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**.

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

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

2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

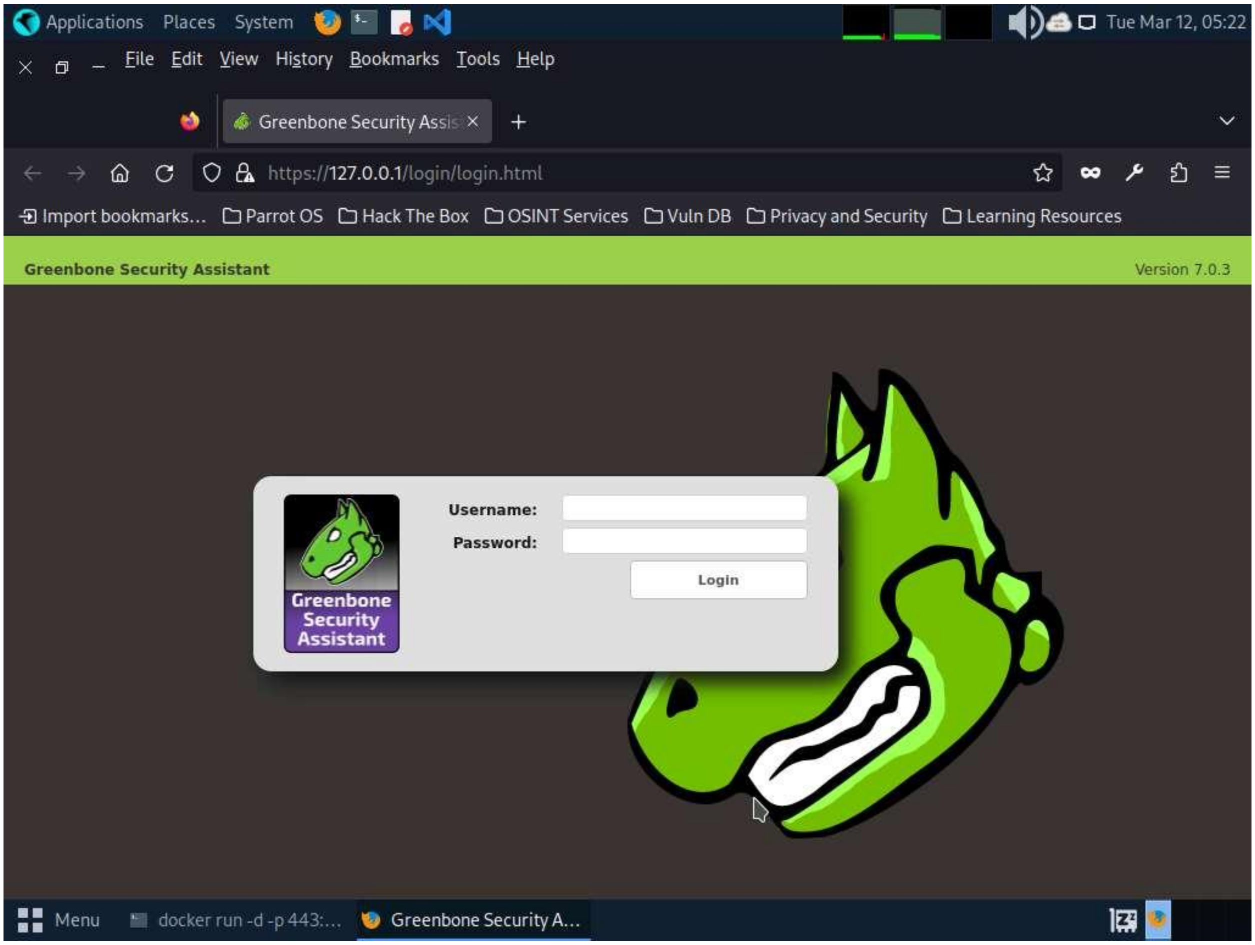
The password that you type will not be visible.

