

# Module 05: Vulnerability Analysis

## Scenario

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

## Objective

The objective of this lab is to extract information about the target system that includes, but not limited to:

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

## Overview of Vulnerability Assessment

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

## Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

1. Perform vulnerability research with vulnerability scoring systems and databases
  - Perform vulnerability research in Common Weakness Enumeration (CWE)
  - Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
  - Perform vulnerability research in National Vulnerability Database (NVD)
2. Perform vulnerability assessment using various vulnerability assessment tools
  - Perform vulnerability analysis using OpenVAS
  - Perform vulnerability scanning using Nessus
  - Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

# Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

## Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

## Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

## Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

## Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.

2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type <https://cwe.mitre.org/> and press **Enter**

Note: If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

Note: If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

4. **CWE** website appears. Click on **Search** tab, in the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search icon.

Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



5. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

Note: The search results might differ when you perform this task

6. Now, click any link (here, **CWE-284**) to view detailed information about the vulnerability.

7. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Shows two tabs: "CWE - Search the CWE Web Site" and "CWE - CWE-284: Improper Access Control".
- Address Bar:** Displays the URL <https://cwe.mitre.org/data/definitions/284.html>.
- Content Area:**
  - CWE Logo and Title:** "Common Weakness Enumeration" with subtitle "A Community-Developed List of Software & Hardware Weakness Types".
  - Badges:** "2021 HW" and "Top 25".
  - Breadcrumbs:** Home > CWE List > CWE- Individual Dictionary Definition (4.6).
  - Navigation Links:** Home, About, CWE List, Scoring, Mapping Guidance, Community, News, Search.
  - Section Headers:** "CWE-284: Improper Access Control", "Description", "Extended Description".
  - Text Content:** Describes the weakness as "The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor." It also lists protection mechanisms like authentication, authorization, and accountability.
  - Footnote:** Notes that when any mechanism is not applied or fails, attackers can compromise security by gaining privileges, reading sensitive info, executing commands, evading detection, etc.
  - Bottom Right:** Shows the date and time as "9:02 AM 3/30/2022".

8. Similarly, you can click on other vulnerabilities and view detailed information.

9. Now, click on **Home** to navigate back to the **CWE** website, and click the **CWE List**.

10. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2021)**.

Note: The result might differ when you perform this task.

11. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

Note: The result showing publishing year might differ when you perform this task.

The screenshot shows the Mozilla Firefox browser window with two tabs open. The active tab is titled "CWE - CWE-1337: Weaknesses" and displays a list of 25 software weaknesses from the 2021 CWE Top 25. The weaknesses are categorized by color-coded severity levels: red (Out-of-bounds Write, Improper Neutralization of Input During Web Page Generation, Out-of-bounds Read, Improper Input Validation, Improper Neutralization of Special Elements used in an OS Command, Improper Neutralization of Special Elements used in an SQL Command, Use After Free, Improper Limitation of a Pathname to a Restricted Directory, Cross-Site Request Forgery (CSRF), Unrestricted Upload of File with Dangerous Type, Missing Authentication for Critical Function, Integer Overflow or Wraparound, Deserialization of Untrusted Data, Improper Authentication, NULL Pointer Dereference, Use of Hard-coded Credentials, Improper Restriction of Operations within the Bounds of a Memory Buffer, Missing Authorization, Incorrect Default Permissions, Exposure of Sensitive Information to an Unauthorized Actor, Insufficiently Protected Credentials, Incorrect Permission Assignment for Critical Resource, Improper Restriction of XML External Entity Reference, Server-Side Request Forgery (SSRF), and Improper Neutralization of Special Elements used in a Command). The browser interface includes standard navigation buttons, a search bar with the URL <https://cwe.mitre.org/data/definitions/1337.html>, and a status bar at the bottom.

12. Similarly, you can go back to the CWE website and explore other options, as well.

13. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.

14. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).

15. Close all open windows and document all the acquired information.

## Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <https://cve.mitre.org/> and press **Enter**
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The result might differ when you perform this task.

3. You can copy the name of any vulnerability under the **Newest CVE Records** section and search on CVE to view detailed information on it.
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-4034**) in the search bar, and click **Submit**.

**TOTAL CVE Records: 172812**

**NOTICE:** Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) is underway and will last up to one year. ([details](#))

**NOTICE:** Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.

HOME > CVE LIST > SEARCH CVE LIST

## Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

[View the search tips.](#)

CVE-2021-4034

Submit

Page Last Updated or Reviewed: December 09, 2020

[Site Map](#) | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | [Follow CVE](#)

Use of the CVE® List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the [U.S. Department of Homeland Security \(DHS\) Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999-2022, [The MITRE Corporation](#). CVE and the CVE logo are registered trademarks of The MITRE Corporation.

9:23 AM 3/30/2022 1

5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

Note: We will exploit this vulnerability in Module 06 System Hacking to gain access to the target system.

6. Click on **Search CVE List** at the top of the browser window under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-44228**) in the search bar, and click **Submit**

CVE - Search CVE List

https://cve.mitre.org/cve/search\_cve\_list.html

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...

**CVE**®

CVE List · CNAs · WGs · News & Blog · Board · About · NVD · Go to for: CVSS Scores · CPE Info

Search CVE List · Downloads · Data Feeds · Update a CVE Record · Request CVE IDs

**TOTAL CVE Records: 174834**

**NOTICE:** Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) is underway and will last up to one year. ([details](#))

**NOTICE:** Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.

HOME > CVE LIST > SEARCH CVE LIST

## Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

[View the search tips.](#)

CVE-2021-44228

Submit

Page Last Updated or Reviewed: December 09, 2020

9:52 PM 4/26/2022 1

7. **Search Results** page appears, displaying the records that match the search, click on [CVE-2021-44228](#) link to view the details of the vulnerability.

8. [CVE-2021-44228](#) page appears displaying the information regarding the searched vulnerability.

Note: We will exploit this vulnerability in Module 14 Hacking Web Applications to gain access to the target system.

9. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

The screenshot shows a web browser window with the URL [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html). The page is titled "CVE - Search CVE List". At the top, there are navigation links for "CVE List", "CNAs", "WGs", "News & Blog", "Board", and "About". On the right, there is a "NVD" logo with links to "CVSS Scores" and "CPE Info". Below the header, a black bar contains links for "Search CVE List", "Downloads", "Data Feeds", "Update a CVE Record", and "Request CVE IDs". A message box displays "TOTAL CVE Records: 172812", a red notice about transitioning to a new website, and another notice about changes to record formats. The main content area shows a search bar with "SMB" typed in and a "Submit" button. Below the search bar, a note says "Page Last Updated or Reviewed: December 09, 2020". At the bottom, there are social media links and a footer with copyright information.

10. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

Note: The result might differ when you perform this task.

CVE - Search Results + https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SMB

**CVE** CVE List CNAs WGs Board About NVD Go to for: CVSS Scores CPE Info

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

**TOTAL CVE Records: 172812**

**NOTICE:** Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) is underway and will last up to one year. ([details](#))

**NOTICE:** Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.

HOME > CVE > SEARCH RESULTS

## Search Results

There are **480** CVE Records that match your search.

Name	Description
<a href="#">CVE-2022-22995</a>	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.
<a href="#">CVE-2021-45100</a>	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.
<a href="#">CVE-2021-44548</a>	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. If the attacker has wider access to the network, this may lead to SMB attacks, which may result in: * The exfiltration of sensitive data such as OS user hashes (NTLM/LM hashes), * In case of misconfigured systems, SMB Relay Attacks which can lead to user impersonation on SMB Shares or, in a worse-case scenario, Remote Code Execution This issue affects all Apache Solr versions prior to 8.11.1. This issue only affects Windows.
<a href="#">CVE-2021-44142</a>	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17. 4.14.12

9:26 AM 3/30/2022 1

11. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.

12. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Record Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.

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

**CVE** CVE List CNAs WGs Board About NVD Go to for: CVSS Scores CPE Info

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

**TOTAL CVE Records: 172812**

**NOTICE:** Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) is underway and will last up to one year. ([details](#))

**NOTICE:** Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.

HOME > CVE > CVE-2022-22995

[Printer-Friendly View](#)

CVE-ID
<b>CVE-2022-22995</b> <a href="#">Learn more at National Vulnerability Database (NVD)</a>

**Description**

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.

**References**

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [MISC:<https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities>](#)
- [URL:<https://www.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities>](#)

**Assigning CNA**

Western Digital

9:27 AM 3/30/2022 1

13. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
14. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
15. Close all open windows and document all the acquired information.

## Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type <https://nvd.nist.gov/> and press **Enter**
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.
3. You can click on the CVE-ID link (here, **CVE-2022-0729**) to view detailed information about the vulnerability.

Note: The result might differ when you perform this task.

4. A new webpage appears, displaying **CVE-2022-0729 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.
5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2022-0729**.

Note: - **Base Score**: The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

Note:

Note: - **Temporal Score**: Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.

Note: - **Overall Score**: Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).



The screenshot shows a web browser window titled "NVD - CVSS v3 Calculator". The URL is <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2022-0729&vector=AV:N/AC:L/PR:N/C:L/I:L/A:N>. The main content is titled "Common Vulnerability Scoring System Calculator" and "CVE-2022-0729". A section titled "Source: NIST" explains the components of the CVSS score. Below this, two bar charts are displayed: "Base Scores" and "Temporal". The "Base Scores" chart shows values of 8.8 for Base, 5.9 for Impact, and 2.8 for Exploitability. The "Temporal" chart is currently empty. At the bottom, there is a note: "Note: The results might differ depending upon the selected vulnerability".

7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**.

Note: The results might differ depending upon the selected vulnerability



The screenshot shows the 'Base Score Metrics' section of the NVD - CVSS v3 Calculator. It includes fields for Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), and Scope (S). Each field has three options: 'Network (AV:N)', 'Adjacent Network (AV:A)', 'Local (AV:L)', 'Physical (AV:P)' for AV; 'Low (AC:L)', 'High (AC:H)' for AC; 'None (PR:N)', 'Low (PR:L)', 'High (PR:H)' for PR; 'None (UI:N)', 'Required (UI:R)' for UI; and 'Unchanged (S:U)', 'Changed (S:C)' for S.



9:39 AM  
3/30/2022 1

8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.

9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



The screenshot shows the NVD - Search and Statistics page. At the top, there are search type options ('Basic' selected), results type options ('Overview' selected), and a keyword search field containing 'SMB'. Below the search form, there are sections for 'Search Type' (set to 'All Time') and 'Exact Match' (unchecked). The status bar at the bottom right shows '9:41 AM 3/30/2022'.

10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.

11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

The screenshot shows the NVD - Results page with a table of vulnerabilities. The columns are 'Vuln ID', 'Summary', and 'CVSS Severity'. The first row is for CVE-2022-22995, which is described as allowing arbitrary file writing via SMB and AFP. It was published on March 25, 2022. The CVSS score is V3.1: 8.8 HIGH and V2.0: 6.0 MEDIUM. The second row is for CVE-2020-24772, which describes a exploit in Dreamacro Clash for Windows v0.11.4. It was published on March 21, 2022. The CVSS score is V3.1: 8.8 HIGH and V2.0: 6.8 MEDIUM. The third row is for CVE-2022-24508, which is a Windows SMBv3 Client/Server Remote Code Execution Vulnerability. It was published on March 09, 2022. The CVSS score is V3.1: 8.8 HIGH and V2.0: 6.5 MEDIUM. The fourth row is for CVE-2020-22844, which is a buffer overflow in Mikrotik RouterOS 6.47 causing a denial of service (DOS). It was published on February 28, 2022. The CVSS score is V3.1: 7.5 HIGH and V2.0: 5.0 MEDIUM. The status bar at the bottom right shows '9:41 AM 3/30/2022'.

Vuln ID	Summary	CVSS Severity
<a href="#">CVE-2022-22995</a>	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.	V3.1: 8.8 HIGH V2.0: 6.0 MEDIUM
<a href="#">CVE-2020-24772</a>	In Dreamacro Clash for Windows v0.11.4, an attacker could embed a malicious iframe in a website with a crafted URL that would launch the Clash Windows client and force it to open a remote SMB share. Windows will perform NTLM authentication when opening the SMB share and that request can be relayed (using a tool like responder) for code execution (or captured for hash cracking).	V3.1: 8.8 HIGH V2.0: 6.8 MEDIUM
<a href="#">CVE-2022-24508</a>	Windows SMBv3 Client/Server Remote Code Execution Vulnerability.	V3.1: 8.8 HIGH V2.0: 6.5 MEDIUM
<a href="#">CVE-2020-22844</a>	A buffer overflow in Mikrotik RouterOS 6.47 allows unauthenticated attackers to cause a denial of service (DOS) via crafted SMB requests.	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM

12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.

## Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

### Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

### Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

### Overview of Vulnerability Assessment

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

There are two approaches to network vulnerability scanning:

- Active Scanning
- Passive Scanning

## Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Here, we will perform a vulnerability analysis using OpenVAS.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as a host machine and the **Windows Server 2022 (10.10.1.22)** machine as a target machine.

1. Click on **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting --> Vulnerability Analysis --> Openvas - Greenbone --> Start Greenbone Vulnerability Manager Service** to launch OpenVAS tool.



4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

Note: The password that you type will not be visible.

5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.

The screenshot shows a Parrot OS desktop environment. At the top, there's a menu bar with 'Applications', 'Places', 'System', and a system tray icon. Below the menu bar, there are three application icons: 'Firefox' (selected), 'Parrot Terminal' (disabled), and another unlabelled icon. The main window is a terminal titled 'Parrot Terminal' showing the output of the command 'systemctl status ospd-openvas.service'. The terminal output indicates that the service is active and running. At the bottom, there's a dock with icons for 'Menu', 'Parrot Terminal', and other desktop applications.

```
● ospd-openvas.service - OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-03-30 23:57:47 EDT; 8s ago
     Docs: man:ospd-openvas(8)
           man:openvas(8)
   Process: 1628 ExecStart=/usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas (code=exited, status=0/SUCCESS)
   Main PID: 1640 (ospd-openvas)
      Tasks: 4 (limit: 9417)
     Memory: 34.0M
        CPU: 375ms
       CGroup: /system.slice/ospd-openvas.service
               ├─1640 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas
               └─1642 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas

Mar 30 23:57:46 parrot systemd[1]: Starting OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)...
Mar 30 23:57:47 parrot systemd[1]: Started OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas).

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
```

6. The **Firefox** browser appears, in the address bar, type **<https://127.0.0.1:9392>** and press **Enter**.

7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

8. **OpenVAS Dashboards** appears, as shown in the screenshot.

Greenbone Security Assistant - Dashboards - Mozilla Firefox

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

Tasks by Severity Class (Total: 0)

Tasks by Status (Total: 0)

CVEs by Creation Time

NVTs by Severity Class (Total: 86680)

Created CVEs

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

Log

Menu Parrot Terminal Greenbone Security Ass...

