

## Domain 04 Demo 01

### Scanning Local VM Using Nessus

**Objective:** To conduct vulnerability scans on a local Windows virtual machine using Nessus, install and configure Nessus, scan the target machine, and generate a report to visualize identified vulnerabilities and necessary patches

**Tools required:** Nessus

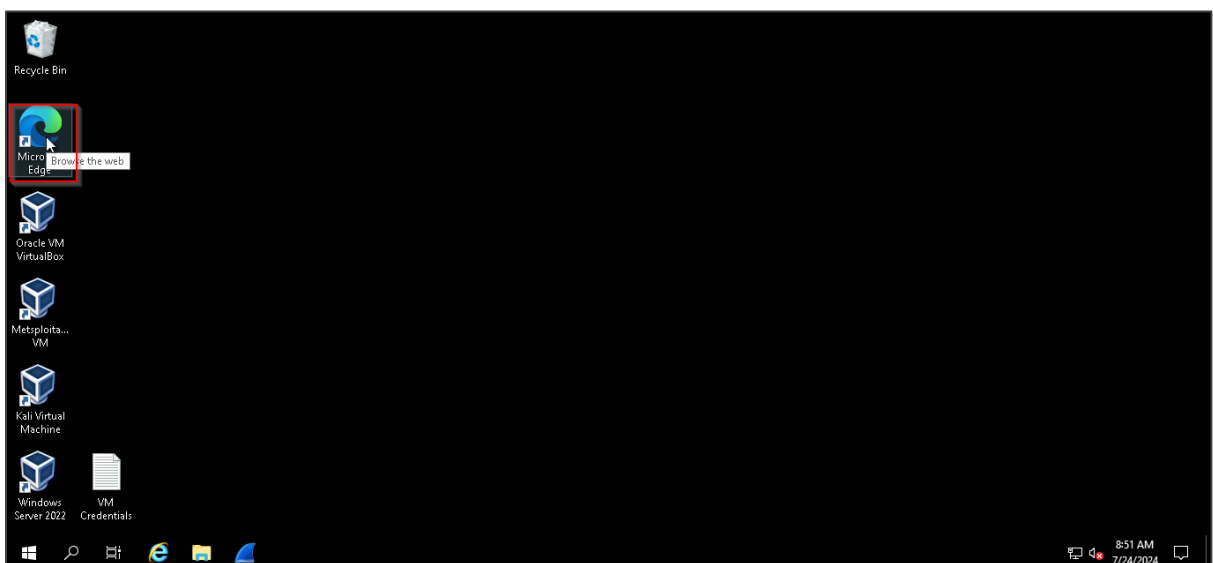
**Prerequisites:** None

Steps to be followed:

1. Install the Nessus vulnerability scanner
2. Configure Nessus
3. Prepare for scanning
4. Conduct a vulnerability scan
5. Review scan results

#### Step 1: Install the Nessus vulnerability scanner

##### 1.1 Open the Microsoft Edge browser

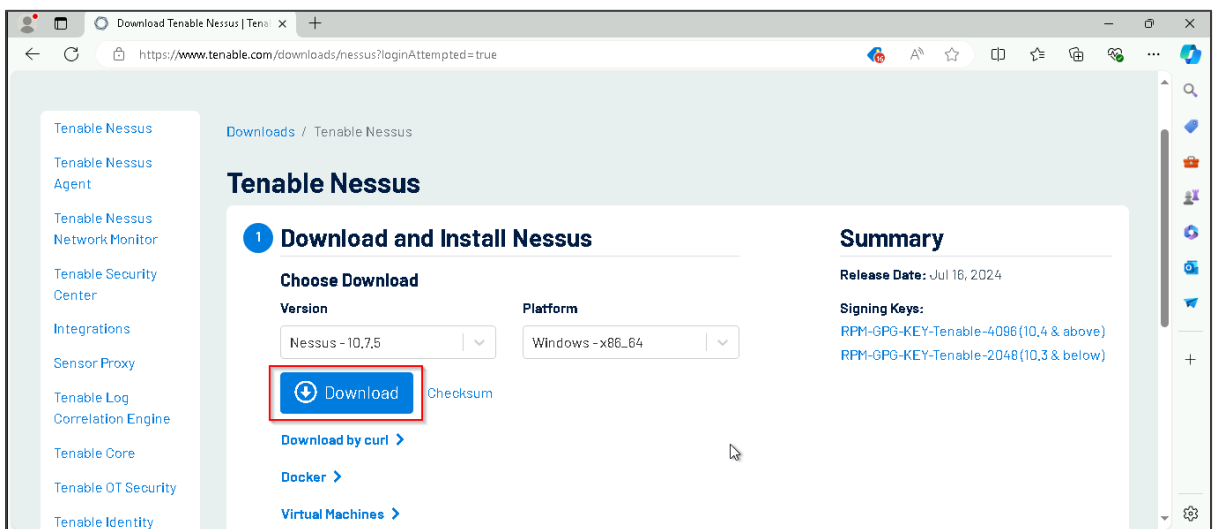


1.2 Browse to the following link:

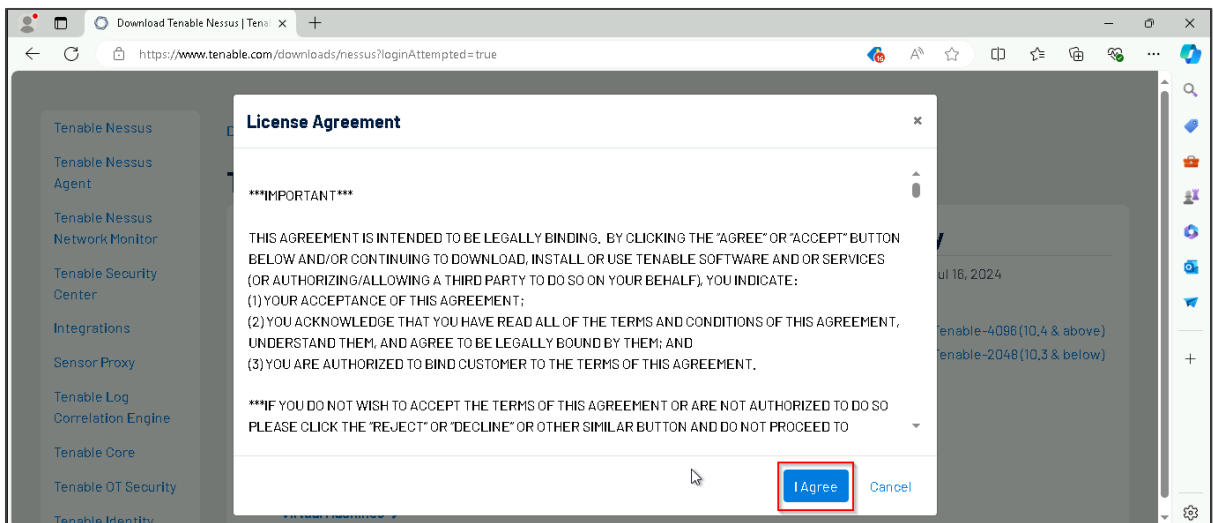
**<https://www.tenable.com/downloads/nessus?loginAttempted=true>**



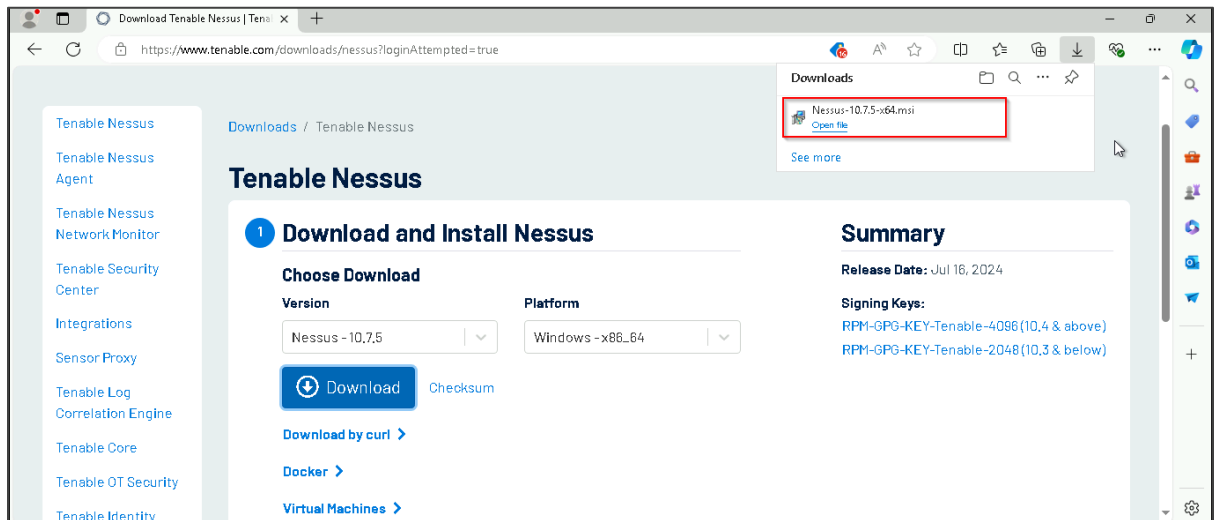
1.3 Click on the **Download** button



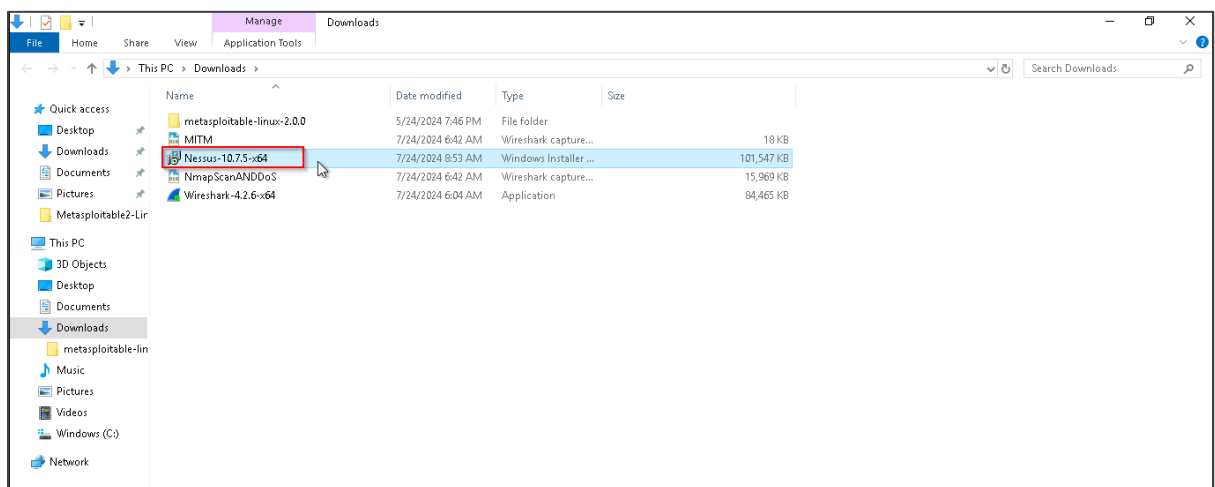
1.4 Click on **I Agree** to begin the download



