Gerren Jerome - Vulnerability Analysis

Scenario:

- You are an ethical hacker with a large organization (EC-Council).
- You need to conduct research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Objectives:

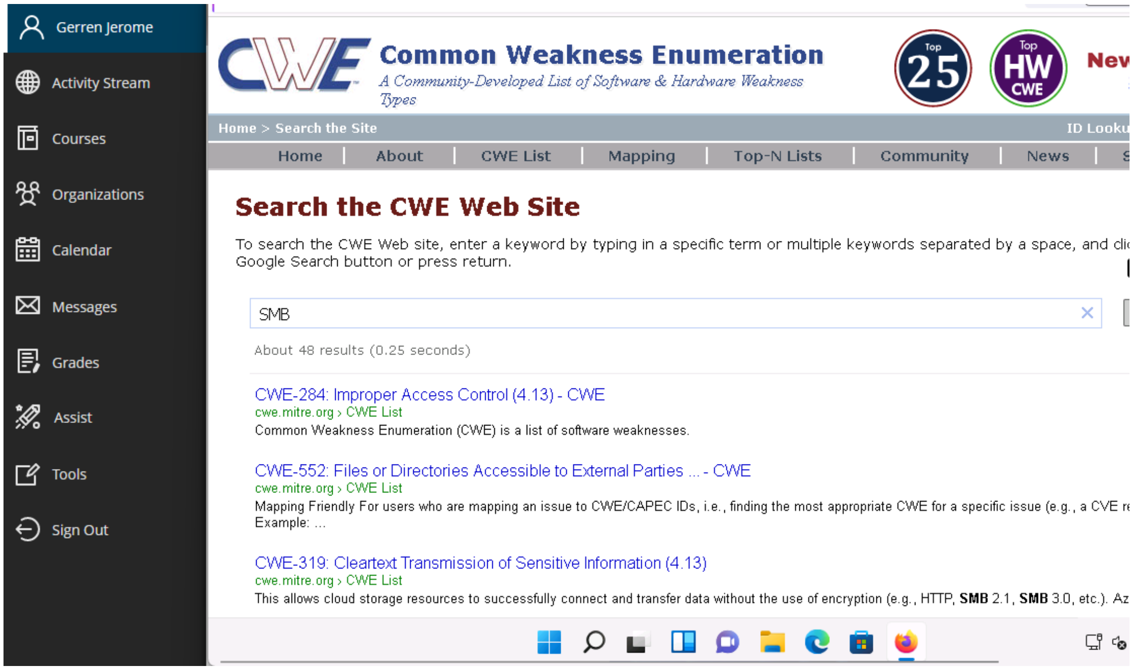
- Extraction various pieces of information about the target
  - Network vulnerabilities, listening IP/ TCP/UDP ports and services
  - Application and service configuration errors/vulnerabilities
  - Running OS versions and applications
  - Weak passwords and weak permissions
  - Default services and applications that may have to be uninstalled

TASKS (XX items total):

Ethical hackers and pentesters use various tools and techniques to enumerate a target network.

The following tasks will assist you in learning various enumeration techniques:

1) Perform vulnerability research with vulnerability scoring systems and databases (8 tasks)
   a) Perform vulnerability research in Common Weakness Enumeration (CWE) (2 tasks)
      i) **Screengrab – Step 5**: CWE search results (SMB)



Gerren Jerome
Activity Stream
Courses
Organizations
Calendar
Messages
Grades
Assist
Tools
Sign Out
CWE
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Top 25
Top HW CWE
New
Home > Search the Site
ID Looku
Home | About | CWE List | Mapping | Top-N Lists | Community | News | S

Search the CWE Web Site

To search the CWE Web site, enter a keyword by typing in a specific term or multiple keywords separated by a space, and cli
Google Search button or press return.

SMB

About 48 results (0.25 seconds)

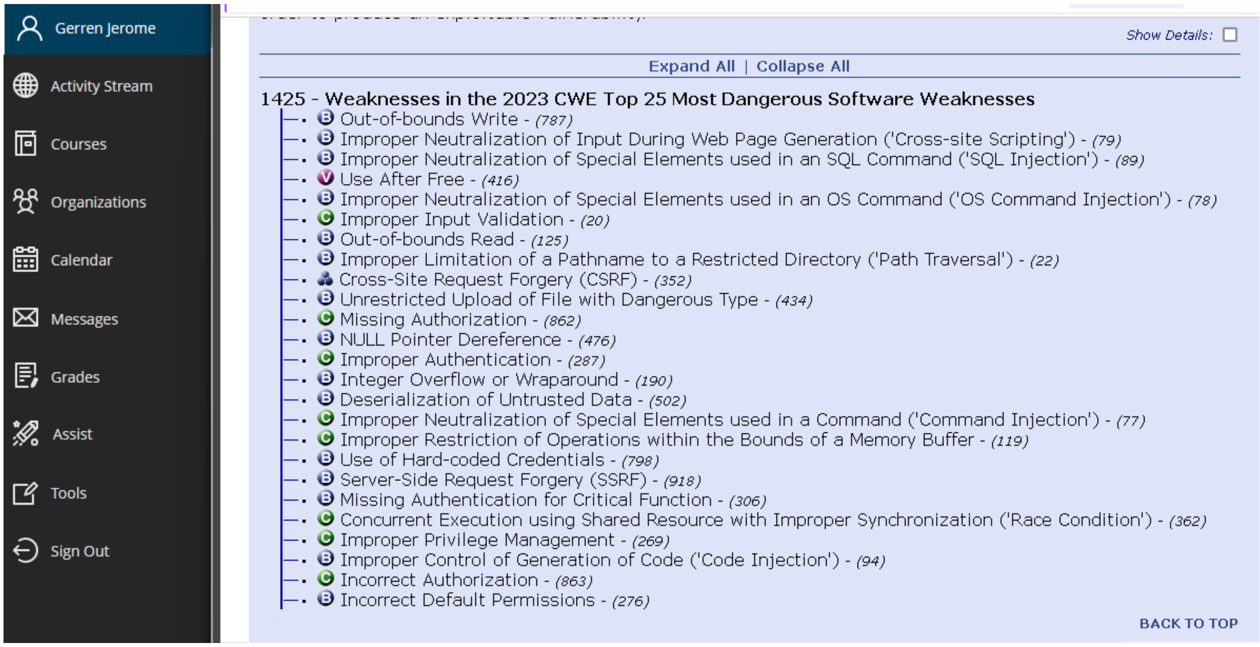
CWE-284: Improper Access Control (4.13) - CWE
cwe.mitre.org › CWE List
Common Weakness Enumeration (CWE) is a list of software weaknesses.

CWE-552: Files or Directories Accessible to External Parties ... - CWE
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE re
Example: ...

CWE-319: Cleartext Transmission of Sensitive Information (4.13)
cwe.mitre.org › CWE List
This allows cloud storage resources to successfully connect and transfer data without the use of encryption (e.g., HTTP, **SMB** 2.1, **SMB** 3.0, etc.). Az

Gerren Jerome - Vulnerability Analysis

ii) **Screengrab – Step 11**: Top 25 Most Dangerous Software Weaknesses (CWE VIEW)

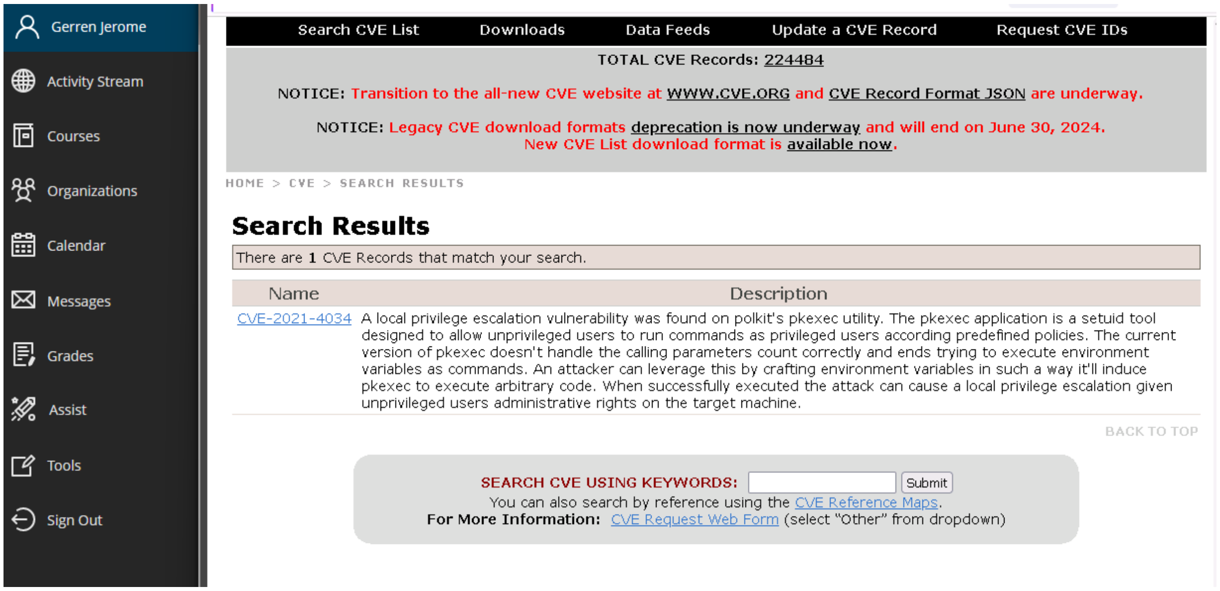


1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Input Validation - *(20)*
- Out-of-bounds Read - *(125)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Missing Authorization - *(862)*
- NULL Pointer Dereference - *(476)*
- Improper Authentication - *(287)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Use of Hard-coded Credentials - *(798)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Missing Authentication for Critical Function - *(306)*
- Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - *(362)*
- Improper Privilege Management - *(269)*
- Improper Control of Generation of Code ('Code Injection') - *(94)*
- Incorrect Authorization - *(863)*
- Incorrect Default Permissions - *(276)*

