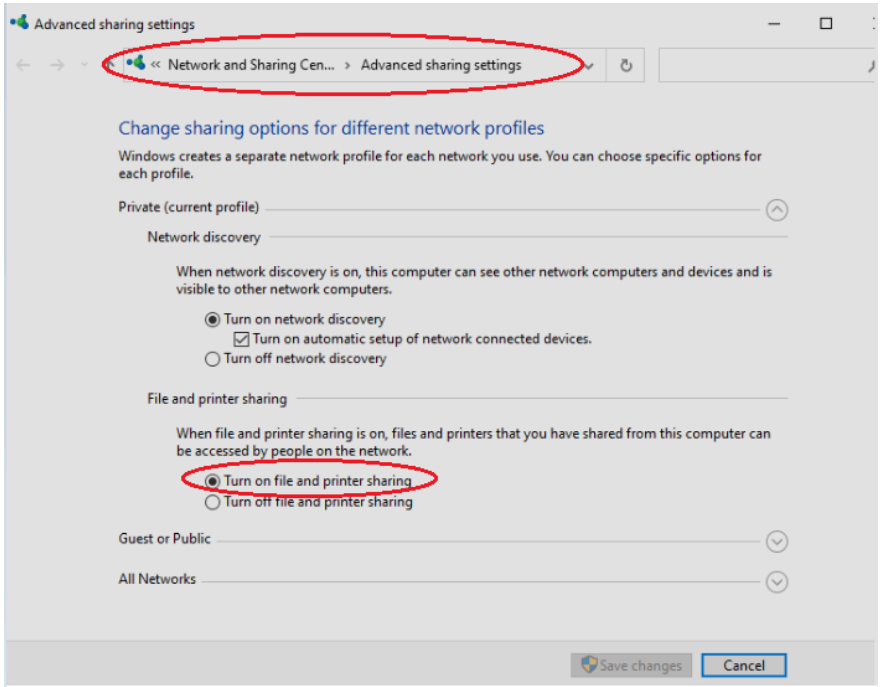
- Create a credential scan to see what more vulnerabilities are there
- Return back the to VM and open “Services”
- Enable “Remote Registry”, it will originally be disabled. The “startup type” should be automatic
- This allows Nessus to connect to the registry


Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Microsoft Edge
Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Name Description Status Startup Type Log On As
ActiveX Installer (AxInstSV) Provides Us... Manual Local Syste...
Agent Activation Runtime_... Runtime for... Manual Local Syste...
AllJoyn Router Service Routes AllJo... Manual (Trig... Local Service
App Readiness Gets apps re... Manual Local Syste...
Application Identity Determines ... Manual (Trig... Local Service
Application Information Facilitates t... Running Manual (Trig... Local Syste...
Application Layer Gateway ... Provides su... Manual Local Service
Application Management Processes in... Manual Local Syste...
AppX Deployment Service (... Provides inf... Running Manual (Trig... Local Syste...
AssignedAccessManager Se... AssignedAc... Manual (Trig... Local Syste...
Auto Time Zone Updater Automatica... Disabled Local Service
AVCTP service This is Audi... Running Manual (Trig... Local Service
Background Intelligent Tran... Transfers fil... Manual Local Syste...
Background Tasks Infrastruc... Windows in... Running Automatic Local Syste...
Base Filtering Engine The Base Fil... Running Automatic Local Service
BitLocker Drive Encryption ... BDESVC hos... Manual (Trig... Local Syste...
Block Level Backup Engine ... The WBENG... Manual Local Syste...
Bluetooth Audio Gateway S... Service sup... Running Manual (Trig... Local Service
Bluetooth Support Service The Bluetoo... Running Manual (Trig... Local Service
Bluetooth User Support Ser... The Bluetoo... Manual (Trig... Local Syste...
BranchCache This service ... Manual Network S...
Capability Access Manager ... Provides fac... Manual Local Syste...
Extended Standard

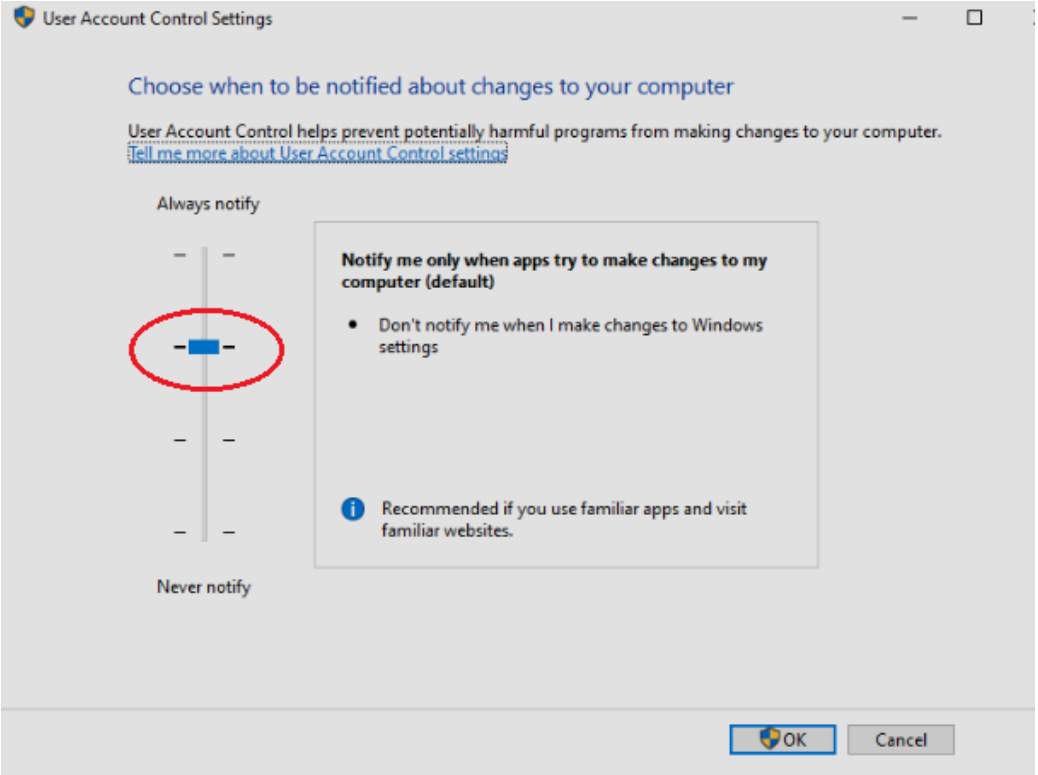

Services
File Action View Help
Services (Local)
Services (Local)
Remote Registry
Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.
Name Description Status Startup Type
PrintWorkflow_a8d65 Provides sup... Manual (Trigg...
Problem Reports Control Pa... This service ... Manual
Program Compatibility Assis... This service ... Running Automatic (De...
Quality Windows Audio Vid... Quality Win... Manual
Radio Management Service Radio Mana... Running Manual
Realtek Audio Universal Serv... Realtek Audi... Running Automatic
Recommended Troubleshoo... Enables aut... Manual
Remote Access Auto Connec... Creates a co... Manual
Remote Access Connection ... Manages di... Running Manual
Remote Desktop Configurati... Remote Des... Manual
Remote Desktop Services Allows users ... Manual
Remote Desktop Services Us... Allows the re... Manual
Remote Procedure Call (RPC) The RPCSS s... Running Automatic
Remote Procedure Call (RPC)... In Windows ... Manual
Remote Registry Enables rem... Disabled
Retail Demo Service The Retail D... Manual
Routing and Remote Access Offers routi... Disabled
RPC Endpoint Mapper Resolves RP... Running Automatic
Secondary Logon Enables start... Running Manual
Secure Socket Tunneling Pro... Provides sup... Running Manual
Security Accounts Manager The startup ... Running Automatic
Extended Standard