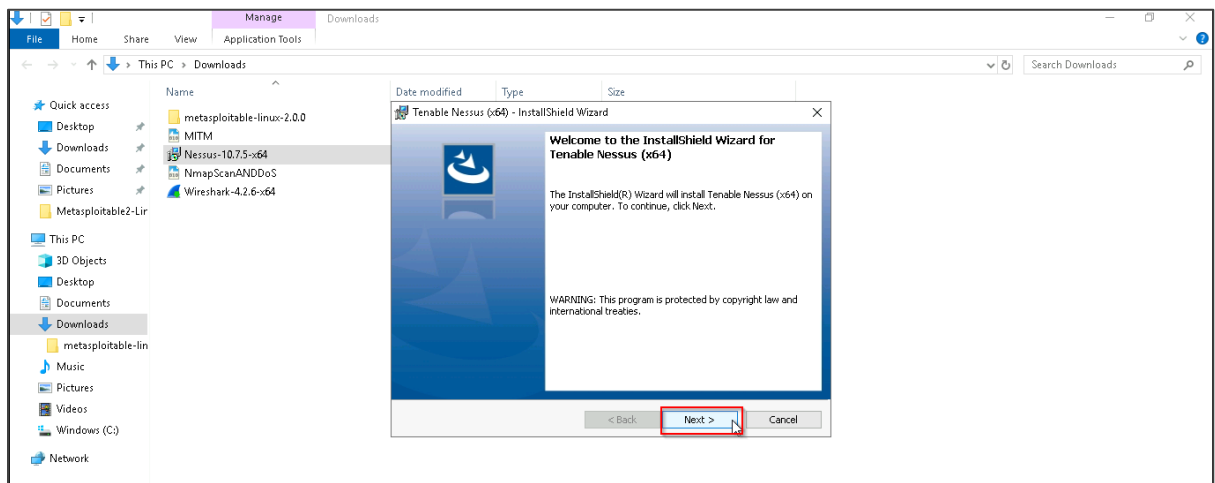
The Nessus software is downloaded successfully.



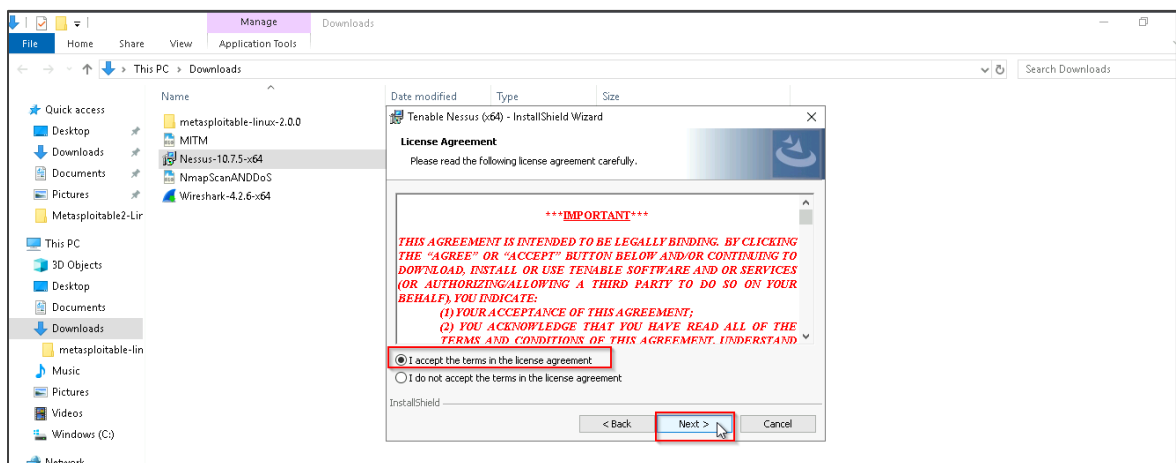
1.5 Navigate to the **Downloads** folder and click on the downloaded **Nessus-10.7.5-x64** file to begin the installation



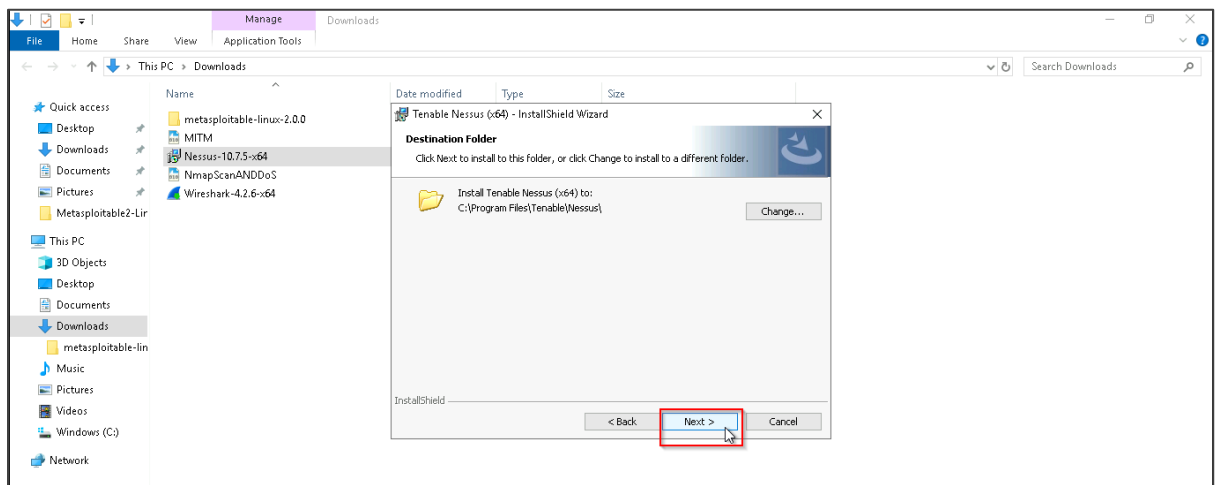
## 1.6 Click on **Next** when the installation wizard appears



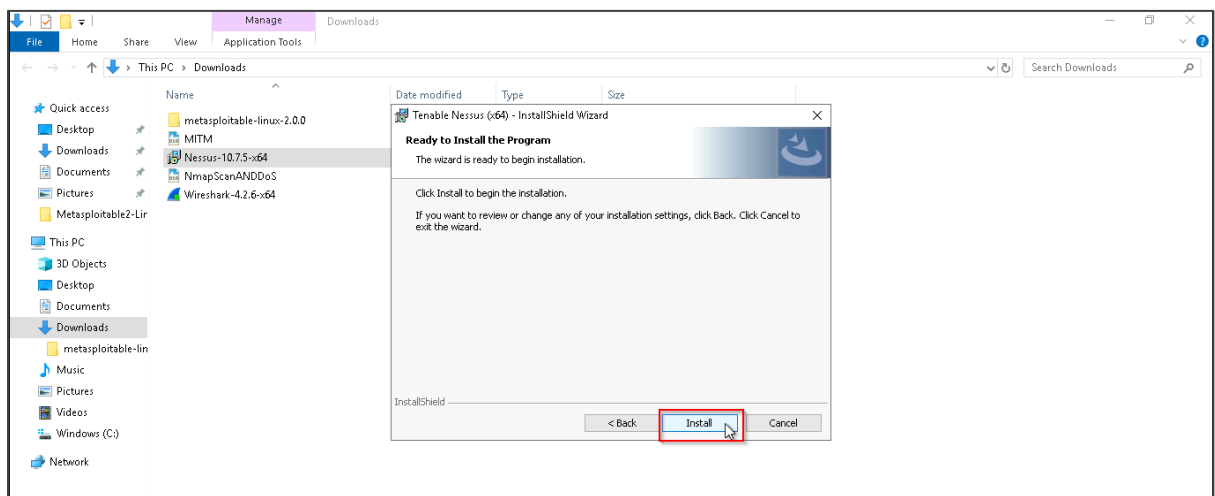
## 1.7 Select **I accept the terms in the license agreement** and click on **Next**



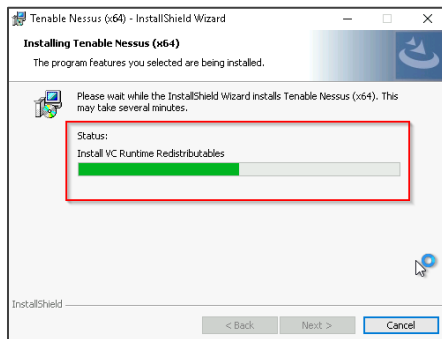
## 1.8 Click on **Next**



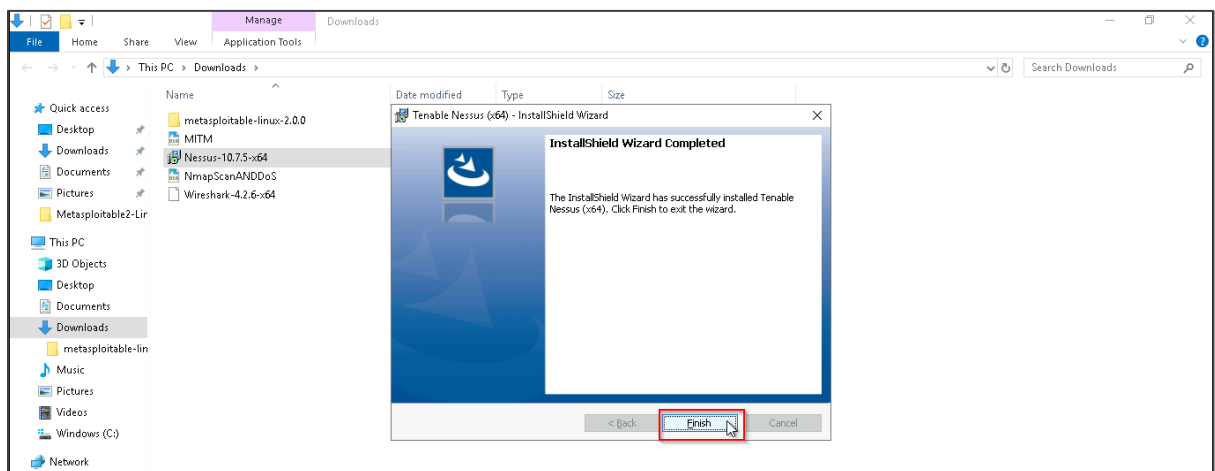
## 1.9 Further, click on the **Install** button to begin the installation process



The installation process starts as shown below:

