

VULNERABILITY SCANNING

By



DEWTON KIPROP

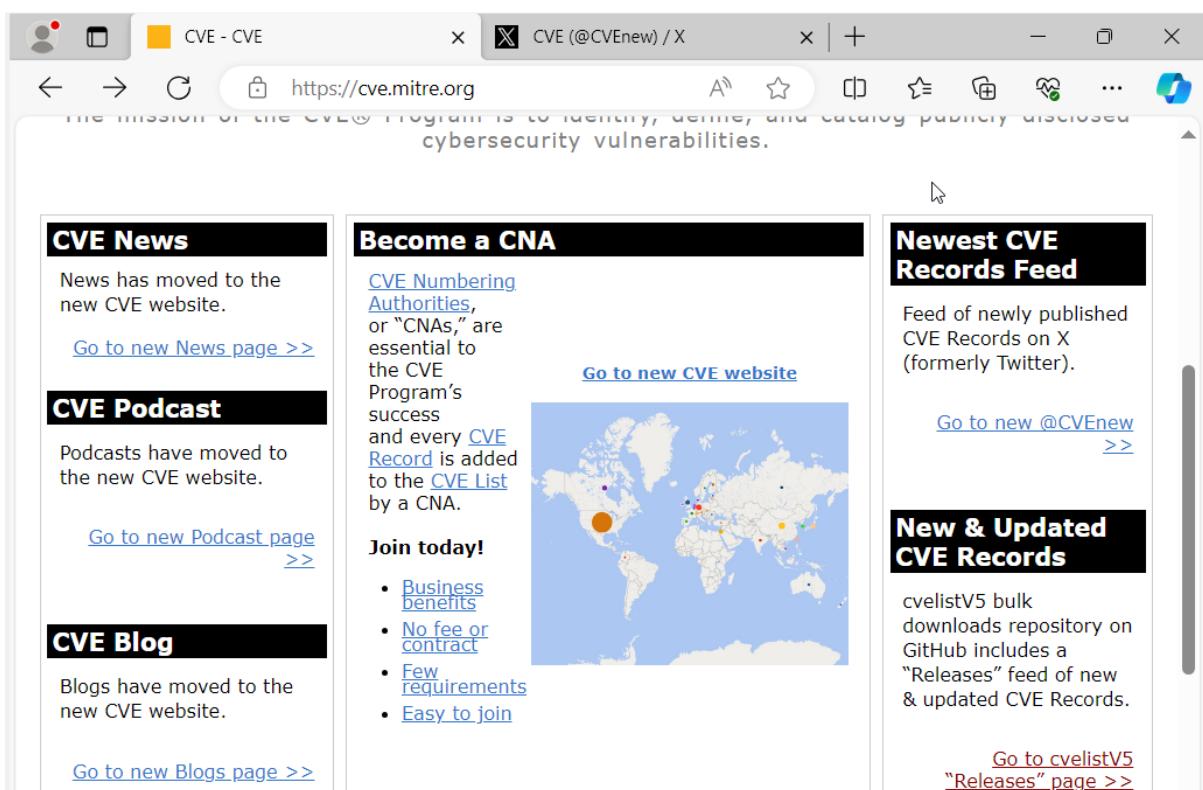
JJJJ

LAB 1

TASK:

PERFORM VULNERABILITY RESEARCH IN COMMON VULNERABILITIES AND EXPOSURES.

- With your windows 10 machine open, navigate to <https://cve.mitre.org/>. using your browser.
- In your <https://cve.mitre.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

The screenshot shows a Twitter profile for 'CVE (@CVEnew) / X'. The profile has 142K posts and 51.5K followers. Two recent tweets are visible:

- CVE @CVEnew · Jan 22, 2023**: CVE-2023-24059 Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023. cve.mitre.org/cgi-bin/cvenam...
- CVE @CVEnew · May 10, 2021**: CVE-2021-32471 Insufficient input validation in the Marvin Minsky 1967 implementation of the Universal Turing Machine allows program users to execute arbitrary code via crafted data. For example, a tape head may have

A blue banner at the bottom of the profile page says 'Don't miss what's happening'.

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

The screenshot shows the 'Search CVE List' page on the MITRE website. The URL is https://cve.mitre.org/cve/search_cve_list.html. A yellow banner at the top states: 'Attention: CVE Records now include product versions & more on the www.cve.org website. Learn about [CVE JSON 5.0](#)'.

The search bar contains 'CVE-2023-24059' and a 'Submit' button is visible below it.

At the bottom of the page, there is a footer with links: Site Map | Terms of Use | Manage Cookies | Cookie Notice | Privacy Policy | Contact Us | Follow CVE. It also includes social media icons for Twitter, LinkedIn, and GitHub.

- 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.

The screenshot shows a web browser window with the title "CVE - Search Results". The URL is <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword...>. A red banner at the top reads: "NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024. New CVE List download format is available now." Below the banner, the page displays "HOME > CVE > SEARCH RESULTS". The main content is titled "Search Results" and shows a message: "There are 1 CVE Records that match your search." A table follows, with columns "Name" and "Description". The single entry is CVE-2023-24059, which is described as "Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023." At the bottom right of the page is a "BACK TO TOP" link.

The screenshot shows a web browser window with the title "CVE - CVE-2023-24059". The URL is <https://cve.mitre.org/cgi-bin/cvename.cgi?name=...>. The page displays detailed information for CVE-2023-24059. The "CVE-ID" section shows the ID and links to the National Vulnerability Database (NVD). The "Description" section contains the text: "Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023." The "References" section lists several URLs, all starting with "MISC:". The "Assigning CNA" section shows "MITRE Corporation". The "Date Record Created" section shows "20230122". A disclaimer at the bottom states: "Disclaimer: The record creation date may reflect when the CVE ID was alloc".

- 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.

This is a screenshot of the CVE-2023-24059 detail page on cve.mitre.org. The page has a header with two tabs: 'CVE - CVE-2023-24059' and 'CVE (@CVEnew) / X'. The main content area has several sections:

- Phase (Legacy)**: Assigned (20230122)
- Votes (Legacy)**
- Comments (Legacy)**
- Proposed (Legacy)**: N/A

A note below the 'Assigned' section states: "This is a record on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities." There is a search bar with the keyword 'SMB' and a 'Submit' button. Below the search bar, it says: "You can also search by reference using the [CVE Reference Maps](#)." At the bottom, there is a link: "For More Information: [CVE Request Web Form](#) (select 'Other' from dropdown)". A 'BACK TO TOP' link is at the very bottom right.

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

This is a screenshot of the CVE Search Results page on cve.mitre.org. The title bar shows 'CVE - Search Results'. The main content area displays a message: "There are 545 CVE Records that match your search." Below this, there is a table with two columns: 'Name' and 'Description'.

Name	Description
CVE-2024-22705	An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strdup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled.
CVE-2024-0565	An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service.
CVE-2023-6610	An out-of-bounds read vulnerability was found in smb2_dump_detail in fs/smb/client/smb2ops.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.
CVE-2023-6606	An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.
CVE-2023-6381	Improper input validation vulnerability in Newsletter Software SuperMailer affecting version 11.20.0.2204. An attacker could exploit this vulnerability by sending a malicious configuration file (file with SMB extension) to a user via a link or email attachment and persuade the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to crash the application when attempting to load the malicious file.
CVE-2023-5345	A use-after-free vulnerability in the Linux kernel's fs/smb/client component can be

- 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.

The screenshot shows a web browser window displaying the details of a specific vulnerability. The URL in the address bar is <https://cve.mitre.org/cgi-bin/cvename.cgi?name=...>. The main content area is organized into several sections:

- CVE-ID**: Shows **CVE-2024-22705** and a link to [Learn more at National Vulnerability Database \(NVD\)](#). Below this are links for CVSS Severity Rating, Fix Information, Vulnerable Software Versions, SCAP Mappings, and CPE Information.
- Description**: Describes an issue discovered in ksmbd in the Linux kernel before 6.6.10. It states that `smb2_get_data_area_len` in `fs/smb/server/smb2misc.c` can cause an `smb_strndup_from_utf16` out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled.
- References**: Notes that references are provided for convenience. It lists two items:
 - [MISC:https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.6.10](https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.6.10)
 - [MISC:https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d10c77873ba1e9e6b91905018e29e196fd5f863d](https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d10c77873ba1e9e6b91905018e29e196fd5f863d)
- Assigning CNA**: MITRE Corporation
- Date Record Created**: 20240111. A disclaimer notes that the record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this

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.

Devices Help

NVD - Home

https://nvd.nist.gov

Here is where you can read the NVD legal disclaimer.

Last 20 Scored Vulnerability IDs & Summaries

	CVSS Severity
CVE-2023-4911 - A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when lau... read CVE-2023-4911	
Published: October 03, 2023; 2:15:10 PM -0400	
V3.1: 7.8 HIGH	
CVE-2023-45868 - The Learning Module in ILIAS 7.25 (2023-09-12 release) allows an attacker (with basic user privileges) to achieve a high-impact Directory Traversal attack on confidentiality and availability. By exploiting this network-based vulnerability, the att... read CVE-2023-45868	
Published: October 26, 2023; 11:15:08 AM -0400	

Created September 20, 2022, Updated February 13, 2024

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

CVE-2023-4911 Detail

Description

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

Severity	CVSS Version 3.x	CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Red Hat, Inc. **Base Score: 7.8 HIGH**

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://packetstormsecurity.com/files/174986/glibc-ld.so-Local-Privilege-Escalation.html	Exploit Third Party Advisory
http://packetstormsecurity.com/files/176288/Glibc-Tunables-Privilege-Escalation.html	Exploit Third Party Advisory
http://seclists.org/fulldisclosure/2023/Oct/11	Exploit Mailing List

Devices Help

NVD - CVE-2023-4911

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
GNU C Library Buffer Overflow Vulnerability	11/21/2023	12/12/2023	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-787	Out-of-bounds Write	NIST
CWE-122	Heap-based Buffer Overflow	Red Hat, Inc.

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1 ([hide](#))

cpe:2.3:a:gnu:glibc:*:*:*:*:*:*	From (including)	Up to (excluding)
---------------------------------	---------------------	----------------------