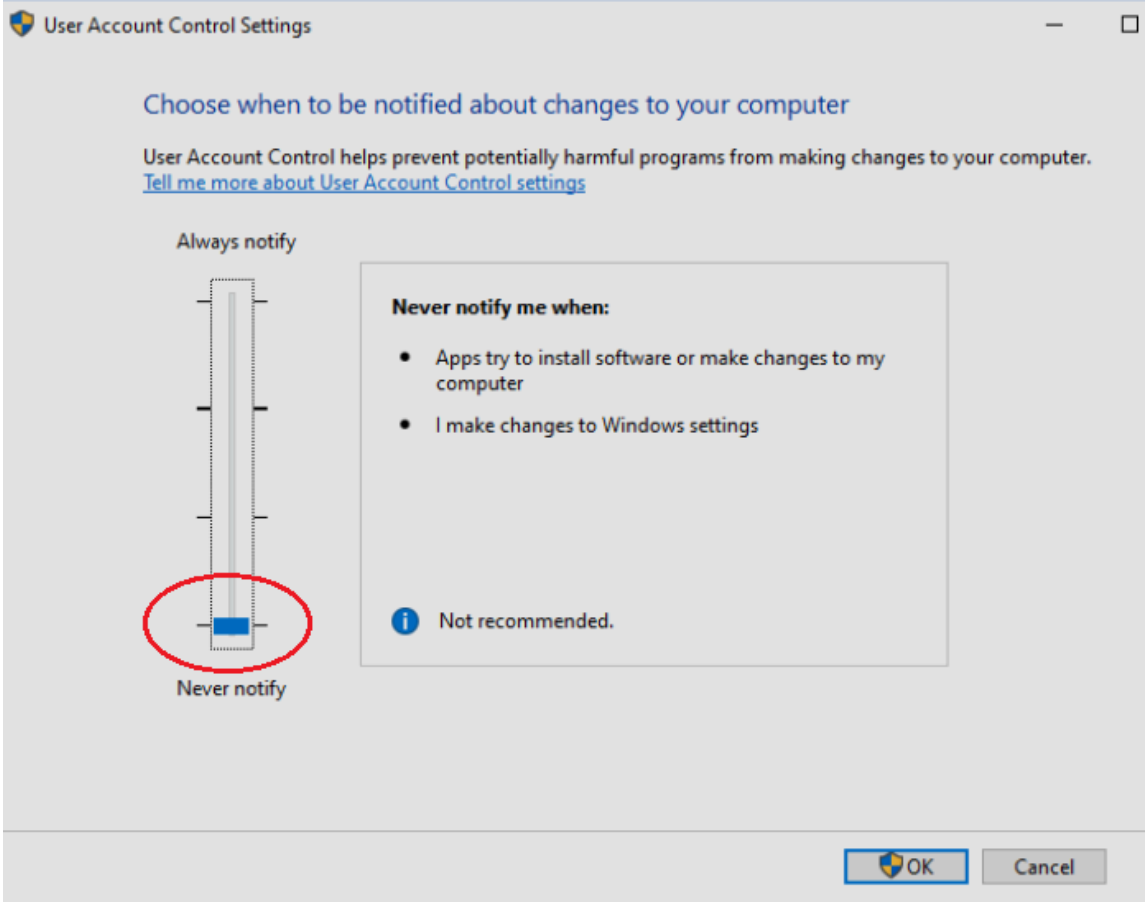


- Next, go to Control plane > Advanced sharing settings
- Make sure “Turn on file and printer sharing” radio button is selected



- Lastly, Adjust the “User Account Control Settings”

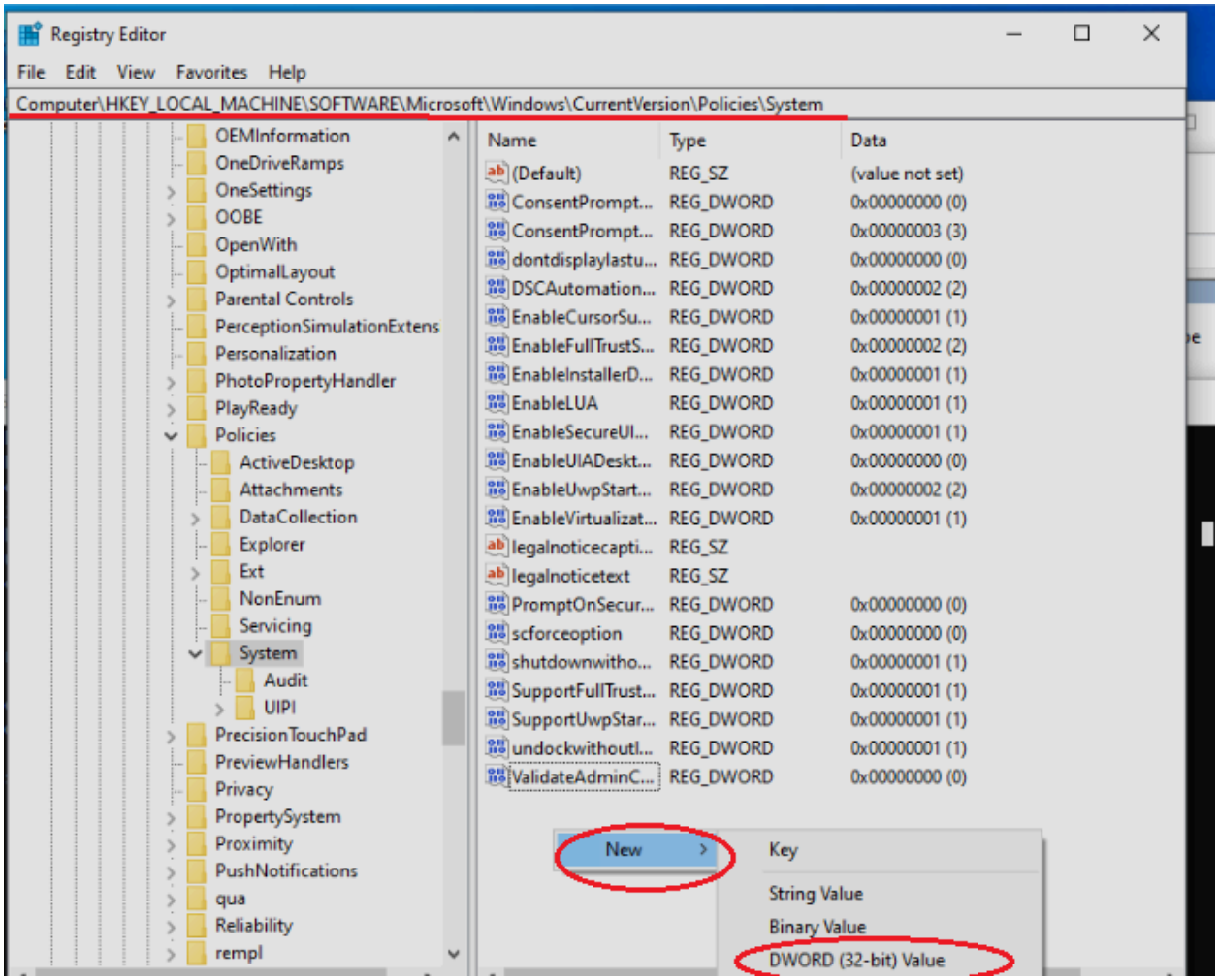




- Nessus recommends these steps for computers that are not on a domain, reminder although these steps are suggested, this does not mean you can perform this on any environment.
- Here is the documentation that suggests these modifications: https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm#Configure-a-Local-Account

