

Module 05: Vulnerability Analysis LAB SCREENSHOTS

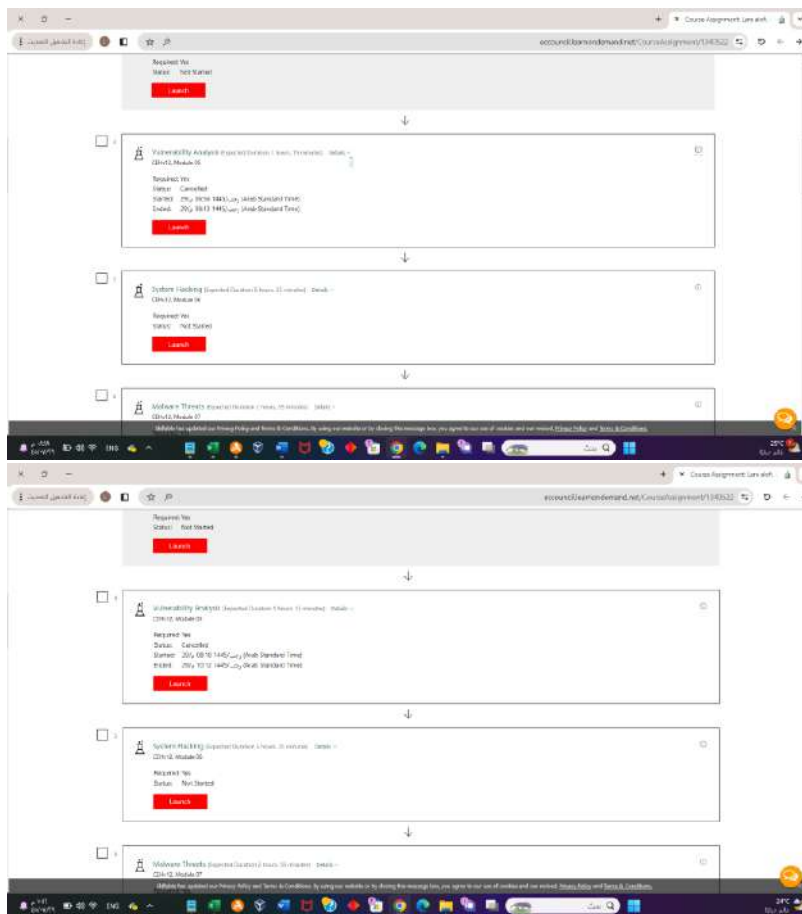
Lara Alofi

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-db5d184651eb?rc=10>
2. <https://labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20ecf15d185?rc=10>
3. <https://labclient.labondemand.com/LabClient/ad668ffb-e1a9-4f7d-9f44-d93fae32efcb?rc=10>

Username on EC-Council System

1. 2110886@uj.edu.sa



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

The image shows a Windows 11 login screen with the 'Admin' user profile selected. The taskbar at the bottom displays various application icons. To the right, a 'Vulnerability Analysis' sidebar is visible, containing instructions for the lab. Below the login screen, a web browser window displays the 'Common Weakness Enumeration (CWE)' website. The website features a search bar, navigation links, and a section titled 'CWE Top 10 KEY Weaknesses'. The sidebar on the right of the browser window provides step-by-step instructions for the lab, including launching a browser, navigating to the CWE website, and searching for vulnerabilities.

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/labClient/40366e64-ea63-4341-8db1-d05d184651eb?rc=10

Windows 11
Admin

Vulnerability Analysis
1 Hr 7 Min Remaining

Instructions Resources Help 100%

Weaknesses based on research concepts, development concepts, and architectural concepts.

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

☐ 1. By default, **Windows 11** machine is selected, click **Ctrl+Alt+Delete** to activate the machine.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under **Commands (thunder icon)** menu.

☐ 2. By default, **Admin** user profile is selected, type **Pe\$Sw0rd** to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pe\$Sw0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text** | **Type Password** button under **Commands (thunder icon)** menu.

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

1% Tasks Complete

< Previous Next: Lab 2: Perform... >

New Tab
CWE - Common Weakness Enumeration
https://cwe.mitre.org

CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home About CWE List Mapping Top-N Lists Community News Search

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

CWE Top 10 KEY Weaknesses **New!**

This list identifies the top ten CWEs in the Cybersecurity and Infrastructure Security Agency's (CISA) "Known Exploited Vulnerabilities (KEV) Catalog," a database of security flaws in software applications that have been exposed and leveraged by attackers. Our analysis/key insights about the list are available [here](#), and our methodology for creating the list is [here](#).

CWE List Quick Access
Search CWE
ENHANCED BY Google
View CWE

Community Engagement
Hardware CWE Special Interest Group [Join HW CWE SIG](#)
ICS/OT Special Interest Group [Join ICS/OT SIG](#)
REST API Working Group [Join REST API WG](#)
User Experience Working Group [Join UE WG](#)

CWE News
Podcast: [Red Hat's CWE Journey](#)
News: ["2023 CWE Top 10 KEV Weaknesses" List Now Available!](#)
News: [Cookie Notice and](#)

Vulnerability Analysis
1 Hr 3 Min Remaining

Instructions Resources Help 100%

☐ 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**

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

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.

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).

1% Tasks Complete

< Previous Next: Lab 2: Perform... >

Windows 11

labclientlabondemand.com/LabClient/40a6ee64-ea63-4341-8db1-d05d184651eb?rc=10

Vulnerability Analysis - Google Chrome

New Tab

CWE - Search the CWE Web Site X

https://cwe.mitre.org/find/index.html

CWE Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Top 25

Top HW CWE

New to CWE? [Start here!](#)

Home > Search the Site

Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

Search the CWE Web Site

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

smb

Page Last Updated: April 29, 2019

[Site Map](#) | [Terms of Use](#) | [Manage Cookies](#) | [Cookie Notice](#) | [Privacy Policy](#) | [Contact Us](#)

Use of the Common Weakness Enumeration (CWE) and the associated references from this website are subject to the [Terms of Use](#). CWE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation.

HSSEDI

MITRE

6:57 AM

25°C

الطقس في الرياض

Vulnerability Analysis

1 hr 1 min remaining

Instructions Resources Help

100%

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.

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 **1983 Linux Command**.

< Previous

Next: Lab 2: Perform...

Windows 11

labclientlabondemand.com/labClient/40a6ee64-ea63-4341-8db1-d05d184651eb?rc=10

Vulnerability Analysis - Google Chrome

New Tab x CWE - Search the CWE Web Site x CWE - CWE-284: Improper Access Control x

https://cwe.mitre.org/data/definitions/284.html

CWE Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE - Individual Dictionary Definition (4.13)

Home About CWE List Mapping Top-N Lists Community News Search

CWE-284: Improper Access Control

Weakness ID: 284
Abstraction: Pillar
Structure: Simple

View customized information: Conceptual Operational Mapping Friendly Complete Custom

Description

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Extended Description

Access control involves the use of several protection mechanisms such as:

- Authentication (proving the identity of an actor)
- Authorization (ensuring that a given actor can access a resource), and
- Accountability (tracking of activities that were performed)

When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

There are two distinct behaviors that can introduce access control weaknesses:

- Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.

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.

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**.

Previous Next: Lab 2: Perform...

Windows 11

labclientlabondemand.com/labClient/40a6ee64-ea63-4341-8db1-d05d184651eb?rc=10

Vulnerability Analysis - Google Chrome

New Tab x CWE - Search the CWE Web Site x CWE - CWE List Version 4.13 x

https://cwe.mitre.org/data/index.html

CWE Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List Version 4.13

Home About CWE List Mapping Top-N Lists Community News Search

CWE List Version 4.13

Total Weaknesses: 934

Latest Version Downloads Reports Visualizations Archive

Latest Version

At its core, the Common Weakness Enumeration (CWE™) is a list of software and hardware weaknesses types. Creating the list is a community initiative aimed at creating specific and succinct definitions for each common weakness type. By leveraging the widest possible group of interests and talents, the hope is to ensure that item in the list is adequately described and differentiated. This is a living effort with ongoing work to capture the specific effects, behaviors, exploit mechanisms, and implementation details within the CWE List as well as to review and revise the presentation approaches to provide those that best suit the community using this information.

Navigate CWE

Use one of the hierarchical representations below to navigate the entire list according to your specific point of view. The Software Development representation groups weaknesses around concepts that are frequently used or encountered in software development, while the Hardware Design representation groups weaknesses around concepts that are frequently used or encountered in hardware design. The Research Concepts representation facilitates research into weakness types and organizes items by behaviors using multiple levels of abstraction.

View by Software Development

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)**.

The result might differ when you perform this task.

Previous Next: Lab 2: Perform...

Windows 11

labclient.labondemand.com/labClient/406ee64-e663-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis - Google Chrome

New Tab x CWE - Search the CWE Web Site x CWE - CWE List Version 4.13 x +

https://cwe.mitre.org/data/index.html

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor.

- CWE Top 25 (2023)
- Most Important Hardware Weaknesses List (2021)
- OWASP Top Ten (2021)
- Seven Perilous Kingdoms
- Software Fault Pattern Clusters
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT Perl Coding Standard
- CISQ Quality Measures (2020)
- CISQ Data Protection Measures
- SEI ETF Security Vulnerabilities in JCS
- Architectural Concepts

BACK TO TOP

Helpful Views

A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight for a certain domain or use case.

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

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.