9. Navigate to Scans --> Tasks from the Menu bar.

Note: If a **Welcome to the scan management!** pop-up appears, close it.

Greenbone Security Assistant - Dashboards - Mozilla Firefox

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

Tasks

Report

Results

Vulnerabilities

Notes

Overrides

Tasks by Severity Class (Total: 0)

Tasks by Status (Total: 0)

CVEs by Creation Time

NVTs by Severity Class (Total: 86680)

Created CVEs

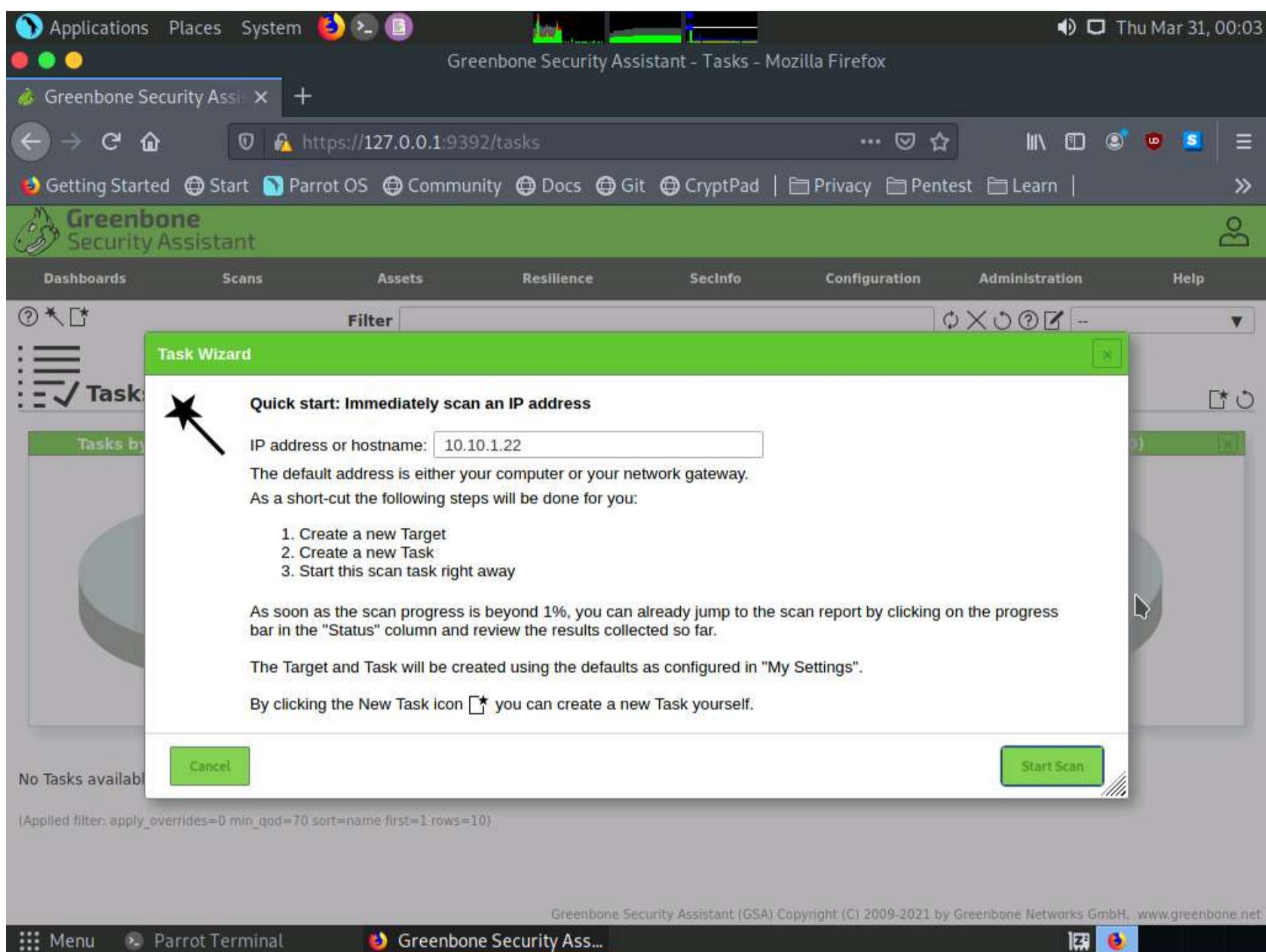
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Log

Menu Parrot Terminal Greenbone Security Ass...

10. Hover over wand icon and click the **Task Wizard** option.

11. The **Task Wizard** window appears; enter the target **IP address in the IP address or hostname** field (here, the target system is **Windows Server 2022 [10.10.1.22]**) and click the **Start Scan** button.



12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Note: It takes approximately 20 minutes for the scan to complete.

Note: If you are logged out of the session then login again using credentials **admin/password**.

14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might differ when you perform this task.

The screenshot shows the Greenbone Security Assistant interface. At the top, there's a navigation bar with links like Applications, Places, System, Getting Started, Start, Parrot OS, Community, Docs, Git, CryptPad, Privacy, Pentest, Learn, and HTTPS Everywhere. Below the navigation bar is a toolbar with various icons for file operations. The main title is "Greenbone Security Assistant - Report Details - Mozilla Firefox". The report details page displays a summary of a scan from March 31, 2022, at 4:03 AM UTC. It includes sections for Information, Results (4 of 46), Hosts (1 of 1), Ports (2 of 17), Applications (0 of 0), Operating Systems (1 of 1), CVEs (1 of 1), Closed CVEs (8 of 8), TLS Certificates (1 of 1), Error Messages (0 of 0), and User Tags (0). A table lists vulnerabilities with columns for Vulnerability, Severity (e.g., 10.0 (High)), QoD (e.g., 97 %), Host IP (e.g., 10.10.1.22), Location (e.g., general/tcp), and Created (e.g., Thu, Mar 31, 2022 4:04 AM UTC). The table shows four entries: Report outdated / end-of-life Scan Engine / Environment (local) (Severity: 10.0 (High)), DCE/RPC and MSRPC Services Enumeration Reporting (Severity: 5.0 (Medium)), SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (Severity: 4.3 (Medium)), and TCP timestamps (Severity: 2.6 (Low)).

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

Menu Parrot Terminal Greenbone Security Ass...

15. Click on any vulnerability under the **Vulnerability** column (here, **Report outdated /end-of-life Scan Engine /Environment (local)**) to view its detailed information.

