

# Introduction to Vulnerability Analysis Project

## Overview

As part of my role as an ethical hacker with the EC-Council, I undertook a comprehensive vulnerability analysis project. This project focused on identifying and analyzing potential security weaknesses within a target network. By leveraging information acquired during the footprinting and scanning phases, I was able to conduct a thorough investigation into the network's vulnerabilities.

## Objectives

The main objectives of this project were to extract critical information about the target network, including:

- **Network Vulnerabilities:** Identification of network vulnerabilities, listening IPs, TCP/UDP ports, and services.
- **Application and Service Configuration Errors:** Detection of configuration errors and vulnerabilities within applications and services.
- **Operating System and Applications:** Enumeration of the operating systems and applications in use.
- **Weak Passwords and Permissions:** Identification of weak passwords and improper permissions.
- **Default Services and Applications:** Recognition of default services and applications that may need to be removed or secured.

## Tasks and Techniques

To achieve these objectives, a variety of tasks were performed using multiple tools and techniques. These tasks provided practical experience in several enumeration techniques essential for ethical hacking and penetration testing. Key tasks included:

**Vulnerability Research:** Utilizing vulnerability scoring systems and databases to perform thorough research, including Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE).

**Vulnerability Assessment:** Conducting vulnerability assessments using tools such as OpenVAS and Nessus, which involved:

- Performing scans to identify vulnerabilities.
- Analyzing scan results to determine the severity of discovered vulnerabilities.

**Web Server and Application Scanning:** Using tools like CGI Scanner Nikto to identify vulnerabilities in web servers and applications.

## Tools Utilized

The project involved the use of several key tools to perform vulnerability assessments and analyses:

- OpenVAS: For comprehensive vulnerability scanning and analysis.
- Nessus: To conduct detailed vulnerability scans and assess security weaknesses.
- CGI Scanner Nikto: For scanning web servers and applications to detect potential vulnerabilities.

Perform vulnerability research with vulnerability scoring systems and databases.

Perform vulnerability research in Common Weakness Enumeration (CWE)

### CWE search results (SMB)

The screenshot shows the CWE website interface. On the left is a sidebar with navigation links: Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main content area has a header with the CWE logo and navigation links: Home, About, CWE List, Mapping, Top-N Lists, Community, News, and Sign Out. Below the header is a search bar with the text 'SMB' entered. The search results show 'About 48 results (0.25 seconds)'. The first three results are listed: CWE-284: Improper Access Control (4.13) - CWE, CWE-552: Files or Directories Accessible to External Parties ... - CWE, and CWE-319: Cleartext Transmission of Sensitive Information (4.13). Each result includes a link to the CWE List and a brief description.

### Top 25 Most Dangerous Software Weaknesses (CWE VIEW)

The screenshot shows the CWE website interface with the 'Top 25 Most Dangerous Software Weaknesses' view. The sidebar is the same as in the previous screenshot. The main content area has a header with 'Expand All' and 'Collapse All' links. Below the header is a list of 25 weaknesses, each with a number, a description, and a count in parentheses. The list starts with '1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses' and includes items like '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)', and 'Incorrect Default Permissions - (276)'. A 'BACK TO TOP' link is at the bottom right.

Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)

CVE Search (CVE-2021-4034)

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

Search CVE List

Downloads

Data Feeds

Update a CVE Record

Request CVE IDs

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](#).

HOME > CVE > SEARCH RESULTS

Search Results

There are 1 CVE Records that match your search.

Name	Description
<a href="#">CVE-2021-4034</a>	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.

BACK TO TOP

SEARCH CVE USING KEYWORDS:

Submit

You can also search by reference using the [CVE Reference Maps](#).

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

CVE Search (CVE-2021-44228)

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

Search Results

There are 7 CVE Records that match your search.

Name	Description
<a href="#">CVE-2022-33915</a>	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.
<a href="#">CVE-2022-23848</a>	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.
<a href="#">CVE-2021-45046</a>	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.
<a href="#">CVE-2021-44530</a>	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.
<a href="#">CVE-2021-44228</a>	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.
<a href="#">CVE-2021-4125</a>	It was found that the original fix for log4j CVE-2021-44228 and CVE-2021-45046 in the OpenShift metering hive

## CVE Search (CVE-2022-22995)

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

[CVE-2022-22995](#)

ACEweb Online Portal 3.0.0.00 allows unauthorized SMB read capture via CVE. By specifying the CVE 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 OGB10X series (Netcommunity OG410Xa, OG410Xi, OGB10Xa, and OGB10Xi 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 network 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>