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

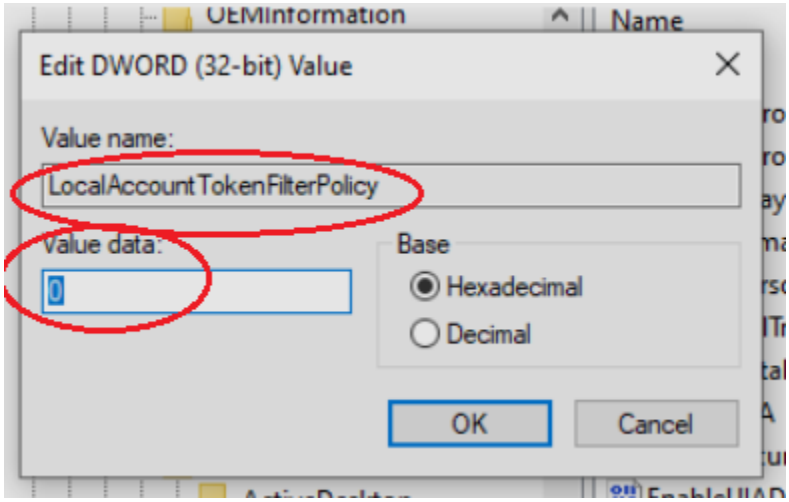
- Next step is to go to the Windows Registry
- Navigate to this location to create a new “DWORD (32-bit) Value”

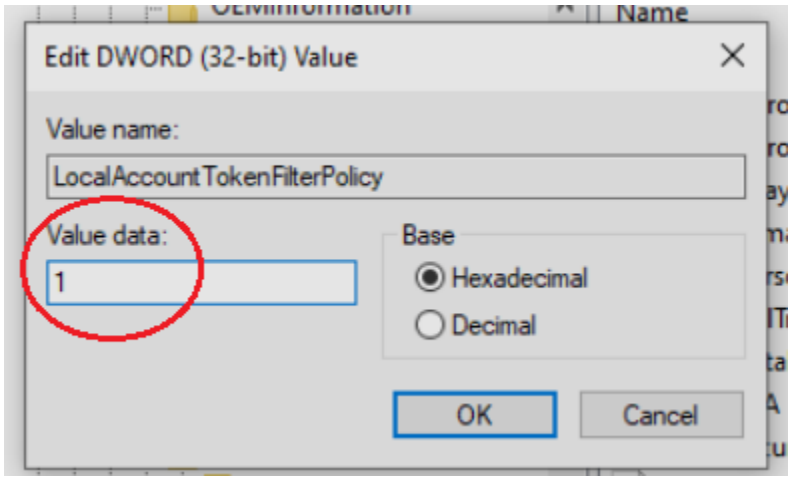


- Name the DWORD: LocalAccountTokenFilterPolicy

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)

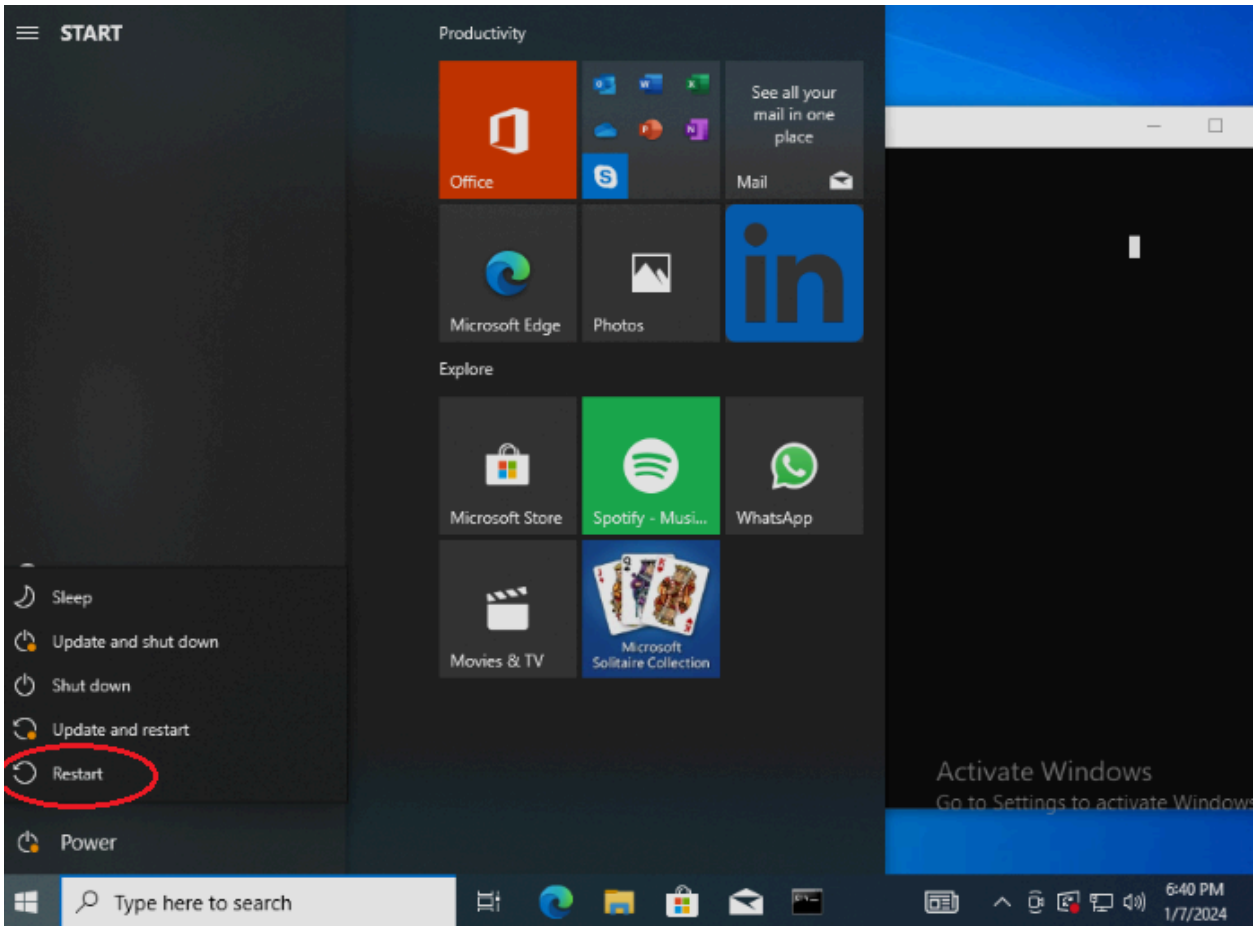
- Modify the DWORD to have a Value data of “1”