Show Matching CPE(s) ▾

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

Jracie Vivi VirtualBox

Devices Help

NVD - CVE-2023-4911

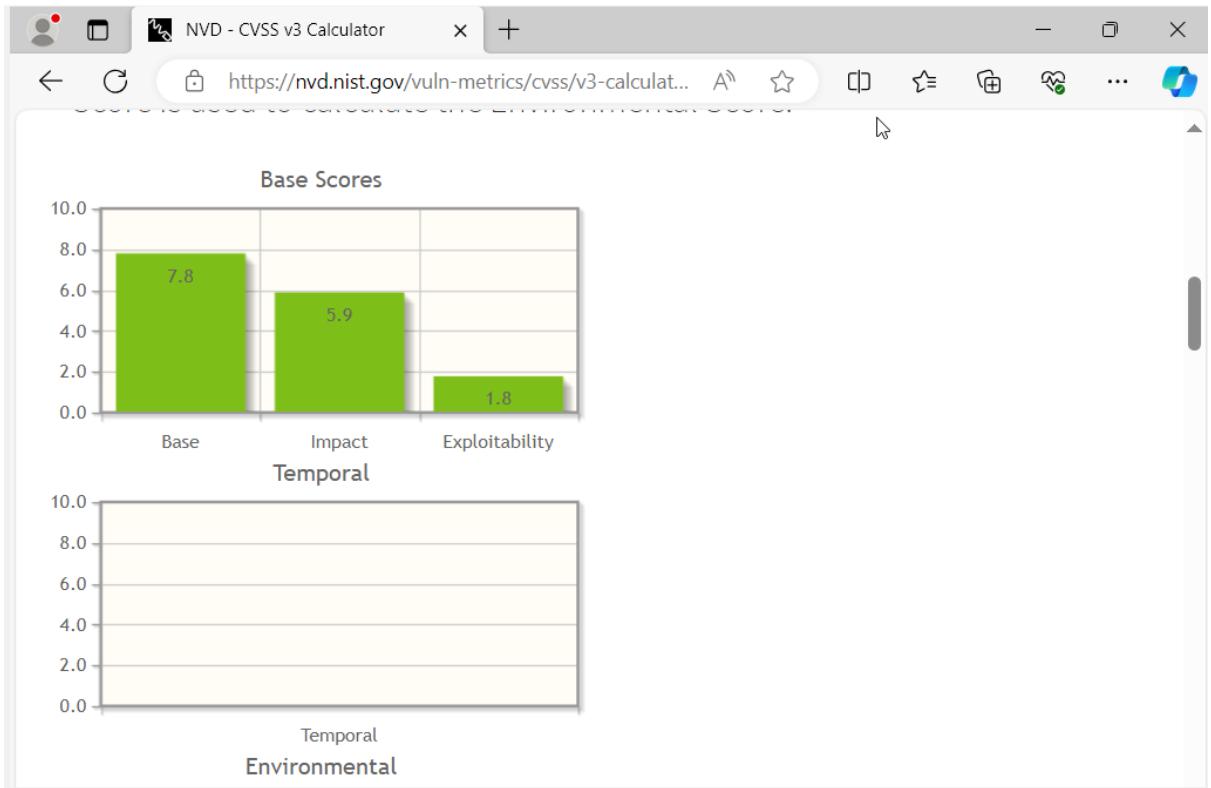
Description

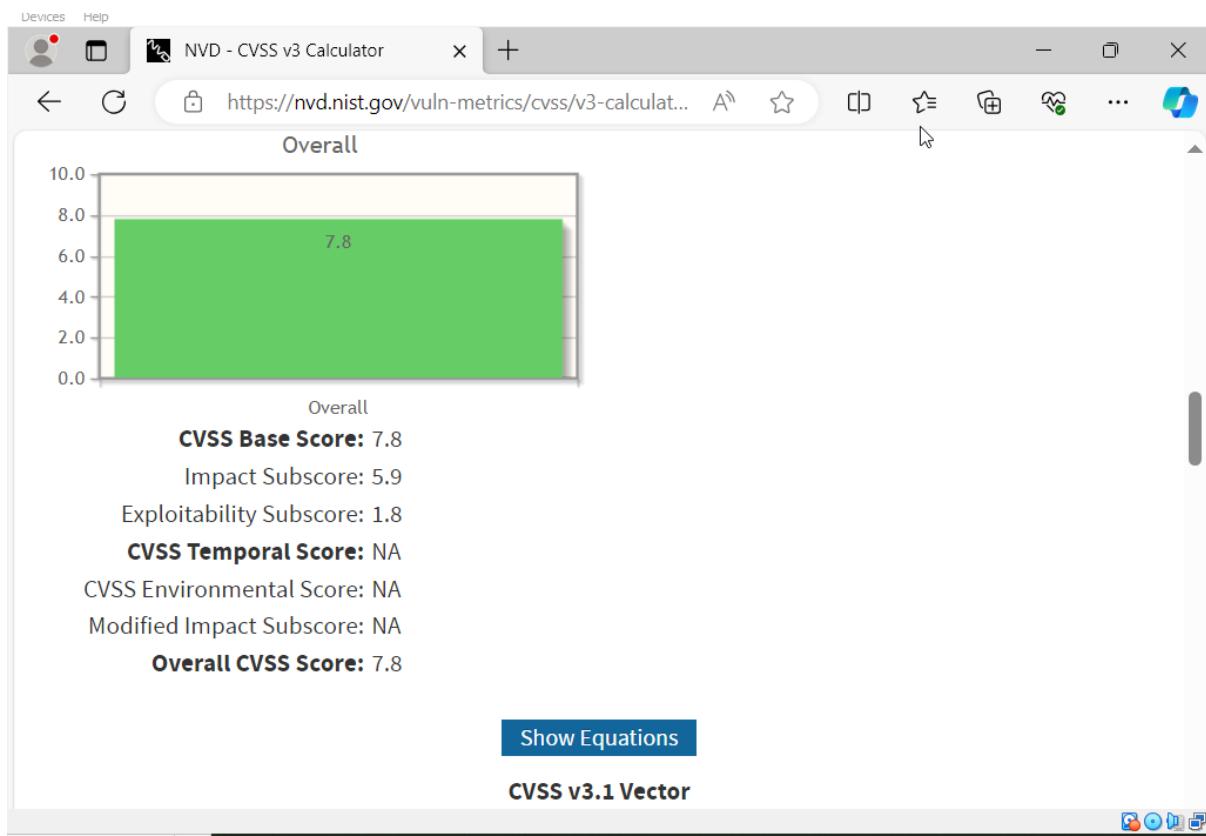
A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
CNA: Red Hat, Inc.	Base Score: 7.8 HIGH	
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

- 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.

The screenshot shows the "Base Score Metrics" configuration page of the NVD - CVSS v3 Calculator. The page is divided into sections for different metrics:

- Exploitability Metrics**
 - Attack Vector (AV)***: Local (AV:L) is selected.
 - Attack Complexity (AC)***: Low (AC:L) is selected.
 - Privileges Required (PR)***: Low (PR:L) is selected.
 - User Interaction (UI)***: None (UI:N) is selected.
 - Scope (S)***: Unchanged (S:U) is selected.
- Impact Metrics**
 - Confidentiality Impact (C)***: None (C:N) is selected.

A tooltip for the Confidentiality Impact section states: "This metric measures the impact to the...".

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)

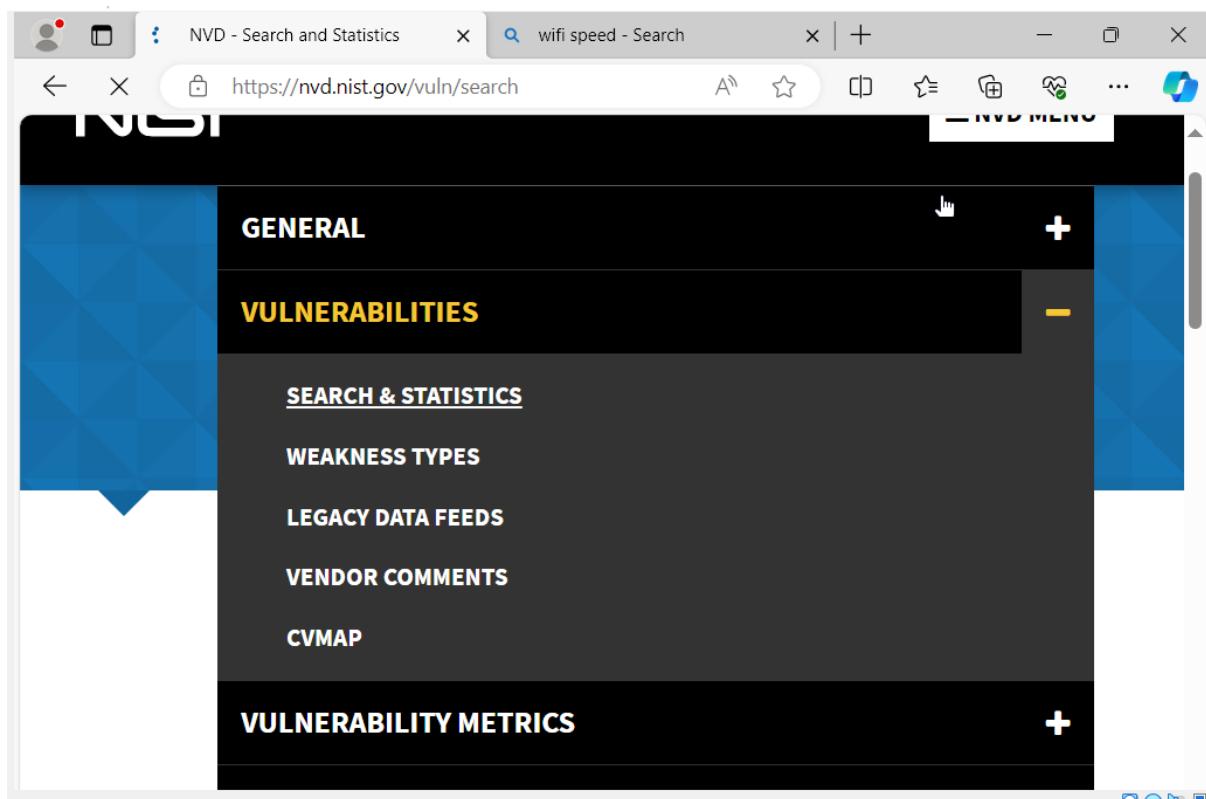
Not Defined (MS:X)	Unchanged (MS:U)	Changed (MS:C)

Impact Metrics

The screenshot shows the NVD - CVSS v3 Calculator interface. At the top, there are three tabs: "Not Defined (MS:X)", "Unchanged (MS:U)", and "Changed (MS:C)". Below these tabs, the title "Impact Metrics" is displayed. Under "Impact Metrics", there are three sections: "Confidentiality Impact (MC)", "Integrity Impact (MI)", and "Availability Impact (MA)". Each section has four buttons: "Not Defined (MC:X)", "None (MC:N)", "Low (MC:L)", and "High (MC:H)". Below these sections, the title "Impact Subscore Modifiers" is shown. Under "Impact Subscore Modifiers", there are three sections: "Confidentiality Requirement (CR)", "Integrity Requirement (IR)", and "Availability Requirement (AR)". Each section has four buttons: "Not Defined (CR:X)", "Low (CR:L)", "Medium (CR:M)", and "High (CR:H)".

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

The screenshot shows the NVD - Home page. The top navigation bar includes links for "Input", "Devices", and "Help". The main content area features the NIST logo and a "NVD MENU" button with a three-bar icon. Below the menu, there are several expandable sections: "GENERAL", "VULNERABILITIES", "VULNERABILITY METRICS", "PRODUCTS", "NOTICE", "DEVELOPERS", and "CONTACT NVD". A yellow sidebar on the left contains the text "NIST is cur..." and "CONTACT NVD". The address bar shows the URL "https://nvd.nist.gov/#" and a search term "wifi speed - Search". A message at the bottom states "An official website of the United States government [Here's how you know](#)".



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

A screenshot of the NVD - Search and Statistics search interface. The URL in the address bar is https://nvd.nist.gov/vuln/search. The interface includes a header with 'Devices' and 'Help' links, and a search bar containing 'Nmap'. Below the search bar are several filter sections:

- Results Type**: Radio buttons for 'Overview' (selected) and 'Statistics'.
- Keyword Search**: A text input field containing 'Nmap' and a checkbox for 'Exact Match'.
- Search Type**: Radio buttons for 'All Time' (selected) and 'Last 3 Months'.
- Contains HyperLinks**: Checkboxes for 'CISA Known Exploited Vulnerabilities', 'US-CERT Technical Alerts', 'US-CERT Vulnerability Notes', and 'OVAL Queries'.

At the bottom of the search interface are two buttons: 'Search' (highlighted in blue) and 'Reset'.

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

Devices Help

Vuln ID	Summary	CVSS Severity
CVE-2023-48310	TestingPlatform is a testing platform for Internet Security Standards. Prior to version 2.1.1, user input is not filtered correctly. Nmap options are accepted. In this particular case, the option to create log files is accepted in addition to a host name (and even without). A log file is created at the location specified. These files are created as root. If the file exists, the existing file is being rendered useless. This can result in denial of service. Additionally, input for scanning can be any CIDR blocks passed to nmap. An attacker can scan 0.0.0.0/0 or even local networks. Version 2.1.1 contains a patch for this issue.	V3.1: 7.5 HIGH V2.0:(not available)
CVE-2022-48252	The jokob-sk/Pi.Alert fork (before 22.12.20) of Pi.Alert allows Remote Code Execution via nmap_scan.php (scan	V3.1: 9.8 CRITICAL V2.0:(not available)

NVD - CVE-2023-48310

https://nvd.nist.gov/vuln/detail/CVE-2023-48310

Enter Immersive Reader (F9)

CVE-2023-48310 Detail

Description

TestingPlatform is a testing platform for Internet Security Standards. Prior to version 2.1.1, user input is not filtered correctly. Nmap options are accepted. In this particular case, the option to create log files is accepted in addition to a host name (and even without). A log file is created at the location specified. These files are created as root. If the file exists, the existing file is being rendered useless. This can result in denial of service. Additionally, input for scanning can be any CIDR blocks passed to nmap. An attacker can scan 0.0.0.0/0 or even local networks. Version 2.1.1 contains a patch for this issue.

