Vulnerability Scanning with Nessus on Windows VM

This project showcases the complete process of setting up a deliberately vulnerable Windows virtual machine and scanning it using **Nessus**. The primary objective is to gain hands-on experience with both **basic** and **credentialed vulnerability scans**, allowing you to identify real-world security flaws in a controlled, risk-free lab environment. In addition to discovering vulnerabilities, this project emphasizes the importance of analyzing scan results and implementing effective **remediation strategies**, which are essential skills for any aspiring cybersecurity professional.

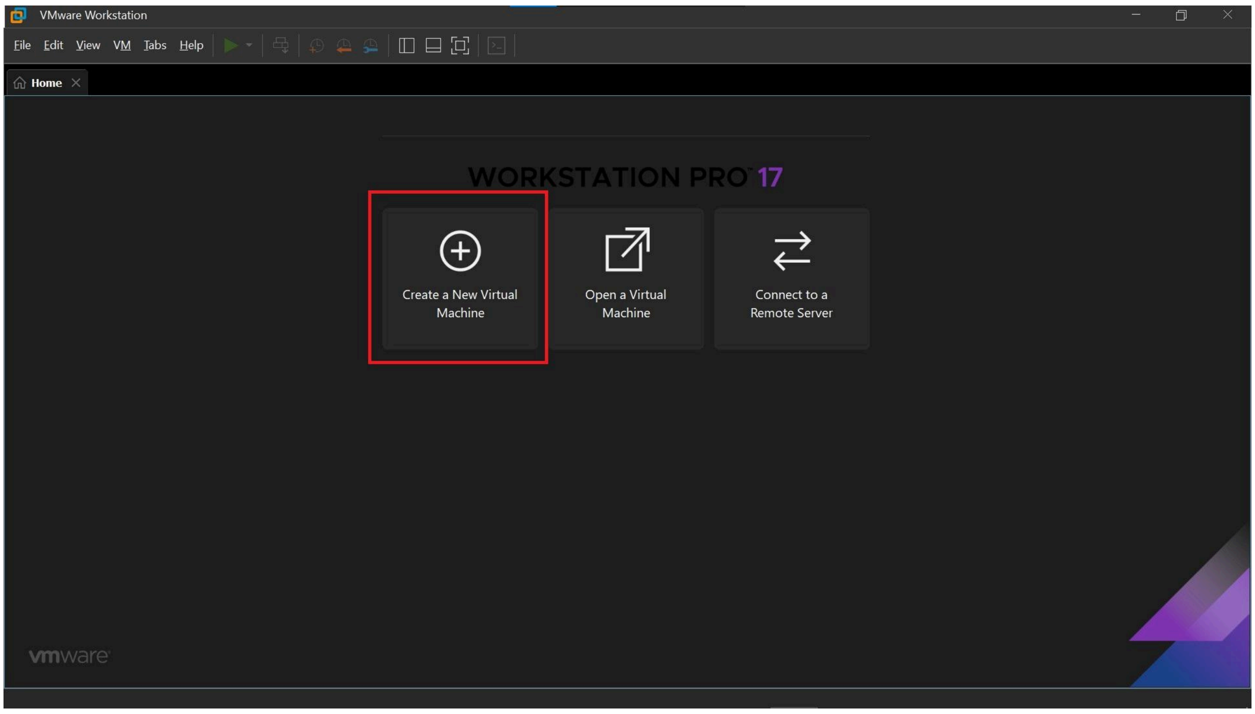
🧰 Prerequisites

Before starting, ensure you have the following:

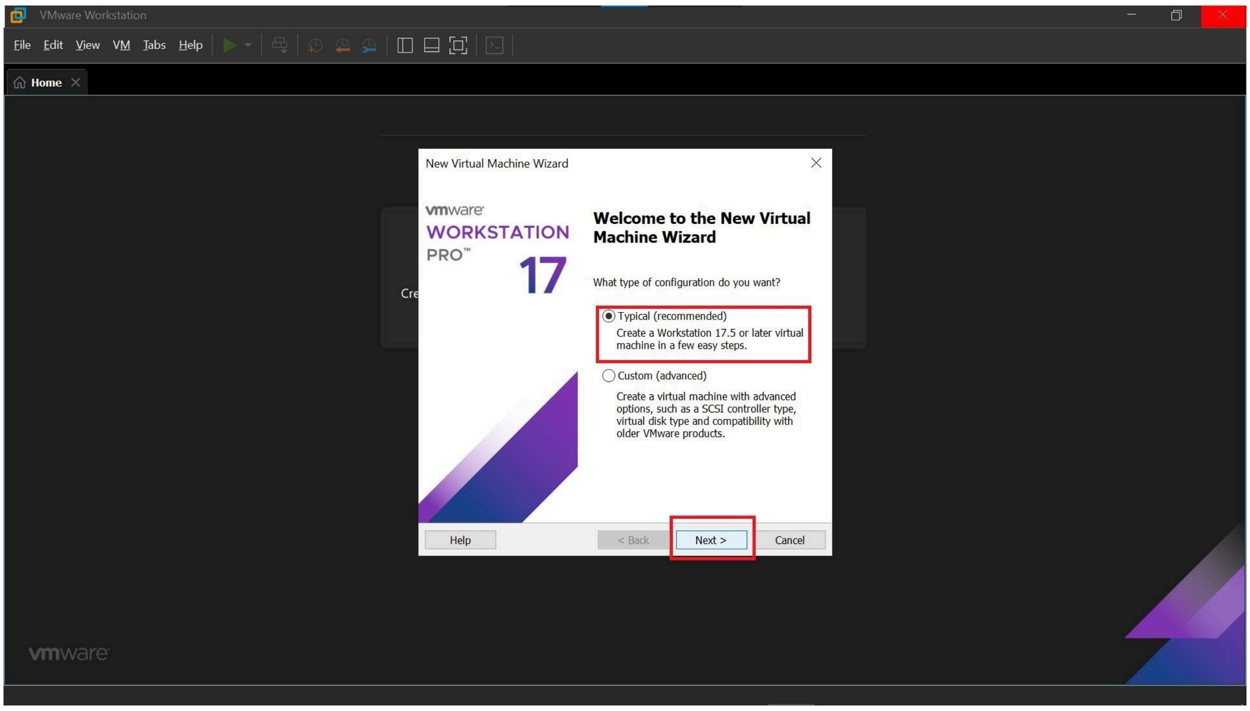
- ➔ VMware Workstation Pro (or VMware Player)
- ➔ Windows 10 ISO image
- ➔ Internet access (for downloading Nessus and software)
- ➔ [Optional] Temporary email (for Nessus activation)
- ➔ Nessus installer: [Download from Tenable]

Setting up a Windows VM in VMware

Once you have your image locally saved on your computer, **Launch VMware Workstation Pro** and click **"Create a New Virtual Machine"**.


VMware Workstation
File Edit View VM Tabs Help
Home
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware

Select **Typical (recommended)** and proceed.



New Virtual Machine Wizard

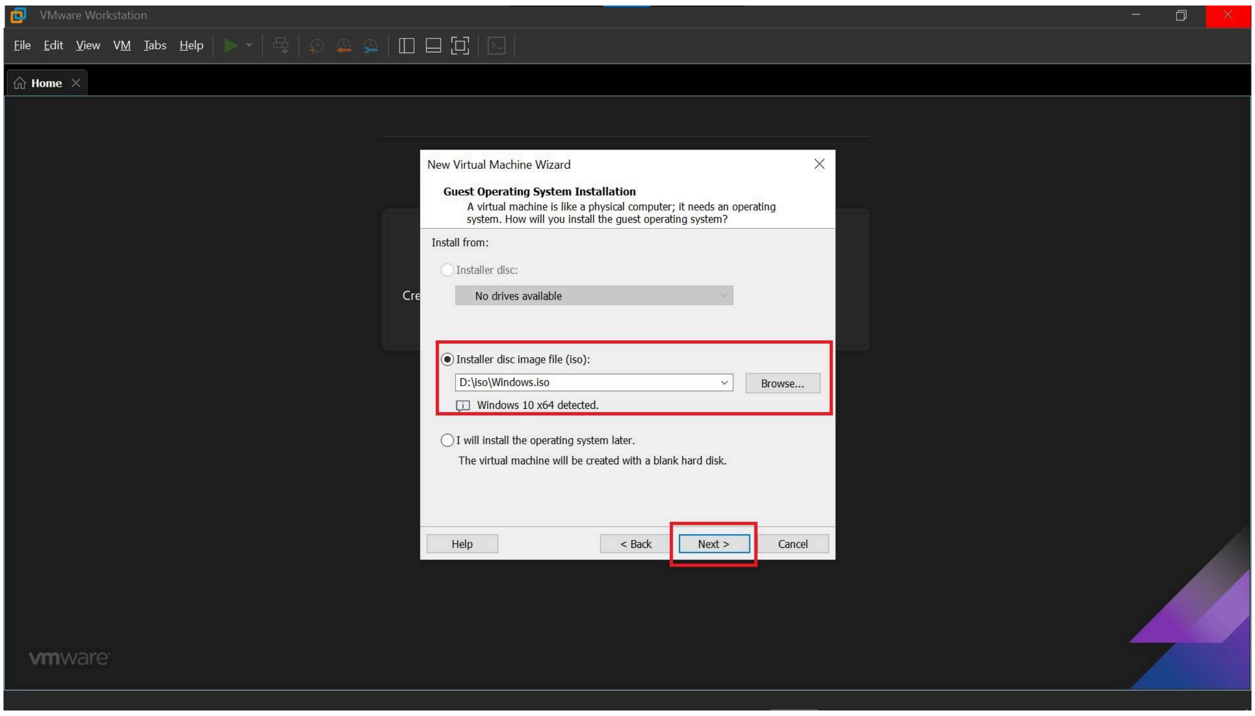
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 17.5 or later virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Browse and select your Windows 10 ISO file.



New Virtual Machine Wizard

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

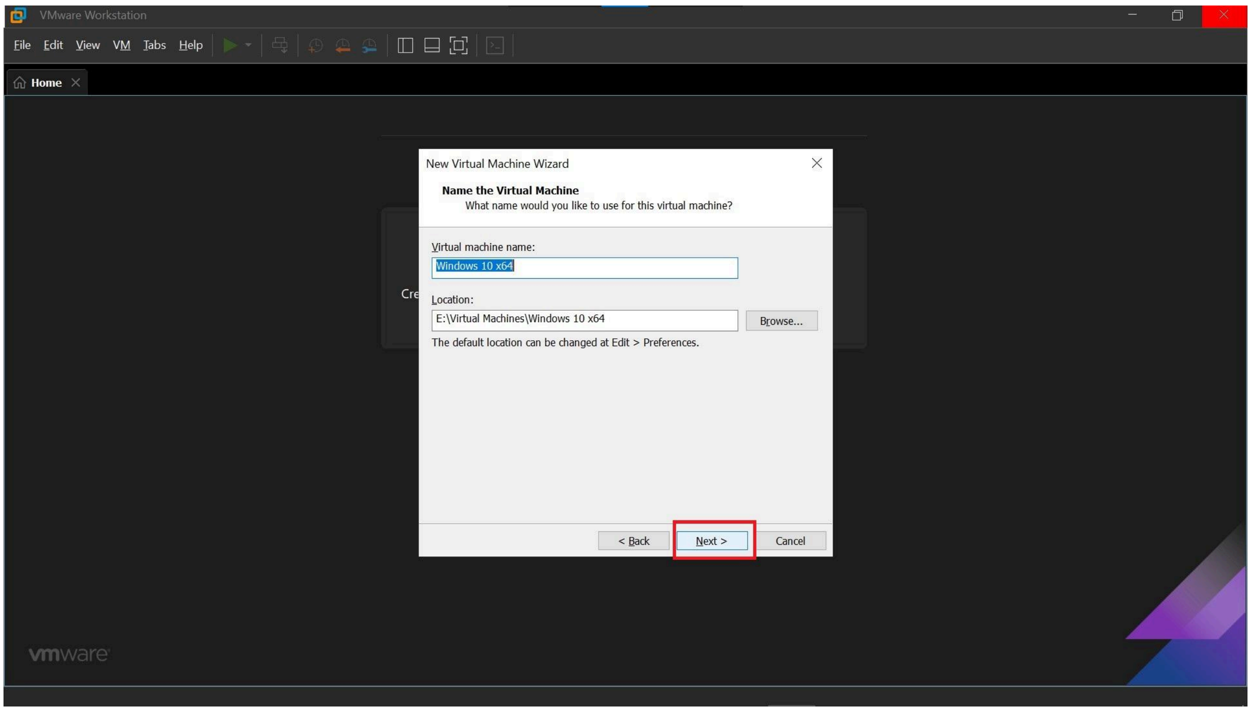
Install from:

○ Installer disc:
No drives available

● Installer disc image file (iso):
D:\iso\Windows.iso
Windows 10 x64 detected.

○ I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Name the VM and choose a location with sufficient disk space.