Previous Next Lab 2: Perform...

Windows 11

labclient.labondemand.com/labClient/406ee64-e663-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis - Google Chrome

New Tab x CWE - Search the CWE Web Site x CWE - CWE-1425 Weaknesses x +

https://cwe.mitre.org/data/definitions/1425.html

exploitable vulnerability, where a composite is a set of weaknesses that must all be present simultaneously in order to produce an exploitable vulnerability.

Show Details: ☐

Expand All | Collapse All

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

- Out-of-bounds Write - (787)
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - (79)
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - (89)
- Use After Free - (416)
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - (78)
- Improper Input Validation - (20)
- Out-of-bounds Read - (125)
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - (22)
- Cross-Site Request Forgery (CSRF) - (352)
- Unrestricted Upload of File with Dangerous Type - (434)
- Missing Authorization - (862)
- NULL Pointer Dereference - (476)
- Improper Authentication - (287)
- Integer Overflow or Wraparound - (190)
- Deserialization of Untrusted Data - (502)
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - (77)
- Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)
- Use of Hard-coded Credentials - (798)
- Server-Side Request Forgery (SSRF) - (928)
- Missing Authentication for Critical Function - (306)
- Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (362)
- Improper Privilege Management - (269)
- Improper Control of Generation of Code ('Code Injection') - (94)
- Incorrect Authorization - (863)
- Incorrect Default Permissions - (276)

BACK TO TOP

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

Previous Next Lab 2: Perform...

Task2:

The image displays two screenshots of a Windows 11 virtual machine environment, likely running on a cloud platform like AWS, as indicated by the URL in the address bar: `labclient.labondemand.com/LabClient/40abce64-e6b3-4341-8db1-d5d184651eb7/rc=10`.

Top Screenshot: The browser window shows the CVE website (<https://cve.mitre.org>). The page features the CVE logo, navigation links (CVE List, CNA, WG, Board, About), and a search bar. A prominent notice states: "NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](https://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." Below the notice, there are sections for CVE News, CVE Podcast, CVE Blog, Become a CNA, and Newest CVE Records Feed. The right sidebar shows a "Vulnerability Analysis" task with 31 minutes remaining, including instructions and a progress bar.

Bottom Screenshot: The browser window shows the CVE website's search page (https://cve.mitre.org/cve/search_cve_list.html). The page features the CVE logo, navigation links, and a search bar. A prominent notice states: "NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](https://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." Below the notice, there is a section for "Search CVE List" with instructions on how to search. A search bar contains the text "cve-2021-4034" and a "Submit" button. The right sidebar shows the "Vulnerability Analysis" task with 29 minutes remaining, including instructions and a progress bar.

Vulnerability Analysis - Google Chrome
labclientlabondemand.com/LabClient/4066ee54-e663-4341-8db1-dbd5d184651eb7rc=10

Windows 11

New Tab CVE - Search Results +

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cve-2021-4034

CVE List * CNA's * WG's * Board * About * NVD Go to First CVE Scores CVE IDs

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

TOTAL CVE Records: 223313

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 |
|-------------------------------|--|
| CVE-2021-4034 | A local privilege escalation vulnerability was found on polkit's plexec utility. The plexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of plexec 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 plexec 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)

Vulnerability Analysis
29 Minutes Remaining

Instructions Resources Help 100%

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.

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

Previous Next Lab 2: Perform...

Vulnerability Analysis - Google Chrome
labclientlabondemand.com/LabClient/4066ee54-e663-4341-8db1-dbd5d184651eb7rc=10

Windows 11

New Tab CVE - Search Results +

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cve-2021-44228

CVE List * CNA's * WG's * Board * About * NVD Go to First CVE Scores CVE IDs

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

TOTAL CVE Records: 223313

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 7 CVE Records that match your search.

| Name | Description |
|--------------------------------|--|
| CVE-2022-33915 | Versions of the Amazon AWS Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.3.5 are affected by a race condition that could lead to a local privilege escalation. This Hotpatch package is not a replacement for updating to a log4j version that mitigates CVE-2021-44228 or CVE-2021-45046; it provides a temporary mitigation to CVE-2021-44228 by hotpatching the local Java virtual machines. To do so, it iterates through all running Java processes, performs several checks, and executes the Java virtual machine with the same permissions and capabilities as the running process to load the hotpatch. A local user could cause the hotpatch script to execute a binary with elevated privileges by running a custom java process that performs exec() of an SUID binary after the hotpatch has observed the process path and before it has observed its effective user ID. |
| CVE-2022-23868 | In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability. |
| CVE-2021-45046 | It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow 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. |

Vulnerability Analysis
28 Minutes Remaining

Instructions Resources Help 100%

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.

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

15% Tasks Complete

Previous Next Lab 2: Perform...

Windows 11

labclient.labondemand.com/LabClient/4036ee54-e663-4341-8db1-db5d184651eb?rc=10

Vulnerability Analysis - Google Chrome

27 Minutes Remaining

Instructions Resources Help 100%

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**.

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

10. **Search Results** page appears, displaying a list of 153 Total CVEs.

Previous Next: Lab 2: Perform...

hpatch has observed the process path and before it has observed its effective user ID.

CVE-2022-23848 In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability.

CVE-2021-45046 It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, \${ctx:loginid}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

CVE-2021-44520 An injection vulnerability exists in a third-party library used in UniFi Network Version 6.5.53 and earlier (Log4j CVE-2021-44228) allows a malicious actor to control the application.

CVE-2021-44228 Apache Log4j 2.0-betas 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. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

CVE-2021-44125 It was found that the original fix for log4j CVE-2021-44228 and CVE-2021-45046 in the OpenShift metering hive containers was incomplete, as not all JndiLookup.class files were removed. This CVE only applies to the OpenShift Metering hive container images, shipped in OpenShift 4.8, 4.7 and 4.6.

CVE-2021-4104 JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. CVE-2021-44228 was reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

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)

Windows 11

labclient.labondemand.com/LabClient/4036ee54-e663-4341-8db1-db5d184651eb?rc=10

Vulnerability Analysis - Google Chrome

27 Minutes Remaining

Instructions Resources Help 100%

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

The result might differ when you perform this task.

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**.

153 Total CVEs

Previous Next: Lab 2: Perform...

HOME > CVE > SEARCH RESULTS

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

TOTAL CVE Records: 223313

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.

There are 544 CVE Records that match your search.

| Name | Description |
|--------------------------------|--|
| CVE-2024-22705 | An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strmidup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled. |
| CVE-2024-05565 | An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memory length, leading to a denial of service. |
| CVE-2023-5610 | An out-of-bounds read vulnerability was found in smb2_dump_detail in fs/smb/client/smb2ops.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information. |
| CVE-2023-6606 | An out-of-bounds read vulnerability was found in smbcalcsize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information. |
| CVE-2023-6381 | Improper input validation vulnerability in Newsletter Software SuperMailer affecting version 11.20.0.2204. An attacker could exploit this vulnerability by sending a malicious configuration file (file with SMB extension) to a user via a link or email attachment and persuade the user to open the file with the affected software on the local machine. |

Windows 11

tabClientLabondemand.com/TabClient/4036ee54-ea63-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis - Google Chrome

New Tab CVE - CVE-2022-22995

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

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 > CVE-2022-22995

Printer-Friendly View

CVE-ID

CVE-2022-22995 [Learn more at National Vulnerability Database \(NVD\)](#)

CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

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.

- FEDORA/FEDORA-2023-39f0ec3679
- URL <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/55F0UII2ASHZX5EM23QAIL7H167EZQK.W/>
- FEDORA/FEDORA-2023-ccc97f7b5d
- URL <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/7XQ34FWQJISV5PH2XY5ZYH8BAAYWPXG2/>
- FEDORA/FEDORA-2023-ef901c862c
- URL <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/75CZLFD0TUP3OYHGHSDUINENGSLPXKGO/>
- GENTOO/GLSA-202311-02
- URL <https://security.gentoo.org/glsa/202311-02>

Vulnerability Analysis

25 Minutes Remaining

Instructions Resources Help

100%

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.

13. Likewise, you can search for other target services

Previous Next Lab 2: Perform...

Task3:

Windows 11

labclient.labondemand.com/LabClient/40abce64-e063-4341-8db1-d05d104651eb?rc=10

Vulnerability Analysis - Google Chrome

New Tab x NVD - Home x +

https://nvd.nist.gov

An official website of the United States government Here's how you know

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

General +

Vulnerabilities +

Vulnerability Metrics +

Products +

Developers +

Contact NVD

Other Sites +

https://nvd.nist.gov/general/news/cisa-exploit-catalog

1110
0110
01000100

API

KNOWN EXPLOITED VULNERABILITIES

New 2.0 APIs **2022-23 Change** **New Parameters**

Timeline

Vulnerability Analysis
24 Minutes Remaining

Instructions Resources Help 100%

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.

The result might differ when you perform this task.

22% Tasks Complete

Previous Next: Lab 2: Perform...

Windows 11

labclient:labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-dbd5d184651eb?rc=10

https://nvd.nist.gov

2022-23 Change Timeline

Search +

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

For information on how to cite the NVD, including the database's Digital Object Identifier (DOI), please consult NIST's Public Data Repository.

