VULNERABILITY SCANNING

By

DEWTON KIPROP

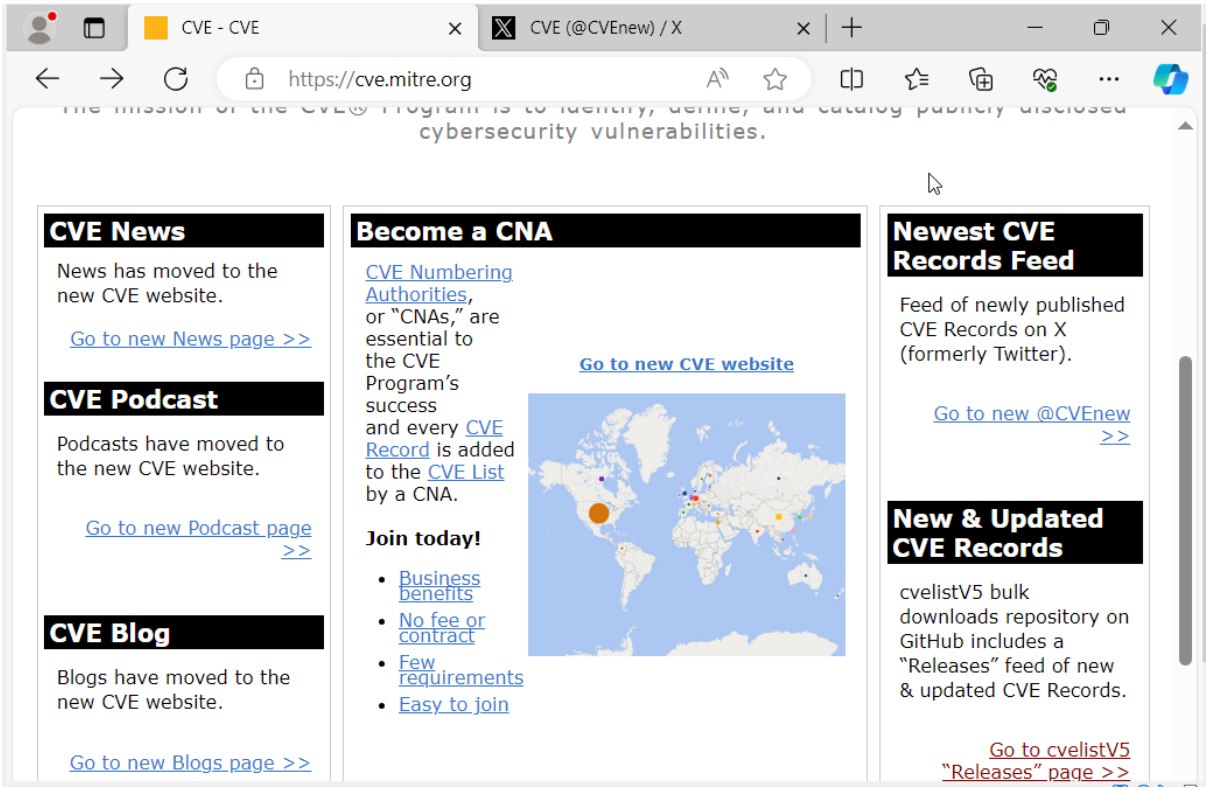
JJJJ

LAB 1

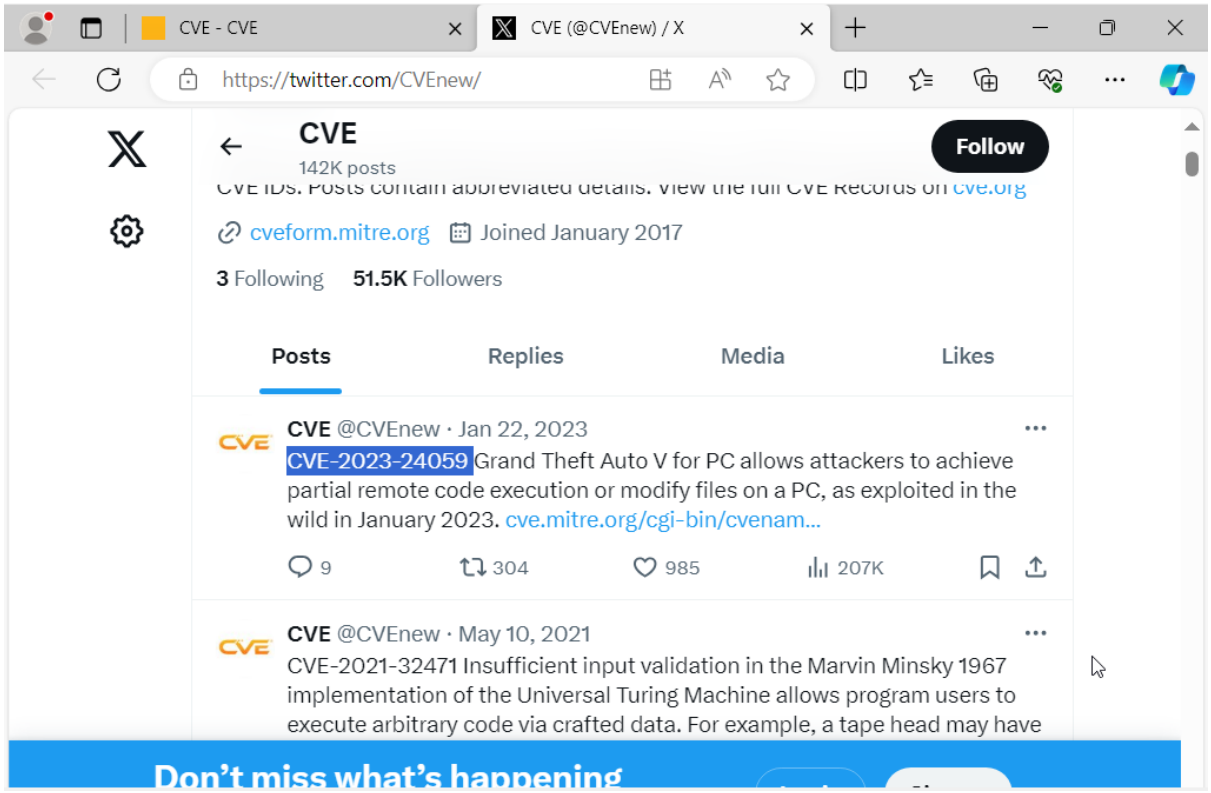
TASK:

PERFORM VULNERABILITY RESEARCH IN COMMON VULNERABILITIES AND EXPOSURES.

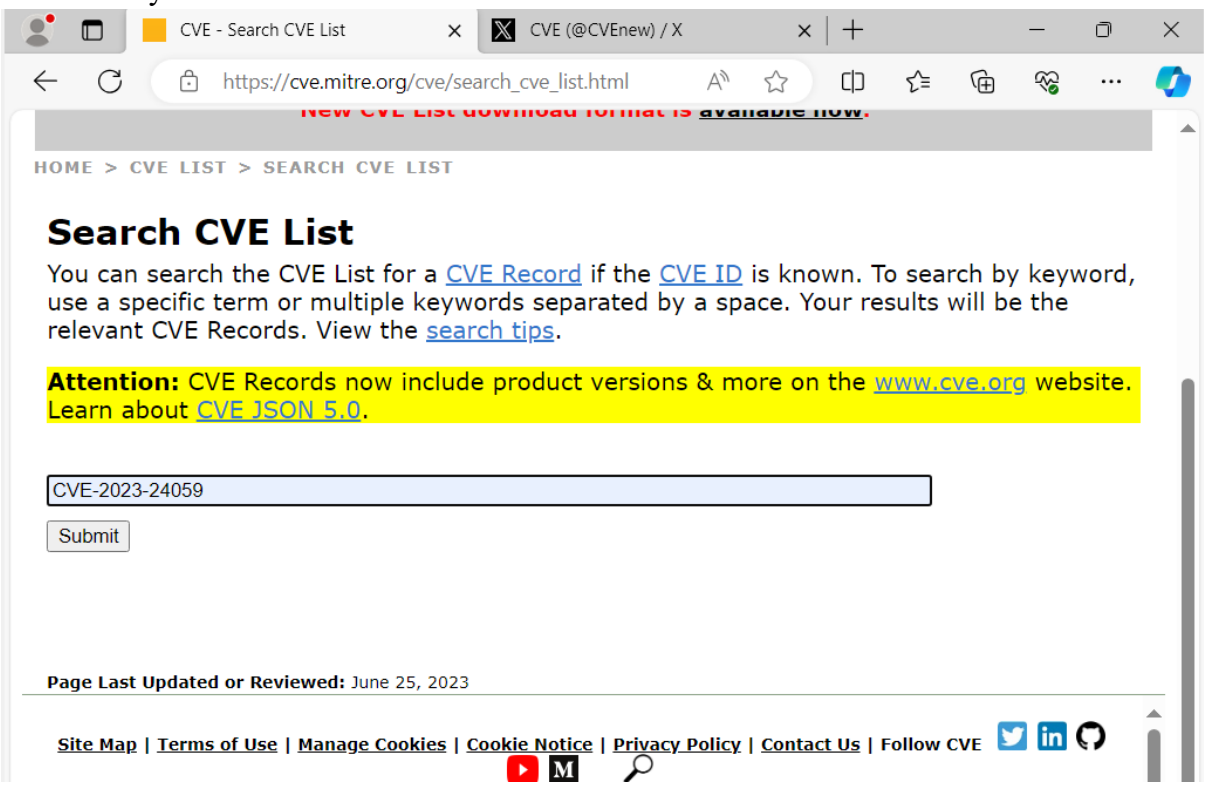
- With your windows 10 machine open, navigate to https://cve.miter.org/. using your browser.
- In your https://cve.miter.org/. web page, navigate to the Newest CVE Records feeds, click on link GO to new@CVE link
-



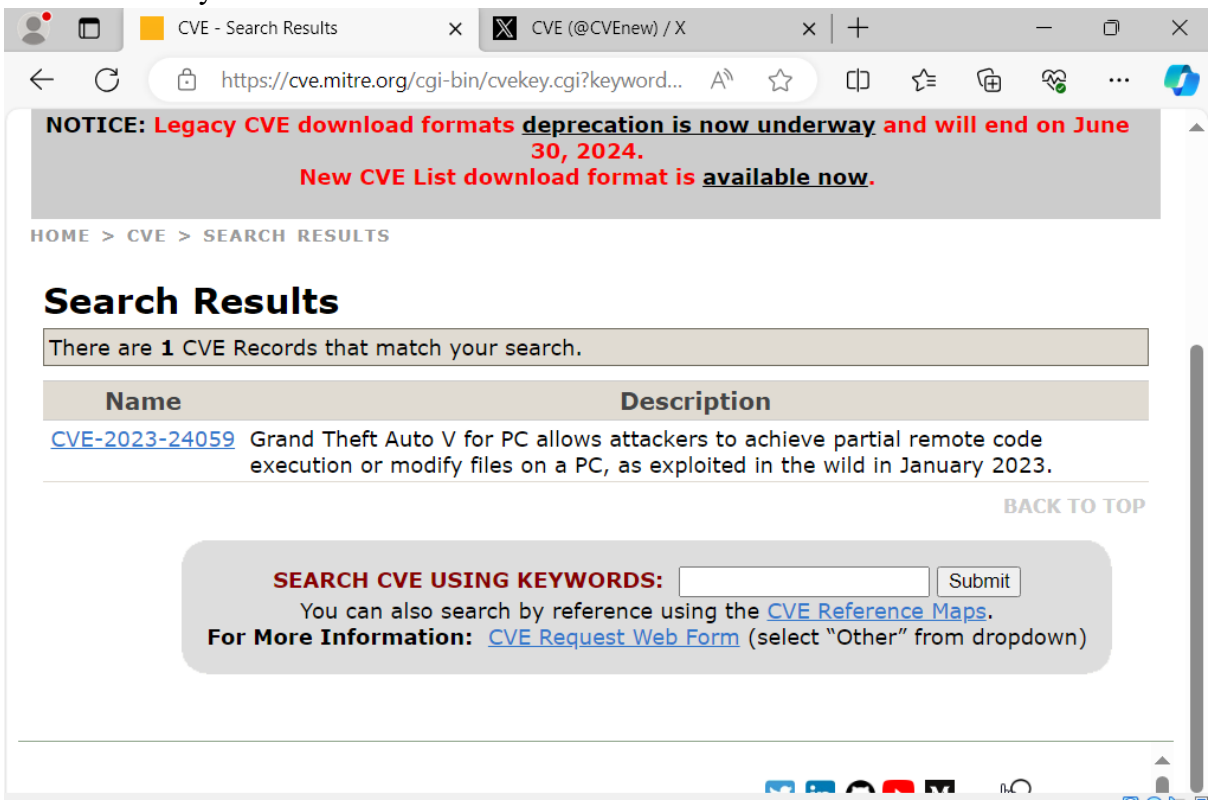
- Copy any vulnerability under the Newest CVE Records feeds

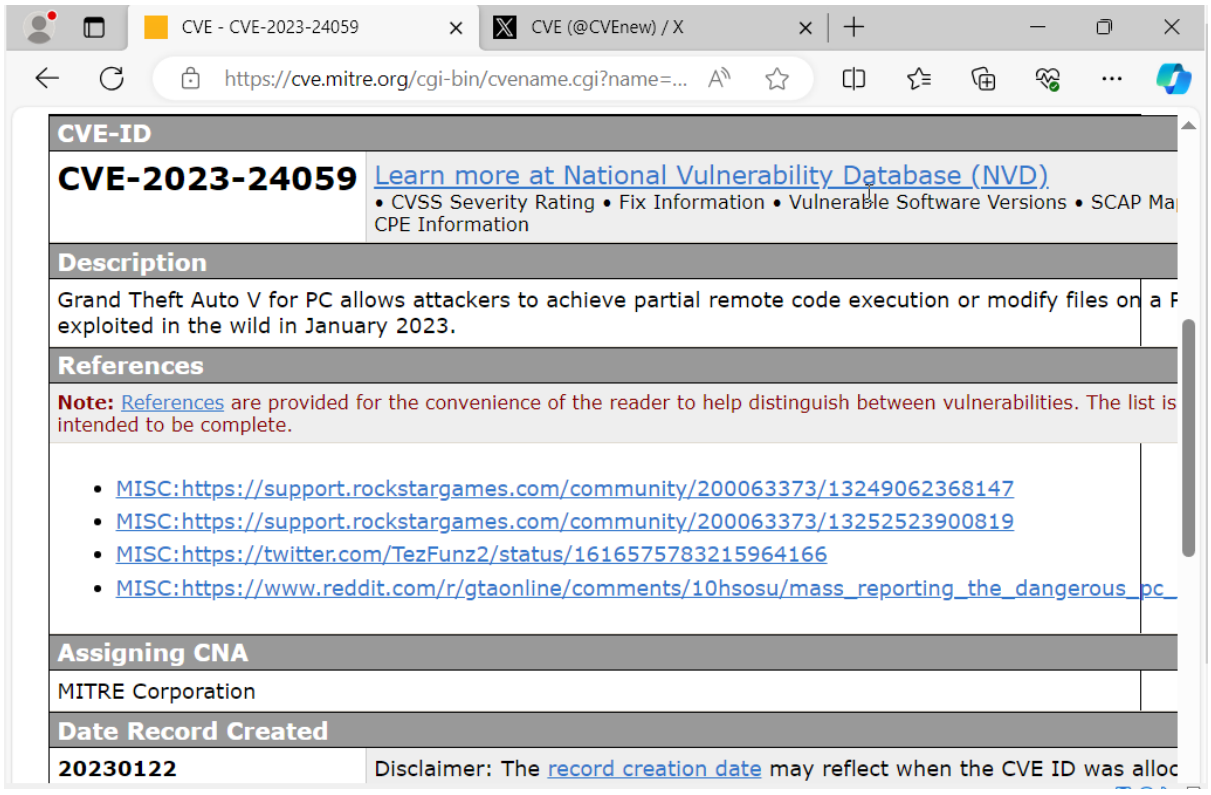


- In this case CVE-2023_24059, click on Search CVE list tab. And search your vulnerability there.

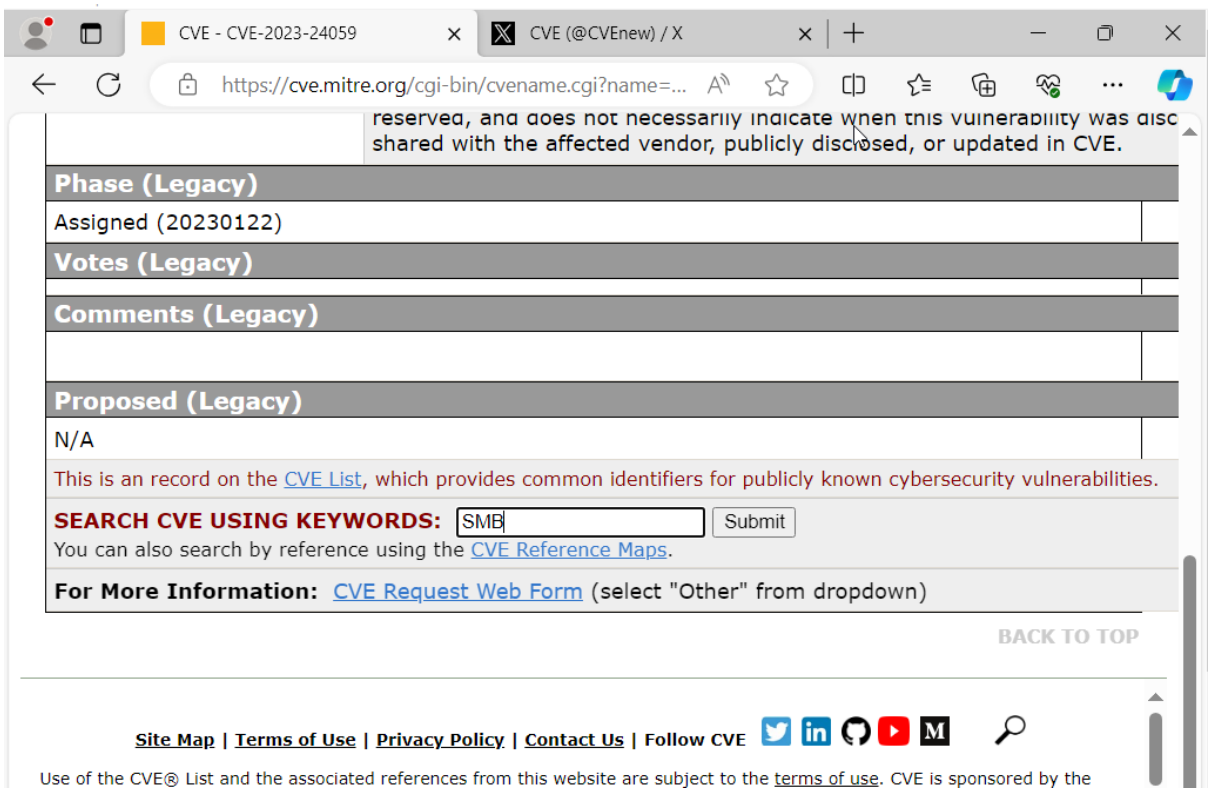


- After, submitting the vulnerability, search result page appears, displaying results of the searched vulnerability. You can click the vulnerability to view further details regarding the vulnerability.