New Virtual Machine Wizard

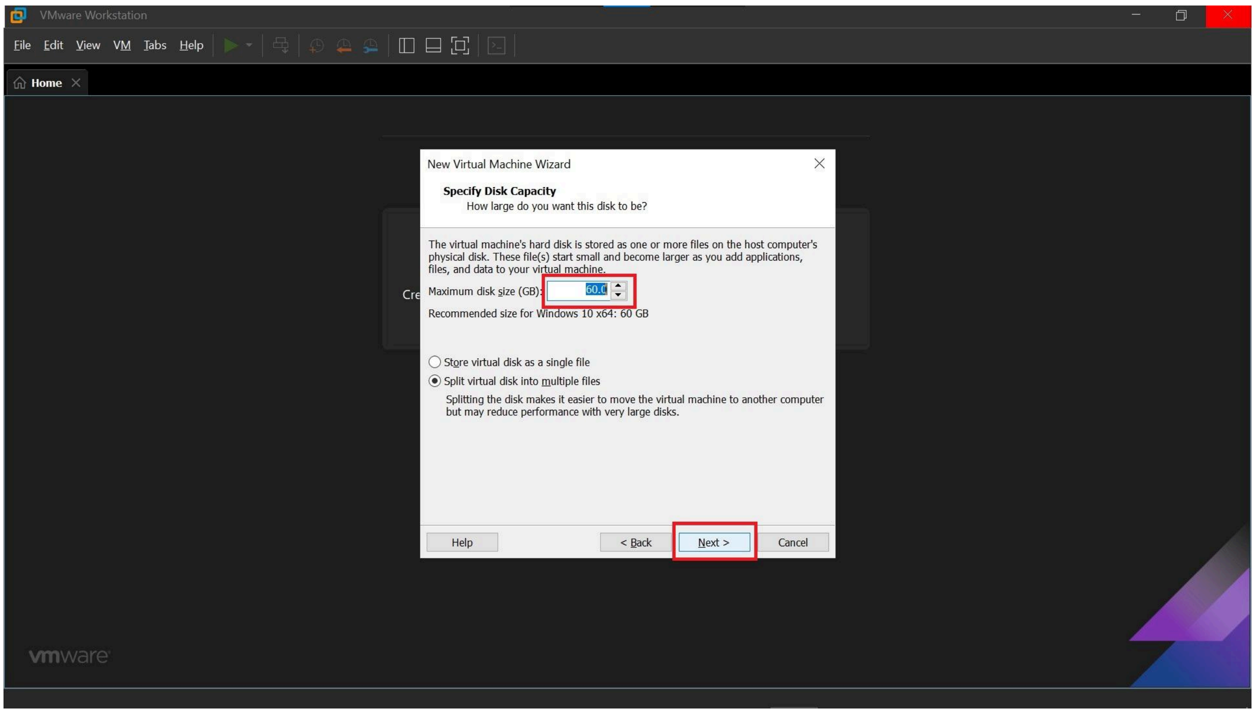
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Windows 10 x64

Location:
E:\Virtual Machines\Windows 10 x64

The default location can be changed at Edit > Preferences.

Use default settings or allocate at least **40 GB** of disk space



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

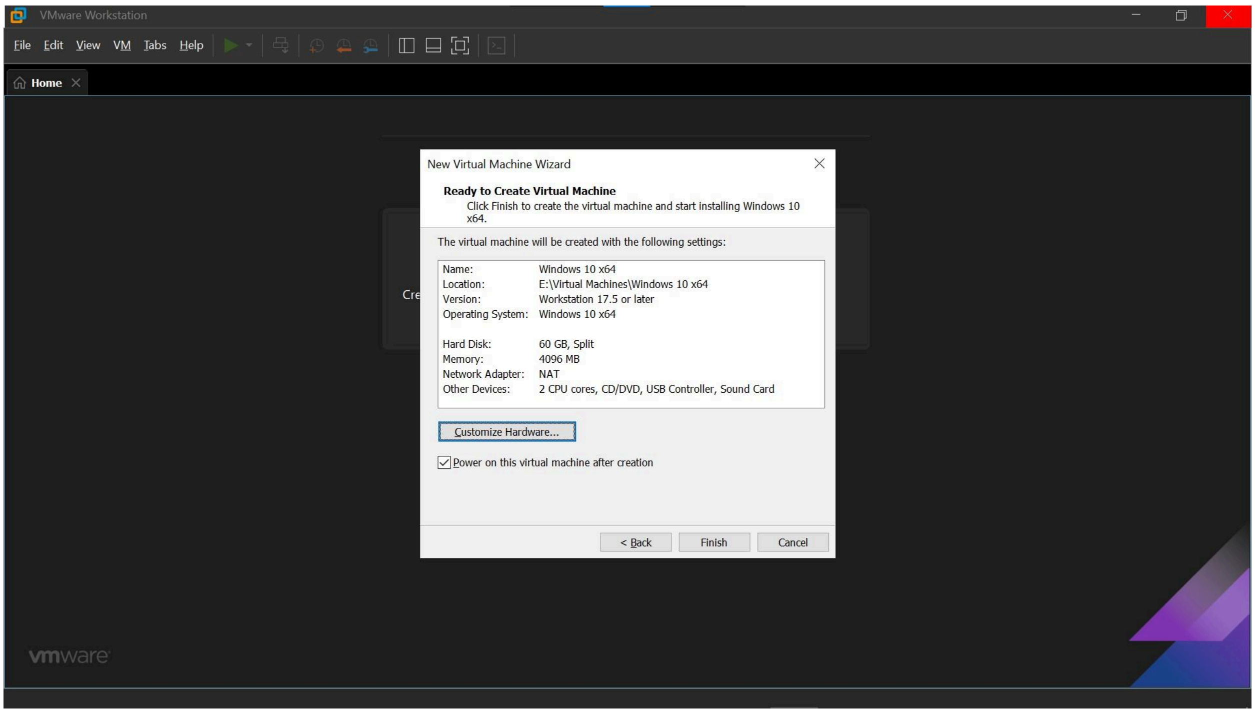
Recommended size for Windows 10 x64: 60 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

You can adjust CPU cores, memory, and other settings via **Customize Hardware**.



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Windows 10 x64.

The virtual machine will be created with the following settings:

Name:	Windows 10 x64
Location:	E:\Virtual Machines\Windows 10 x64
Version:	Workstation 17.5 or later
Operating System:	Windows 10 x64
Hard Disk:	60 GB, Split
Memory:	4096 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

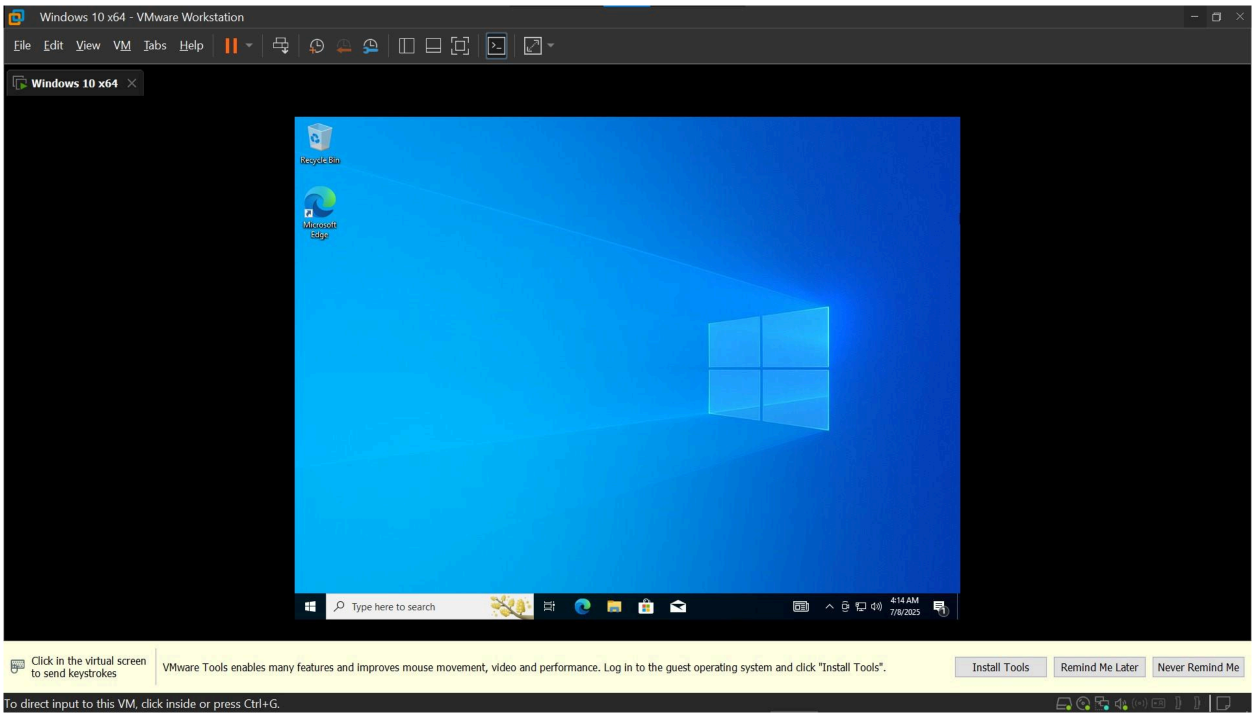
☑ Power on this virtual machine after creation

Finish and begin the Windows installation process.

Select:

- **Windows 10 Pro**
- **Custom: Install Windows only**

The process may take around **15–20 minutes**.



VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.

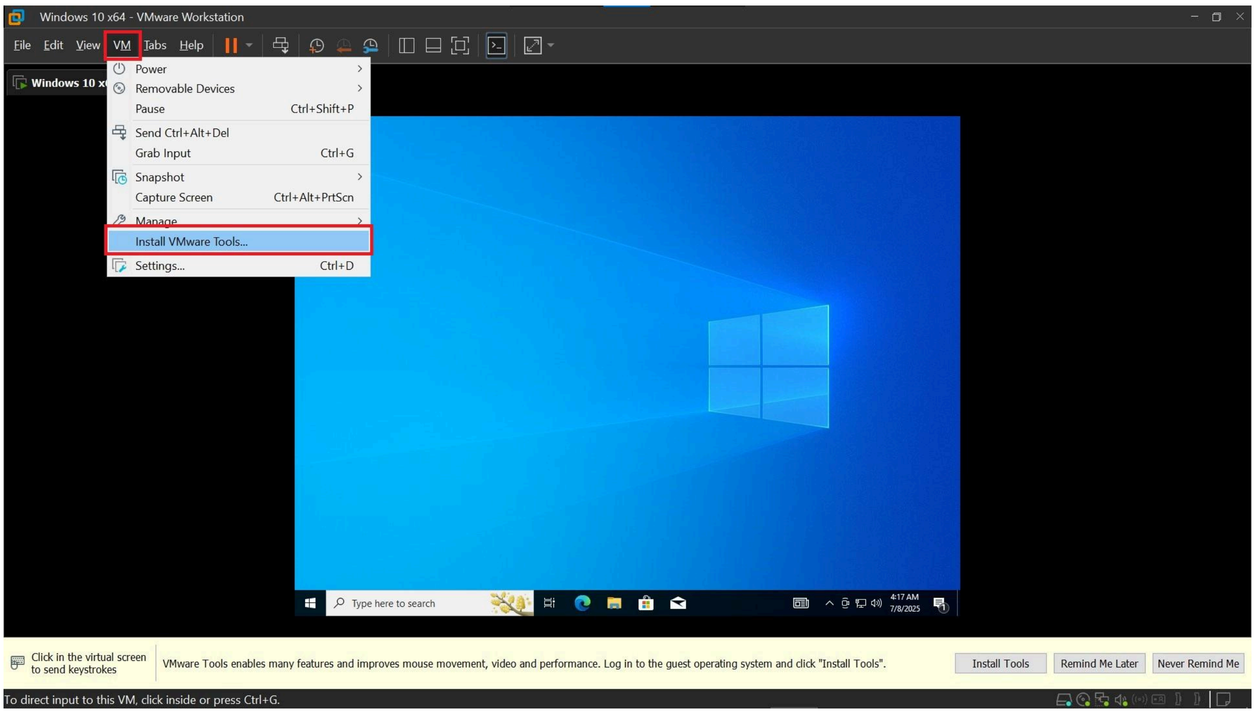
After installation, you might notice the screen resolution can't be changed. This usually happens if **VMware Tools (Guest Additions)** are not installed.

To fix it:

1. In the VM window, go to **VM > Install VMware Tools**.

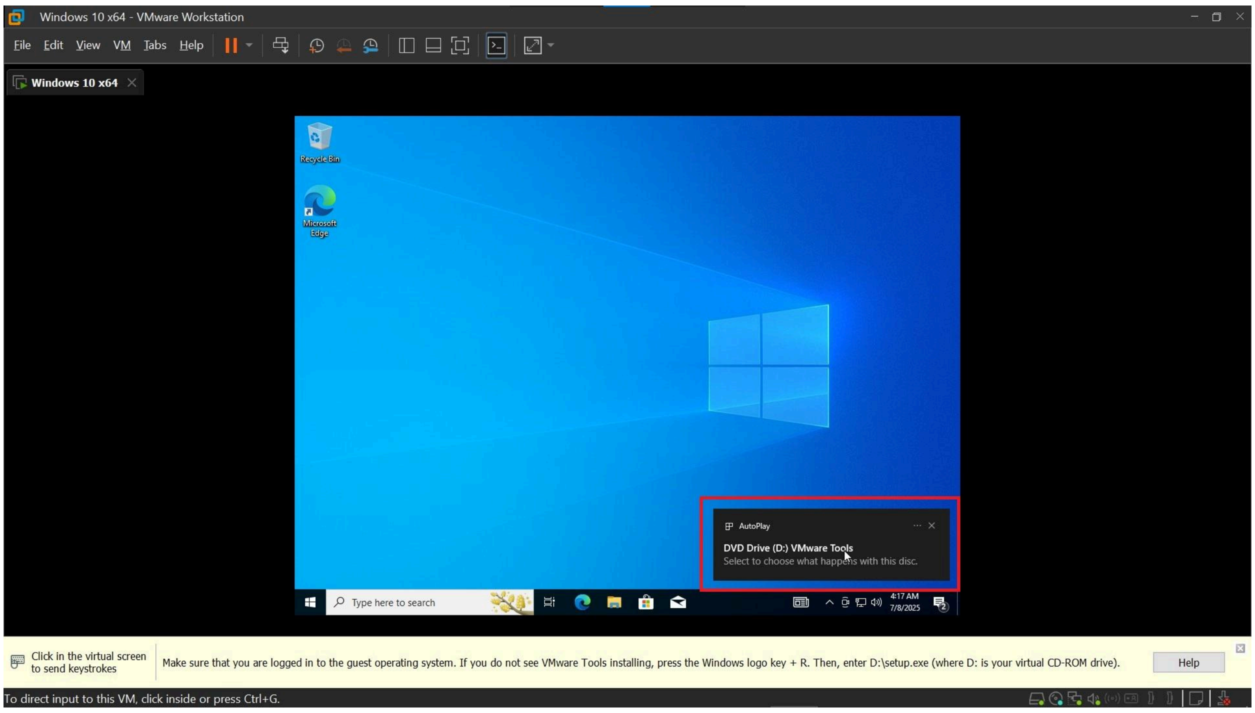
2. A virtual CD will mount inside the VM. Click the **popup notification** or open **File Explorer**.