b) Perform vulnerability research in Common Vulnerabilities and Exposures (CVE) (3 tasks)

i) **Screengrab – Step 5**: CVE Search (CVE-2021-4034)



TOTAL CVE Records: 224484

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024. New CVE List download format is available now.

Search Results

There are **1** CVE Records that match your search.

Name	Description
CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

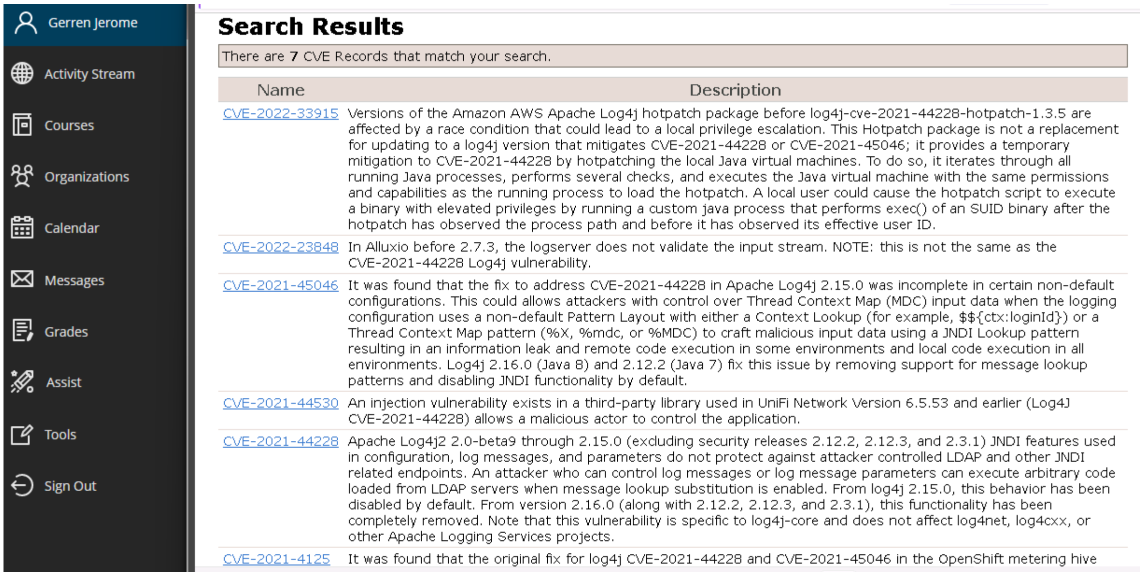
SEARCH CVE USING KEYWORDS:

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

Gerren Jerome - Vulnerability Analysis

ii) **Screengrab – Step 7**: CVE Search (CVE-2021-44228)

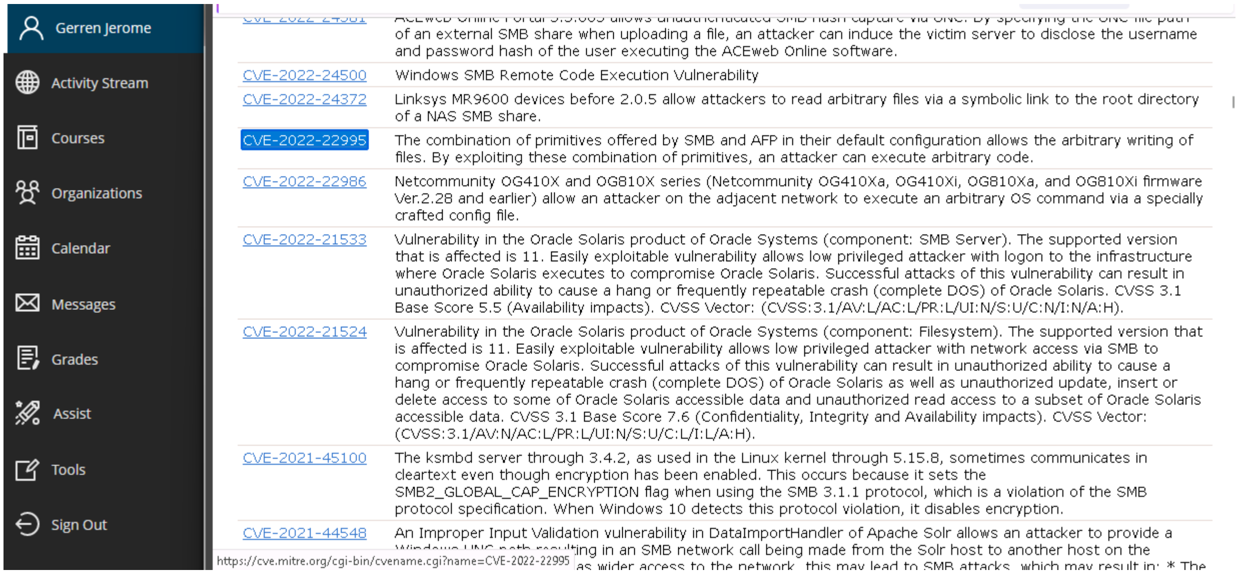


Search Results

There are **7** CVE Records that match your search.

Name	Description
CVE-2022-33915	Versions of the Amazon AWS Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.3.5 are affected by a race condition that could lead to a local privilege escalation. This Hotpatch package is not a replacement for updating to a log4j version that mitigates CVE-2021-44228 or CVE-2021-45046; it provides a temporary mitigation to CVE-2021-44228 by hotpatching the local Java virtual machines. To do so, it iterates through all running Java processes, performs several checks, and executes the Java virtual machine with the same permissions and capabilities as the running process to load the hotpatch. A local user could cause the hotpatch script to execute a binary with elevated privileges by running a custom java process that performs exec() of an SUID binary after the hotpatch has observed the process path and before it has observed its effective user ID.
CVE-2022-23848	In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability.
CVE-2021-45046	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.
CVE-2021-44530	An injection vulnerability exists in a third-party library used in UniFi Network Version 6.5.53 and earlier (Log4J CVE-2021-44228) allows a malicious actor to control the application.
CVE-2021-44228	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.
CVE-2021-4125	It was found that the original fix for log4j CVE-2021-44228 and CVE-2021-45046 in the OpenShift metering hive