CVE-2024-1109 - The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `init_download()` and `init()` functions in all versions up to, and including, 4.0.11. This makes it possible for ... read CVE-2024-1109

Published: February 07, 2024, 6:15:08 AM -0500

V3.1: **5.3 MEDIUM**

CVE-2024-1110 - The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `init()` function in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated ... read CVE-2024-1110

Published: February 07, 2024, 6:15:09 AM -0500

8:52 AM 2/9/2024

Vulnerability Analysis - Google Chrome

21 Minutes Remaining

Instructions Resources Help 100%

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.

The result might differ when you perform this task.

24% Tasks Complete

< Previous Next: Lab 2: Perform...

Windows 11

labclient:labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-dbd5d184651eb?rc=10

https://nvd.nist.gov/vuln/detail/CVE-2024-1109

CVE-2024-1109 Detail

Description

The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `init_download()` and `init()` functions in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated attackers to export the plugin's tracking data and podcast information.

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Wordfence **Base Score:** **5.3 MEDIUM**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/SU:C/L:N/N/A/N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information.

QUICK INFO

CVE Dictionary Entry: CVE-2024-1109

NVD Published Date: 02/07/2024

NVD Last Modified: 02/09/2024

Source: Wordfence

8:52 AM 2/9/2024

Vulnerability Analysis - Google Chrome

21 Minutes Remaining

Instructions Resources Help 100%

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.

24% Tasks Complete

< Previous Next: Lab 2: Perform...

Common Vulnerability Scoring System Calculator

CVE-2024-1109

Source: Wordfence

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

Base Scores

Temporal

Temporal Overall

Vulnerability Analysis

20 Minutes Remaining

Instructions Resources Help

100%

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.

CVCE-2022-0729 Detail

Current Description

Severity

References

Weakness Enumeration

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**.

24% Tasks Complete

Previous Next: Lab 2: Perform...

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

Vulnerability Analysis

19 Minutes Remaining

Instructions Resources Help

100%

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

The results might differ depending upon the selected vulnerability

Base Score Metrics

Exploitability Metrics

Impact Metrics

Temporal Score Metrics

24% Tasks Complete

Previous Next: Lab 2: Perform...

Windows 11

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2024-1109&vector=AV:N/AU...

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A) Local (MAV:L) Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) Low (MAC:L) High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) None (MPR:N) Low (MPR:L) High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) None (MUI:N) Required (MUI:R)

Scope (MS)

Windows 11 8:54 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/4066ee64-e663-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis

19 Minutes Remaining

Instructions Resources Help

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

The results might differ depending upon the selected vulnerability

Base Score Metrics

Temporal Score Metrics

Environmental Score Metrics

Previous Next: Lab 2: Perform...

Windows 11

https://nvd.nist.gov

An official website of the United States government Here's how you know

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

General +

Vulnerabilities -

Search & Statistics

Weakness Types

Legacy Data Feeds

Vendor Comments

CVMAP

KNOWN EXPLOITED VULNERABILITIES

New 2.0 APIs 2022-23 Change New Parameters

Timeline

Windows 11 8:55 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/4066ee64-e663-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis

18 Minutes Remaining

Instructions Resources Help

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**.

You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs

24% Tasks Complete

Previous Next: Lab 2: Perform...

Windows 11

Search vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type: Basic (selected), Advanced

Results Type: Overview (selected), Statistics

Keyword Search: smb

Exact Match: ☐

Search Type: All Time (selected), Last 3 Months

Contains HyperLinks: CISA Known Exploited Vulnerabilities, US-CERT Technical Alerts, US-CERT Vulnerability Notes, OVAL Queries

Search Reset

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Windows taskbar: 8:56 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis 17 Minutes Remaining

Instructions Resources Help

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.

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

Search Vulnerability Database

24% Tasks Complete

Previous Next: Lab 2: Perform...

Windows 11

Search vulnerability Database

There are 457 matching records. Displaying matches 1 through 20.

Vuln ID Summary CVSS Severity

CVE-2024-22705 An issue was discovered in smb2 in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb2_mdup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled. V3.1: 7.5 HIGH V2.0: (not available) Published: January 23, 2024, 6:15:09 AM -0500

CVE-2024-0565 An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcopy length, leading to a denial of service. V3.1: 7.5 HIGH V2.0: (not available) Published: January 15, 2024, 3:15:43 PM -0500

CVE-2023-51071 An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily disable the SMB service on a victim's Qstar instance by executing a specific command in a link. V3.1: 6.5 MEDIUM V2.0: (not available) Published: January 12, 2024, 11:15:08 PM -0500

CVE-2023-51070 An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily adjust sensitive SMB settings on the QStar Server. V3.1: 7.5 HIGH V2.0: (not available)

Windows taskbar: 8:56 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/40a6ee64-ea63-4341-8db1-d5d184651eb7rc=10

Vulnerability Analysis 17 Minutes Remaining

Instructions Resources Help

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.

12. Likewise, you can search for other target services for the underlying vulnerability in the Search Vulnerability Database section.

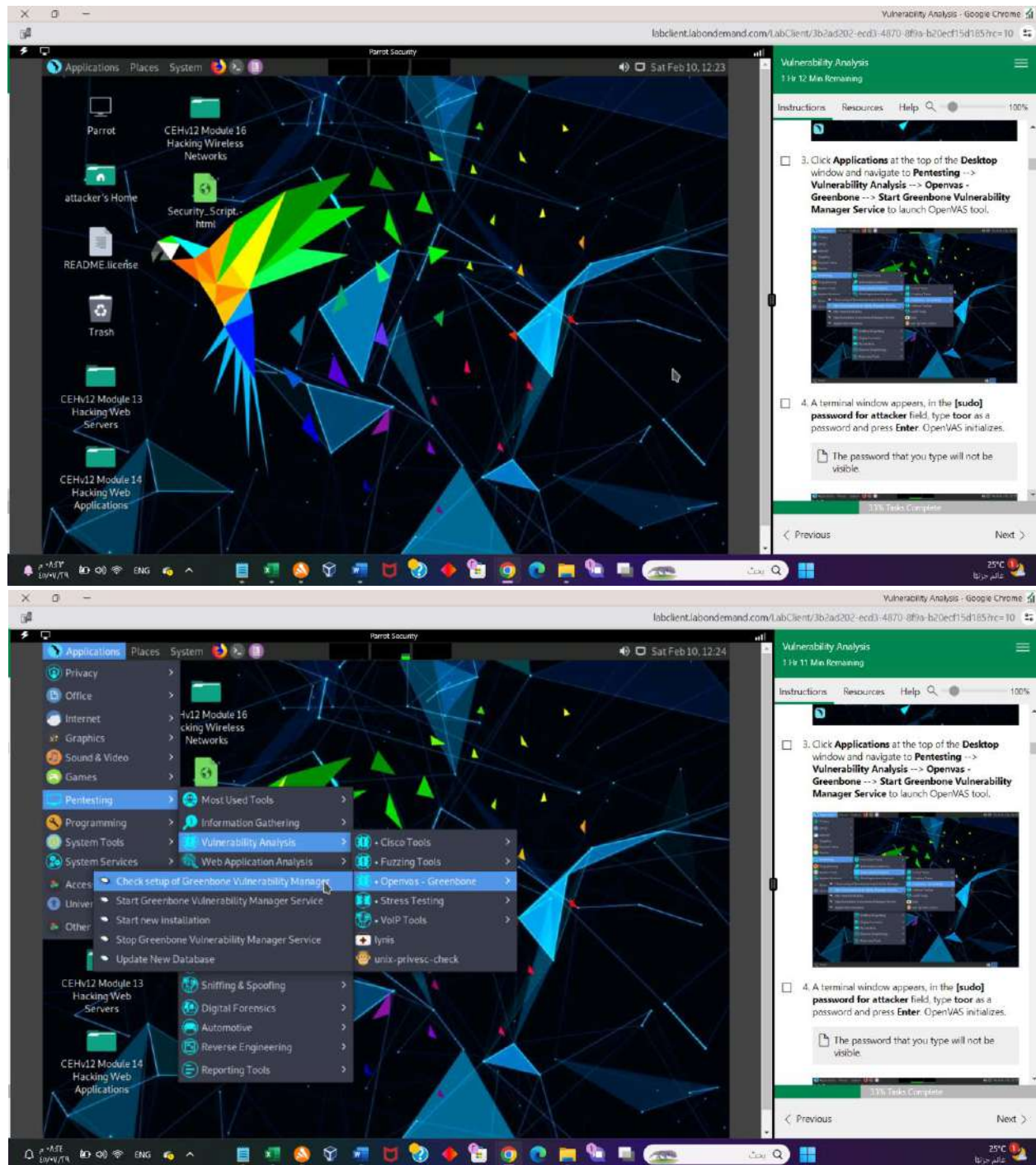
13. This concludes the demonstration of checking.

24% Tasks Complete

Previous Next: Lab 2: Perform...

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Task1:



Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Applications Places System Sat Feb 10, 12:24

Parrot Terminal

```
[sudo] password for attacker:
gvm-check-setup 21.4.1
Test completeness and readiness of GVM-21.4.1
attacker's Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 21.4.1.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
ERROR: redis-server is not running or not listening on socket: /var/run/redis-openvas/redis-server.sock
FIX: You should start the redis-server with 'systemctl start redis-server@openvas.service' or configure it to listen on socket: /var/run/redis-openvas/redis-server.sock.
ERROR: Your GVM-21.4.1 installation is not yet complete!
Please follow the instructions marked with FIX above and run this script again.
[root@parrot]-[/home/attacker]
```

Parrot Security

Vulnerability Analysis
11:11 Min Remaining

Instructions Resources Help 100%

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

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.

33% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Applications Places System Sat Feb 10, 12:37

Parrot Terminal

Greenbone Security Assistant - Mozilla Firefox

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Sign in to your account

Username
admin

Password
password

Sign In

Greenbone Security Assistant

Vulnerability Analysis
59 Minutes Remaining

Instructions Resources Help 100%

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.

33% Tasks Complete

Previous Next

Applications Places System Parrot Security

Greenbone Security Assistant - Dashboards - Mozilla Firefox

Parrot Security

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Dashboards

Overview

Tasks by Severity Class (Total: 0)

Tasks by Status (Total: 0)

CVEs by Creation Time

NVTs by Severity Class (Total: 86680)

1,940 180,200 Created CVEs

Log

Greenbone Security Assistant (GSA) Copyright © 2009-2021 by Greenbone Networks

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis

50 Minutes Remaining

Instructions Resources Help

100%

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

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

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

13% Tasks Complete

Previous Next

Applications Places System Parrot Security

Greenbone Security Assistant - Dashboards - Mozilla Firefox

Parrot Security

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Tasks Reports Results Vulnerabilities Notes Overrides

Dashboards

Overview

Tasks by Severity Class (Total: 0)

Tasks by Status (Total: 0)

CVEs by Creation Time

NVTs by Severity Class (Total: 86680)

1,940 180,200 Created CVEs

Log

Greenbone Security Assistant (GSA) Copyright © 2009-2021 by Greenbone Networks

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis

57 Minutes Remaining

Instructions Resources Help

100%

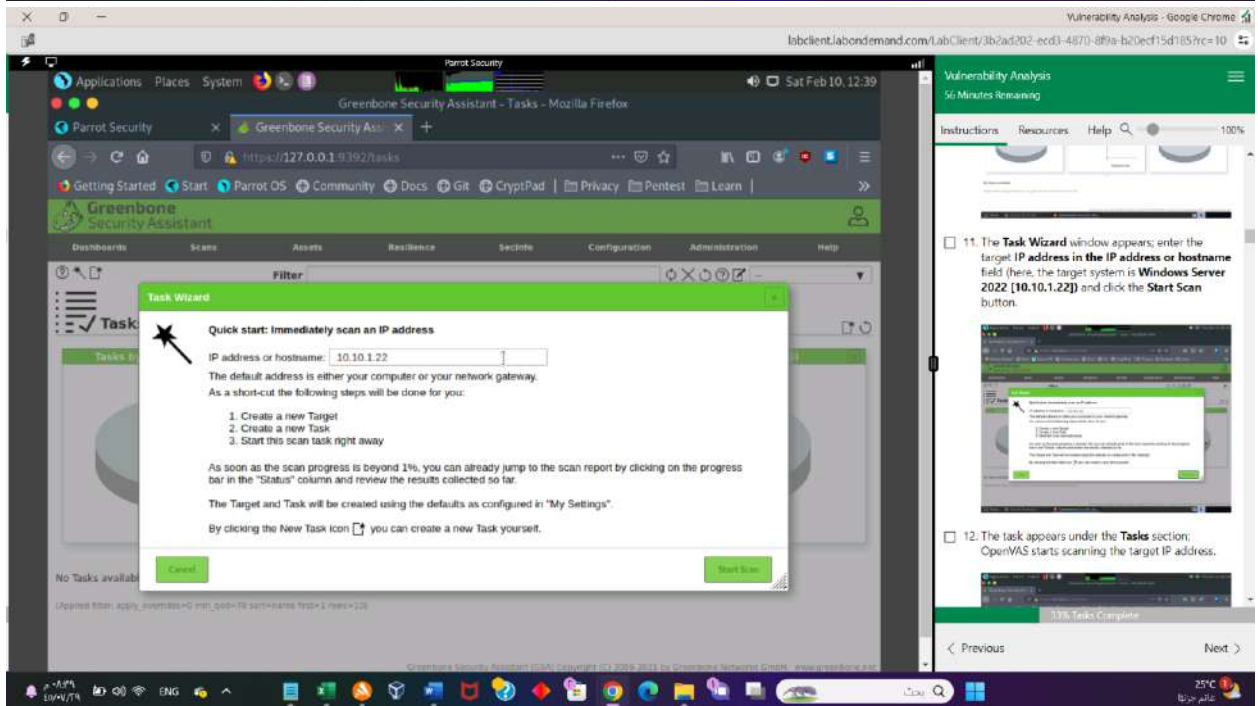
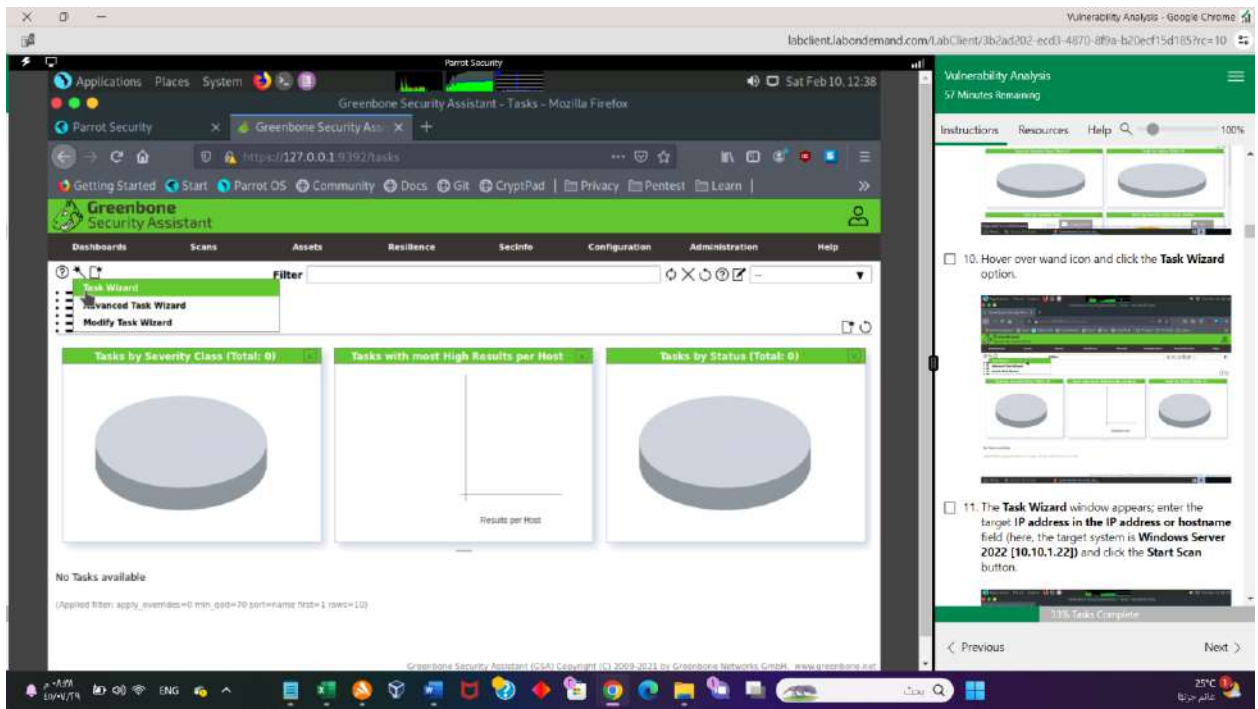
9. Navigate to **Scans** --> **Tasks** from the **Menu** bar.

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

13% Tasks Complete

Previous Next

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



Greenbone Security Assistant - Tasks - Mozilla Firefox

https://127.0.0.1:9392/tasks

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Filter

Tasks 1 of 1

Tasks by Severity Class (Total: 1)

Tasks with most High Results per Host

Tasks by Status (Total: 1)

Name Status Reports Last Report Severity Trend Actions

Immediate scan of IP 10.10.1.22 Done 1 Sat, Feb 10, 2024 5:39 PM UTC 10.0 (High)

Apply to page contents

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone Networks GmbH. www.greenbone.net

Vulnerability Analysis 37 Minutes Remaining

Instructions Resources Help 100%

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.

It takes approximately 20 minutes for the scan to complete.

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.

43% Tasks Complete

Previous Next

Greenbone Security Assistant - Report Details - Mozilla Firefox

https://127.0.0.1:9392/report/508ba7f1-8489-449b-b67-6d9

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Filter

RepoSat, Feb 10, 2024 5:39 PM UTC

Done

508ba7f1-8489-449b-b67-6d9

Created: Sat, Feb 10, 2024 5:39 PM UTC Modified: Sat, Feb 10, 2024 5:58 PM UTC Owner: admin

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

1 - 4 of 4

| 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 | Sat, Feb 10, 2024 5:40 PM UTC |
| DCE/RPC and MSRPC Services Enumeration Reporting | 9.0 (High) | 80 % | 10.10.1.22 | | 135/tcp | Sat, Feb 10, 2024 5:48 PM UTC |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 6.0 (Medium) | 98 % | 10.10.1.22 | | 5389/tcp | Sat, Feb 10, 2024 5:48 PM UTC |
| TCP timestamps | 2.0 (Low) | 80 % | 10.10.1.22 | | general/tcp | Sat, Feb 10, 2024 5:40 PM UTC |

Applied filter: apply_severities=0 levels=html rows=100 max_qod=70 first=1 sort=reverse=severity

1 - 4 of 4

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone Networks GmbH. www.greenbone.net

Vulnerability Analysis 37 Minutes Remaining

Instructions Resources Help 100%

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

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.