Severity

CVSS Version 3.x CVSS Version 2.0

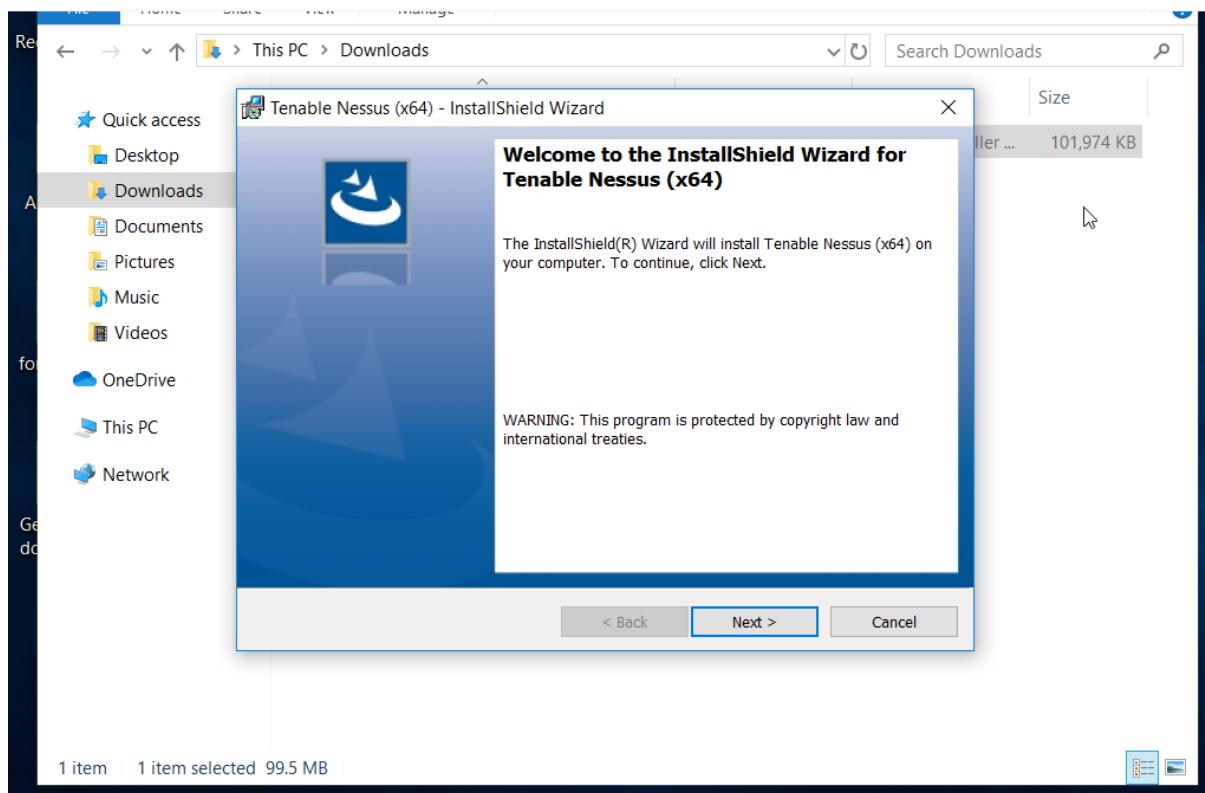
CVSS 3.x Severity and Metrics:

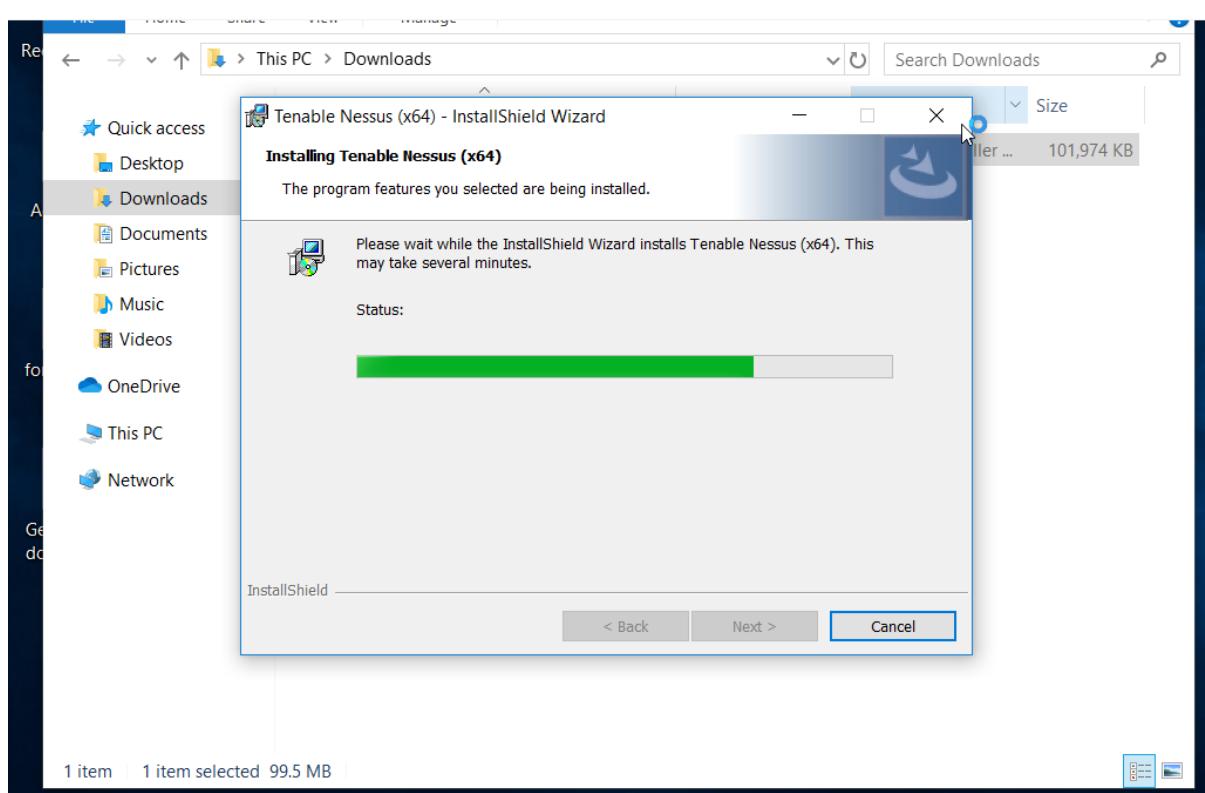
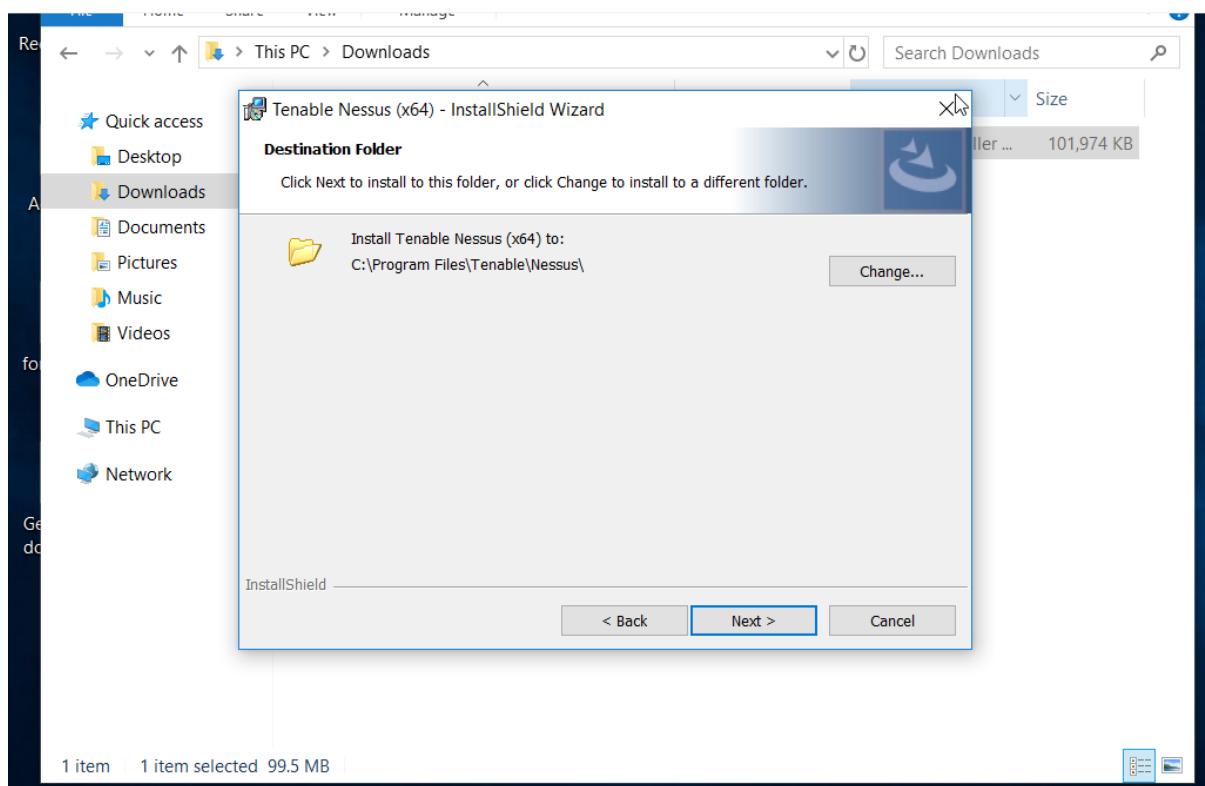
- Likewise, you can search for other targets services for the underlined vulnerability in the search Vulnerability database section.

LAB :2

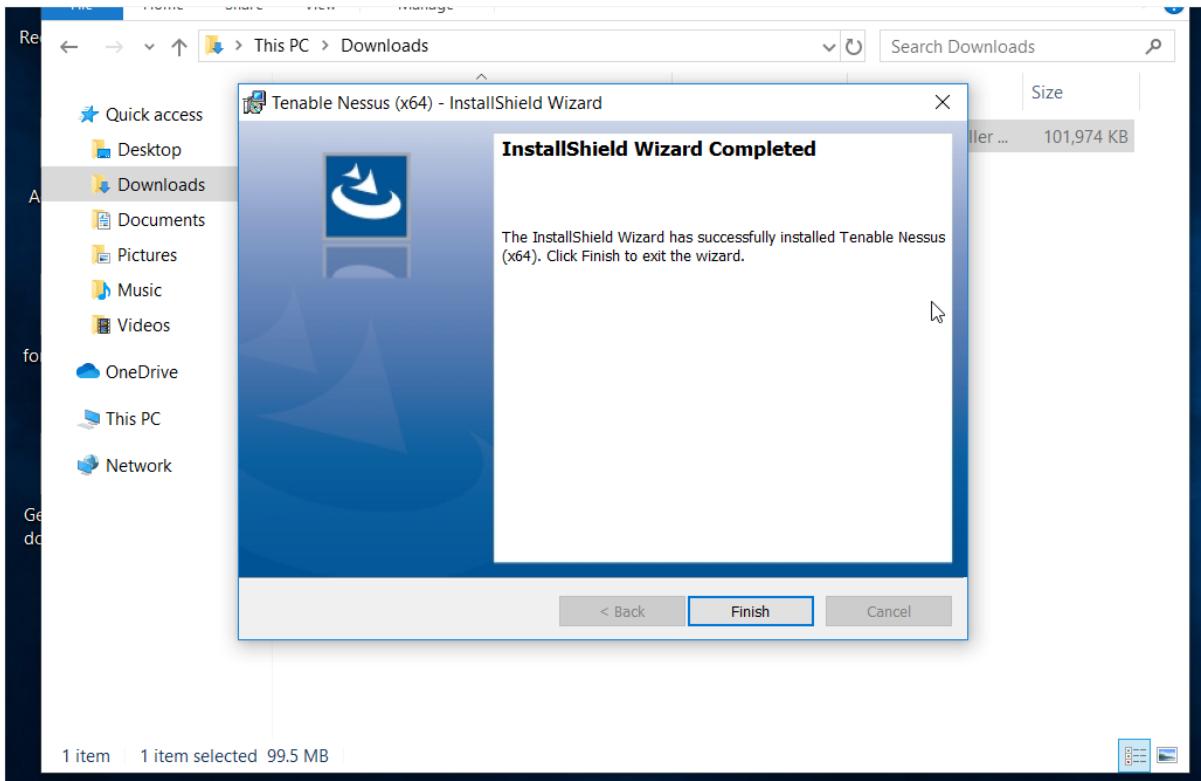
TASK: Perform Vulnerability Scanning using Nessus