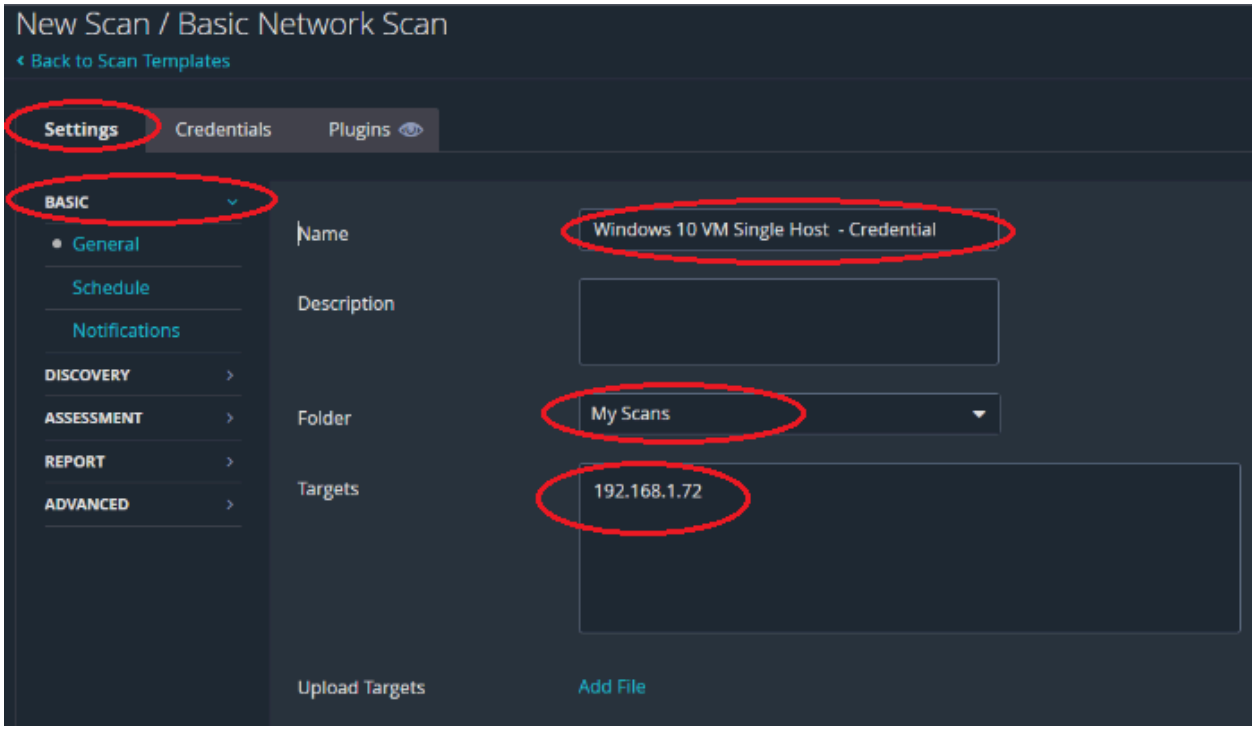


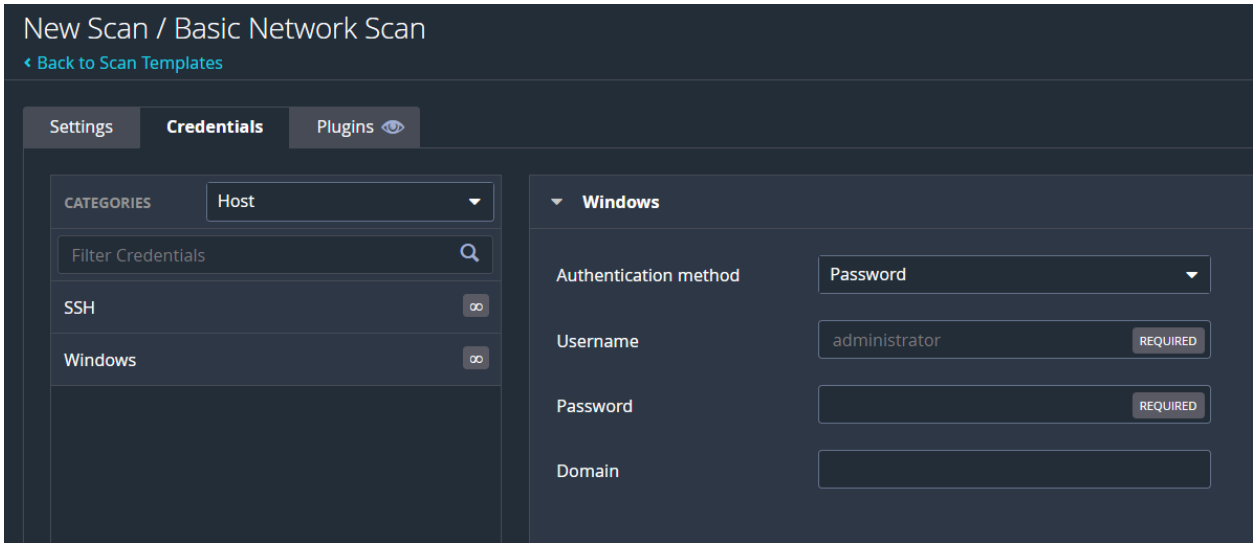
SupportFullTrust...	REG_DWORD	0x00000001 (1)
SupportUwpStar...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)
LocalAccountTo...	REG_DWORD	0x00000001 (1)

- Now, Restart your VM

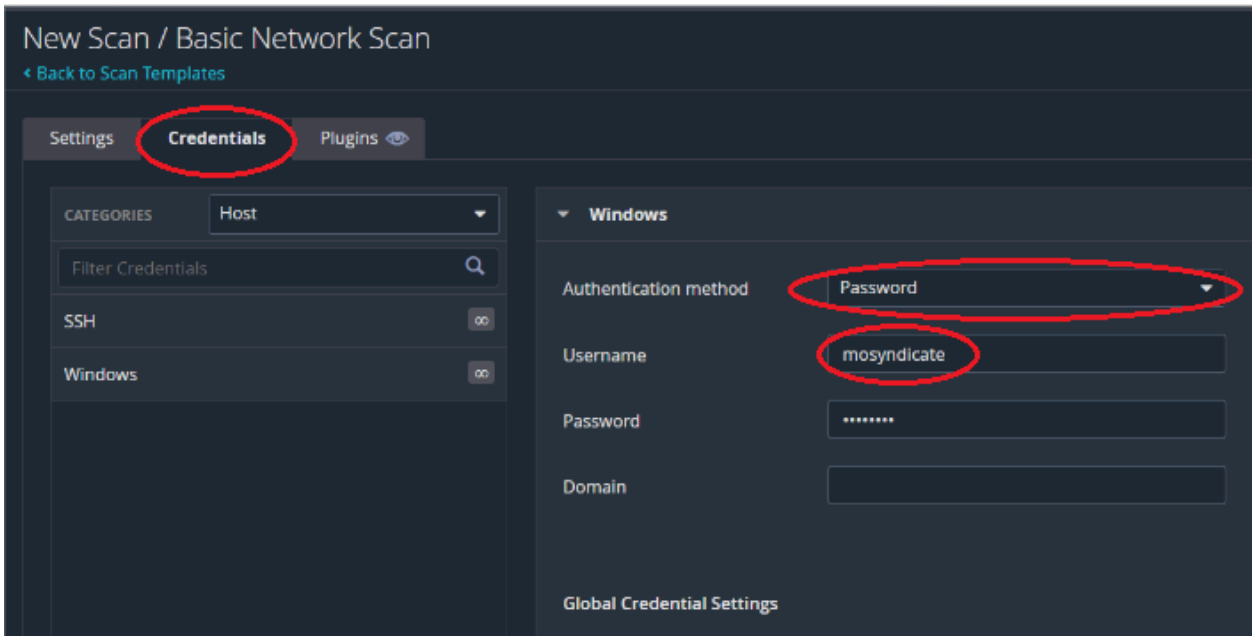


- On you physical workstation, go to Nessus to create a new scan (credential)
- Ensure that the IP address remains unchanged after the restart. If it has changed, you will be using the new IP address for the scan.