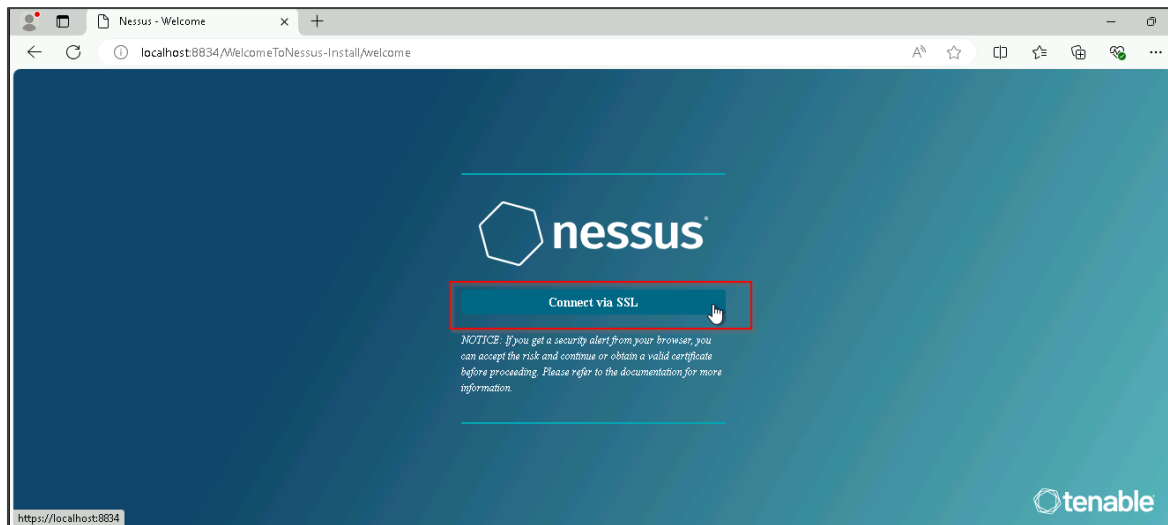


1.10 Once the installation is done, click on **Finish**

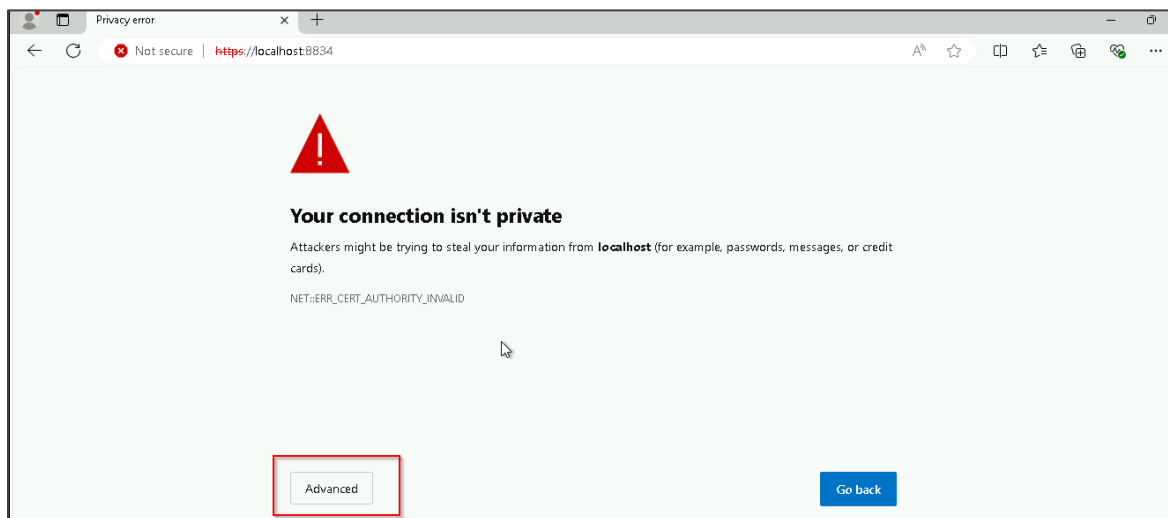


## Step 2: Configure Nessus

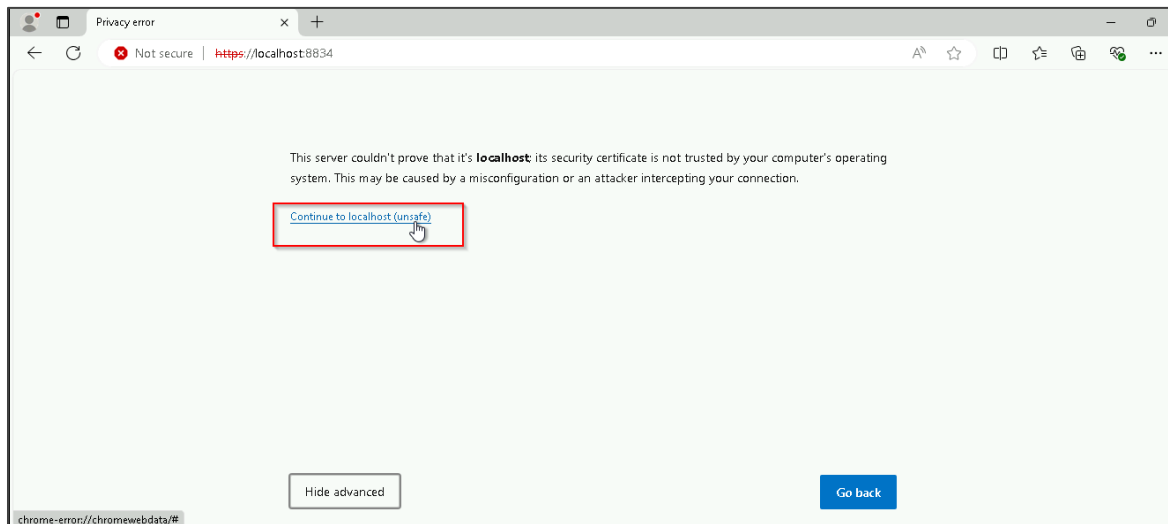
2.1 After installation, a web page will open. Click on **Connect via SSL** as shown below:



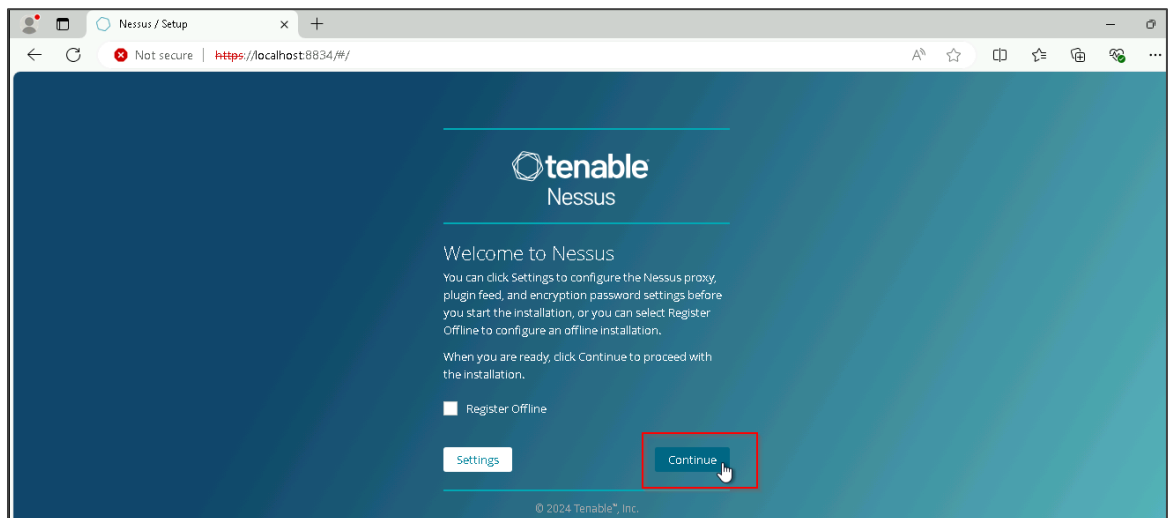
2.2 Click on the **Advanced** button on the warning page