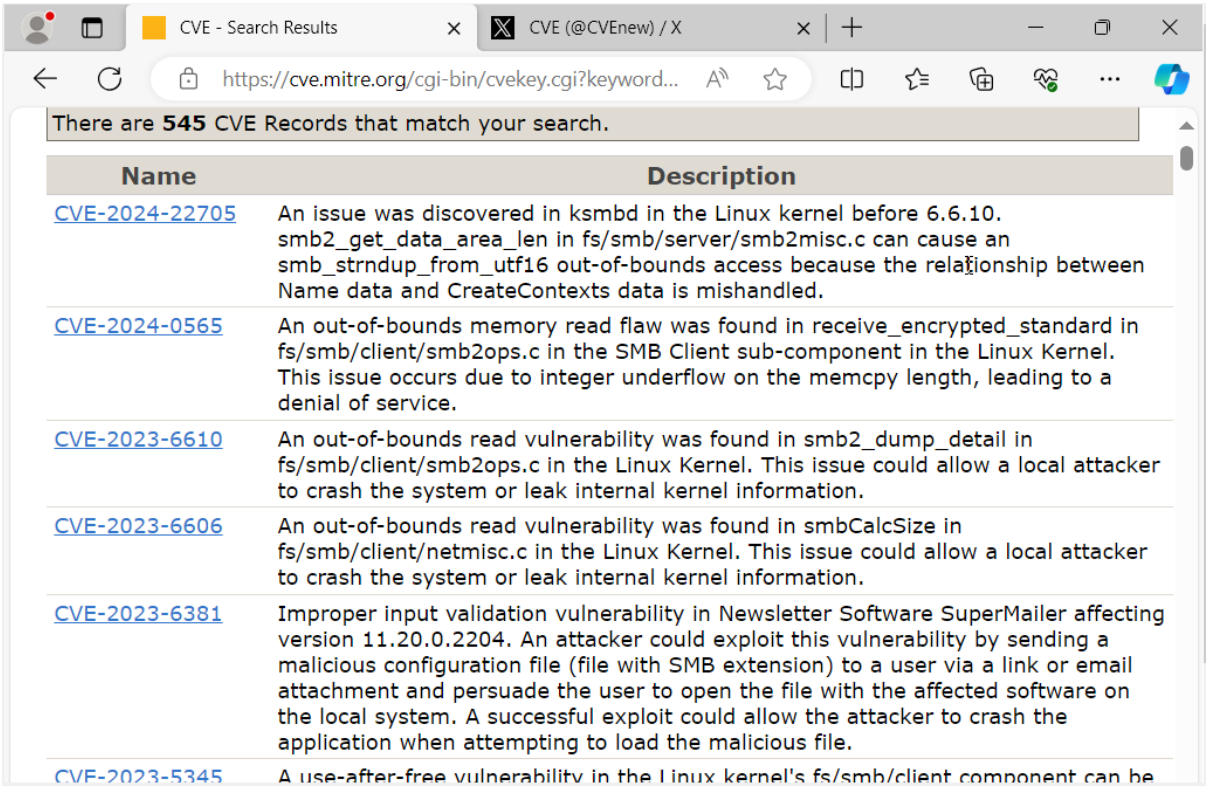




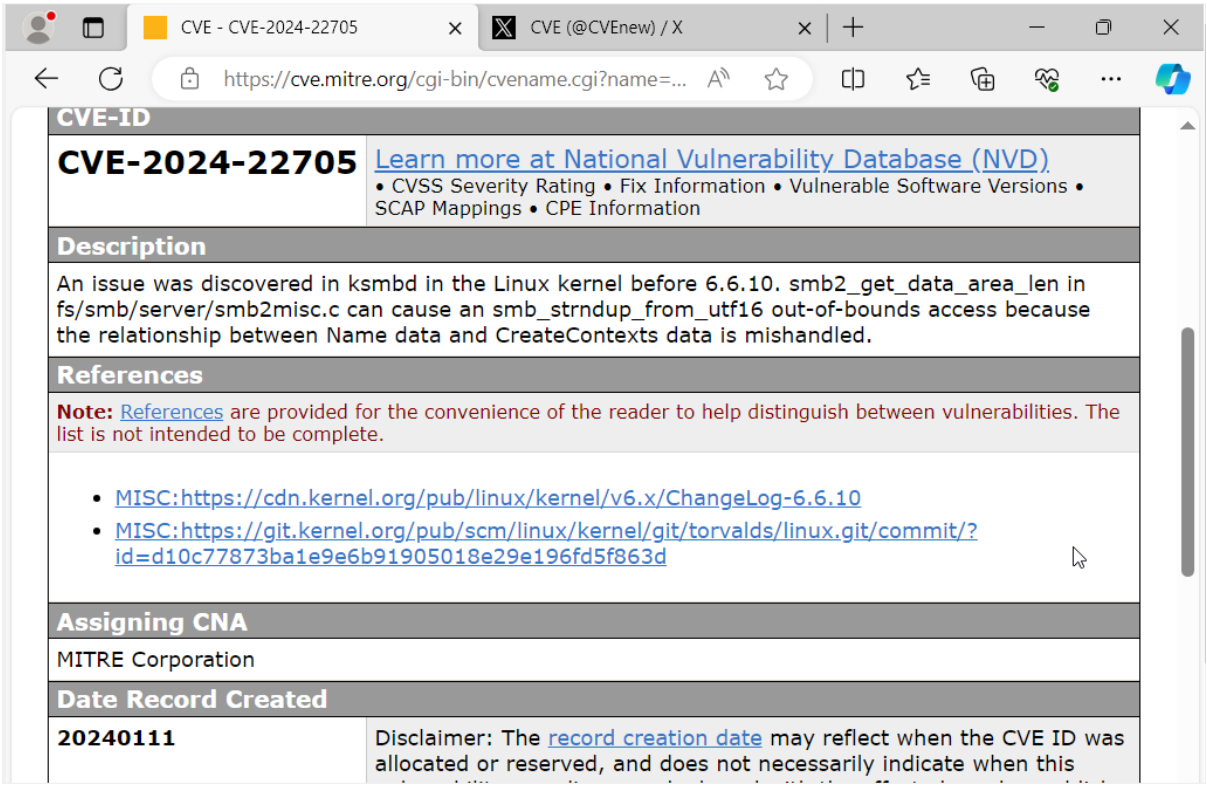
- similarly, in the search CVE section, you can search for a service-related vulnerability by typing the service name. in this case (SMB) and click submit.



- search result page appears displaying a list of vulnerabilities in the target service (SMB) along with their description as shown



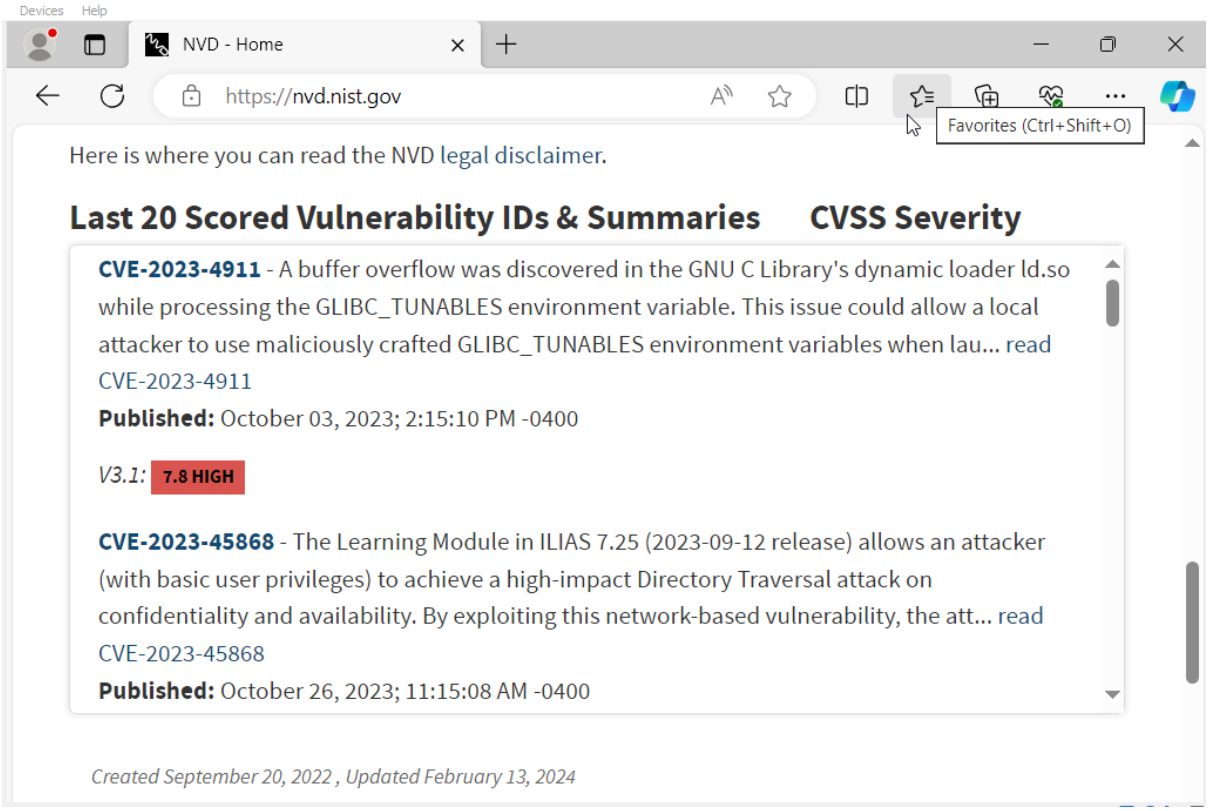
- Further you can click on the CVE id of any vulnerability to view its details information, here we click on the first id link
- Detailed information regarding the vulnerability is displayed. You can click on links under the references section to view more information on the vulnerability.



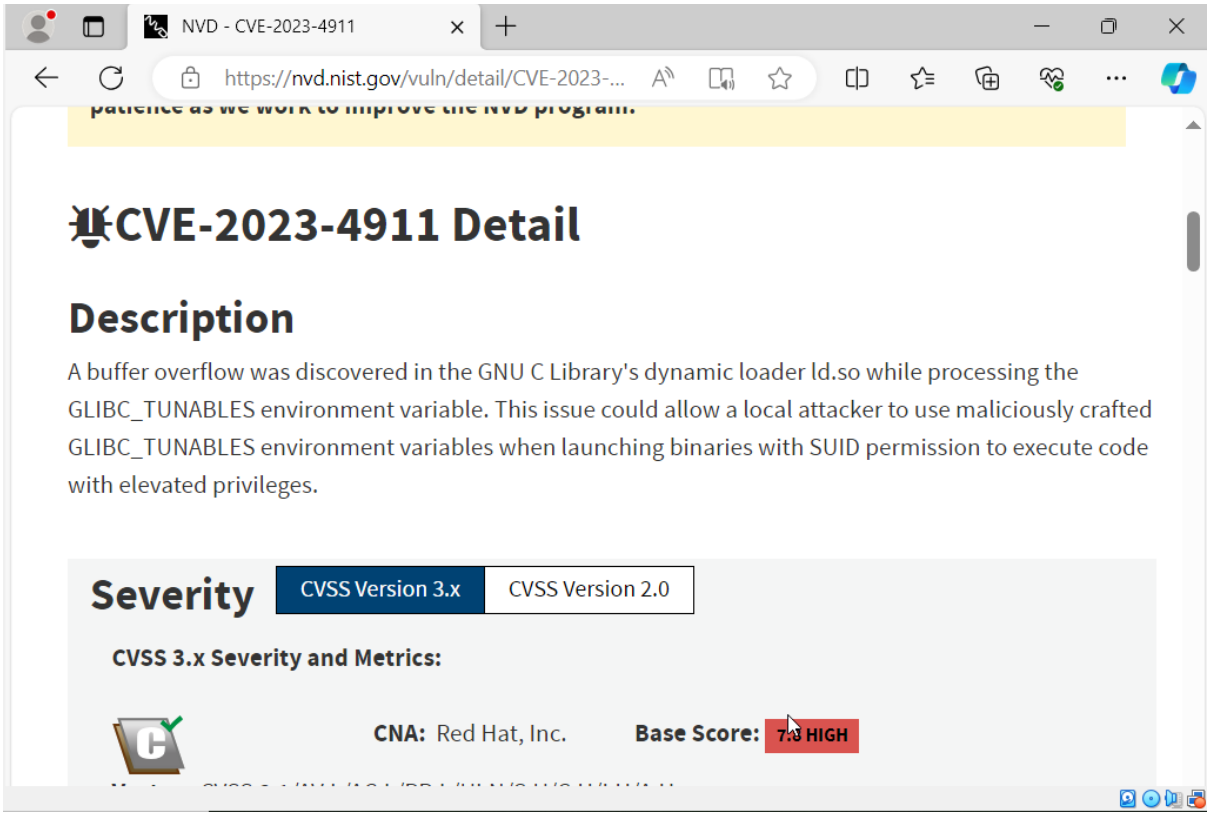
Task :

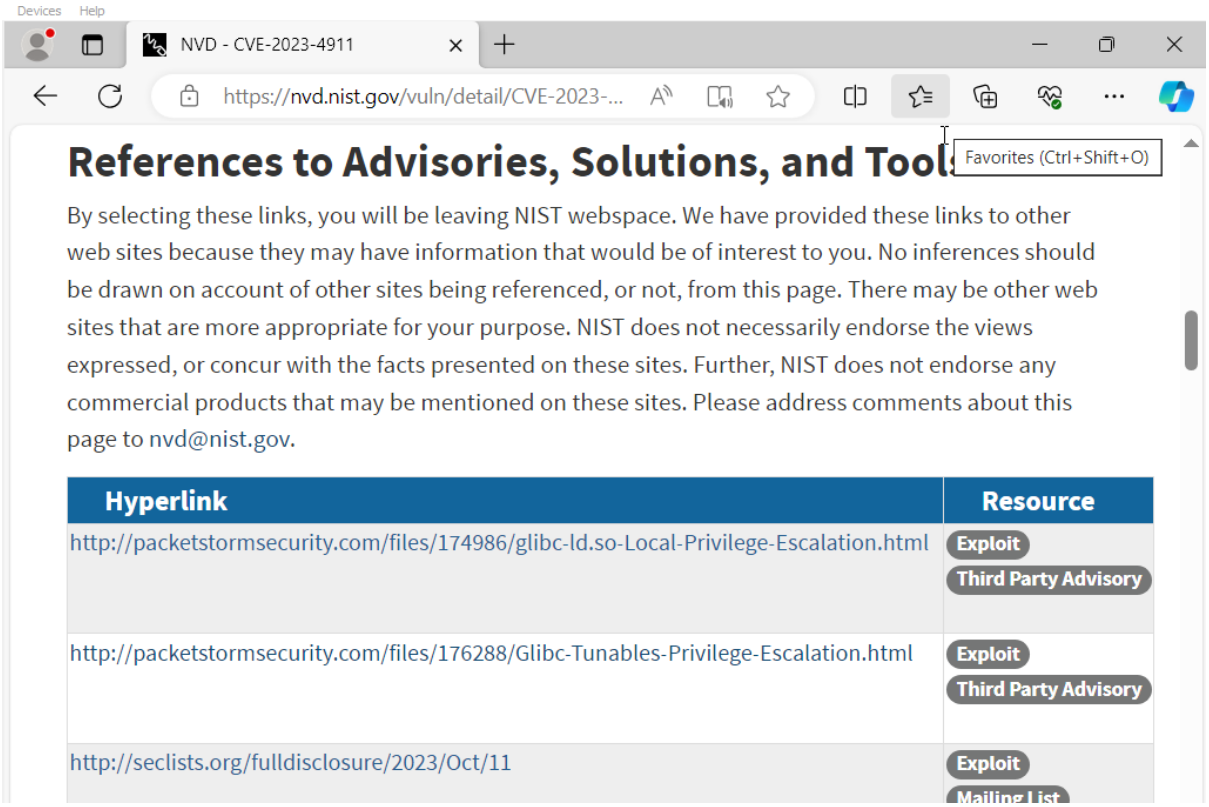
PERFORM VULNERABILITY RESEARCH IN National Vulnerability Databases. (NVD)

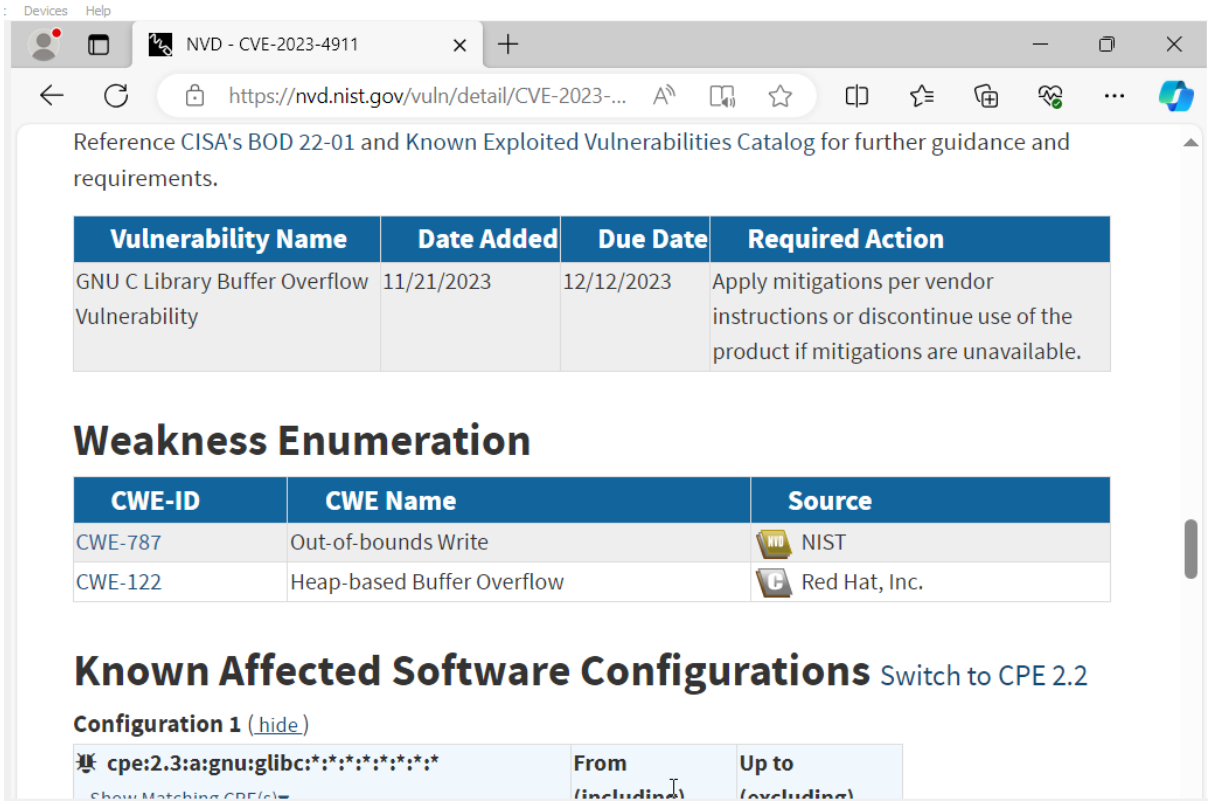
- In Windows 10, open your browser and search https//nvd.nist.gov/. when the web page appears, the recent vulnerability can be viewed
- You can click on CVE -ID (CVE-2023-4911) link to view detailed information.



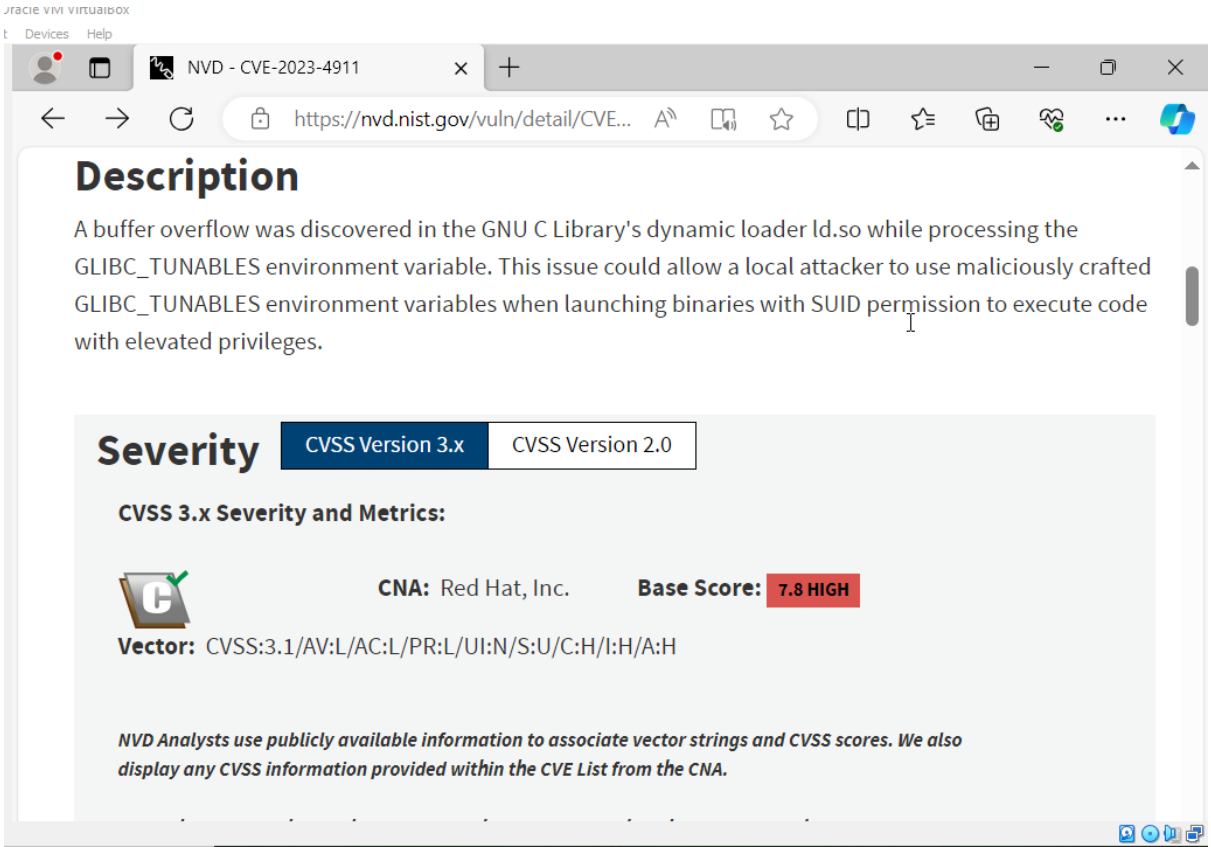
- New web page appears displaying CVE-2023-4911 details, you can view detailed information such as current description, severity, References and weakness enumeration.