## Perform vulnerability research in National Vulnerability Database (NVD)

## NVD Search (CVE-2022-0729)

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

## 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:

NVD

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

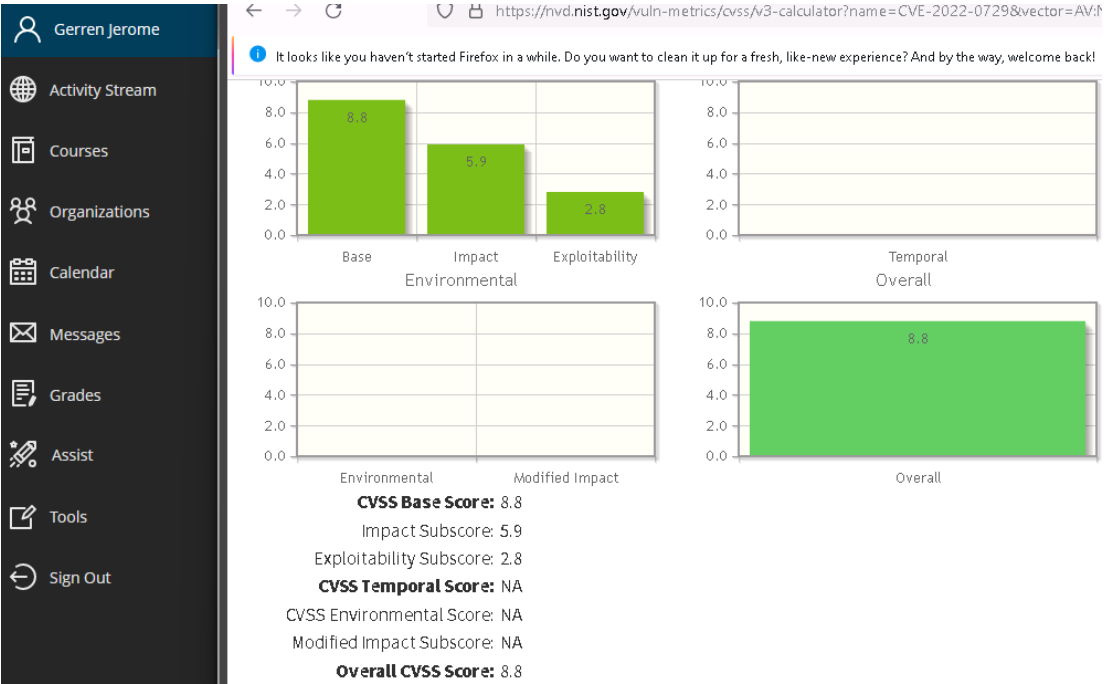
NVD Last Modified:

11/06/2023

Source:

huntr.dev

Graphical Score Representation (CVE-2022-0729)



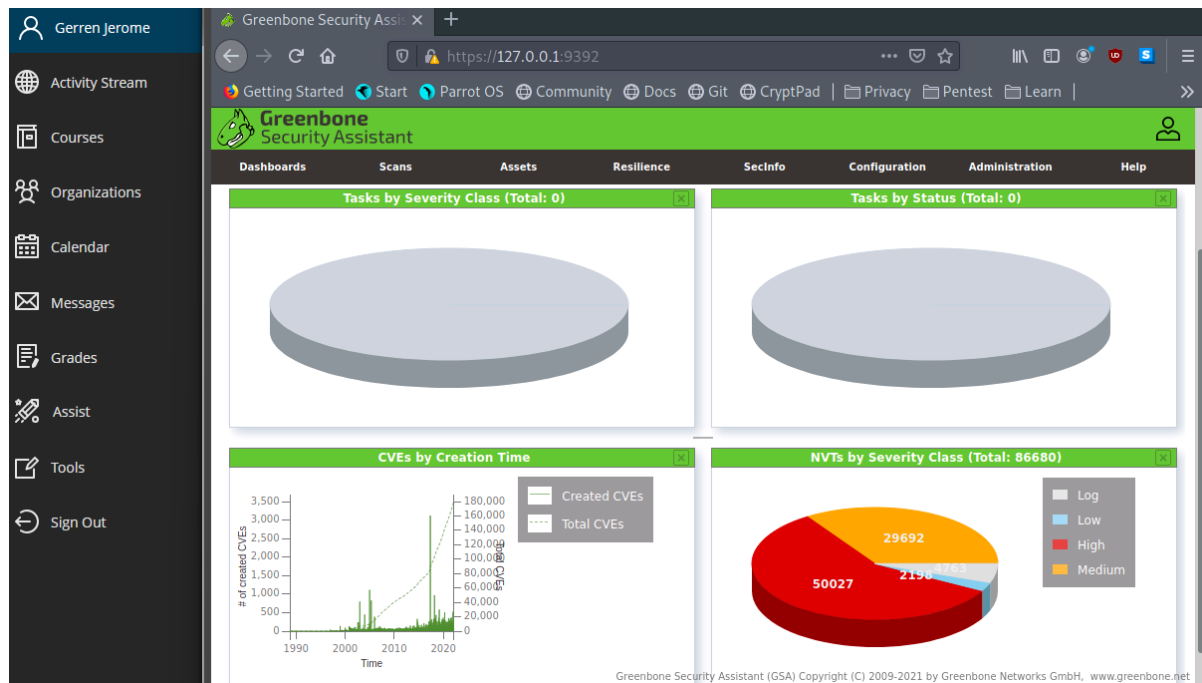
NVD Search (SMB)