iii) **Screengrab – Step 12**: CVE Search (CVE-2022-22995



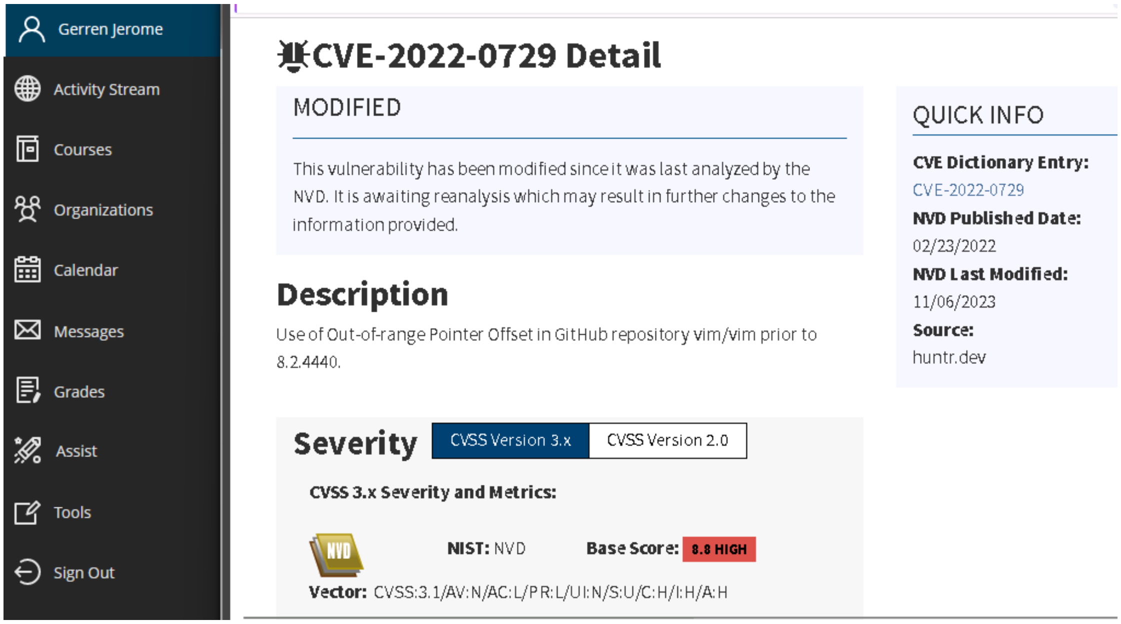
CVE-2022-24581	ACEweb Online Portal 3.5.065 allows unauthenticated SMB hash capture via UNC. By specifying the UNC file path of an external SMB share when uploading a file, an attacker can induce the victim server to disclose the username and password hash of the user executing the ACEweb Online software.
CVE-2022-24500	Windows SMB Remote Code Execution Vulnerability
CVE-2022-24372	Linksys MR9600 devices before 2.0.5 allow attackers to read arbitrary files via a symbolic link to the root directory of a NAS SMB share.
CVE-2022-22995	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code.
CVE-2022-22986	Netcommunity OG410X and OG810X series (Netcommunity OG410Xa, OG410Xi, OG810Xa, and OG810Xi firmware Ver.2.28 and earlier) allow an attacker on the adjacent network to execute an arbitrary OS command via a specially crafted config file.
CVE-2022-21533	Vulnerability in the Oracle Solaris product of Oracle Systems (component: SMB Server). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2022-21524	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with network access via SMB to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H).
CVE-2021-45100	The ksmbd server through 3.4.2, as used in the Linux kernel through 5.15.8, sometimes communicates in cleartext even though encryption has been enabled. This occurs because it sets the SMB2_GLOBAL_CAP_ENCRYPTION flag when using the SMB 3.1.1 protocol, which is a violation of the SMB protocol specification. When Windows 10 detects this protocol violation, it disables encryption.
CVE-2021-44548	An Improper Input Validation vulnerability in DataImportHandler of Apache Solr allows an attacker to provide a Windows UNC path resulting in an SMB network call being made from the Solr host to another host on the as wider access to the network, this may lead to SMB attacks, which may result in: * The

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22995

Gerren Jerome - Vulnerability Analysis

c) Perform vulnerability research in National Vulnerability Database (NVD) (3 tasks)

i) **Screengrab – Step 4**: NVD Search (CVE-2022-0729)



CVE-2022-0729 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

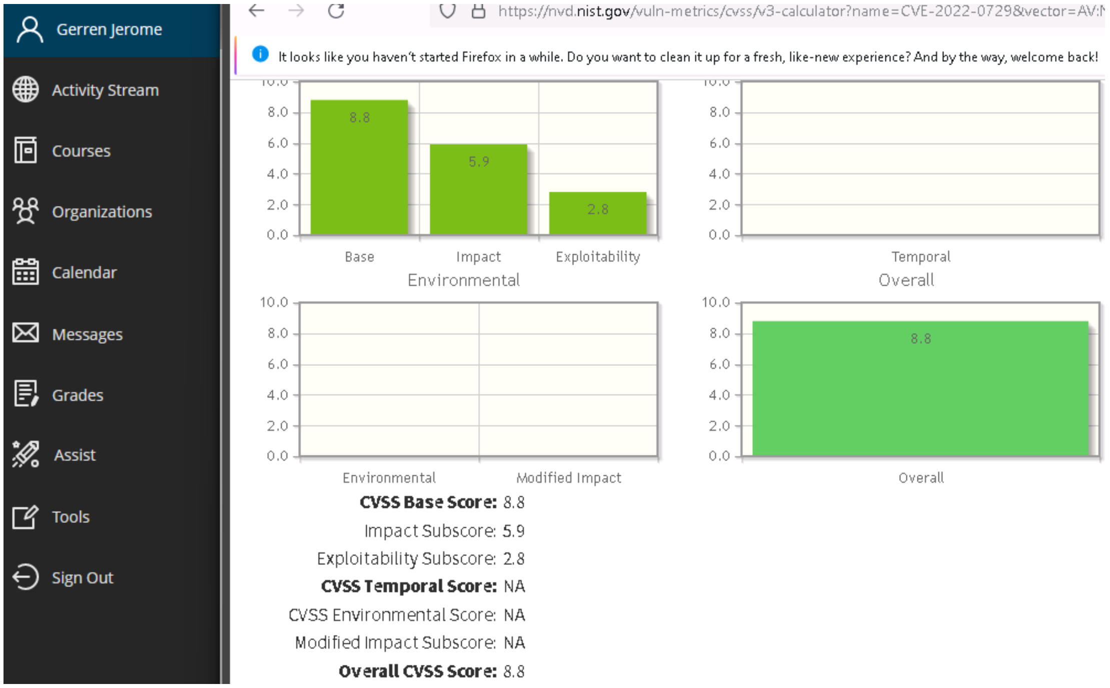
CVE Dictionary Entry: CVE-2022-0729

NVD Published Date: 02/23/2022

NVD Last Modified: 11/06/2023

Source: huntr.dev

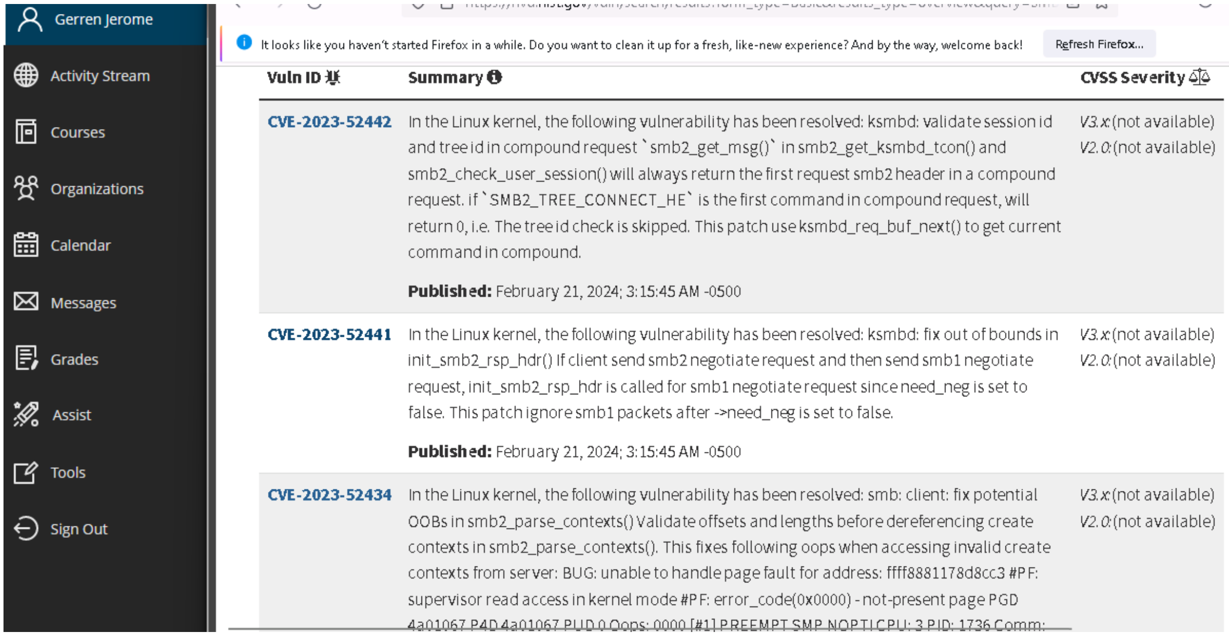
ii) **Screengrab – Step 6**: Graphical Score Representation (CVE-2022-0729)



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

iii) **Screengrab – Step 10**: NVD Search (SMB)