3. Run **docker run -d -p 443:443 –-name openvas mikesplain/openvas** command to launch OpenVAS.

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

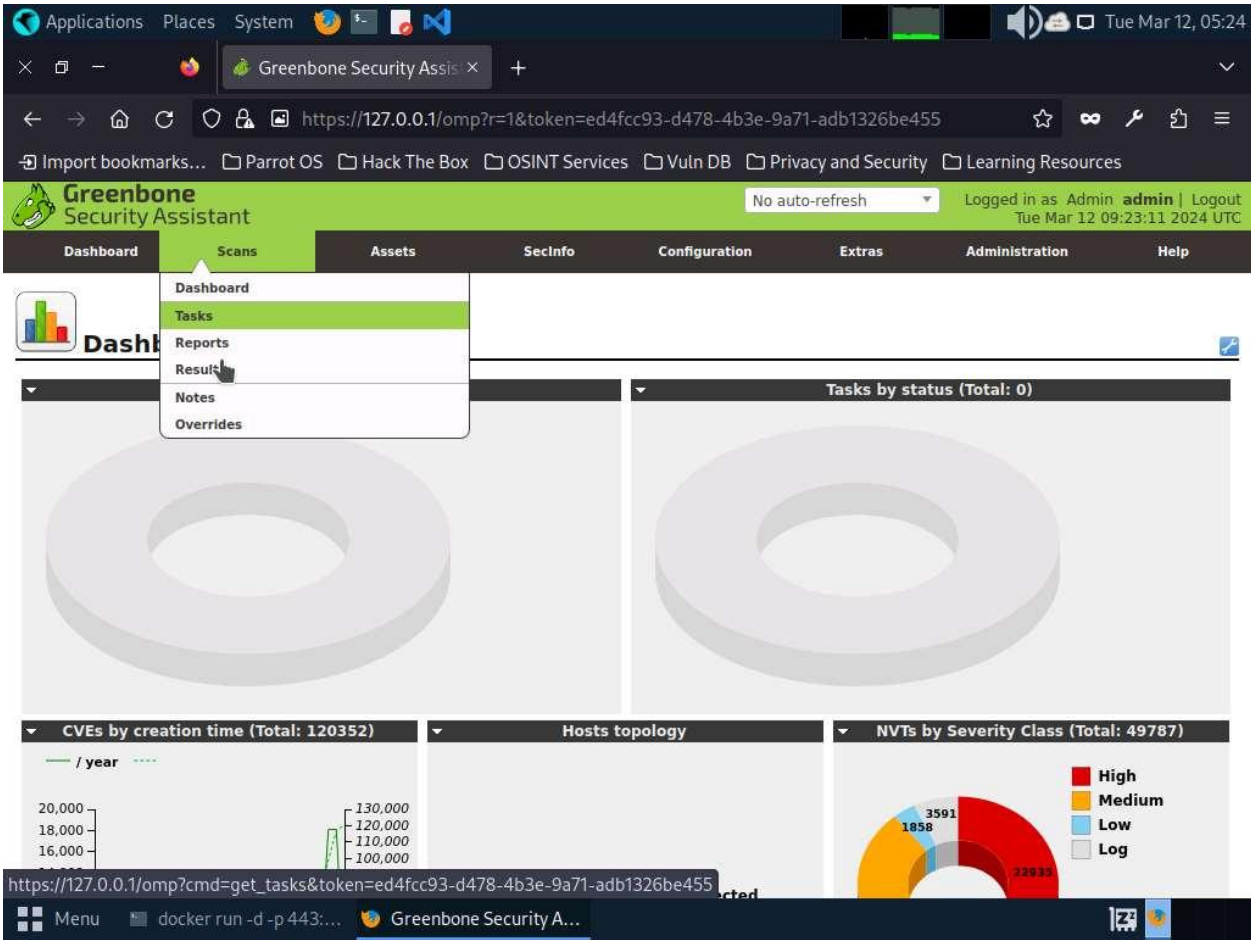
5. The **Firefox** browser appears, go to **https://127.0.0.1/**. OpenVAS login page appears, log in with **admin/admin**.

If a **Warning** page appears, click **Advanced** and select **Accept the Risk and Continue**.