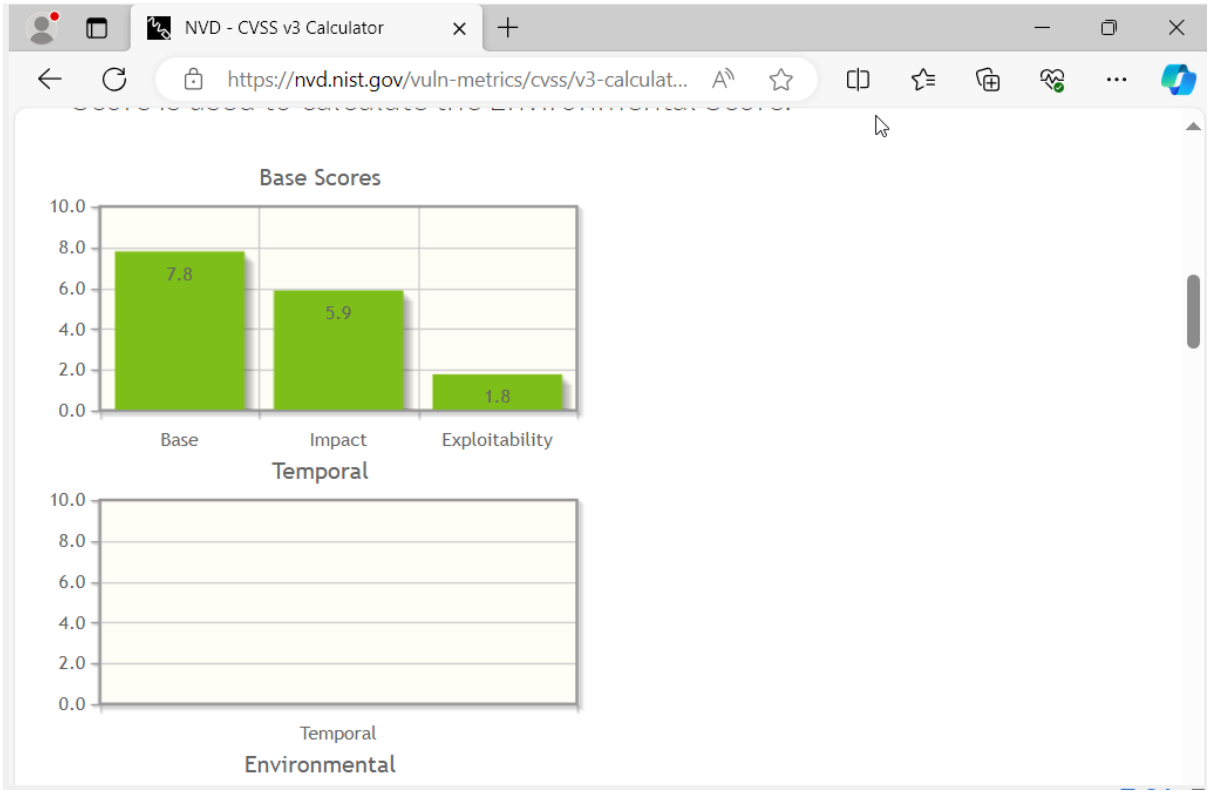


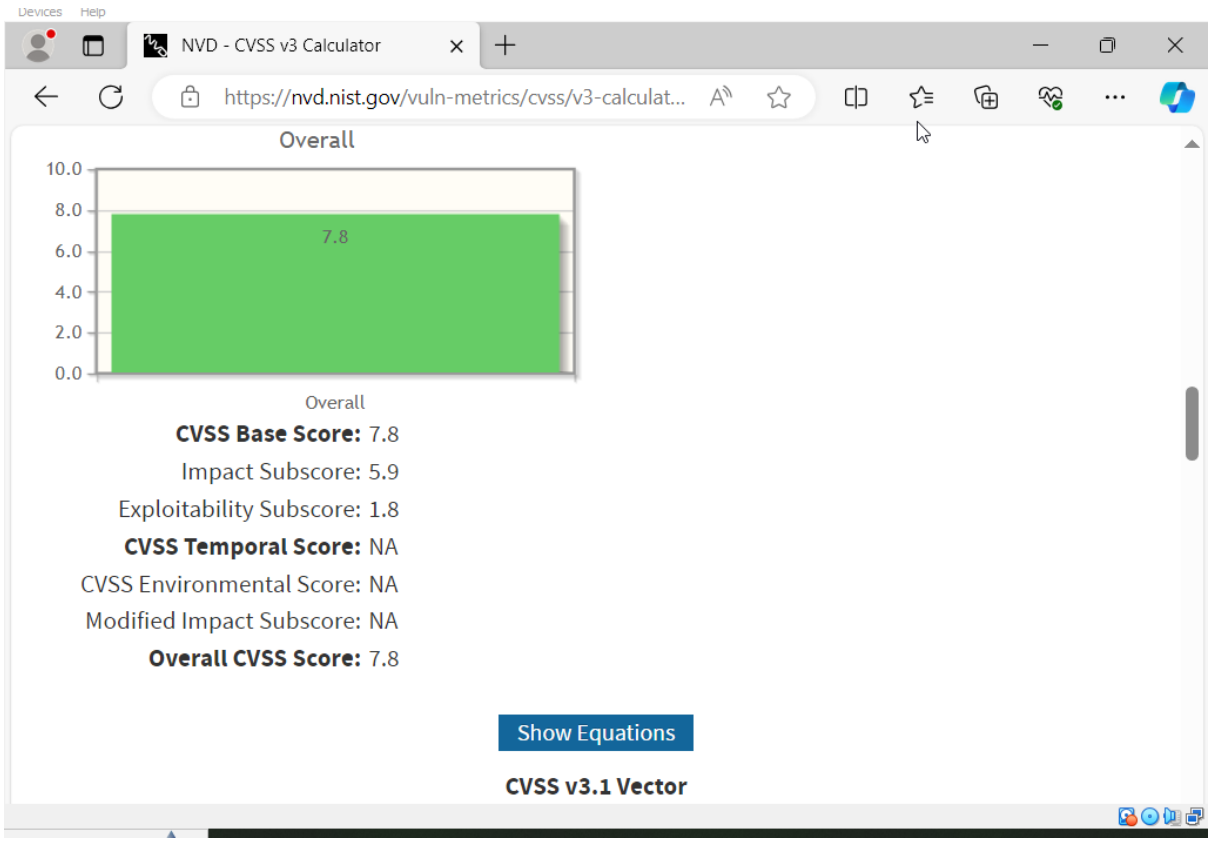


- Under the severity section click the Base score link to view the CVSS details regarding the vulnerabilities.

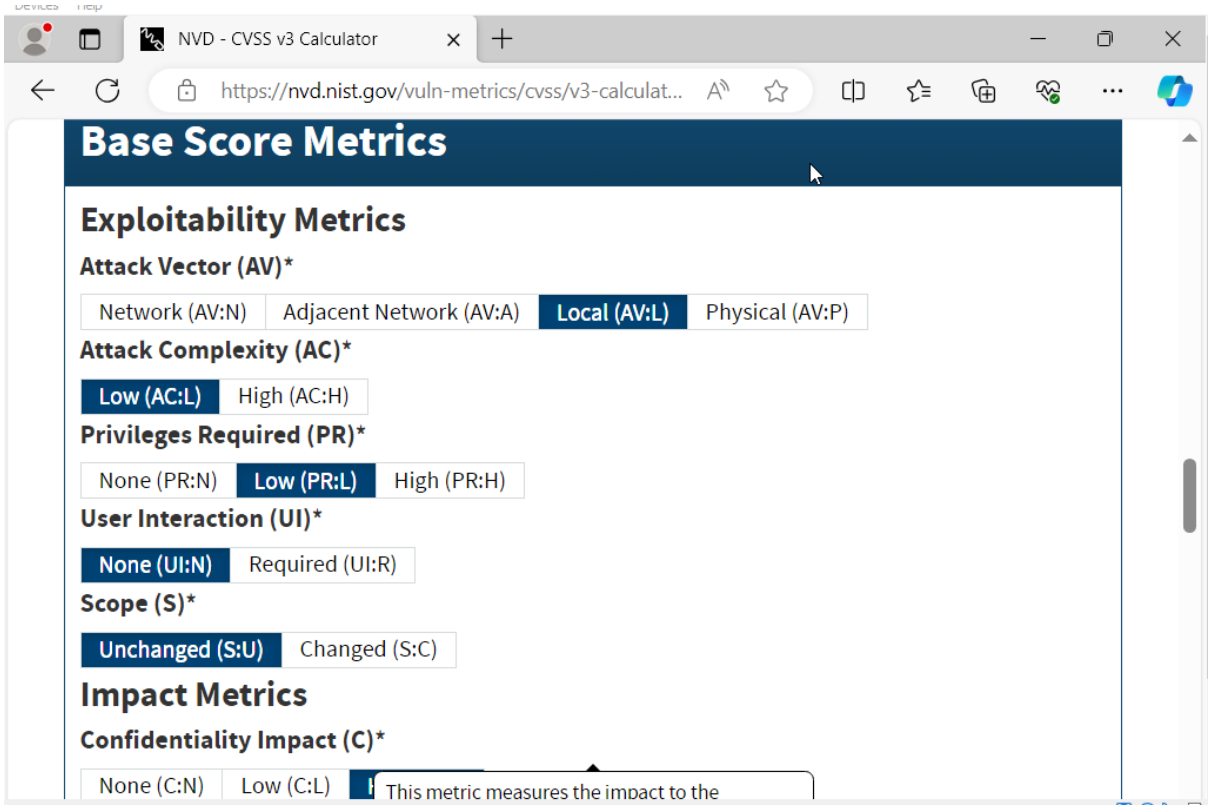


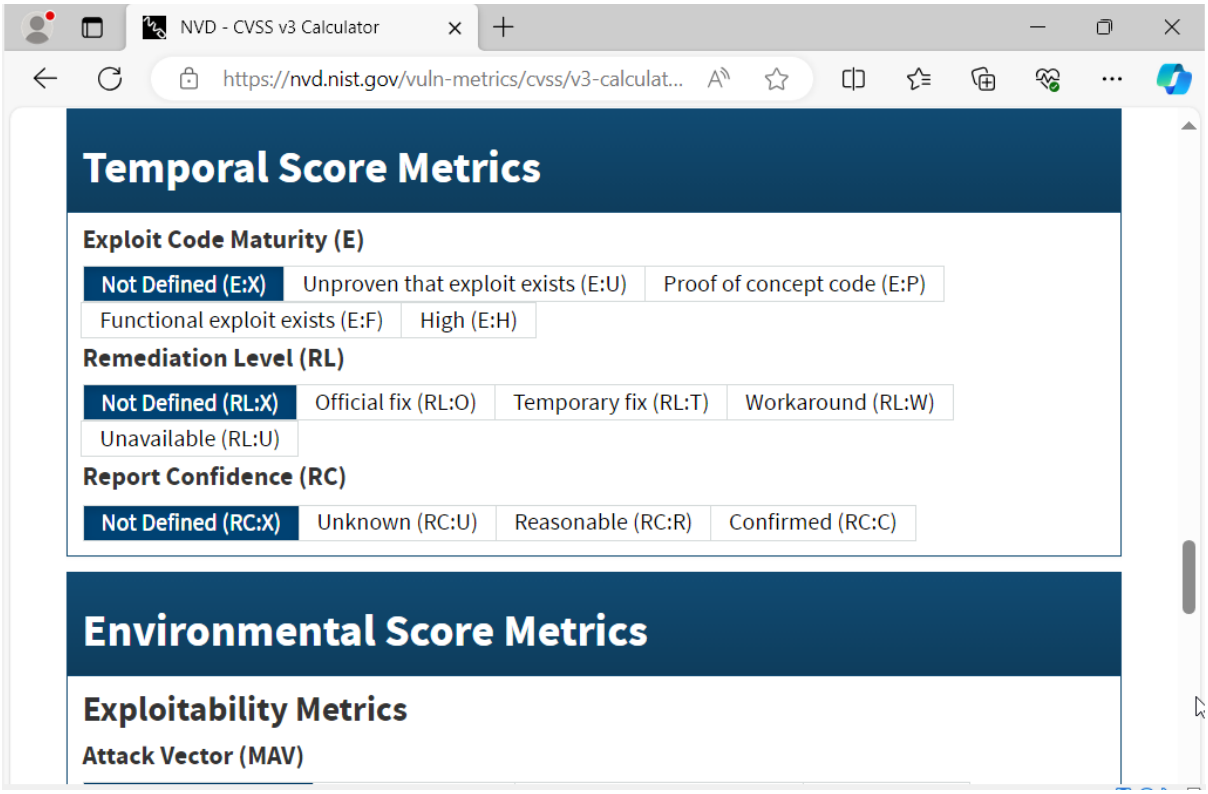
- A webpage appears displaying information such as Base scores, Temporal score, and Environmental scores overall scores related to vulnerability in graphical form, under common vulnerability scoring system calculator.

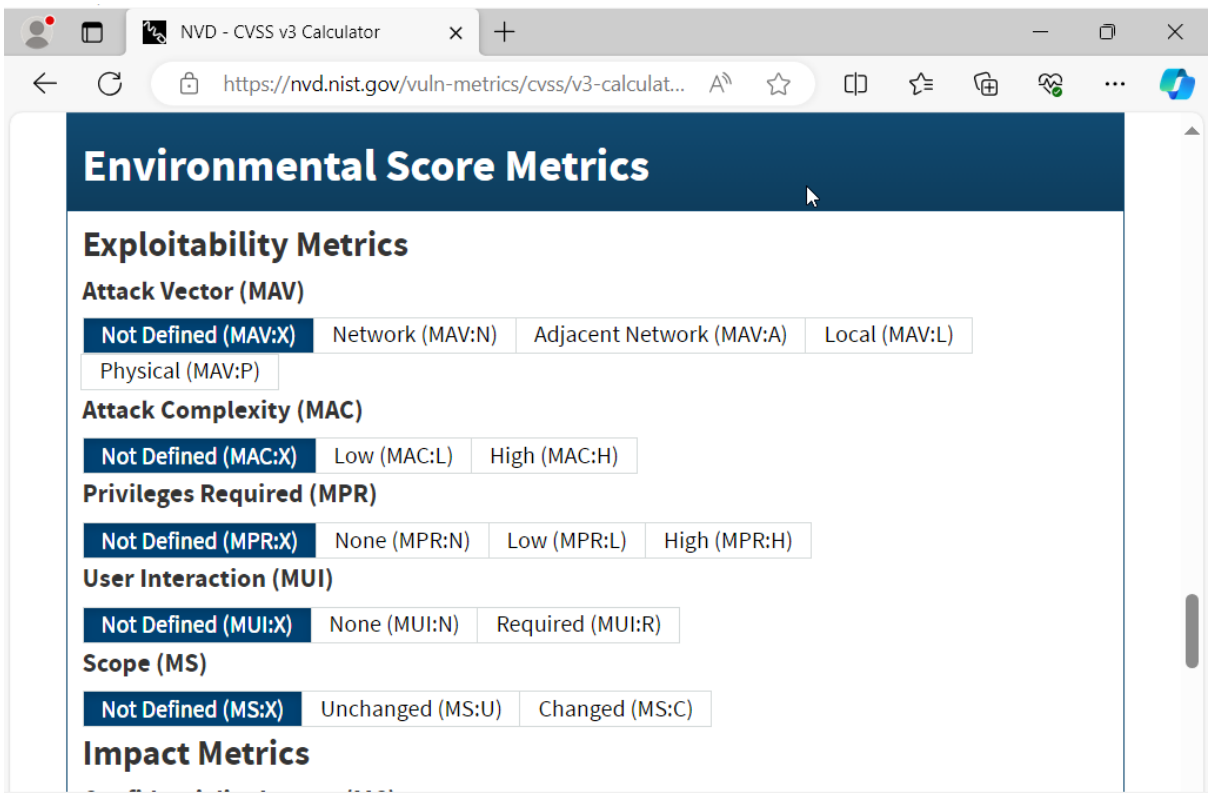


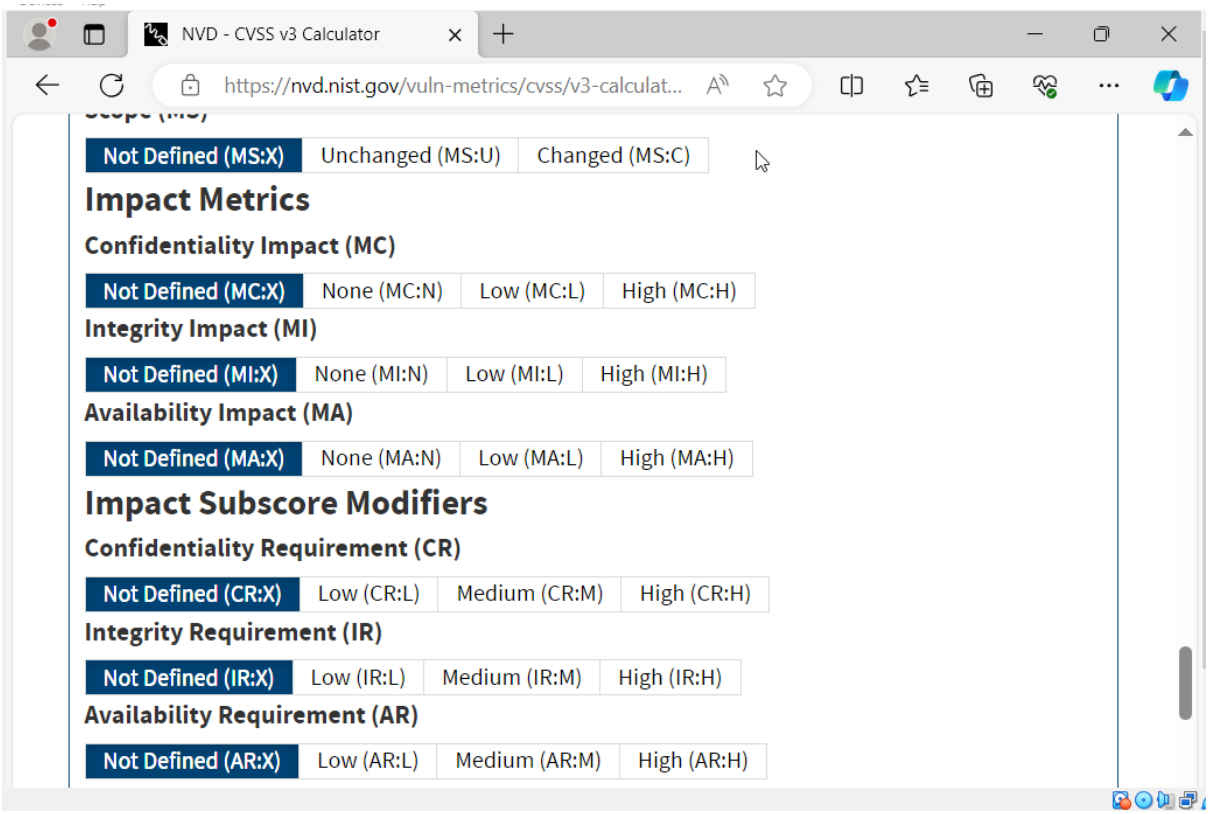


- Scroll down to view more detailed information on different score metrics.

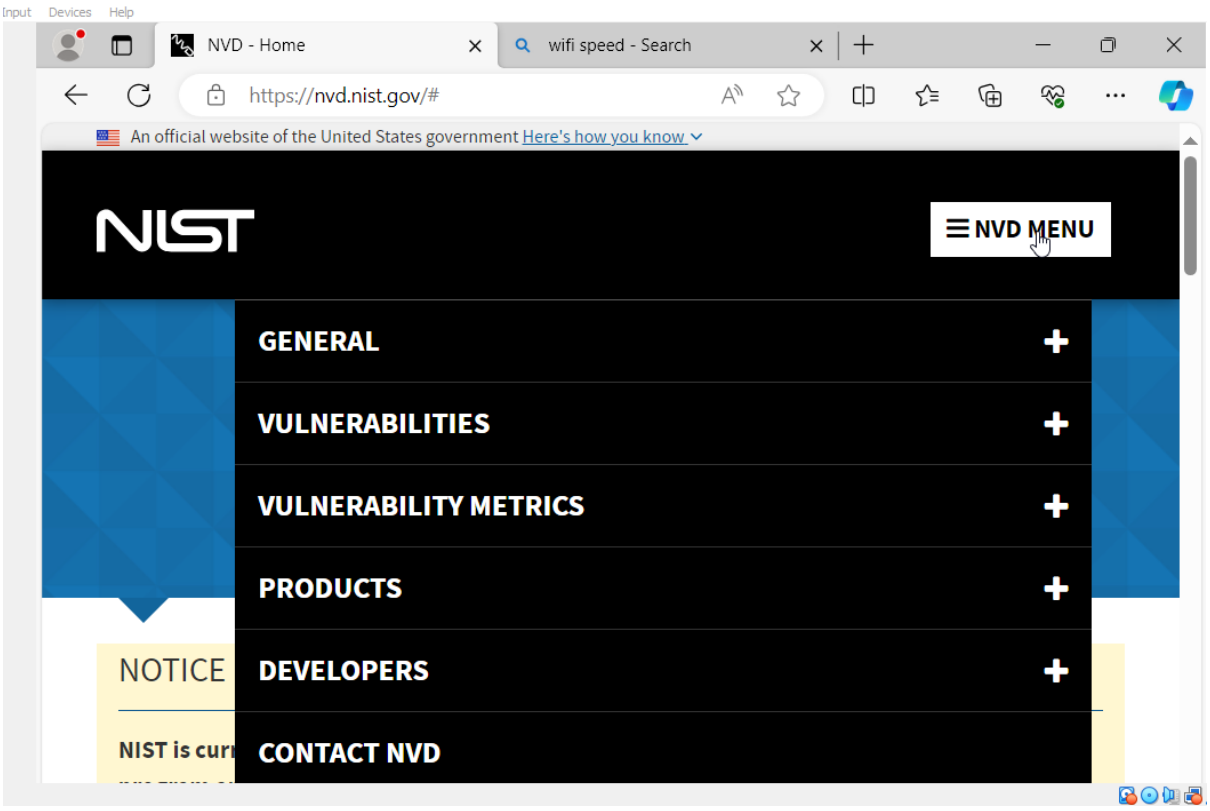


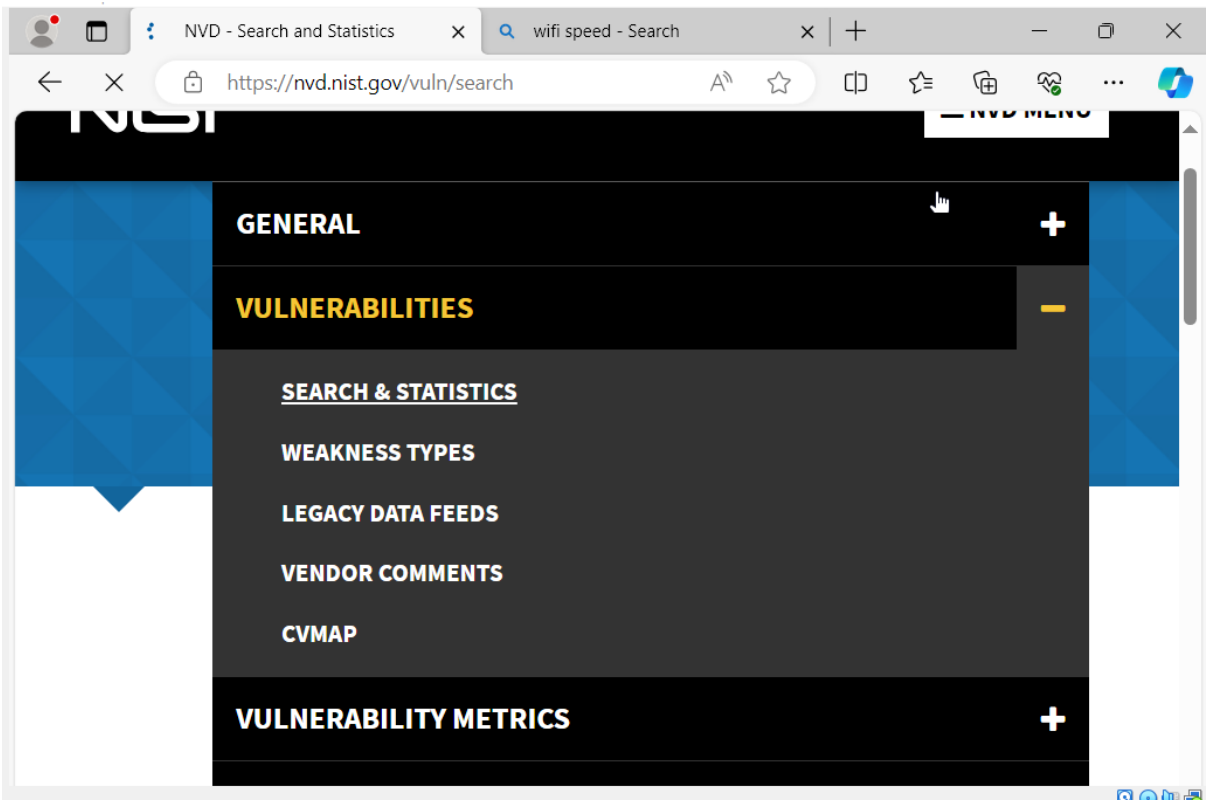

NVD - CVSS v3 Calculator
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculat...
Temporal Score Metrics
Exploit Code Maturity (E)
Not Defined (E:X)
Unproven that exploit exists (E:U)
Proof of concept code (E:P)
Functional exploit exists (E:F)
High (E:H)
Remediation Level (RL)
Not Defined (RL:X)
Official fix (RL:O)
Temporary fix (RL:T)
Workaround (RL:W)
Unavailable (RL:U)
Report Confidence (RC)
Not Defined (RC:X)
Unknown (RC:U)
Reasonable (RC:R)
Confirmed (RC:C)
Environmental Score Metrics
Exploitability Metrics
Attack Vector (MAV)