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

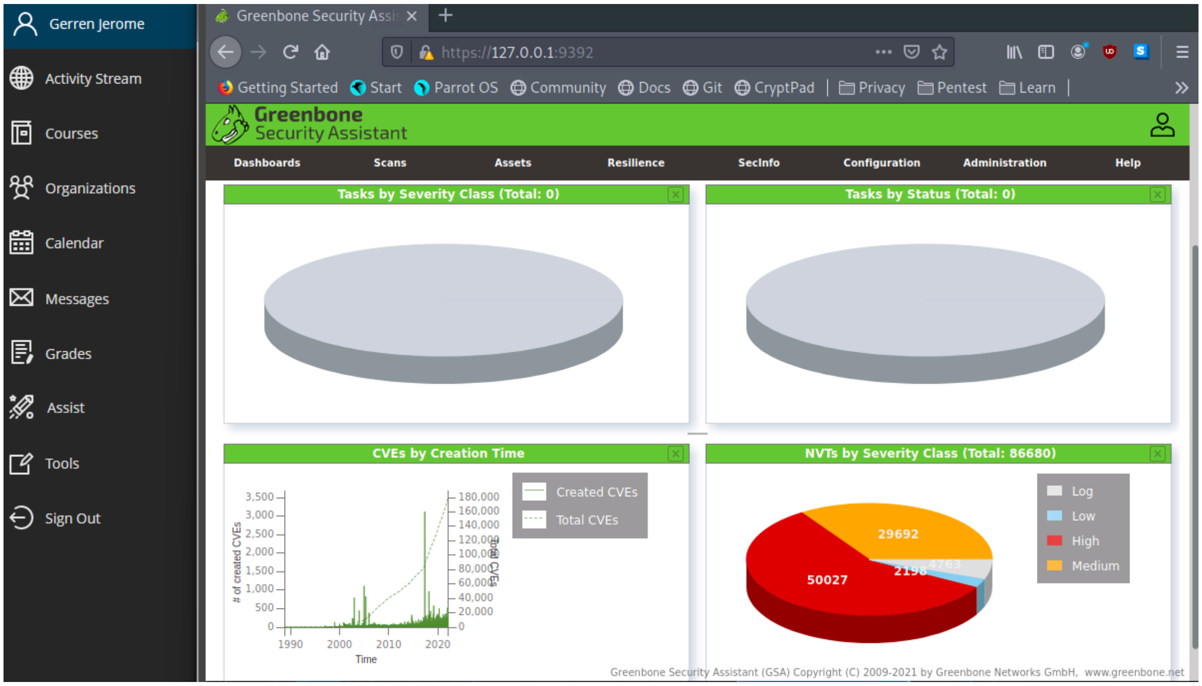
Vuln ID	Summary	CVSS Severity
CVE-2023-52442	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate session id and tree id in compound request `smb2_get_msg()` in smb2_get_ksmbd_tcon() and smb2_check_user_session() will always return the first request smb2 header in a compound request. if `SMB2_TREE_CONNECT_HE` is the first command in compound request, will return 0, i.e. The tree id check is skipped. This patch use ksmbd_req_buf_next() to get current command in compound. **Published:** February 21, 2024; 3:15:45 AM -0500	*V3.x:* (not available) *V2.0:* (not available)
CVE-2023-52441	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out of bounds in init_smb2_rsp_hdr() If client send smb2 negotiate request and then send smb1 negotiate request, init_smb2_rsp_hdr is called for smb1 negotiate request since need_neg is set to false. This patch ignore smb1 packets after ->need_neg is set to false. **Published:** February 21, 2024; 3:15:45 AM -0500	*V3.x:* (not available) *V2.0:* (not available)
CVE-2023-52434	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential OOBs in smb2_parse_contexts() Validate offsets and lengths before dereferencing create contexts in smb2_parse_contexts(). This fixes following oops when accessing invalid create contexts from server: BUG: unable to handle page fault for address: ffff8881178d8cc3 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 4a01067 P4D 4a01067 PUD 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 1736 Comm:	*V3.x:* (not available) *V2.0:* (not available)

Gerren Jerome - Vulnerability Analysis

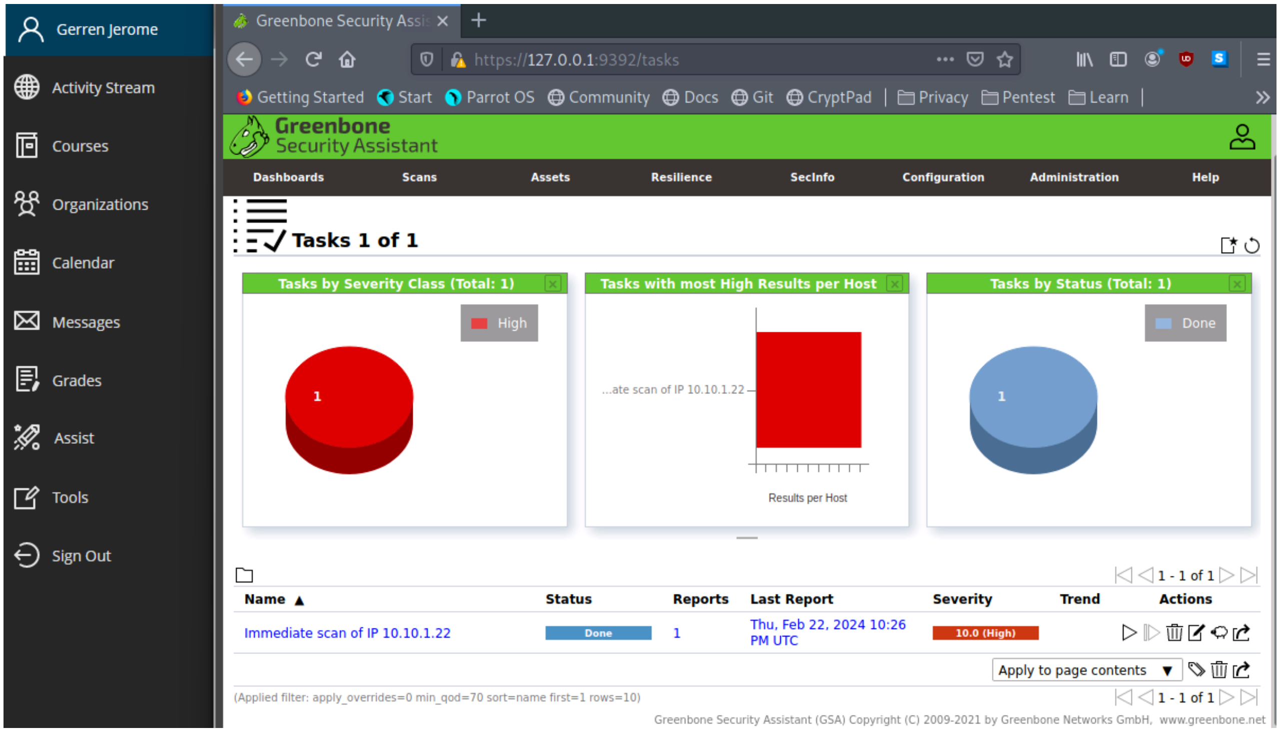
2) Perform vulnerability assessment using various vulnerability assessment tools.

a) Perform vulnerability analysis using OpenVAS (5 tasks)

i) **Screengrab – Step 8**: OpenVAS Dashboard post-login



ii) **Screengrab – Step 13**: OpenVAS scan completed.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.22	Done	1	Thu, Feb 22, 2024 10:26 PM UTC	10.0 (High)		

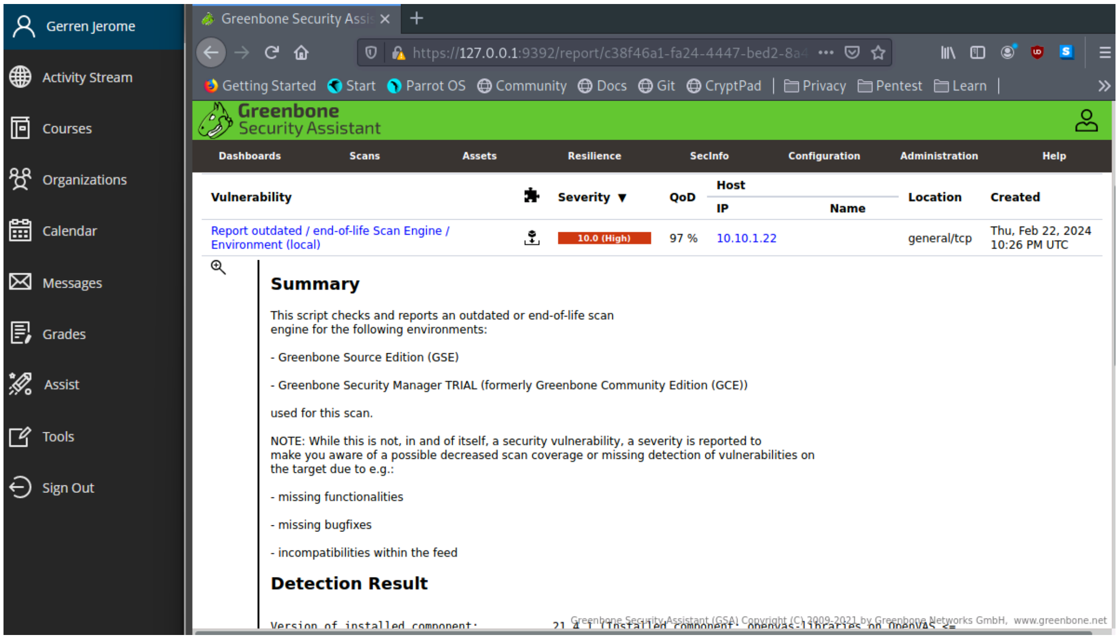
Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Gerren Jerome - Vulnerability Analysis

iii) **Screengrab – Step 16**: Detailed results re: vulnerability under “Report outdated/end of life/scan engine/Environment (local)”