43% Tasks Complete

Previous Next

Parrot Security

Greenbone Security Assistant - Report Details - Mozilla Firefox

Getting Started Start Parrot OS Community Docs GR CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Environment (local)

Summary

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

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

used for this scan.

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

- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Detection Result

Version of installed component: 21.4.1 (Installed component: openvas-libraries on OpenVAS <= 9, openvas-scanner on GVM >= 10)
Latest available openvas-scanner version: 21.4.3
Reference URL(s) for the latest available version: <https://community.greenbone.net/t/gvm-21-04-stable-initial-release-2021-04-16/8942>

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

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Vulnerability Analysis

35 Minutes Remaining

Instructions Resources Help 100%

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.

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

43% Task Complete

Previous Next

Windows Server 2022

Control Panel > System and Security > Windows Defender Firewall > Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps.
 - ☐ Notify me when Windows Defender Firewall blocks a new app.
- ☐ Turn off Windows Defender Firewall (not recommended)

Private network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps.
 - ☐ Notify me when Windows Defender Firewall blocks a new app.
- ☐ Turn off Windows Defender Firewall (not recommended)

Public network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps.
 - ☐ Notify me when Windows Defender Firewall blocks a new app.
- ☐ Turn off Windows Defender Firewall (not recommended)

OK Cancel

Type here to search

10:01 AM 2/10/2024

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Vulnerability Analysis

34 Minutes Remaining

Instructions Resources Help 100%

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

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 **Parrot Security** to switch to **Parrot Security** machine and perform **Steps# 9-11** to

49% Task Complete

Previous Next

Vulnerability Analysis - Google Chrome
lbclient.labdemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Parrot Security

Greenbone Security Assistant - Tasks - Mozilla Firefox

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Filter

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 | Sat, Feb 10, 2024 5:39 PM UTC | 10.0 (High) | | |
| Immediate scan of IP 10.10.1.22 | 0 % | 1 | | | | |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. All rights reserved.

Vulnerability Analysis
32 Minutes Remaining

Instructions Resources Help 100%

22. click on 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.

It takes approximately 15-20 minutes for 50% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
lbclient.labdemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185?rc=10

Parrot Security

Greenbone Security Assistant - Tasks - Mozilla Firefox

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Filter

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 | Sat, Feb 10, 2024 5:39 PM UTC | 10.0 (High) | | |
| Immediate scan of IP 10.10.1.22 | Done | 1 | Sat, Feb 10, 2024 6:03 PM UTC | 10.0 (High) | | |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. All rights reserved.

Vulnerability Analysis
16 Minutes Remaining

Instructions Resources Help 100%

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

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

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

The results might differ when you perform this task.

50% Tasks Complete

Previous Next

Parrot Security

Greenbone Security Assistant - Report Details - Mozilla Firefox

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

RepoSat, Feb 10, 2024 6:03 PM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

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 | Sat, Feb 10, 2024 6:04 PM UTC |
| DCE/RPC and MSRPC Services Enumeration Reporting | 5.0 (Medium) | 80 % | 10.10.1.22 | | 135/tcp | Sat, Feb 10, 2024 6:12 PM UTC |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 5.0 (Medium) | 98 % | 10.10.1.22 | | 3389/tcp | Sat, Feb 10, 2024 6:11 PM UTC |
| TCP timestamps | 2.5 (Low) | 80 % | 10.10.1.22 | | general/tcp | Sat, Feb 10, 2024 6:04 PM UTC |

Applied filter: apply_avertides=0 levels=html max=100 min_qod=70 first=1 sort=reverse=severity

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

Vulnerability Analysis 15 Minutes Remaining

Instructions Resources Help 100%

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

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.

50% Tasks Complete

Previous Next

Windows Server 2022

Customize Settings

Control Panel > System and Security > Windows Defender Firewall > Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps
 - ☐ Notify me when Windows Defender Firewall blocks a new app
- ☒ Turn off Windows Defender Firewall (not recommended)

Private network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps
 - ☐ Notify me when Windows Defender Firewall blocks a new app
- ☒ Turn off Windows Defender Firewall (not recommended)

Public network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps
 - ☐ Notify me when Windows Defender Firewall blocks a new app
- ☒ Turn off Windows Defender Firewall (not recommended)

OK Cancel

Vulnerability Analysis 14 Minutes Remaining

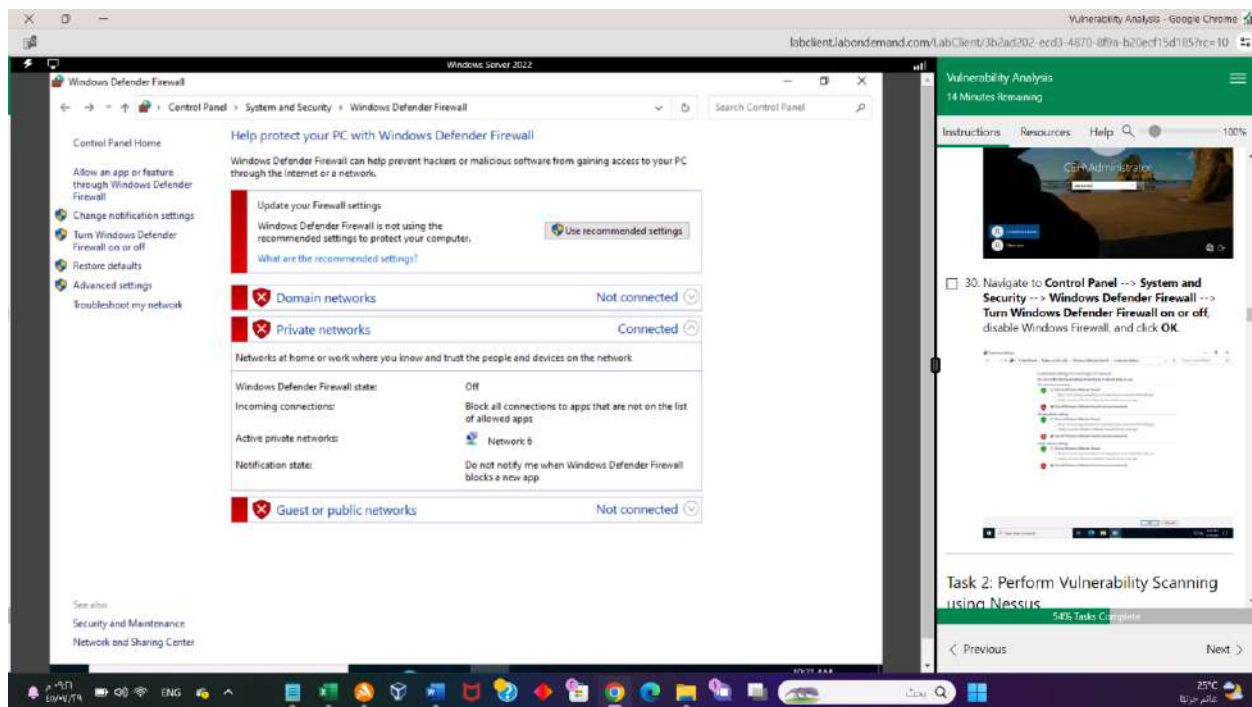
Instructions Resources Help 100%

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

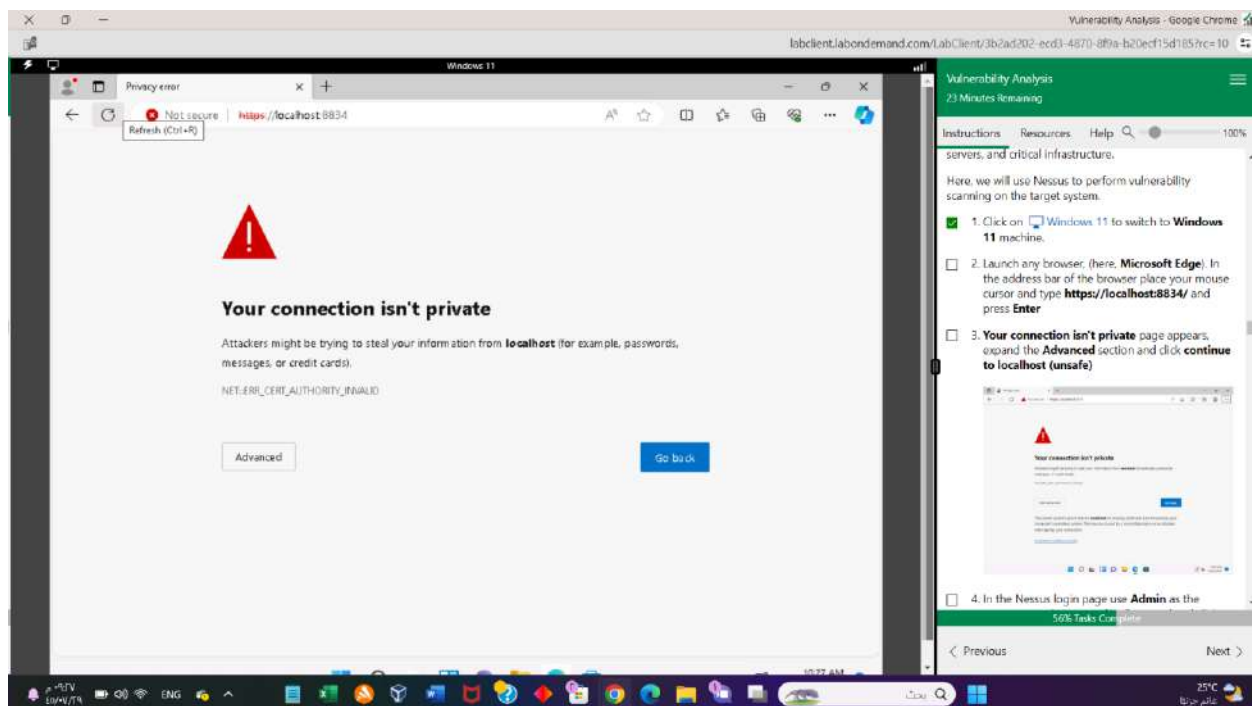
Task 2: Perform Vulnerability Scanning using Nessus

54% Tasks Complete

Previous Next



Task2:



Vulnerability Analysis - Google Chrome
lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Windows 11
Not secure | <https://localhost:8834/#/>

nessus Essentials

admin
password

Remember Me Sign in

© 2024 Tenable, Inc.