3. Run setup.exe and complete the installation.



VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.



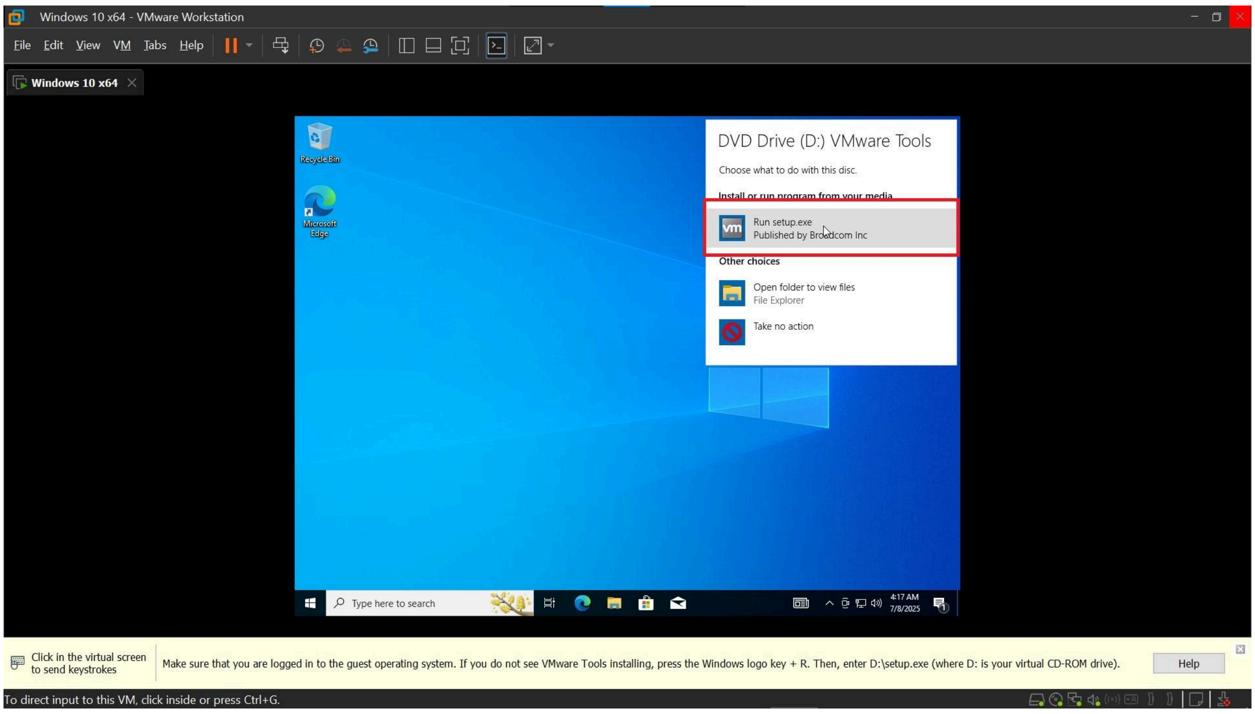
Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
Recycle Bin
Microsoft Edge
AutoPlay
Type here to search
4:17 AM
7/8/2025
Click in the virtual screen to send keystrokes
Help

DVD Drive (D:) VMware Tools

Select to choose what happens with this disc.

Make sure that you are logged in to the guest operating system. If you do not see VMware Tools installing, press the Windows logo key + R. Then, enter D:\setup.exe (where D: is your virtual CD-ROM drive).

To direct input to this VM, click inside or press Ctrl+G.



Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
Recycle Bin
Microsoft Edge
Install or run program from your media
Run setup.exe
Published by Broadcom Inc
Other choices
Open folder to view files
File Explorer
Take no action
Type here to search
4:17 AM
7/8/2025
Click in the virtual screen to send keystrokes
Help

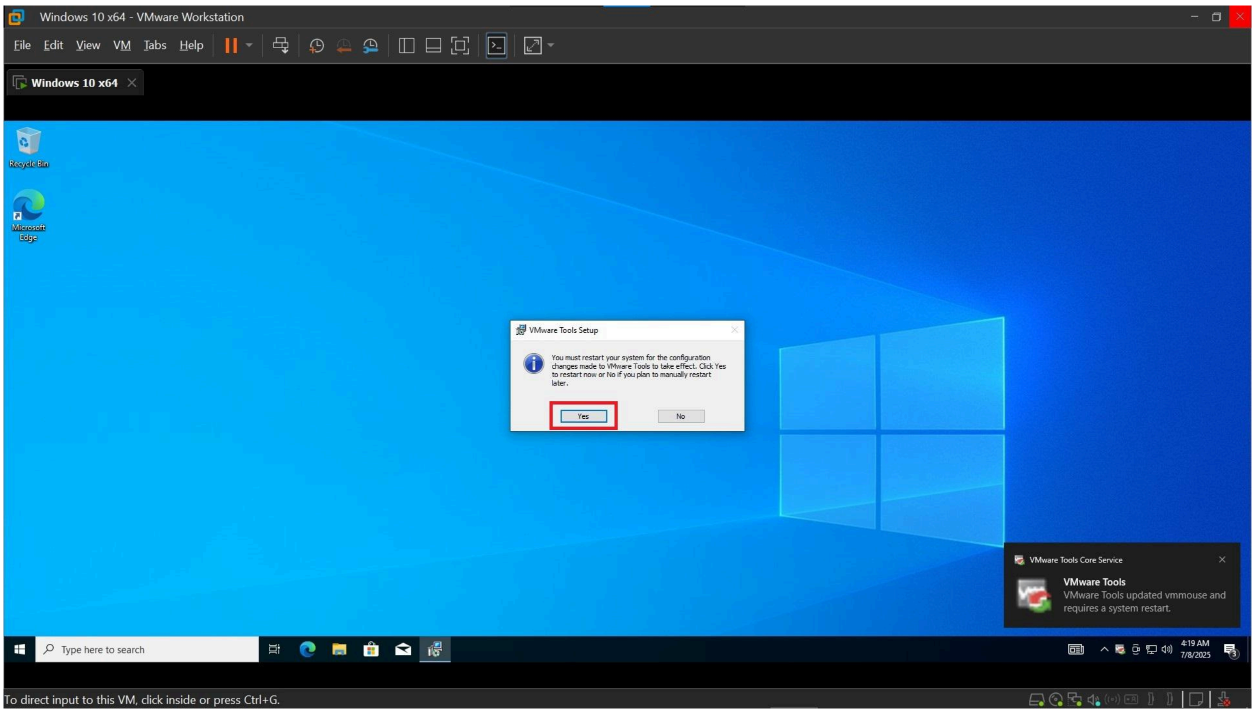
DVD Drive (D:) VMware Tools

Choose what to do with this disc.

Make sure that you are logged in to the guest operating system. If you do not see VMware Tools installing, press the Windows logo key + R. Then, enter D:\setup.exe (where D: is your virtual CD-ROM drive).

To direct input to this VM, click inside or press Ctrl+G.

After installation and a reboot, your screen resolution should be adjustable.



You must restart your system for the configuration changes made to VMware Tools to take effect. Click Yes to restart now or No if you plan to manually restart later.

VMware Tools

VMware Tools updated vmmouse and requires a system restart.

To direct input to this VM, click inside or press Ctrl+G.

Preparing the Windows VM for Vulnerability Scanning

Before scanning with Nessus, it's important to **intentionally reduce certain security features** to make the VM more vulnerable for testing purposes. This ensures that Nessus can effectively identify common misconfigurations and weaknesses — valuable for learning in a controlled lab environment.

> ⚠️ **Note**: Perform these steps **only in a lab/test environment**. Never expose a weakened system to the internet.

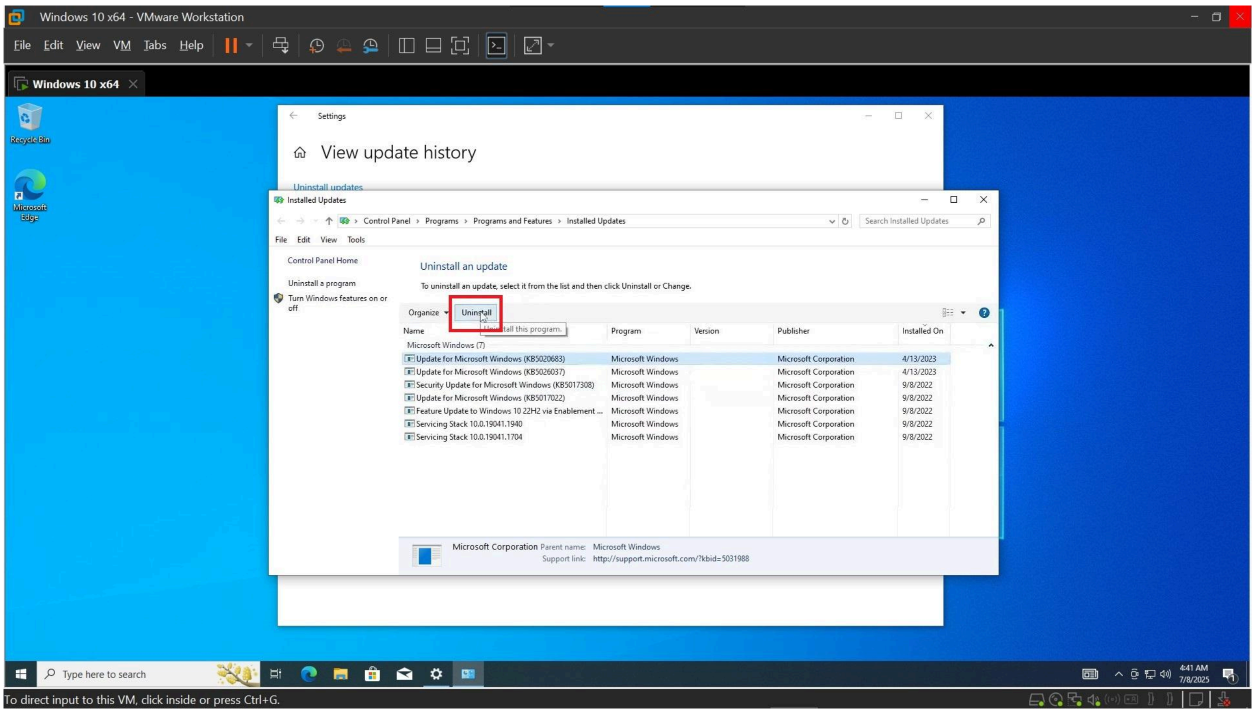
🛑 Disable Windows Updates

1. Go to **Start > Settings > Update & Security**.

2. Click **Pause updates for 7 days**. Click again to extend (up to a certain limit).

3. Click **View update history > Uninstall updates**.

4. In the new window, attempt to uninstall listed updates (if the option is available).



Uninstall an update

To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version	Publisher	Installed On
Microsoft Windows (7)				
Update for Microsoft Windows (KB5020683)	Microsoft Windows		Microsoft Corporation	4/13/2023
Update for Microsoft Windows (KB5026037)	Microsoft Windows		Microsoft Corporation	4/13/2023
Security Update for Microsoft Windows (KB5017308)	Microsoft Windows		Microsoft Corporation	9/8/2022
Update for Microsoft Windows (KB5017022)	Microsoft Windows		Microsoft Corporation	9/8/2022
Feature Update to Windows 10 22H2 via Enablement ...	Microsoft Windows		Microsoft Corporation	9/8/2022
Servicing Stack 10.0.19041.1940	Microsoft Windows		Microsoft Corporation	9/8/2022
Servicing Stack 10.0.19041.1704	Microsoft Windows		Microsoft Corporation	9/8/2022

Microsoft Corporation Parent name: Microsoft Windows
Support link: http://support.microsoft.com/?kbid=5031988

To direct input to this VM, click inside or press Ctrl+G.