- Installation of Nessus in windows 10

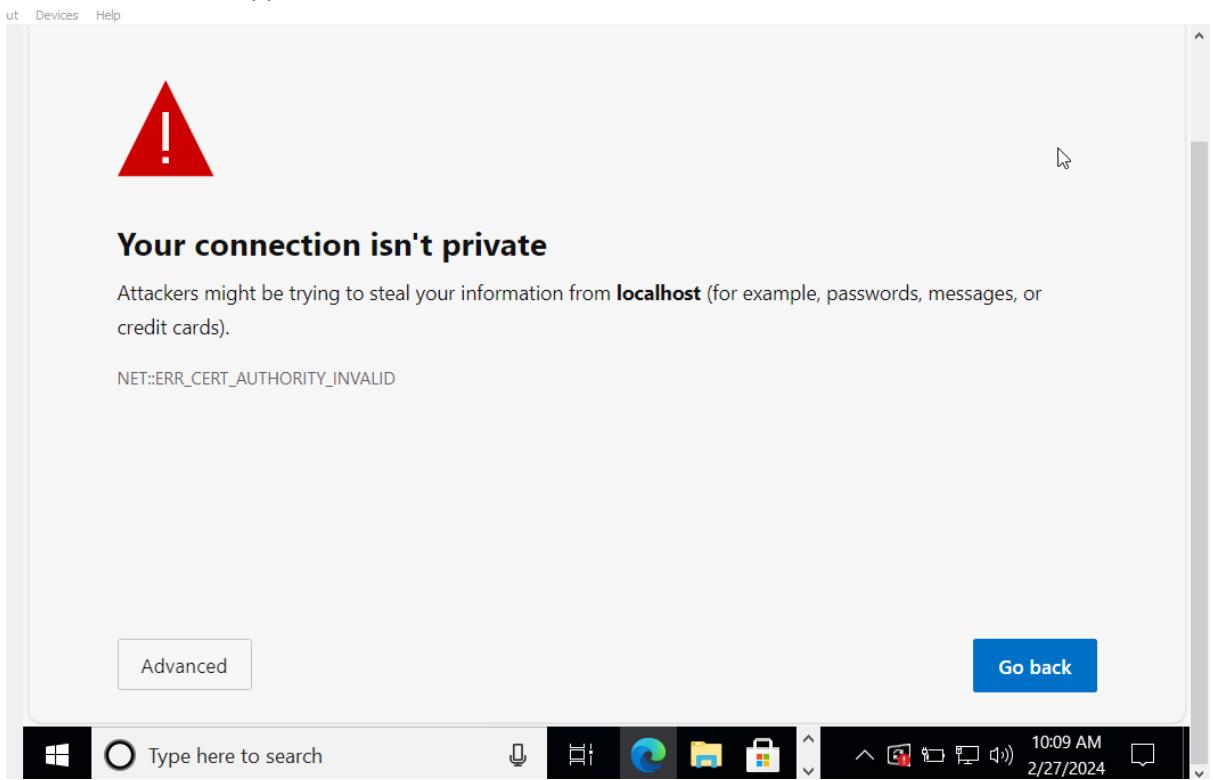




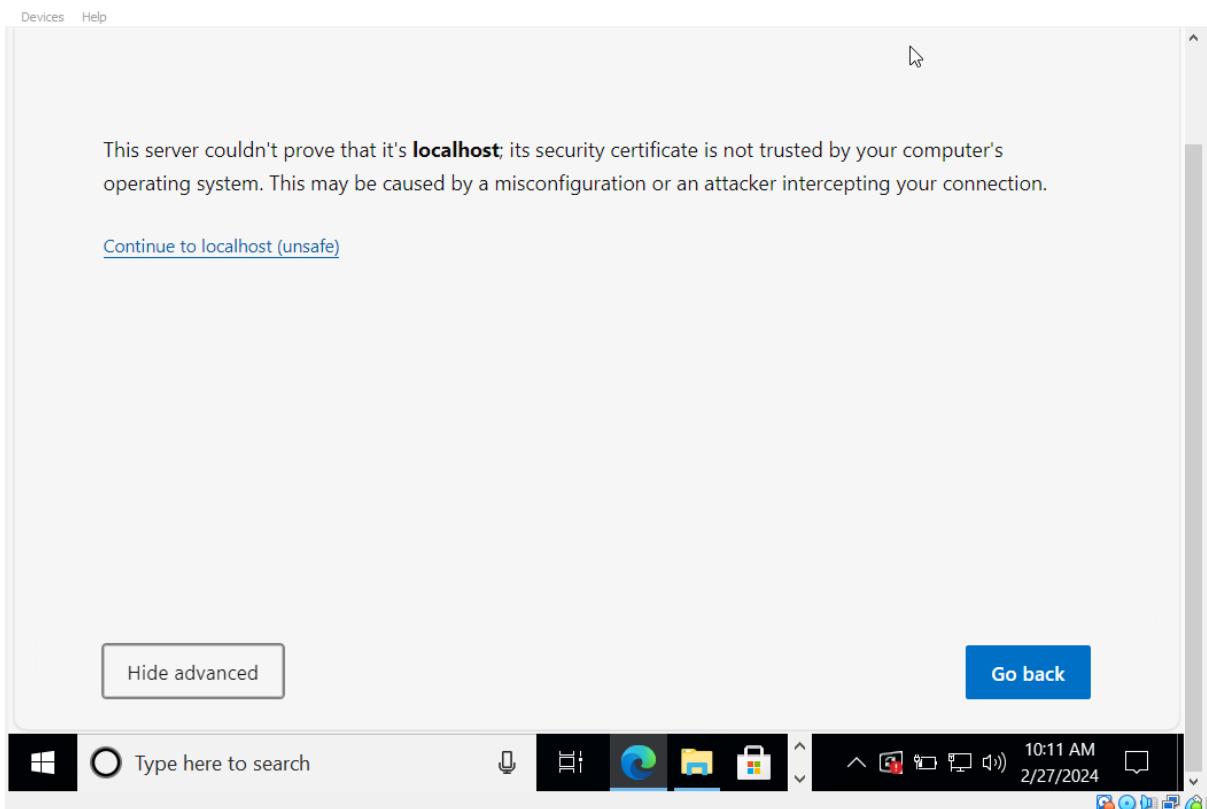
- Click finish and finish with installation



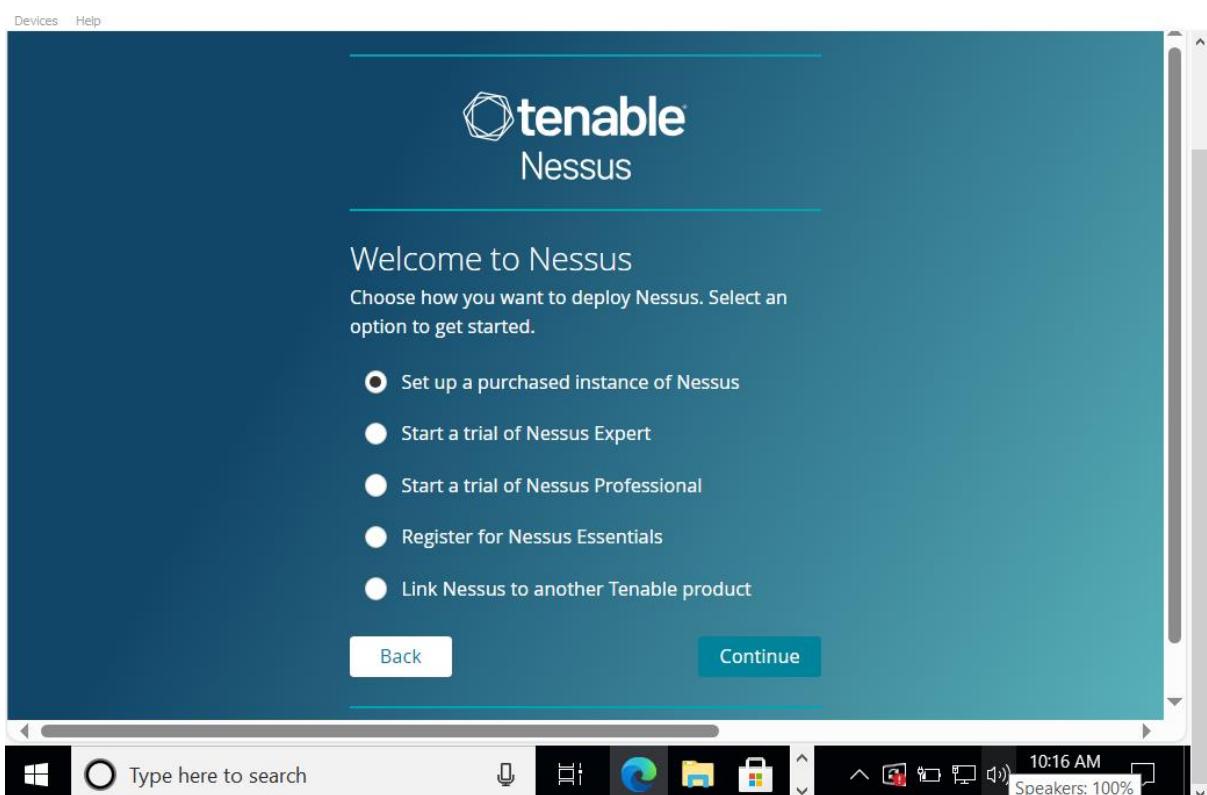
- Next step with start by launching Nessus
- When this window appear in the browser, click on advance



