

Analyzing the Results of a Credentialed Vulnerability Scan

Scenario

In this activity, you will explore the capabilities of the OpenVAS (openvas.org) vulnerability scanner and analyze reports.

Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 1.7 Summarize the techniques used in security assessments.

Lab

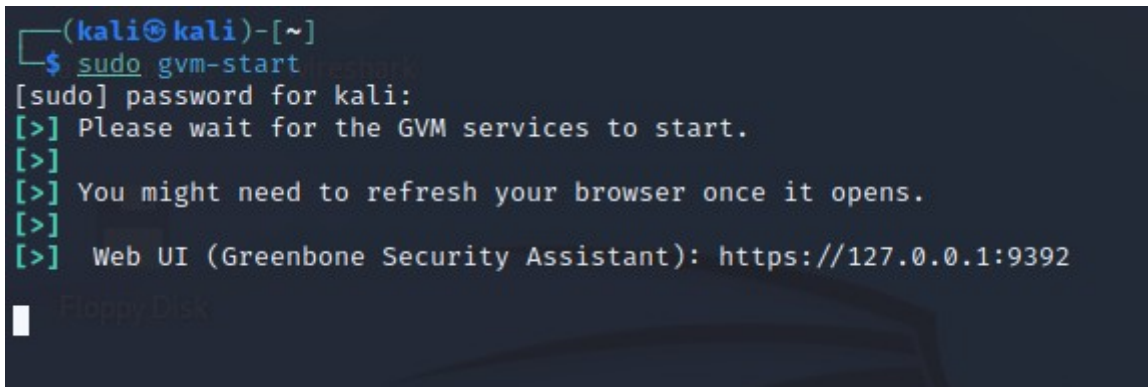
- DC1 VM
- MS1 VM
- Kali VM
- pfSense VM

Task 1

Run OpenVAS scanner

OpenVAS can be managed using a web application called Greenbone Security Assistant. On the Kali VM, start the OpenVAS services and log on via the web application.

1. Connect to the **Kali** VM, and then sign in as **kali** using **Pa\$\$w0rd** as the password.
2. In the menu at the top of the desktop select the **Terminal**.
3. In the terminal window, type **sudo gvm-start** and press **ENTER**. Type the sudo password of **Pa\$Sw0rd**. Wait for the prompt to return.



```
(kali㉿kali)-[~]  
$ sudo gvm-start  
[sudo] password for kali:  
[>] Please wait for the GVM services to start.  
[>]  
[>] You might need to refresh your browser once it opens.  
[>]  
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392  
[>]  
Floppy Disk
```

Figure 1.1 – Starting OpenVAS service.

TIP: It may take one or two minutes for the service to start. You must wait before proceeding to the next steps.

4. The **Firefox** browser automatically launches when the OpenVAS service starts. It connects to **https://127.0.0.1:9392**

NOTE: You might receive a Self-Signed certificate warning from Firefox. Accept it by clicking **Advanced** and **Accept the Risk and Continue** button.