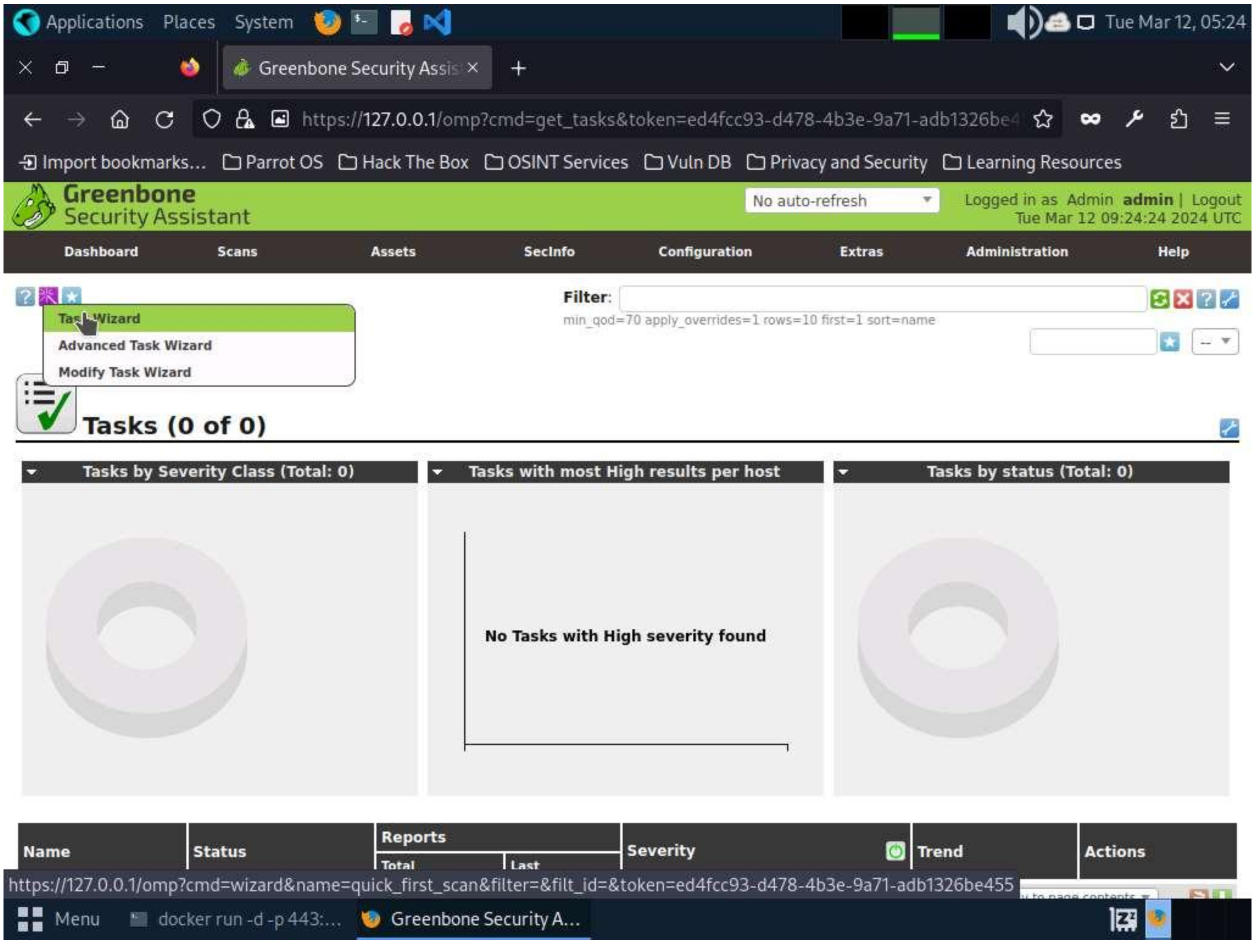


6. The **OpenVAS Dashboards** appears. Navigate to **Scans --> Tasks** from the **Menu** bar.

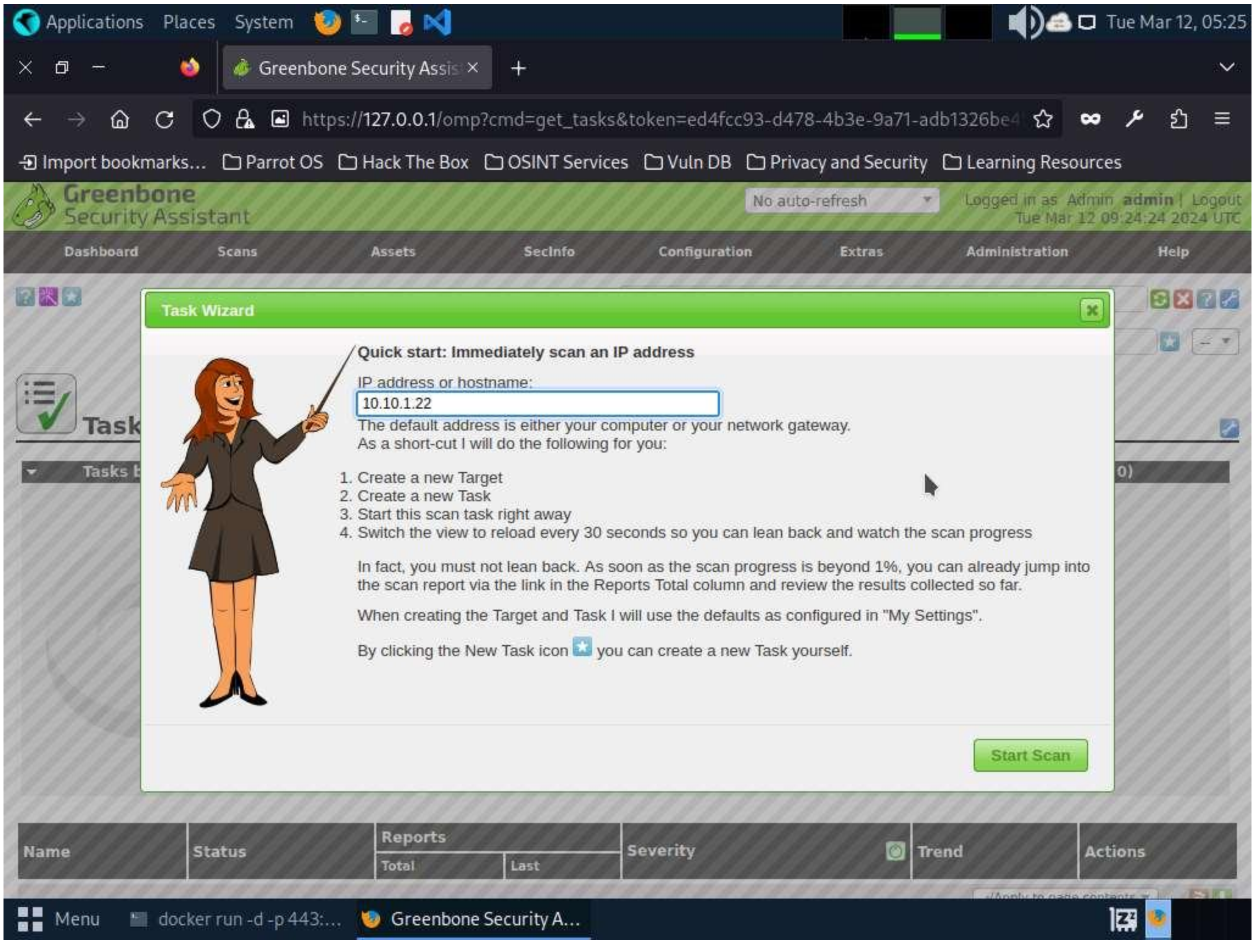
If a **Welcome to the scan task management!** pop-up appears, close it.



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


Applications Places System
Tue Mar 12, 05:24
Greenbone Security Assis
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 Total Last Severity Trend Actions