Vuln ID	Summary	CVSS Severity
CVE-2023-52442	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate session id and treeid 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 treeid check is skipped. This patch use ksmbd_req_buf_next() to get current command in compound.	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.	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:PUID 0.Oops: 0000.[#1]PREEMPT SMP NOPTICPU: 3.PID: 1736 Comm: _____	V3.x(not available) V2.0(not available)

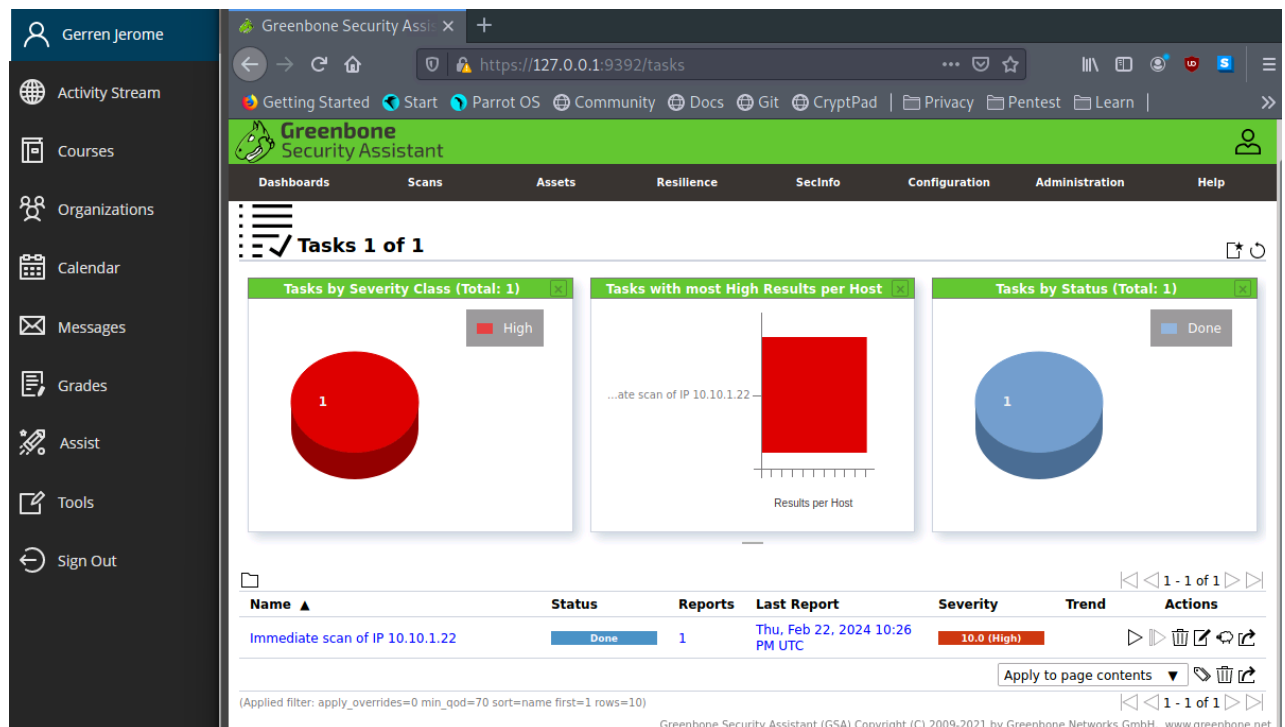
Perform vulnerability assessment using various vulnerability assessment tools.

