

Your virtual machines are starting  
Your lab will be ready in about 30 seconds.  
Show while starting Close Window

1

---

Close

2

3

- Reconnect
- Power On
- Pause
- Resume
- Reset/Reboot
- Power Off
- Fit Window to Machine
- Fit Machine To Window
- Open in New Window
- Split Windows
- Revert Machine
- Reset Internet Gateway

4

- Ctrl+Alt+Delete
- ALT+Tab
- Windows Key
  - Windows Key
  - Windows Key + D
  - Windows Key + E
  - Windows Key + F
  - Windows Key + M
  - Windows Key + R
  - Windows Key + X
  - Windows Key + ...
- Windows Key
- Type Text
  - Type Username
  - Type Password
  - Type Clipboard Text
- Virtual Keyboard

Windows 11<sup>5</sup>

Windows 11  
Windows Server 2022  
Windows Server 2019  
Parrot Security

## Poor Connection

---

Full Screen  
Power and Display  
Keyboard  
Machine Selection

This machine must be controlled outside of your browser via Remote Desktop.

Launch Remote Desktop

Username:

Password:

The selected machine is off.

Start

Machine is open in a separate window. [Close Window](#)

X

- Esc
- F1
  - F2
  - F3
  - F4
  - F5
  - F6
  - F7
  - F8
  - F9
  - F10
  - F11
  - F12
  - PrtSc
  - ScrLk
  - Pause
  - `
  - 1
  - 2
  - 3
  - 4
  - 5
  - 6
  - 7
  - 8
  - 9
  - 0
  - -
  - =
  - ← Backspace
  - Insert
  - Home
  - P Up

- NLock

- /
- \*
- -
- Tab
- q
- w
- e
- r
- t
- y
- u
- i
- o
- p
- [
- ]
- \
- Delete
- End
- P Down

- 7

- 8
- 9
- +
- Caps
- a
- s
- d
- f
- g
- h
- j
- k
- l
- ;
- '
- ↵ Enter

- 4

- 5
- 6
- Shift
- z
- x
- c
- v
- b
- n

- m
- ,
- .
- /
- Shift
- ↑

- 1

- 2
- 3
- Enter
- Ctrl
- Win
- Alt
- Alt
- Win
- Ctrl
- ←
- ↓
- →

- 0

- .

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

6

Password

7

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

- Not Connected

Username

Password

Reconnect

Vulnerability Analysis<sup>8</sup>

[Exit Lab](#)

Save Progress And Exit

End Lab

[InstructionsResources](#)

## Module 05: Vulnerability Analysis

### Scenario

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

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to

---

Type Text

Type Text

Vulnerability Analysis

conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

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

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

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

### **Objective**

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

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

### **Overview of Vulnerability Assessment**

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

### **Lab Tasks**

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

1. Perform vulnerability research with vulnerability scoring systems and databases
  - o Perform vulnerability research in Common Weakness Enumeration (CWE)
2. Perform vulnerability assessment using various vulnerability assessment tools
  - o Perform vulnerability analysis using OpenVAS
3. Perform Vulnerability Analysis using AI
  - o Perform vulnerability analysis using ShellGPT

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

#### **Lab Scenario**

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

#### **Lab Objectives**

- Perform vulnerability research in Common Weakness Enumeration (CWE)

### **Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases**

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

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

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

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

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

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

1. By default, **Windows 11** machine is selected, click [Ctrl+Alt+Delete](#) to activate the machine and login with **Admin/Pa\$\$w0rd**.
2. Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Launch any web browser, and go to **<https://cwe.mitre.org/>** website (here, we are using **Mozilla Firefox**).
4. If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
5. If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click start browsing to finish viewing the information.
6. **CWE** website appears. Navigate to **Search** tab, in the **Google Custom Search** under **Access Content** section and search for **SMB** in the search field.
7. 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).

8.

CWE - Common Weakness Enum

https://cwe.mitre.org

software developers, hardware designers, and security architects can eliminate them before deployment, when it is much easier and cheaper to do so

### Learn About CWE

Overview – Learn what CWE is and how to use the information available on this website

[Basics](#)  
[FAQs](#)  
[Glossary](#)

Root Cause Mapping – Learn about identifying the underlying cause(s) of a vulnerability

[Guidance](#)  
[Quick Tips](#)  
[Examples](#)

### Access Content

[All Weaknesses \(943 total\)](#)  
[Top-N Lists](#)

Search CWE

SMB

View CWEs by

Software Development

Hardware Design

All Weaknesses

Other Select Options

### Contribute

[Contribute CWE Content](#)  
[Participate in Working Groups](#)

### Latest News and Updates

**News** [Videos of Three CWE-Focused Sessions at VulnCon 2025 Now Available](#)

**Podcast** [“Root Cause Mapping and the CWE Top 25”](#)

**News** [CWE Version 4.17 Now Available!](#)

**News** [“2024 CWE Top 10 KEV Weaknesses” List Now Available](#)

**Community** [View and Comment on Community Submissions in the “CWE Content Development Repository \(CDR\)”](#)

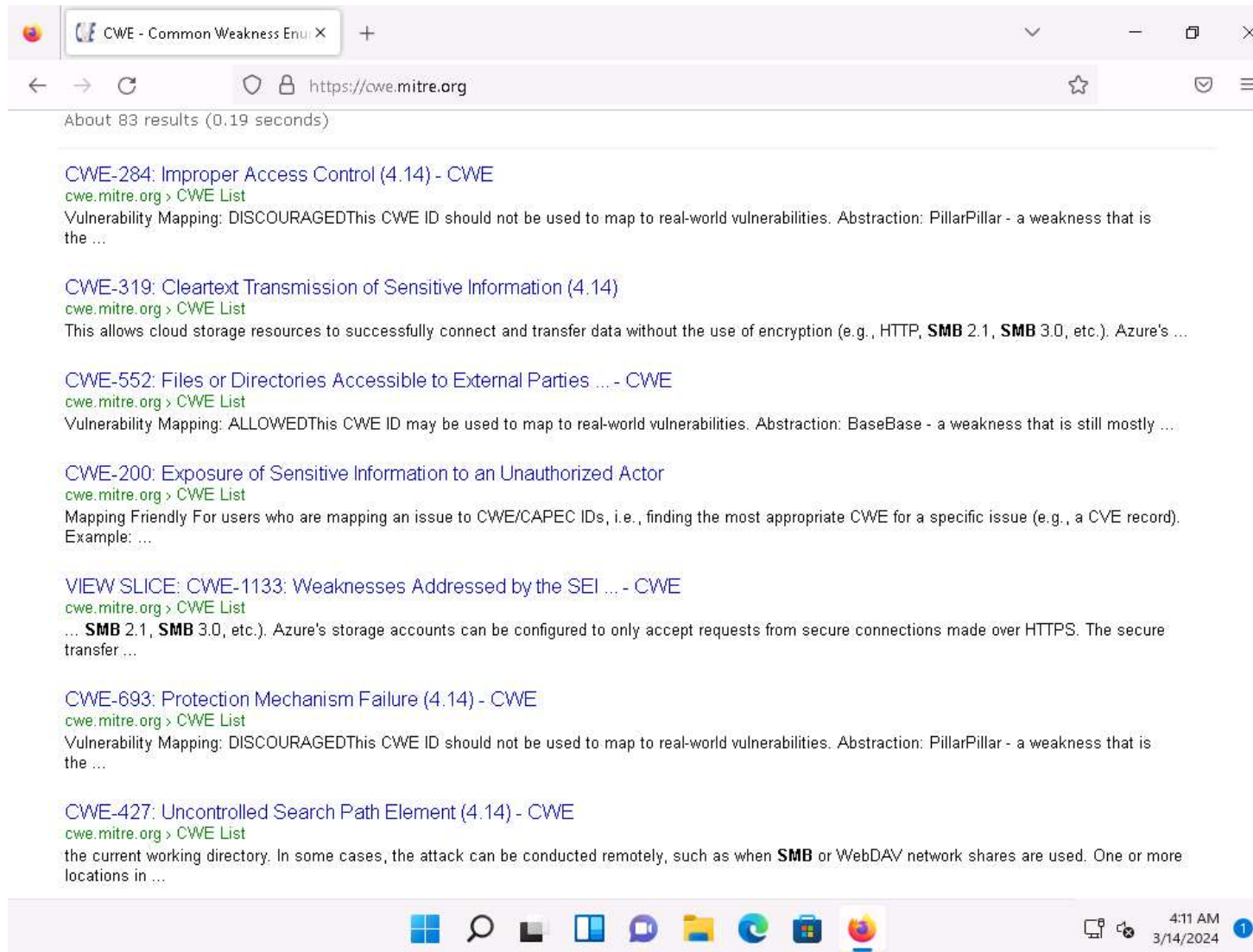
**Community** [CWE Is Focus of Four Talks at VulnCon 2025](#)