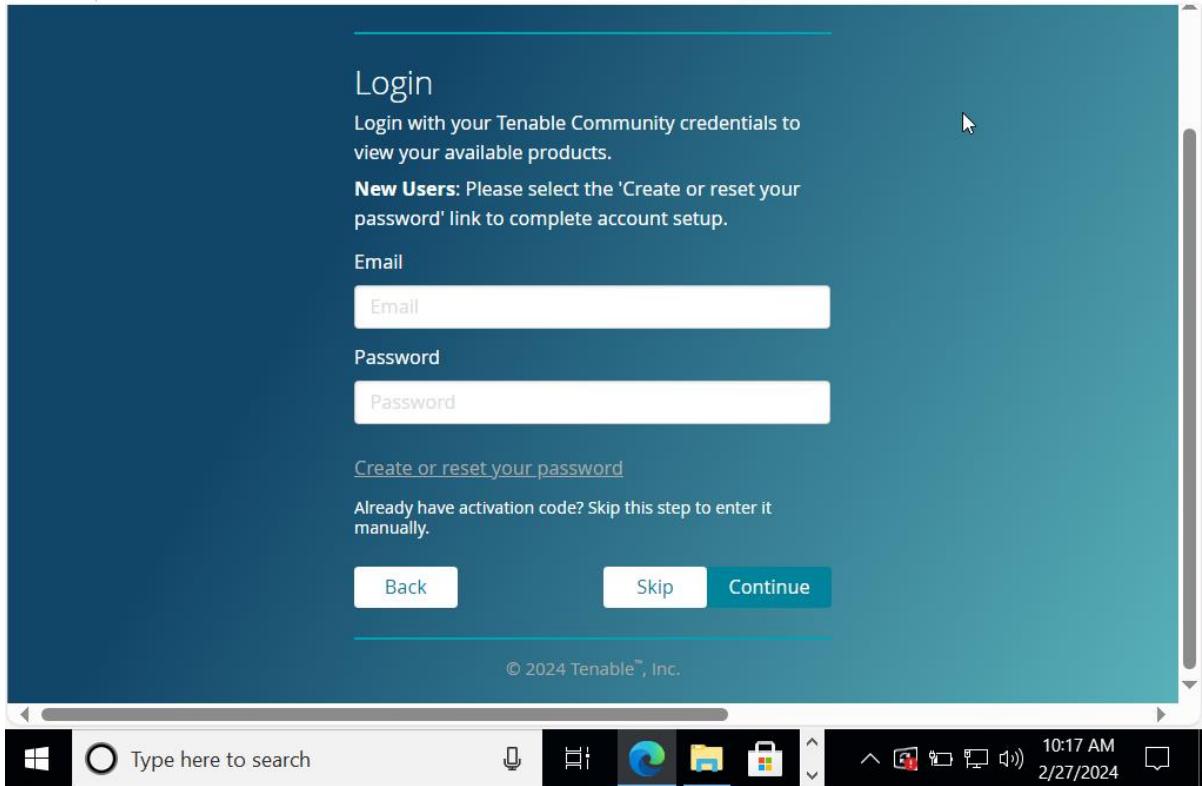
- Click continue to localhost



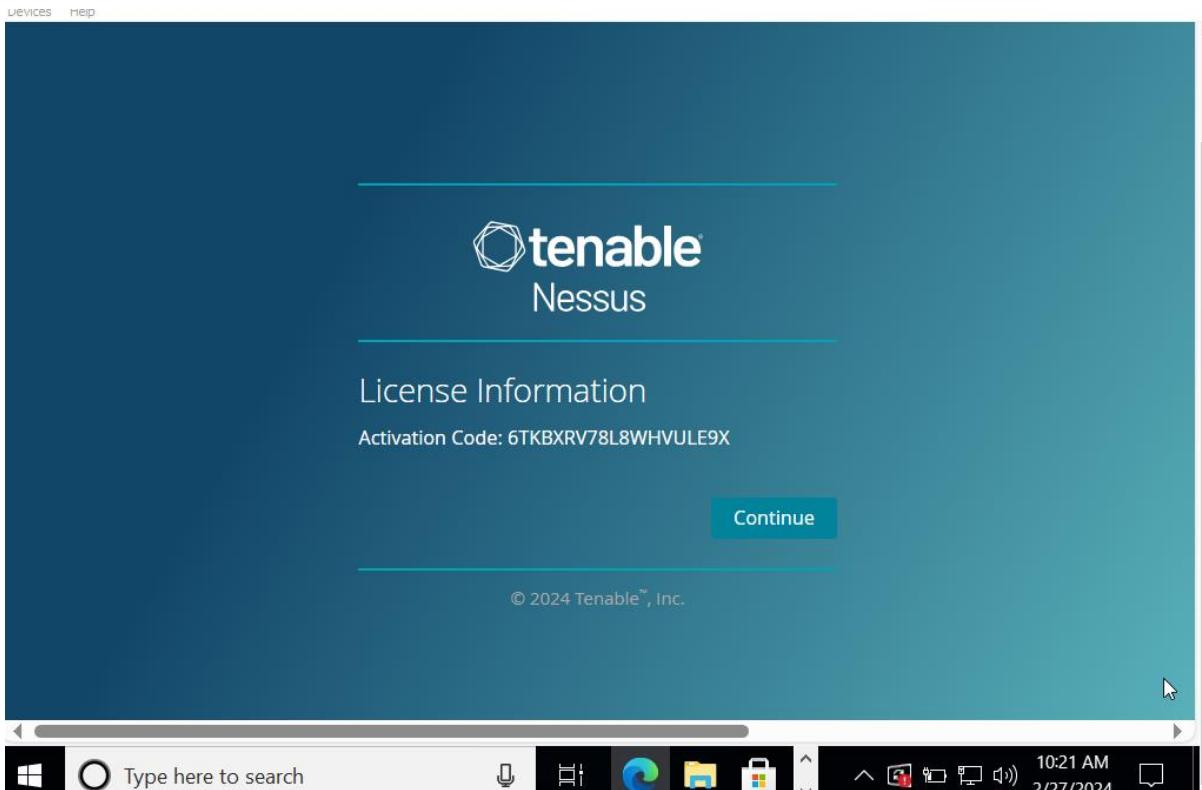
- When welcome to Nessus windows appears, click on Nessus Essentials, then continue.



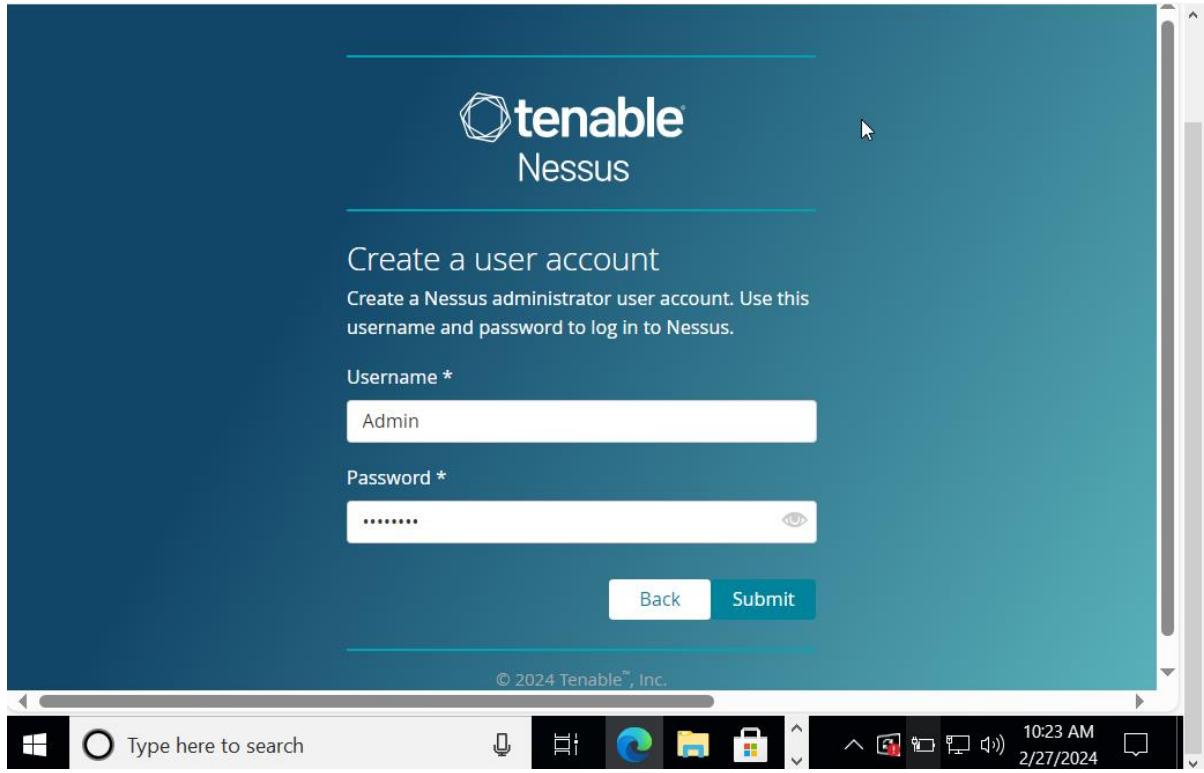
- On this page you are required to register to Nessus.



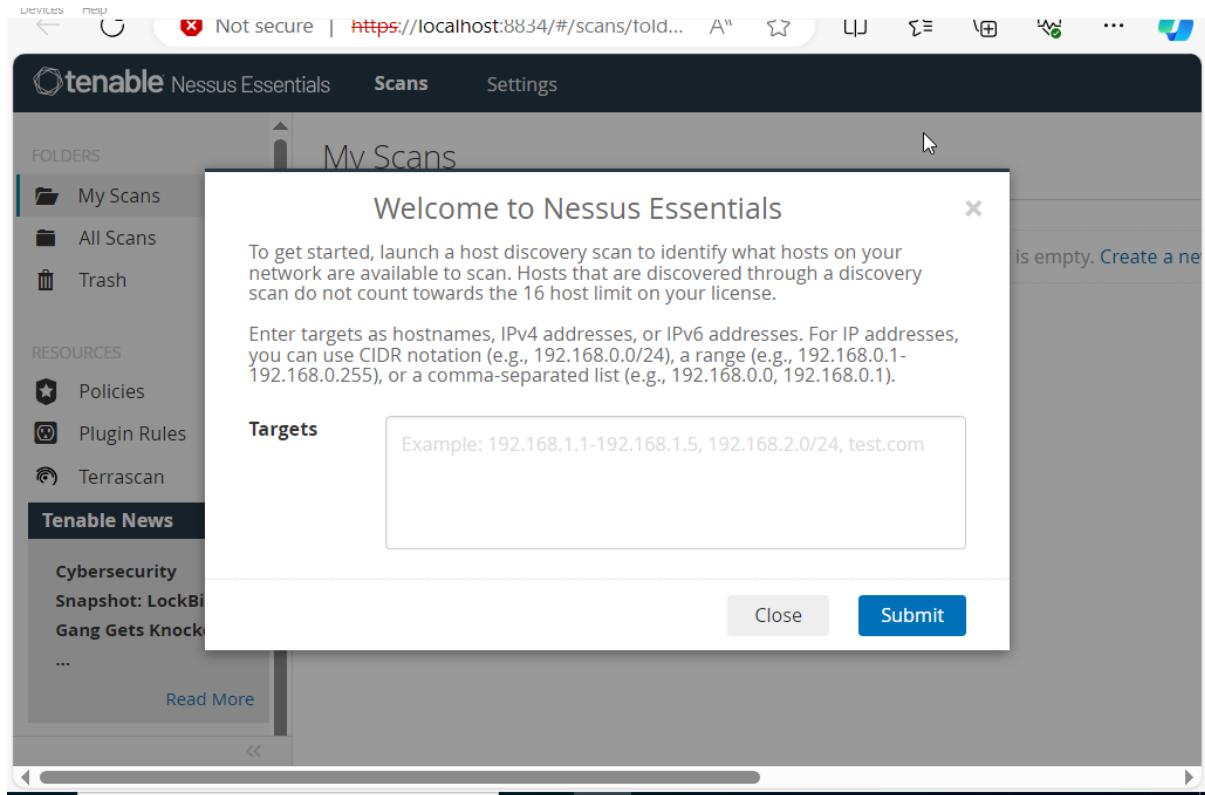
- After Registration, you are required to fill in the code sent to your working email.



- After inputting 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 screenshot shows the Nessus Essentials interface. The top navigation bar includes 'Devices' and 'Help' on the left, and a search bar with 'Not secure | https://localhost:8834/#/scans/poli...' in the center. On the right are standard browser controls like back, forward, and refresh. Below the header is a dark navigation bar with 'tenable' logo, 'Nessus Essentials', 'Scans', and 'Settings' tabs. A sidebar on the left contains 'FOLDERS' with 'My Scans', 'All Scans', and 'Trash' options; 'RESOURCES' with 'Policies' (which is selected and highlighted in blue), 'Plugin Rules', and 'Terrascan'; and a 'Tenable News' section with 'Protecting DoD', 'Building', 'Management', and 'Systems with Ad...'. Below these are 'Import' and '+ New Policy' buttons. The main content area is titled 'Policies' and contains a large circular icon with a star and a document. A descriptive text block states: 'Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of [scan templates](#). From this page you can view, create, import, download, edit, and delete policies.' At the bottom of this section is a message: 'No policies have been created. [Create a new policy](#)'. The bottom of the screen shows a taskbar with several icons and a notification bar indicating '3 new notifications' at 9:01 AM.

- The policy templates windows appears, click advance scan.

This screenshot shows the same Nessus Essentials interface as the previous one, but with a different content area. The main content area now displays a large text box containing the following text:

Import + New Policy

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of [scan templates](#). From this page you can view, create, import, download, edit, and delete policies.

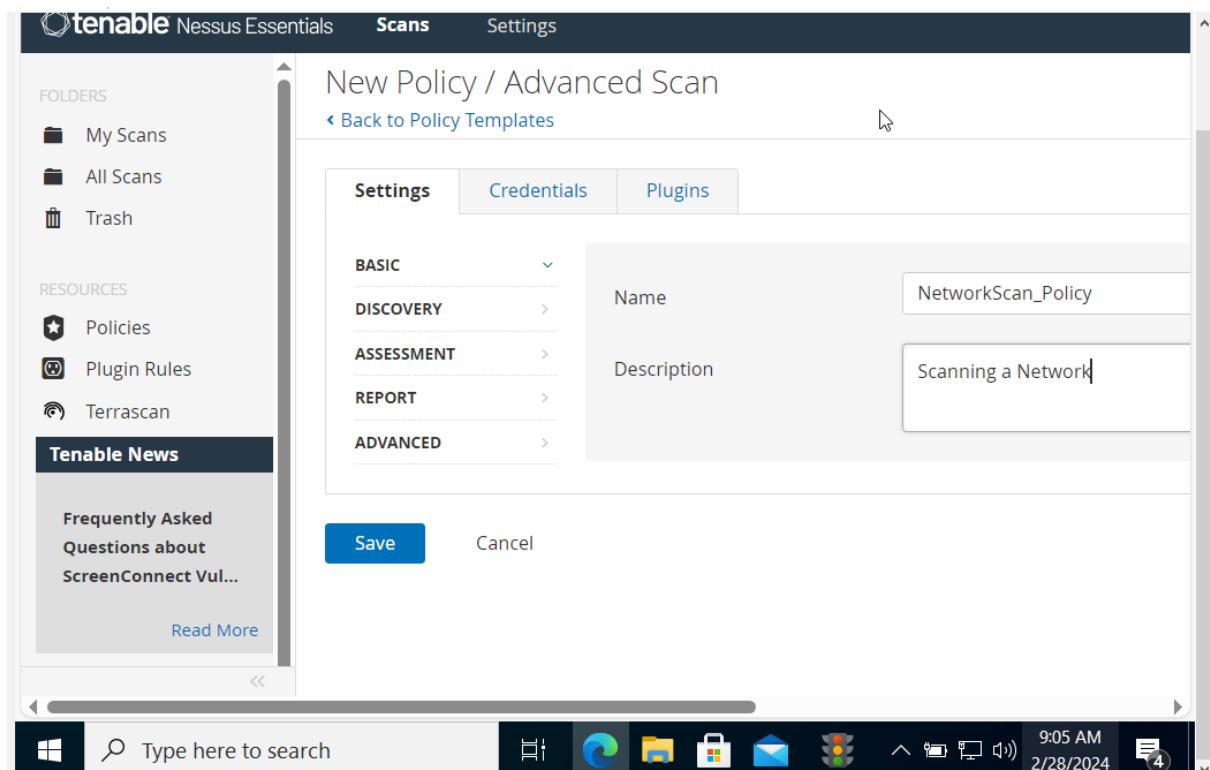
No policies have been created. [Create a new policy](#).