Perform vulnerability analysis using OpenVAS (5 tasks)

### OpenVAS Dashboard post-login



### OpenVAS scan completed.



Detailed results re: vulnerability under “Report outdated/end of life/scan engine/Environment (local)”

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

Greenbone Security Assistant

DashboardsScansAssetsResilienceSecinfoConfigurationAdministrationHelp

Vulnerability

Severity▼QoDHost IPNameLocationCreated

Report outdated / end-of-life Scan Engine / Environment (local)10.0 (High)97 %10.10.1.22general/tcpThu, 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: 21.1.1

New task in OpenVAS' Tasks section

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

Greenbone Security Assistant

DashboardsScansAssetsResilienceSecinfoConfigurationAdministrationHelp

Tasks 2 of 2

Tasks by Severity Class (Total: 2)

Tasks with most High Results per Host

Tasks by Status (Total: 2)

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)		

Report results (Severity of vulnerabilities)

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

Greenbone Security Assistant

DashboardsScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Filter

Rep Thu, Feb 22, 2024  
ort: 10:53 PM UTC

Done

bdc772cc-9db6-4e6a-9efb-bd6e268229f3

Thu, Feb 22, 2024  
Created: 2024 10:53 PM UTC

Thu, Feb 22, 2024  
Modified: 2024 11:08 PM UTC

Owner: admin

InformationResults (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)

Vulnerability

Severity

QoD

Host IP

Name

Location

Created

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)

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

Perform vulnerability scanning using Nessus.

Nessus Dashboard post-login

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

nessus Essentials

ScansSettings

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!

Refresh Firefox...

There's an error with your feed. [Click here to view your license information.](#)

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

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

Read More

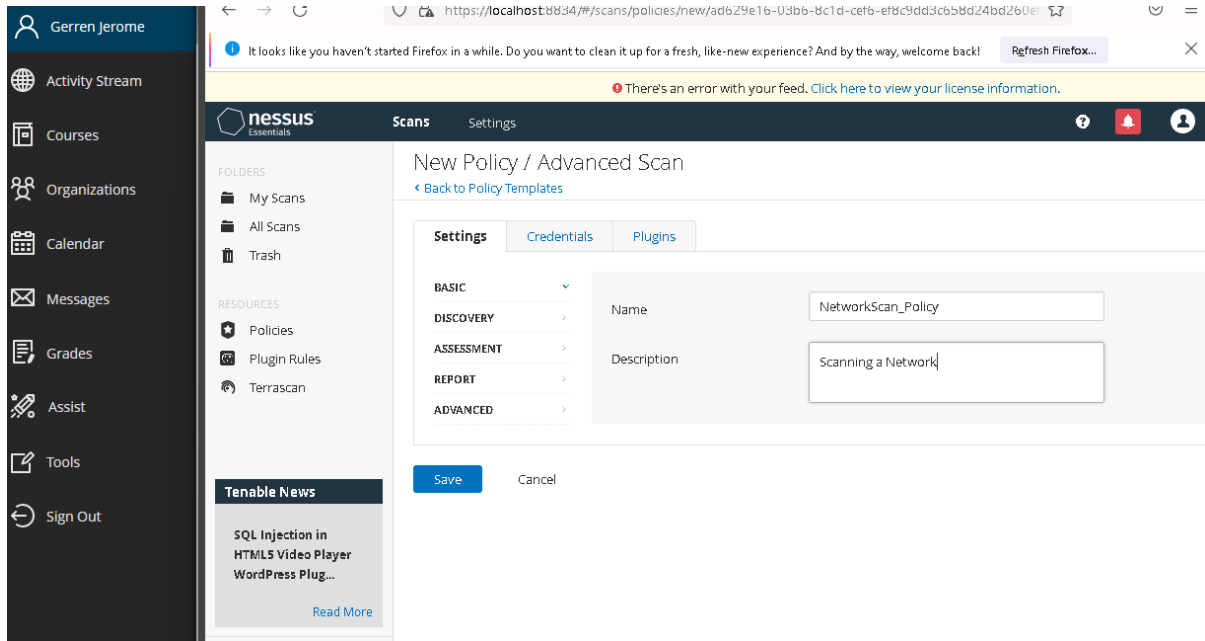
Policies

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.](#)



## Nessus Advanced Scan settings – BASIC



The screenshot shows the Nessus Essentials interface for creating a new policy. The left sidebar contains navigation links: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main content area is titled "New Policy / Advanced Scan" with a "Back to Policy Templates" link. The "Settings" tab is active, showing a list of categories: BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The "BASIC" category is expanded, showing fields for "Name" (NetworkScan\_Policy) and "Description" (Scanning a Network). Below these fields are "Save" and "Cancel" buttons. A "Tenable News" section at the bottom left mentions "SQL Injection in HTML5 Video Player WordPress Plug..." with a "Read More" link.