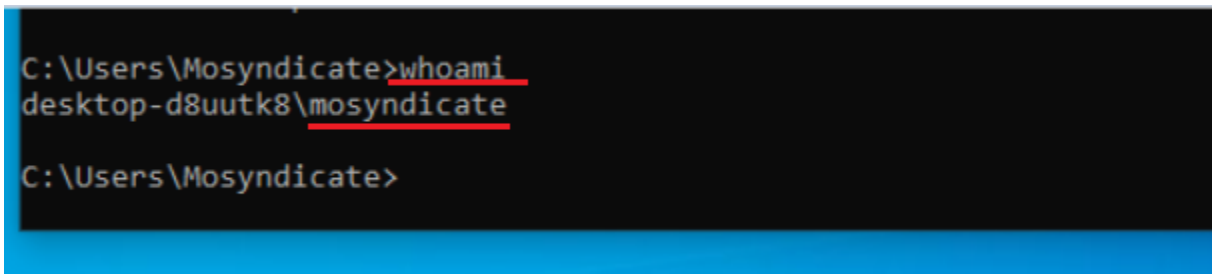




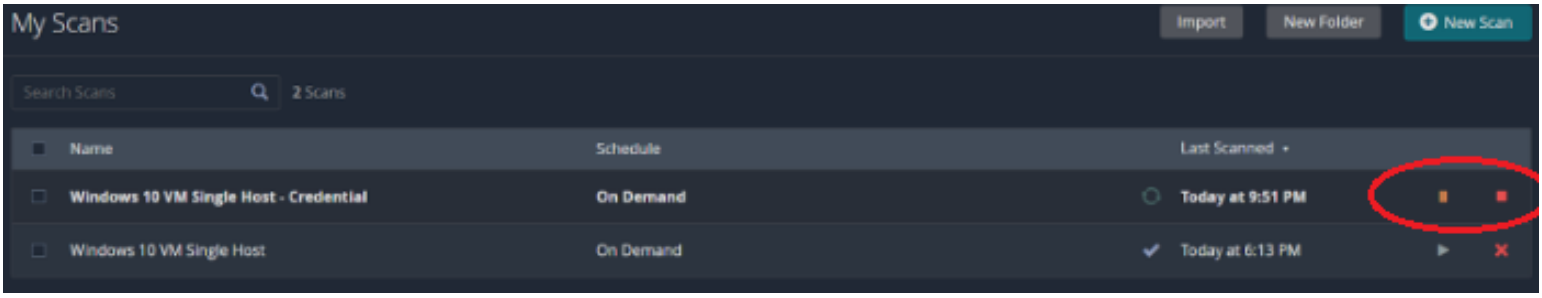
- Fill in the username and password for the VM



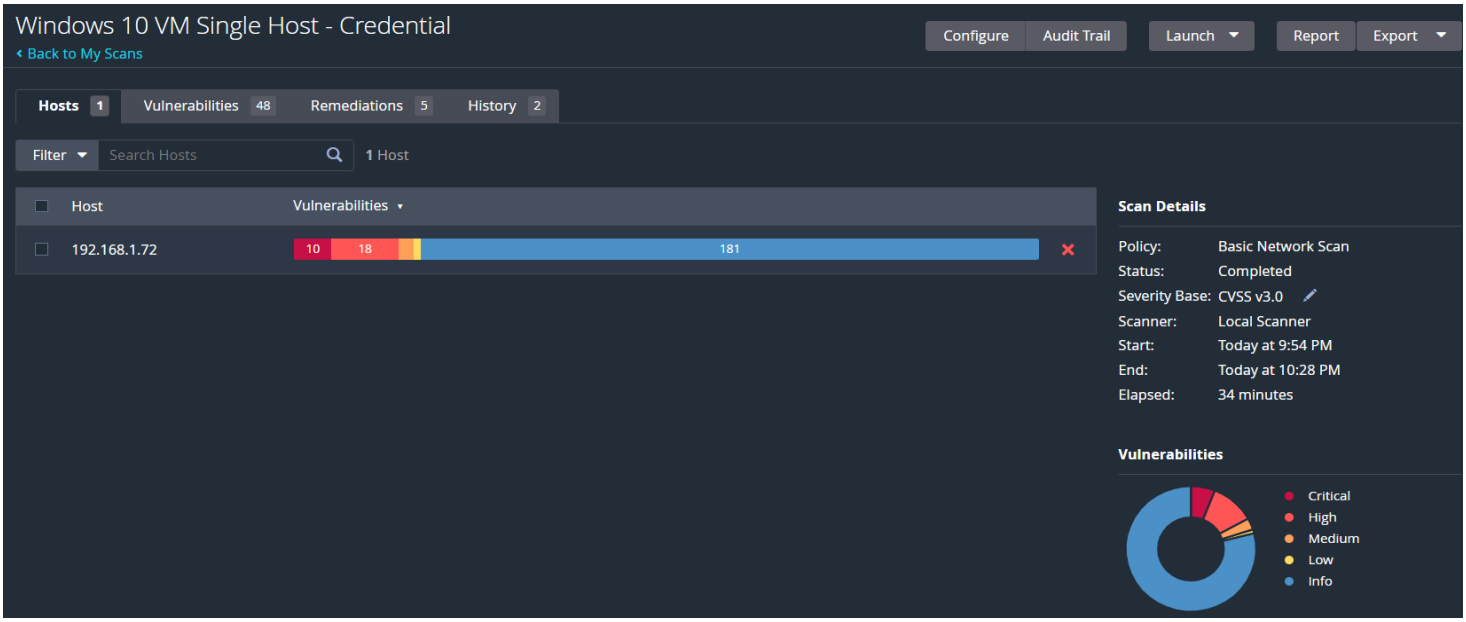
- If you do not know your username, return back to the command prompt and type in “whoami”