The rest of the interface, including the sidebar, navigation bar, and taskbar, remains the same as in the first screenshot.

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'Devices' and 'Help' on the left, and 'Scans' and 'Settings' on the right. The left sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main content area displays several scan options: 'Host Discovery' (a simple scan to discover live hosts and open ports), 'Basic Network Scan' (a full system scan suitable for any host), 'Advanced Scan' (configure a scan without using any recommendations), 'Mobile Device Scan' (with an 'UPGRADE' button), 'Web Application Tests', and 'Credentialed Patch Audit'. At the bottom, a Windows taskbar shows the search bar, pinned icons for File Explorer, Control Panel, Mail, and File History, battery status, and the date/time.

- 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)

The screenshot shows the 'New Policy / Advanced Scan' configuration page. The top navigation bar includes 'Devices' and 'Help' on the left, and 'Scans' and 'Settings' on the right. The left sidebar has sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main content area is titled 'New Policy / Advanced Scan' and includes a 'Back to Policy Templates' link. It features tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'Settings' tab, there's a 'BASIC' dropdown menu with sections for 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. To the right, there are fields for 'Name' and 'Description'. At the bottom, there are 'Save' and 'Cancel' buttons. The bottom of the screen shows a Windows taskbar with the search bar, pinned icons for File Explorer, Control Panel, Mail, and File History, battery status, and the date/time.



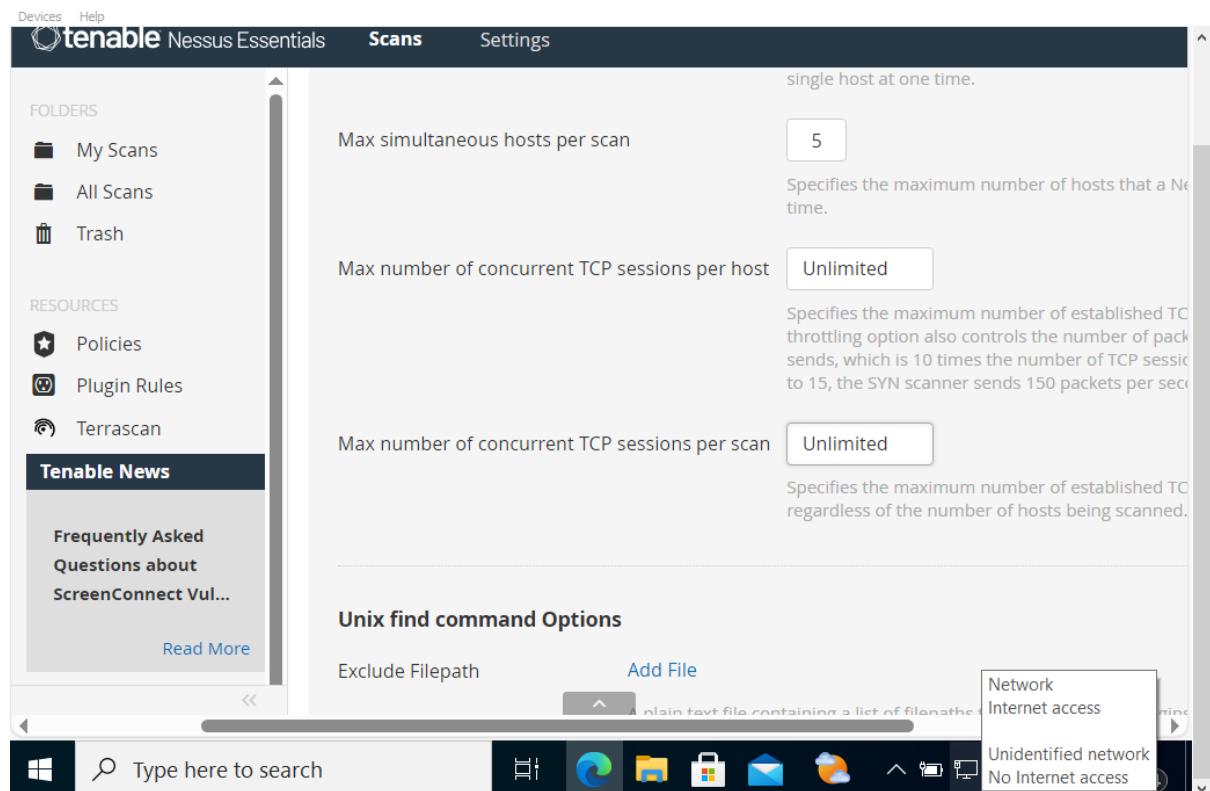
- In the settings tab, click discovery setting type and turn off the ping the remote host option from the right pane.

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'Devices' and 'Help' on the left, followed by the Tenable logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left sidebar, under 'FOLDERS', are 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', are 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is also present. The main content area is titled 'New Policy / Advanced Scan' with a 'Back to Policy Templates' link. It features three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. The 'Settings' tab has sections for 'BASIC', 'DISCOVERY' (with 'Host Discovery', 'Port Scanning', 'Service Discovery', and 'Identity' options), 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'DISCOVERY' section is expanded, showing the 'Port Scanning' option. The 'Port Scanning' section contains two settings: 'Remote Host Ping' (a toggle switch set to 'OFF') and 'Fragile Devices' (checkboxes for 'Scan Network Printers' and 'Scan Novell Netware hosts'). The status bar at the bottom shows '9:07 AM 2/28/2024' and a notification icon.

- 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

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'Devices' and 'Help' on the left, followed by the Tenable logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left sidebar, under 'FOLDERS', are 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', are 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is also present. The main content area is titled 'Network Port Scanners' with a 'Pimcore Multiple Vulnerabilities' link and a 'Read More' button. It features a 'Network Port Scanners' section with a 'SYN' checkbox. The status bar at the bottom shows '9:08 AM 2/28/2024' and a notification icon.

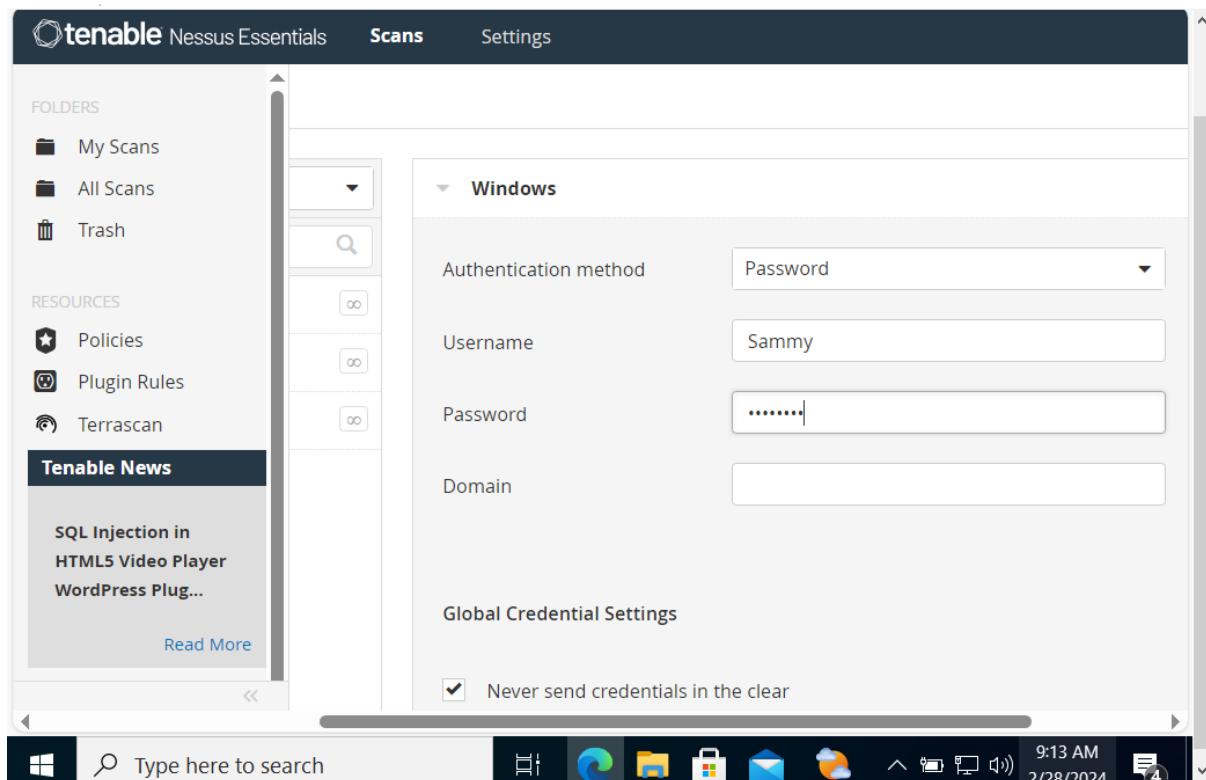
- Select the advance setting type. In the right pane under the performance options settings, set the values of max no. of concurrent TCP sessions per host and max no of concurrent TCP Sessions per scan to unlimited.



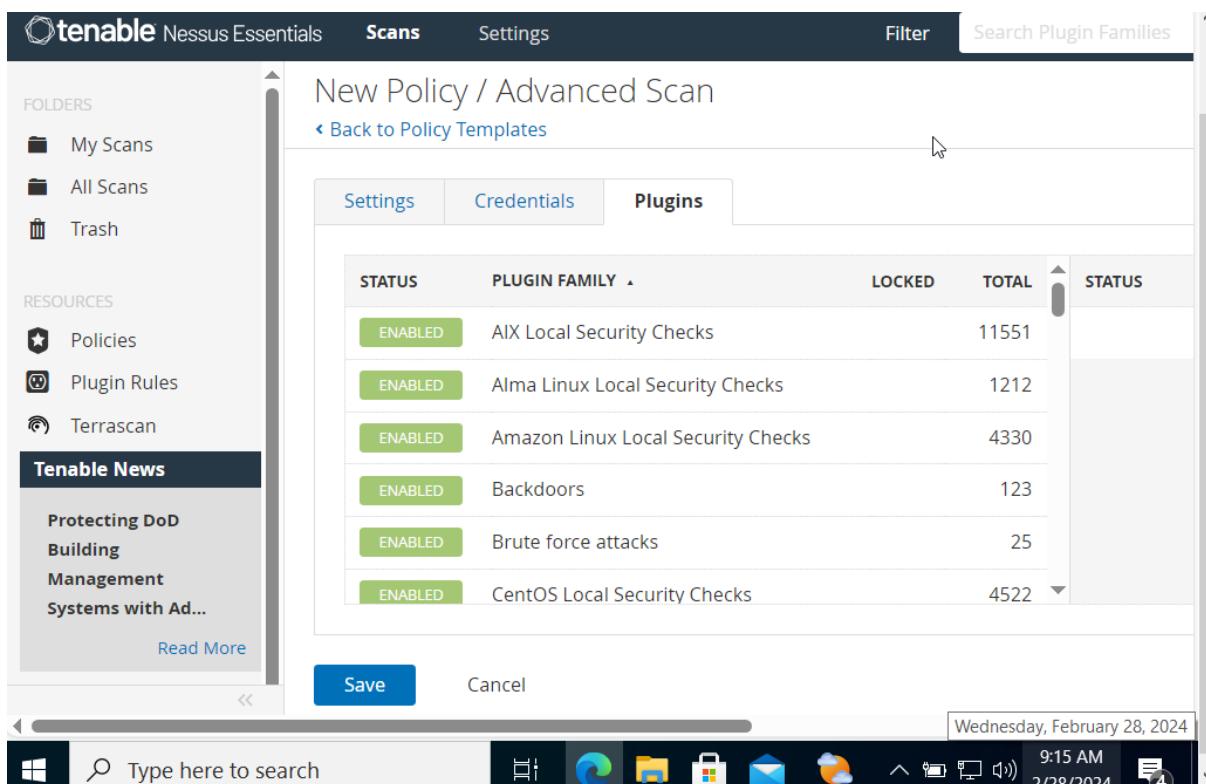
- To configure the credentials of a new policy, click the credentials tab and select windows from the options.