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

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! Refresh Firefox...

There's an error with your feed. [Click here to view your license information.](#)

nessus Essentials

Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

SQL Injection in HTML5 Video Player WordPress Plug... [Read More](#)

New Policy / Advanced Scan

[Back to Policy Templates](#)

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

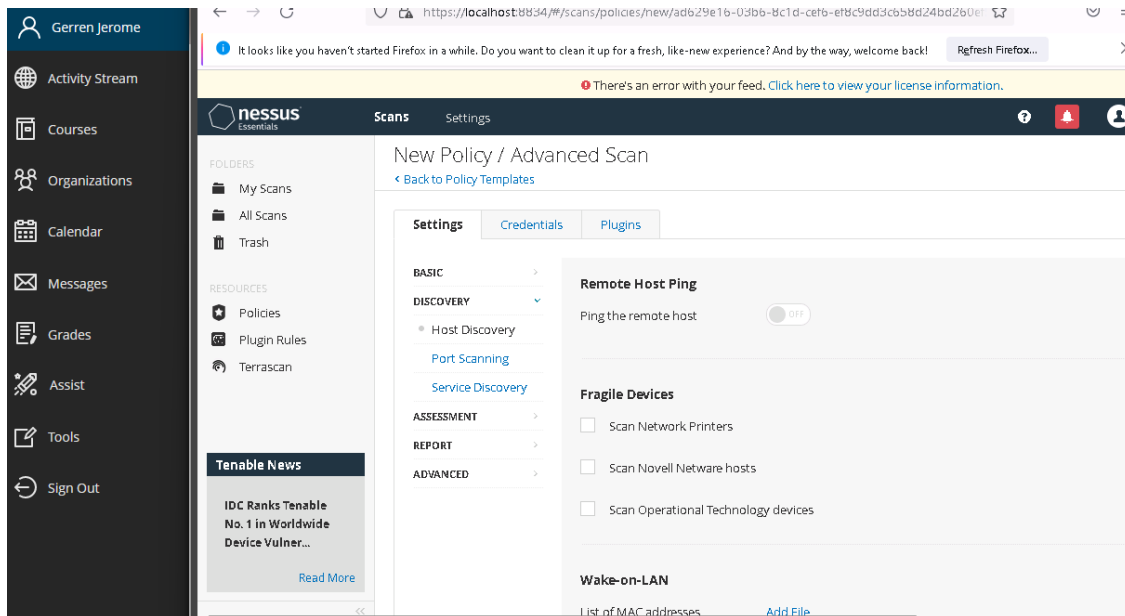
ADVANCED

Name: NetworkScan\_Policy

Description: Scanning a Network

Save Cancel

## Nessus Advanced Scan settings – DISCOVERY



The screenshot shows the Nessus Essentials interface for creating a new policy, specifically the "DISCOVERY" tab. The left sidebar is identical to the previous screenshot. The main content area is titled "New Policy / Advanced Scan" with a "Back to Policy Templates" link. The "Settings" tab is active, and the "DISCOVERY" category is expanded. It shows sub-categories: Host Discovery, Port Scanning, and Service Discovery. The "Remote Host Ping" section has a toggle switch set to "OFF". The "Fragile Devices" section has three checkboxes: "Scan Network Printers", "Scan Novell Network hosts", and "Scan Operational Technology devices". The "Wake-on-LAN" section has a link to "List of MAC addresses" and an "Add File" button. A "Tenable News" section at the bottom left mentions "IDC Ranks Tenable No. 1 in Worldwide Device Vulner..." with a "Read More" link.

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Tools

Sign Out

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! Refresh Firefox...