NVD - CVSS v3 Calculator
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculat...
Environmental Score Metrics
Exploitability Metrics
Attack Vector (MAV)
Not Defined (MAV:X)
Network (MAV:N)
Adjacent Network (MAV:A)
Local (MAV:L)
Physical (MAV:P)
Attack Complexity (MAC)
Not Defined (MAC:X)
Low (MAC:L)
High (MAC:H)
Privileges Required (MPR)
Not Defined (MPR:X)
None (MPR:N)
Low (MPR:L)
High (MPR:H)
User Interaction (MUI)
Not Defined (MUI:X)
None (MUI:N)
Required (MUI:R)
Scope (MS)
Not Defined (MS:X)
Unchanged (MS:U)
Changed (MS:C)
Impact Metrics

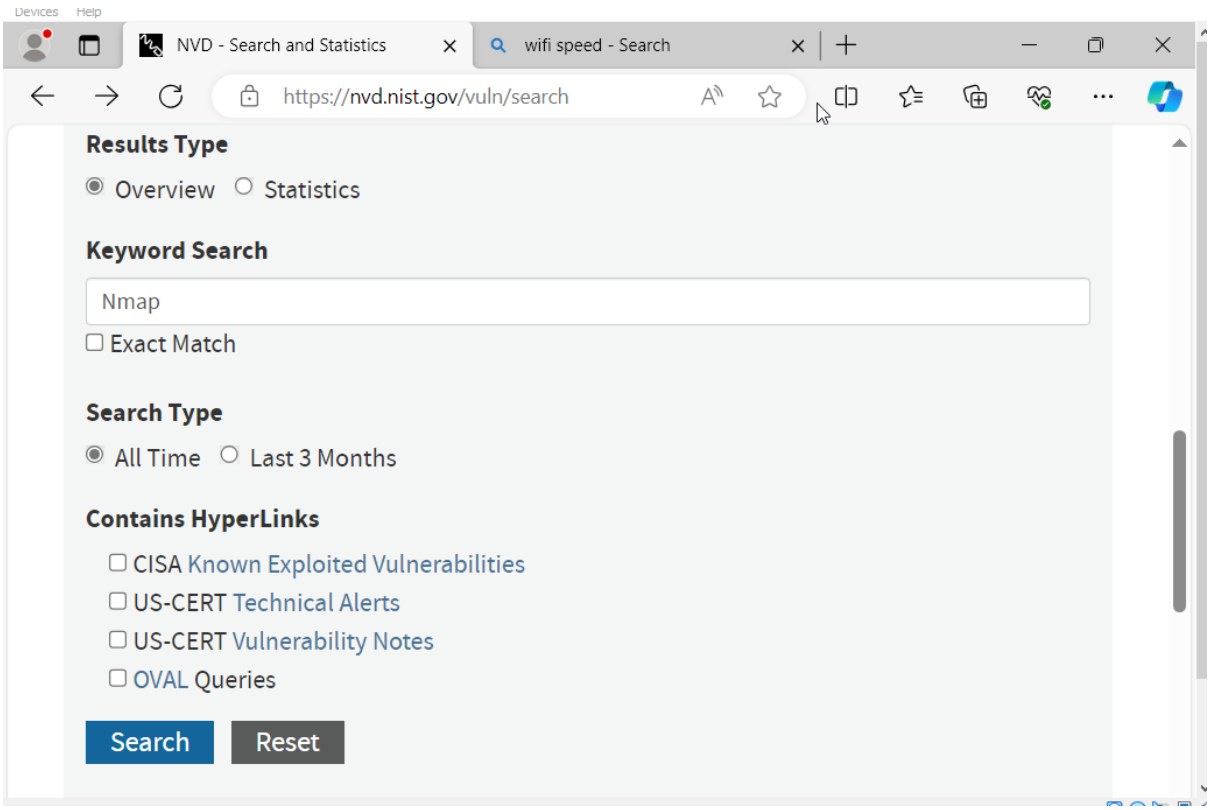


- Now navigate back to the main page of the National Vulnerability Database, Expand vulnerabilities and click search and statistics option.

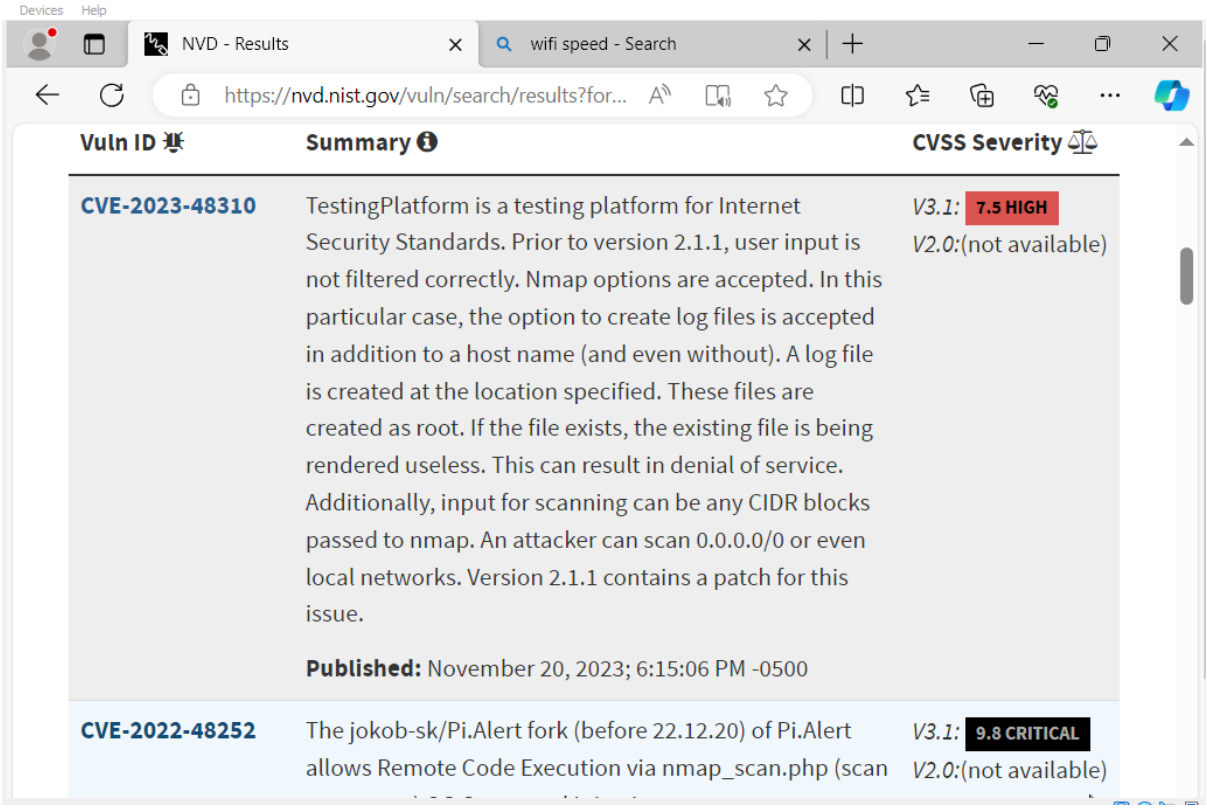


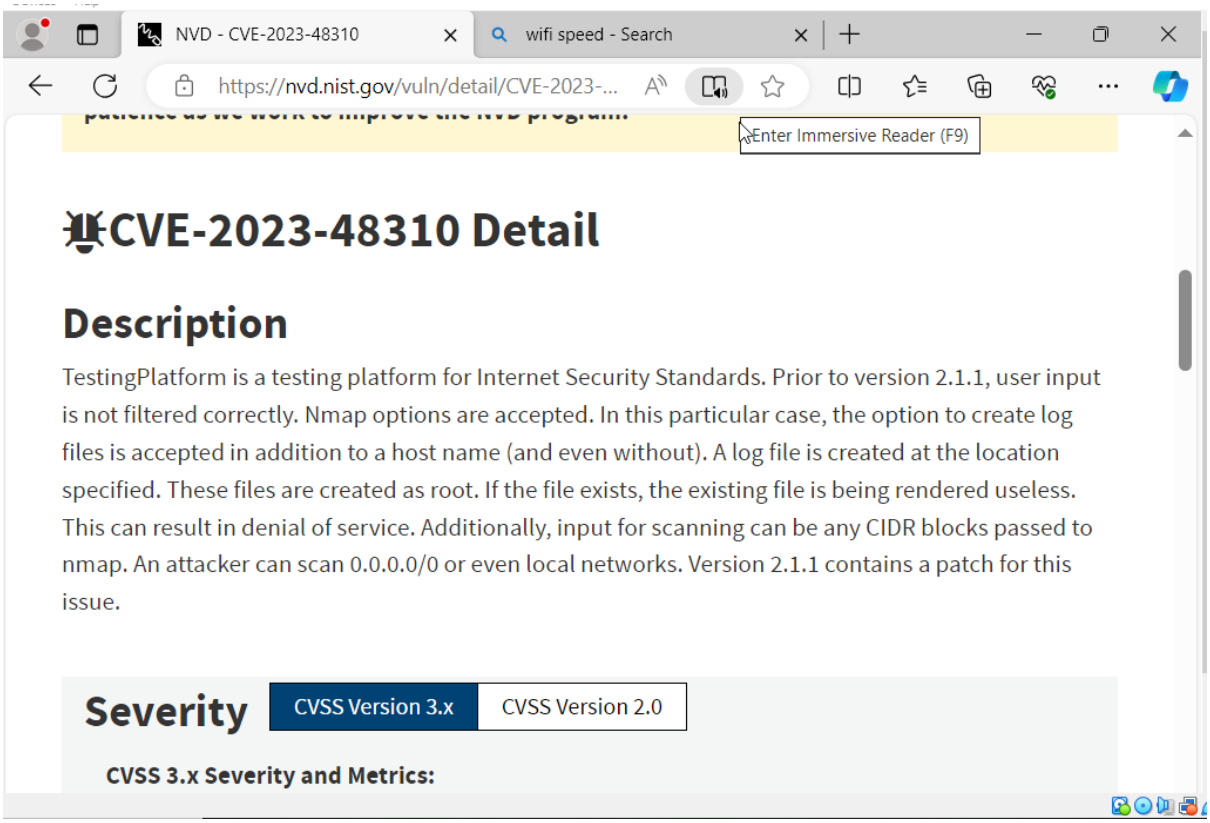


- Search vulnerabilities database page appears. In the keyword search field type a target service (Nmap) and click search.



- You can view information of vulnerabilities by clicking on the VULN ID link.



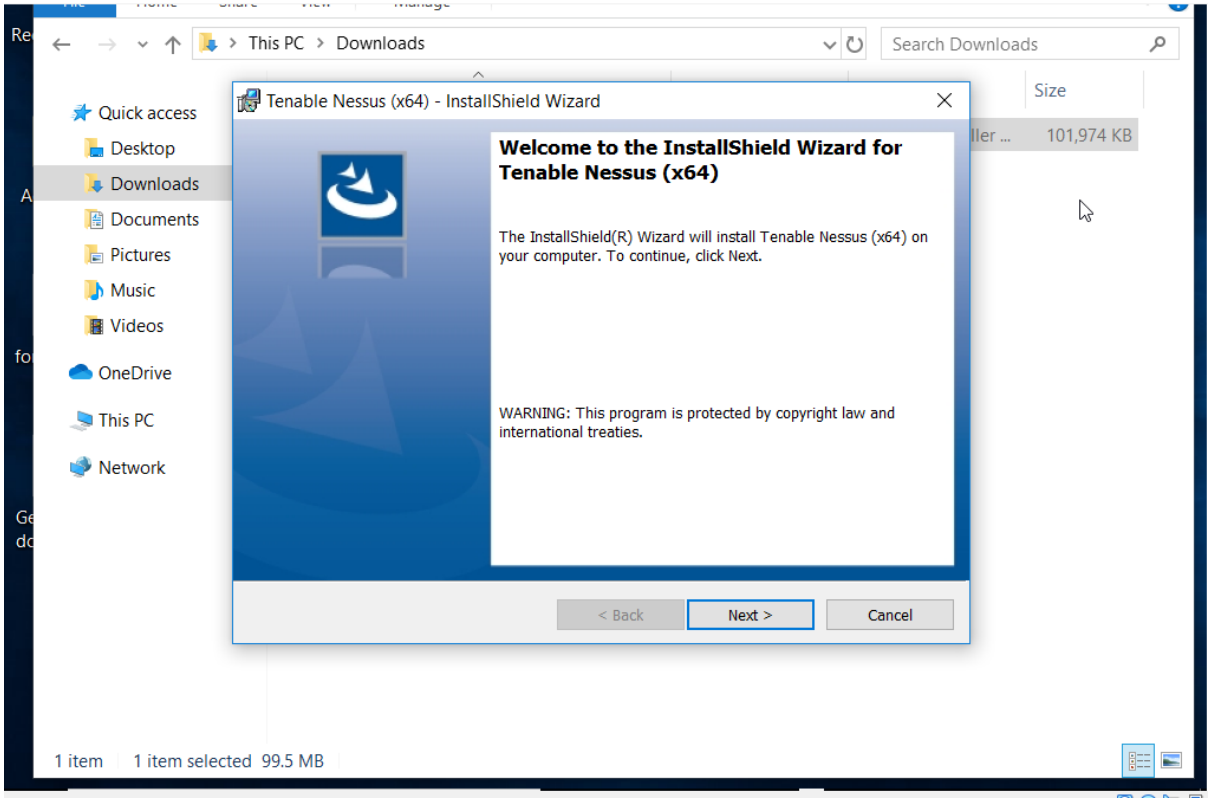


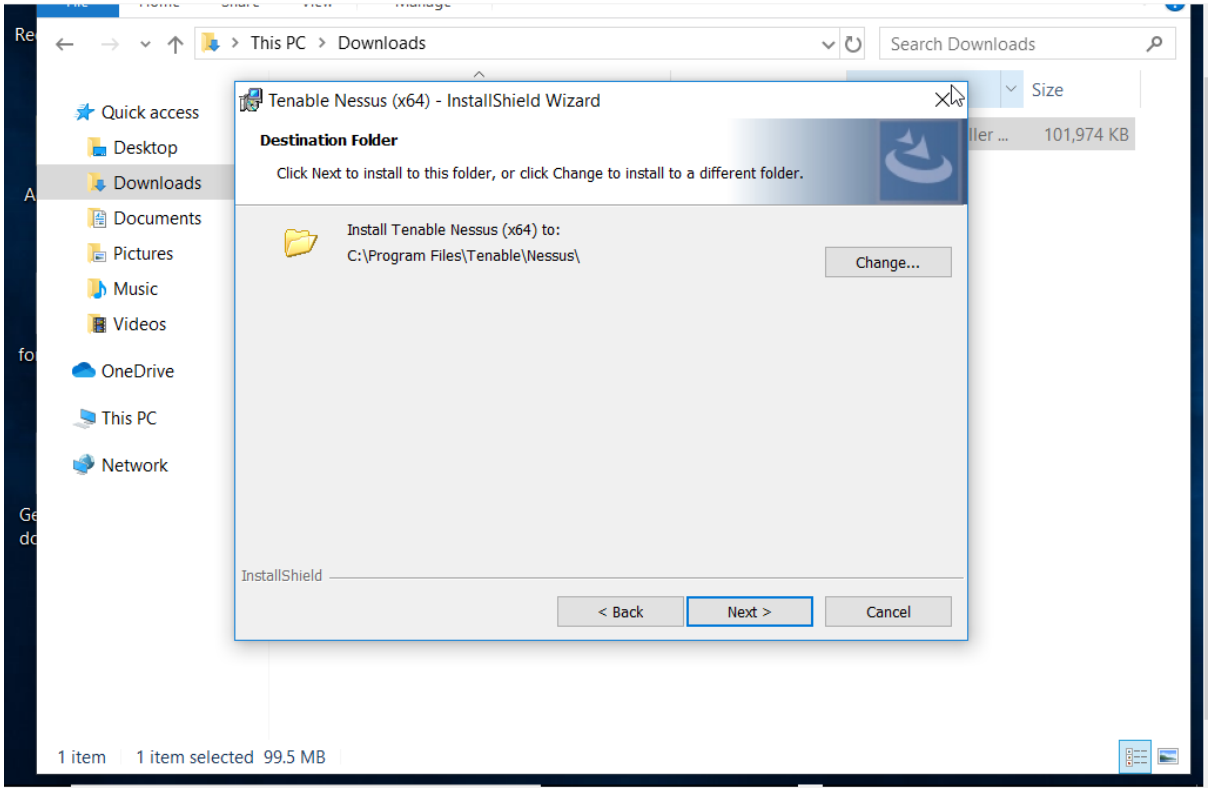
- Likewise, you can search for other targets services for the underlined venerability in the search Vulnerability database section.