Java Update Checker
Java Update Available
A new version of Java is ready to be installed.
Click here to continue.

10:30 AM 2/10/2024

Vulnerability Analysis
20 Minutes Remaining

Instructions Resources Help 100%

4. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In**

5. 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.

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

57% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Windows 11
Not secure | <https://localhost:8834/#/scans/folders/my-scans>

nessus Essentials

Scans Settings

My Scans

My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
TerraScan

Tenable News
CVE-2024-21762: Critical Fortinet FortiOS Out-of-B...

Read More

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

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets
Example: 192.168.0.1-192.168.0.255, 192.168.0.0/24, IPv6.com

Close Submit

10:30 AM 2/10/2024

Vulnerability Analysis
20 Minutes Remaining

Instructions Resources Help 100%

5. 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.

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

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

59% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/folders/my-scans>

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

nessus Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Cybersecurity Snapshot: Critical Infrastructure Or...

Read More

My Scans

Import

This folder is empty. [Create a new scan](#)

10:31 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis 19 Minutes Remaining

Instructions Resources Help

100%

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

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

59% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies>

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

nessus Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Keep the Water Flowing for the DoD: Securing Opera...

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](#)

10:33 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis 18 Minutes Remaining

Instructions Resources Help

100%

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

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

60% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/new>

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

nessus Scans Settings

Policy Templates

Scanner

DISCOVERY

Host Discovery

VULNERABILITIES

Basic Network Scan

Advanced Scan

Advanced Dynamic Scan

Malware Scan

Tenable News

Keep the Water Flowing for the DoD: Securing Operations...

Read More

10:32 AM 2/10/2024

Vulnerability Analysis 18 Minutes Remaining

Instructions Resources Help 100%

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

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

61% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/new/ad529e16-03b6-8c1d-af...>

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

nessus Scans Settings

New Policy / Advanced Scan

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Save Cancel

Tenable News

Frequently Asked Questions on Security Incident at...

Read More

10:32 AM 2/10/2024

Vulnerability Analysis 18 Minutes Remaining

Instructions Resources Help 100%

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**).

61% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/new/ad529e16-03b6-8c1d-adf...>

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

nessus

Scans Settings

My Scans
All Scans
Trash

Policies
Plugin Rules
TerraScan

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

Tenable News

SQL Injection in HTML5 Video Player WordPress Plug...

Read More

10:35 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis

17 Minutes Remaining

Instructions Resources Help

100%

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.

61% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/4f3config/settings/discovery/ha...>

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

nessus

Scans Settings

My Scans
All Scans
Trash

Policies
Plugin Rules
TerraScan

NetworkScan_Policy / Configuration

[Back to Policies](#)

Settings Credentials Plugins

BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Host Discovery
Port Scanning
Service Discovery

Remote Host Ping

Ping the remote host ☐

Fragile Devices

☐ Scan Network Printers

☐ Scan Novell Netware hosts

☐ Scan Operational Technology devices

Wake-on-LAN

List of MAC addresses [Add File](#)

10:35 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis

16 Minutes Remaining

Instructions Resources Help

100%

11. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.

63% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/4/config/settings/discovery/networkscanpolicy>

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

nessus Scans Settings

NetworkScan_Policy / Configuration

Settings Credentials Plugins

BASE

DISCOVERY

Host Discovery

Port Scanning

Service Discovery

ASSESSMENT

REPORT

ADVANCED

Ports

☐ Consider unscanned ports as closed

Port scan range: default

Local Port Enumerators

☒ SSH (netstat)

☒ WMI (netstat)

☒ SNMP

☒ Only run network port scanners if local port enumeration failed

☒ Verify open TCP ports found by local port enumerators

Tenable News

Avant! Avalanche Multiple Vulnerabilities

Read More

10:35 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rce=10

Vulnerability Analysis

15 Minutes Remaining

Instructions Resources Help

100%

12. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.

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**.

64% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/4/config/settings/advanced>

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

nessus Scans Settings

Performance Options

☐ Slow down the scan when network congestion is detected

Network timeout (in seconds): 5

Max simultaneous checks per host: 5

Max simultaneous hosts per scan: 5

Max number of concurrent TCP sessions per host: Unlimited

Max number of concurrent TCP sessions per scan: Unlimited

Unix find command Options

Exclude Filepath [Add File](#)

Exclude Filesystem [Add File](#)

Tenable News

Cybersecurity Snapshot: Critical Infrastructure Or...

Read More

10:36 AM 2/10/2024

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rce=10

Vulnerability Analysis

14 Minutes Remaining

Instructions Resources Help

100%

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**.

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

64% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies/4/config/credentials>

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

nessus Scans Settings

My Scans All Scans Trash

Policies Plugin Rules Terrascan

Tenable News

Frequently Asked Questions on Security Incident at...

Read More

CATEGORIES Host

Filter Credentials

SNMPv3 SSH Windows

Windows

Authentication method Password

Username CEH123

Password

Domain

Global Credential Settings

☒ Never send credentials in the clear

☒ Do not use NTLMv1 authentication

☐ Start the Remote Registry service during the scan

☐ Enable administrative shares during the scan

☐ Start the Server service during the scan

10:37 AM 2/10/2024

Vulnerability Analysis 13 Minutes Remaining

Instructions Resources Help 100%

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

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

64% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/policies>

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

nessus Scans Settings

My Scans All Scans Trash

Policies Plugin Rules Terrascan

Tenable News

SQL Injection in HTML5 Video Player - WordPress Plug...

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.

Search Policies 1 Policy

| Name | Template | Last Modified |
|--------------------|---------------|-------------------|
| NetworkScan_Policy | Advanced Scan | Today at 10:38 AM |

10:38 AM 2/10/2024

Vulnerability Analysis 12 Minutes Remaining

Instructions Resources Help 100%

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

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

67% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/folders/my-scans>

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

nessus

Scans Settings

My Scans

Import

This folder is empty. [Create a new scan](#)

My Scans

All Scans

Trash

Policies

Plugin Rules

Terrascan

Tenable News

Pimcore Multiple Vulnerabilities

[Read More](#)

10:35 AM 2/10/2024

25°C

69% Tasks Complete

Previous Next

Vulnerability Analysis

12 Minutes Remaining

Instructions Resources Help

100%

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

69% Tasks Complete

Previous Next

Windows 11

Not secure | <https://localhost:8834/#/scans/reports/new>

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

nessus

Scans Settings

Scan Templates

[Back to Scans](#)

Scanner User Defined

NetworkScan_Policy

Scanning a network

My Scans

All Scans

Trash

Policies

Plugin Rules

Terrascan

Tenable News

Pimcore Multiple Vulnerabilities

[Read More](#)

10:35 AM 2/10/2024

25°C

69% Tasks Complete

Previous Next

Vulnerability Analysis

11 Minutes Remaining

Instructions Resources Help

100%

19. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan_Policy**.

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.

69% Tasks Complete

Previous Next

Windows 11

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis - Google Chrome

Not secure | https://localhost:8834/#/scans/reports/new/db4bac2-05f6-425c-9d... There's an error with your feed. Click here to view your license information.

nessus Scans Settings

My Scans All Scans Trash

Resources Policies Plugin Rules Terrascan

Tenable News CVE-2024-21762: Critical Fortinet FortiOS Out-of-B...

New Scan / NetworkScan_Policy

Back to Scan Templates

Settings

BASE

General

Name: Local Network

Description: Scanning a local Network.

Folder: My Scans

Targets: 10.10.1.22

Upload Targets Add File

10:40 AM 2/10/2024

25°C

Vulnerability Analysis 25 Minutes Remaining

Instructions Resources Help 100%

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)**.

21. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the **down** icon.

69% Tasks Complete

Previous Next

Windows 11

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Vulnerability Analysis - Google Chrome

Not secure | https://localhost:8834/#/scans/folders There's an error with your feed. Click here to view your license information.

nessus Scans Settings

My Scans All Scans Trash

Resources Policies Plugin Rules Terrascan

Tenable News D-Link D-View 8 Unauthenticated Probe-Core Server ...

Import New Folder New Scan

| Schedule | Last Modified |
|-----------|-------------------|
| On Demand | Today at 10:49 AM |

10:49 AM

24°C

Vulnerability Analysis 16 Minutes Remaining

Instructions Resources Help 100%

next to the **Save** button and select **Launch** to start the scan.