## 2.3 Click on the **Continue to localhost(unsafe)** link

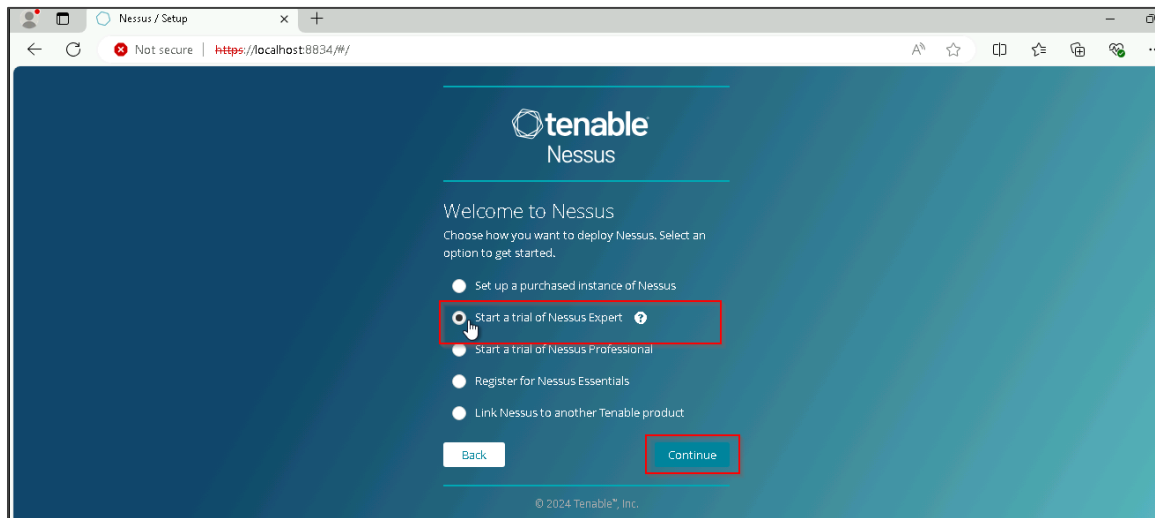


## 2.4 Click on **Continue** on the Nessus welcome page

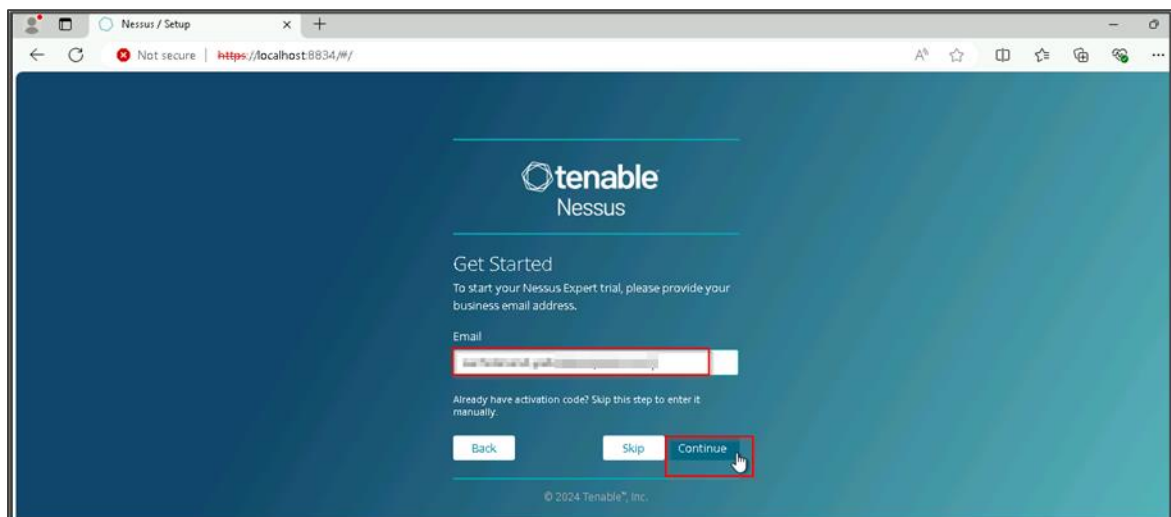




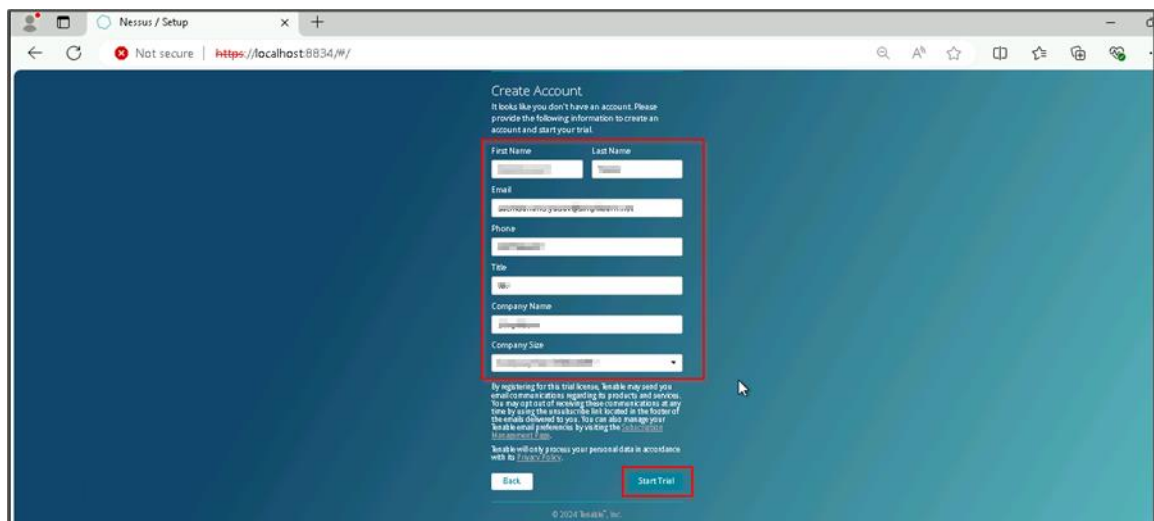
## 2.5 Select the option stating **Start a trial of Nessus Expert** and click on **Continue**



## 2.6 Provide your **Email** and click on **Continue**



## 2.7 Enter the required details and click on **Start Trial**



Create Account

It looks like you don't have an account. Please provide the following information to create an account and start your trial.

First Name

Last Name

Email

Phone

Title

Company Name

Company Size

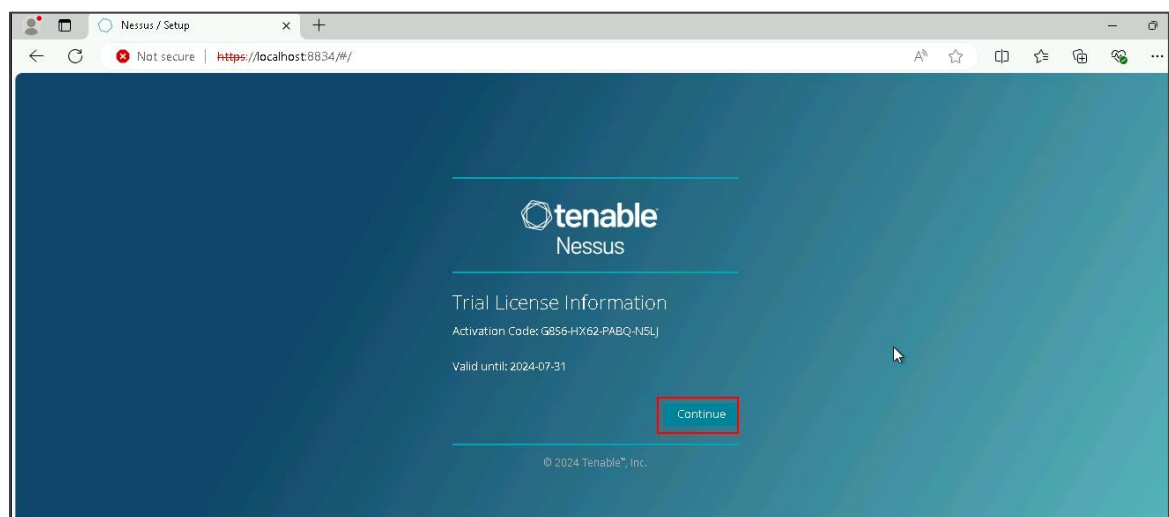
By registering for this trial license, Tenable may send you email communications regarding its products and services. You may opt out of receiving these communications at any time by clicking the unsubscribe link located in the footer of the emails delivered to you. You can also manage your Tenable email preferences by visiting the [privacy policy](#).


Tenable will only process your personal data in accordance with its [privacy policy](#).

[Back](#) [Start Trial](#)

© 2024 Tenable®, Inc.

## 2.8 Further, click on **Continue**



 **tenable**  
Nessus

Trial License Information

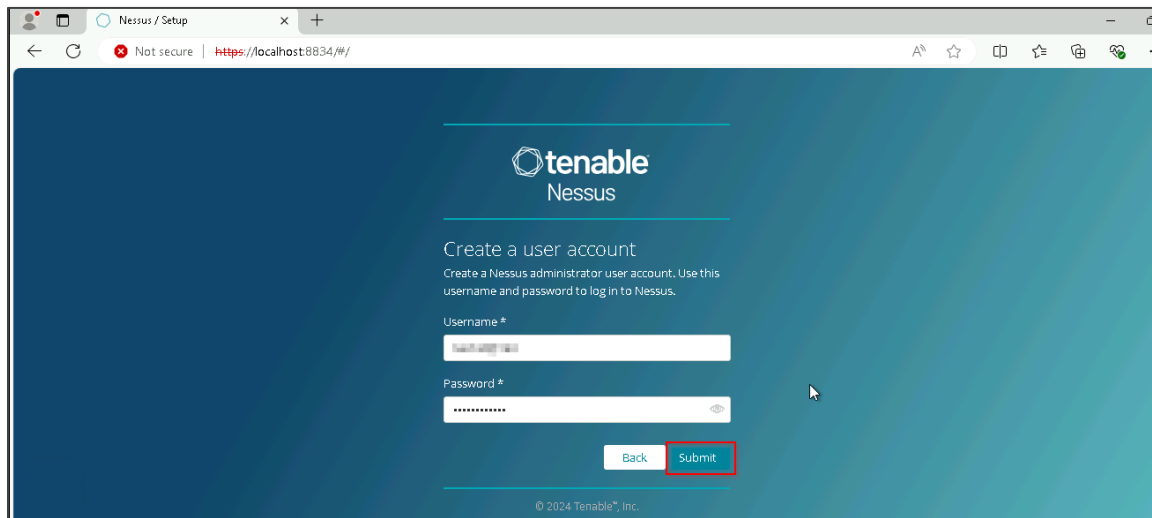
Activation Code: G856-HX62-PABQ-NSUJ

Valid until: 2024-07-31

[Continue](#)

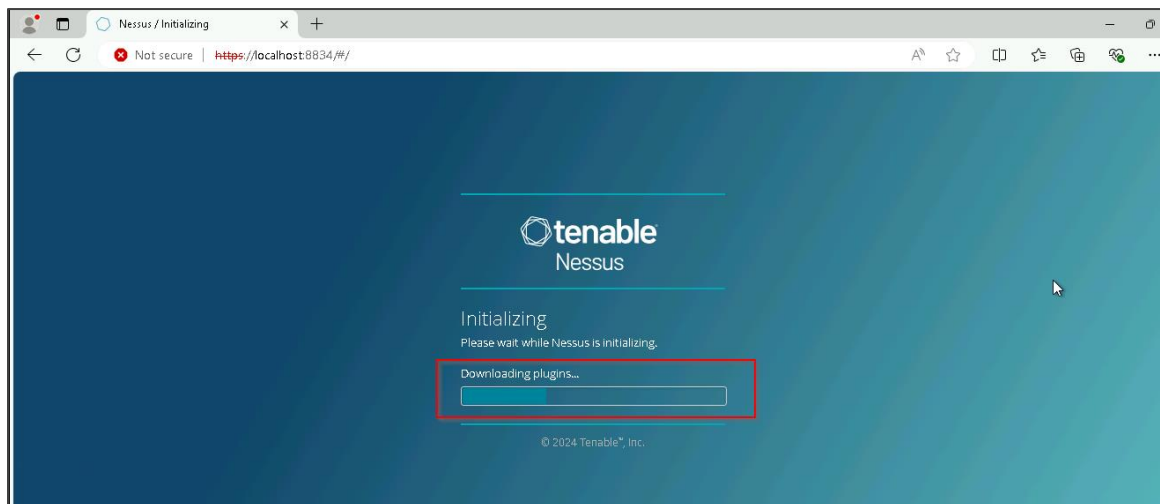
© 2024 Tenable®, Inc.

2.9 Provide the desired **Username** and **Password** and click on **Submit**



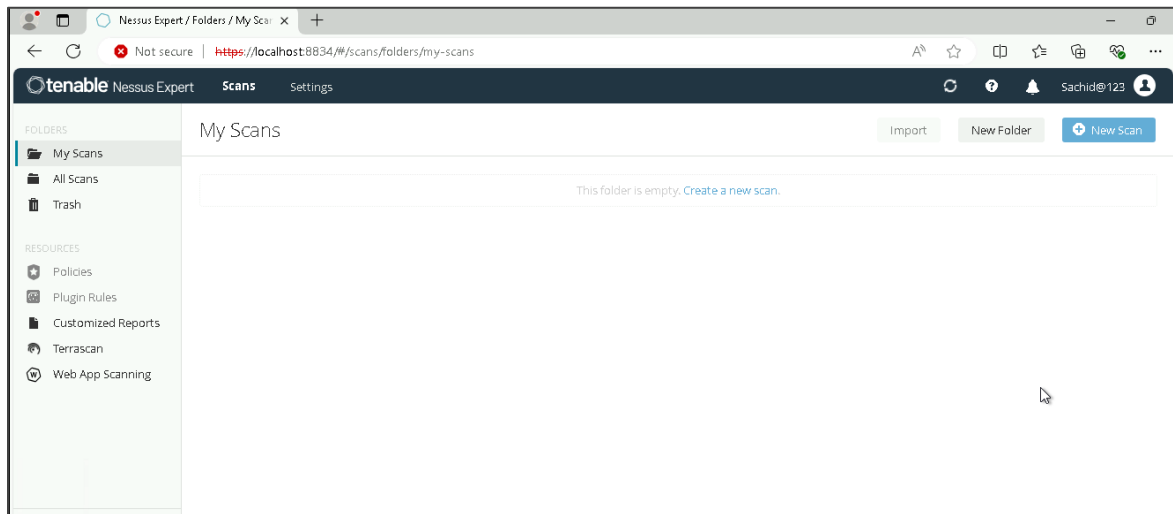
The screenshot shows the Nessus Setup page in a web browser. The page has a dark blue background with the Tenable Nessus logo at the top. Below the logo, it says "Create a user account" and "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are two input fields: "Username \*" and "Password \*". The "Submit" button is highlighted with a red box. The browser address bar shows "https://localhost:8834/#/" and the page is marked as "Not secure".