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:... Greenbone Security A...

8. 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.



Quick start: Immediately scan an IP address

IP address or hostname:

10.10.1.22

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

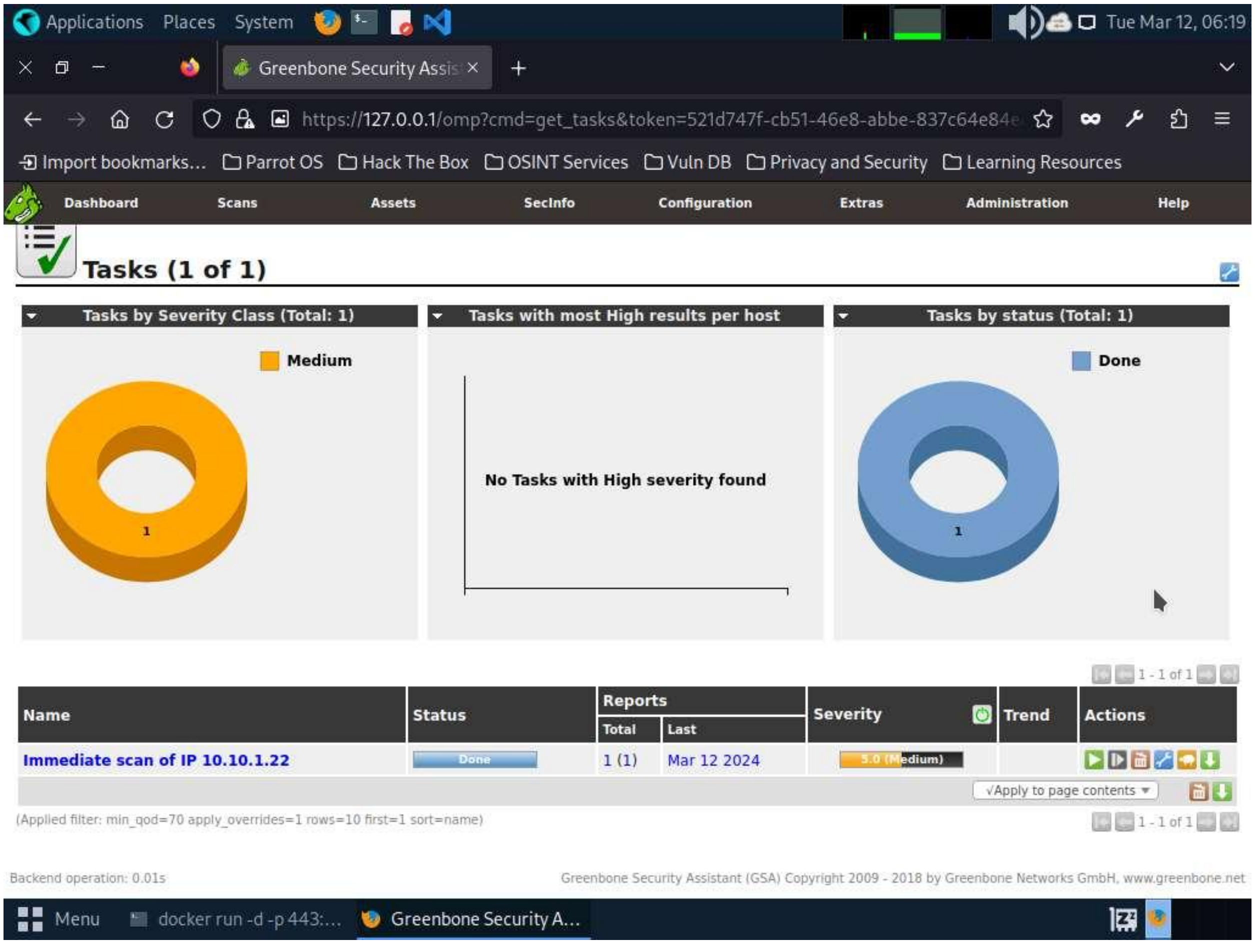
By clicking the New Task icon ★ you can create a new Task yourself.