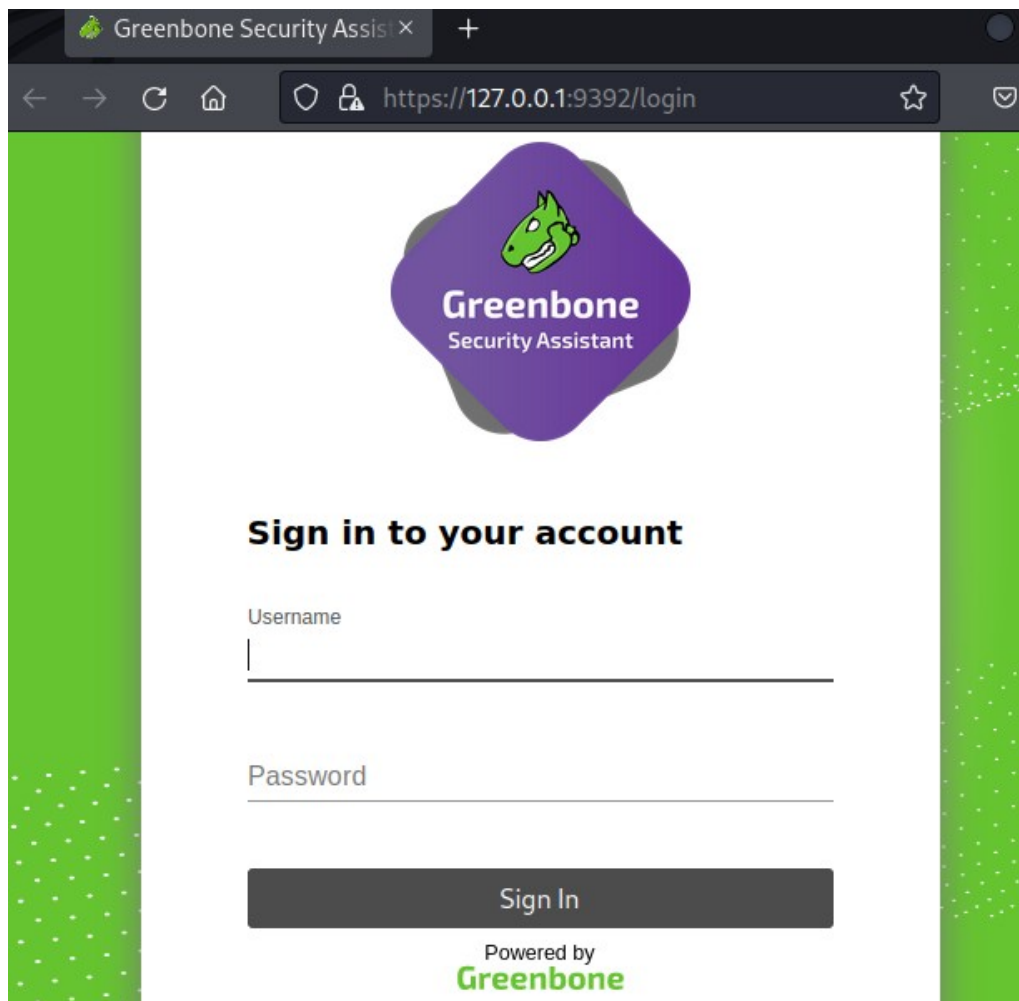


Figure 1.2 – The Greenbone Security Assistant.

5. Log on with the username **admin** and **Pa\$\$w0rd** as the password.

Task 2

Configure credentialed scan

Use credentialed scan to get a detailed report. Use the Configuration menu to configure a new credentials object.

1. From the **Configuration** menu, select **Credentials**.

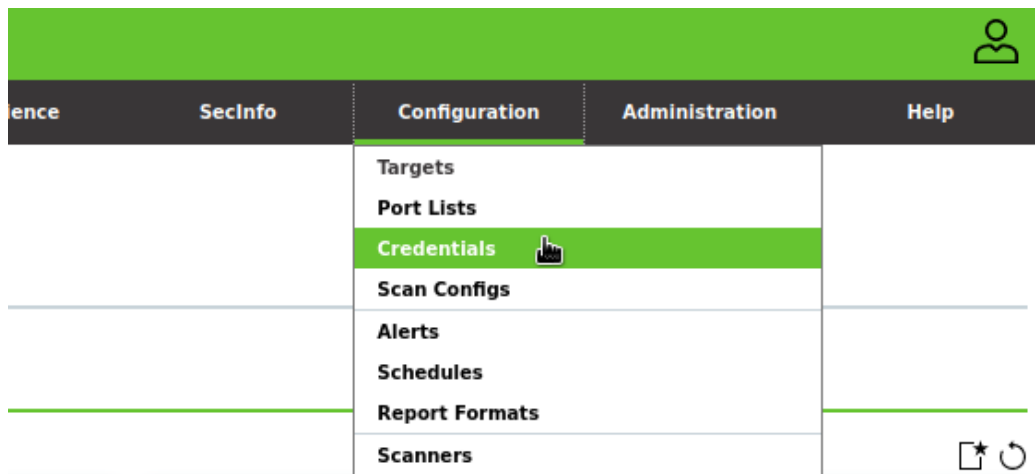


Figure 2.1 – From the Dashboard select Configuration > Credentials.

NOTE: If at any time you receive an error message from Greenbone stating “internal error” with the reference “Could not authenticate to the manager daemon” then retry this step again.