16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

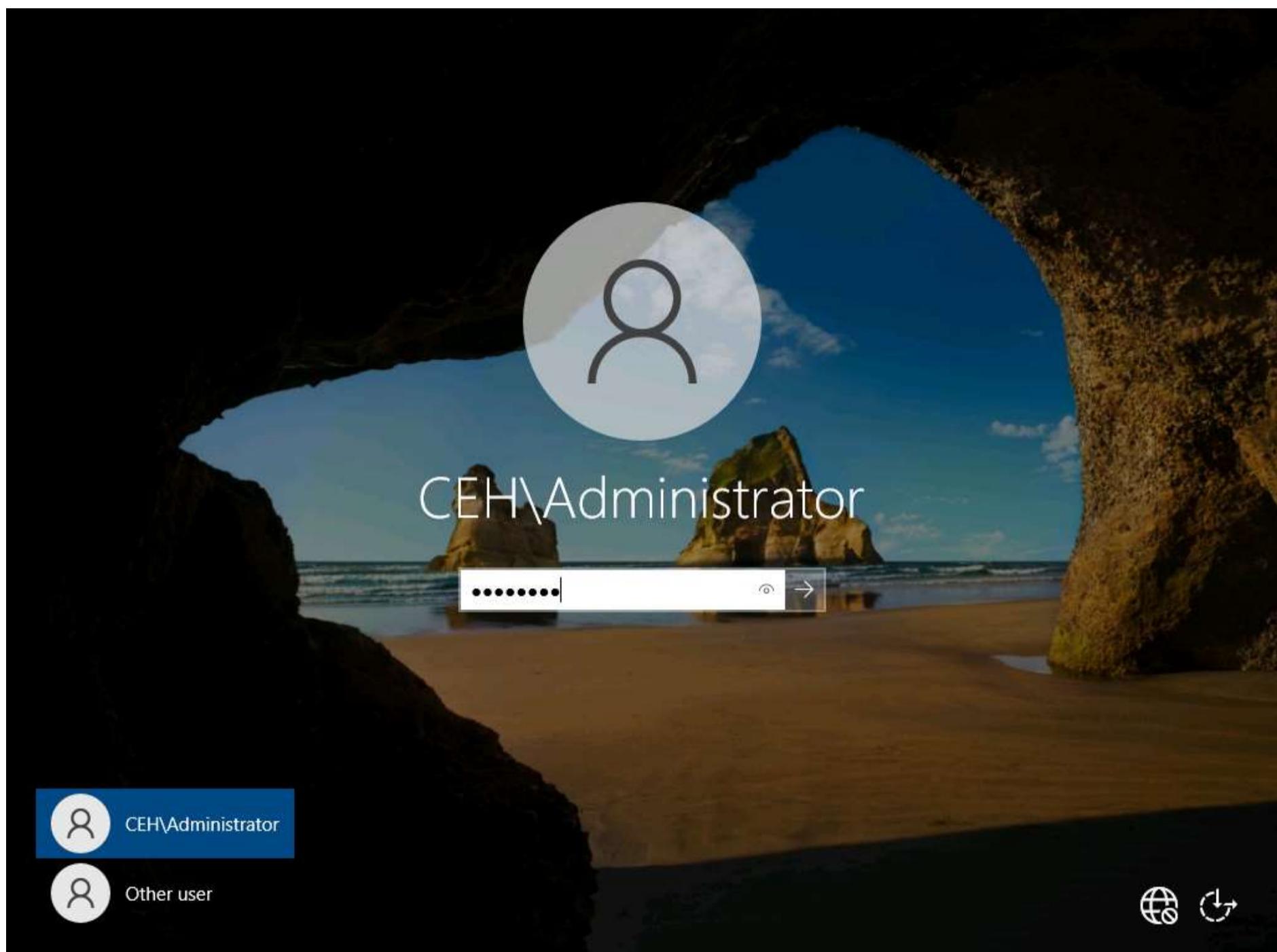
The screenshot shows the detailed information for the selected vulnerability: "Report outdated / end-of-life Scan Engine / Environment (local)". The summary section explains that the script checks for outdated or end-of-life scan engines in environments like GSE and GCE. It notes that while it's not a security vulnerability, it alerts users to potential decreased scan coverage or missing detections. The detection result section states that the installed component is 21.4.1 (OpenVAS libraries on OpenVAS <= 9, openvas-scanner on GVM >= 10), the latest available version is 21.4.3, and the reference URL is https://community.greenbone.net/t/gvm-21-04-stable-initial-release-2021-04-16/8942.

17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.

18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2022** machine.

19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.

20. Click on **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



21. Navigate to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off, enable Windows Firewall**, and click **OK**.

Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.

22. click on **CEHv12 Parrot Security** to switch to **Parrot Security** machine and perform **Steps# 9-11** to create another task for scanning the target system.

23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.

24. After the completion of the scan, click the **Done** button under the **Status** column.

Note: It takes approximately 15-20 minutes for the scan to complete.

**Tasks by Severity Class (Total: 2)**

High

2

**Tasks with most High Results per Host**

...ated scan of IP 10.10.1.22

Results per Host

**Tasks by Status (Total: 2)**

Done

2

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.22	Done	1	Thu, Mar 31, 2022 4:03 AM UTC	10.0 (High)	< > 1 - 2 of 2	
Immediate scan of IP 10.10.1.22	Done	1	Thu, Mar 31, 2022 4:28 AM UTC	10.0 (High)	< > 1 - 2 of 2	

(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

1 - 2 of 2

Menu Parrot Terminal Greenbone Security Ass...

25. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

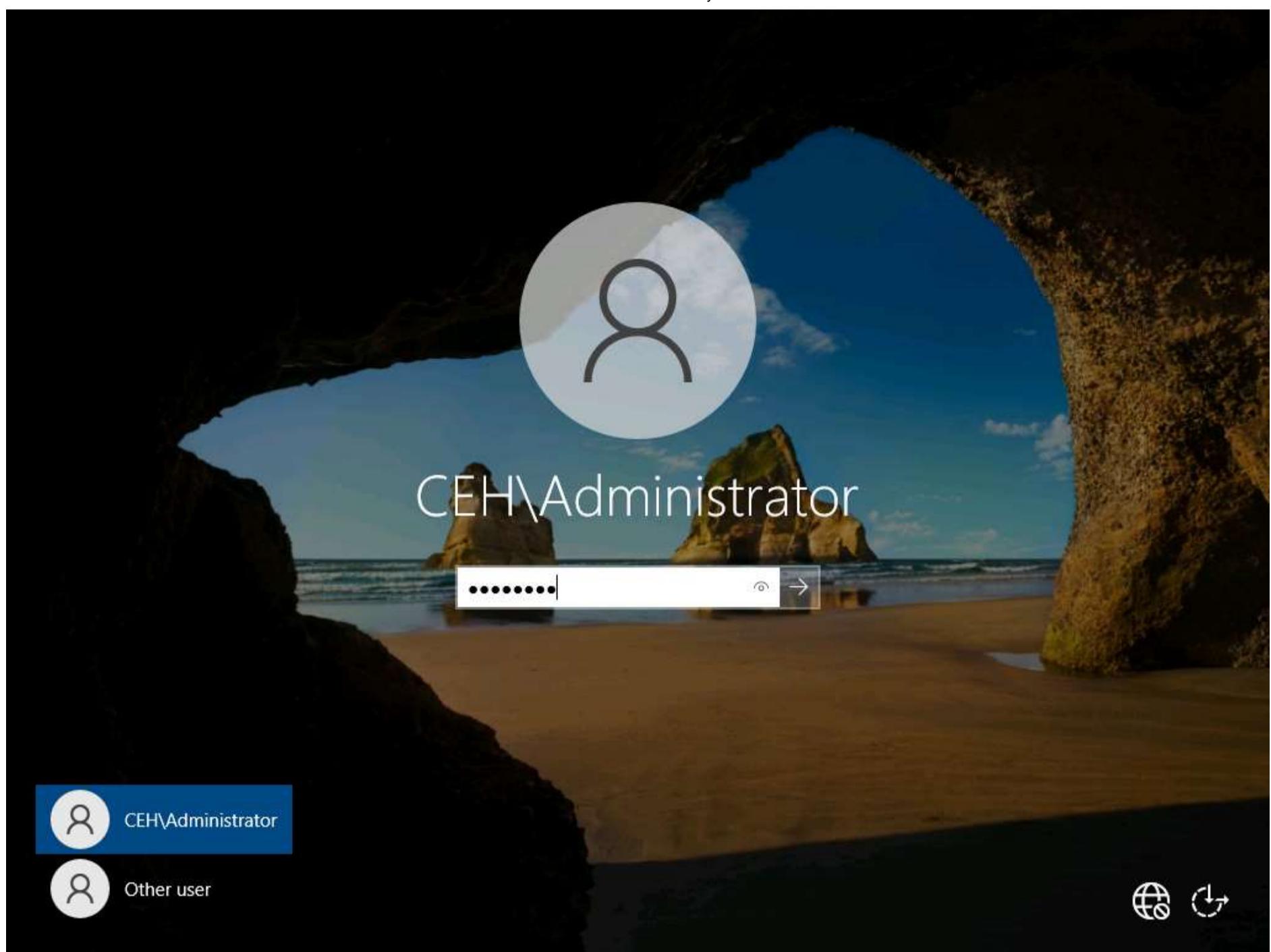
Note: The results might differ when you perform this task.