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

10. 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**/**admin**.



Tasks (1 of 1)

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 10.10.1.22	Done	1 (1)	Mar 12 2024	5.0 (Medium)		

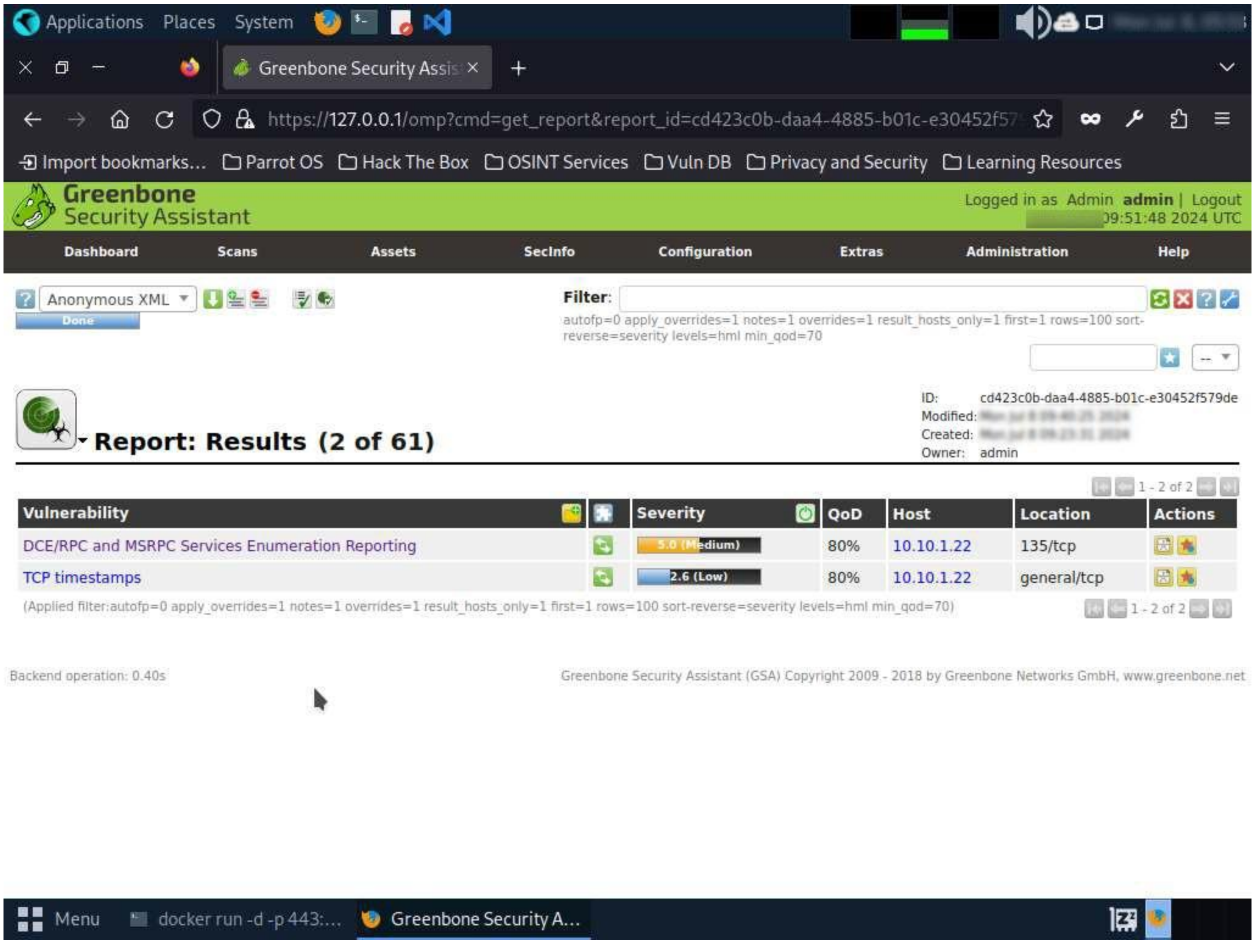
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.01s