Disable Windows Firewall

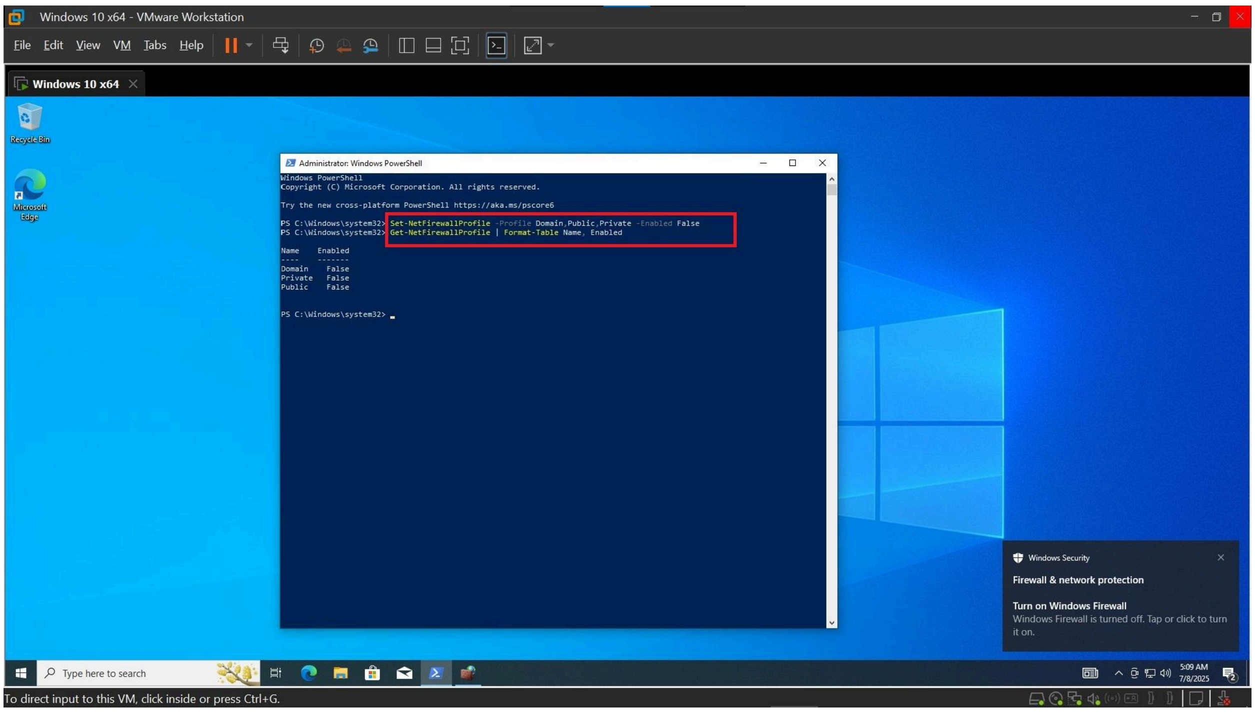
Open **PowerShell as Administrator** and run the following commands:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

```
# Verify firewall status
```

```
Get-NetFirewallProfile | Format-Table Name, Enabled
```

This step is necessary to ensure Nessus can reach the VM over the network.



Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
Recycle Bin
Microsoft Edge
Administrator: Windows PowerShell
Windows Security
Firewall & network protection
Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
Type here to search
5:09 AM
7/8/2025
To direct input to this VM, click inside or press Ctrl+G.

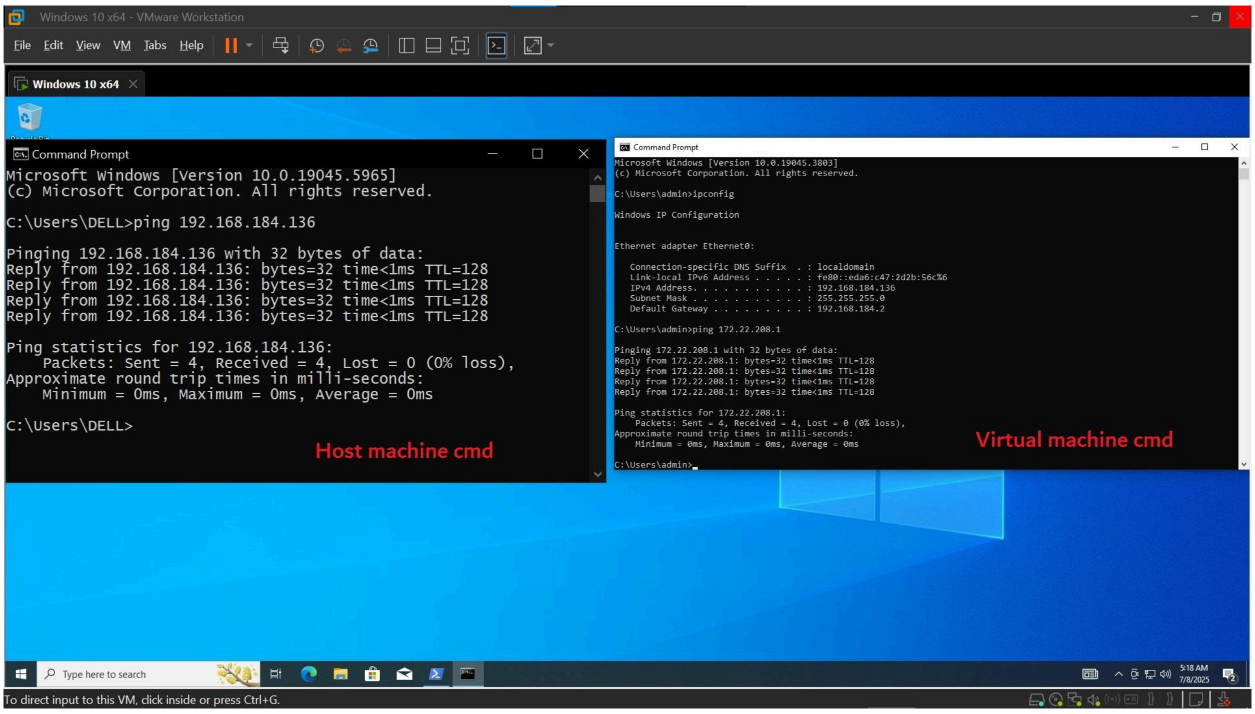
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
PS C:\Windows\system32> Get-NetFirewallProfile | Format-Table Name, Enabled

Name    Enabled
----    -------
Domain    False
Private   False
Public    False


PS C:\Windows\system32>
```

Verify Network Connectivity (Ping Test)

To confirm both systems are on the same network:

1. Open **Command Prompt (Admin)** inside the VM and run:
   Note the IP address.
2. On your host system, open Command Prompt and run:
   ping <VM_IP_Address>

Successful replies confirm that the VM is reachable for scanning.



Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
Command Prompt
Host machine cmd
Command Prompt
Virtual machine cmd
Type here to search
5:18 AM
7/8/2025
To direct input to this VM, click inside or press Ctrl+G.

```
Microsoft Windows [Version 10.0.19045.5965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping 192.168.184.136

Pinging 192.168.184.136 with 32 bytes of data:
Reply from 192.168.184.136: bytes=32 time<1ms TTL=128
Reply from 192.168.184.136: bytes=32 time<1ms TTL=128
Reply from 192.168.184.136: bytes=32 time<1ms TTL=128
Reply from 192.168.184.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.184.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\DELL>
```

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::eda6:c47:2d2b:56c%6
   IPv4 Address. . . . . . . . . . . : 192.168.184.136
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.184.2

C:\Users\admin>ping 172.22.208.1

Pinging 172.22.208.1 with 32 bytes of data:
Reply from 172.22.208.1: bytes=32 time<1ms TTL=128
Reply from 172.22.208.1: bytes=32 time<1ms TTL=128
Reply from 172.22.208.1: bytes=32 time<1ms TTL=128
Reply from 172.22.208.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.22.208.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin>
```

If the **ping is successful**, your VM is properly configured and reachable — you're good to go!

❗ If the ping fails:

- Double-check that **Windows Firewall** is disabled.

- Ensure the **network adapter** is correctly set (e.g., **NAT** or **Bridged** mode depending on your setup).

- Confirm both host and VM are on the same subnet.

Tweaking the windows so that nessus credential scan can pass authentication and do the scan

Preparing Windows for Nessus Credentialed Scanning

To allow Nessus to perform authenticated scans on your Windows VM, some Windows services and settings must be adjusted.

> ⚠️ **Important**: These changes reduce system security. Only apply them in **isolated lab environments**.

Enable Remote Registry Service

```
# Set the service to start automatically
Set-Service -Name RemoteRegistry -StartupType Automatic

# Start the service
Start-Service -Name RemoteRegistry

# Confirm it's running
Get-Service -Name RemoteRegistry
```

Disable UAC Prompts (for local admin credential access)

```
# Disable consent prompts for administrators

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" `
-Name "ConsentPromptBehaviorAdmin" -Value 0

# Disable secure desktop overlay for UAC

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" `
-Name "PromptOnSecureDesktop" -Value 0
```

Enable Remote Use of Local Admin Account

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" `
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Open SMB Port for Nessus

Enable the **File and Printer Sharing** rule to open TCP port 445:

```
Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"
```

🧠 **Note**: Without this, Nessus cannot authenticate or access admin shares.

Reboot the VM:A restart is recommended after making these system changes.

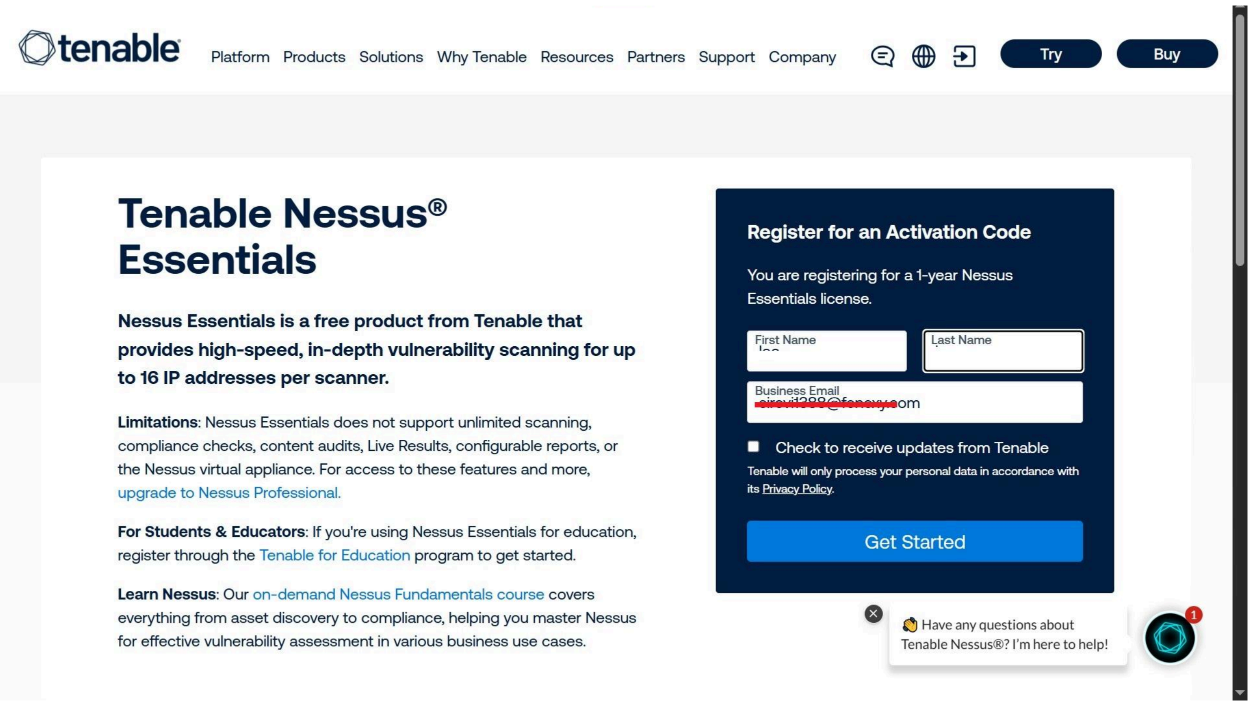
Installing Nessus on Host Machine

1. Go to the Tenable Nessus Download Page

2. Fill in basic details (name, email — a temporary email works).

3. You'll receive an **activation code** via email.

4. Download the **Windows** version and install it.



Tenable Nessus® Essentials

Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner.

Limitations: Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance. For access to these features and more, upgrade to Nessus Professional.

For Students & Educators: If you're using Nessus Essentials for education, register through the Tenable for Education program to get started.

Learn Nessus: Our on-demand Nessus Fundamentals course covers everything from asset discovery to compliance, helping you master Nessus for effective vulnerability assessment in various business use cases.

Register for an Activation Code

You are registering for a 1-year Nessus Essentials license.

First Name:

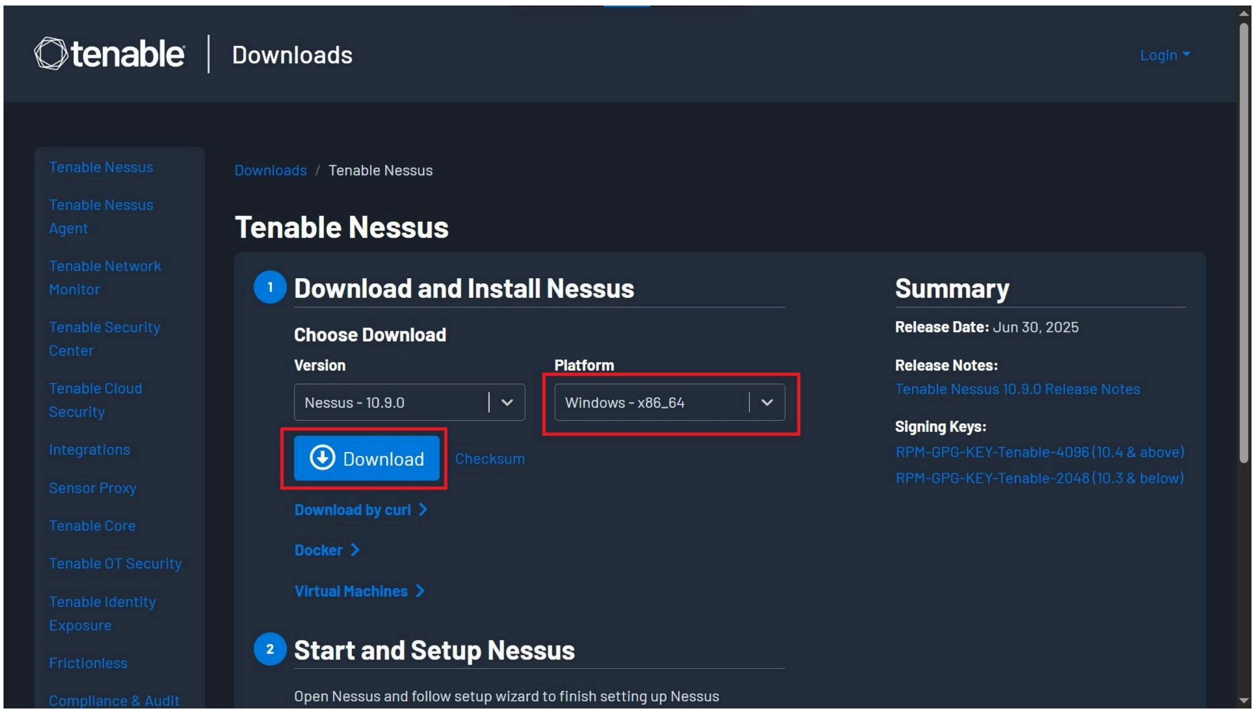
Last Name:

Business Email: [redacted]

□ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its Privacy Policy.