2. Select the **white paper star icon** on the left to open the New Credential web dialog box.

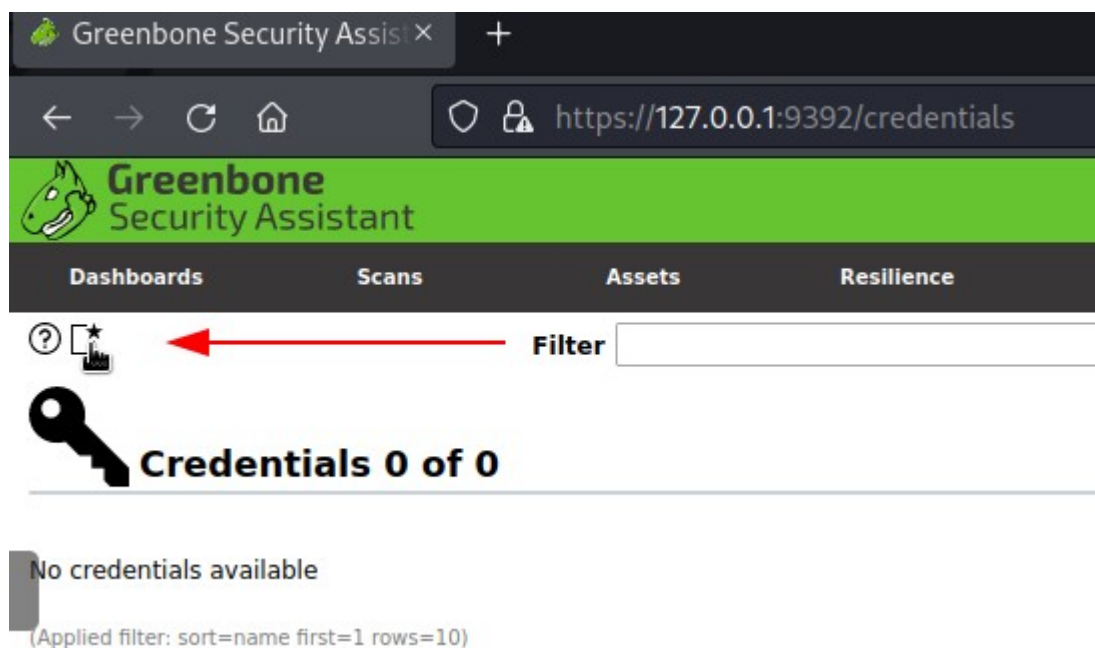


Figure 2.2 – Clicking on the New Credentials icon.

3. Complete the dialog box with the following information:

- Name – Enter **Contoso Support**
- Allow insecure use – Select **Yes**
- Username – **CONTOSO\Administrator**
- Password – **Pa\$\$w0rd**

New Credential

Name

Comment

Type

Allow insecure use ☒ Yes ☐ No

Auto-generate ☐ Yes ☒ No

Username

Password

Figure 2.3 – Contoso Support Administrator Credentials.

NOTE: Vulnerability scans should not use administrative privileges such as the Domain Administrator account used in this activity. Credentialed scans use dedicated logon accounts that have audit or read-only privileges.

4. Select **Save**.

Task 3

Configure scan target

The scan scope is the range of hosts or IP addresses that will be assessed. Create a task to scan Windows servers.

1. From the **Configuration** menu, select **Targets**.

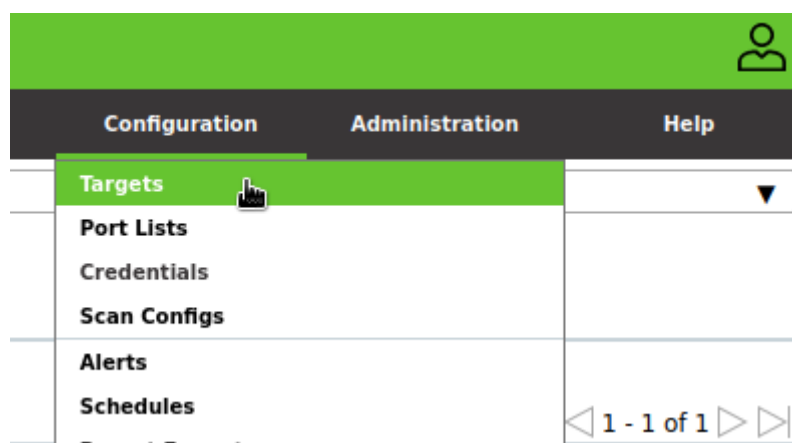


Figure 3.1 – Select Configuration > Targets.