26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.

27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.

28. Close all open windows and document all the acquired information.

29. Click on **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



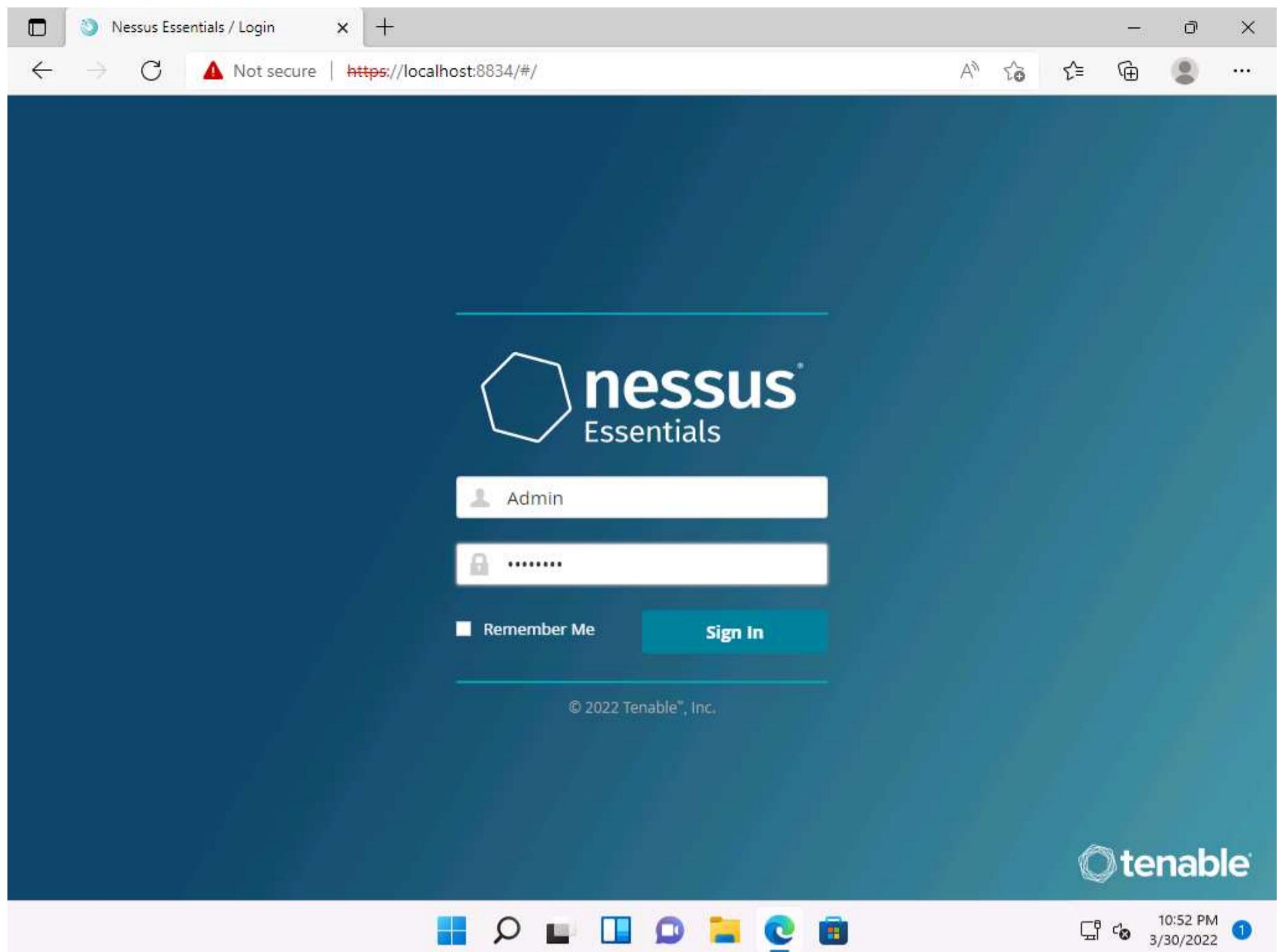
30. Navigate to **Control Panel** --> **System and Security** --> **Windows Defender Firewall** --> **Turn Windows Defender Firewall on or off**, disable Windows Firewall, and click **OK**.

## Task 2: Perform Vulnerability Scanning using Nessus

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

Here, we will use Nessus to perform vulnerability scanning on the target system.

1. Click on **CEHv12 Windows 11** to switch to **Windows 11** machine.
2. Launch any browser, (here, **Microsoft Edge**). In the address bar of the browser place your mouse cursor and type <https://localhost:8834/> and press **Enter**
3. **Your connection isn't private** page appears, expand the **Advanced** section and click **continue to localhost (unsafe)**
4. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In**



- Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.

The screenshot shows the Nessus Essentials interface. On the left sidebar, under the 'RESOURCES' section, the 'Policies' item is selected. A modal dialog box titled 'Welcome to Nessus Essentials' is displayed in the center. The dialog contains instructions about host discovery scans and a 'Targets' input field with an example value. At the bottom of the dialog are 'Close' and 'Submit' buttons.

6. The Nessus Essentials dashboard appears; click **Policies** under RESOURCES section from the pane on the left.

The screenshot shows the Nessus Essentials interface with the 'Policies' item selected in the 'RESOURCES' sidebar. A sub-menu 'Policies (P)' is visible next to it. The main content area displays a message: 'This folder is empty. Create a new scan.' Below this message is a 'Tenable News' section. The browser's address bar shows the URL <https://localhost:8834/#/scans/policies>.

7. The Policies window appears; click **Create a new policy**.

8. The **Policy Templates** window appears; click **Advanced Scan**.

9. The **New Policy / Advanced Scan** section appears.

10. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan\_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).

11. 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 Nessus Essentials interface for creating a new policy. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). A Tenable News sidebar is present. The main area title is 'New Policy / Advanced Scan'. The 'Settings' tab is active. On the left, a navigation tree includes BASIC, DISCOVERY (selected), ASSESSMENT, REPORT, and ADVANCED. Under DISCOVERY, Host Discovery is expanded, showing Port Scanning (selected) and Service Discovery. Under ADVANCED, Performance Options settings are shown, with 'Max number of concurrent TCP sessions per host' and 'Max number of concurrent TCP sessions per scan' both set to 'Unlimited'. The right pane contains sections for Ports (unchecked for unscanned ports) and Local Port Enumerators (SSH, WMI, SNMP checked; 'Verify open TCP ports found by local port enumerators' checked).

13. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.