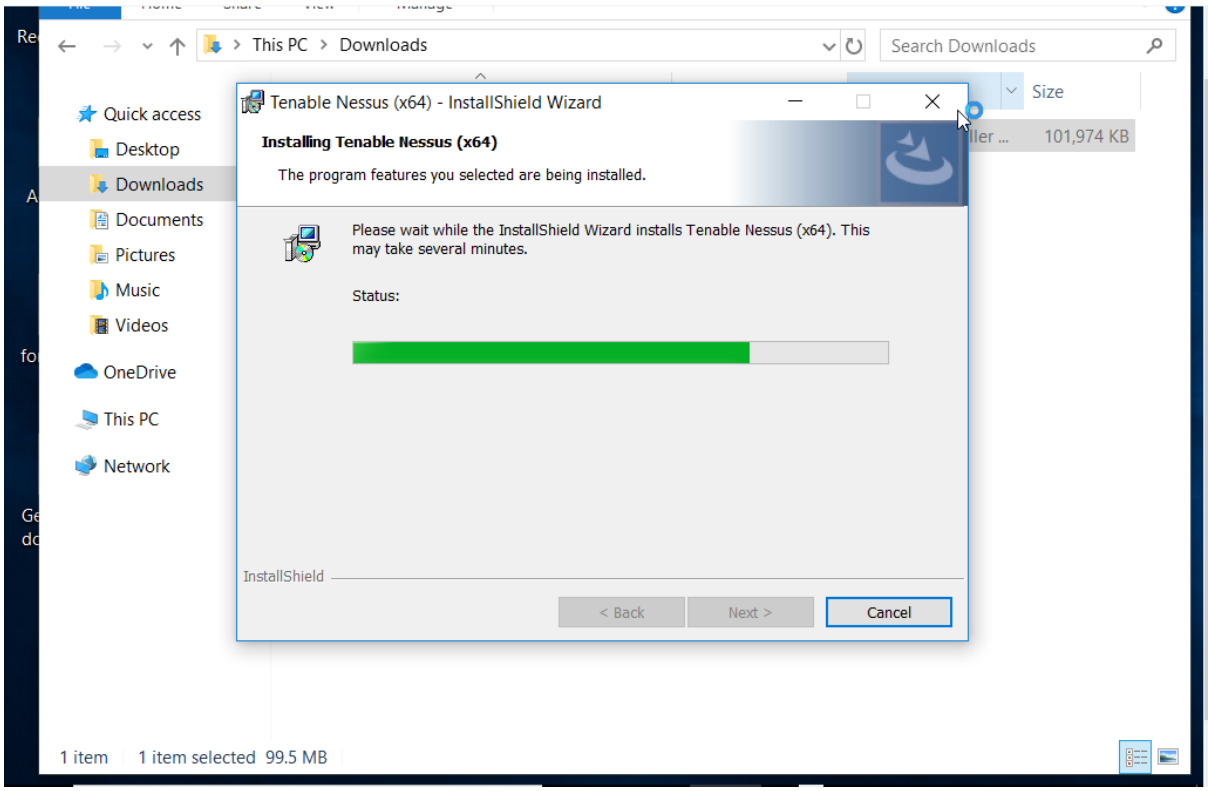
LAB :2

TASK: Perform Vulnerability Scanning using Nessus

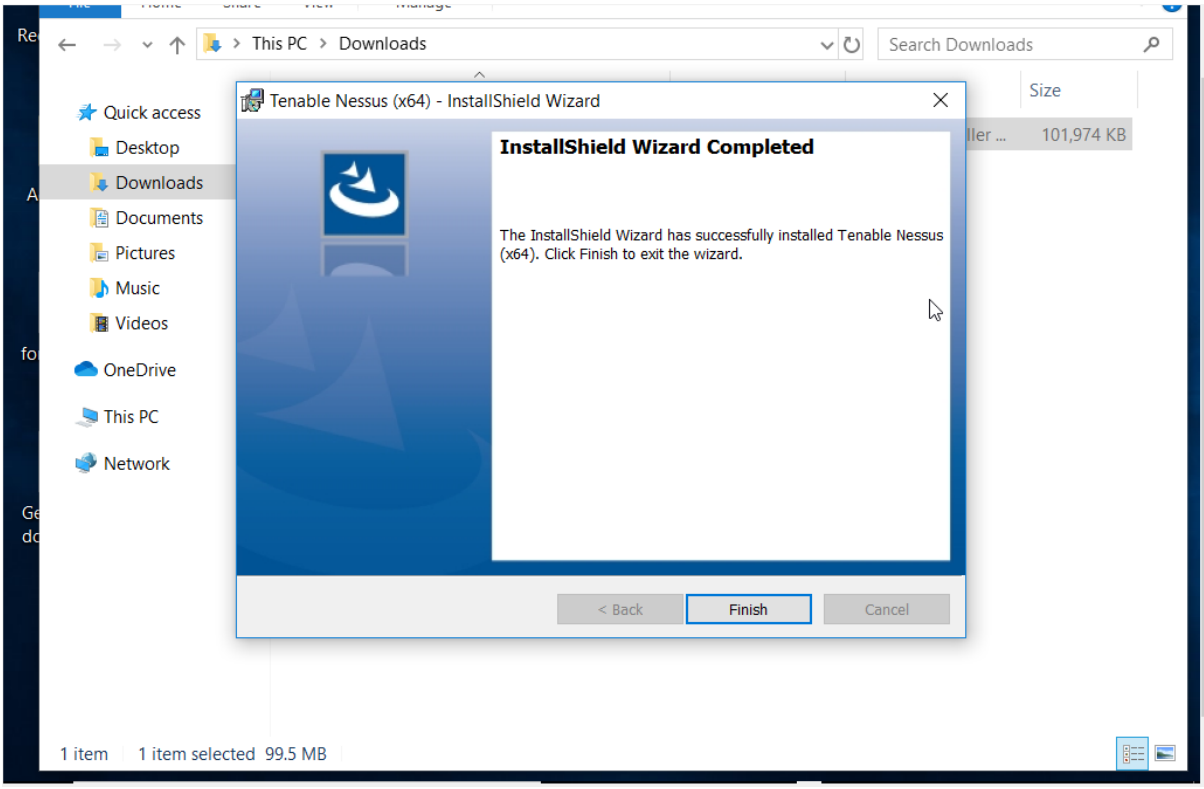
- Installation of Nessus in windows 10



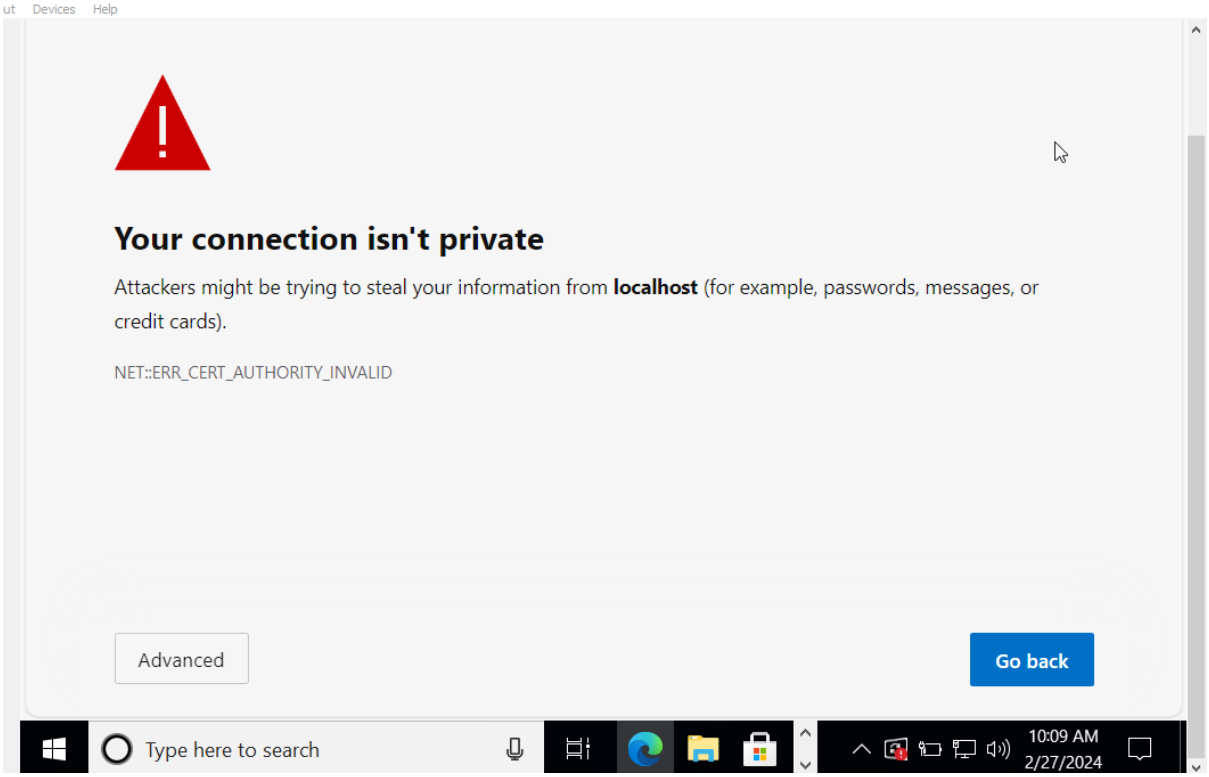

This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Size
101,974 KB
Tenable Nessus (x64) - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Tenable Nessus (x64) to:
C:\Program Files\Tenable\Nessus\
Change...
InstallShield
< Back
Next >
Cancel
1 item
1 item selected 99.5 MB


This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Size
101,974 KB
Tenable Nessus (x64) - InstallShield Wizard
Installing Tenable Nessus (x64)
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel
1 item
1 item selected 99.5 MB

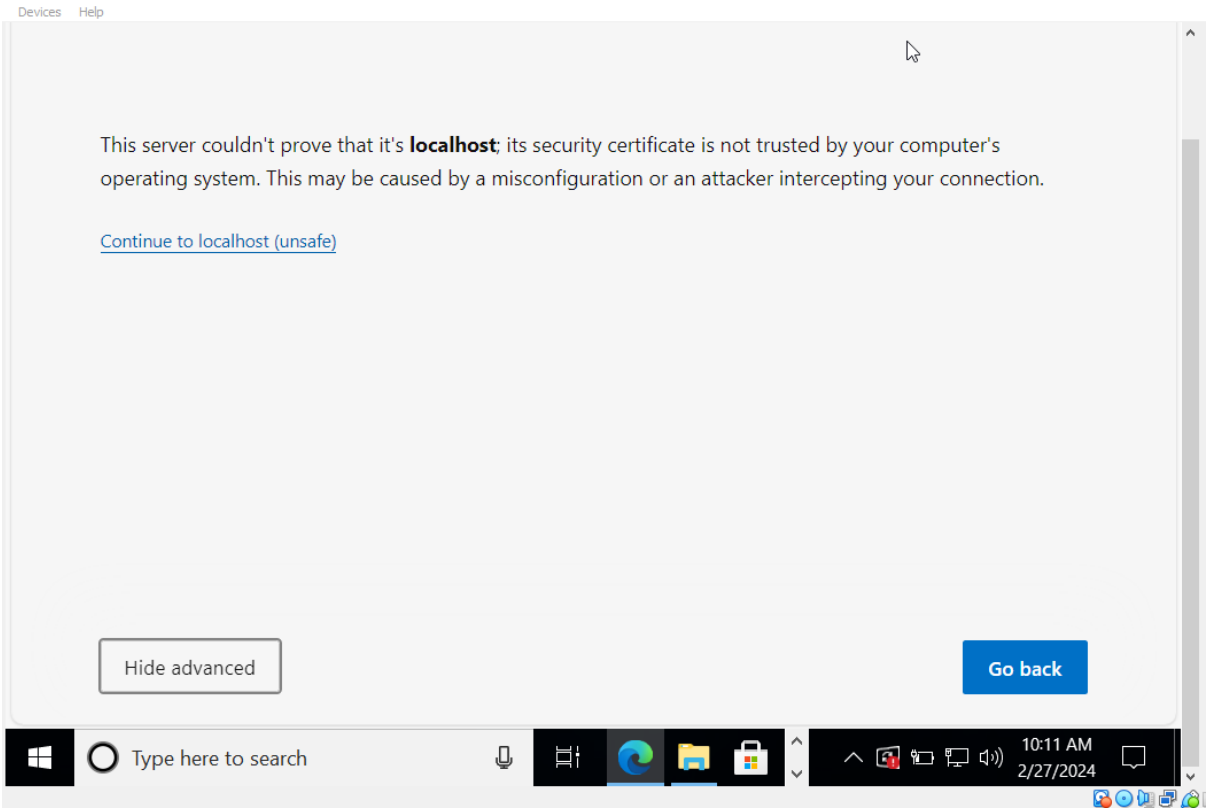
- Click finish and finish with installation



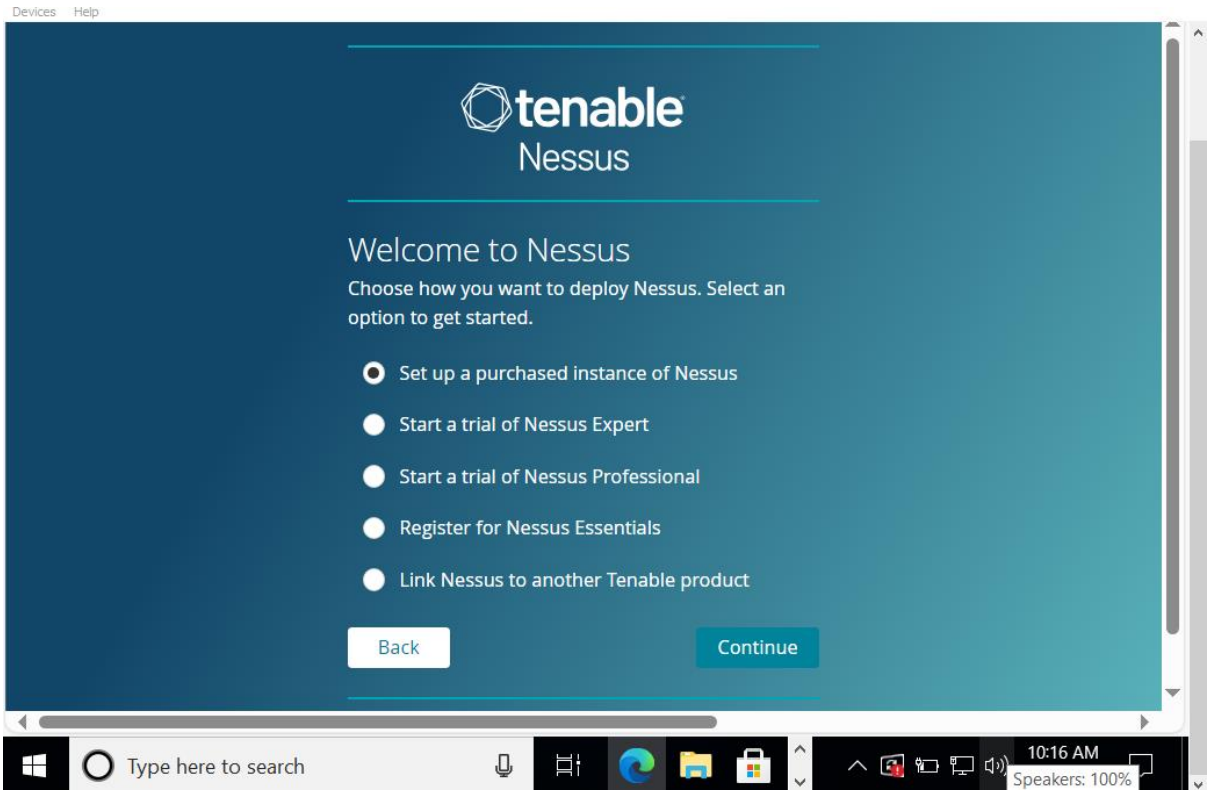
- Next step with start by launching Nessus
- When this window appear in the browser, click on advance



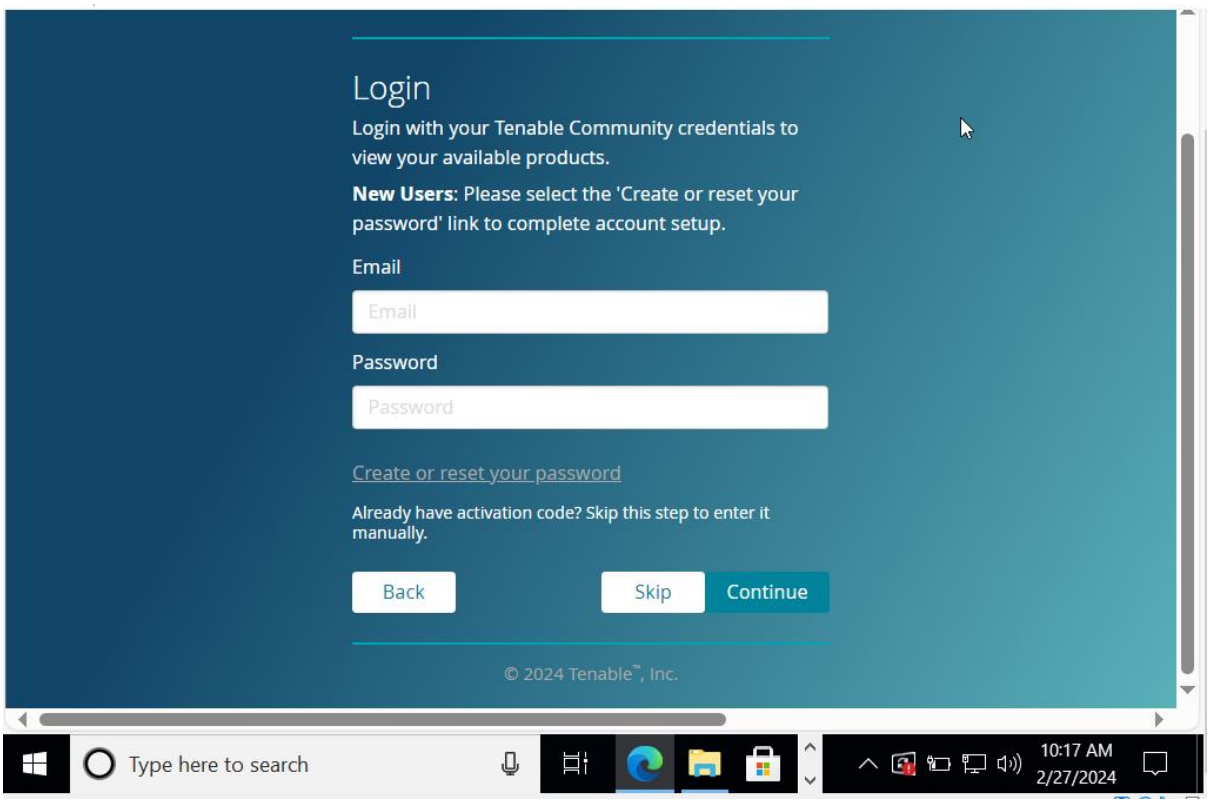
- Click continue to localhost



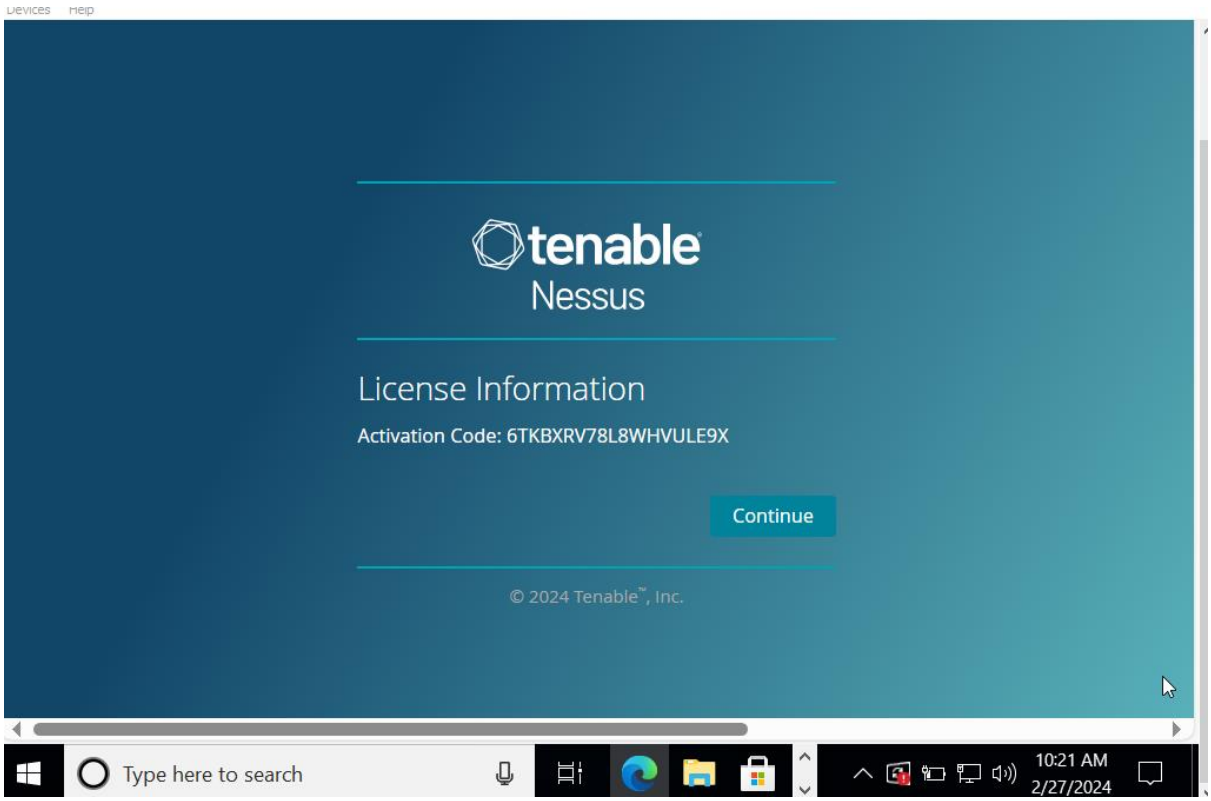
- When welcome to Nessus windows appears, click on Nessus Essentials, then continue.



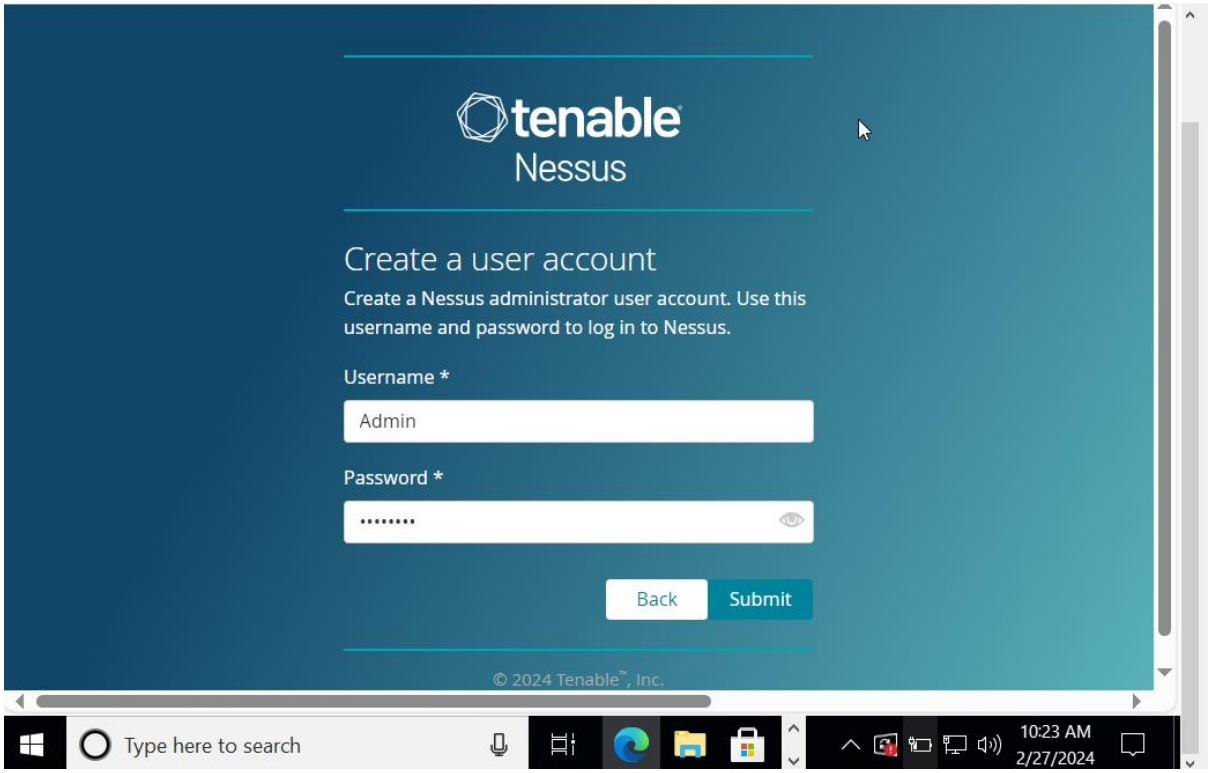
- On this page you are required to register to Nessus.