**News** [Follow the CWE Program on Bluesky](#)

9. The search results appear, scroll-down to view the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.
10. The search results might differ when you perform this task



11.



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

13.

The screenshot shows a web browser window with two tabs: 'CWE - Common Weakness Enum...' and 'CWE - CWE-284: Improper Access Control'. The address bar shows the URL 'https://cwe.mitre.org/data/definitions/284.html'. The page header includes the CWE logo, the text 'Common Weakness Enumeration', and a tagline 'A community-developed list of SW & HW weaknesses that can become vulnerabilities'. There are also circular badges for 'Top 25' and 'Top HW CWE', and a 'New to CWE Start here!' link. A navigation bar contains links: Home, About, CWE List, Mapping, Top-N Lists, Community, News, and Search. The main heading is 'CWE-284: Improper Access Control'. Below this, it shows 'Weakness ID: 284', 'Vulnerability Mapping: DISCOURAGED', and 'Abstraction: Pillar'. There are buttons for 'View customized information:' with options: Conceptual, Operational, Mapping Friendly, Complete (selected), and Custom. The 'Description' section states: 'The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.' The 'Extended Description' section states: 'Access control involves the use of several protection mechanisms such as:'. It lists three bullet points: 'Authentication (proving the identity of an actor)', 'Authorization (ensuring that a given actor can access a resource), and', and 'Accountability (tracking of activities that were performed)'. It then states: '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.' and 'There are two distinct behaviors that can introduce access control weaknesses:'. It lists two bullet points: '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.' and 'Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the...'. The Windows taskbar at the bottom shows the Start button, search, and several application icons, along with the system clock showing 4:12 AM on 3/14/2024.

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

15. Now, navigate to the **CWE List** tab. **CWE List Version** will be displayed. Scroll down, and under the **External Mappings** section, select **CWE Top 25 (2023)**.

16. The result might differ when you perform this task.

17.

The screenshot shows a web browser with two tabs: "CWE - Common Weakness Enumeration" and "CWE - CWE List Version 4.14". The address bar shows the URL "https://cwe.mitre.org/data/index.html". The page content includes a section titled "External Mappings" with a description: "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." Below this is a vertical list of 15 buttons: "CWE Top 25 (2023)", "Most Important Hardware Weaknesses List (2021)", "OWASP Top Ten (2021)", "Seven Pernicious Kingdoms", "Software Fault Pattern Clusters", "SEI CERT Oracle Coding Standard for Java", "SEI CERT C Coding Standard", "SEI CERT Perl Coding Standard", "Addressed by ISA/IEC 62443 Requirements", "CISQ Quality Measures (2020)", "CISQ Data Protection Measures", "SEI ETF Security Vulnerabilities in ICS", and "Architectural Concepts". A "BACK TO TOP" link is visible on the right. Below this is a section titled "Helpful Views" with a description: "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." Below the description is a search bar containing the URL "https://cwe.mitre.org/data/definitions/1425.html" and a button labeled "Introduced During Design". The bottom of the screenshot shows a Windows taskbar with various application icons and a system clock displaying "4:15 AM 3/14/2024".

18. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can check each weakness to view detailed information on it.
19. This information can be used to exploit the vulnerabilities in the software and further launch attacks.
20. The result showing publishing year might differ when you perform this task.

21.

The screenshot shows a web browser window with two tabs: 'CWE - Common Weakness Enum...' and 'CWE - CWE-1425: Weaknesses'. The address bar shows the URL 'https://cwe.mitre.org/data/definitions/1425.html'. The page content is titled '1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses'. It lists 25 weaknesses with their respective counts in parentheses. The list includes: Out-of-bounds Write (787), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (79), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (89), Use After Free (416), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (78), Improper Input Validation (20), Out-of-bounds Read (125), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (22), Cross-Site Request Forgery (CSRF) (352), Unrestricted Upload of File with Dangerous Type (434), Missing Authorization (862), NULL Pointer Dereference (476), Improper Authentication (287), Integer Overflow or Wraparound (190), Deserialization of Untrusted Data (502), Improper Neutralization of Special Elements used in a Command ('Command Injection') (77), Improper Restriction of Operations within the Bounds of a Memory Buffer (119), Use of Hard-coded Credentials (798), Server-Side Request Forgery (SSRF) (918), Missing Authentication for Critical Function (306), Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (362), Improper Privilege Management (269), Improper Control of Generation of Code ('Code Injection') (94), Incorrect Authorization (863), and Incorrect Default Permissions (276). At the bottom of the list is a 'BACK TO TOP' link. Below the list is a section titled 'Vulnerability Mapping Notes' with a 'Usage: PROHIBITED' warning and a 'Reason: View' link. The Windows taskbar at the bottom shows the time as 4:16 AM on 3/14/2024.

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

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

BACK TO TOP

Vulnerability Mapping Notes

Usage: **PROHIBITED** (this CWE ID must not be used to map to real-world vulnerabilities)

Reason: View

22. Similarly, you can go back to the CWE website and explore other options, as well.
23. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.
24. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
25. Close all open windows and document all the acquired information.

#### Question 5.1.1.1

Search the Common Weakness Enumeration (CWE) list and find the name of the vulnerability with the CWE ID 591.  
Score

#### Question 5.1.1.2

Search the Common Weakness Enumeration (CWE) list and find the top weakness in the list "Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weakness."  
Score

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

### Lab Scenario



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

### Lab Objectives

- Perform vulnerability analysis using OpenVAS

### Overview of Vulnerability Assessment

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

There are two approaches to network vulnerability scanning:

- Active Scanning
- Passive Scanning

### Task 1: Perform Vulnerability Analysis using OpenVAS

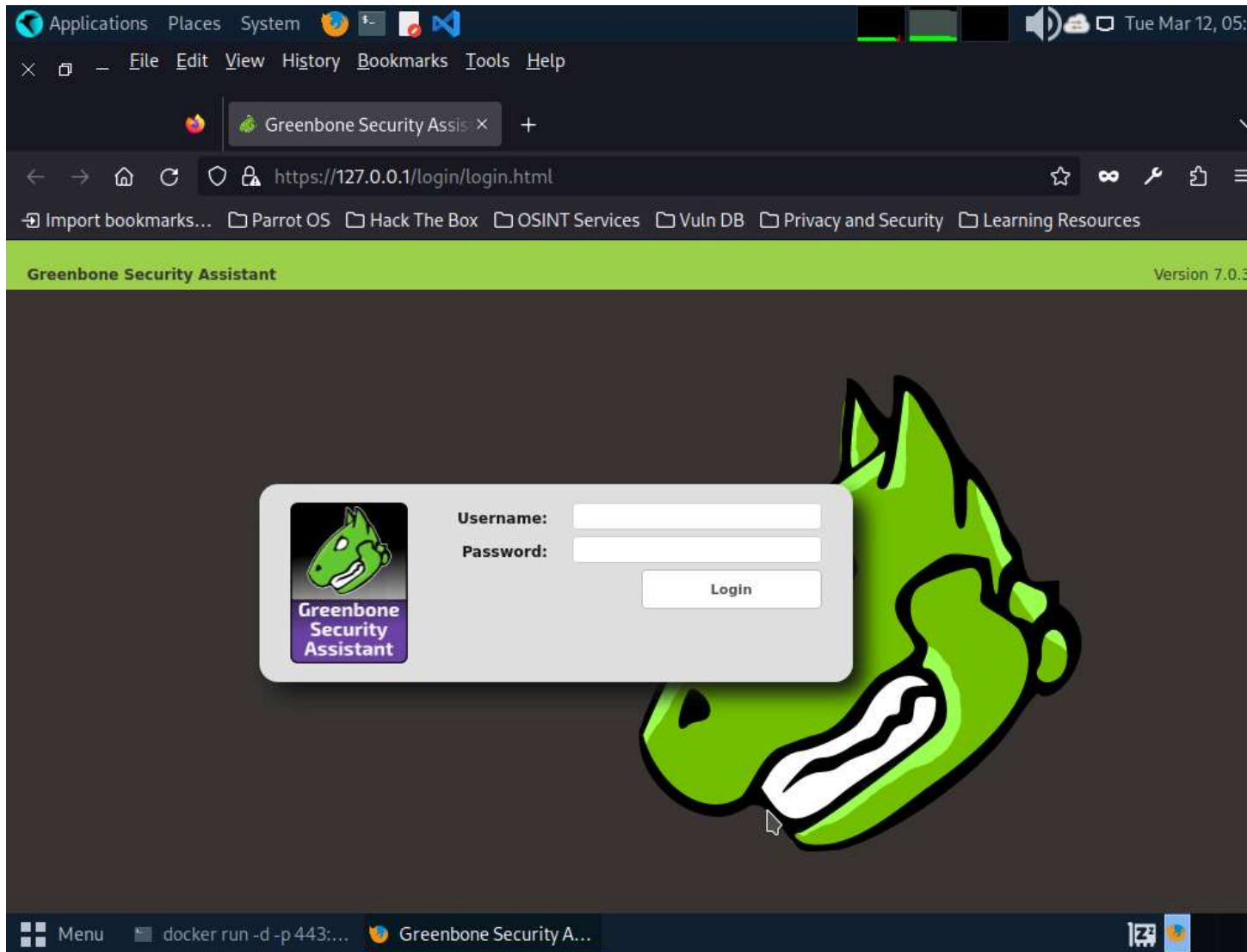
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance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

Here, we will perform a vulnerability analysis using OpenVAS.

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

1. Click on [Parrot Security](#) to switch to the **Parrot Security** machine and login with **attacker/toor**.
2. If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
3. If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
5. The password that you type will not be visible.
6. Run **docker run -d -p 443:443 --name openvas mikesplain/openvas** command to launch OpenVAS.
7. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.
8. The **Firefox** browser appears, go to **https://127.0.0.1/**. OpenVAS login page appears, log in with **admin/admin**.
9. If a **Warning** page appears, click **Advanced** and select **Accept the Risk and Continue**.

10.



11. The **OpenVAS Dashboards** appears. Navigate to **Scans --> Tasks** from the **Menu** bar.
12. If a **Welcome to the scan task management!** pop-up appears, close it.

13.

Applications Places System Tue Mar 12, 05:...

Greenbone Security Assis x

https://127.0.0.1/omp?r=1&token=ed4fcc93-d478-4b3e-9a71-adb1326be455

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

**Greenbone**  
Security Assistant

No auto-refresh Logged in as Admin **admin** | Logout  
Tue Mar 12 09:23:11 2024 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Dashboard

Dashboard

Tasks

Reports

Results

Notes

Overrides

Tasks by status (Total: 0)

CVEs by creation time (Total: 120352)

/ year

20,000 18,000 16,000

130,000 120,000 110,000 100,000

Hosts topology

NVTs by Severity Class (Total: 49787)

High

Medium

Low

Log

3591

1858

22033

https://127.0.0.1/omp?cmd=get\_tasks&token=ed4fcc93-d478-4b3e-9a71-adb1326be455

Menu docker run -d -p 443:... Greenbone Security A...

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

15.

Applications Places System

Greenbone Security Assistant

https://127.0.0.1/omp?cmd=get\_tasks&token=ed4fcc93-d478-4b3e-9a71-adb1326be4

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

**Greenbone Security Assistant** No auto-refresh Logged in as Admin **admin** | Logout Tue Mar 12 09:24:24 2024 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Task Wizard  
Advanced Task Wizard  
Modify Task Wizard

Filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name

**Tasks (0 of 0)**

Tasks by Severity Class (Total: 0)

Tasks with most High results per host  
No Tasks with High severity found

Tasks by status (Total: 0)

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
https://127.0.0.1/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=ed4fcc93-d478-4b3e-9a71-adb1326be455						

Menu docker run -d -p 443:443 Greenbone Security Assistant

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



17.

The screenshot shows the Greenbone Security Assistant (GSA) web interface. A 'Task Wizard' modal is open, guiding the user through a quick start scan. The wizard includes a list of steps and a 'Start Scan' button. The background shows the GSA dashboard with a table of tasks.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

18. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.
19. 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.
20. It takes approximately 20 minutes for the scan to complete.
21. If you are logged out of the session then login again using credentials **admin/admin**.

22.

Applications Places System Tue Mar 12, 06:...

Greenbone Security Assis x

← → Home Refresh Lock [https://127.0.0.1/omp?cmd=get\\_tasks&token=521d747f-cb51-46e8-abbe-837c64e84e](https://127.0.0.1/omp?cmd=get_tasks&token=521d747f-cb51-46e8-abbe-837c64e84e) ☆ ∞ 🔧 📁


Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

## Tasks (1 of 1)

Tasks by Severity Class (Total: 1)

Medium



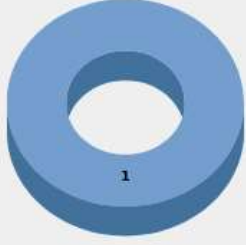
1

Tasks with most High results per host

No Tasks with High severity found

Tasks by status (Total: 1)

Done



1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
<a href="#">Immediate scan of IP 10.10.1.22</a>	Done	1 (1)	Mar 12 2024	5.0 (Medium)		

(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.

Menu docker run -d -p 443:... Greenbone Security A...

23. **Report: Results** appear, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

24. The results might differ when you perform this task.

25.