The screenshot shows the Nessus Essentials interface for editing a new policy. The left sidebar includes 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section with a link to 'Cr8escape: How Tenable Can Help (CVE-2022-0811)' and a 'Read More' button. The main content area has tabs for 'Scans' and 'Settings'. Under 'Scans', there are sections for 'Discovery' (Folders: My Scans, All Scans, Trash; Resources: Policies, Plugin Rules, Terrascan), 'Assessment' (Report: Scan IP addresses in a random order; Advanced: Automatically accept detected SSH disclaimer prompts, Scan targets with multiple domain names in parallel), and 'Performance Options' (Network timeout: 5 seconds, 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). The status bar at the bottom shows icons for file operations, search, and refresh, along with the date and time (10:59 PM, 3/30/2022).

14. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.

15. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**.

Note: Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.

The screenshot shows the Nessus Essentials interface with the title bar "Nessus Essentials / Policies / Edit". The address bar indicates "Not secure" and the URL "https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8...". The main content area is titled "Windows" and contains fields for "Authentication method" (set to "Password"), "Username" (set to "CEH123"), "Password" (represented by a series of dots), and "Domain" (empty). Below this is a section titled "Global Credential Settings" with several checkboxes:

- 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
- Start the Server service during the scan

Enabling the Server service may allow remote access to file shares, named pipes and other system services. This may weaken the security of target systems or even facilitate a complete compromise.

The bottom right corner of the window shows the date and time "11:03 PM 3/30/2022" and a notification badge with the number "1".

16. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.

17. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.

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.

<input type="checkbox"/> Name	Template	Last Modified
<input type="checkbox"/> NetworkScan_Policy	Advanced Scan	Today at 11:04 PM

18. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.

19. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan\_Policy**.

Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser --> Click on History --> Clear History and make sure that cache and cookies are checked and click on clear and login to the **Nessus Essentials** again.

The screenshot shows the Nessus Essentials / Scan Template interface. The main pane displays 'Scan Templates' with a single entry: 'NetworkScan\_Policy' (Scanning a Network). The 'User Defined' tab is active. The left sidebar includes sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' sidebar is present. The bottom right corner shows system status icons and the date/time '11:06 PM 3/30/2022'.

20. The **New Scan / NetworkScan\_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 target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.1.22 (Windows Server 2022)**.

New Scan / NetworkScan\_Policy

[Back to Scan Templates](#)

**Settings**

**BASIC**

- General
- Schedule
- Notifications

Name	Local Network
Description	Scanning a local network
Folder	My Scans
Targets	10.10.1.22

Upload Targets      Add File

**Save** ▾      Cancel

11:09 PM  
3/30/2022

21. 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.

New Scan / NetworkScan\_Policy

[Back to Scan Templates](#)

**Settings**

**BASIC**

- General
- Schedule
- Notifications

Enabled	<input type="radio"/> Off
---------	---------------------------

**Save** ▾      Cancel

**Launch**

11:09 PM  
3/30/2022

22. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.

The screenshot shows the Nessus Essentials web interface. The top navigation bar displays the URL <https://localhost:8834/#/scans/folders>. The main content area is titled "My Scans" and shows one scan entry:

Name	Schedule	Last Modified
Local Network	On Demand	Today at 11:10 PM

The sidebar on the left contains sections for "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). A "Tenable News" sidebar on the left features a news item about the 2021 Top Vulnerabilities. The bottom right corner of the screen shows the Windows taskbar with the date 3/30/2022 and time 11:10 PM.

23. After the completion of the scan: click **Local Network** to view the detailed results.

Note: It takes approximately 15-20 minutes for the scan.

24. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with '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 'Local Network' and shows a scan report for host 10.10.1.22. The 'Vulnerabilities' tab is selected, showing 34 vulnerabilities. A pie chart indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue). A note at the bottom states: 'Note: The list of vulnerabilities may differ when you perform this task.'

25. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ when you perform this task.

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

27. The **Local Network / SSL (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SSL Medium...**) to view its detailed information.

28. The report regarding selected vulnerability **SSL Medium Strength Cipher Suites Supported (SWEET32)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

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

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

31. Once the download is finished, a pop-up appears at the top of the browser; click **Open file**.

32. The Nessus scan report appears in the **Edge** web browser, as shown in the screenshot.

Note: Screenshots and browser might differ when you perform this task.

33. You can click the **Expand All** option to view the detailed scan report.

Nessus logo

Report generated by Nessus™

## Local Network

Wed, 30 Mar 2022 23:27:10 Pacific Standard Time

### TABLE OF CONTENTS

- [Vulnerabilities by Host](#)
  - 10.10.1.22

#### Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

Category	Count
Information Disclosure	0
Denial of Service	2
File Disclosure	5
Protocol Issues	0
Software Vulnerabilities	51

Windows taskbar icons: Start, Search, Task View, Mail, File Explorer, Edge, Taskbar settings. Date and time: 11:49 PM 3/30/2022. Notification: 1.

34. A list of discovered vulnerabilities appears. You can further click on plugins (here, [42873](#)) to view more detailed information on the vulnerability

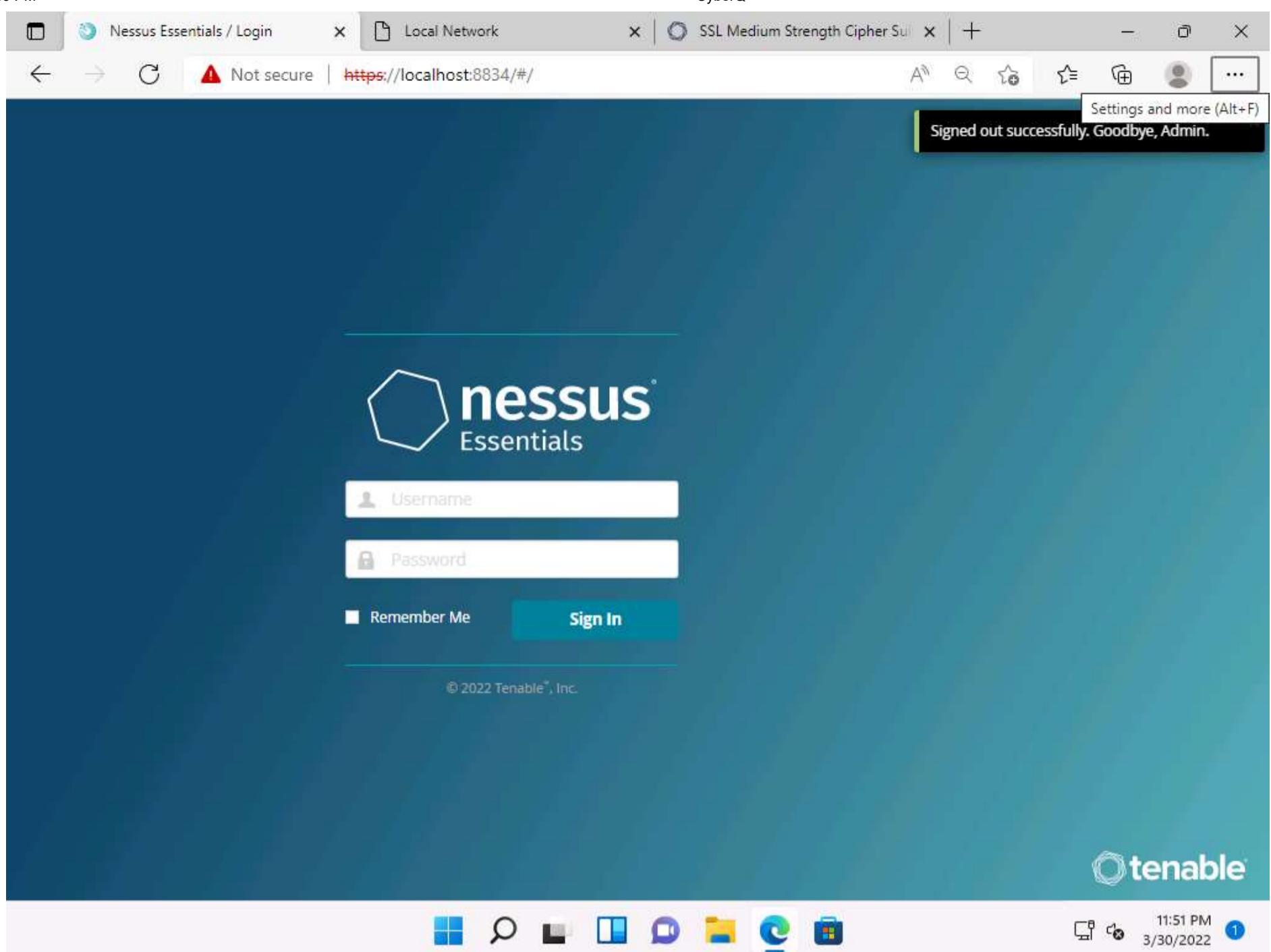
Note: The results might differ when you perform this task.