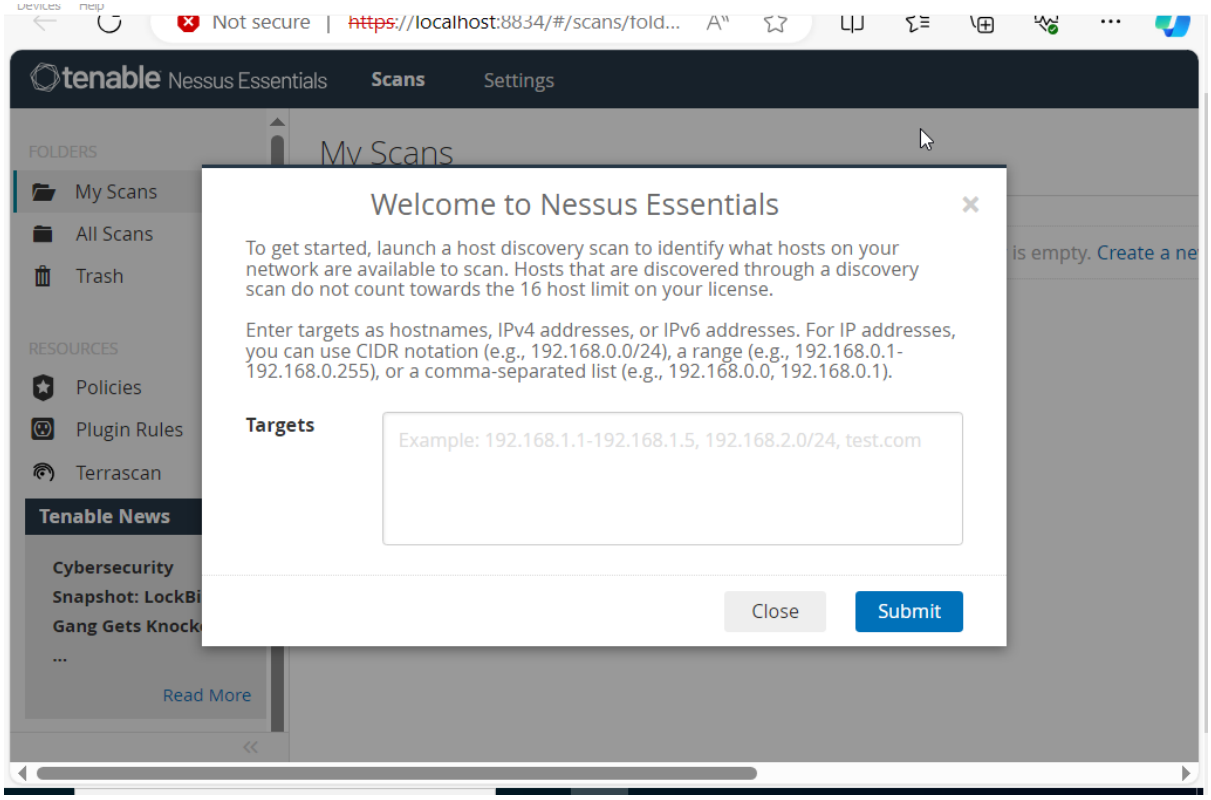
- After Registration, you are required to fill in the code sent your working email.



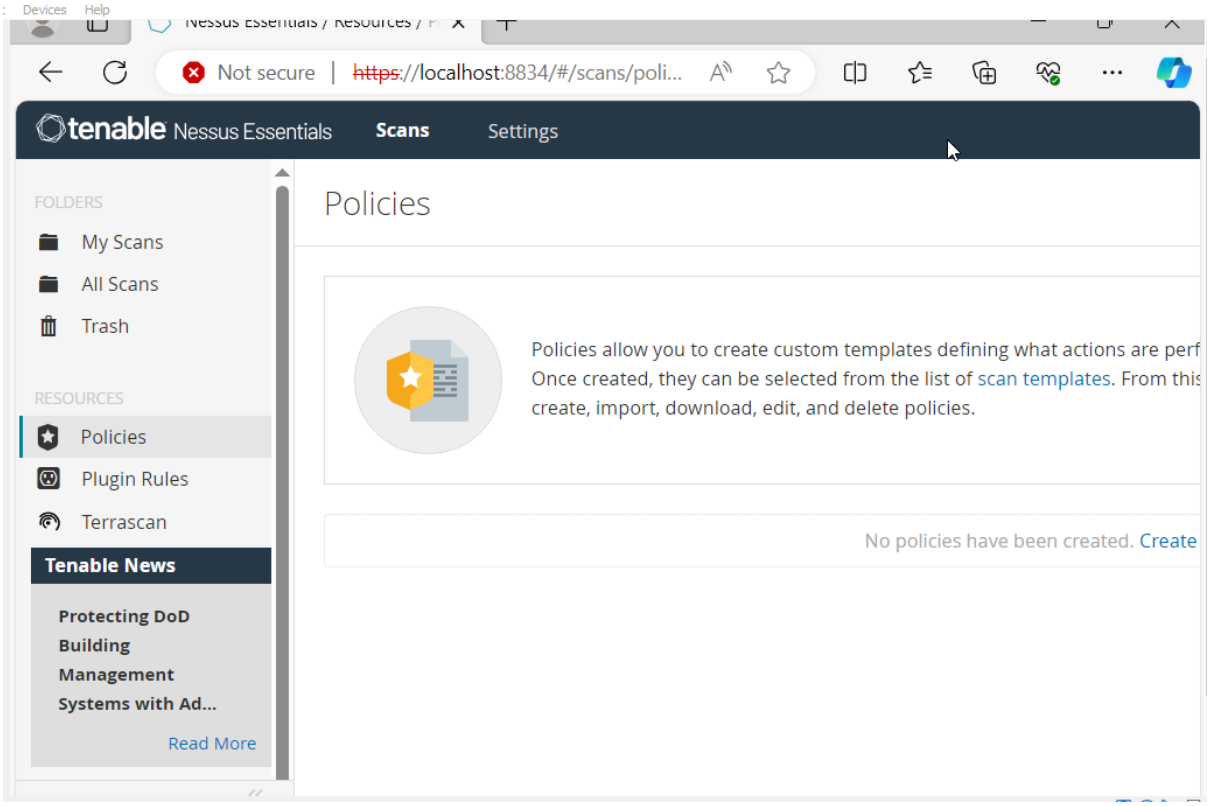
- After in-putting your activation click continue, it will open a login page, login as an admin and click continue.



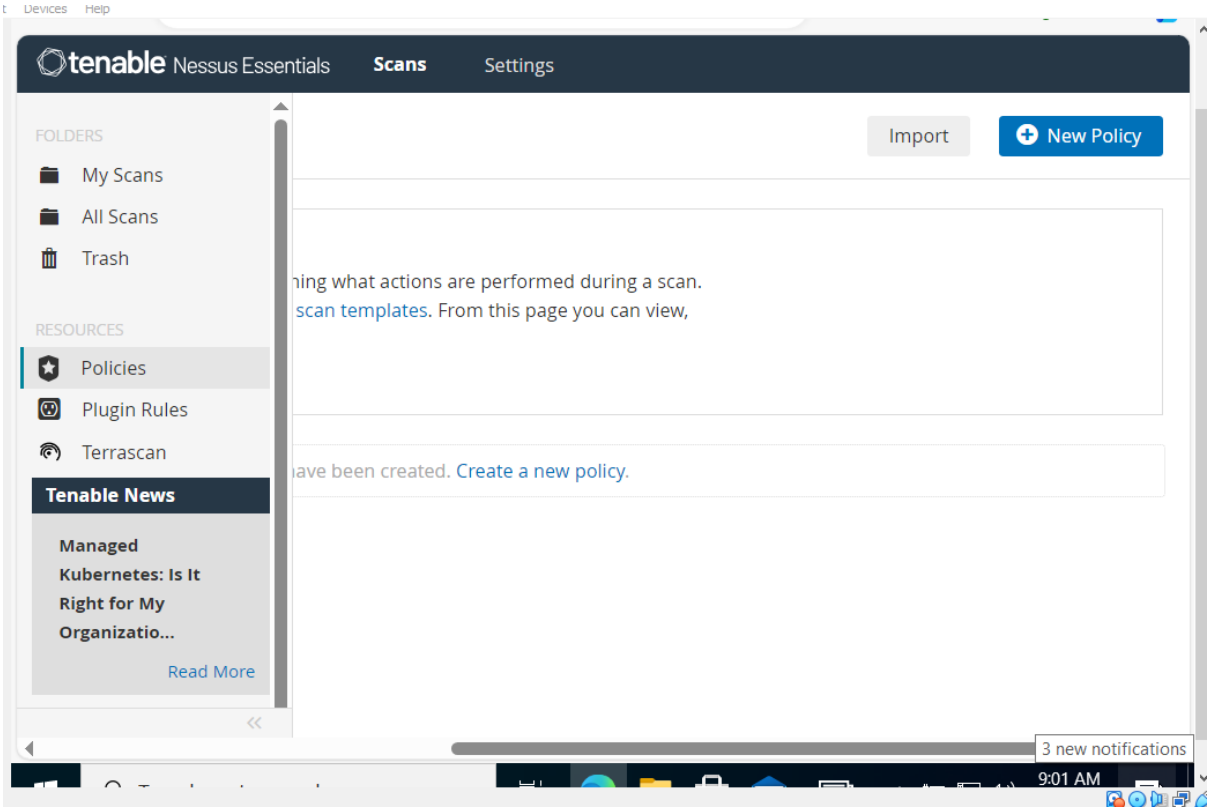
- The Network essentials page appears, click on the policies section from the pane on the left.

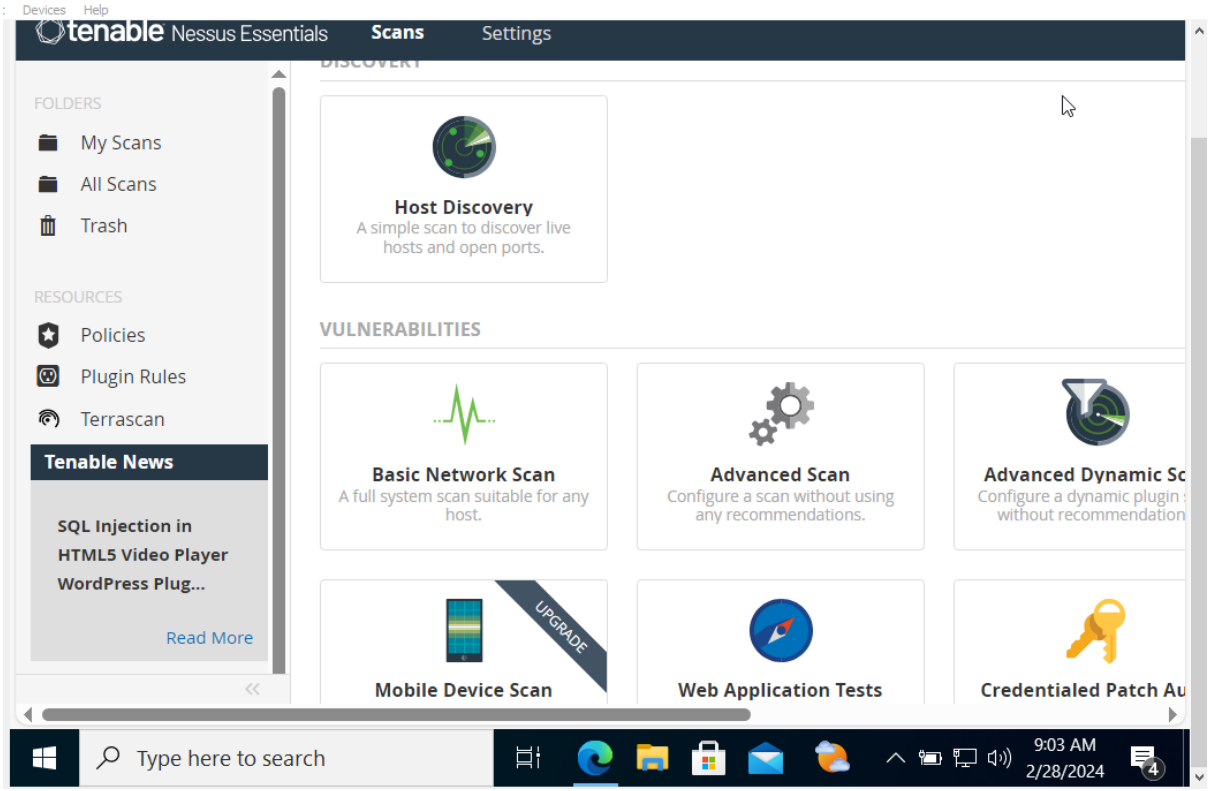


- The policy window appears, create new policies.

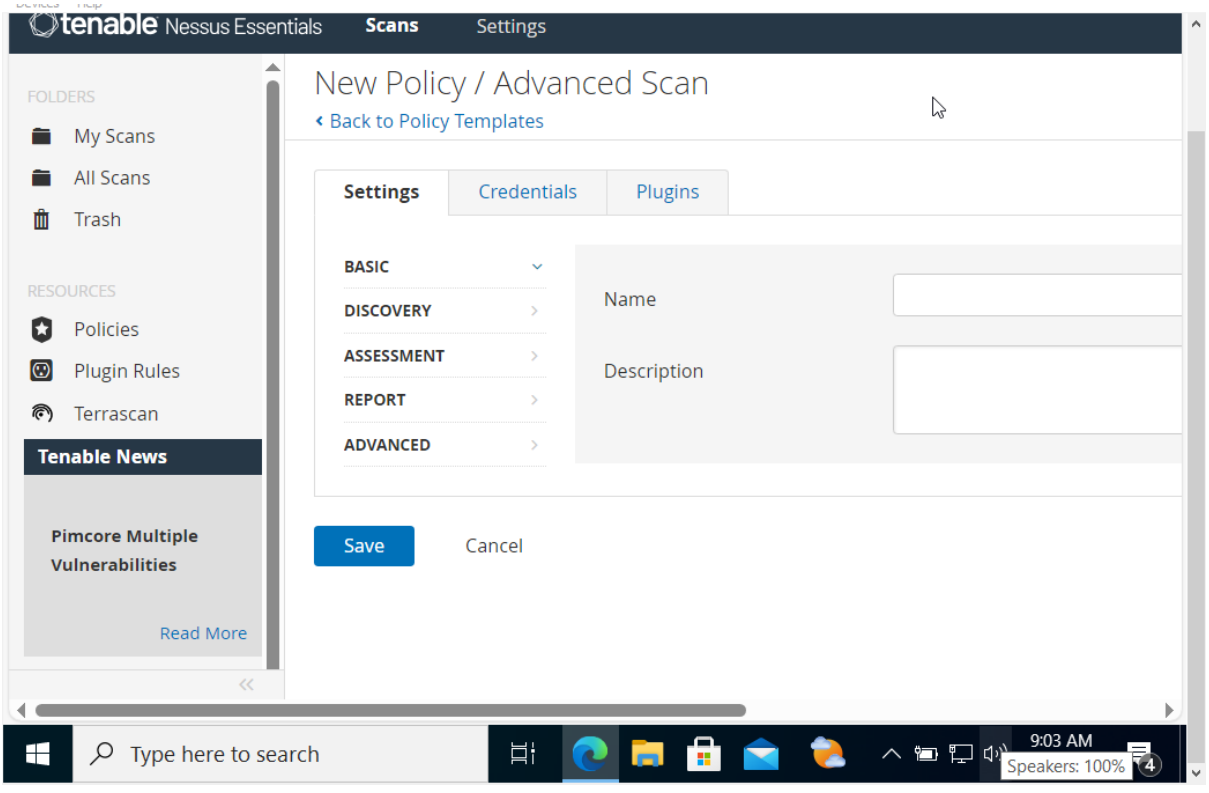


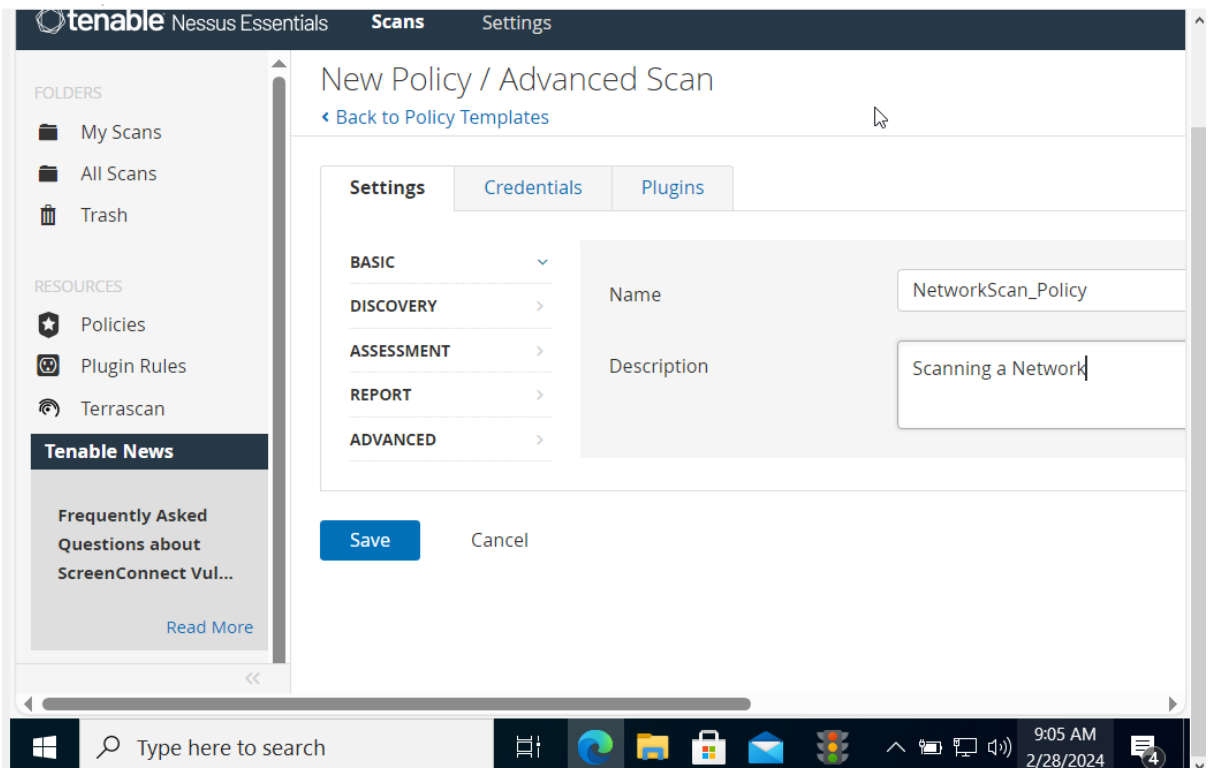
- The policy templates windows appears, click advance scan.



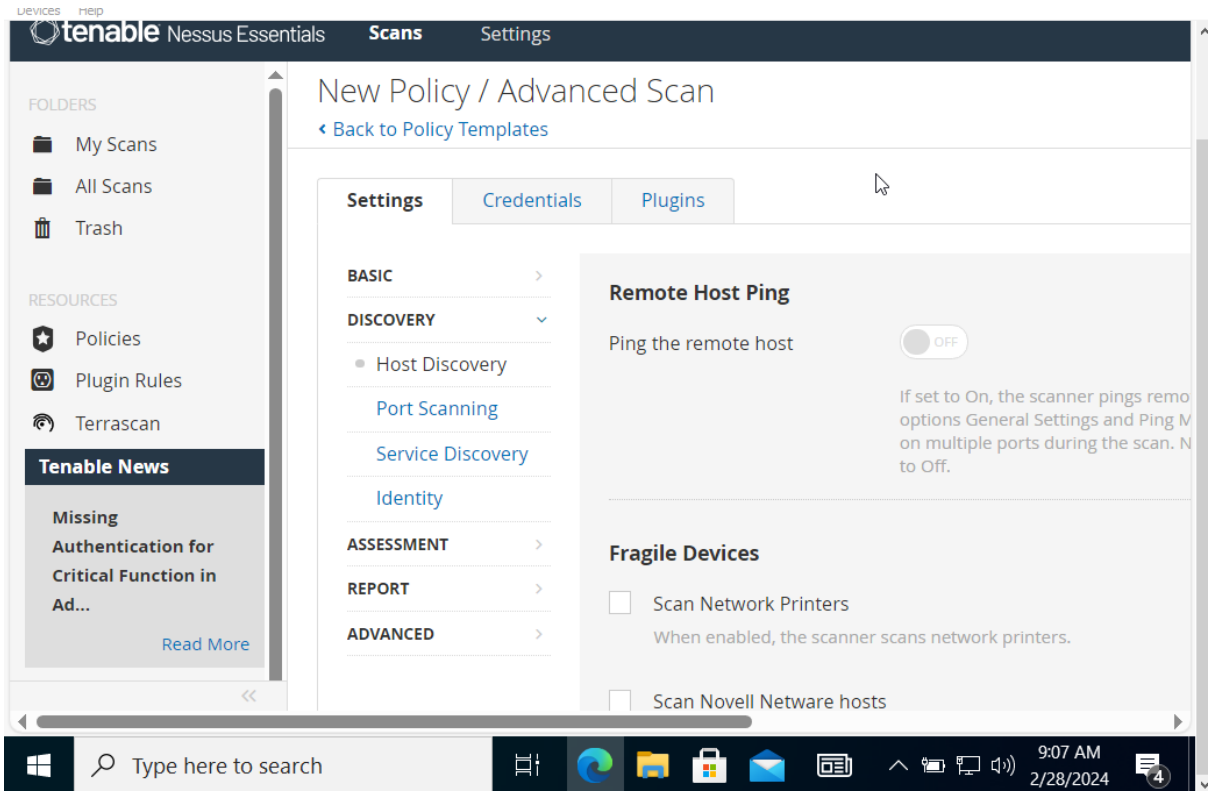


- In the settings tab, under the basic setting type specify a policy name in the name
- field (here Network scan policy), and give a description about the policy (Here, Scanning A Network