Applications Places System

Greenbone Security Assistant

https://127.0.0.1/omp?cmd=get\_report&report\_id=cd423c0b-daa4-4885-b01c-e30452f579

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Greenbone Security Assistant

Logged in as Admin admin | Logout

99:51:48 2024 U

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done

Filter: autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70

Report: Results (2 of 61)

ID: cd423c0b-daa4-4885-b01c-e30452f579  
Modified: Mon Jul 8 09:45:25 2024  
Created: Mon Jul 8 09:29:35 2024  
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.1.22	135/tcp	
TCP timestamps	2.6 (Low)	80%	10.10.1.22	general/tcp	

(Applied filter:autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70)

Backend operation: 0.40s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Menu docker run -p 443:... Greenbone Security A...

26. Click on any vulnerability under the **Vulnerability** column to view its detailed information.

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

28.

The screenshot shows the Greenbone Security Assistant web interface. The top navigation bar includes links for Applications, Places, System, and various system icons. The main header displays the Greenbone logo and the user is logged in as 'Admin' (admin). The navigation menu includes Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help.

The main content area displays a vulnerability report titled "Result: DCE/RPC and MSRPC Services Enumeration Reporting". The report details are as follows:

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.1.22	135/tcp	[Icons]

**Summary**  
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Vulnerability Detection Result**  
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 2103/tcp

```

UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
Endpoint: ncacn_ip_tcp:10.10.1.22[2103]
Annotation: Message Queuing - QM2QM V1

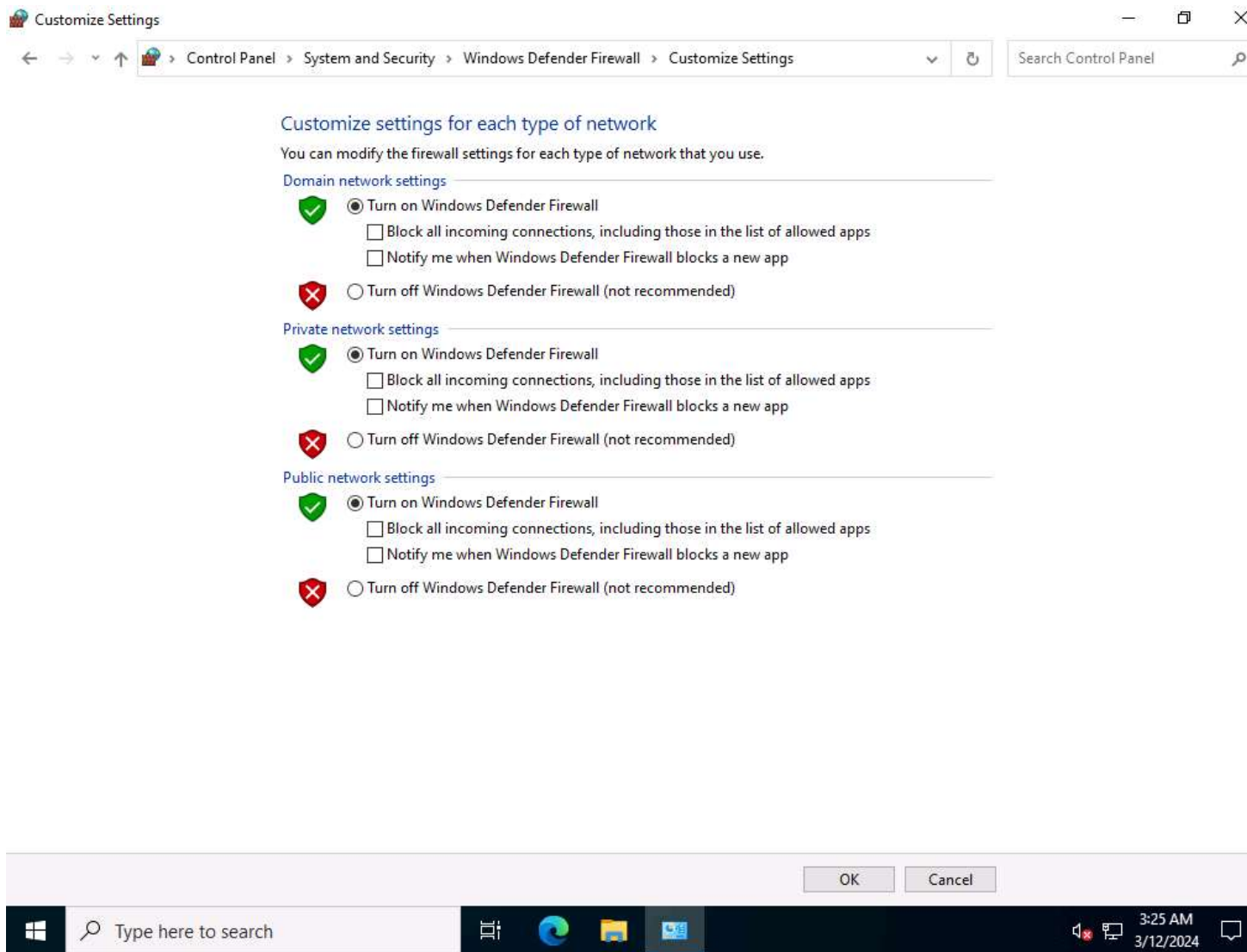
UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
Endpoint: ncacn_ip_tcp:10.10.1.22[2103]
Annotation: Message Queuing - RemoteRead V1
  
```

The bottom of the screenshot shows a terminal window with the command `docker run -d -p 443:...` and the Greenbone Security Assistant logo.

29. Similarly, you can check other Reports by hovering over the **Report: Results** section to view other Reports regarding the vulnerabilities in the target system.
30. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2022** machine.
31. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
32. Click on [Windows Server 2022](#) to switch to the **Windows Server 2022** machine and click [Ctrl+Alt+Delete](#) and login with **CEHAdministrator / Pa\$\$w0rd**.
33. Navigate to **Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, enable Windows Firewall**, and click **OK**.
34. By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.



35.



36. Click on [Parrot Security](#) to switch to **Parrot Security** machine and perform **Steps# 7-9** to create another task for scanning the target system.
37. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.
38. After the completion of the scan, click the **Done** button under the **Status** column.
39. It takes approximately 15-20 minutes for the scan to complete.
40. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.
41. The results might differ when you perform this task.

42.

Applications Places System

Greenbone Security Assistant

https://127.0.0.1/omp?cmd=get\_report&report\_id=8a9680fe-5bb8-4207-9631-8d009f8bf2

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Greenbone Security Assistant

Logged in as Admin admin | Logout

10:10:07 2024 U

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done

Filter: autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70

Report: Results (2 of 43)

ID: 8a9680fe-5bb8-4207-9631-8d009f8bf2

Modified:

Created:

Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.1.22	135/tcp	
TCP timestamps	2.6 (Low)	80%	10.10.1.22	general/tcp	

(Applied filter:autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70)

Backend operation: 0.40s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.

43. 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.
44. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
45. Close all open windows and document all the acquired information.
46. Click on [Windows Server 2022](#) to switch to the **Windows Server 2022** machine and click [Ctrl+Alt+Delete](#) login with **Administrator/Pa\$\$w0rd**.
47. Navigate to **Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off**, disable Windows Firewall, and click **OK**.

#### Question 5.2.1.1

Perform vulnerability analysis for the target machine (10.10.1.22) using OpenVAS and find the number of vulnerabilities in the system. Enter the Severiety level of the DCE/RPC and MSRPC Services Enumeration Reporting vulnerability.

Score

### Lab 3: Perform Vulnerability Analysis using AI

#### Lab Scenario

As a professional ethical hacker or pen tester, you must acknowledge the limitations of conventional approaches in revealing all potential vulnerabilities. Therefore, you will utilize AI-driven vulnerability analysis tools to identify and assess security weaknesses in a simulated network environment.