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

36. In this way, you can select a vulnerability of your choice to view the complete details.

37. Once the vulnerability analysis is done, switch back to the tab where Nessus is running and click **Admin --> Sign Out** in the top-right corner.

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



39. This concludes the demonstration of performing vulnerability assessment using Nessus.

40. Close all open windows and document all the acquired information.

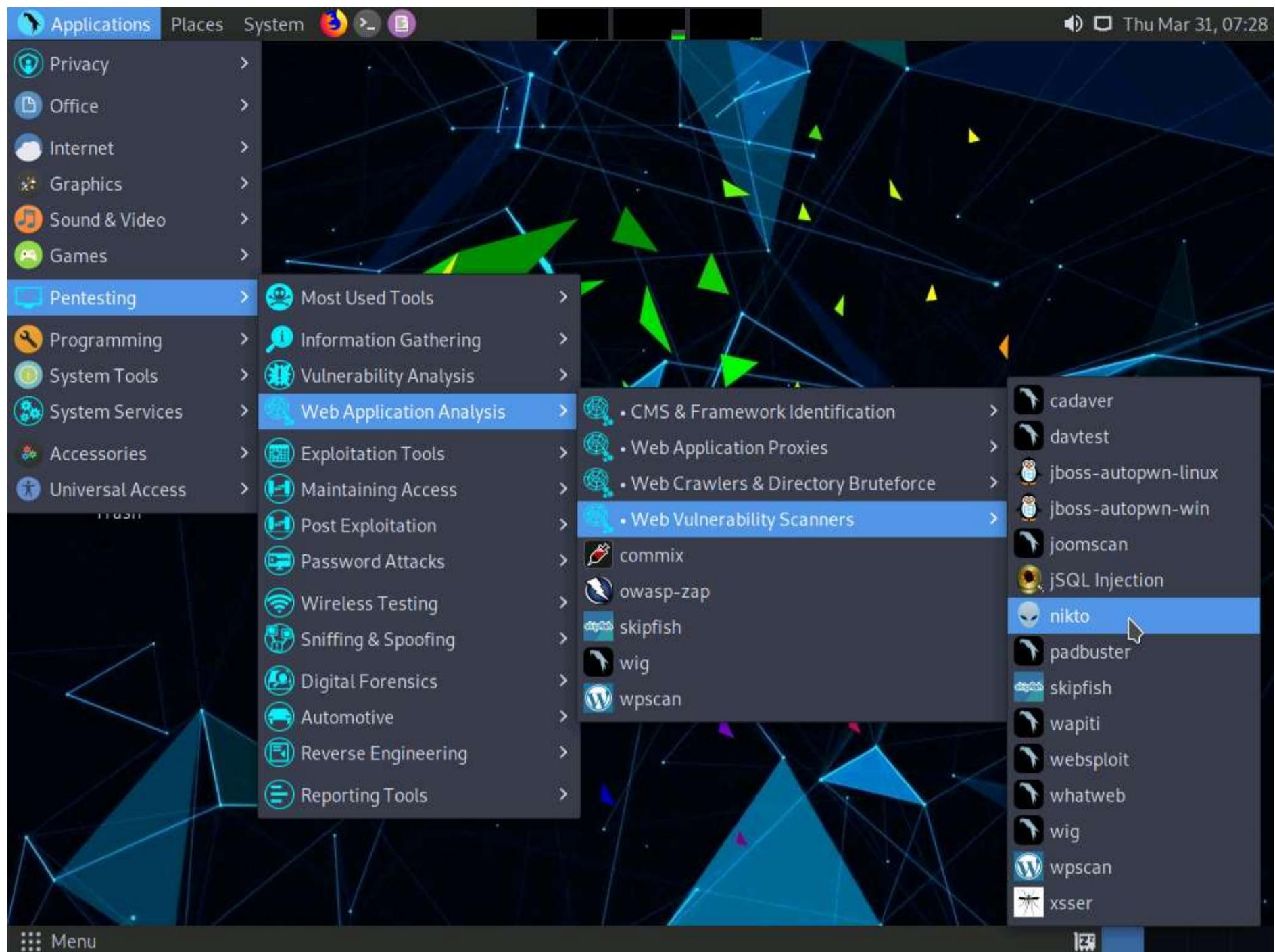
## Task 3: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

Here, we will use Nikto to scan web servers and applications for vulnerabilities.

Note: In this task, we will target the [www.certifiedhacker.com](http://www.certifiedhacker.com) website.

1. Click on **CEHv12 Parrot Security** to switch to **Parrot Security** machine.
2. Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting --> Web Application Analysis --> Web Vulnerability Scanners --> nikto** to open Nikto in the **Terminal** window.



3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

Note: The password that you type will not be visible.

4. Nikto scanning options will be displayed to scan the target website.

5. You can further type **nikto -H** and press **Enter** to view various available commands with full help text

The screenshot shows a terminal window titled "nikto -H - Parrot Terminal". The terminal displays the help menu for the Nikto tool. The menu includes various options such as -ask+, -Cgidirs+, -config+, -Display+, -dbcheck, and -evasion+. It also provides detailed descriptions and lists of available options for each command.

```

[root@parrot]~[/home/attacker]
#nikto -H

Options:
  -ask+           Whether to ask about submitting updates
                  yes Ask about each (default)
                  no  Don't ask, don't send
                  auto Don't ask, just send
  -Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
                  1 Show redirects
                  2 Show cookies received
                  3 Show all 200/OK responses
                  4 Show URLs which require authentication
                  D Debug output
                  E Display all HTTP errors
                  P Print progress to STDOUT
                  S Scrub output of IPs and hostnames
                  V Verbose output
  -dbcheck         Check database and other key files for syntax errors
  -evasion+       Encoding technique:
                  1 Random URI encoding (non-UTF8)
                  2 Directory self-reference (./.)
                  3 Premature URL ending
                  4 Prepend long random string
                  5 Fake parameter
                  6 TAB as request spacer
                  7 Change the case of the URL
                  8 Use Windows directory separator (\)

```

6. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

**Note:** A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply “interesting” files is undesired.

7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is <https://www.certifiedhacker.com>) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

**Note:** **-h:** specifies the target host and **x:** specifies the Reverse Tuning Options (i.e., include all except specified).

**Note:** The scan takes approximately 10 minutes to complete.

8. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

**Note:** The result might differ when you perform this task.

9. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.