2. Select the **white paper star icon** on the left to open the **New Target** web dialog box.

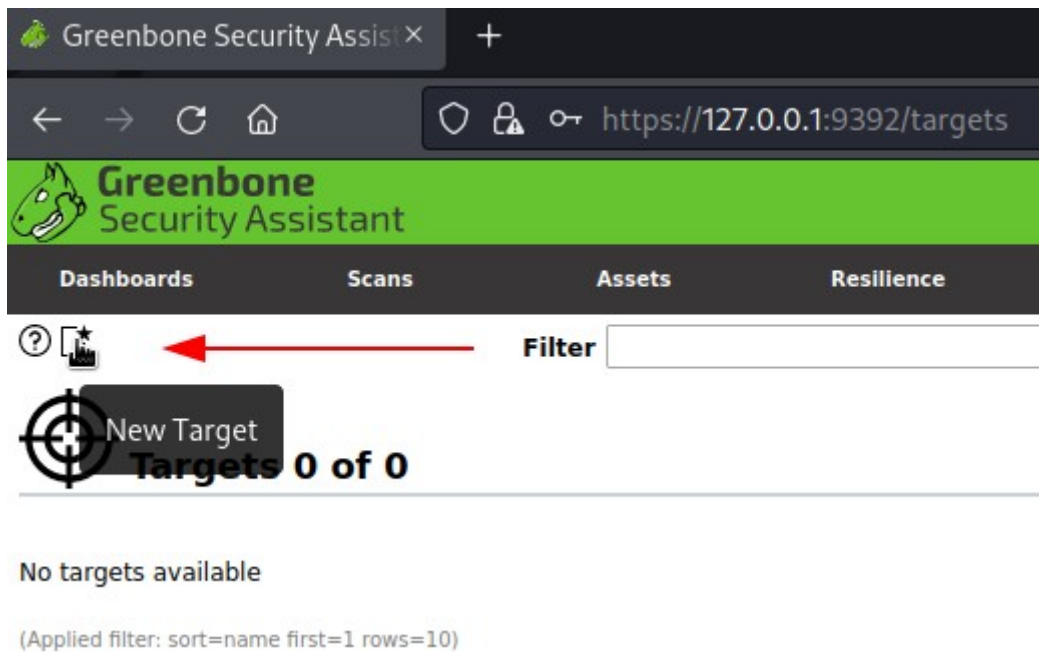


Figure 3.2 – The New Target configuration option.

3. Complete the dialog box with the following information:

- Name – enter **Windows Servers**
- Hosts – select **Manual** and enter **192.168.1.1-192.168.1.2** in the box
- Credentials – from the **SMB** drop-down list box, select **Contoso Support**

New Target

Name

Comment

Hosts ☒ Manual
☐ From file No file selected.

Exclude Hosts ☒ Manual
☐ From file No file selected.

Allow simultaneous scanning via multiple IPs ☒ Yes ☐ No

Port List

Alive Test

Credentials for authenticated checks

SSH on port

SMB

Figure 3.3 – Configuring the Target of the scan.

4. Select **Save**.

Task 4

Configure scan schedule

Configure scan to run on a set schedule.

1. From the **Configuration** menu, select **Schedules**.

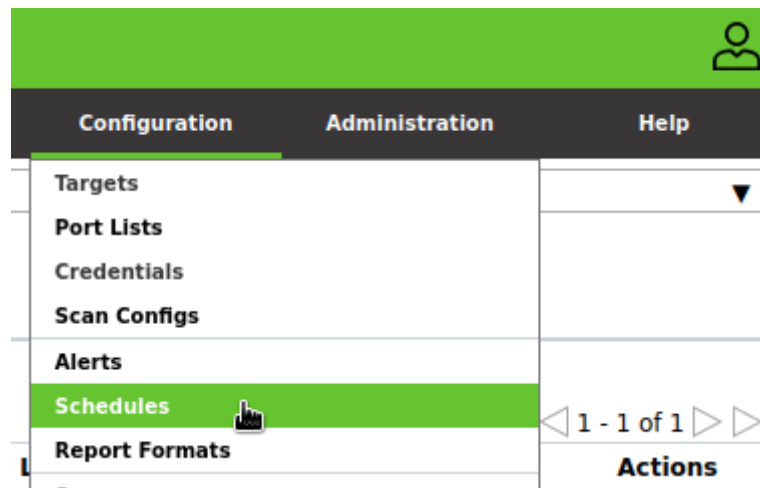


Figure 4.1 – Selecting Schedule configuration from the menu.