The screenshot shows the Tenable Nessus Essentials web interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left sidebar, there are sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (with a link to 'Pimcore Multiple Vulnerabilities' and a 'Read More' button). The main content area has tabs for 'Settings', 'Credentials' (which is selected), and 'Plugins'. Under 'Credentials', there's a 'CATEGORIES' dropdown set to 'Host' with a search bar labeled 'Filter Credentials'. Below it is a list of credential types: 'SNMPv3', 'SSH', and 'Windows'. To the right, a panel titled 'Windows' shows fields for 'Authentication method', 'Username', 'Password', and 'Domain'. At the bottom right of the panel is a checkbox for 'Never send credentials in t'. The taskbar at the bottom of the screen shows various icons for system functions like battery status (93% available) and network.

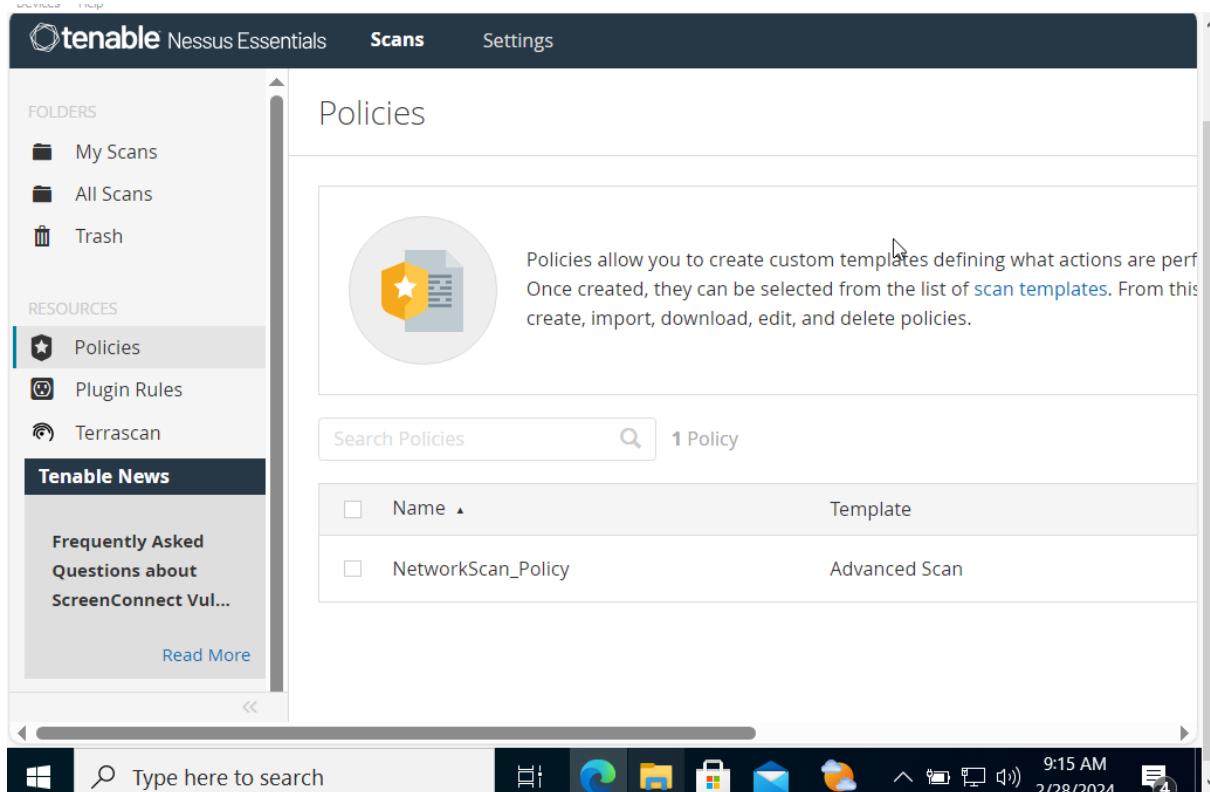
- Specify the username and password in the windows, here the specified credentials are, CEH123/qwerty@123, Note, reenter the created user account credentials admin/password if session time out notification pop up appears.



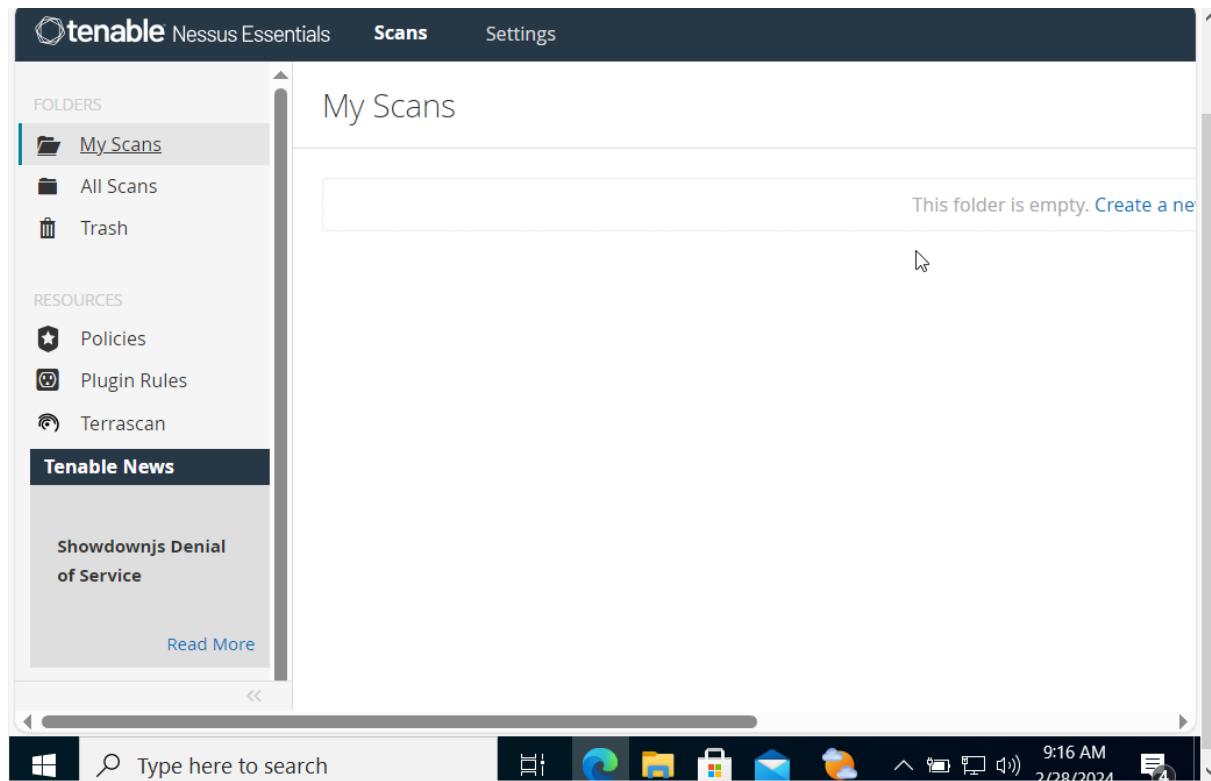
- Click the plugins tab and do not alter any of the options in this window, click the save button.



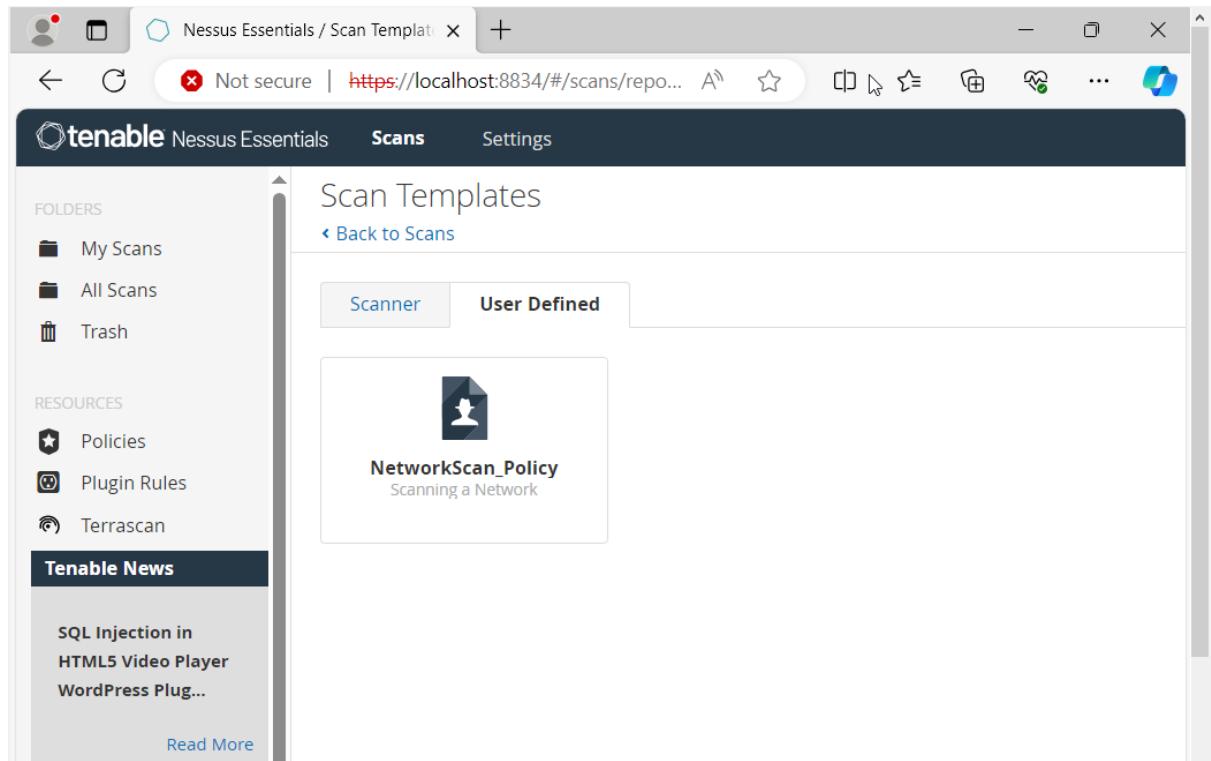
- A policy step successfully notification pop up appears, and the policy is added in the policies windows as shown.