The Nessus plugins will start downloading as shown below:



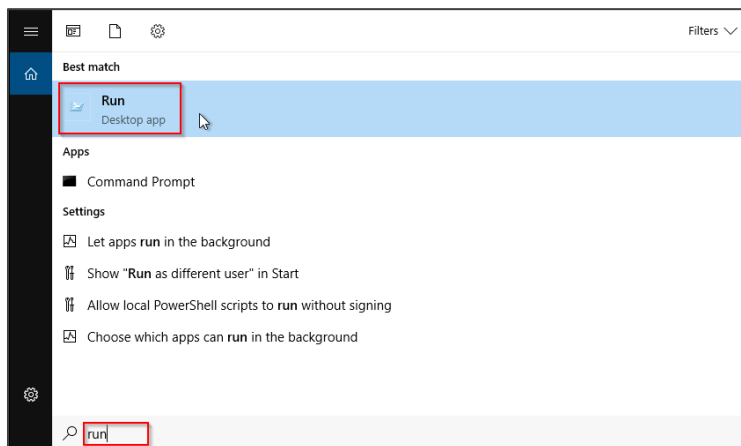
**Note:** Once the Nessus plugins are downloaded, they will be automatically installed without any prompt. Typically, it will take 30 to 60 minutes to complete the installation process.

Upon completion, the Nessus Homepage page will open as shown below:

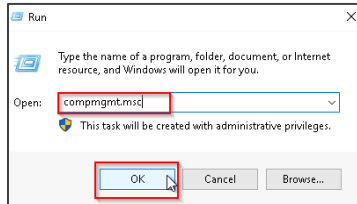


## Step 3: Prepare for scanning

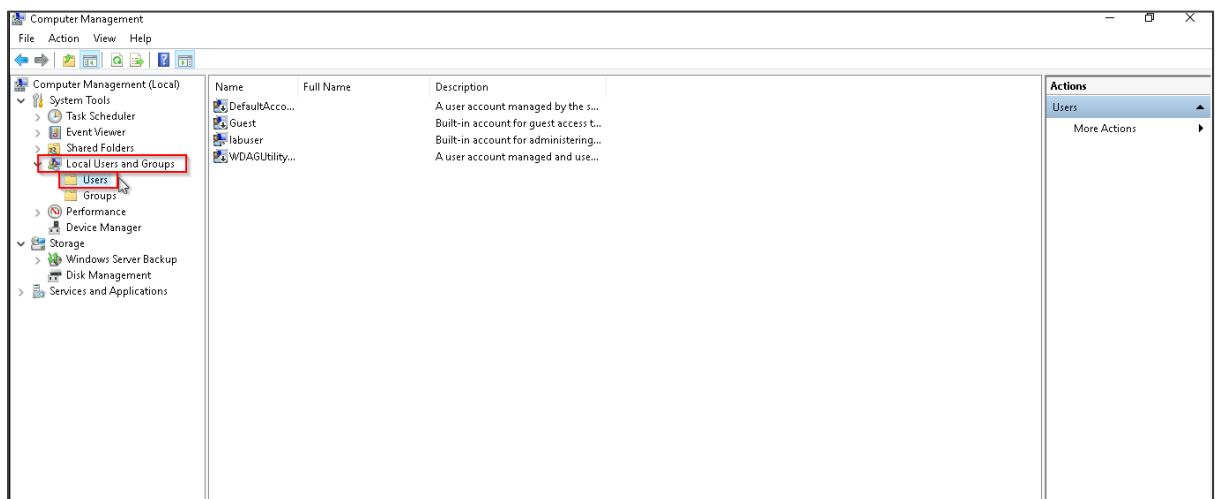
3.1 Search for **run** in Windows search and click on the **Run** icon



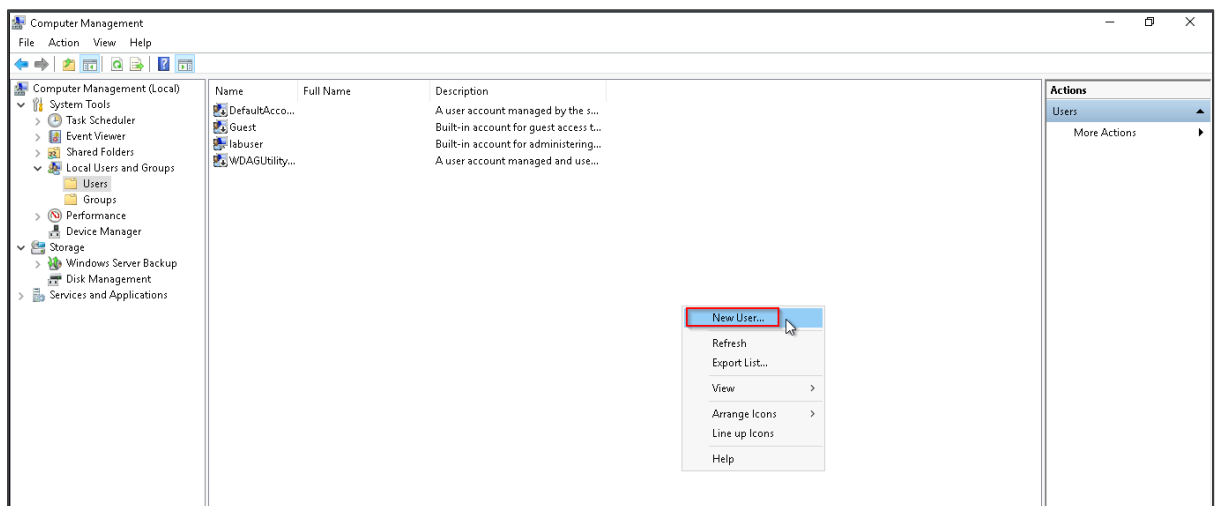
### 3.2 Run the command given below to open the **Computer Management:** **compmgmt.msc**



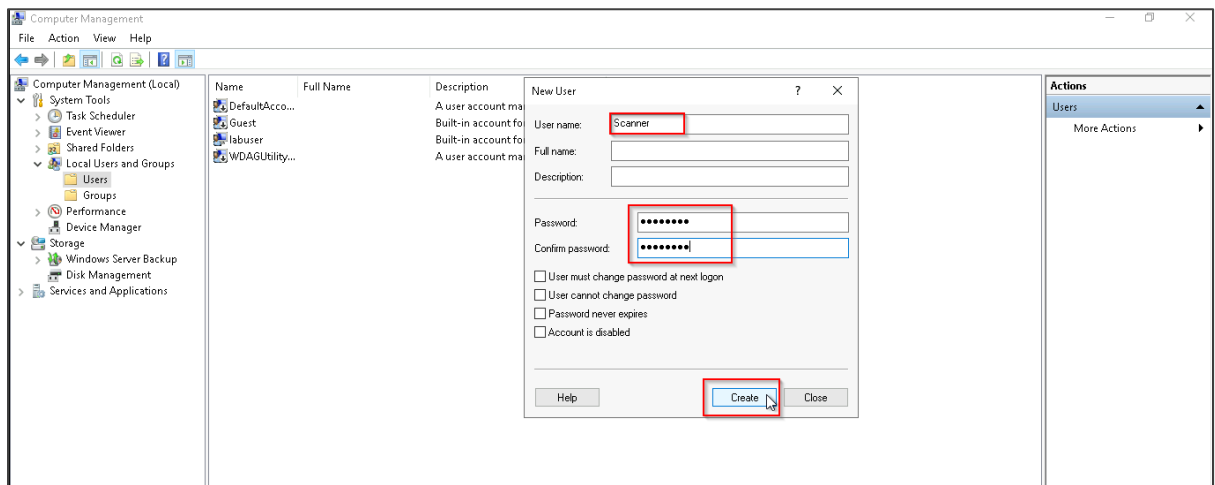
### 3.3 Navigate to **Local Users and Groups** in the left navigation pane and then select **Users**



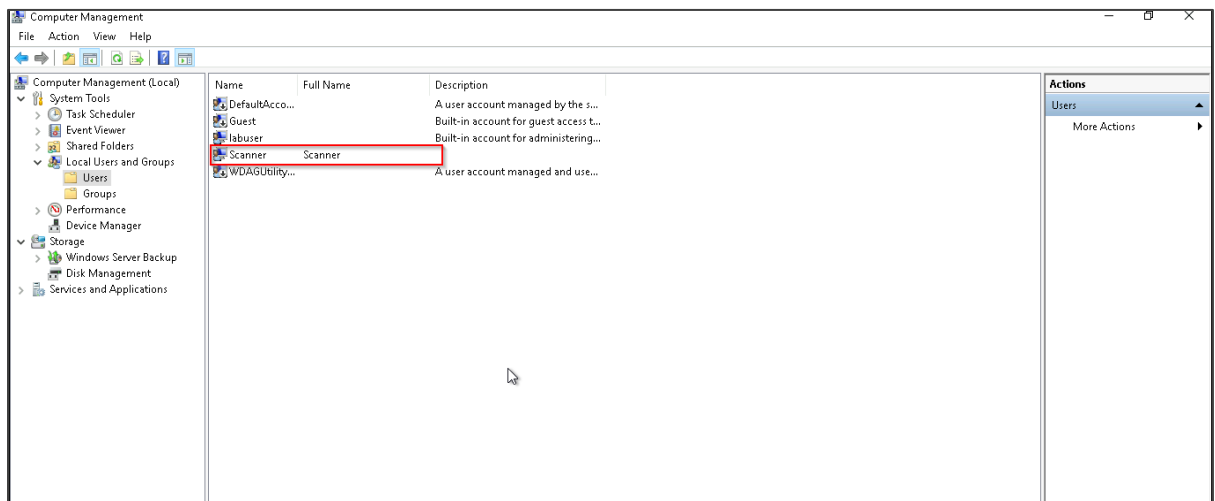
### 3.4 Right-click and select the **New User** option