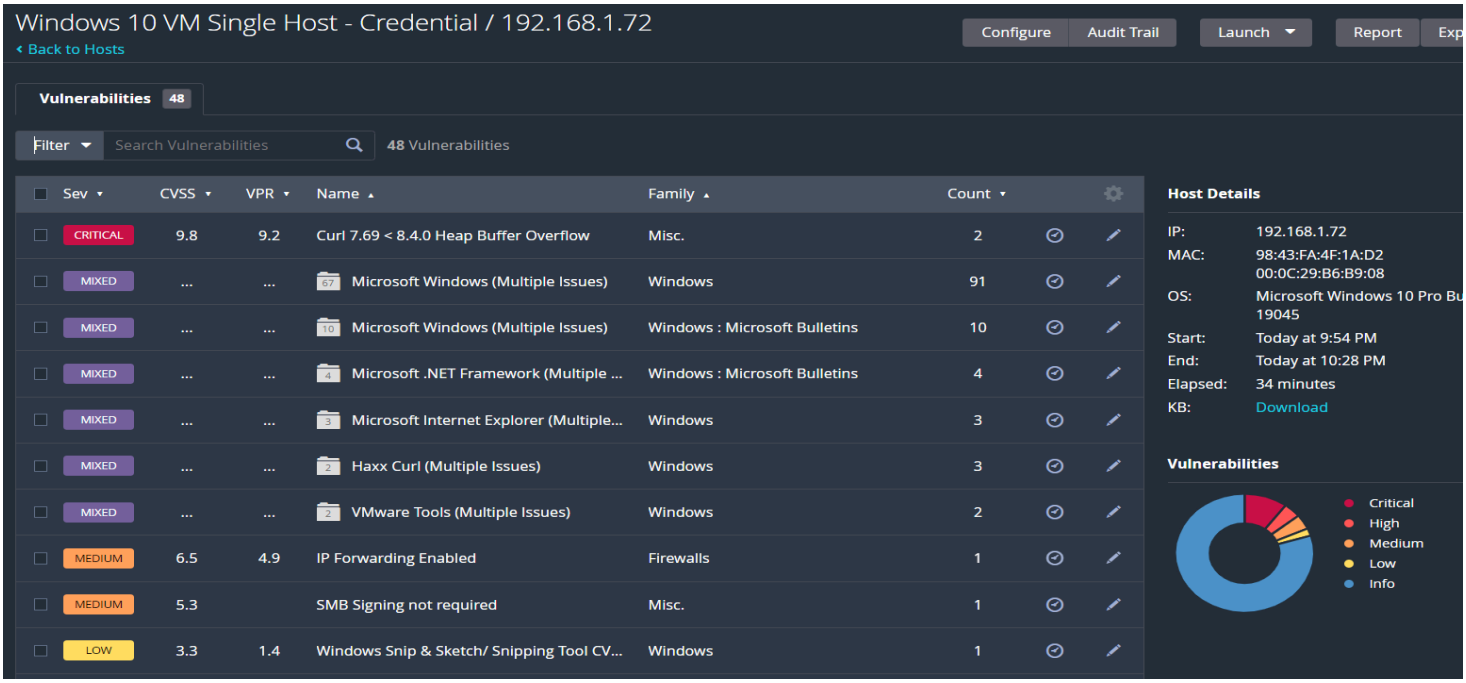


- Once the new scan is complete, review the results which may reveal an increased number of vulnerabilities.

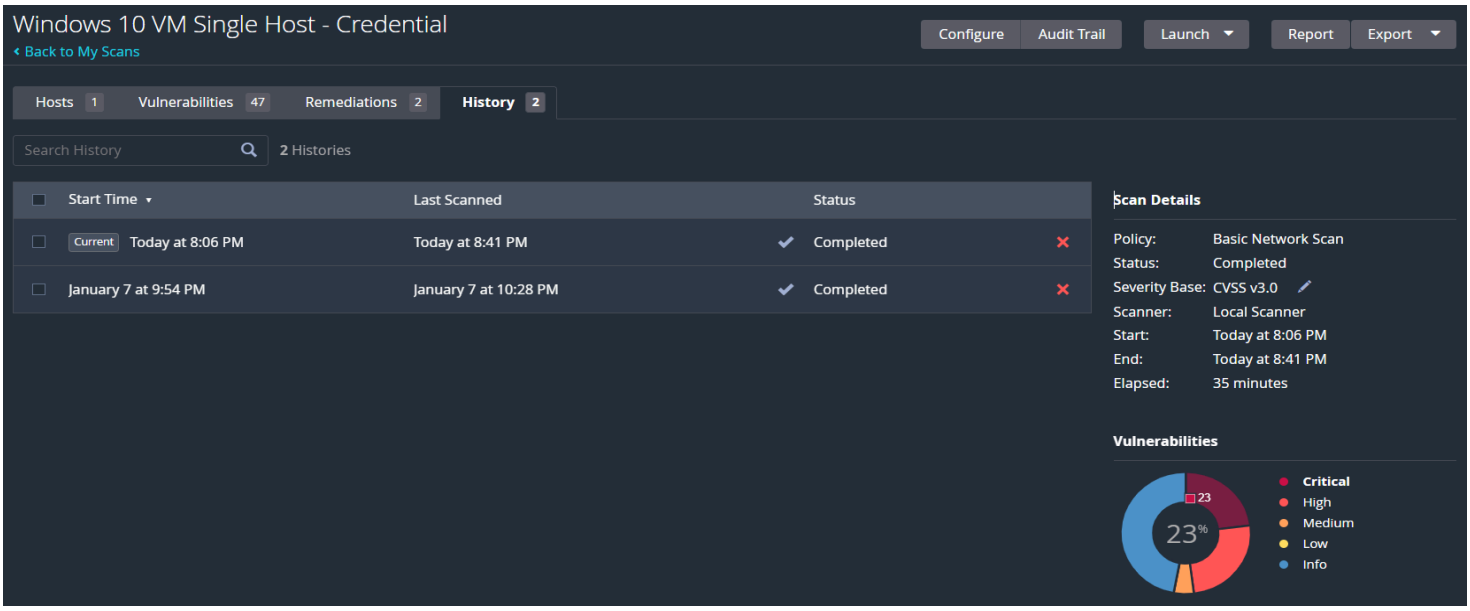


- After adding a credentialed scan, the vulnerabilities have jumped to 48 total. The highest being a critical with a CVSS of 9.5.