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

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

The results might differ when you perform this task.



[redacted] 09:51:48 2024 UTC

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-e30452f579de
Modified: [redacted]
Created: [redacted]
Owner: admin

1 - 2 of 2

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	

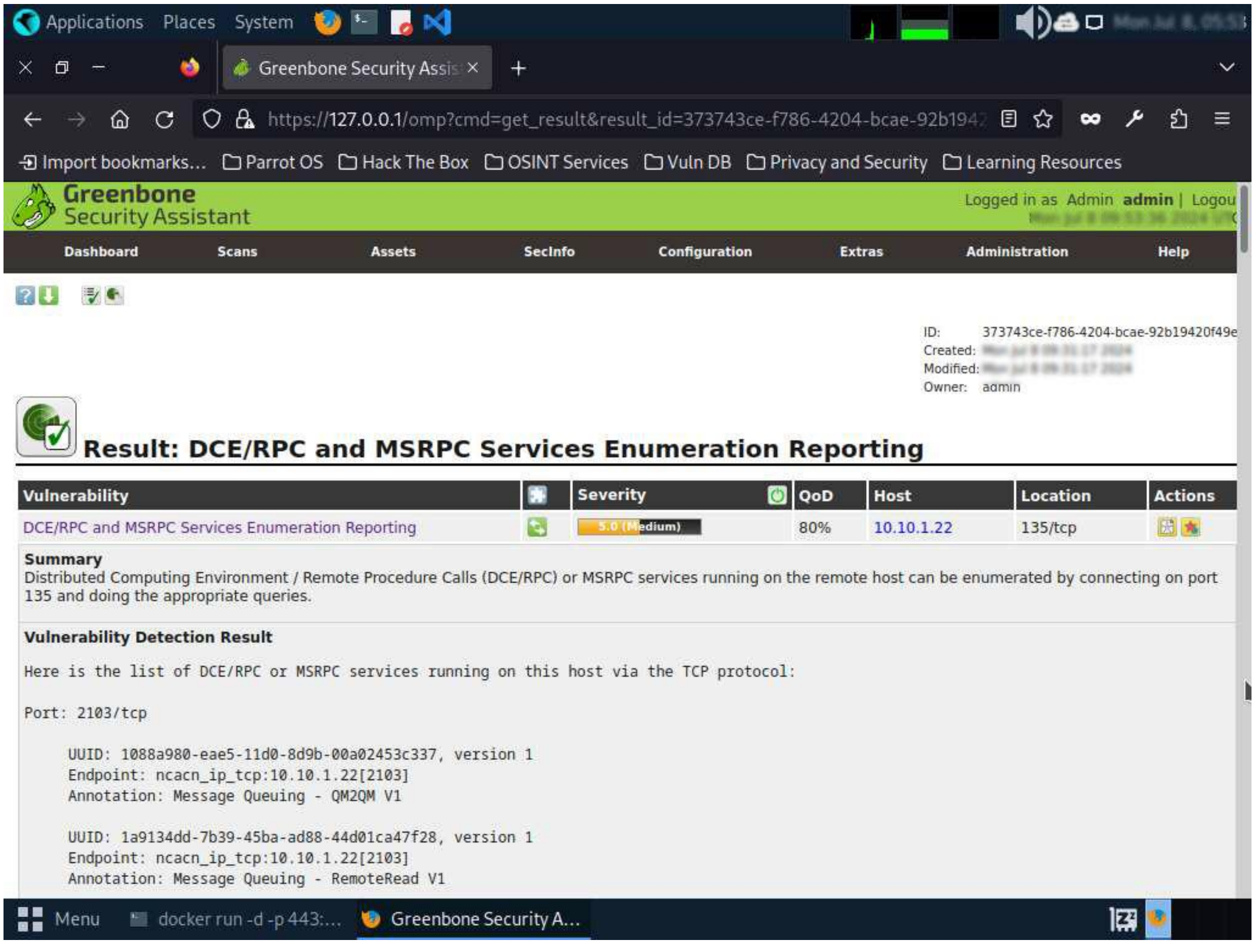
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 2 of 2