There's an error with your feed. [Click here to view your license information.](#)

nessus Essentials

Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

IDC Ranks Tenable No. 1 in Worldwide Device Vulner... [Read More](#)

New Policy / Advanced Scan

[Back to Policy Templates](#)

Settings Credentials Plugins

BASIC

DISCOVERY

- Host Discovery
- Port Scanning
- Service Discovery

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host ☐

Fragile Devices

- ☐ Scan Network Printers
- ☐ Scan Novell Network hosts
- ☐ Scan Operational Technology devices

Wake-on-LAN

List of MAC addresses [Add File](#)

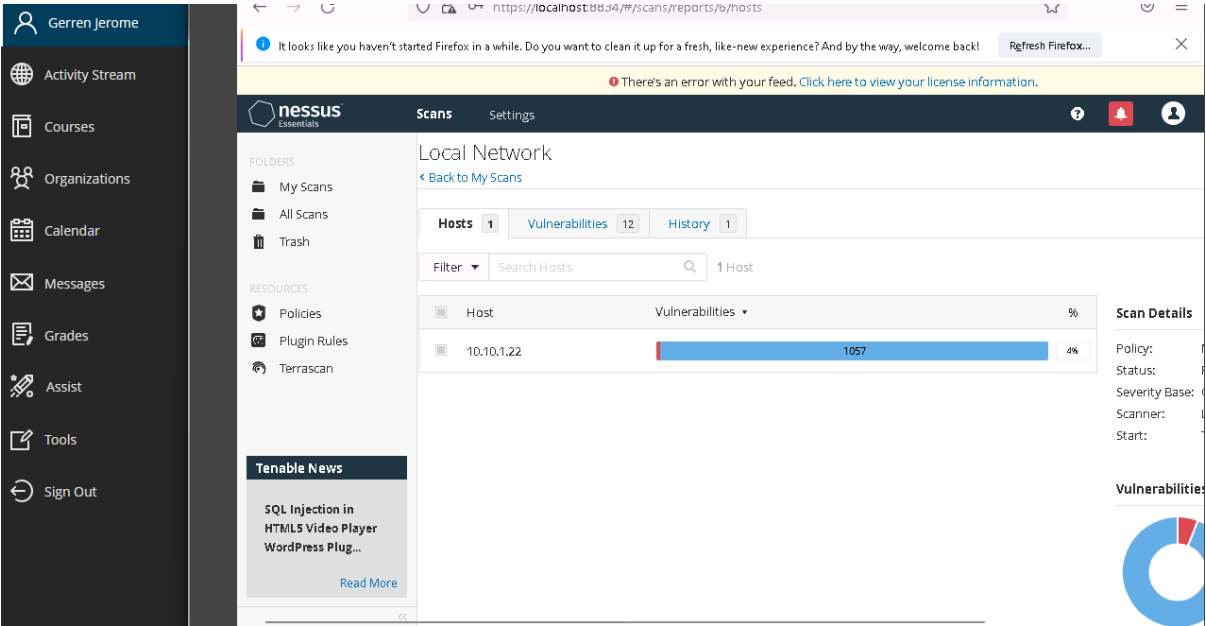
## Nessus Advanced Scan settings – ADVANCED

The screenshot shows the Nessus Scans Settings page. The left sidebar contains navigation links: Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main content area is titled 'Scans Settings' and includes a 'FOLDERS' section with 'My Scans', 'All Scans', and 'Trash'. Below this is a 'RESOURCES' section with 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is also present. The 'Performance Options' section is expanded, showing settings for 'Automatically accept detected SSH disclaimer prompts', 'Scan targets with multiple domain names in parallel', 'Slow down the scan when network congestion is detected', 'Network timeout (in seconds)' (set to 5), 'Max simultaneous checks per host' (set to 5), 'Max simultaneous hosts per scan' (set to 5), 'Max number of concurrent TCP sessions per host' (set to Unlimited), and 'Max number of concurrent TCP sessions per scan' (set to Unlimited). The bottom of the page shows the 'Unix find command Options' section.