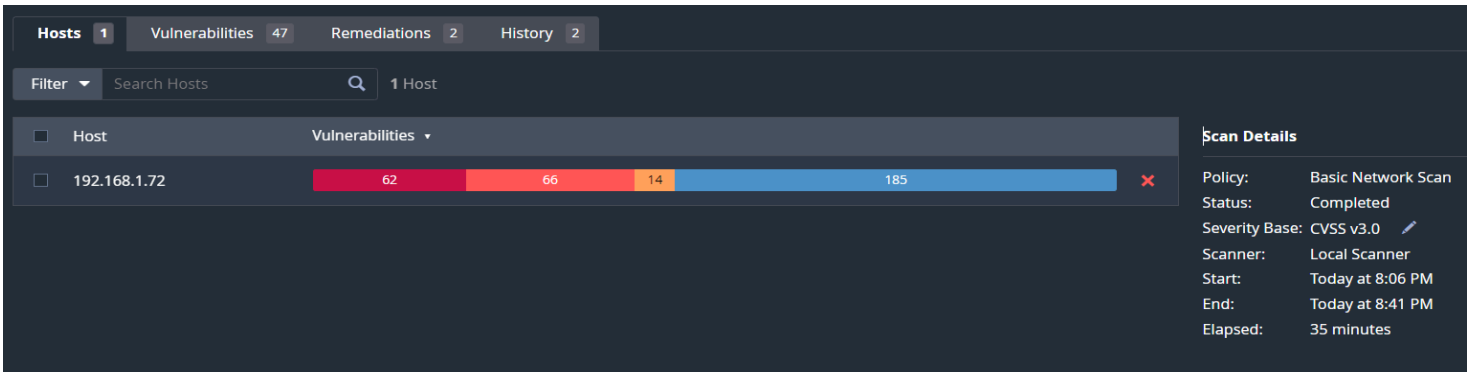


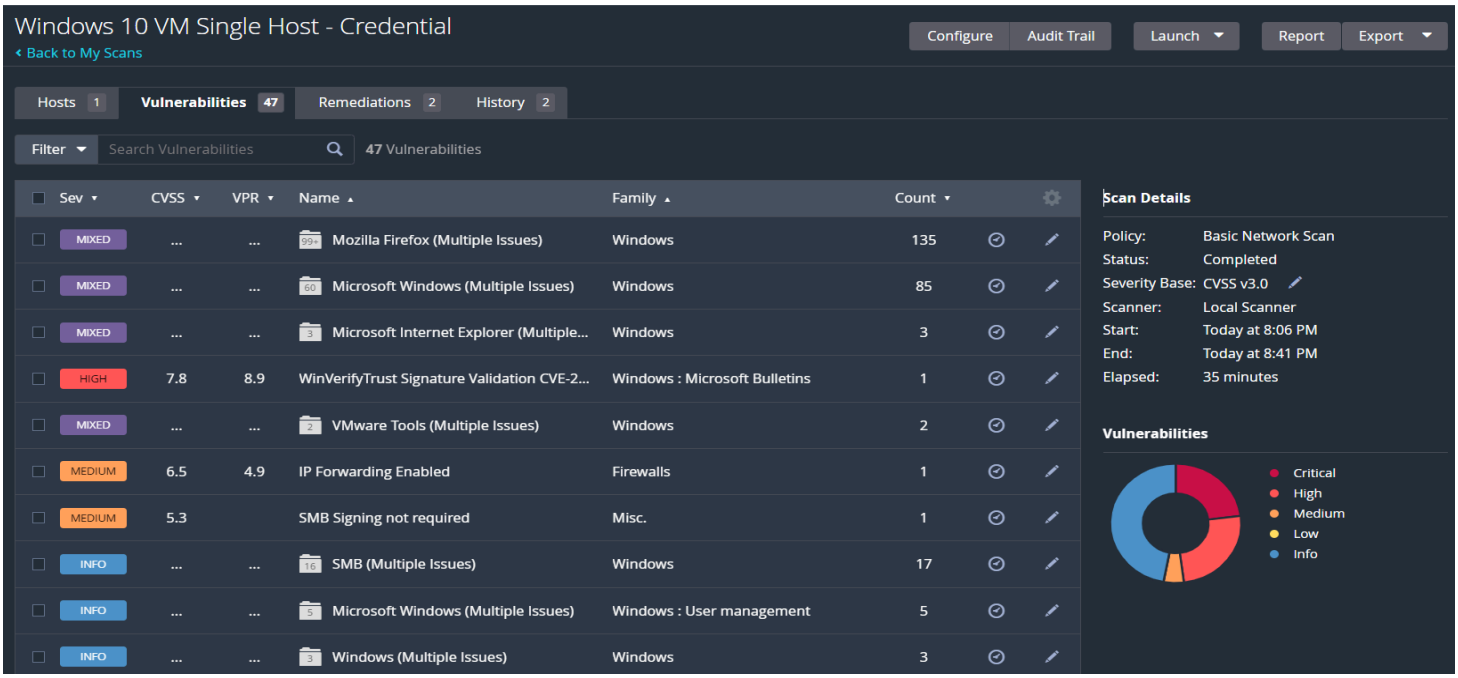


- From here I will download some legacy applications and make the system even more insecure. And then the challenge is to remediate all the vulnerabilities to the best of our ability.



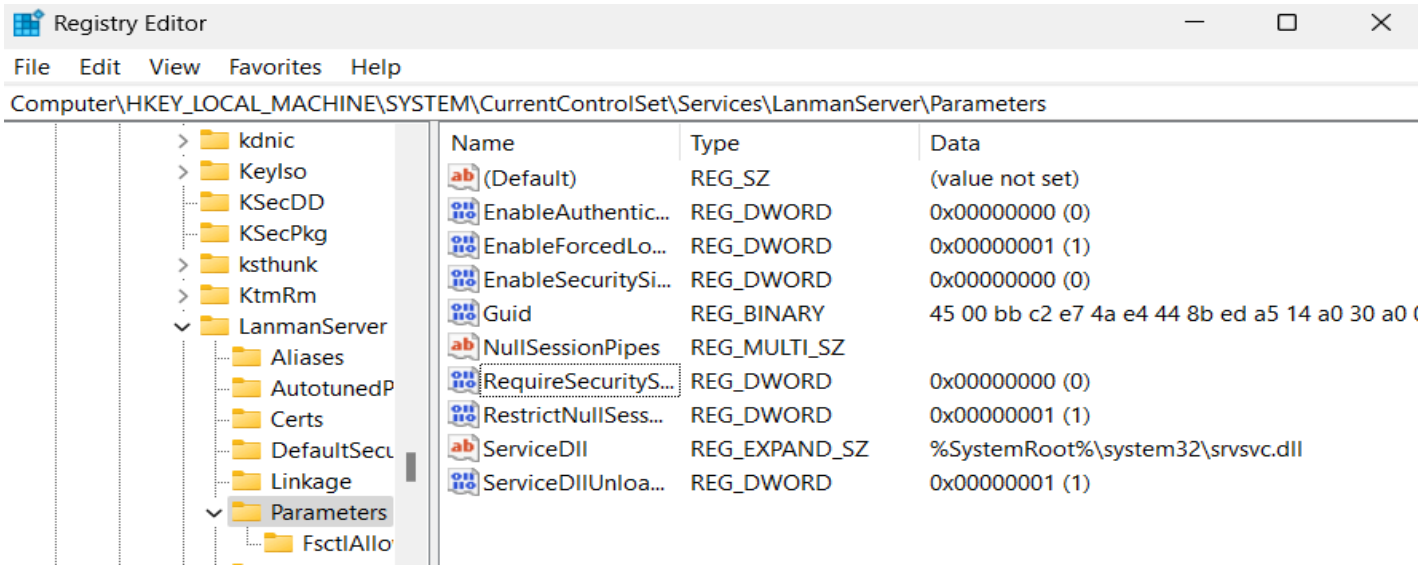
- Here are the results after downloading legacy softwares and modifying the VM to be even more insecure.



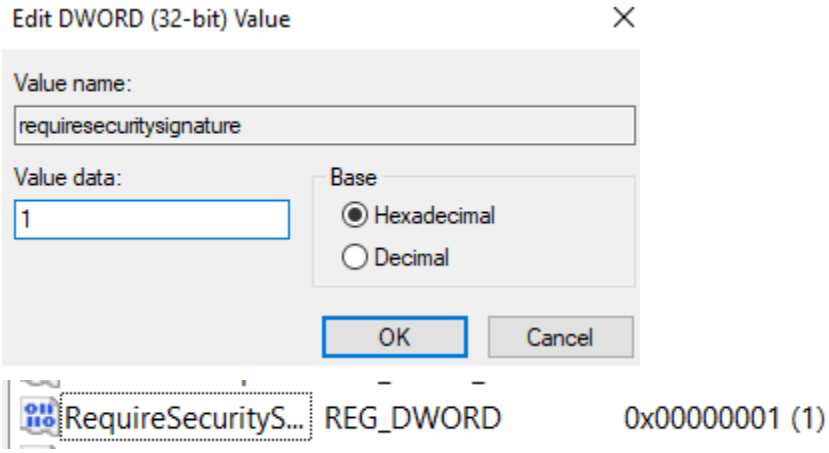


- From here, your goal is to remediate all the issues presented on Nessus. You will need to use the scan details, solutions mentioned in the remediation tab and researching about the CVEs. This is a challenge, you can delete this specific virtual machine after when you are done or use it as your personal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