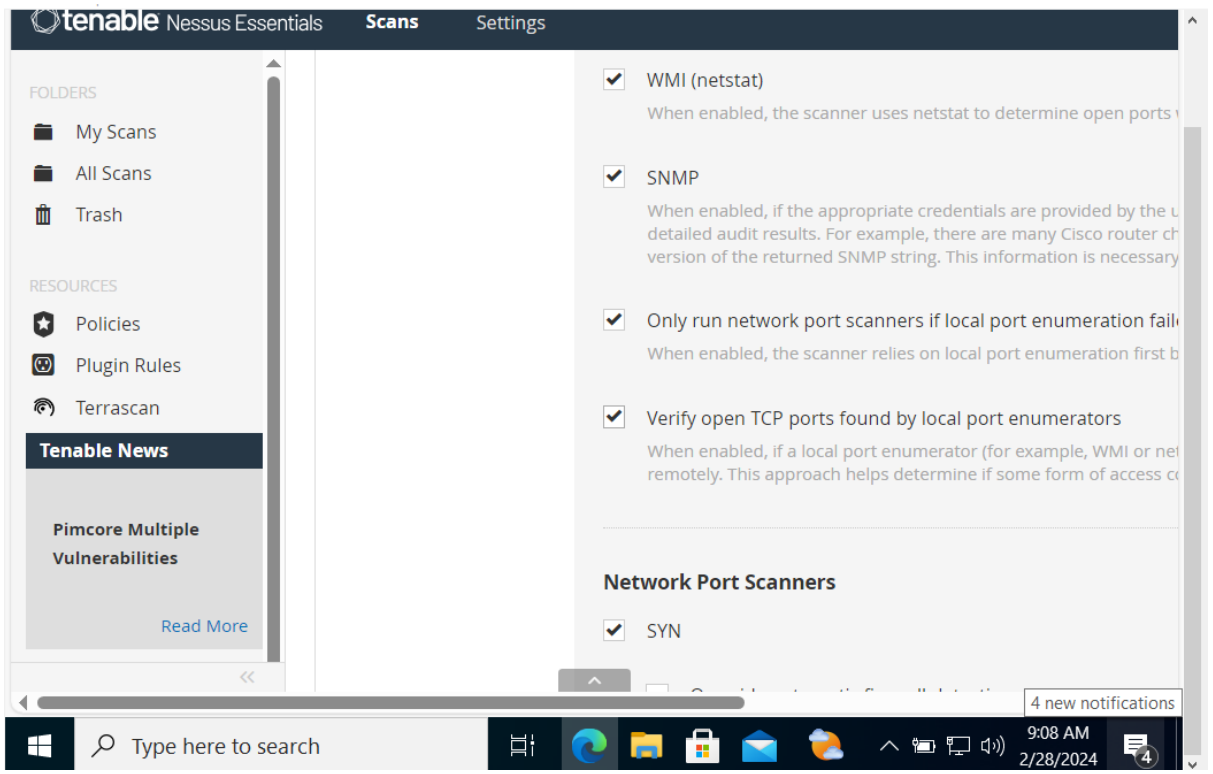




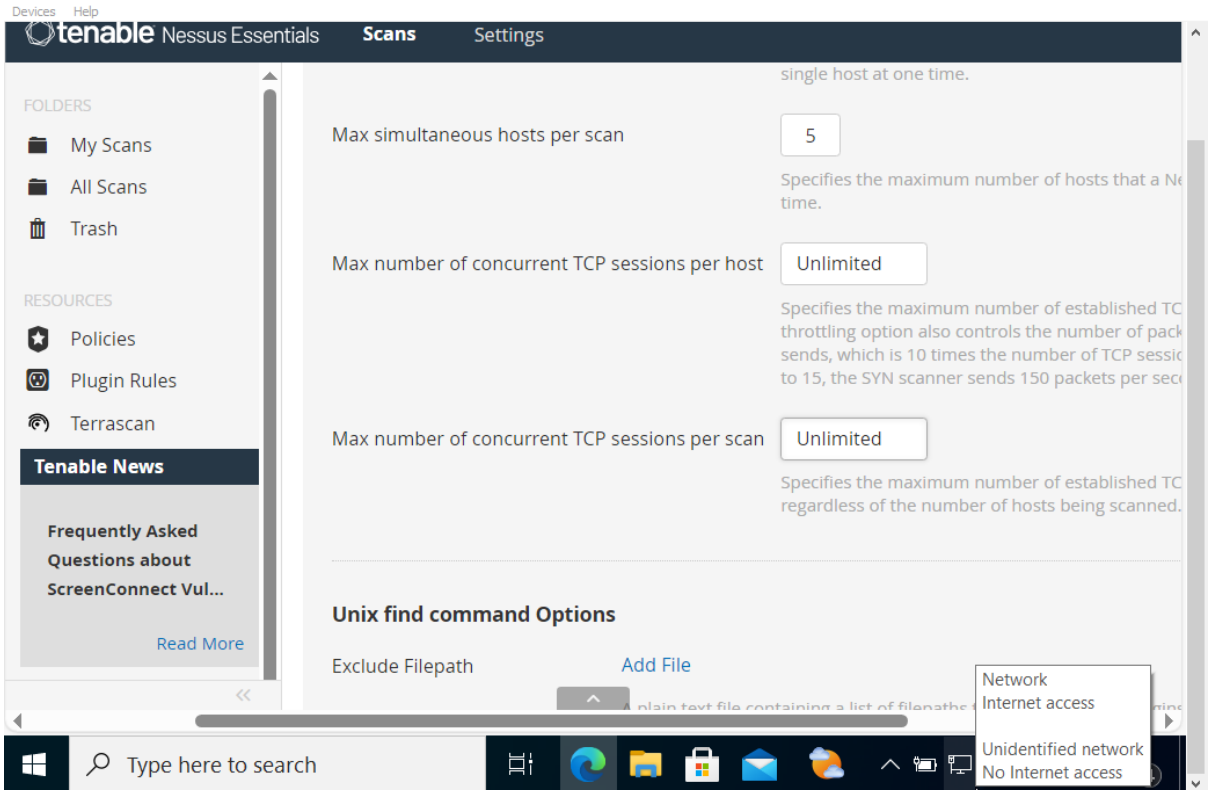
- In the settings tab, click discovery setting type and turn off the ping the remote host option from the right pane.



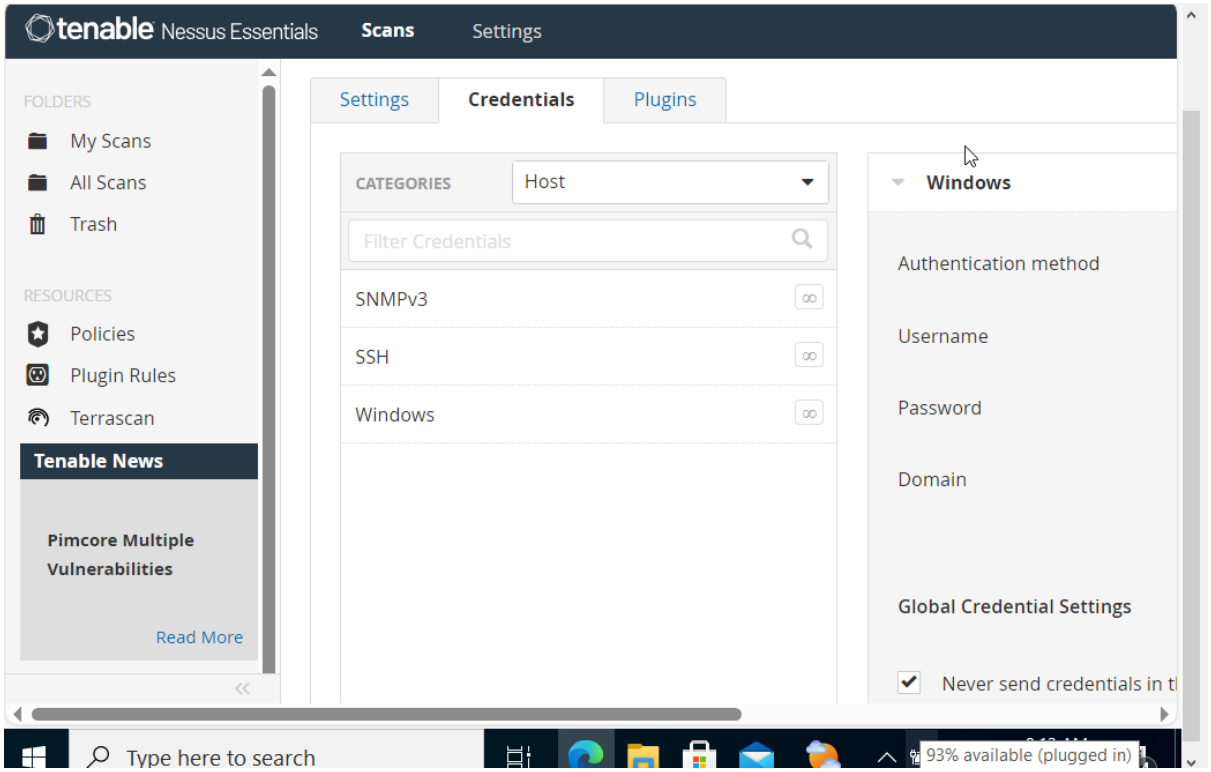
- Select the port scanning option under the discovery setting type and then click the verify open TCP ports found by local port enumerator checkbox. Leave the other fields with default options as shown



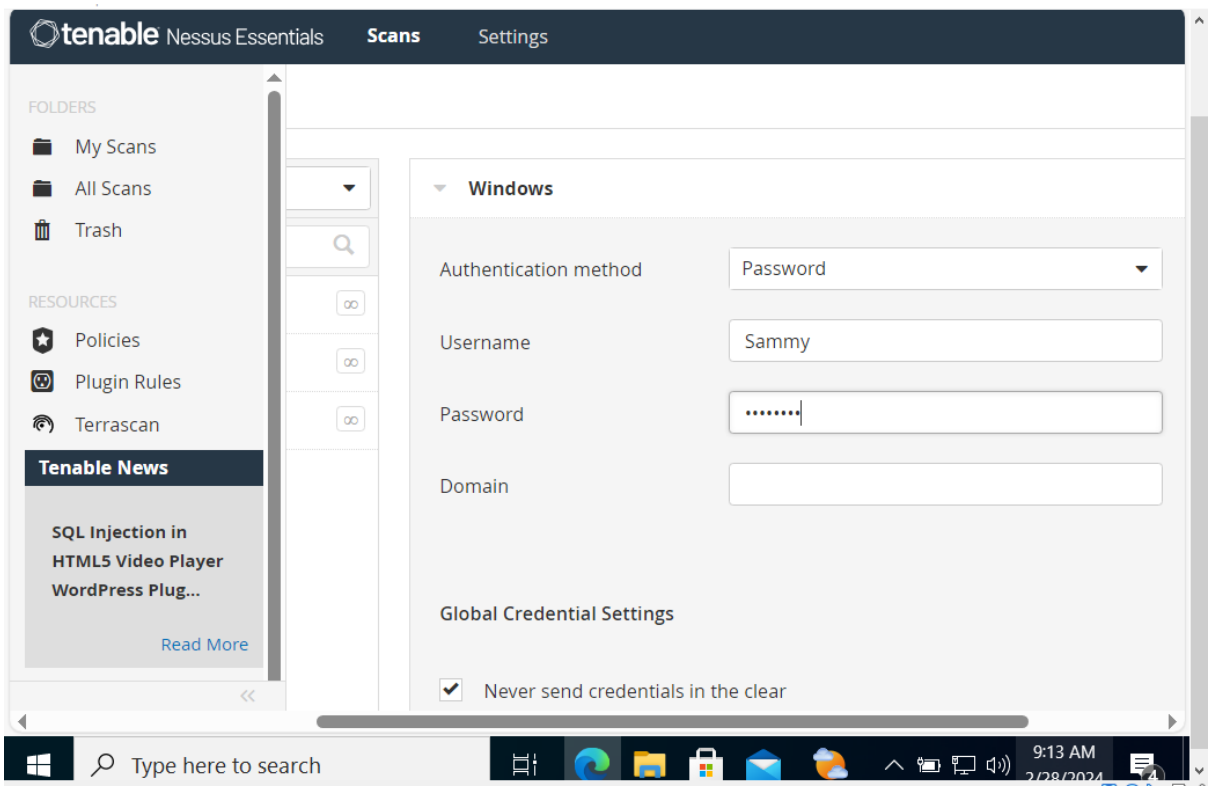
- Select the advance setting type. I the right pane under the performance options settings, set the values of max no. of concurrent TCP sessions per host and max no of concurrent TCP Sessions per scan to unlimited.



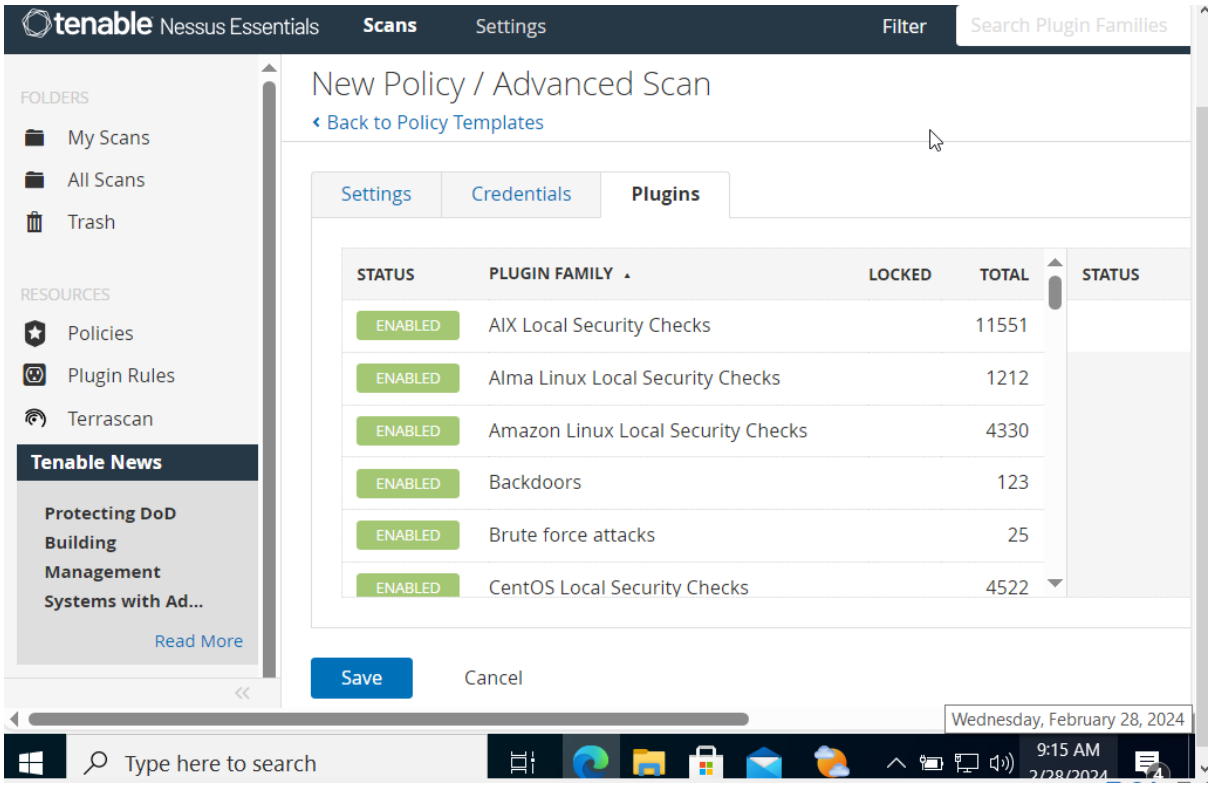
- To configure the credentials of a new policy, click the credentials tab and select windows from the options.



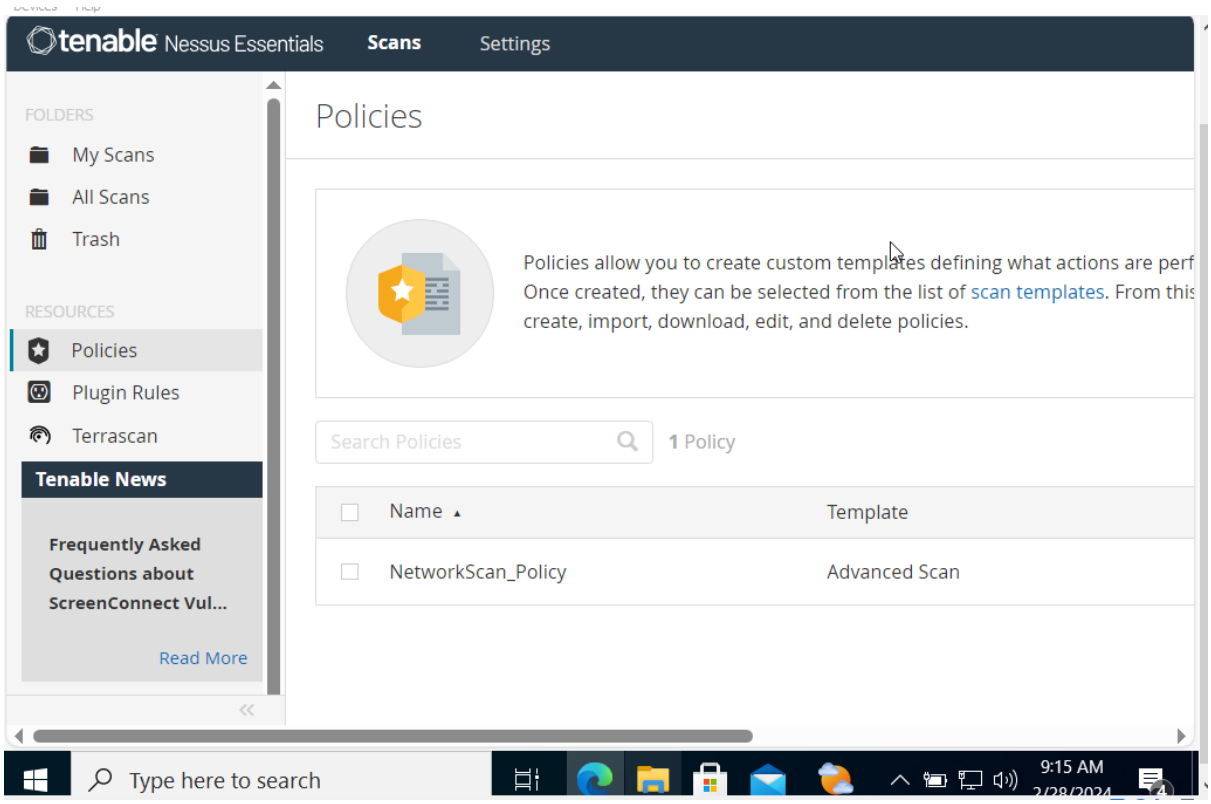
- Specify the username and password in the windows, here the specified credentials are, CEH123/qwerty@123, Note, reenter the created user account credentials admin/password if session time out notification pop up appears.



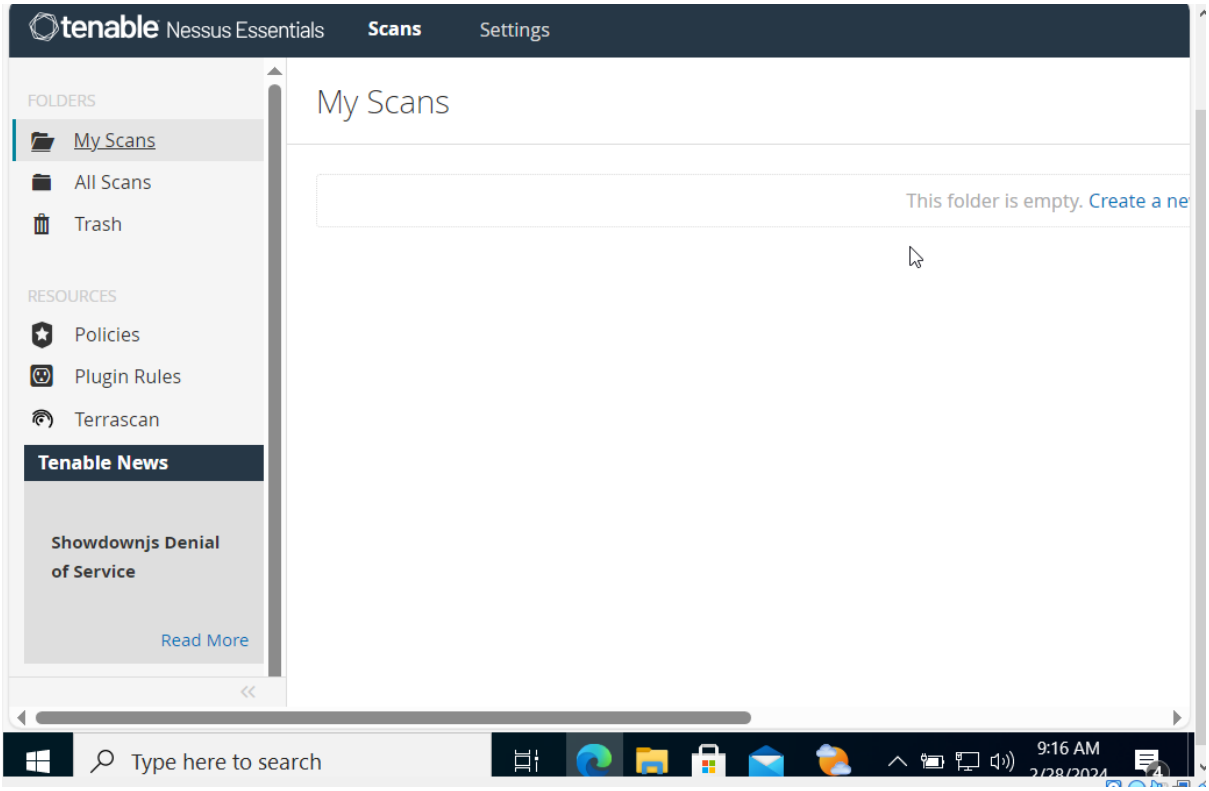
- Click the plugins tab and do not alter any of the options in this window, click the save button.



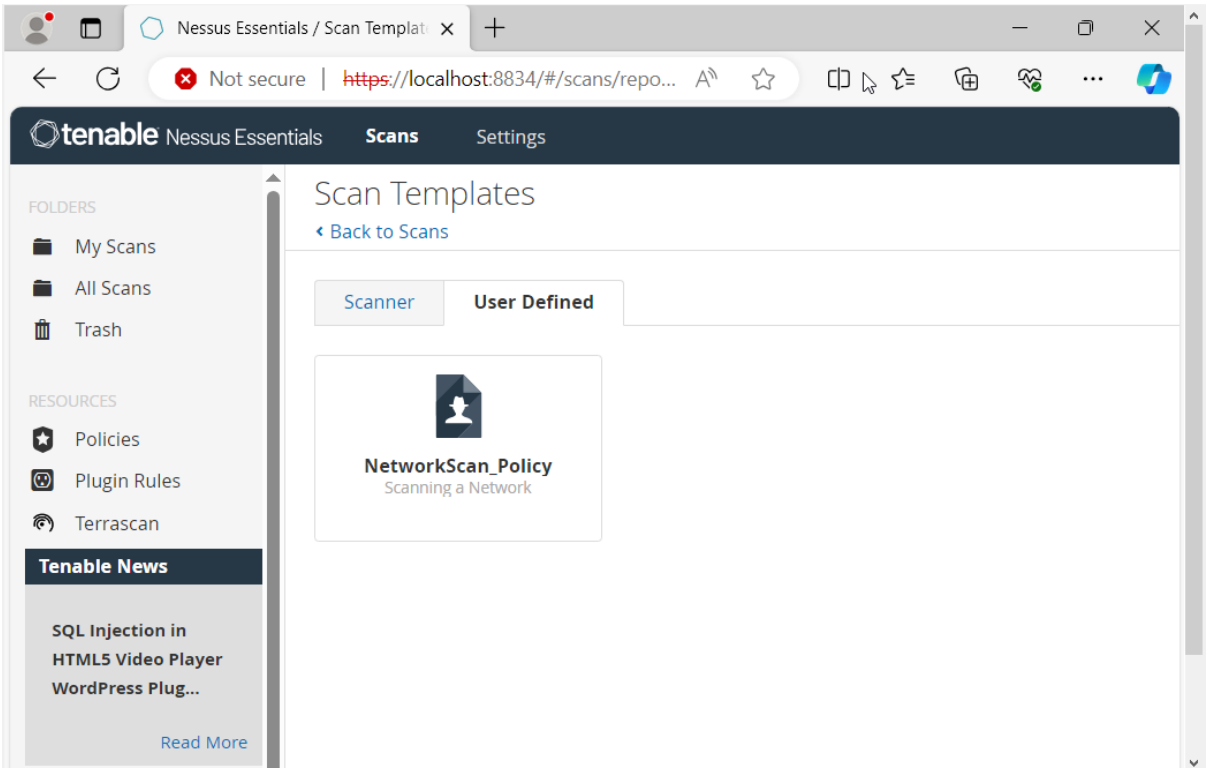
- A policy step successfully notification pop up appears, and the policy is added in the policies windows as shown.