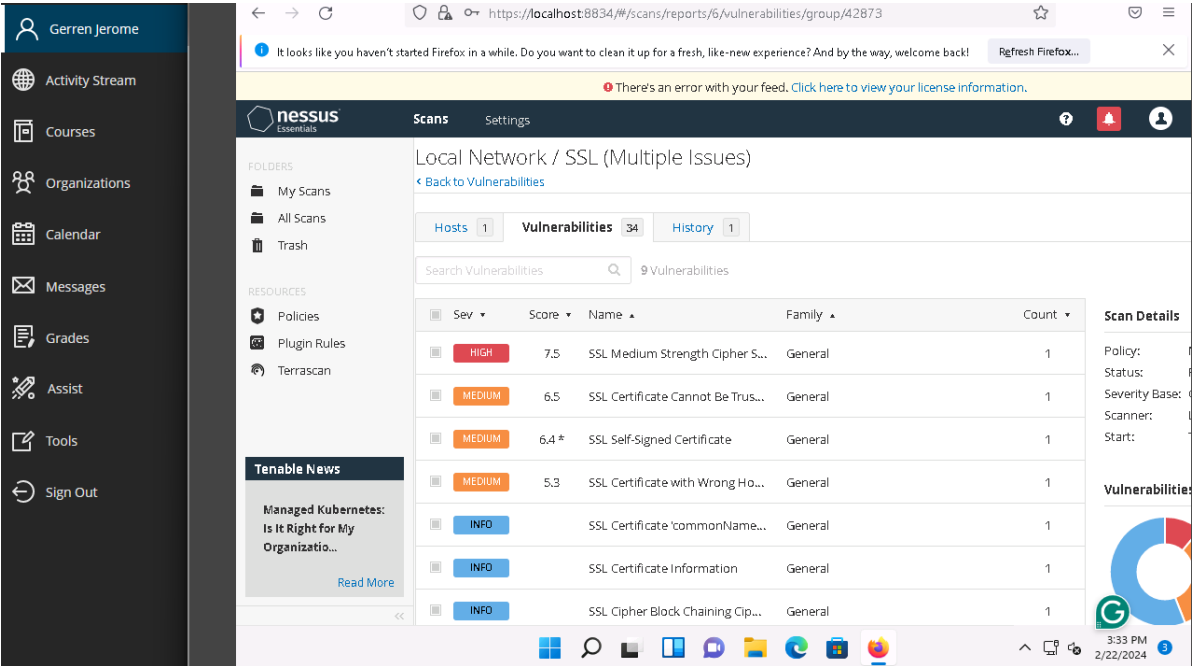
## Specify username and password for Windows credentials.

The screenshot shows the Nessus Scans Settings page, specifically the 'Windows' section. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Scans Settings' and includes a 'FOLDERS' section with 'My Scans', 'All Scans', and 'Trash'. Below this is a 'RESOURCES' section with 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is also present. The 'Windows' section is expanded, showing settings for 'Authentication method' (set to Password), 'Username' (set to CEH123), 'Password' (masked with dots), and 'Domain' (empty). The 'Global Credential Settings' section is also visible, with options for 'Never send credentials in the clear' (checked), 'Do not use NTLMv1 authentication' (checked), 'Start the Remote Registry service during the scan' (unchecked), and 'Enable administrative shares during the scan' (unchecked).

Confirm scan is saved and launched successfully.