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	10.10.1.22		general/tcp	Thu, Feb 22, 2024 10:26 PM UTC

Summary

This script checks and reports an outdated or end-of-life scan engine for the following environments:

- Greenbone Source Edition (GSE)

- Greenbone Security Manager TRIAL (formerly Greenbone Community Edition (GCE))

used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:

- missing functionalities

- missing bugfixes

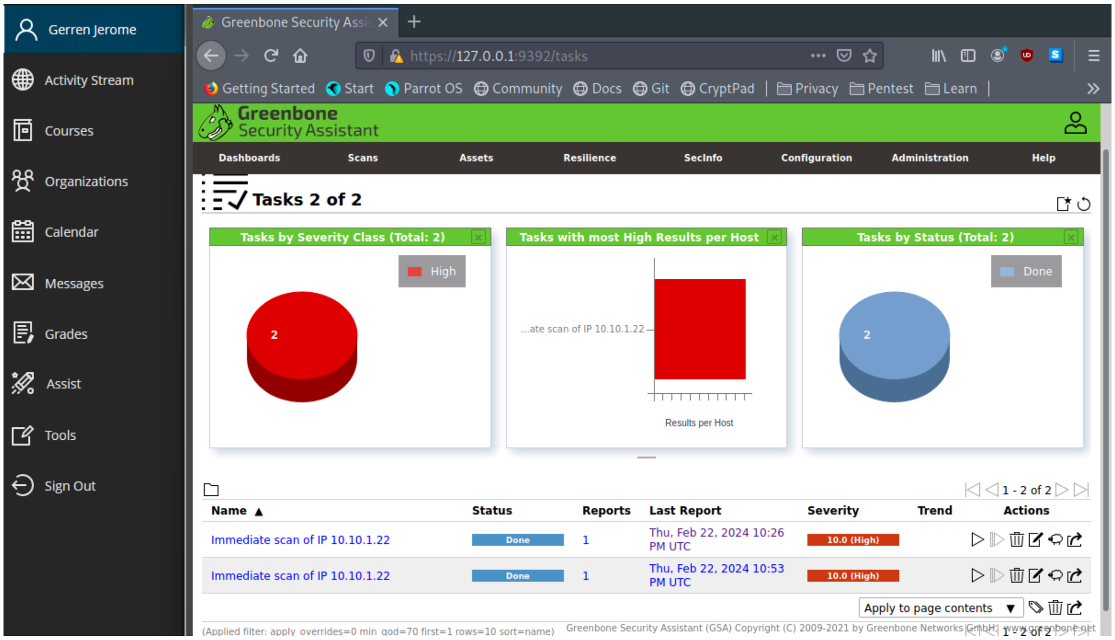
- incompatibilities within the feed

Detection Result

```
Version of installed component:          21.4.1 (Installed component: openvas-libraries on OpenVAS <=
```

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

iv) **Screengrab – Step 23**: New task in OpenVAS’ Tasks section



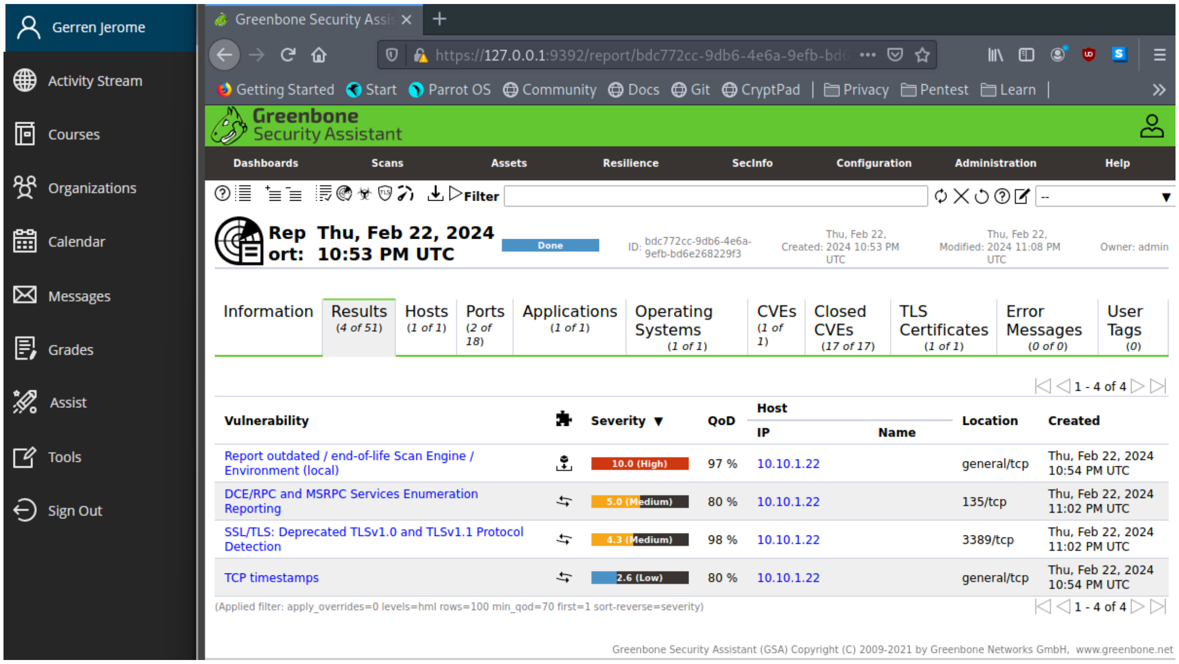
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.22	Done	1	Thu, Feb 22, 2024 10:26 PM UTC	10.0 (High)		
Immediate scan of IP 10.10.1.22	Done	1	Thu, Feb 22, 2024 10:53 PM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Gerren Jerome - Vulnerability Analysis

v) Screengrab – Step 25: Report results (Severity of vulnerabilities)



Report: Thu, Feb 22, 2024 10:53 PM UTC   Done   ID: bdc772cc-9db6-4e6a-9efb-bd6e268229f3   Created: Thu, Feb 22, 2024 10:53 PM UTC   Modified: Thu, Feb 22, 2024 11:08 PM UTC   Owner: admin

Information | Results (4 of 51) | Hosts (1 of 1) | Ports (2 of 18) | Applications (1 of 1) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (17 of 17) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 4 of 4

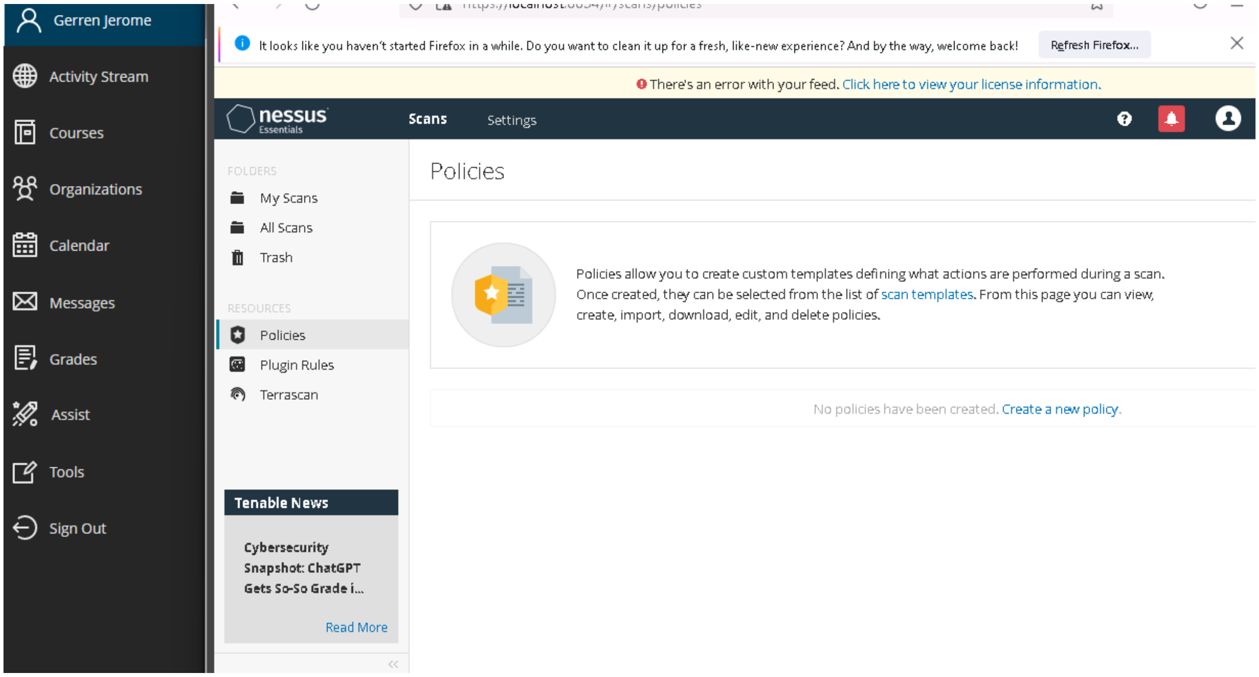
Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	10.10.1.22		general/tcp	Thu, Feb 22, 2024 10:54 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.10.1.22		135/tcp	Thu, Feb 22, 2024 11:02 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	10.10.1.22		3389/tcp	Thu, Feb 22, 2024 11:02 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	10.10.1.22		general/tcp	Thu, Feb 22, 2024 10:54 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)   1 - 4 of 4

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

b) Perform vulnerability scanning using Nessus (8 tasks)

i) Screengrab – Step 6: Nessus Dashboard post-login



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

There's an error with your feed. Click here to view your license information.