2. Select the **white paper with a star** icon on the left to open the **New Schedule** web dialog box.

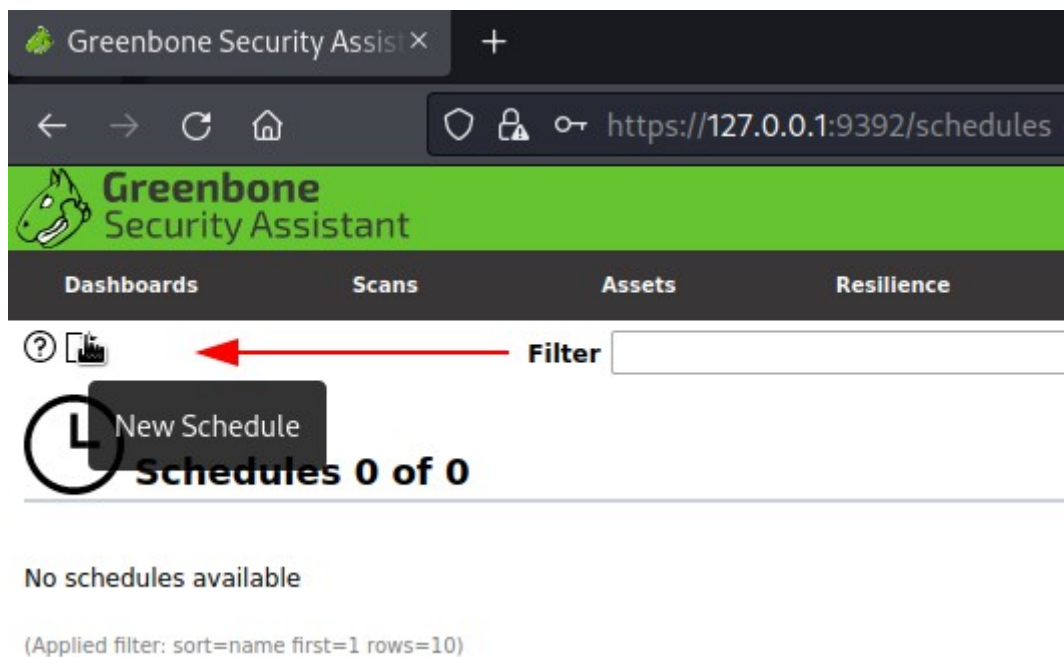


Figure 4.2 – Selecting to create a New Schedule.

3. Complete the dialog box with the following information:

- Name – enter **Contoso Daily Scan**
- First Time – set to 1
- Duration – **Entire Operation**
- Recurrence - **Once**

New Schedule
✕

Name

Comment

Timezone Coordinated Universal Time/UTC ▼

First Run 07/31/2022 ⋮ ▲▼ h ▲▼ m Now

Run Until 07/31/2022 ⋮ ▲▼ h ▲▼ m ☒ Open End

Duration Entire Operation

Recurrence Once ▼

Cancel
Save

Figure 4.3 – Configuring a schedule for scans to run.

4. Select **Save**.

NOTE: Vulnerability scanning can be disruptive so it is more typical to schedule it out-of-office hours. On a production network you may also need some mechanism of powering on computers remotely. Also, consider your timezone.

Task 5

Configure scan task

Create a task object to complete the configuration, and then run the scan task.