## Lab Objectives

- Perform vulnerability analysis using ShellGPT

### Overview of vulnerability analysis using AI

Vulnerability Analysis with AI employs advanced algorithms to unearth hidden security flaws in networks. AI-driven tools extract comprehensive data, prioritize risks, and fortify defenses, empowering ethical hackers to anticipate and mitigate emerging threats effectively. This innovative approach enhances cybersecurity readiness by leveraging AI's precision and adaptability.

### Task 1: Perform Vulnerability Analysis using ShellGPT

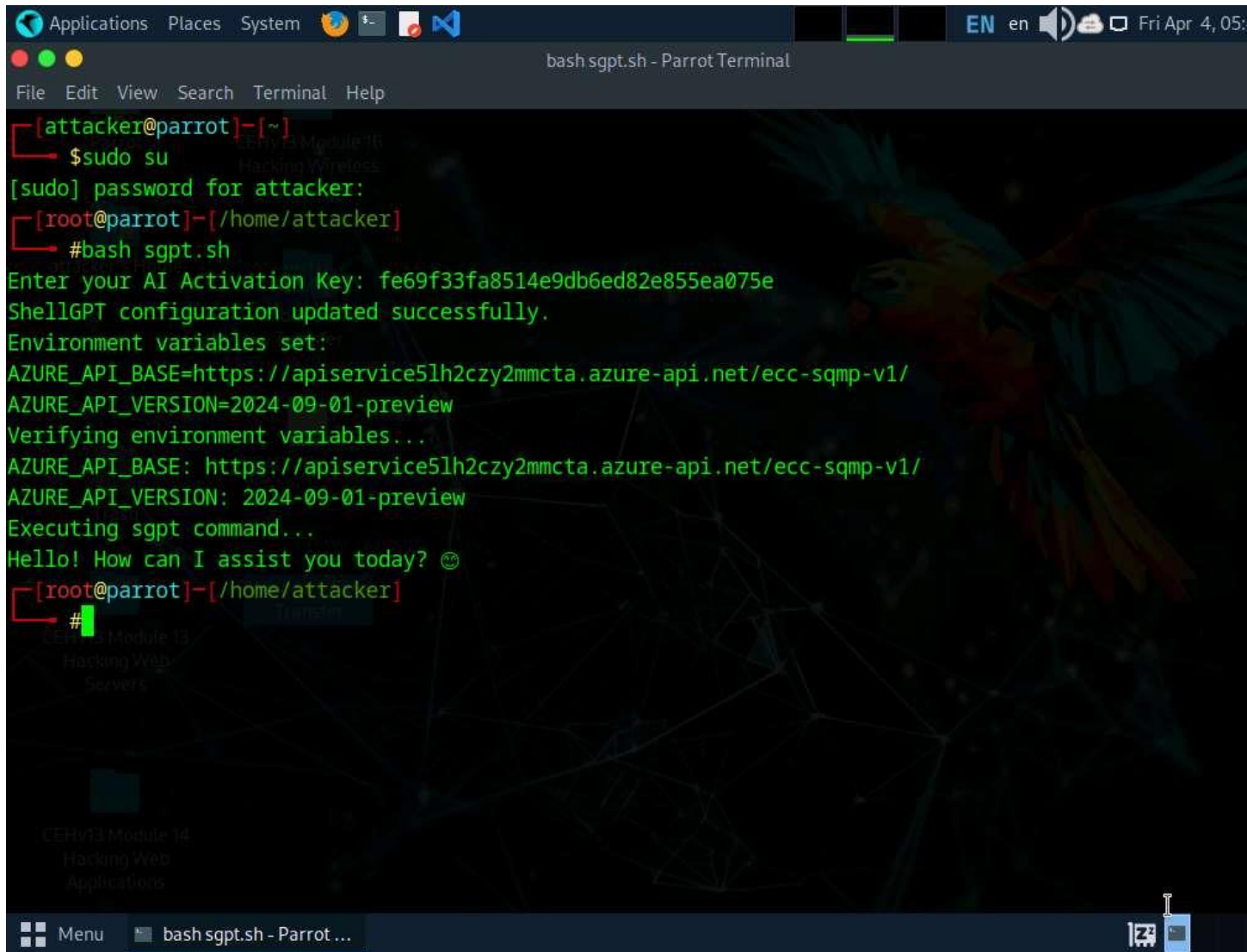
ShellGPT swiftly interprets and executes commands, conducting scans, identifying weaknesses, and suggesting mitigation strategies in real-time. Its adaptive nature facilitates dynamic navigation through complex systems, enhancing efficiency and precision in vulnerability analysis. By integrating ShellGPT, you can gain a powerful ally in their quest to safeguard digital ecosystems, leveraging AI's capabilities to uncover and address security risks with unparalleled speed and accuracy.

Here, we will use ShellGPT to discover potential vulnerabilities in the target.

The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Click [Parrot Security](#) to switch to Parrot machine, and login with **attacker/toor**. Open a Terminal window and execute **sudo su** to run the program as a root user (When prompted, enter the password **toor**).
2. The password that you type will not be visible.
3. Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.
4. You can follow the **Instructions to Download your AI Activation Key** in **Module 00: CEH Lab Setup** to obtain the AI activation key. Alternatively, follow the instructions available in the file, [Instructions to Download your AI Activation Key.pdf](#)

5.