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

71% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / My Scans

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

Notifications

- Scan saved successfully. 4 minutes ago (repeated 1 time)
- Scan moved to trash successfully. 5 minutes ago
- Policy saved successfully. 15 minutes ago (repeated 1 time)
- Error: Enter an ip range to scan for hosts. 22 minutes ago
- Error: Your plugin feed hasn't been updated in 640 days. 23 minutes ago

View Notification History Clear Notifications

Local Network

Hosts: 1 Vulnerabilities: 25 History: 1

Filter: Search Hosts 1 Host

| Host | Vulnerabilities | % |
|------------|-----------------|-----|
| 10.10.1.22 | 1108 | 99% |

Scan Details

Policy: Status: Severity Base: Scanner: Start:

Vulnerability

Tenable News

Appwrite Blind SSRF

Read More

Vulnerability Analysis 12 Minutes Remaining

Instructions Resources Help 100%

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

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

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.

72% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

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

Local Network

Back to My Scans

Hosts: 1 Vulnerabilities: 25 History: 1

Filter: Search Hosts 1 Host

| Host | Vulnerabilities | % |
|------------|-----------------|-----|
| 10.10.1.22 | 1108 | 99% |

Scan Details

Policy: Status: Severity Base: Scanner: Start:

Vulnerability

Tenable News

Pimcore Multiple Vulnerabilities

Read More

Vulnerability Analysis 12 Minutes Remaining

Instructions Resources Help 100%

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

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.

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

72% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

Not secure | https://localhost:8834/#/scans/reports/8/vulnerabilities

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

Scans Settings

Local Network

Back to My Scans

HOSTS 1 Vulnerabilities 35 History 1

Filter Search Vulnerabilities 35 Vulnerabilities

| Sev | Score | Name | Family | Count |
|------|-------|-------------------------|-------------------|-------|
| MOD | ... | SSL (Multiple Issues) | General | 9 |
| MOD | ... | SNMP (Multiple Issues) | SNMP | 7 |
| MOD | ... | Microsoft Windows (M... | Windows | 2 |
| MOD | ... | TLS (Multiple Issues) | Service detection | 4 |
| MOD | ... | Microsoft Windows (M... | Misc | 2 |
| INFO | ... | HTTP (Multiple Issues) | Web Servers | 7 |
| INFO | ... | SMB (Multiple Issues) | Windows | 7 |
| INFO | ... | TLS (Multiple Issues) | General | 2 |

Scan Details

Policy: Status: Severity Base: Scanner: Start:

Vulnerability

Tenable News

D-Link D-View 8 Unauthenticated Probe-Core Server ...

Read More

Windows 11

11:04 AM

24°C

عالم جربا

Vulnerability Analysis

8 Minutes Remaining

Instructions Resources Help 100%

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

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)**.

73% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

Not secure | https://localhost:8834/#/scans/reports/8/vulnerabilities/group/...

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

Scans Settings

Local Network / SSL (Multiple Issues)

Back to Vulnerabilities

HOSTS 1 Vulnerabilities 35 History 1

Search Vulnerabilities 9 Vulnerabilities

| Sev | Score | Name | Family | Count |
|--------|-------|---------------------------------|---------|-------|
| HIGH | 7.5 | SSL Medium Strength Ciphers | General | 1 |
| MEDIUM | 6.5 | SSL Certificate Cannot Be Tr... | General | 1 |
| MEDIUM | 6.4 * | SSL Self-Signed Certificate | General | 1 |
| MEDIUM | 5.3 | SSL Certificate with Wrong ... | General | 1 |
| INFO | ... | SSL Certificate 'commonNa... | General | 1 |
| INFO | ... | SSL Certificate information | General | 1 |
| INFO | ... | SSL Cipher Block Chaining O... | General | 1 |
| INFO | ... | SSL Cipher Suites Supported | General | 1 |

Scan Details

Policy: Status: Severity Base: Scanner: Start:

Vulnerability

Tenable News

Avast! Avast! Multiple Vulnerabilities

Read More

Windows 11

11:05 AM

24°C

عالم جربا

Vulnerability Analysis

8 Minutes Remaining

Instructions Resources Help 100%

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.

73% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

Scans Settings

Local Network / Plugin #42873

Back to Vulnerability Group

HOSTS 1 Vulnerabilities 38 History 1

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Plugin Detail

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

<https://www.schneier.com/blog/archives/2016/08/24/sweet32.html>
<https://sweet32.info>

Output

Severity: High
ID: 42873
Version: 1.0
Type: SSL
Family: SSL
Published: 2016-08-24
Modified: 2016-08-24

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/Au:N/C:N/I:N/CR:L/RR:R/EA:N/SC:N/UC:N/

Tenable News

Avanti Avalanche Multiple Vulnerabilities

Read More

Vulnerability Analysis

7 Minutes Remaining

Instructions Resources Help

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**).

73% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / My Scans

Scans Settings

My Scans

Import

Search scans

1 scan

| Name | Schedule | Last Mod |
|---------------|-----------|-------------------|
| Local Network | On Demand | Today at 11:07 AM |

Tenable News

Shoring Up Water Security: Industry Leaders Testif...

Read More

Vulnerability Analysis

5 Minutes Remaining

Instructions Resources Help

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.

78% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

Not secure | https://localhost:8834/#/scans/reports/B/hosts

Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

- Complete List of Vulnerabilities By Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Generate Report Cancel Save as default

Vulnerability Analysis

3 Minutes Remaining

Instructions Resources Help 100%

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**.

78% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

labclient.labondemand.com/LabClient/3b2ad202-ec03-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View

Not secure | https://localhost:8834/#/scans/reports/B/hosts

Downloads: Local_Network_schive.pdf Open file

Configure Audit Trail Launch Report Export

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

Notes 1 VPR Top Threats History 1

1 Host

Vulnerabilities 37

Scan Details

Policy: NetworkScan_Policy
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:49 AM
End: Today at 11:09 AM
Elapsed: 17 minutes

Vulnerabilities

Critical High Medium Low Info

Tenable News

Appwrite Blind SSRF

Read More

Vulnerability Analysis

3 Minutes Remaining

Instructions Resources Help 100%

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.

Screenshots and browser might differ when you perform this task.

79% Tasks Complete


Previous Next

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View Local_Network_ecnhae.pdf

File | C:\Users\Admin\Downloads\Local_Network_ecnhae.pdf



Local Network

Report generated by Nessus™

Sat, 10 Feb 2024 11:07:22 Pacific Standard Time

11:10 AM

Vulnerability Analysis

3 Minutes Remaining

Instructions Resources Help 100%

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.

Screenshots and browser might differ when you perform this task.

79% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome

lobclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rc=10

Nessus Essentials / Folders / View Local_Network_ecnhae.pdf

File | C:\Users\Admin\Downloads\Local_Network_ecnhae.pdf

4 of 6

10.10.1.22

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|----------|-----------|--------|------|
| CRITICAL | 0 | | |
| HIGH | 3 | | |
| MEDIUM | 6 | | |
| LOW | 0 | | |
| INFO | 56 | | |

Vulnerabilities Total: 65

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|----------|-----------|--------|---|
| HIGH | 7.5 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.3 | 26020 | Microsoft Windows SMB NULL Session Authentication |
| HIGH | 7.5* | 41028 | SNMP Agent Default Community Name (public) |
| MEDIUM | 6.5 | 51190 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 6.5 | 157288 | TLS Version 1.1 Protocol Deprecated |
| MEDIUM | 5.3 | 45411 | SSL Certificate with Wrong Hostname |
| MEDIUM | 4.0 | 58453 | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| MEDIUM | 6.4* | 57582 | SSL Self-Signed Certificate |

11:10 AM

Vulnerability Analysis

2 Minutes Remaining

Instructions Resources Help 100%

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

The results might differ when you perform this task.

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

79% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rce=10

Nessus Essentials / Folders / View X SSL Medium Strength Cipher Suites Supported (SWEET32) X

https://www.tenable.com/plugins/nessus/42873

tenable Plugins Settings

DETECTIONS

Plugins Overview Plugins Pipeline Release Notes Newest Updated Search Nessus Families WAS Families NNM Families LCE Families Tenable OT Security Families About Plugin Families Audits

Plugins / Nessus / 42873

SSL Medium Strength Cipher Suites Supported (SWEET32)

HIGH Nessus Plugin ID 42873

Language: English

Information Dependencies Dependents Changelog

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 84 bits and less than 112 bits, or else that uses the 3DES

Plugin Details

Severity: High

ID: 42873

File Name: ssl_medium_supported_ciphers.nasl

Version: 1.21

Vulnerability Analysis

Instructions Resources Help 100%

1 Minute Remaining

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.

79% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/3b2ad202-ecd3-4870-8f9a-b20edf15d185/rce=10

Nessus Essentials / Folders / View X SSL Medium Strength Cipher Suites Supported (SWEET32) X

https://localhost:8834/#/scans/reports/hosts

nessus Scans Settings

Configure Audit Trail

Admin My Account Sign Out

Notes 1 VPR Top Threats History 1

1 Host

Vulnerabilities 87

Scan Details

Policy: NetworkScan_Policy

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 10:49 AM

End: Today at 11:09 AM

Elapsed: 17 minutes

Vulnerabilities

Critical High Medium Low Info

Tenable News

D-Link D-View 8 Unauthenticated Probe-Core Server ...