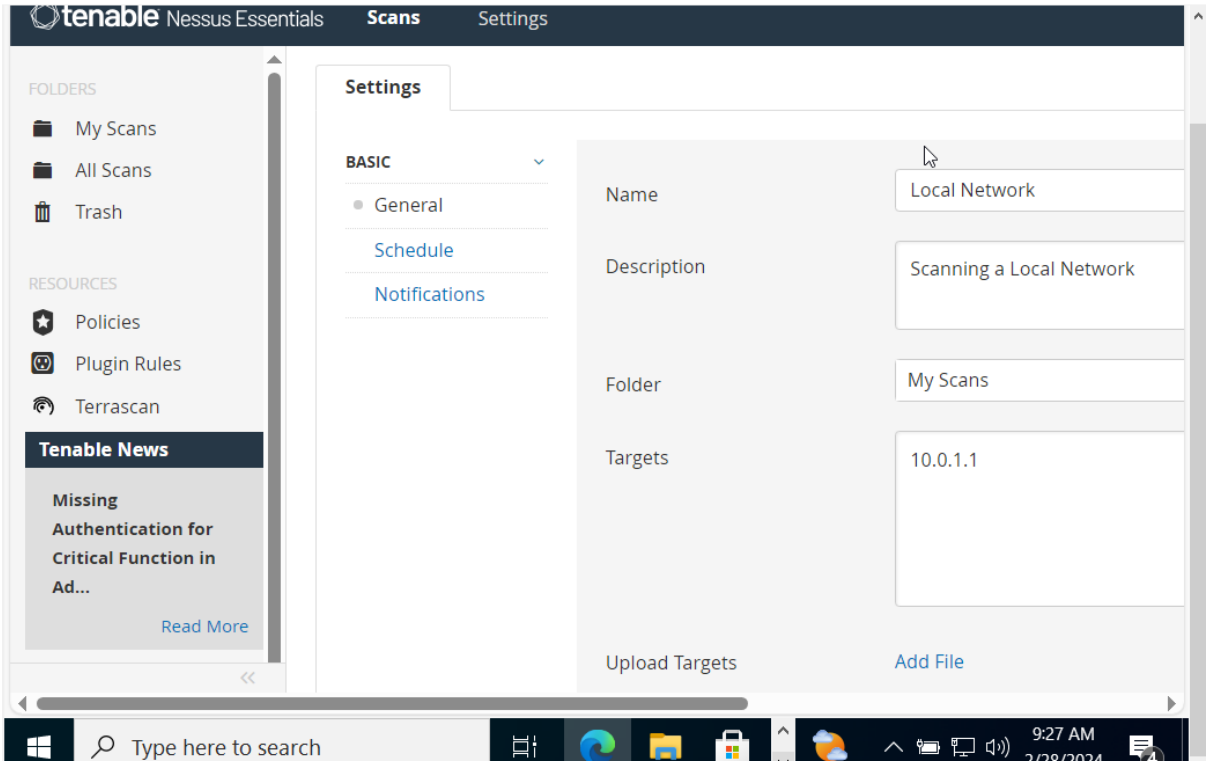
- Now click scans from the menu bar to open my scans window; click create a new scan



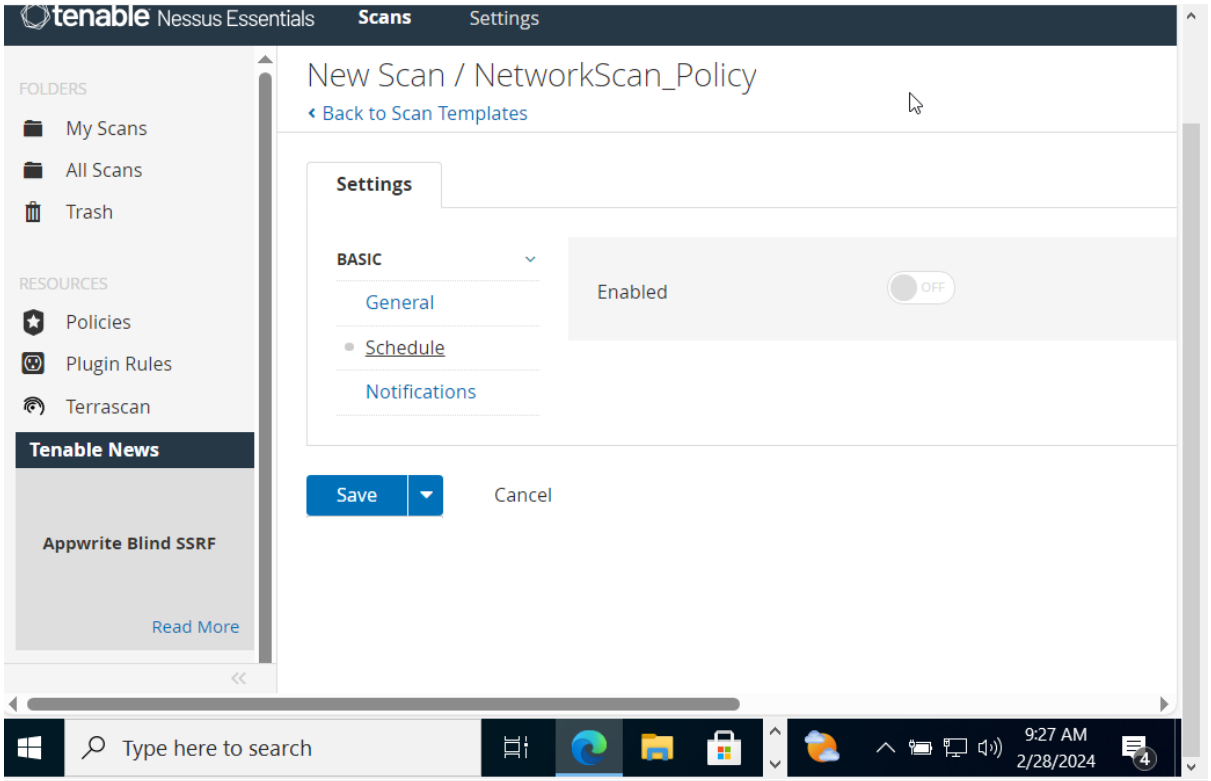
- The scans templates windows appear, click the user defined tab and select network scan policy, Note, if the Api disabled pop up appears refresh the browser and login again to the Nessus essentials using your credentials.

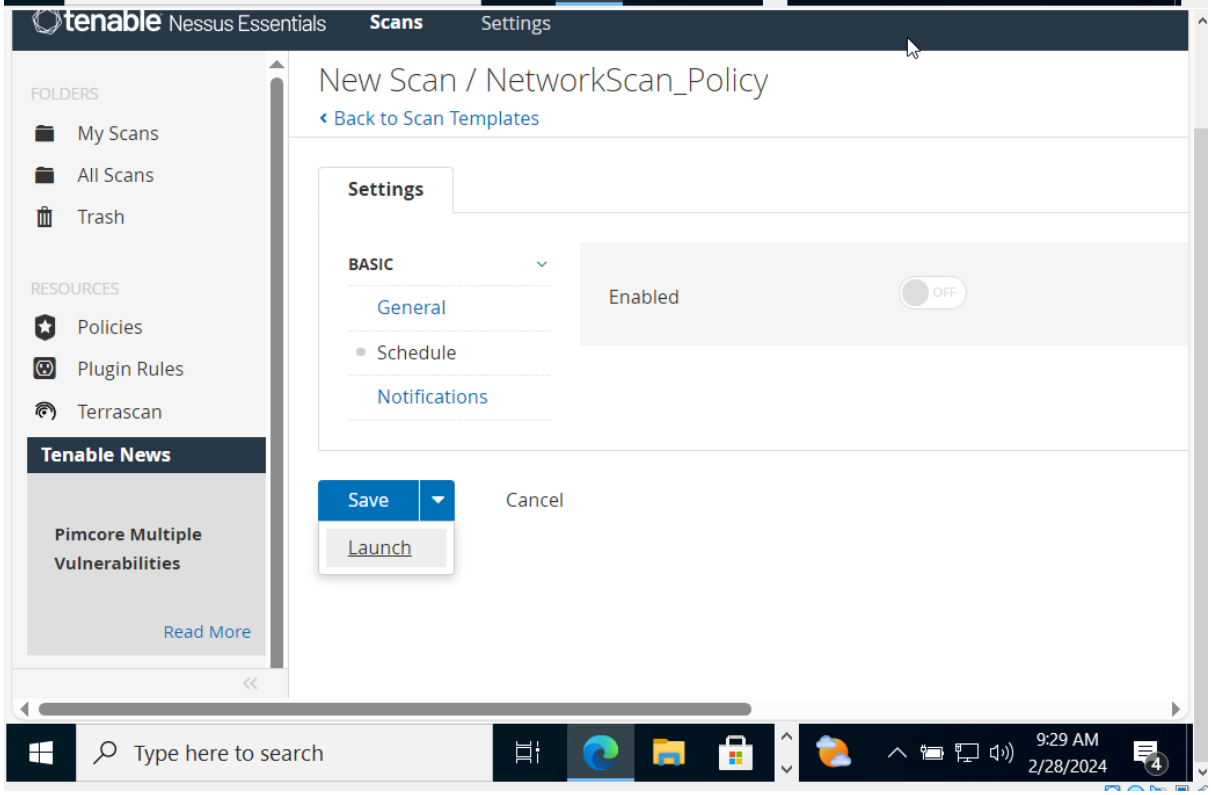


- The new scan/Network scan policy window appears, under general settings in the right pane, input the name of the scan (Here Local Network) and enter the description for the scan (here, scanning a Local network); In the targets field, enter the Ip address of the targets on which you want to perform the vulnerabilities analysis.

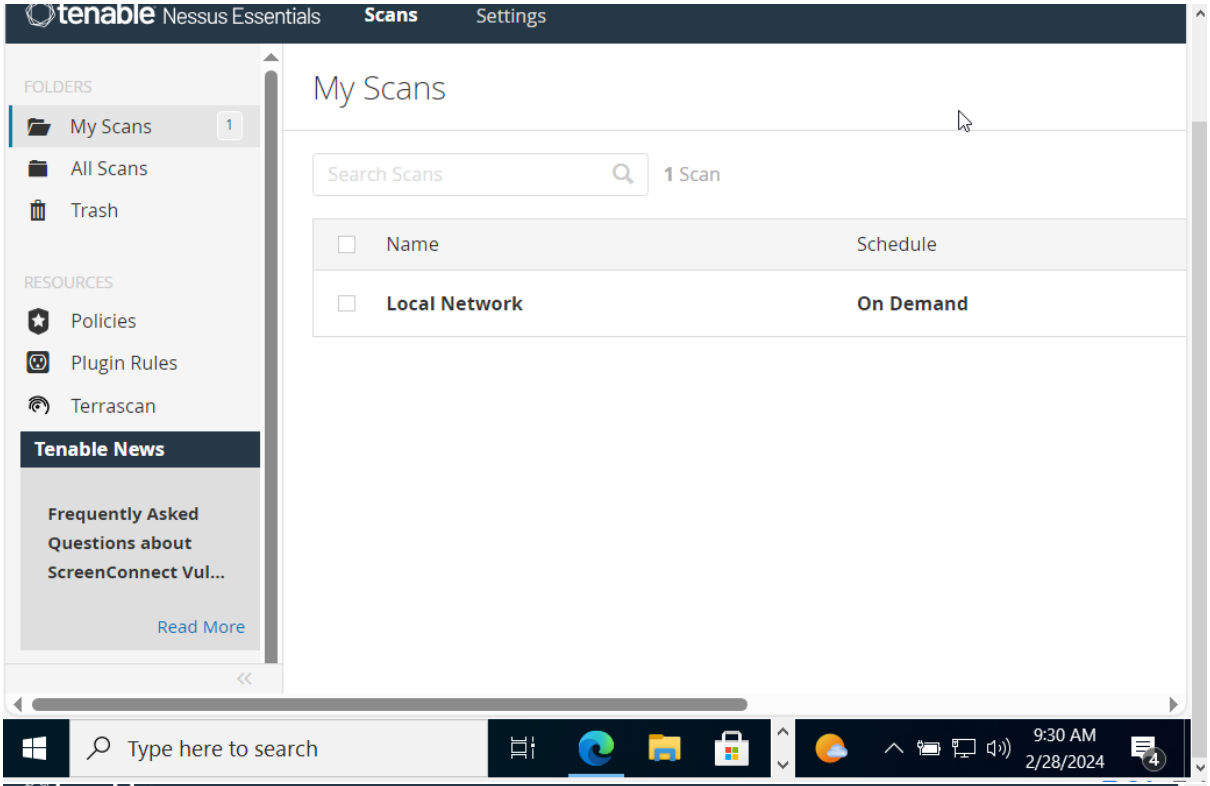


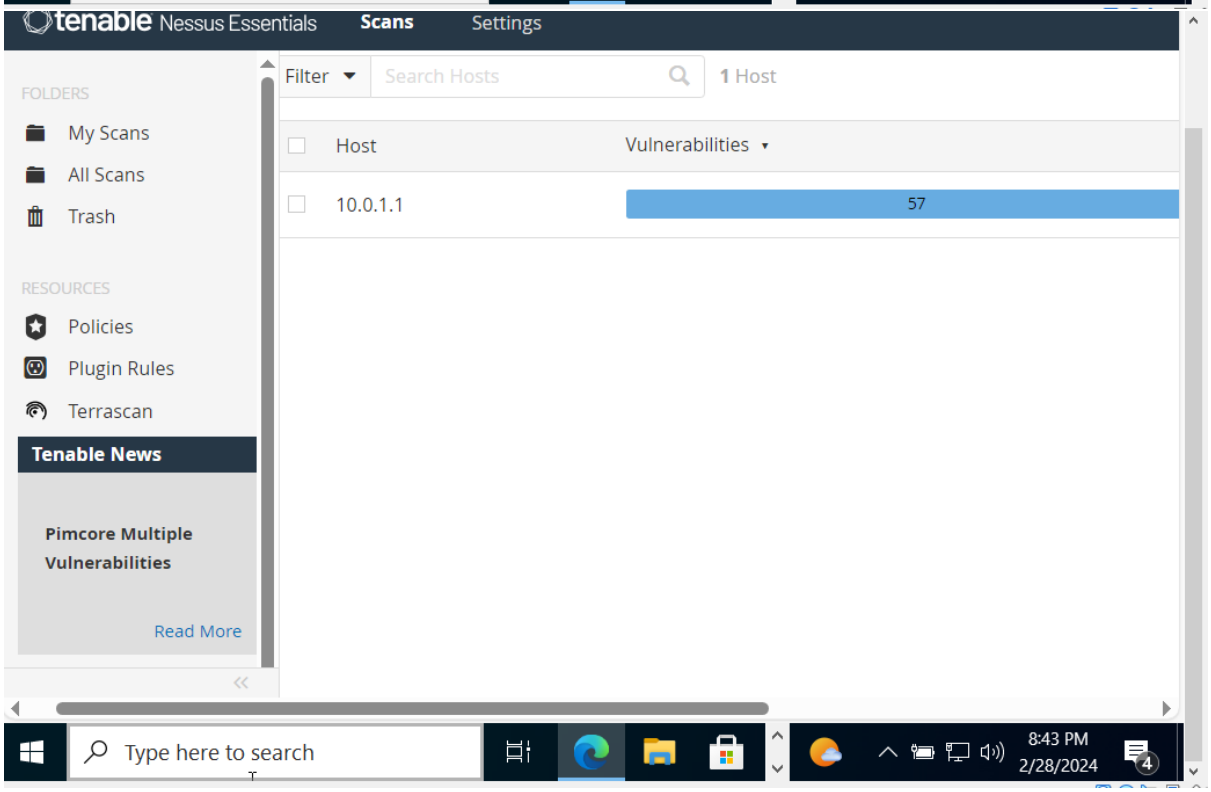
- Click schedule settings; ensure that the enabled switch is turned off, click the drop-down icon, next to the save button and select launch to start the scan.

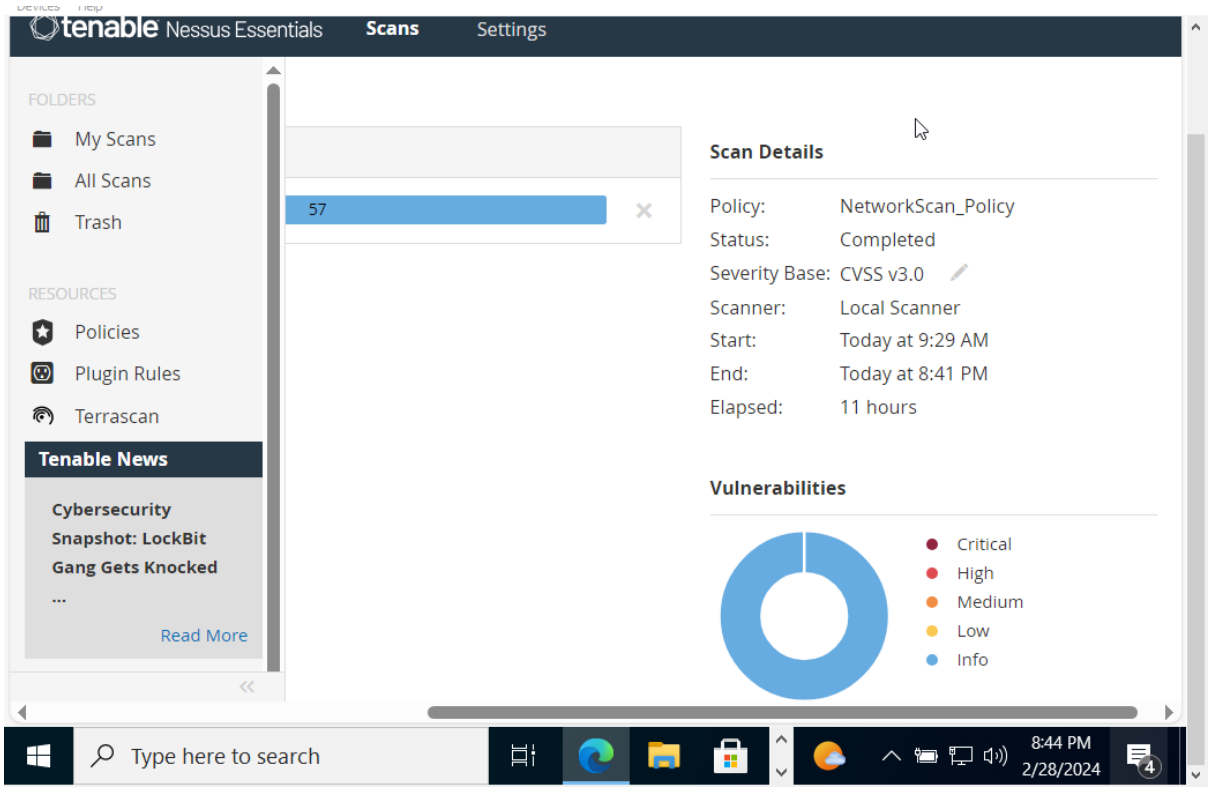

tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Appwrite Blind SSRF
Read More
New Scan / NetworkScan_Policy
Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Enabled
OFF
Save
Cancel
Type here to search
9:27 AM
2/28/2024


tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Pimcore Multiple Vulnerabilities
Read More
New Scan / NetworkScan_Policy
Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Enabled
OFF
Save
Launch
Cancel
Type here to search
9:29 AM
2/28/2024

- The scan saved and launched successfully notification pop up appears, the scan is launched and Nessus begin to scan the target.







- Click these vulnerabilities to view detailed report about each. For each instance, in this lab we are selecting the first vulnerability in the list, that is, **SNMP (Multiple Issues)**.

- The local network/SNMP (multiple Issues) window appears, displaying multiple issues in SNMP service. Click on any issue (SNMP agent default) to view its detailed information.

- The report regarding selected vulnerability SNMP Agent Default Community Name (public) appear with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

- On completing the vulnerability analysis, click Scans, and then click the recently performed scan (here, Local Network).

- In the Local Network window click the Report tab from the top-right corner, and choose a file format (here, HTML) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

- The Generate HTML Report pop-up appears: leave the Report type option on default (Executive Summary). Click Generate Report to download the report.
  Note: If the What do you want to do with Local_Network_5cfvy7.html? pop-up appears, click Save.
  Note: The file name might differ in)our lab environment

- Once the download is finished, a pop-up appear at the bottom of the browser; click Open.
- If the "How do you want to open this file?" pop-up appears, choose any browser (here, Firefox) to view the downloaded HTML file.

- The Nessus scan report appears in the Firefox web browser, as shown in the screenshot.
  Note: Screenshots might differ in your lab environment.
- You can click the Expand All option to view the detailed scan report.

- list of discovered vulnerabilities appears. You can further click on plugins (here, 41028) to view more detailed information on the vulnerability.
- Note: The result might differ in your lab environment.

- The selected plugin details are displayed, as shown in the screenshot.

- In this way, you can select a vulnerability of your choice to view the complete details.
- Once the vulnerability analysis is done, switch back to Microsoft Edge where Nessus is running and click Admin Sign Out in the top-right corner.

- Once the session is successfully logged out, a Signed out successfully. Goodbye, admin notification appears.

- This concludes the demonstration of performing vulnerability assessment using Nessus.
- Close all open windows and document all the acquired information.
- Turn off the Windows 10 virtual machine.