Backend operation: 0.40s

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

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

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



[redacted]

ID: 373743ce-f786-4204-bcae-92b19420f49e
Created: [redacted]
Modified: [redacted]
Owner: admin

Result: DCE/RPC and MSRPC Services Enumeration Reporting

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

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
```

14. Similarly, you can check other Reports by hovering over the **Report: Results** section to view other Reports regarding the vulnerabilities in the target system.

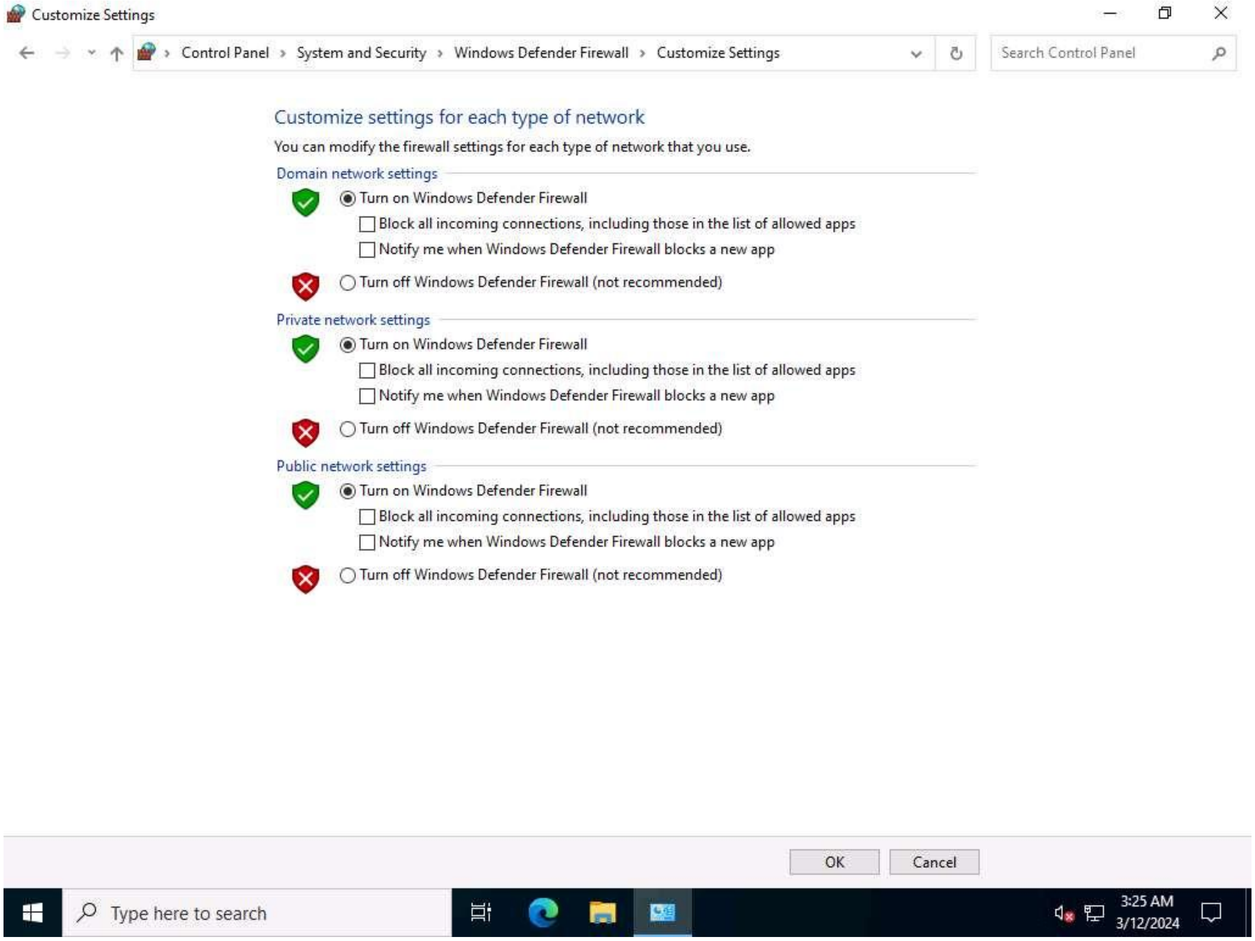
15. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will 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.

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

17. Click on Windows Server 2022 to switch to the **Windows Server 2022** machine and click Ctrl+Alt+Delete and login with **CEH\Administrator** / **Pa$$w0rd**.

18. 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.


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)