Read More

https://localhost:8834/#/settings/my-account

Vulnerability Analysis

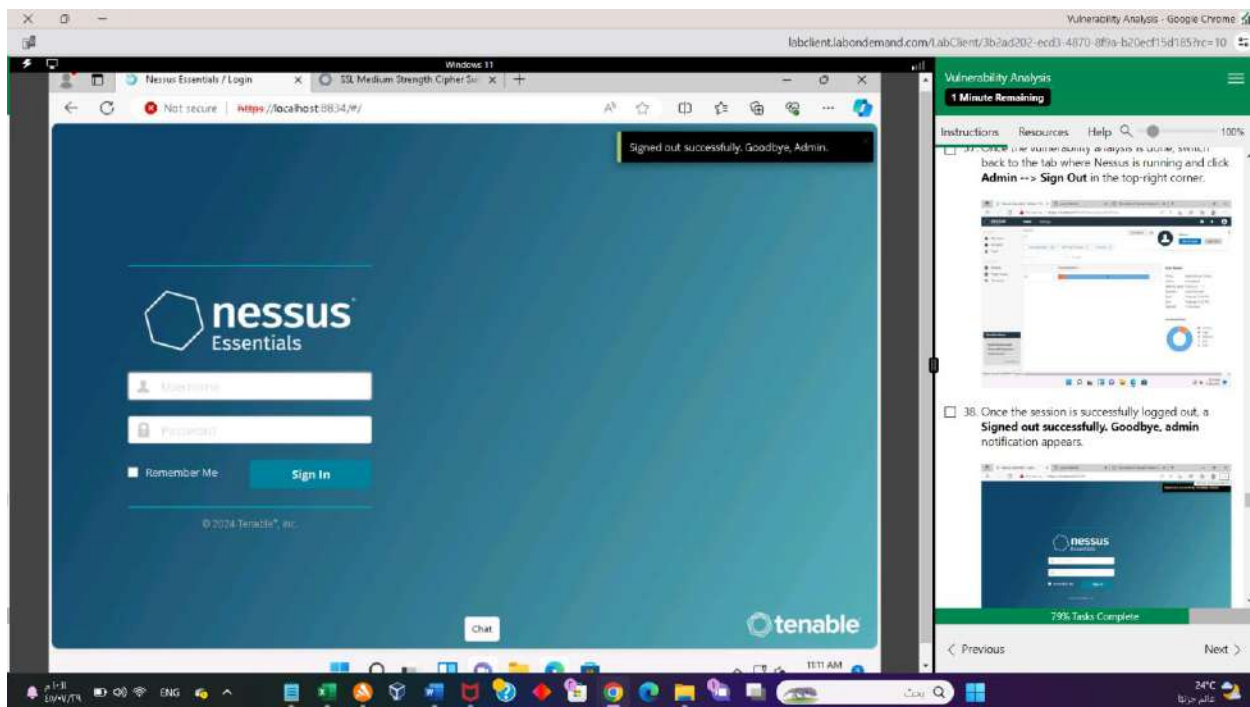
Instructions Resources Help 100%

1 Minute Remaining

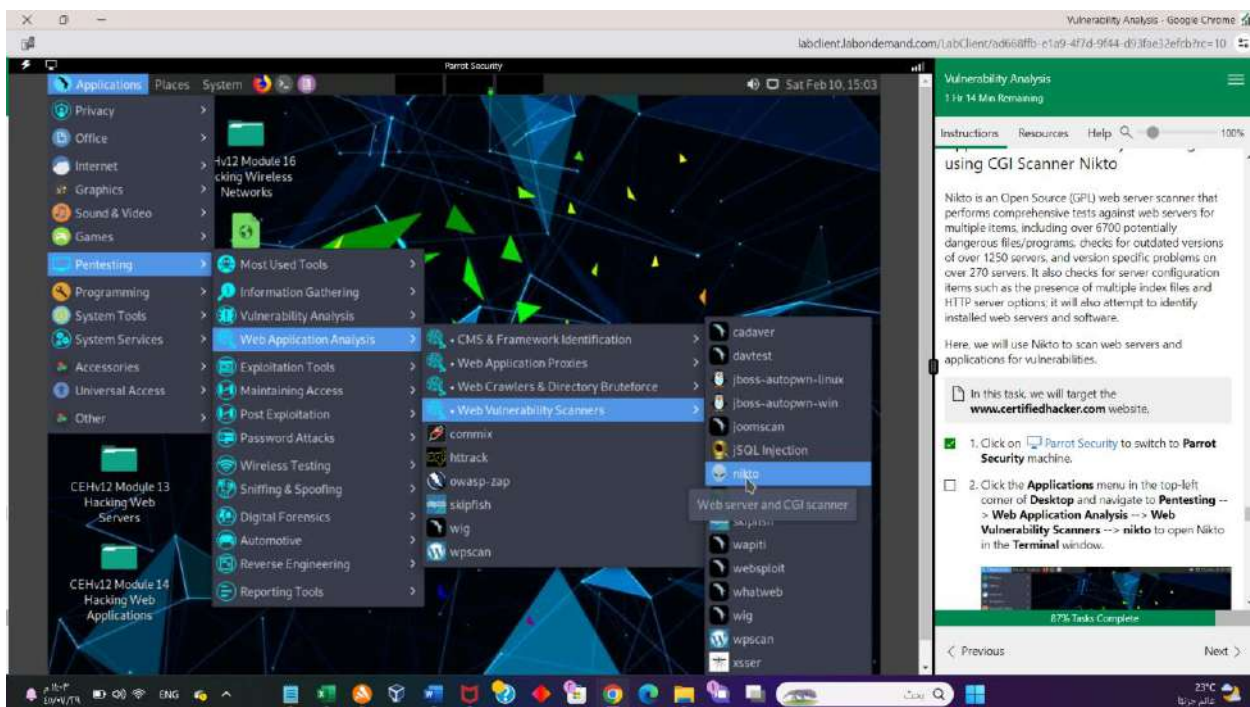
38. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.

79% Tasks Complete

Previous Next



Task3:



Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/ad668ffb-c1a9-4f7d-9f44-d938ae32efcb?hc=10

Parrot Security

Parrot Terminal

```
File Edit View Search Terminal Help
-Host+ Extended help information
-target+ target host/URL
-id+ Host authentication to use, format is id:pass or id:p
attacker's ass:realm
-List-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /direct
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value

Note: This is the short help output. Use -H for full help text.
```

CEHv12 Mo Hacking! Applications

Vulnerability Analysis
1 Hr 13 Min Remaining

Instructions Resources Help 100%

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.

87% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/ad668ffb-c1a9-4f7d-9f44-d938ae32efcb?hc=10

Parrot Security

nikto -H - Parrot Terminal

```
File Edit View Search Terminal Help
Note: This is the short help output. Use -H for full help text.
[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
          0 Debug output
          E Display all HTTP errors
          P Print progress to STDOUT
          C Scrub output of IPs and hostnames
          V Verbose output
          G database and other key files for syntax errors
          g technique:
            Random URI encoding (non-UTF8)
            Directory self-reference (./)
            Premature URL ending
            Prepend long random string
            Fake parameter
            TAB as request soacer
```

OMEN Gaming Hub

إعادة تشغيل التطبيق
تم تحديث أحد مكونات البرنامج وإزالة
تسجيل OMEN Gaming Hub. هل تريد إعادة
تسجيل OMEN Gaming Hub الآن؟
إعادة تشغيل التطبيق عدم الإظهار مرة أخرى

Vulnerability Analysis
1 Hr 12 Min Remaining

Instructions Resources Help 100%

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.

87% Tasks Complete

Previous Next

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/6d688ff0-e1a9-4f7d-9f44-d33ae32efcb7rc=10

Applications Places System Parrot Security Sat Feb 10, 15:06

File Edit View Search Terminal Help

```
-save Save positive responses to this directory ( . for auto-name)
-ssl Force ssl mode on port
-Tuning+ Scan tuning:
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (XSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
0 File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d Webservice
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdb+ Load only user databases, not the standard databases
all Disable standard dbs and load only user dbs
tests Disable only db tests and load udb_tests
-useragent Over-rides the default useragent
-until Run until the specified time or duration
-update Update databases and plugins from CIRT.net
-url+ Target host/URL (alias of -host)
-useproxy Use the proxy defined in nikto.conf, or argument http://server:port
-version Print plugin and database versions
-vhost+ Virtual host (for Host header)
```

Vulnerability Analysis
1 Hr 10 Min Remaining

Instructions Resources Help 100%

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.

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.

90% Tasks Complete

< Previous Next >

Vulnerability Analysis - Google Chrome
labclient.labondemand.com/LabClient/6d688ff0-e1a9-4f7d-9f44-d33ae32efcb7rc=10

Applications Places System Parrot Security Sat Feb 10, 15:08

File Edit View Search Terminal Help

```
-useproxy Use the proxy defined in nikto.conf, or argument http://server:port
-version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value

[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: 2024-02-10 15:08:11 (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 'host-header' found, with contents: c2hhcmV/KLmJsdWVob3N0LnNvbQ==
+ 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
```

Vulnerability Analysis
1 Hr 9 Min Remaining

Instructions Resources Help 100%

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.

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

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.

The result might differ when you perform this task.

90% Tasks Complete

< Previous Next >