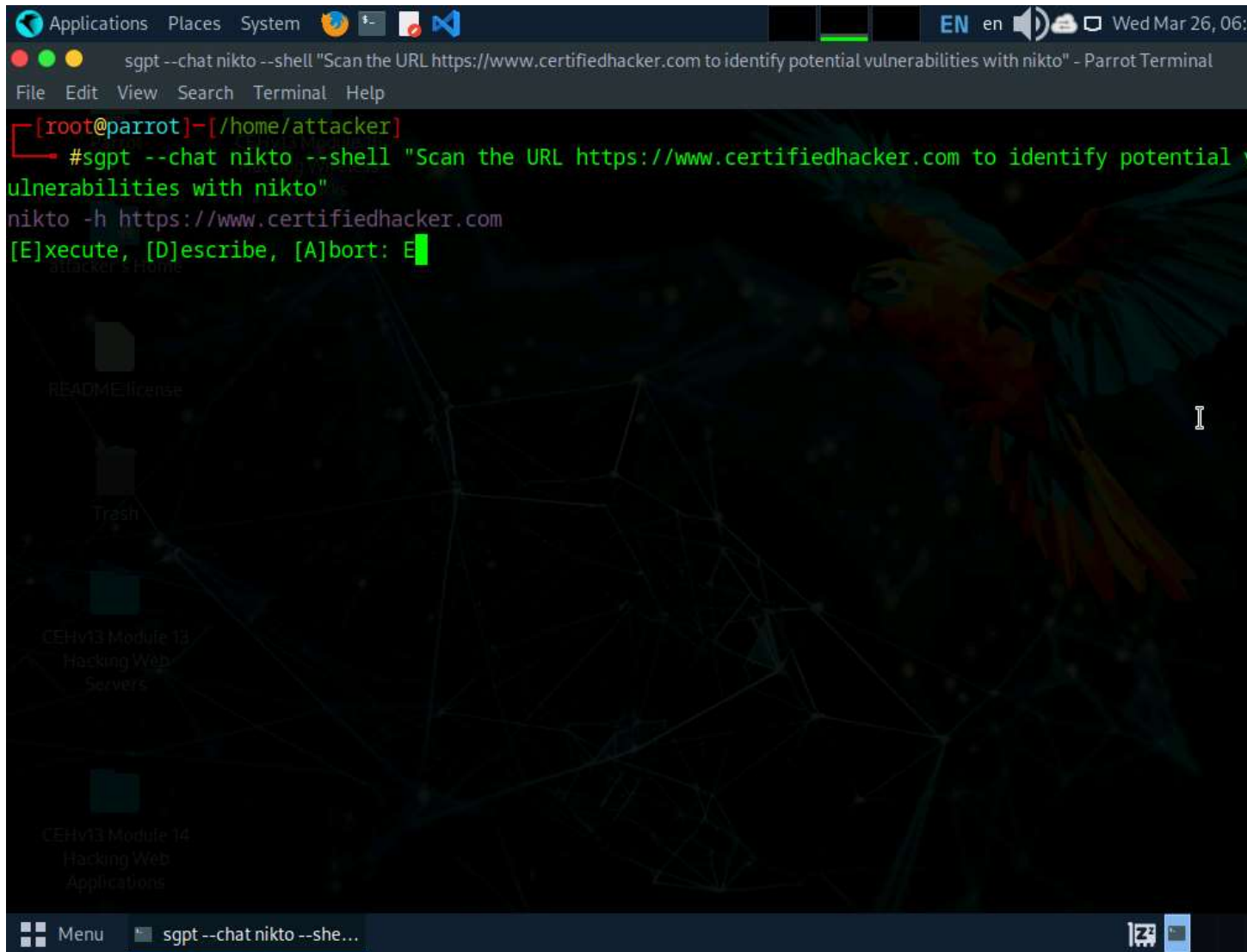


```
Applications Places System [Icons] [Terminal] [EN] en [Speaker] [Network] [Battery] [Clock] Fri Apr 4, 05:
bash sgpt.sh - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# bash sgpt.sh
Enter your AI Activation Key: fe69f33fa8514e9db6ed82e855ea075e
ShellGPT configuration updated successfully.
Environment variables set:
AZURE_API_BASE=https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION=2024-09-01-preview
Verifying environment variables...
AZURE_API_BASE: https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION: 2024-09-01-preview
Executing sgpt command...
Hello! How can I assist you today? 😊
[root@parrot]-[/home/attacker]
#
```

6. After configuring the ShellGPT in Parrot Security machine, in the terminal window, run `**sgpt`
7. `--chat nikto --shell "Scan the URL https://www.certifiedhacker.com to identify potential vulnerabilities with nikto"` to launch Nikto scan on the target website.
8. In the prompt, type **E** and press **Enter** to execute the command.



9.



10. Scan result appears displaying the discovered vulnerabilities in the target website (here, **www.certifiedhacker.com**), as shown in the screenshot.

11.

Applications Places System EN en Wed Mar 26, 06:00

sgpt --chat nikto --shell "Scan the URL https://www.certifiedhacker.com to identify potential vulnerabilities with nikto" - Parrot Terminal

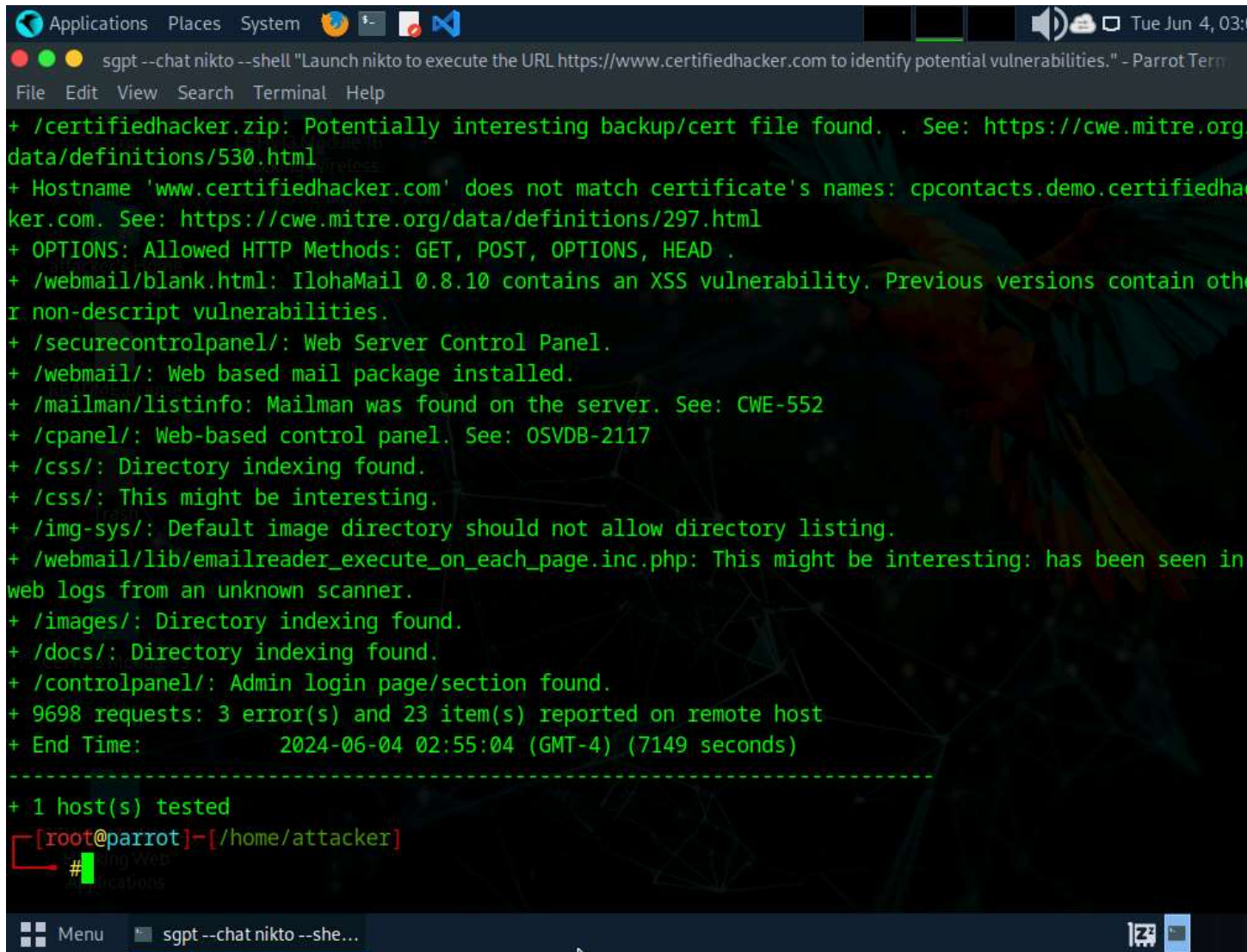
File Edit View Search Terminal Help

```
[root@parrot]-[/home/attacker]
#sgpt --chat nikto --shell "Scan the URL https://www.certifiedhacker.com to identify potential
vulnerabilities with nikto"
nikto -h https://www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
- Nikto v2.5.0

-----
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        443
-----
+ SSL Info:           Subject:  /CN=webdisk.certifiedhacker.com
                      Ciphers:  TLS_AES_256_GCM_SHA384
                      Issuer:   /C=US/O=Let's Encrypt/CN=R10
+ Start Time:         2025-03-26 06:37:53 (GMT-4)
-----
+ Server: nginx/1.25.5
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ /: Uncommon header 'x-server-cache' found, with contents: true.
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWVob3N0LmNvbQ==.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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. See: https://www.netsparker.com/web-vulneral
```

Menu sgpt --chat nikto --she...