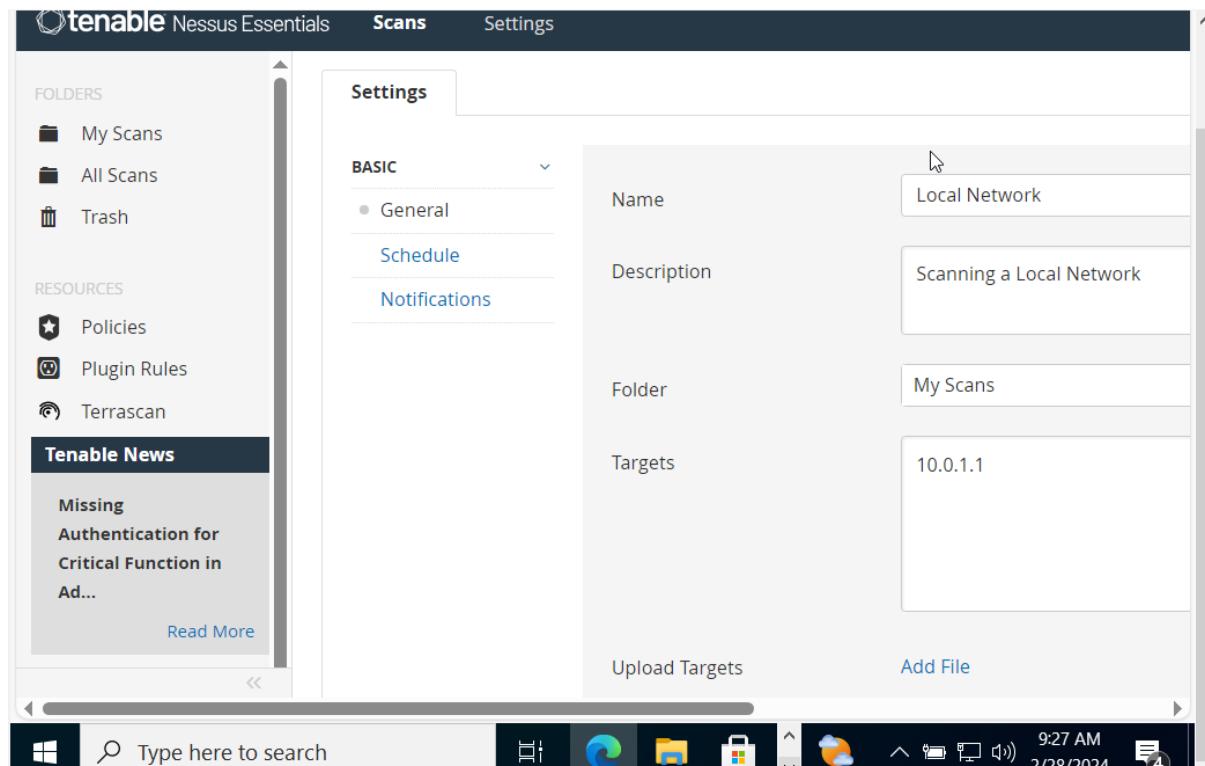
- Now click scans from the menu bar to open my scans window; click create a new scan



- 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

New Scan / NetworkScan_Policy

[Back to Scan Templates](#)

Settings

BASIC

General Enabled OFF

Schedule

Notifications

Save | **Cancel**

FOLDERS

- My Scans
- All Scans
- Trash

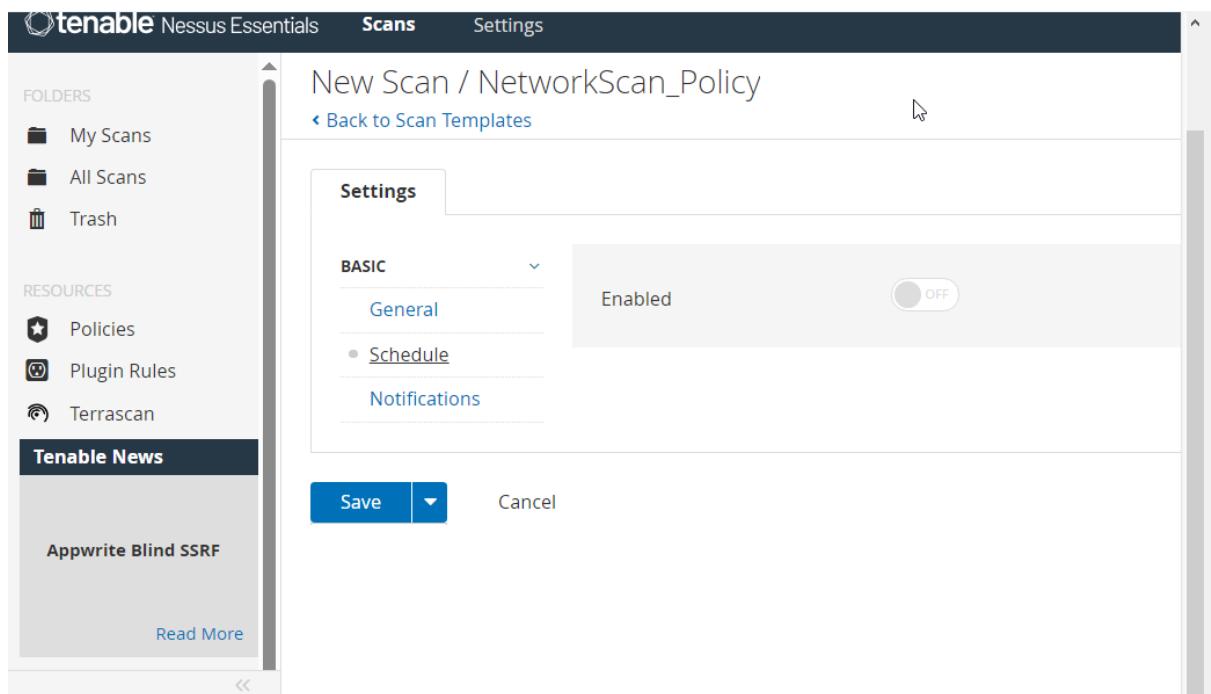
RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Appwrite Blind SSRF

[Read More](#)



Tenable Nessus Essentials Scans Settings

New Scan / NetworkScan_Policy

[Back to Scan Templates](#)

Settings

BASIC

General Enabled OFF

Schedule

Notifications

Save | **Launch** | **Cancel**

FOLDERS

- My Scans
- All Scans
- Trash

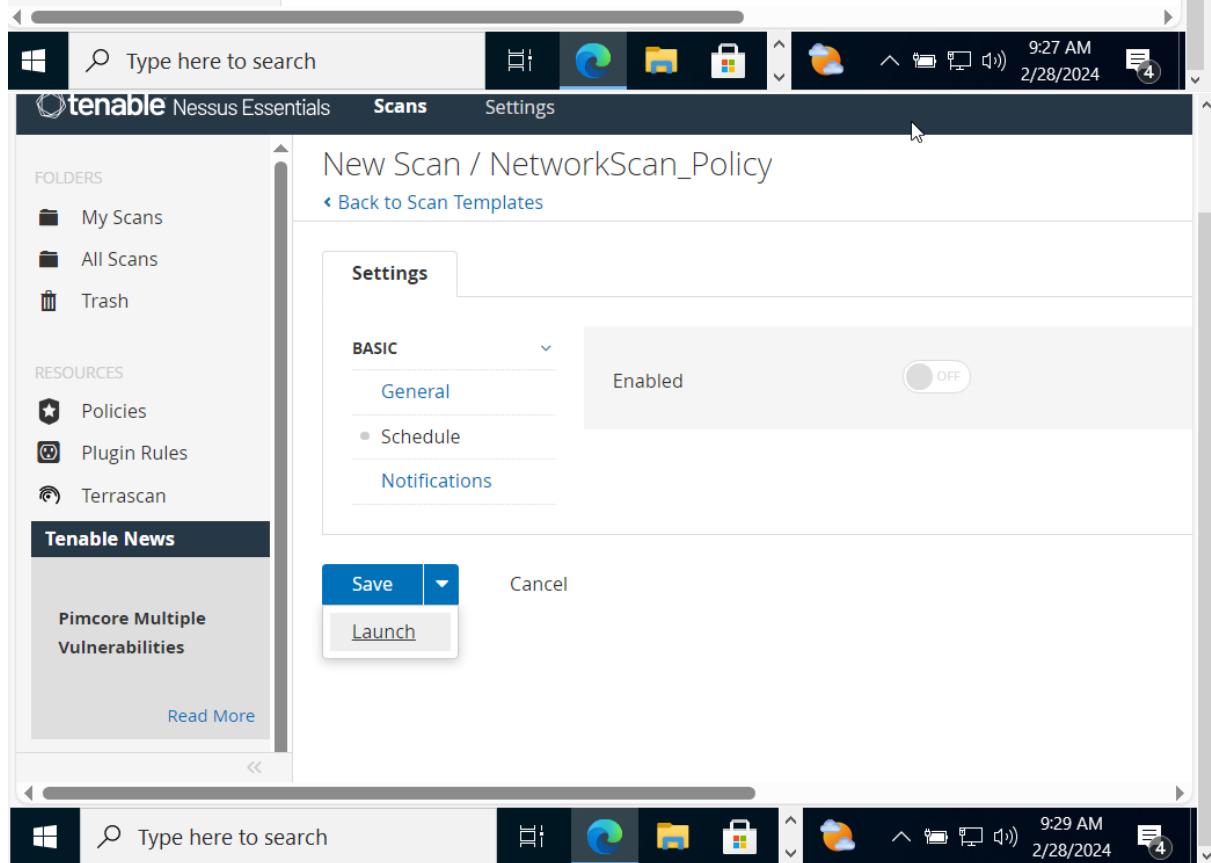
RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Pimcore Multiple Vulnerabilities

[Read More](#)



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

The screenshot displays the Tenable Nessus Essentials application interface across three horizontal sections, likely representing different times or steps in a process.

Top Section (Left Column):

- FOLDERS:** My Scans (1), All Scans, Trash.
- RESOURCES:** Policies, Plugin Rules, Terrascan.
- Tenable News:** Frequently Asked Questions about ScreenConnect Vul...
- Read More** button.

Middle Section (Main Content):

My Scans page:

- Search bar: Search Scans, 1 Scan.
- Table headers: Name, Schedule.
- Scan entry: Local Network, On Demand.

Bottom Section (Right Column):

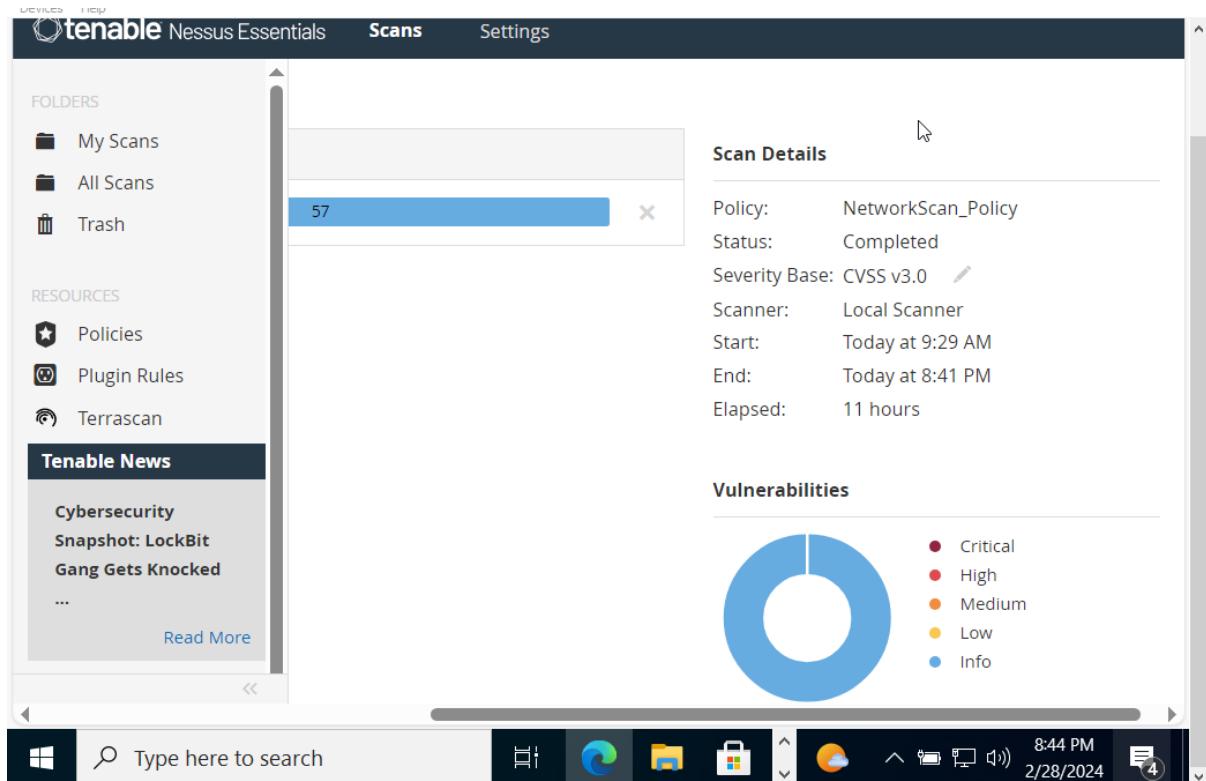
Host Details page:

- Filter dropdown: Host, Vulnerabilities.
- Host list: 10.0.1.1 (highlighted in blue), 57 vulnerabilities.
- Search bar: Search Hosts.
- System tray: Windows Start button, Task View, File Explorer, Microsoft Edge, Taskbar icons, Date/Time: 9:30 AM, 2/28/2024, Notifications: 4.

Bottom-most Section (Right Column):

Host Details page (continued):

- Host list: 10.0.1.1 (highlighted in blue), 57 vulnerabilities.
- Search bar: Search Hosts.
- System tray: Windows Start button, Task View, File Explorer, Microsoft Edge, Taskbar icons, Date/Time: 8:43 PM, 2/28/2024, Notifications: 4.



- 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 your 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.