Have any questions about Tenable Nessus®? I'm here to help!



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.9.0

Platform: Windows - x86_64

2 Start and Setup Nessus

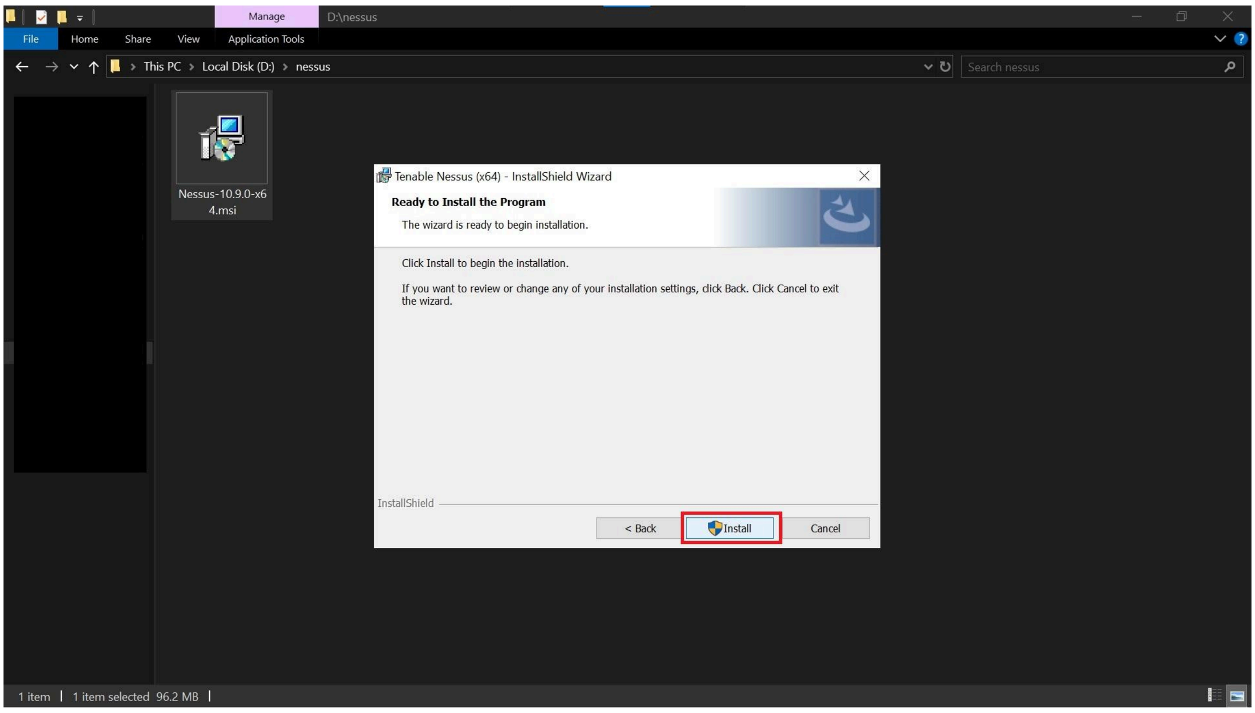
Open Nessus and follow setup wizard to finish setting up Nessus

Summary

Release Date: Jun 30, 2025

Release Notes: Tenable Nessus 10.9.0 Release Notes

Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)



[redacted]

Tenable Nessus (x64) - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

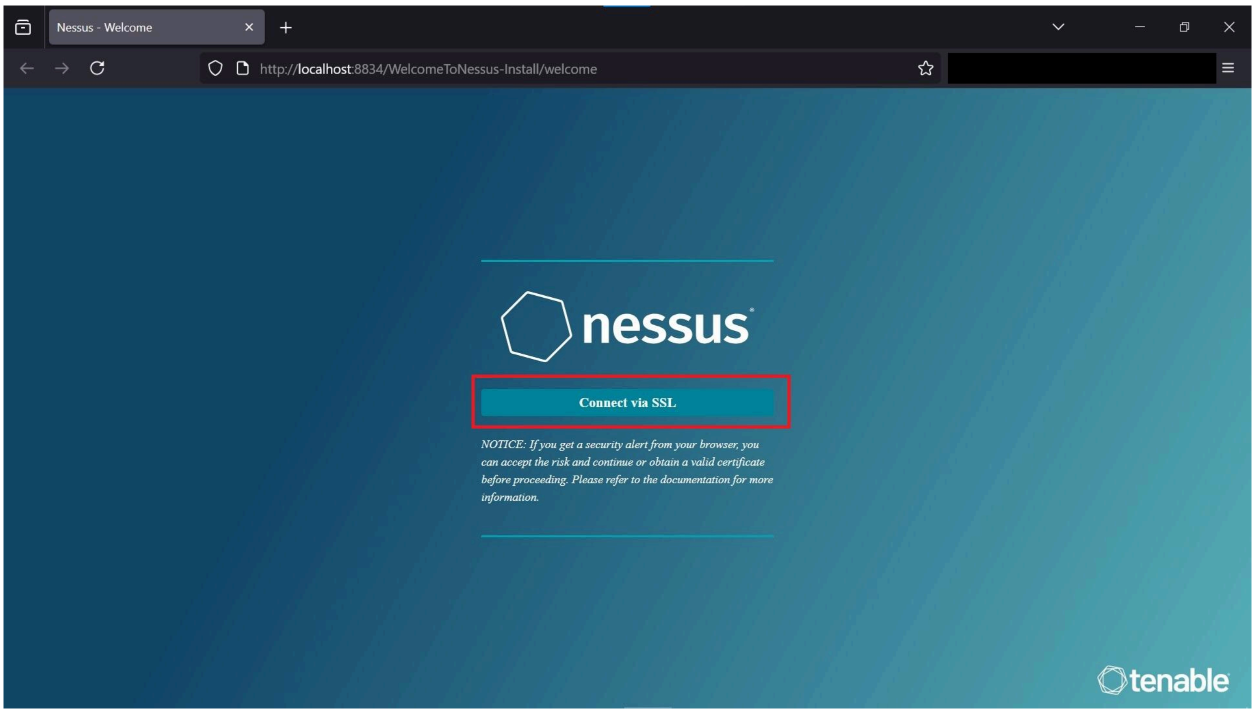
Follow the installation wizard:

- Accept terms, click **Next** through the prompts.
- Once complete, a browser window opens on: `https://localhost:8834`
- If warned about security risk, click **Advanced > Proceed**.

Nessus Setup in Browser

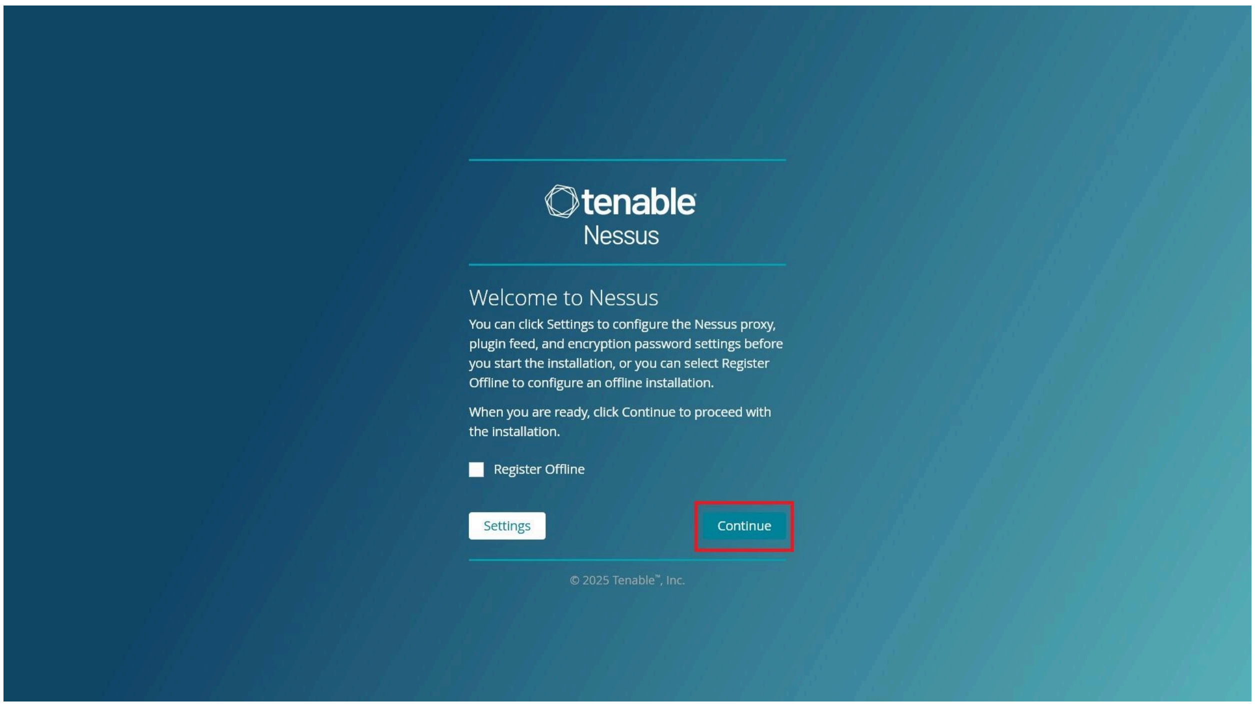
1. Choose **Nessus Essentials** and click **Continue**
2. If prompted to register, click **Skip** (you already have the activation code)
3. Paste the activation code and proceed
4. Create a Nessus admin account

This setup may take a few minutes to complete.



[redacted]

NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.



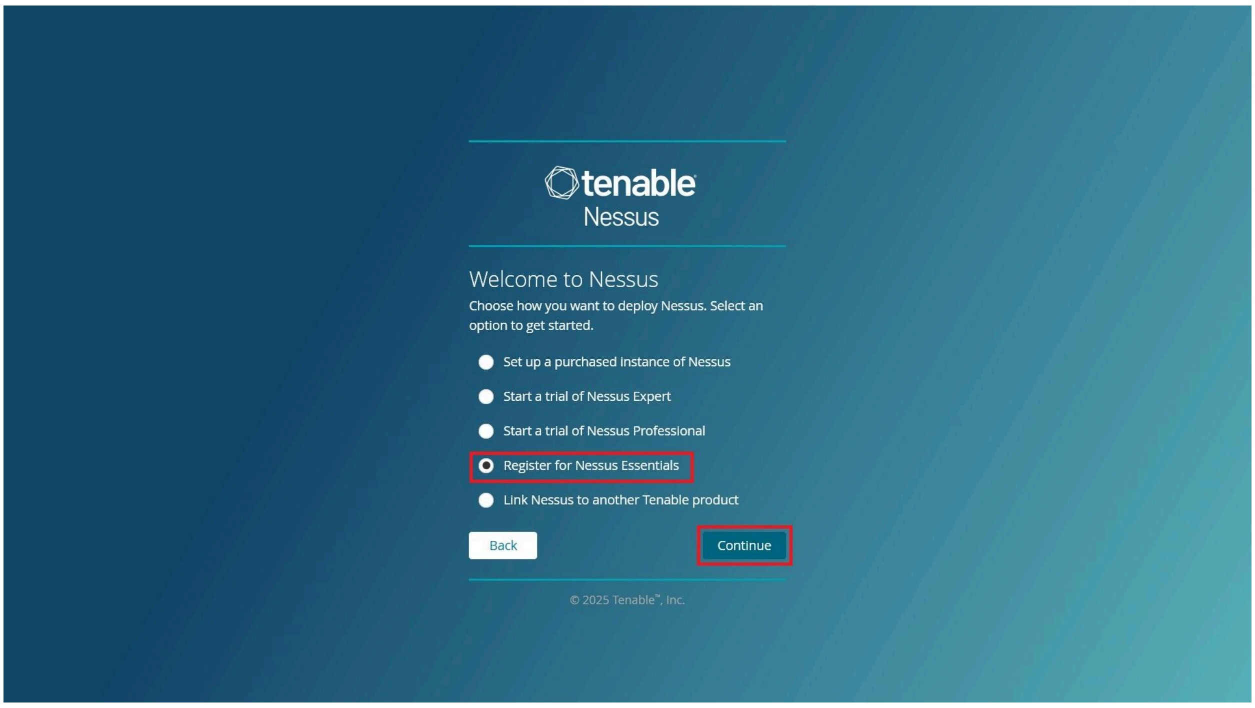
Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

☐ Register Offline

© 2025 Tenable™, Inc.



Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

○ Set up a purchased instance of Nessus

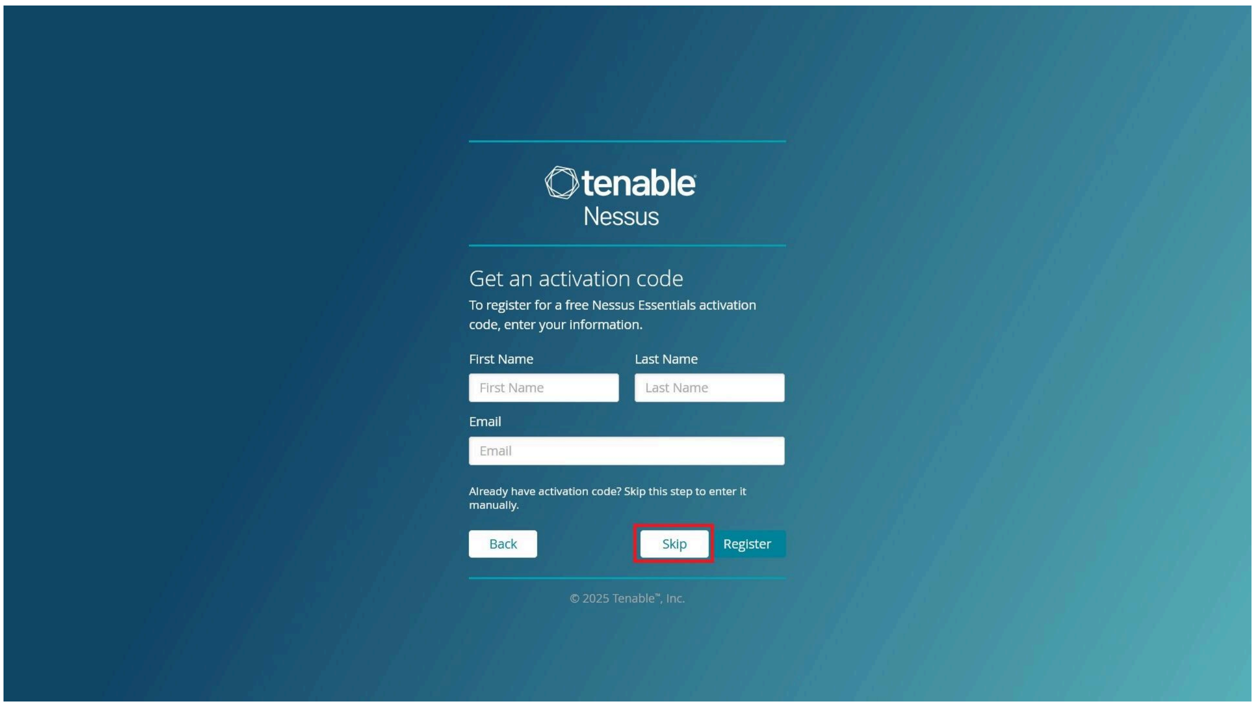
○ Start a trial of Nessus Expert

○ Start a trial of Nessus Professional

● Register for Nessus Essentials

○ Link Nessus to another Tenable product

© 2025 Tenable™, Inc.



Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

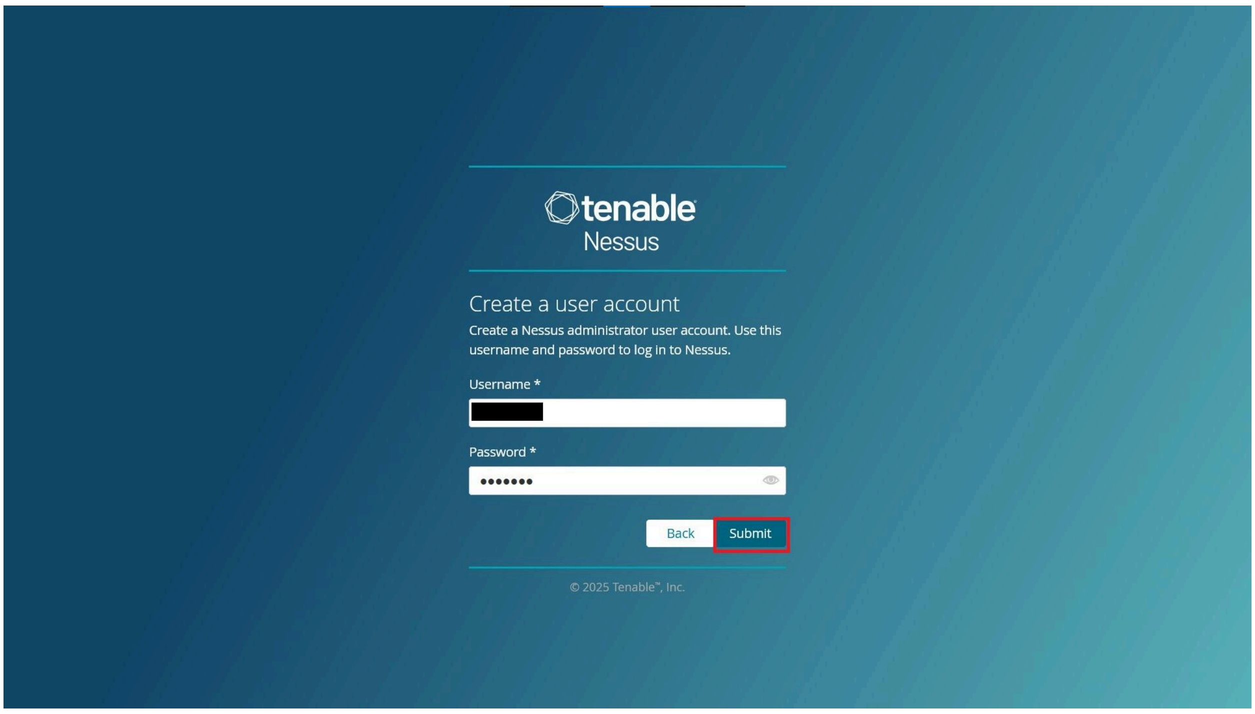
First Name: First Name

Last Name: Last Name

Email: Email

Already have activation code? Skip this step to enter it manually.

© 2025 Tenable™, Inc.



Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

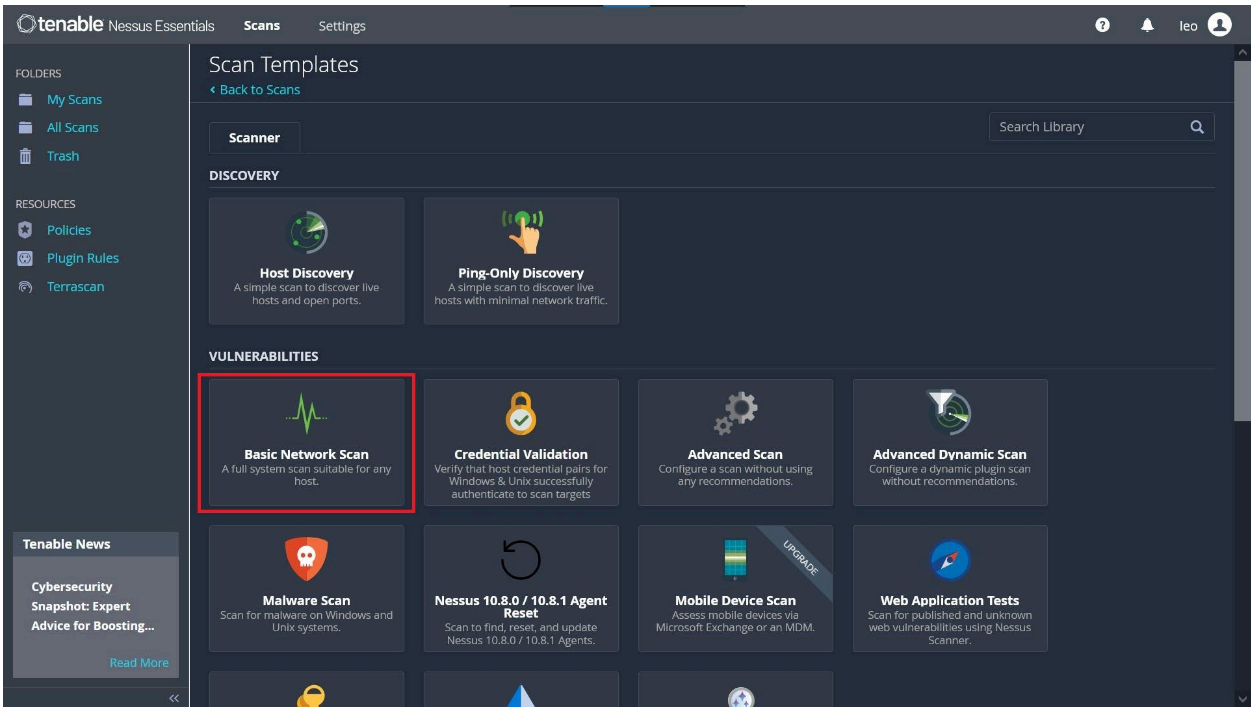
Username *: [redacted]

Password *: •••••••

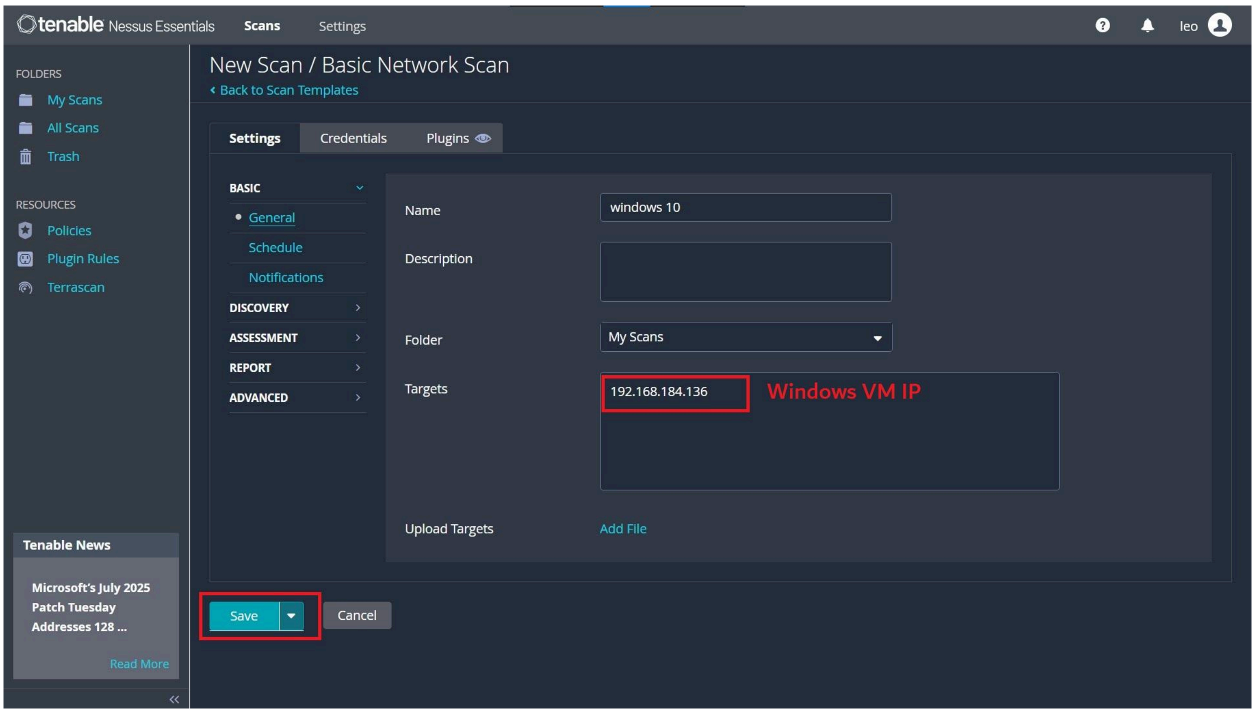
© 2025 Tenable™, Inc.