12.



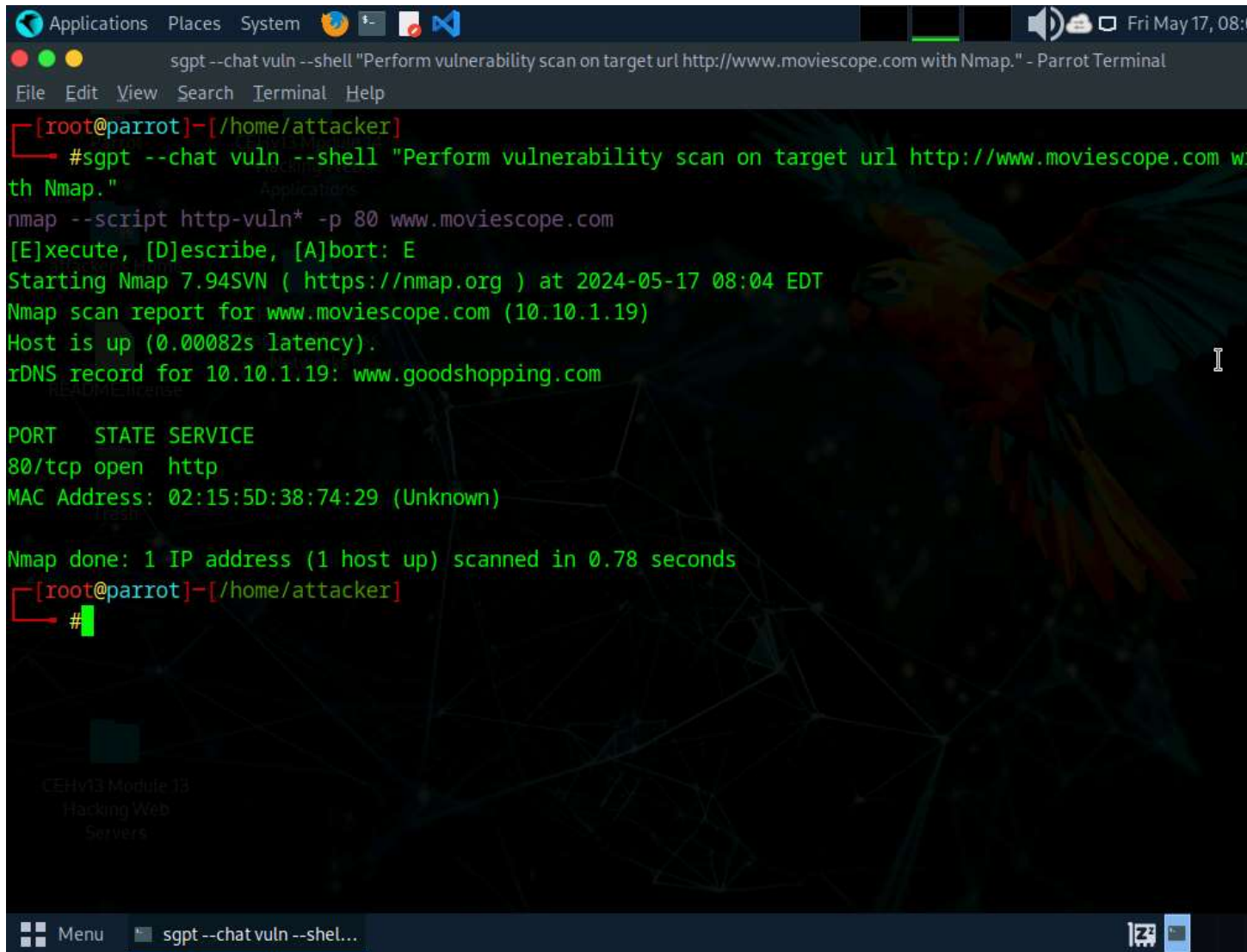
```
Applications Places System [icons] [system tray] Tue Jun 4, 03:
sgpt --chat nikto --shell "Launch nikto to execute the URL https://www.certifiedhacker.com to identify potential vulnerabilities." - Parrot Tern
File Edit View Search Terminal Help
+ /certifiedhacker.zip: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org
data/definitions/530.html
+ Hostname 'www.certifiedhacker.com' does not match certificate's names: cpcontacts.demo.certifiedha
ker.com. See: https://cwe.mitre.org/data/definitions/297.html
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain oth
r non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel.
+ /webmail/: Web based mail package installed.
+ /mailman/listinfo: Mailman was found on the server. See: CWE-552
+ /cpanel/: Web-based control panel. See: OSVDB-2117
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img-sys/: Default image directory should not allow directory listing.
+ /webmail/lib/emailreader_execute_on_each_page.inc.php: This might be interesting: has been seen in
web logs from an unknown scanner.
+ /images/: Directory indexing found.
+ /docs/: Directory indexing found.
+ /controlpanel/: Admin login page/section found.
+ 9698 requests: 3 error(s) and 23 item(s) reported on remote host
+ End Time: 2024-06-04 02:55:04 (GMT-4) (7149 seconds)
-----
+ 1 host(s) tested
[root@parrot]-[/home/attacker]
#
```






13. Nikto scan takes long time to complete. You can terminate the scan, by pressing **Ctrl + Z**.

14. In the terminal, run **sgpt --chat vuln --shell "Perform vulnerability scan on target url <http://www.moviescope.com> with Nmap"** command to perform vulnerability scan on the target website. The result appears displaying open ports and services running on the target website.



15.



```
Applications Places System      Fri May 17, 08:04
sgpt --chat vuln --shell "Perform vulnerability scan on target url http://www.moviescope.com with Nmap." - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sgpt --chat vuln --shell "Perform vulnerability scan on target url http://www.moviescope.com with Nmap."
nmap --script http-vuln* -p 80 www.moviescope.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 08:04 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00082s latency).
rDNS record for 10.10.1.19: www.goodshopping.com

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:15:5D:38:74:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
[root@parrot]~/home/attacker
#
```