10. In the terminal window, type **nikto -h (Target Website) -Cgidirs all**, (here, the target website is <https://www.certifiedhacker.com>) and hit **Enter**.

**Note:** **-Cgidirs:** scans the specified CGI directories; users can use filters such as “**none**” or “**all**” to scan all CGI directories or none).

**Note:** The scan takes approximately 10 minutes to complete.

11. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

Note: You can use try this command on another website to obtain information about CGI directories.

```
nikto -h https://www.certifiedhacker.com -Cgidirs all - Parrot Terminal
File Edit View Search Terminal Help
#nikto -h https://www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        443
+ SSL Info:           Subject: /CN=cpanel.certifiedhacker.com
                      Ciphers: TLS_AES_256_GCM_SHA384
                      Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2023-07-11 01:00:19 (GMT-4)
+ 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 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ 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 WAF, load balancer or proxy is in place
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Hostname 'www.certifiedhacker.com' does not match certificate's names: cpanel.certifiedhacker.com
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

12. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd** and press **Enter** to jump to the root directory.

13. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.

A screenshot of a Parrot OS desktop environment. The desktop background is dark with a green and blue geometric pattern. In the top left corner, there's a dock with icons for Applications, Places, System, and a terminal. The top right corner shows system status with a battery icon, signal strength, and the date/timestamp "Tue Jul 11, 01:07". A terminal window titled "cd Desktop - Parrot Terminal" is open at the bottom, showing a command-line session:

```
[root@parrot]~/Desktop]$ cd
```

The terminal window has a dark theme with white text. Below the terminal is a file browser window titled "File Manager". It shows a tree view of the file structure:

```
[root@parrot]~/Desktop]$ [root@parrot]~$ [root@parrot]~/Desktop]$ #
```

The file browser lists several folders:

- attacker's Home
- CEHV12 Module 16
- Hacking Wireless Networks
- Security Scripts
- README license
- Trash
- CEHV12 Module 13
- Hacking Web Servers
- CEHV12 Module 11
- Hacking Web Applications

The "Security Scripts" folder contains some files: "html", "Security\_Script", and "Security\_Script.html".

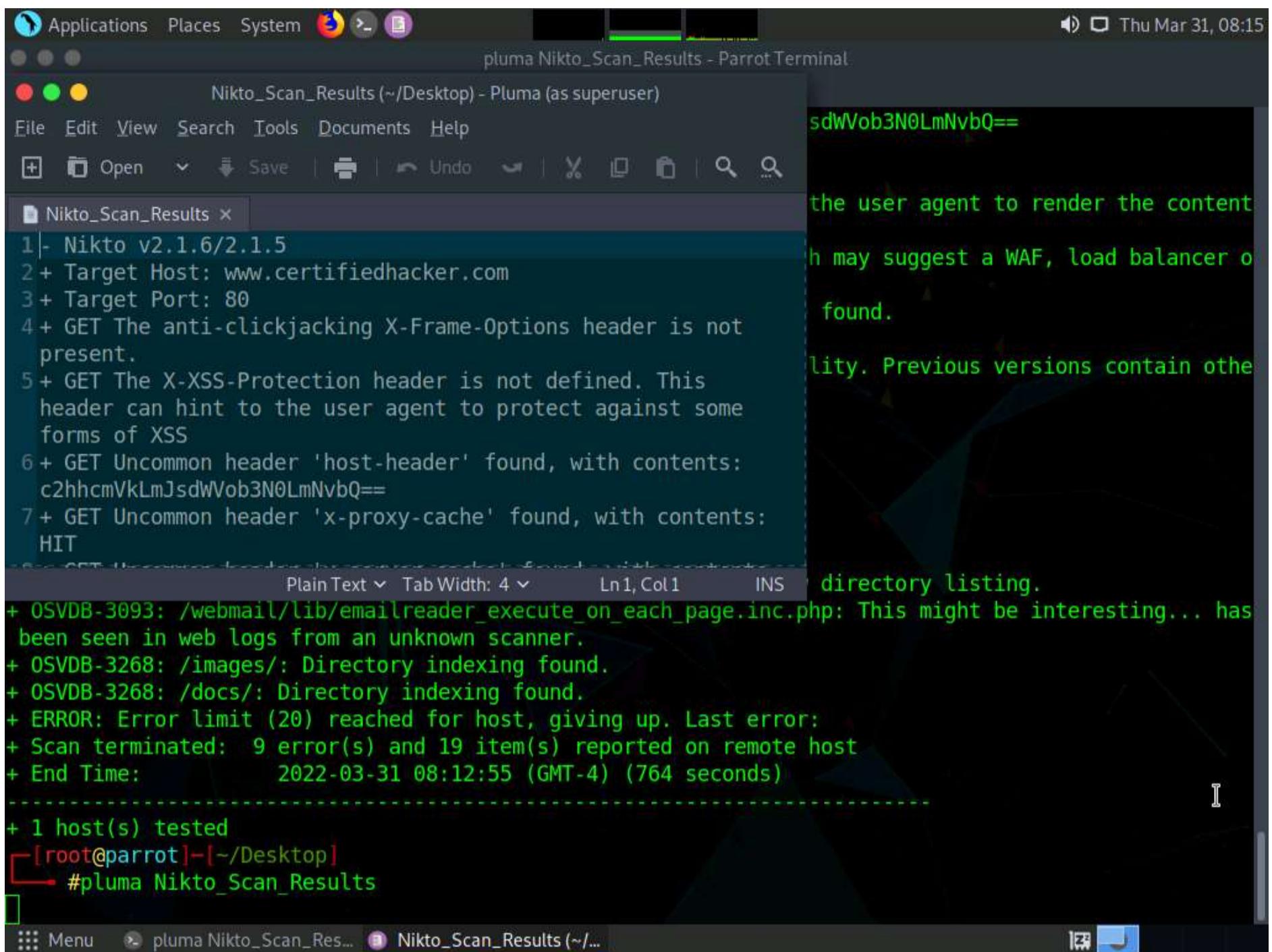
14. Type **nikto -h (Target Website) -o (File\_Name) -F txt**, (here, the target website is <https://www.certifiedhacker.com>) and press **Enter**

Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

Note: Name the file **Nikto\_Scan\_Results**

Note: The scan takes approximately 10 minutes to complete.

15. Now, type **pluma Nikto\_Scan\_Results** and press **Enter** to open the created file in a text editor window. The file appears displaying the scanned results, as shown in the screenshot.



The screenshot shows a terminal window titled "pluma Nikto\_Scan\_Results - Parrot Terminal". The window contains the output of a Nikto scan. The text is color-coded: green for informational messages, red for errors, and blue for warnings. Key findings include:

- Target Host: www.certifiedhacker.com
- Target Port: 80
- GET requests show missing X-Frame-Options and X-XSS-Protection headers.
- Uncommon headers 'host-header' and 'x-proxy-cache' were found.
- An OSVDB-3093 vulnerability was identified in /webmail/lib/emailreader\_execute\_on\_each\_page.inc.php.
- Directory indexing was found in /images/ and /docs/.
- The scan reached an error limit of 20 and terminated.
- Scan completed at 2022-03-31 08:12:55 (GMT-4).
- 1 host(s) were tested.

The terminal window has a dark theme with a light-colored text area. The status bar at the bottom shows "Plain Text" and "Ln1, Col1". The title bar says "pluma Nikto\_Scan\_Results - Parrot Terminal". The menu bar includes File, Edit, View, Search, Tools, Documents, Help, and a toolbar with Open, Save, Undo, Redo, Cut, Copy, Paste, Find, and Replace.

16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.

17. Close all open windows and document all the acquired information.