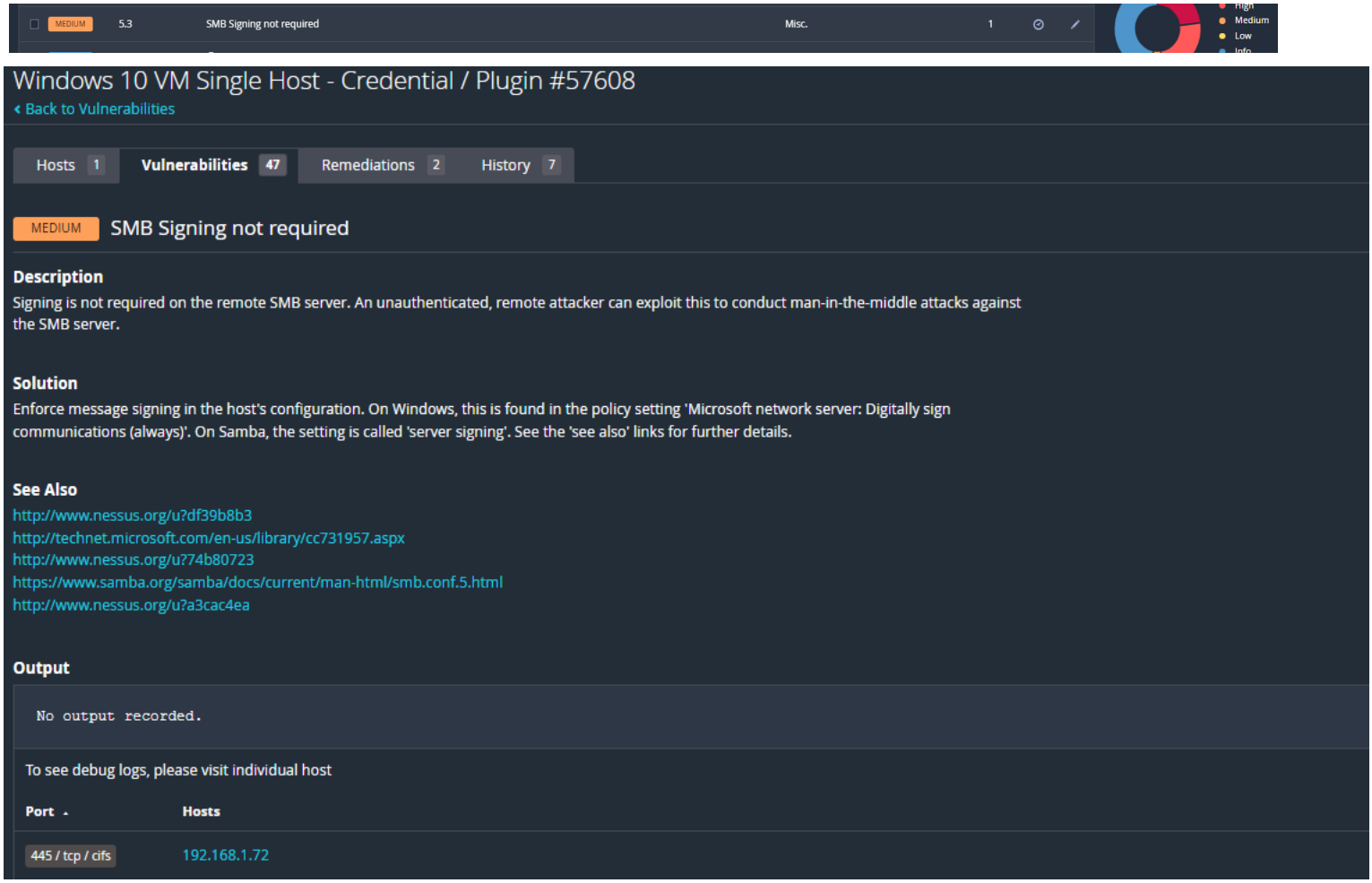
- Here, we will try to remove this vulnerability



- 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



- 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.

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

OSG | ServiceNow |... Imported

Filter by title

- SMB Multichannel troubleshooting
- System error 67 has occurred. The network name cannot be found
- System error 1331 when you connect to a share
- TCP connection is aborted during Validate Negotiate
- TCP three-way handshake failure during SMB connection
- Troubleshoot DFSN access failures
- Troubleshooting guidance: DFS Namespace
- Troubleshooting guidance: SMB
- Background Intelligent Transfer Service (BITS)
- DFSR
- DNS
- Dynamic Host Configuration Protocol (DHCP)
- FRS
- IP Address Management (IPAM)
- Network Load Balancing (NLB)
- RADIUS - Network Policy Server (NPS) or Internet Authentication Service (IAS)
- Remote access
- TCP/IP communications

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

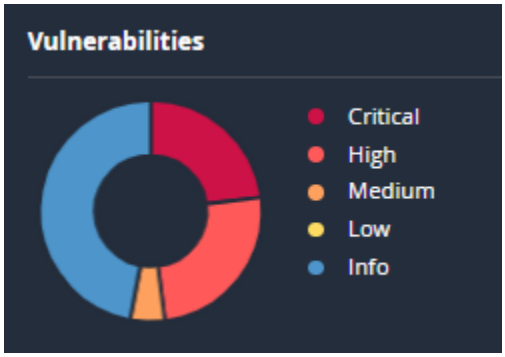
Configure SMB Signing with Confidence

How to Defend Users from Interception Attacks via SMB Client Defense

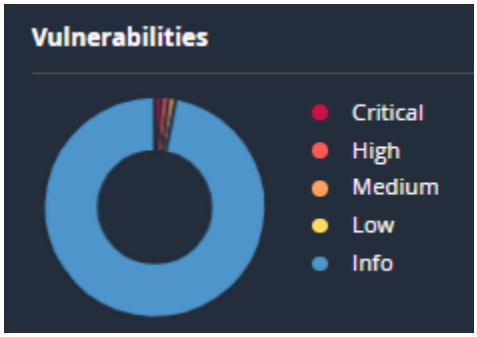
SMB 2 and SMB 3 security in Windows 10: the anatomy of signing and cryptographic keys

SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions

Netdom computername

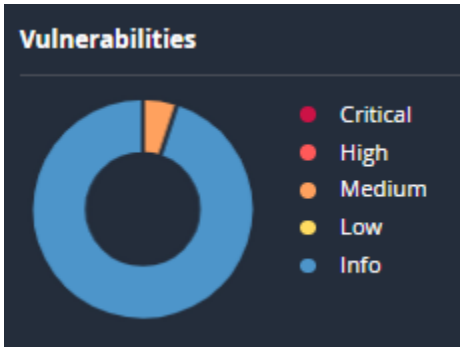


- Results after the first credentialed scan

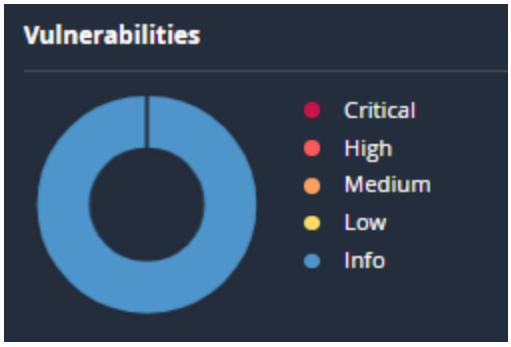


- Results after remediating and doing a few more scans to see the progress of my remediation efforts

- 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.