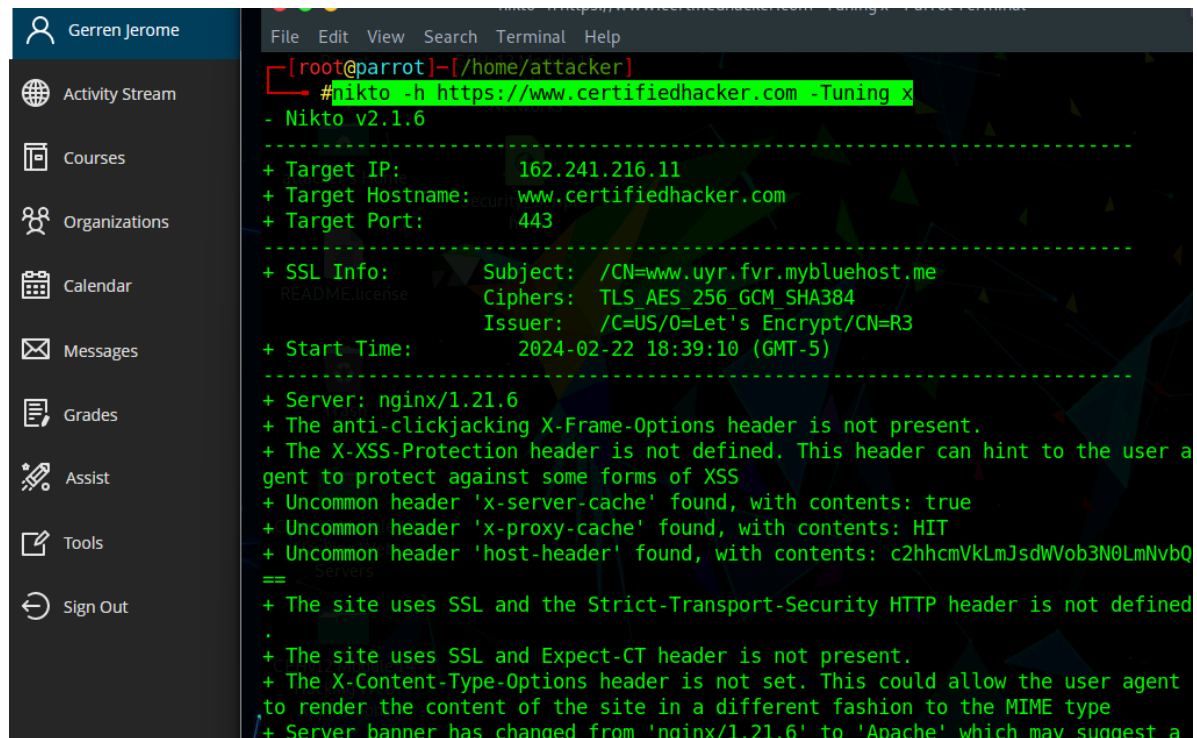


Results of Nessus vulnerability scan (SSL)



## Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

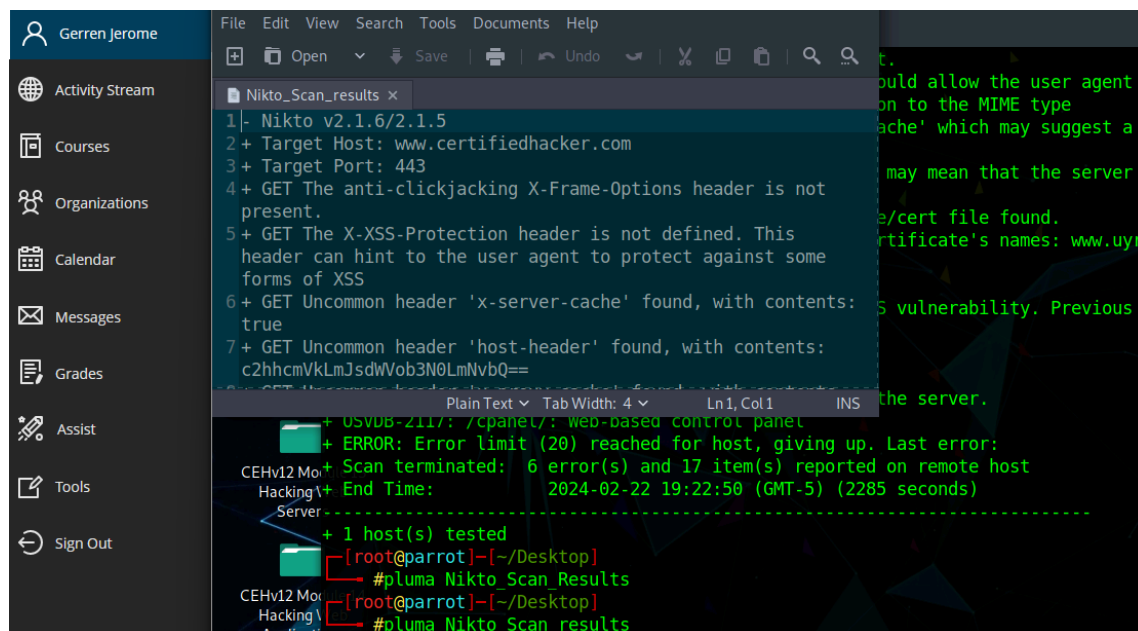
### Results (Nikto -h TARGET -Tuning x)



```
[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 agent 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
```

### Open Nikto scan results in Pluma to audit scan results.



```
File Edit View Search Tools Documents Help
Nikto_Scan_results x
1- Nikto v2.1.6/2.1.5
2+ Target Host: www.certifiedhacker.com
3+ Target Port: 443
4+ GET The anti-clickjacking X-Frame-Options header is not present.
5+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
6+ GET Uncommon header 'x-server-cache' found, with contents: true
7+ GET Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LmNvbQ==
+ 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
```

## Reflection

This project provided hands-on experience with various enumeration techniques and tools critical for effective ethical hacking and penetration testing. Through this project, I developed a deeper understanding of how to identify, analyze, and mitigate potential security threats within a network.