Policies

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.

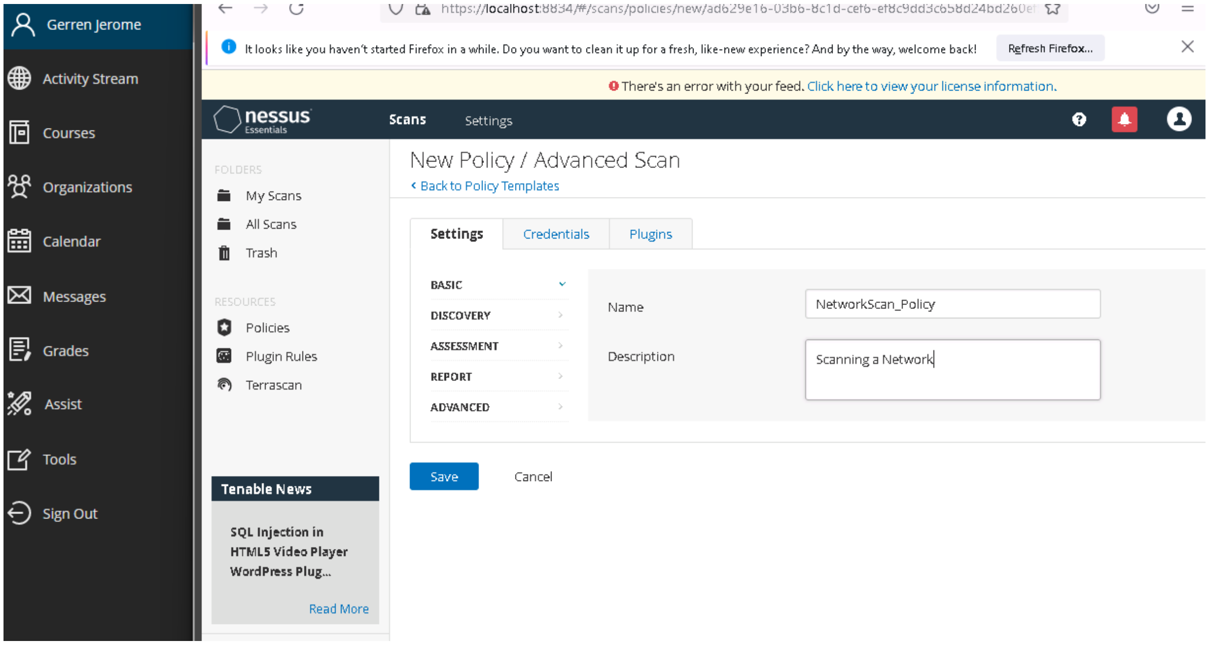
No policies have been created. Create a new policy.

Tenable News

Cybersecurity Snapshot: ChatGPT Gets So-So Grade i...

Gerren Jerome - Vulnerability Analysis

ii) **Screengrab – Step 10**: Nessus Advanced Scan settings – BASIC



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

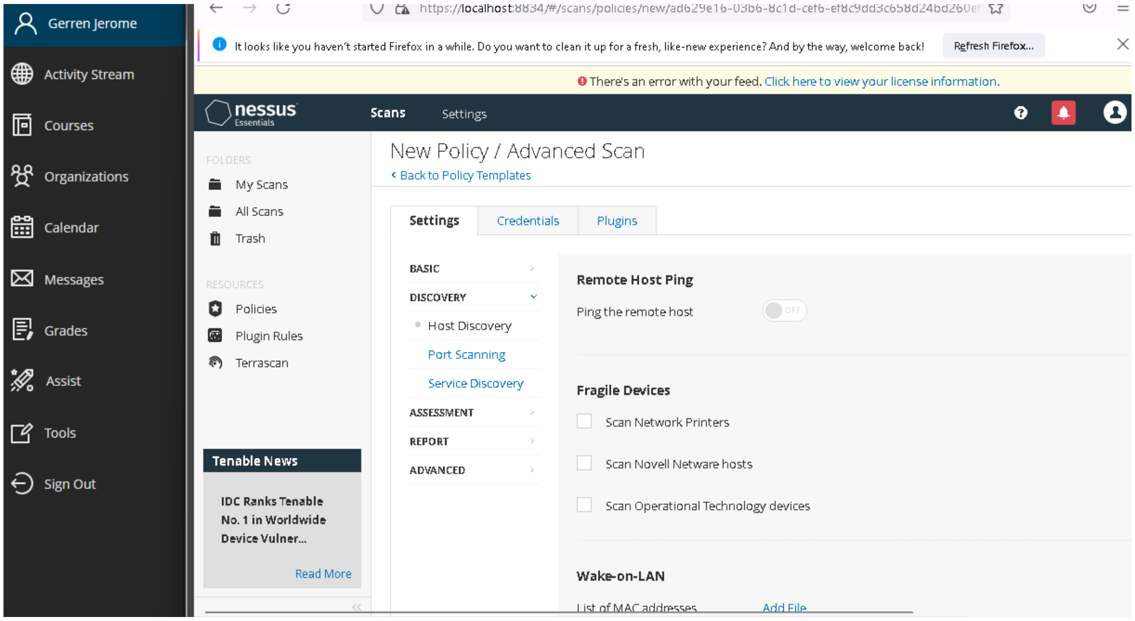
There's an error with your feed. Click here to view your license information.

New Policy / Advanced Scan

Name: NetworkScan_Policy

Description: Scanning a Network

iii) **Screengrab – Step 11**: Nessus Advanced Scan settings – DISCOVERY



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

There's an error with your feed. Click here to view your license information.

New Policy / Advanced Scan

Remote Host Ping

Ping the remote host: OFF

Fragile Devices

□ Scan Network Printers

□ Scan Novell Netware hosts

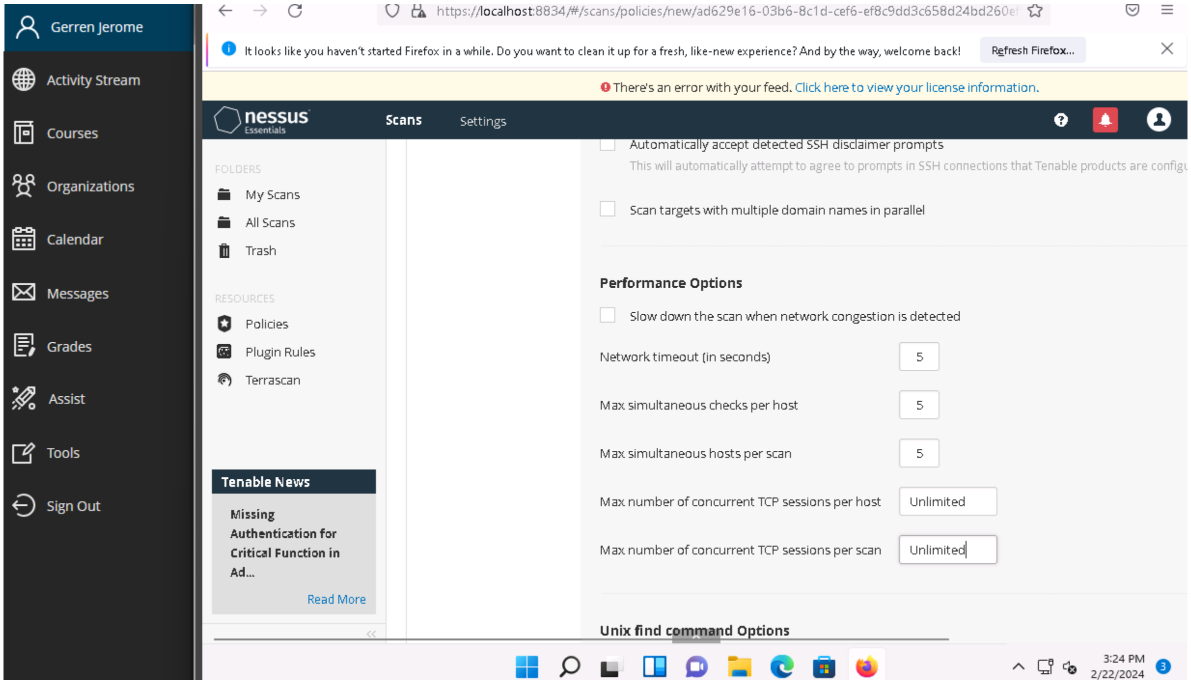
□ Scan Operational Technology devices

Wake-on-LAN

List of MAC addresses

Gerren Jerome - Vulnerability Analysis

iv) Screengrab – Step 13: Nessus Advanced Scan settings – ADVANCED



https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260e

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

There's an error with your feed. Click here to view your license information.