19. Click on Parrot Security to switch to **Parrot Security** machine and perform **Steps# 7-9** to create another task for scanning the target system.

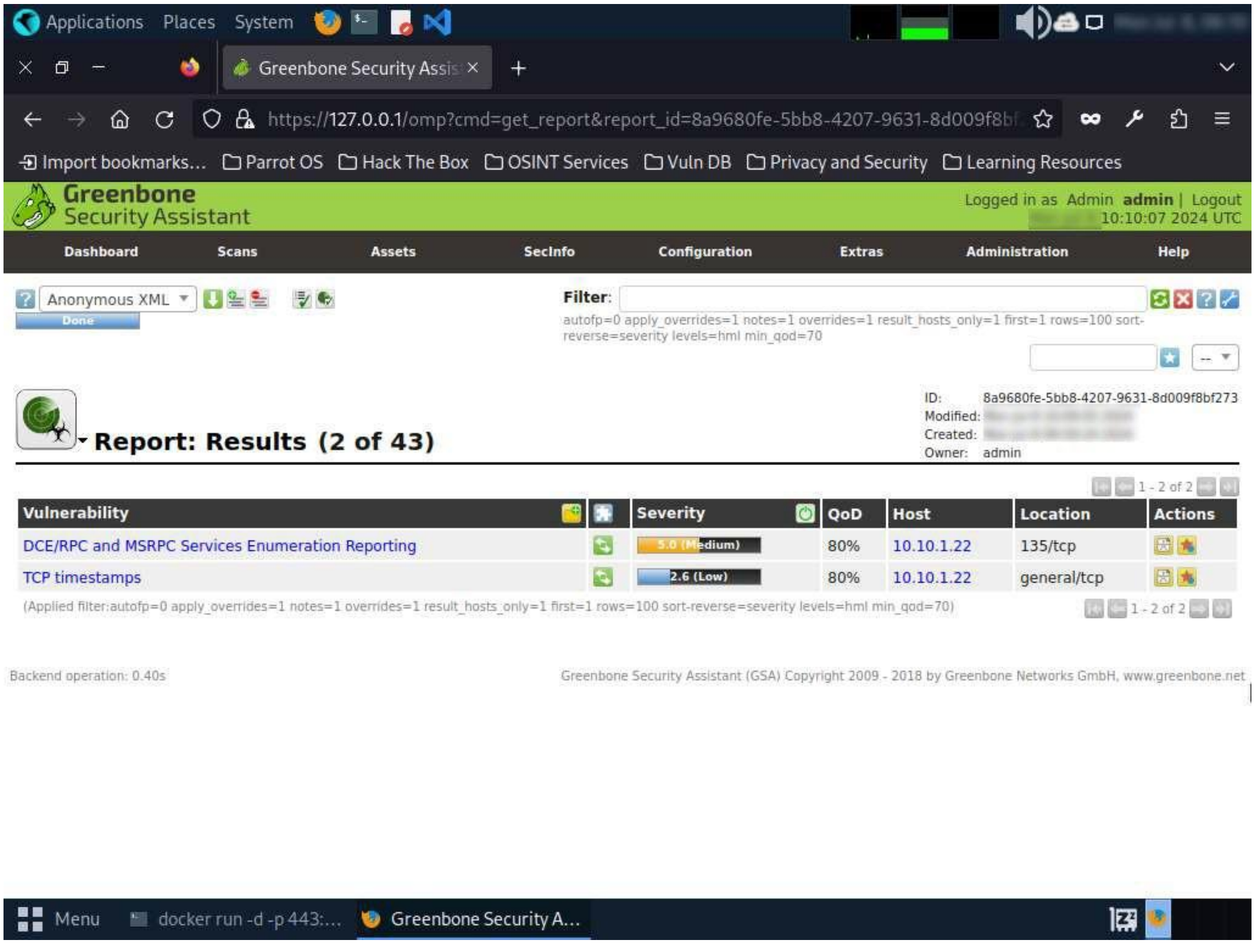
20. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.

21. 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.

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

The results might differ when you perform this task.



Logged in as Admin **admin** | Logout
[redacted] 10:10:07 2024 UTC

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-5bb8-4207-9631-8d009f8bf273
Modified: [redacted]
Created: [redacted]
Owner: admin

1 - 2 of 2

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) 1 - 2 of 2

Backend operation: 0.40s

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

23. 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.

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

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

26. Click on Windows Server 2022 to switch to the **Windows Server 2022** machine and click Ctrl+Alt+Delete login with **Administrator/Pa$$w0rd**.

27. 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.