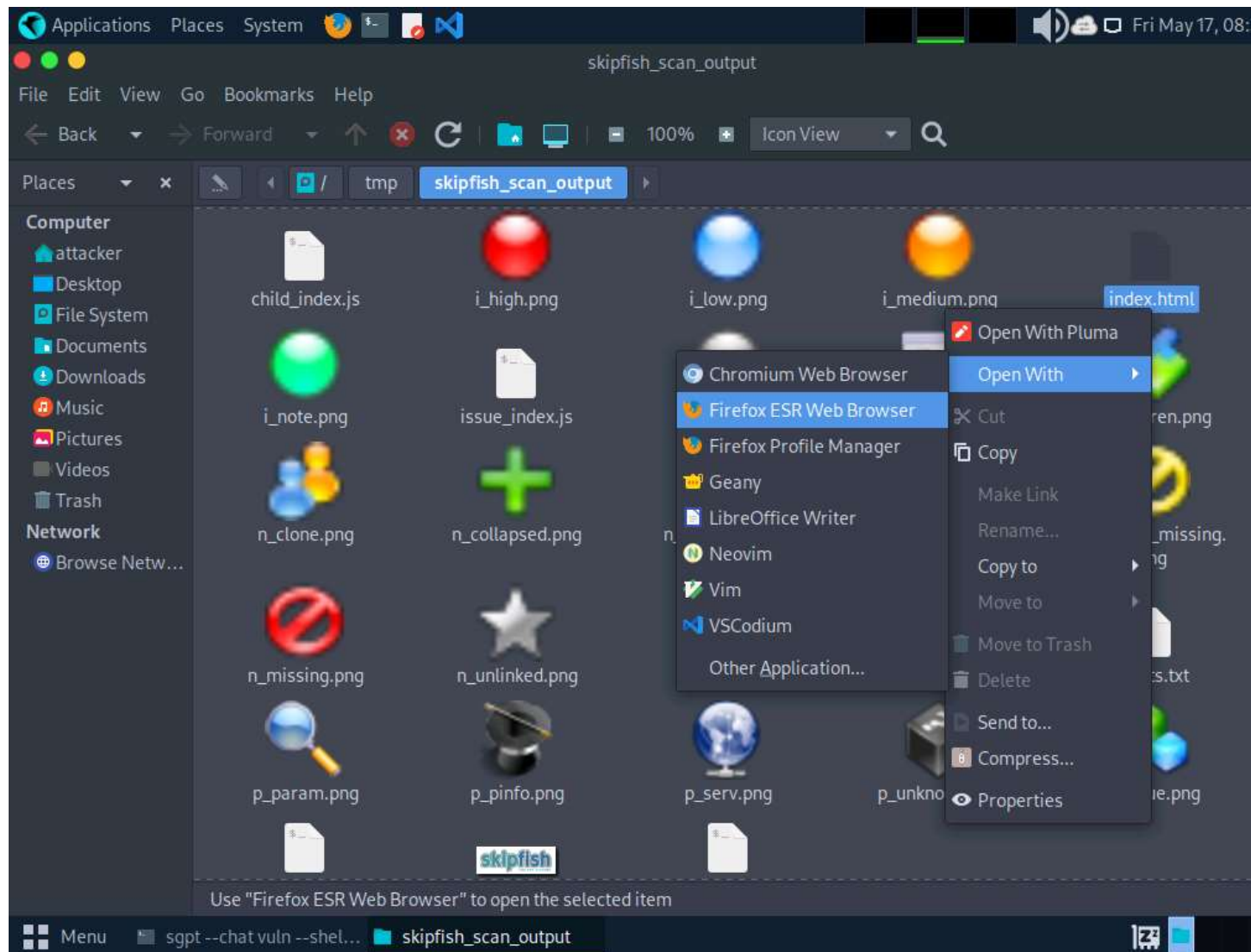
16. Run **sgpt --chat vuln --shell "Perform a vulnerability scan on target url http://testphp.vulnweb.com with skipfish"** to scan the target URL using skipfish tool.
17. If a prompt appears, enter any key to continue the scanning process.

18.

```
Applications  Places  System  Fri May 17, 08:
sgpt --chat vuln --shell "Perform a vulnerability scan on target url http://testphp.vulnweb.comwith skipfish" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --chat vuln --shell "Perform a vulnerability scan on target url http://testphp.vulnweb.comwith skipfish"
skipfish -o /tmp/skipfish_output http://testphp.vulnweb.com
[E]xecute, [D]escribe, [A]bort: E
```

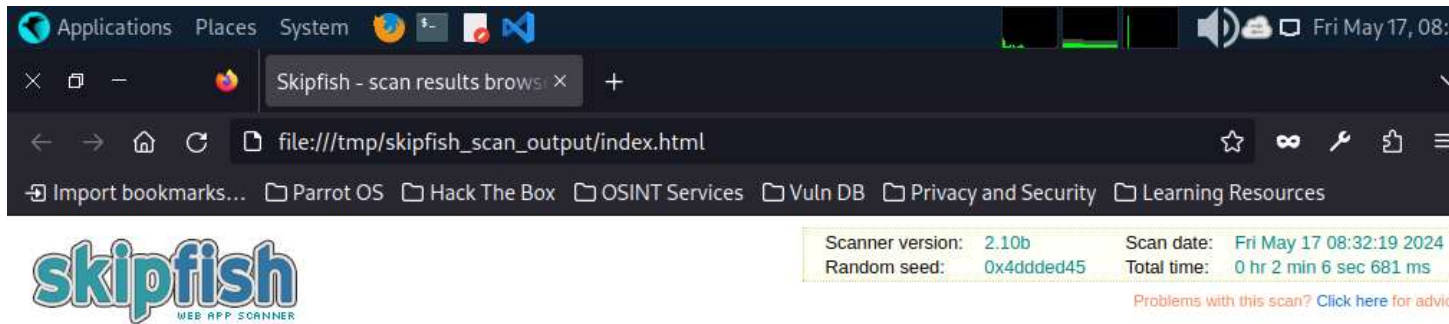
19. The skipfish begins scanning the target url. After the successful completion of the scan, report is saved at the **/tmp/skipfish\_scan\_output/** location, named as **index.html**. Navigate to the location, right-click on **index.html** and open with **Firefox ESR Web Browser**, as shown in the screenshot.
20. The location of scan report might differ. You can view the location in the skipfish command generated by ShellGPT.

21.



22. Firefox browser window appears displaying the complete scan report, as shown in the screenshot.

23.









**Crawl results - click to expand:**

**Document type overview - click to expand:**

-  **application/xhtml+xml** (8)
-  **text/css** (1)
-  **text/html** (5)
-  **text/plain** (2)

**Issue type overview - click to expand:**

-  **Conflicting MIME / charset info (higher risk)** (9)
-  **HTML form with no apparent XSRF protection** (6)
-  **External content embedded on a page (lower risk)** (6)
-  **Limits exceeded, fetch suppressed** (30)
-  **Resource fetch failed** (21)
-  **Numerical filename - consider enumerating** (2)



24. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct vulnerability assessments on the target.
25. This concludes the demonstration of performing vulnerability assessment on the target system using ShellGPT.
26. Close all open windows and document all the acquired information.

#### Question 5.3.1.1

Write a prompt using ShellGPT to perform vulnerability scan on [www.certifiedhacker.com](http://www.certifiedhacker.com) website using Nikto vulnerability scanner. Enter the contents of Uncommon header 'host header' found during the vulnerability scan.  
Score

- Check this box to confirm completion of this module.

**Previous<sup>9</sup>Next<sup>10</sup>**

33 Minutes Remaining

Thumbnail screenshot of virtual machineLab52682174-Windows 11

Windows 11

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Admin<sup>12</sup>

Password

Pa\$\$w0rd<sup>13</sup>

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682174-Windows Server 2022

Windows Server 2022

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator<sup>14</sup>

Password

Pa\$\$w0rd<sup>15</sup>

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682174-Windows Server 2019

Windows Server 2019

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Administrator<sup>16</sup>

Password

Pa\$\$w0rd<sup>17</sup>

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

Thumbnail screenshot of virtual machineLab52682174-Parrot Security

Parrot Security

To release mouse, press **Ctrl+Alt+Left Arrow**

Username

Attacker<sup>18</sup>

Password

toor<sup>19</sup>

DVD Drive

- No Media

Ctrl+Alt+Delete [Open in New Window](#)

**Help**

## Support Information

ID

52682174

Host

EU-HV47

Datacenter

EU North (London)

## FAQs

[Frequently asked questions about the lab interface](#)

## Other Help Options

[Submit a Support Request](#)

---

Type Text

Type Text

Type Text

Type Text

Type Text

Type Text

Type Text

Type Text



Powered by [Skillable](#)•[Review Us](#)

## Notifications

## Settings

### Text Size

100 Standard

150 Large Text

200 Extra Large Text

---

### Color Mode

- Light
- Dark
- High Contrast

---

### Actions

[Split Windows](#)

Close Window

Close Window