□ Automatically accept detected SSH disclaimer prompts
This will automatically attempt to agree to prompts in SSH connections that Tenable products are configu

□ Scan targets with multiple domain names in parallel

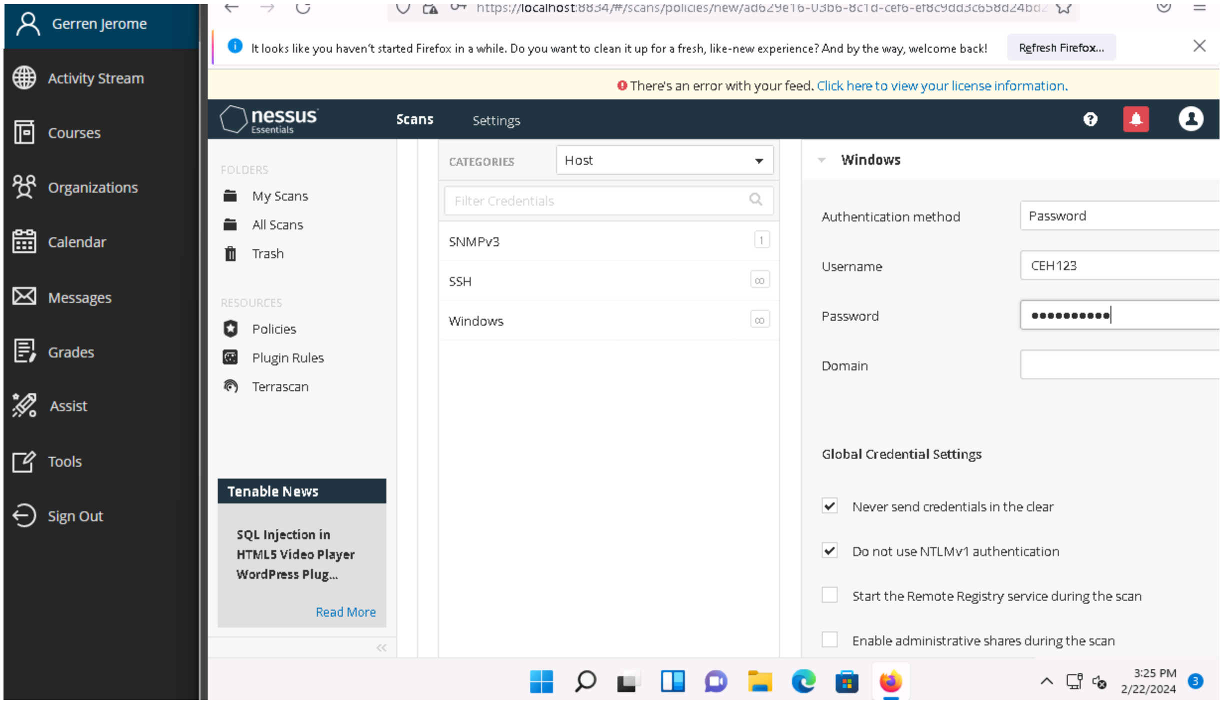
Performance Options

□ Slow down the scan when network congestion is detected

Network timeout (in seconds)	5
Max simultaneous checks per host	5
Max simultaneous hosts per scan	5
Max number of concurrent TCP sessions per host	Unlimited
Max number of concurrent TCP sessions per scan	Unlimited

Unix find command Options

v) Screengrab – Step 15: Specify username and password for Windows credentials.



https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

There's an error with your feed. Click here to view your license information.

CATEGORIES: Host

Filter Credentials

SNMPv3	1
SSH	∞
Windows	∞

Windows

Authentication method	Password
Username	CEH123
Password	••••••••••
Domain	

Global Credential Settings

☑ Never send credentials in the clear

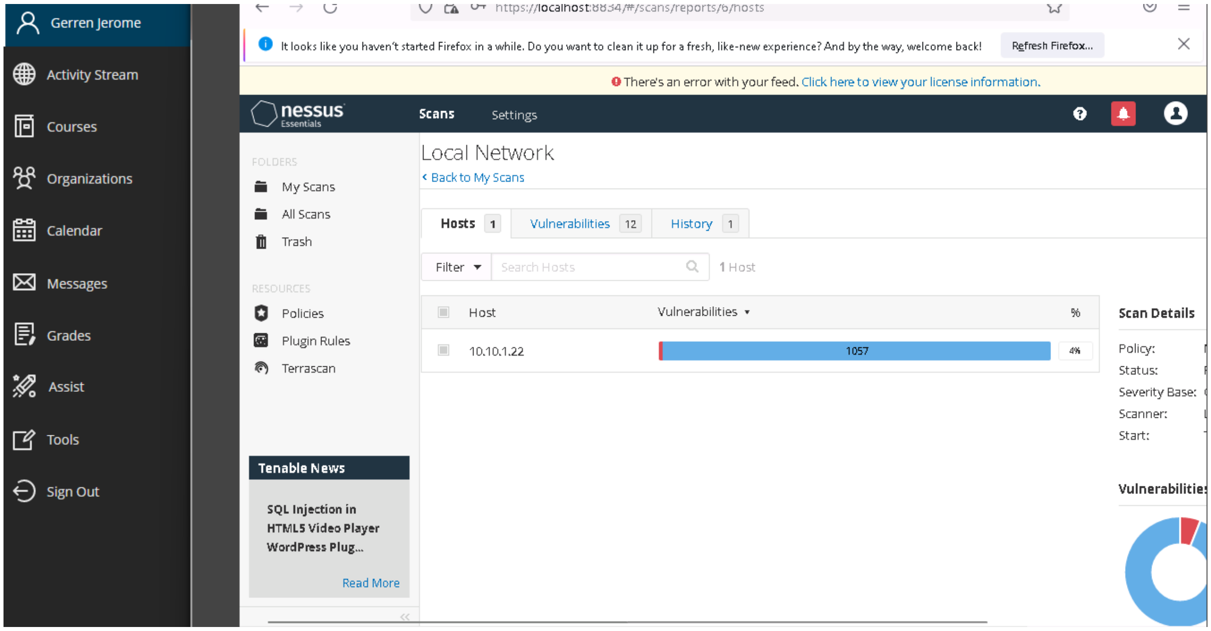
☑ Do not use NTLMv1 authentication

□ Start the Remote Registry service during the scan

□ Enable administrative shares during the scan

Gerren Jerome - Vulnerability Analysis

vi) **Screengrab – Step 22**: Confirm scan is saved and launched successfully



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

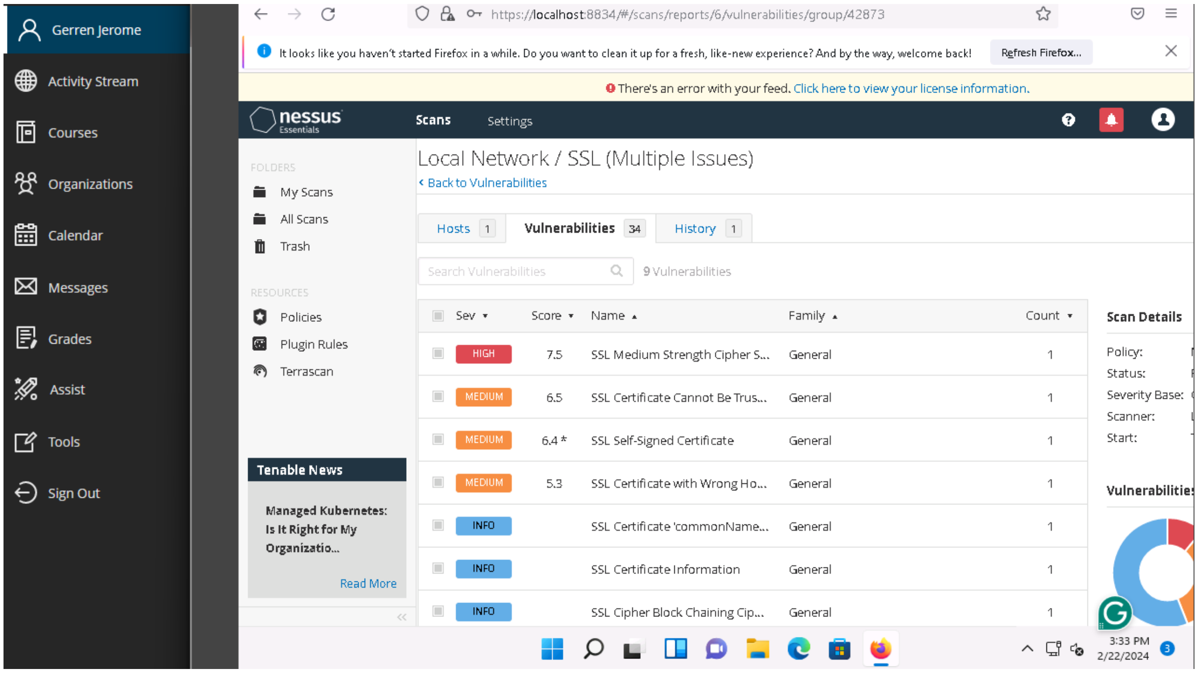
There's an error with your feed. Click here to view your license information.