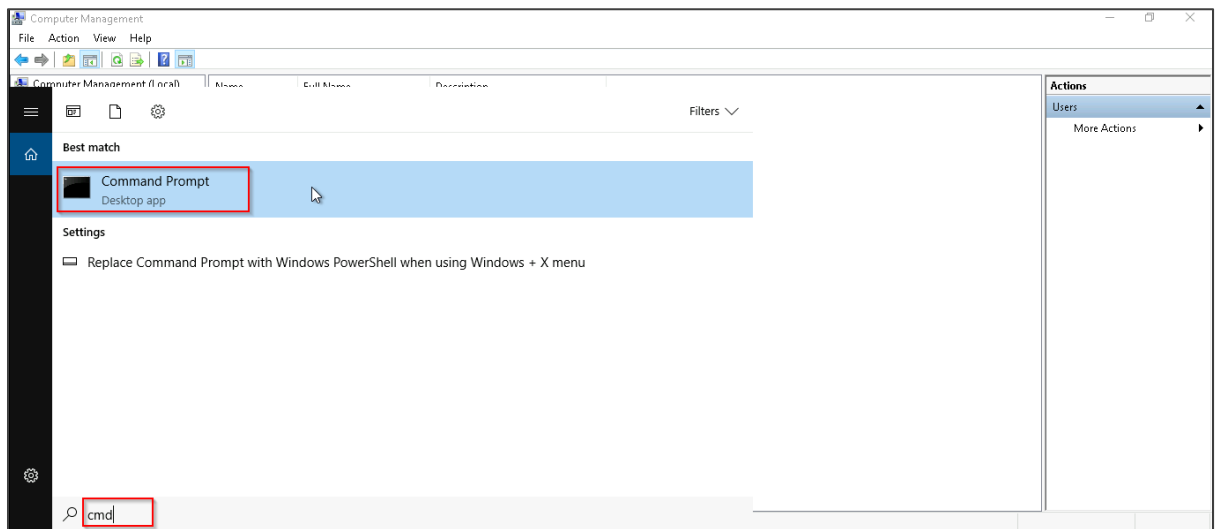
### 3.5 Enter the **User name** as **Scanner** and the **Password** as **Pa\$\$w0rd**, and click on **Create**



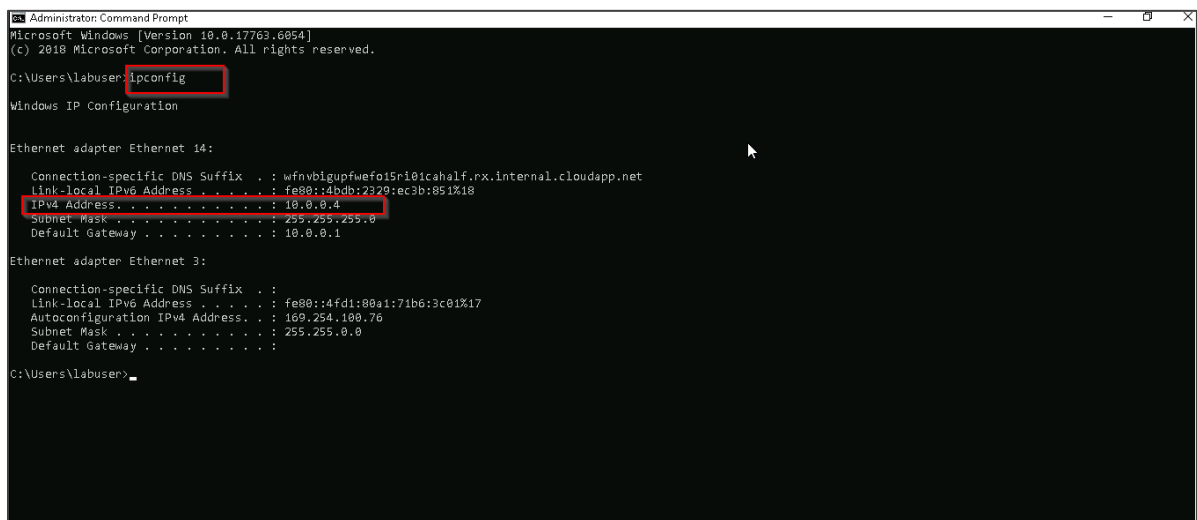
The new user named **Scanner** is created successfully, as shown below:



### 3.6 Enter **cmd** in the Windows search to open the **Command Prompt**



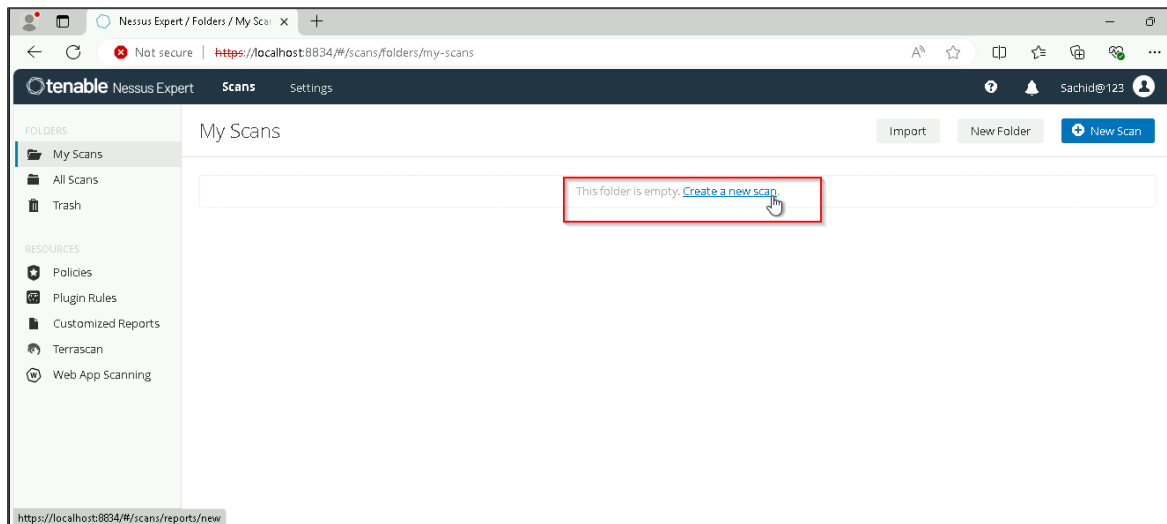
### 3.7 Enter the command given below to get the information on the IP of the current system: **ipconfig**



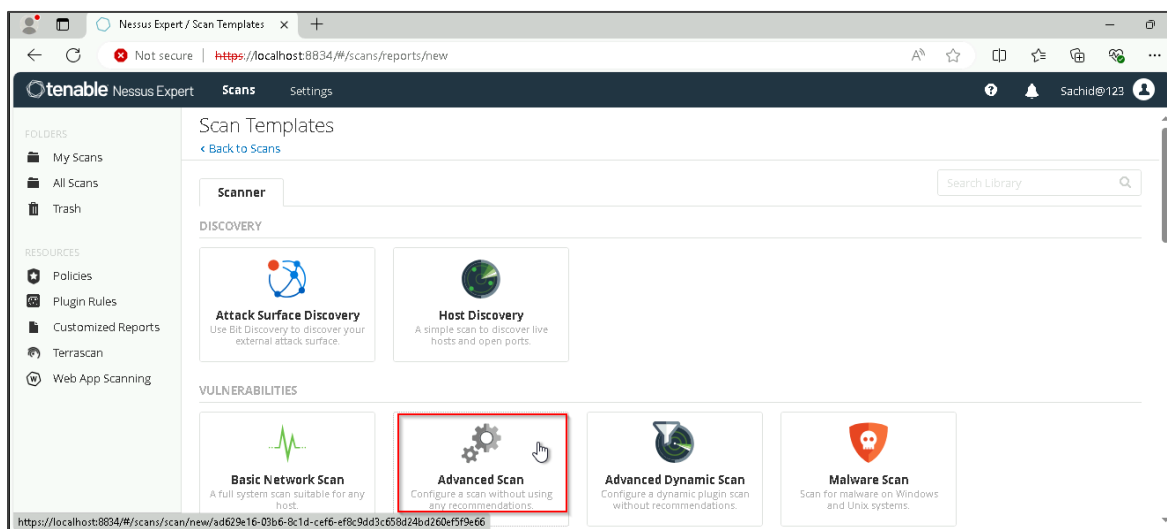
The IP of the current system is **10.0.0.4**.

## Step 4: Conduct a vulnerability scan

### 4.1 Navigate back to the browser page where the Nessus portal was opened and click on **Create a new scan**



### 4.2 Click on the **Advanced Scan** tab

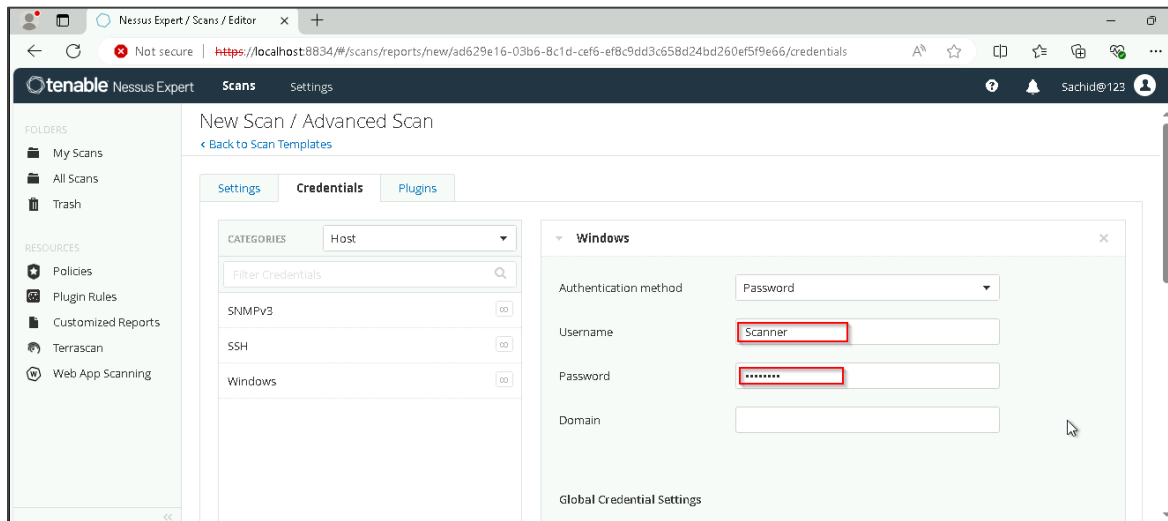




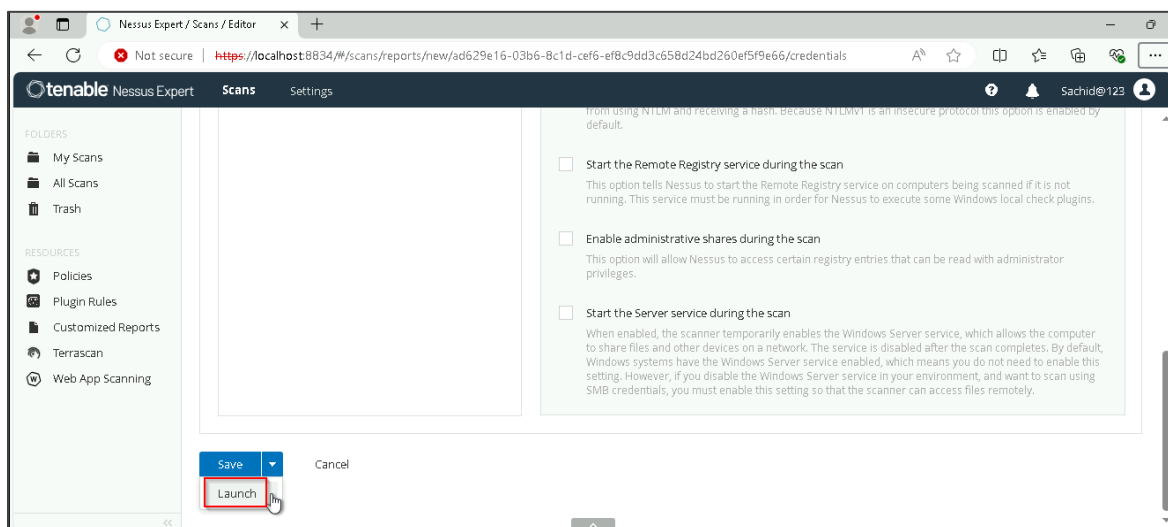
The New Scan page appears as shown below:

4.3 In **Name**, enter **windows\_scan**, give the **Description** as **Scanning user Scanner**, and in the **Targets** field, use the IP of the Windows machine as obtained in step 3.7

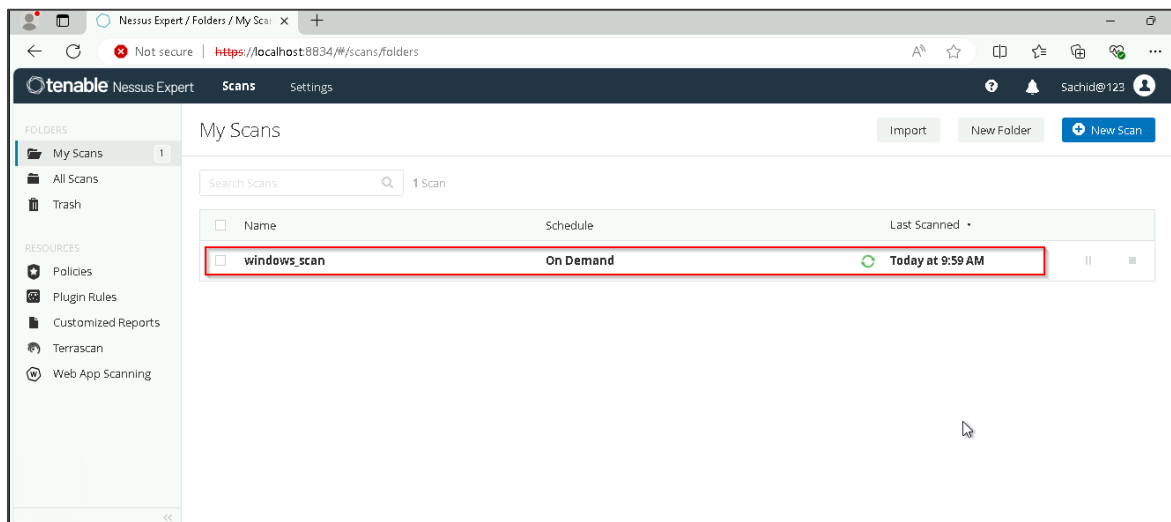
#### 4.4 Navigate to the **Credentials** tab and enter the **Username** as **Scanner** and the **Password** as **Pa\$\$w0rd**



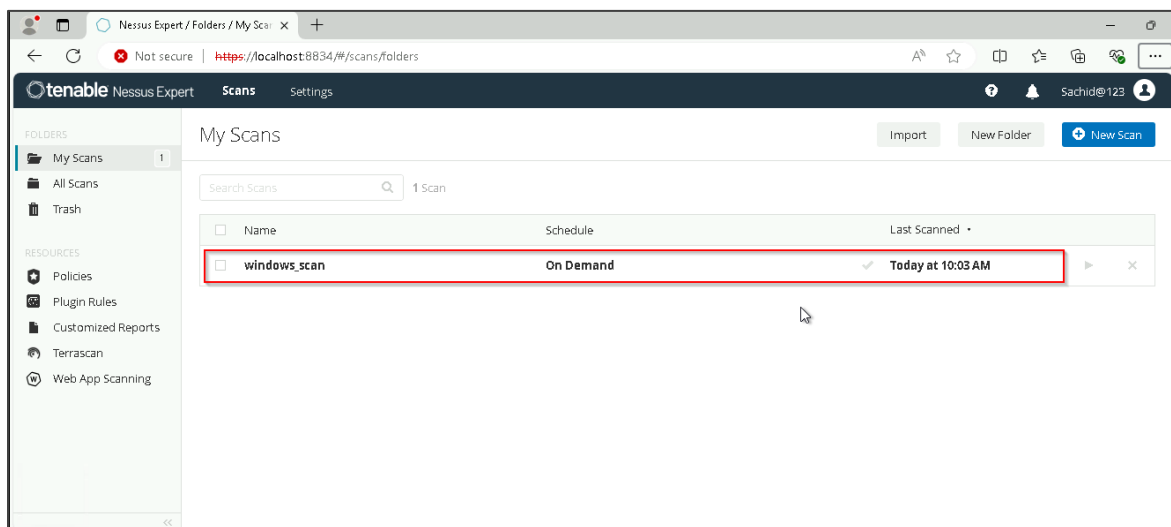
#### 4.5 Scroll down and click on the **Launch** button



The Nessus will start the scanning process as shown below:

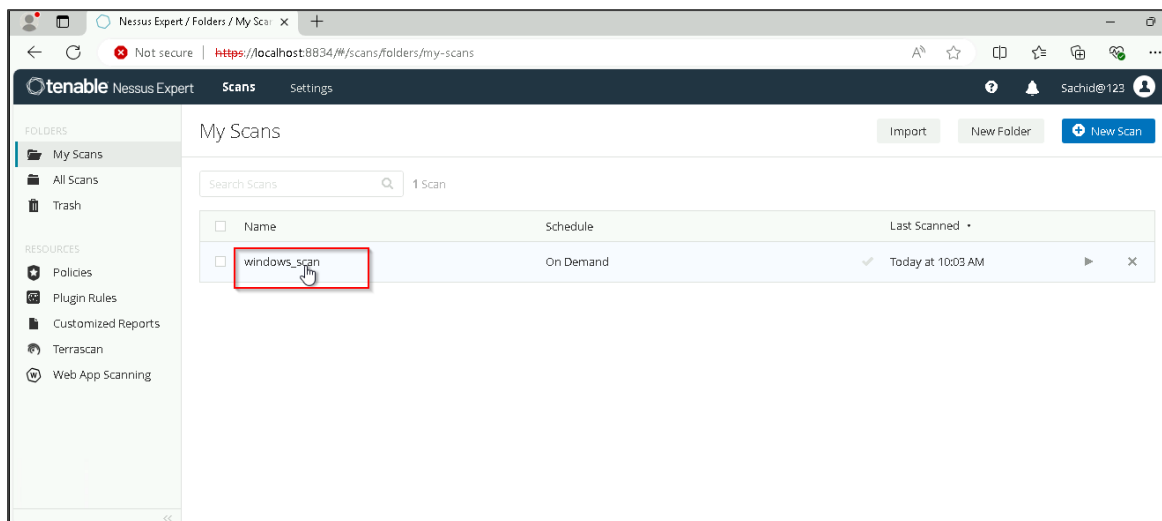


Once the scanning is done, the completion mark will appear as shown below:

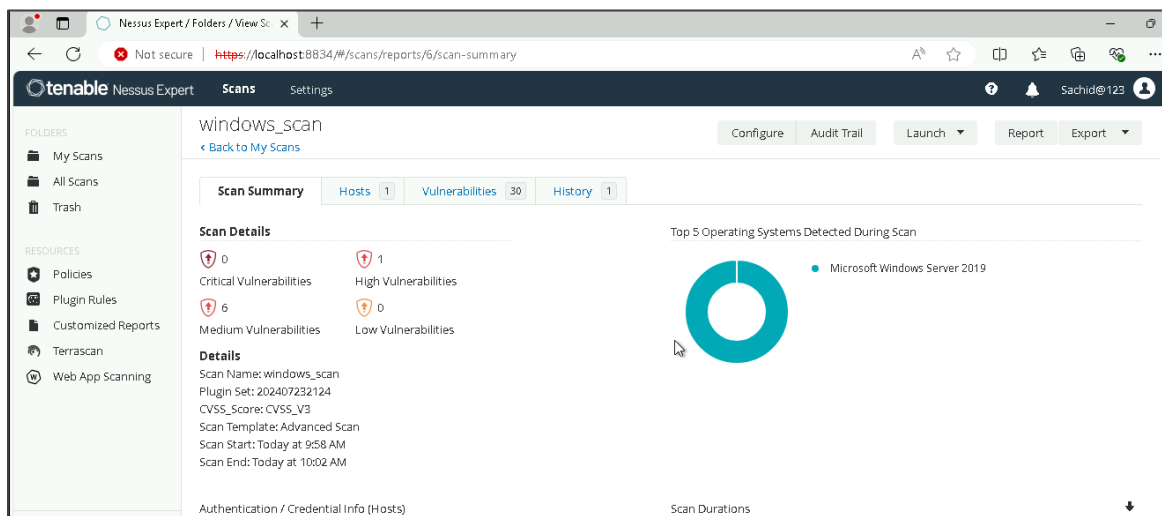


## Step 5: Review scan results

### 5.1 Click on the **windows\_scan** to see the scan summary



The scan summary for the **windows\_scan** is available as shown below:



## 5.2 Click on the **Hosts** tab to view the hosts

The screenshot shows the Tenable Nessus Expert interface. The left sidebar contains a 'FOLDERS' section with 'My Scans', 'All Scans', and 'Trash', and a 'RESOURCES' section with 'Policies', 'Plugin Rules', 'Customized Reports', 'TerraScan', and 'Web App Scanning'. The main content area is titled 'windows\_scan' and includes a 'Back to My Scans' link. Below this, there are tabs for 'Scan Summary', 'Hosts', 'Vulnerabilities', and 'History'. The 'Hosts' tab is selected and highlighted with a red box. It shows a search bar with '1 Host' and a table with one entry: '10.0.0.4' with a vulnerability count of 91. To the right, the 'Scan Details' section shows: Policy: Advanced Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 9:58 AM, End: Today at 10:02 AM, and Elapsed: 5 minutes. At the bottom right, there is a 'Vulnerabilities' section with a donut chart and a legend for Critical, High, Medium, Low, and Info.

## 5.3 Click on the **Vulnerabilities** tab to view the vulnerabilities

The screenshot shows the Tenable Nessus Expert interface with the 'Vulnerabilities' tab selected and highlighted with a red box. The main content area displays a table of vulnerabilities. The table has columns for 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. The vulnerabilities listed are: 'SSL (Multiple Issues)' (11), 'SMB Signing not required' (1), 'TLS (Multiple Issues)' (6), 'SMB (Multiple Issues)' (12), 'HTTP (Multiple Issues)' (6), 'Microsoft Windows (Multiple Issues)' (4), 'TLS (Multiple Issues)' (3), 'Netstat Portscanner (SSH)' (22), and 'DCE Services Enumeration' (9). To the right, the 'Scan Details' section is repeated. At the bottom right, the 'Vulnerabilities' section shows a donut chart and a legend for Critical, High, Medium, Low, and Info.