Running a basic (non-credentialed) scan

1. Once setup completes, go to **My Scans**
2. Click **Create a New Scan**
3. Choose **Basic Network Scan**


tenable Nessus Essentials
Scans
Settings
leo
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Expert Advice for Boosting...
Read More
Scan Templates
Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

4. Enter target details (e.g., IP of the Windows VM)



Name: windows 10

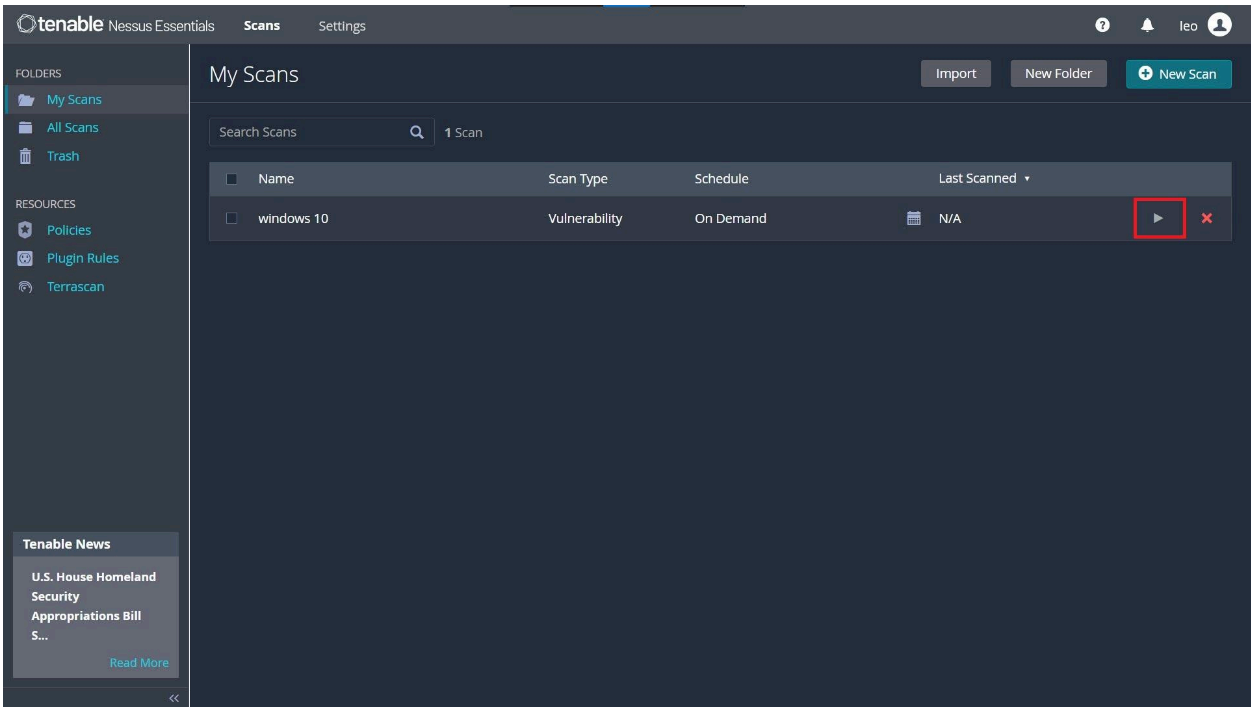
Description:

Folder: My Scans

Targets: 192.168.184.136

Windows VM IP

5. Launch the scan



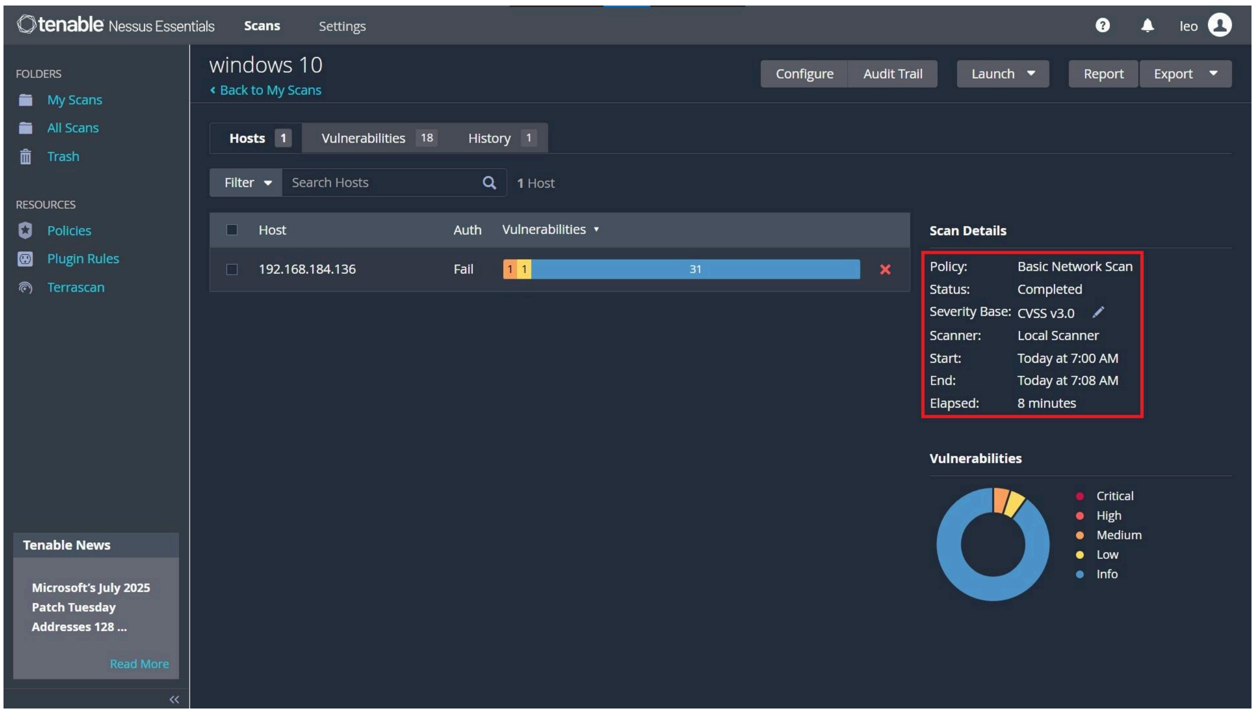
Name	Scan Type	Schedule	Last Scanned
windows 10	Vulnerability	On Demand	N/A

Launching the Initial Basic Scan

Once your scan is configured and launched, Nessus will begin scanning the specified IP. In this case, the scan took **approximately 8 minutes**.

After completion:

- The scan status will show **"Completed"**
- Click the **IP address** to view detailed findings.



Host	Auth	Vulnerabilities
192.168.184.136	Fail	1 1 31

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:00 AM
End: Today at 7:08 AM
Elapsed: 8 minutes

Reviewing the Findings

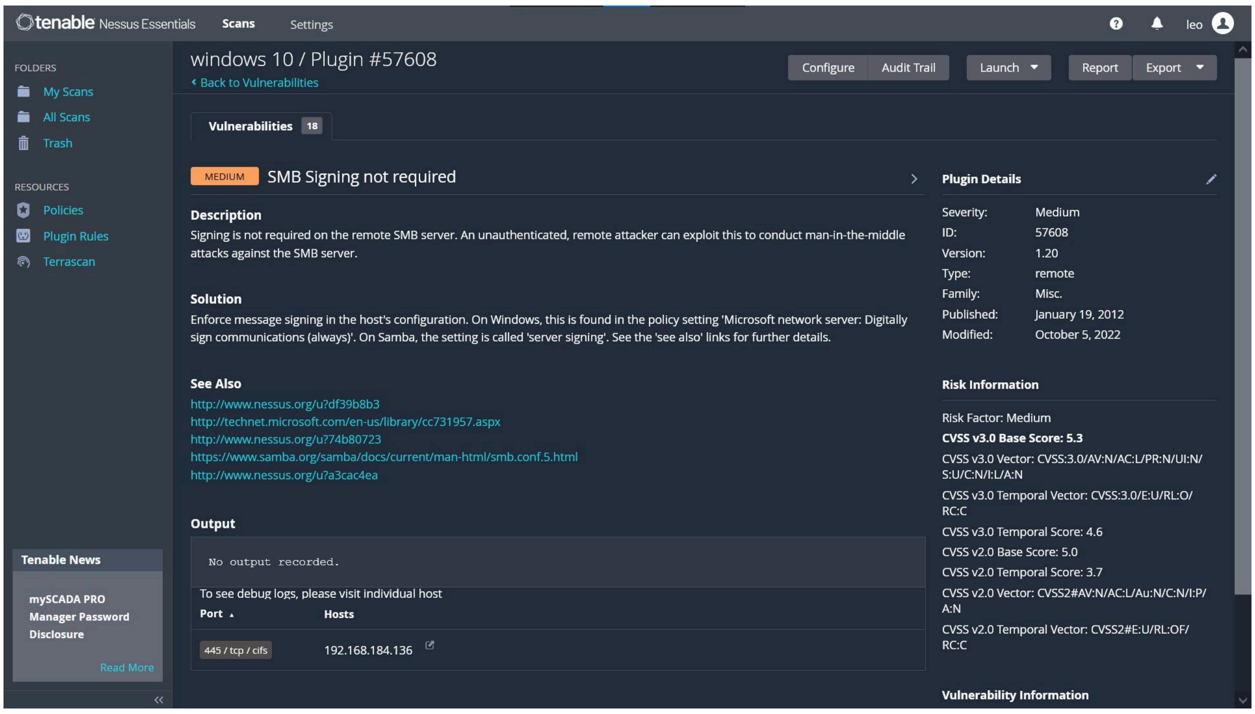
Click on any listed vulnerability to view:

- A description of the issue
- Risk level

- Recommended solution
- Reference URLs (under **See Also**) for further reading

These insights help guide the remediation process for the identified vulnerabilities.

Nessus stores each scan under the **History tab**, allowing you to revisit past results at any time.



windows 10 / Plugin #57608

MEDIUM SMB 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	192.168.184.136

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

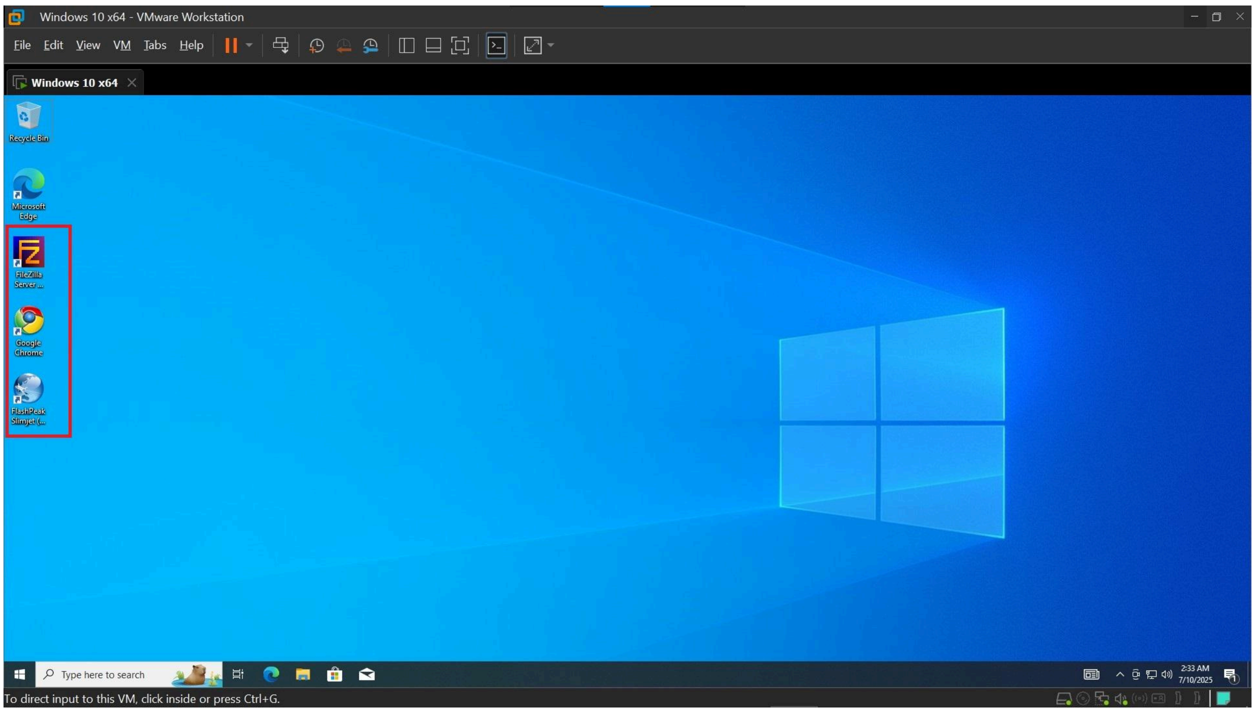
Installing outdated software to simulate vulnerabilities

The initial scan detected only a **medium-severity vulnerability**. To get deeper insights, we'll perform a **credentialed scan**, which allows Nessus to:

- Identify **installed software**
- Review **missing patches**
- Detect **configuration risks**

Simulating Real-World Vulnerabilities with Outdated Software

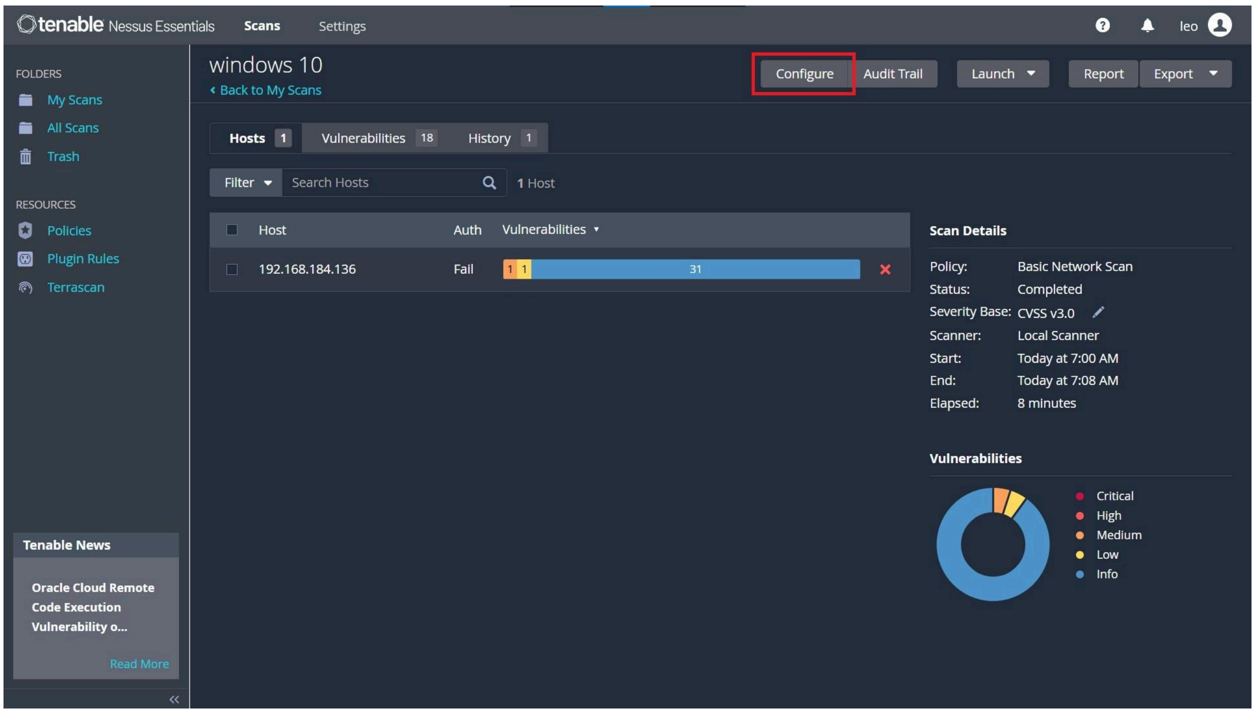
- Installed legacy versions of commonly used applications:
    - **Google Chrome**
    - **Slimjet**
    - **FileZilla**