Local Network

SQL Injection in HTML5 Video Player WordPress Plug...

Host	Vulnerabilities	%
10.10.1.22	1057	4%

vii) **Screengrab – Step 26**: Results of Nessus vulnerability scan (SSL)



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

There's an error with your feed. Click here to view your license information.

Local Network / SSL (Multiple Issues)

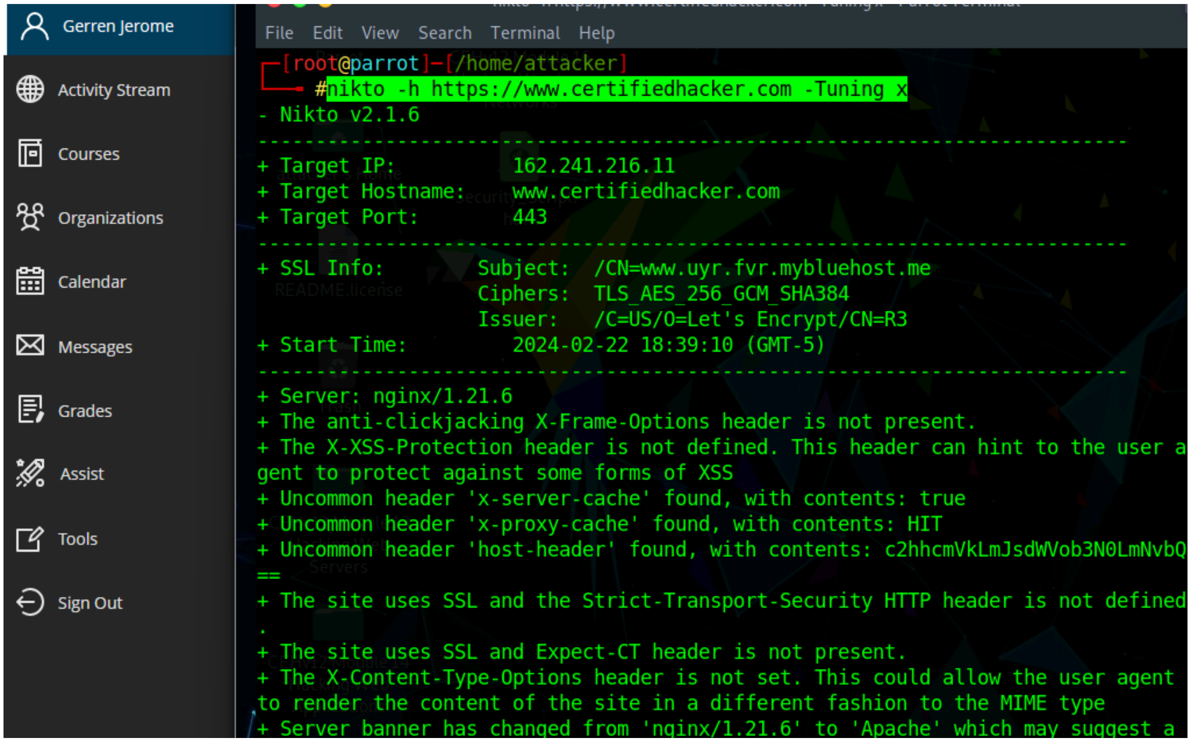
Managed Kubernetes: Is It Right for My Organizatio...

Sev	Score	Name	Family	Count
HIGH	7.5	SSL Medium Strength Cipher S...	General	1
MEDIUM	6.5	SSL Certificate Cannot Be Trus...	General	1
MEDIUM	6.4 *	SSL Self-Signed Certificate	General	1
MEDIUM	5.3	SSL Certificate with Wrong Ho...	General	1
INFO		SSL Certificate 'commonName...	General	1
INFO		SSL Certificate Information	General	1
INFO		SSL Cipher Block Chaining Cip...	General	1

Gerren Jerome - Vulnerability Analysis

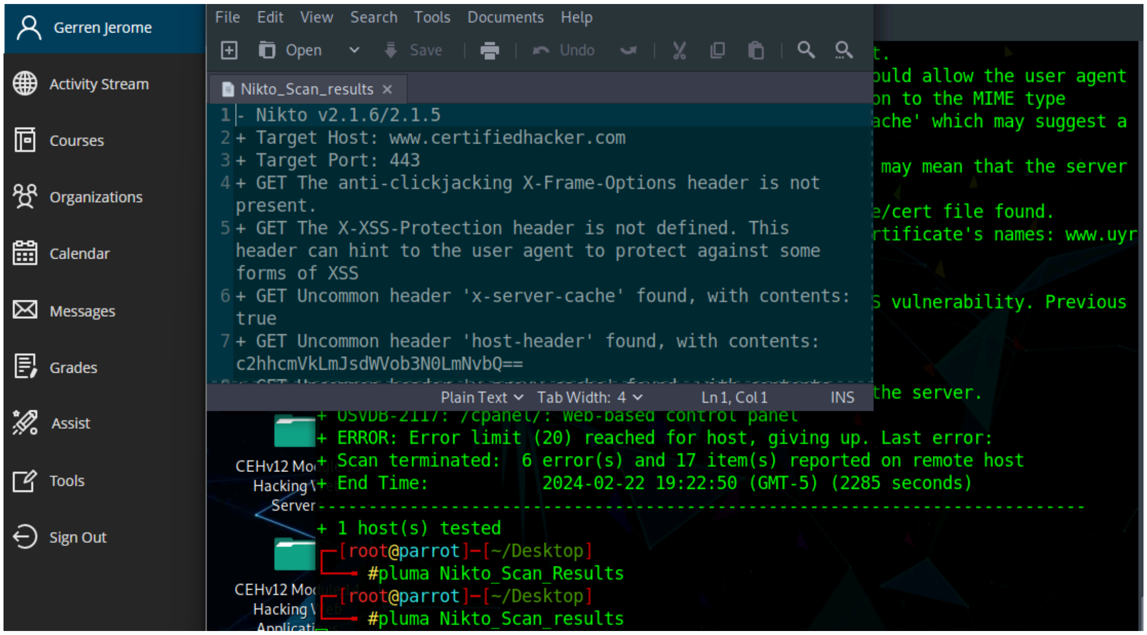
c) Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

i) **Screengrab – Step 8**: Results (Nikto -h TARGET -Tuning x)



```
┌─[root@parrot]─[/home/attacker]
└──╼ #nikto -h https://www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.uyr.fvr.mybluehost.me
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-02-22 18:39:10 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.21.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ
==
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.21.6' to 'Apache' which may suggest a
```

ii) **Screengrab – Step 15**: Open Nikto_Scan_Results in Pluma to audit scan results from Step 14



```
- Nikto v2.1.6/2.1.5
+ Target Host: www.certifiedhacker.com
+ Target Port: 443
+ GET The anti-clickjacking X-Frame-Options header is not
present.
+ GET The X-XSS-Protection header is not defined. This
header can hint to the user agent to protect against some
forms of XSS
+ GET Uncommon header 'x-server-cache' found, with contents:
true
+ GET Uncommon header 'host-header' found, with contents:
c2hhcmVkLmJsdWVob3N0LmNvbQ==
```

```
t.
ould allow the user agent
on to the MIME type
ache' which may suggest a

 may mean that the server

e/cert file found.
rtificate's names: www.uyr

S vulnerability. Previous

the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  6 error(s) and 17 item(s) reported on remote host
+ End Time:          2024-02-22 19:22:50 (GMT-5) (2285 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[root@parrot]─[~/Desktop]
└──╼ #pluma Nikto_Scan_Results
┌─[root@parrot]─[~/Desktop]
└──╼ #pluma Nikto_Scan_results
```