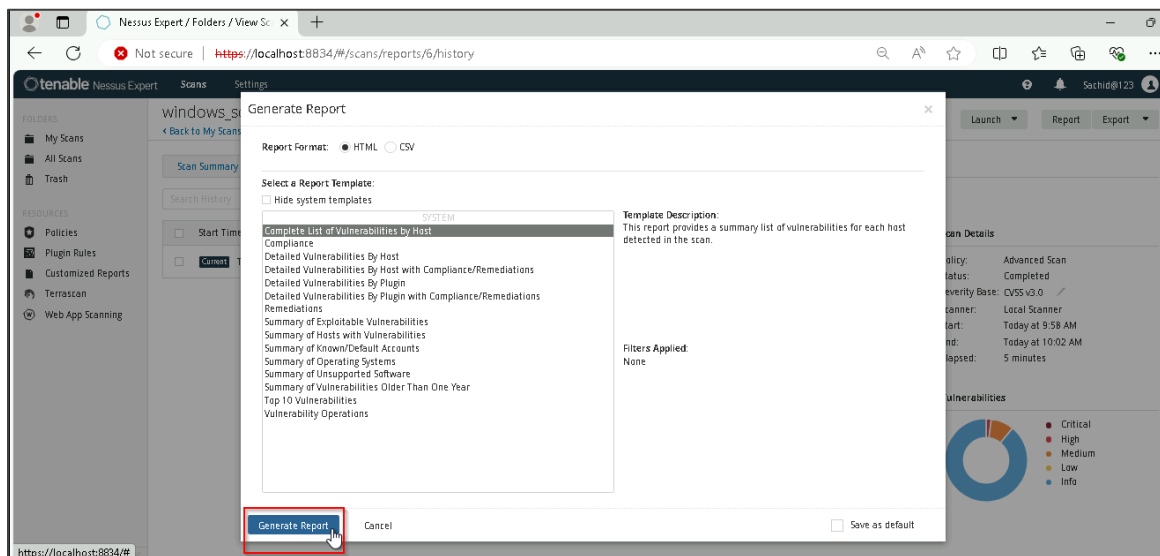
## 5.4 Further, click on the **History** tab to view the history

The screenshot shows the Tenable Nessus Expert interface. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Terrascan, Web App Scanning). The main content area is titled 'windows\_scan' and has tabs for 'Scan Summary', 'Hosts', 'Vulnerabilities', and 'History'. The 'History' tab is selected and highlighted with a red box. Below the tabs is a search bar and a table with columns: Start Time, Last Scanned, and Status. The table shows one entry: 'Current' at 'Today at 9:58 AM' with a status of 'Completed' at 'Today at 10:03 AM'. To the right, 'Scan Details' are shown: Policy: Advanced Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 9:58 AM, End: Today at 10:02 AM, Elapsed: 5 minutes. Below this is a 'Vulnerabilities' donut chart with a legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

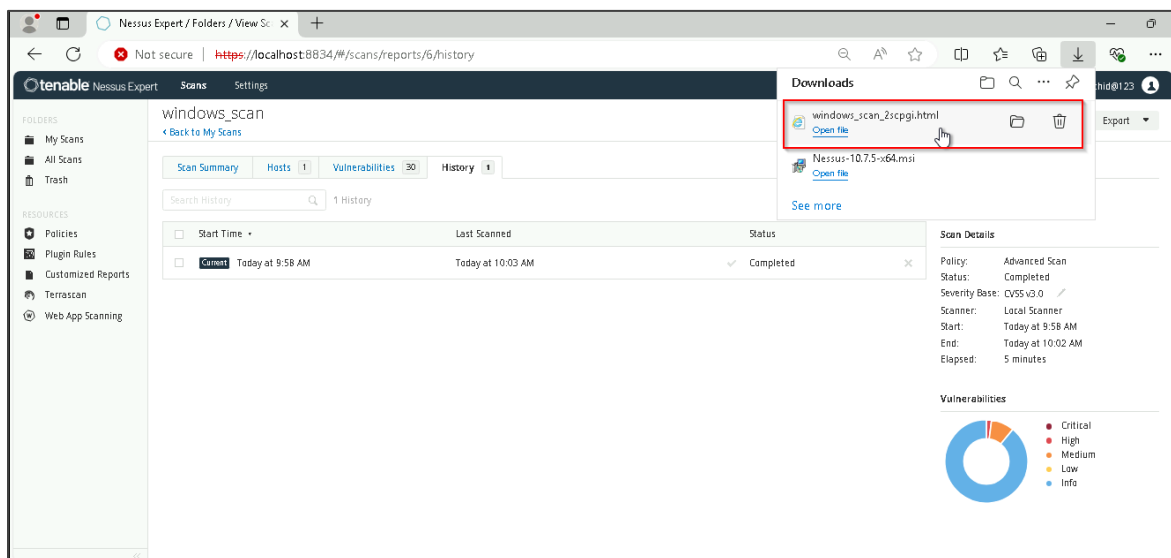
## 5.5 Click on the **Report** tab to view the overall report

The screenshot shows the Tenable Nessus Expert interface, similar to the previous one, but with the 'Report' tab selected and highlighted with a red box. The 'Report' tab is located in the top right corner of the main content area, next to 'Launch', 'Export', and 'Configure'. The rest of the interface, including the sidebar, 'History' tab, table, and 'Scan Details', remains the same as in the previous screenshot.

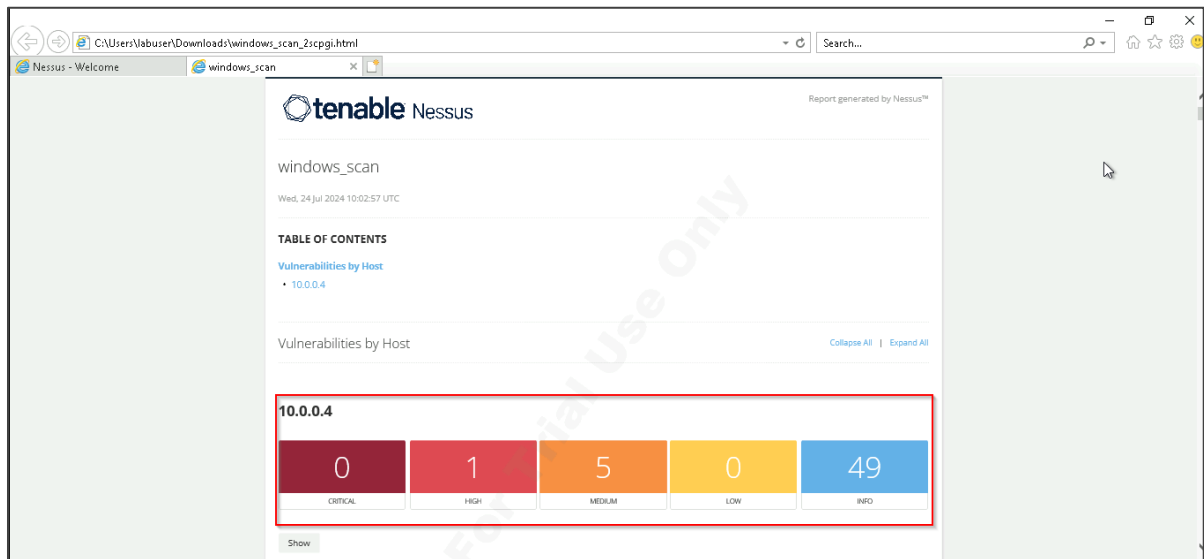
## 5.6 Click on **Generate Report** to get the report in downloadable format



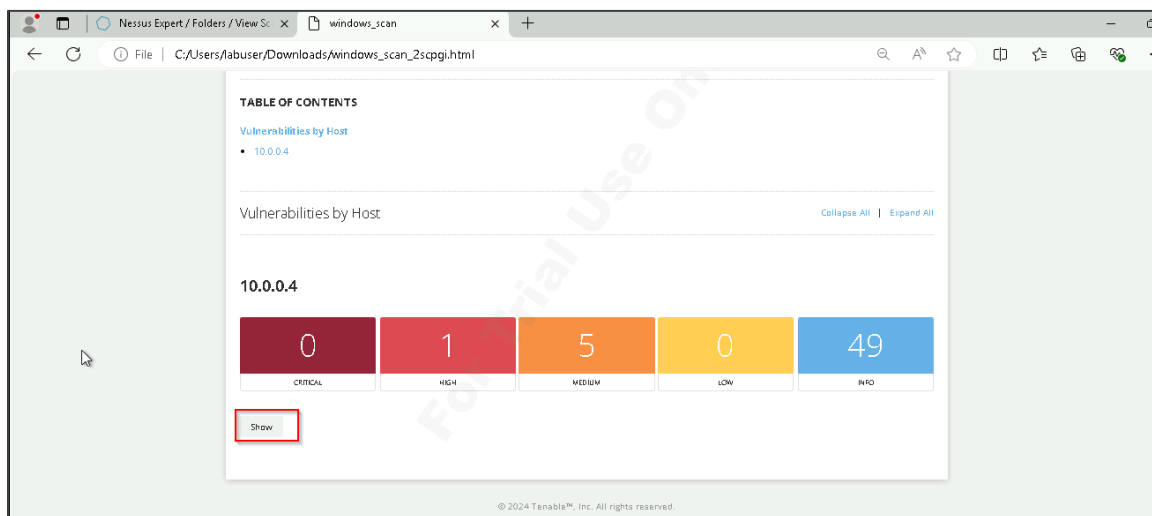
## 5.7 Open the downloaded Nessus scan report



The generated report opens as shown below:



5.8 Click on the **Show** tab to open the report on each plugin





## 5.9 Click on any of the plugins to see the solution

Severity	CVSS v3.0	VPR Score	Plugin	Name
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	34097	BIOS Info (SMB)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type

A new page will open with details on the report synopsis, description, and suggested solution, which can be implemented as shown below:

[Nessus Families](#)  
[WAS Families](#)  
[NNM Families](#)  
[LCE Families](#)  
[Tenable OT Security Families](#)  
[About Plugin Families](#)  
[Audits](#)  
[Policies](#)  
[Indicators](#)  
**ANALYTICS**  
[CVEs](#)  
[Attack Path Techniques](#)

### Synopsis

The remote service supports the use of medium strength SSL ciphers.

### Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

### Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

### See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>  
<https://sweet32.info>

### Plugin Details

**Severity:** High  
**ID:** 42873  
**File Name:** ssl\_medium\_supported\_ciphers.nasl  
**Version:** 1.21  
**Type:** remote  
**Family:** General  
**Published:** 11/23/2009  
**Updated:** 2/3/2021  
**Supported Sensors:** Nessus

### Risk Information

**VPR**  
**Risk Factor:** Medium

Following the above steps, you have successfully conducted vulnerability scans on a local virtual machine using Nessus, installed and configured Nessus, scanned the target machine, and generated a report to visualize identified vulnerabilities and necessary patches.