Performing a credentialed scan

To configure credentials for your existing scan:

1. Go to **My Scans**
2. Click the **three-dot menu > Configure**
3. Navigate to the **Credentials** tab
4. Under **Windows**, provide:
   - Username
   - Password
   - Domain name

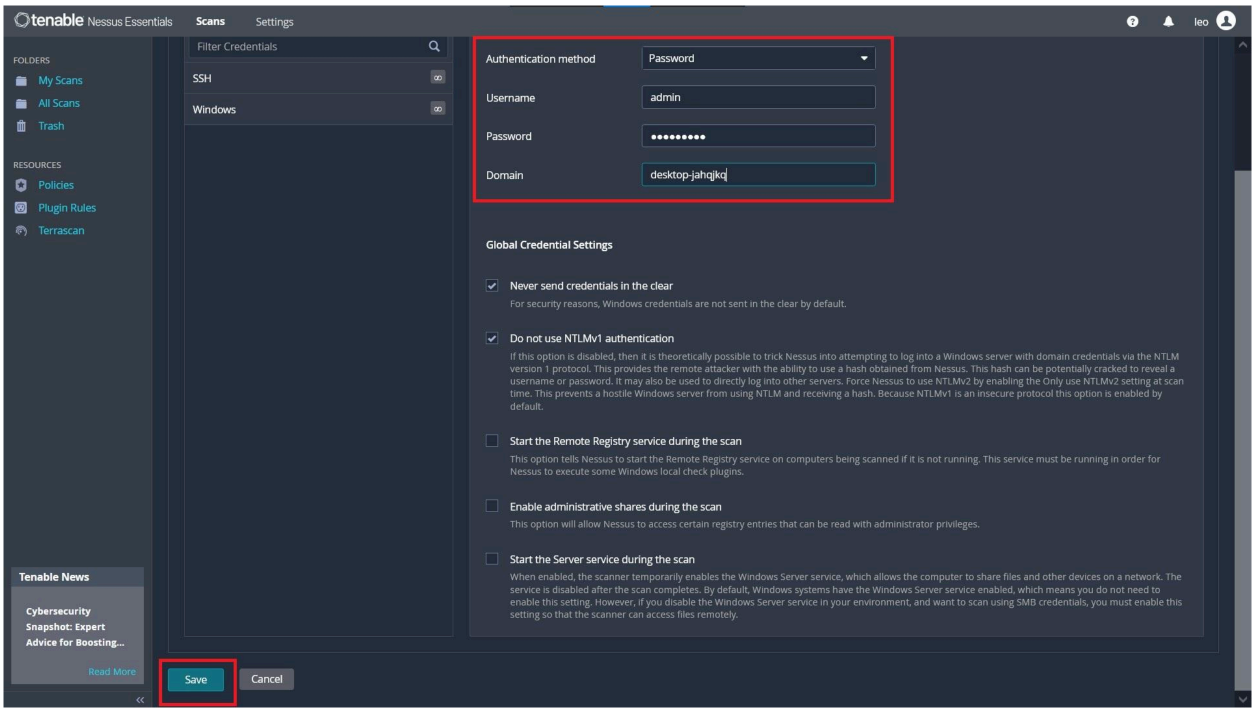


Host	Auth	Vulnerabilities
192.168.184.136	Fail	1 1 31

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:00 AM
End: Today at 7:08 AM
Elapsed: 8 minutes

Vulnerabilities



Authentication method: Password

Username: admin

Password: •••••••••

Domain: desktop-jahqjkq

Global Credential Settings

☑ Never send credentials in the clear
For security reasons, Windows credentials are not sent in the clear by default.

☑ Do not use NTLMv1 authentication
If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Nessus to use NTLMv2 by enabling the Only use NTLMv2 setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol this option is enabled by default.

☐ Start the Remote Registry service during the scan
This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.

☐ Enable administrative shares during the scan
This option will allow Nessus to access certain registry entries that can be read with administrator privileges.

☐ Start the Server service during the scan
When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.

💡 Use **`whoami`** in Command Prompt inside the VM to find your credentials:
Format: **`DESKTOP-XYZ\admin`**

- **`DESKTOP-XYZ`** = Domain
- **`admin`** = Username

Click **Save**, then **Launch** the scan.

Fixing Authentication Failures

If Nessus shows **"Authentication Failed"**, it likely means:

- You're using a **non-default admin account** that lacks the required permissions.

Ensure the following configurations are applied during VM setup:

➔ **Remote Registry:** Enabled

➔ **UAC Prompts:** Disabled for smoother remote access

➔ **LocalAccountTokenFilterPolicy:** Modified to allow full remote administrative rights

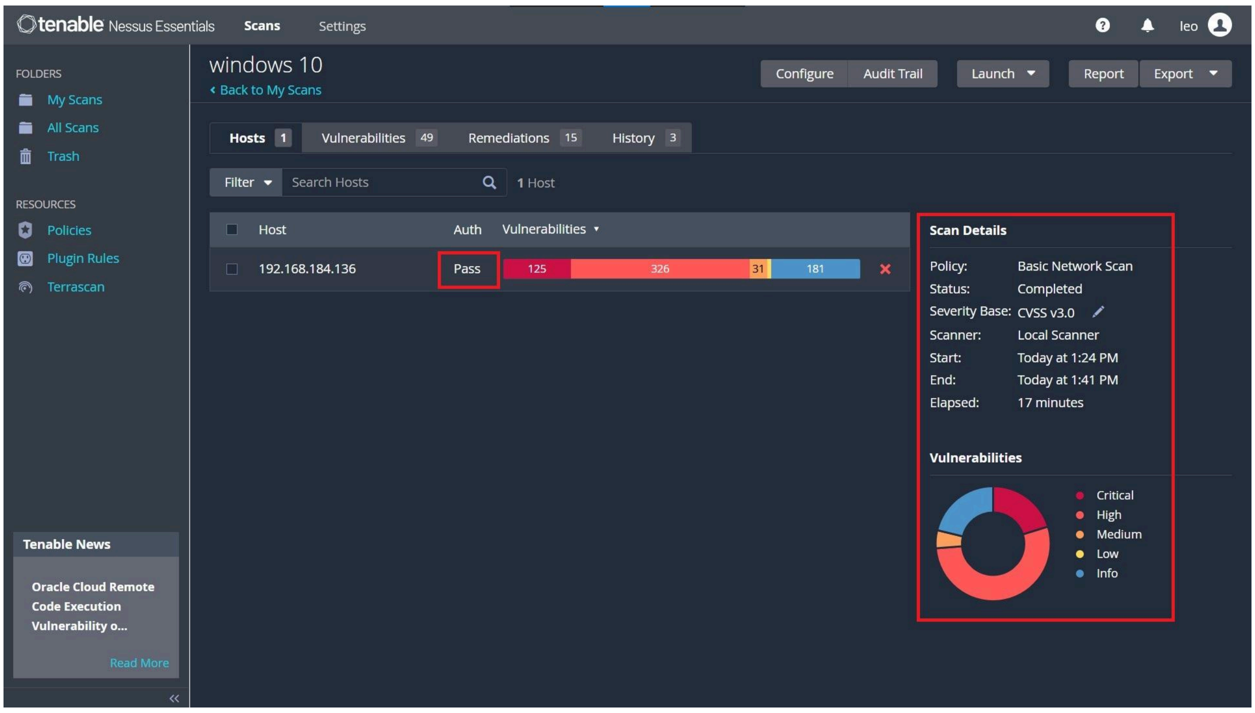
➔ **File and Printer Sharing:** Firewall rules enabled

Reviewing results and remediation steps

After scanning, Nessus reported:

- **49 vulnerabilities**, including **Critical**, **High**, and **Medium** severity issues
- Several related to **Google Chrome** missing updates

Use the listed **CVE IDs** to search for more info online — they provide detailed technical references and write-ups.



windows 10

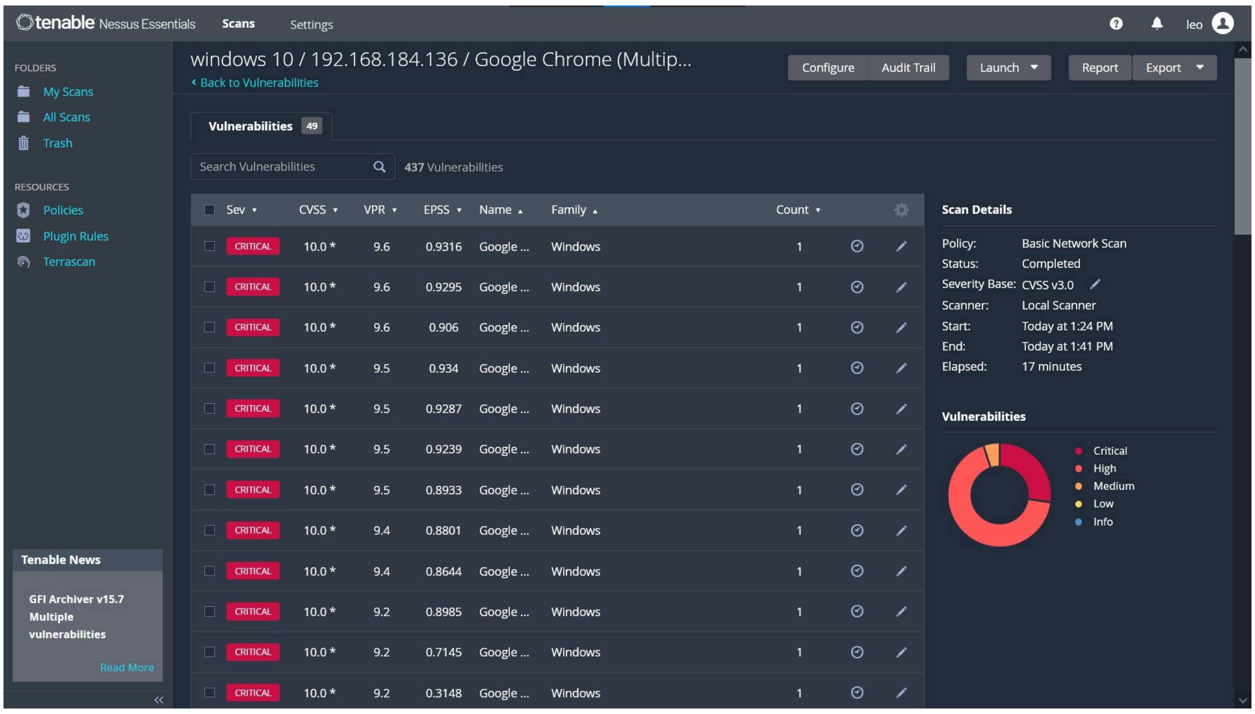
‹ Back to My Scans

Host	Auth	Vulnerabilities
192.168.184.136	Pass	125 326 31 181

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:24 PM
End: Today at 1:41 PM
Elapsed: 17 minutes

Vulnerabilities



windows 10 / 192.168.184.136 / Google Chrome (Multip...

‹ Back to Vulnerabilities

437 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	9.6	0.9316	Google ...	Windows	1
CRITICAL	10.0 *	9.6	0.9295	Google ...	Windows	1
CRITICAL	10.0 *	9.6	0.906	Google ...	Windows	1
CRITICAL	10.0 *	9.5	0.934	Google ...	Windows	1
CRITICAL	10.0 *	9.5	0.9287	Google ...	Windows	1
CRITICAL	10.0 *	9.5	0.9239	Google ...	Windows	1
CRITICAL	10.0 *	9.5	0.8933	Google ...	Windows	1
CRITICAL	10.0 *	9.4	0.8801	Google ...	Windows	1
CRITICAL	10.0 *	9.4	0.8644	Google ...	Windows	1
CRITICAL	10.0 *	9.2	0.8985	Google ...	Windows	1
CRITICAL	10.0 *	9.2	0.7145	Google ...	Windows	1
CRITICAL	10.0 *	9.2	0.3148	Google ...	Windows	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:24 PM
End: Today at 1:41 PM
Elapsed: 17 minutes

Vulnerabilities

To remediate vulnerabilities:

- **Resume Windows Updates**:
  - Go to **Settings > Windows Update > Resume Updates**
- **Update vulnerable software**:
  - Open outdated apps (e.g., Chrome)
  - Navigate to **Settings > About** and check for updates
- **Remove intentionally outdated software** once testing is complete

After applying patches and updates, run a **final credentialed scan** to confirm improvements and validate that vulnerabilities have been mitigated.

🎉 Vulnerability Remediation Completed

Congratulations you’ve successfully completed this vulnerability detection and remediation exercise!

After applying the necessary remediation steps,

Throughout this hands-on project, you’ve learned to:

- Use **Nessus** for vulnerability scanning
- Interpret scan results effectively
- Remediate discovered vulnerabilities
- Validate fixes with a follow-up scan