1. From the **Scans** menu, select **Tasks**.

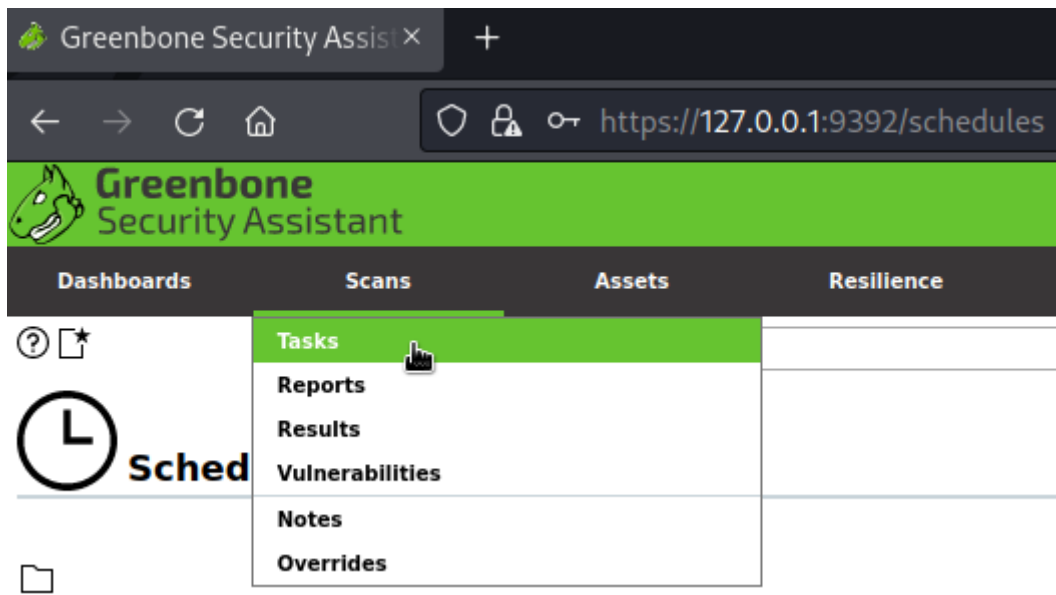


Figure 5.1 – Selecting Scans > Tasks from the menu.

2. Select the **white paper star icon** on the left to open the **New Task** web dialog box.

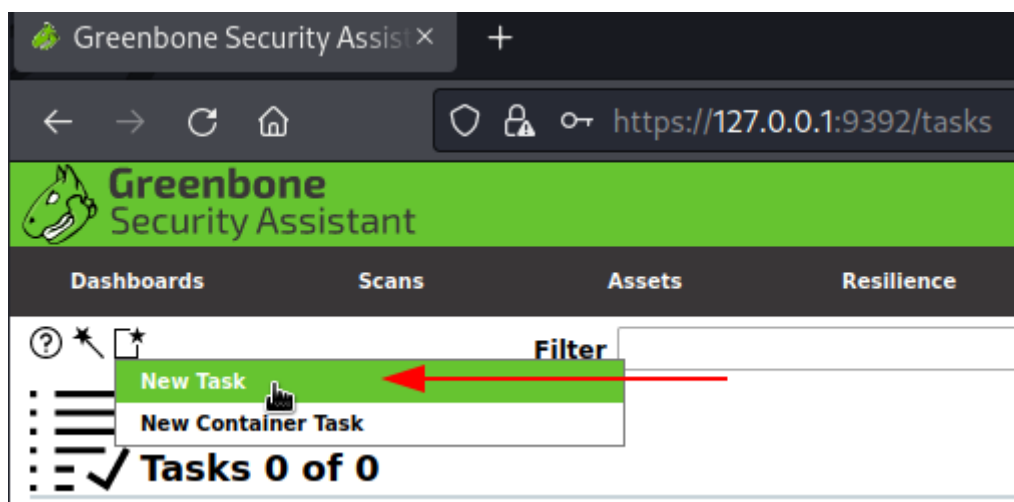


Figure 5.2 – Selecting a New Task.

3. Complete the dialog box with the following information.

- Name – enter **Contoso Full and fast**
- Scan Targets – **Windows Servers**
- Schedule – **Contoso Daily Scan**

New Task

Name Contoso Full and fast

Comment

Scan Targets Windows Servers

Alerts

Schedule Contoso Daily Scan ☐ Once

Add results to Assets ☒ Yes ☐ No

Apply Overrides ☒ Yes ☐ No

Min QoD 70 %

Alterable Task ☐ Yes ☒ No

Auto Delete Reports ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 reports

Scanner OpenVAS Default

Scan Config Full and fast

Network Source Interface

Order for target hosts Sequential

Maximum concurrently executed 1

Cancel **Save**

Figure 5.3 – Configuring the Task in the New Task dialog box.

4. Select **Save**.

You will run the scan manually to ensure that it works as expected.

5. Under Name at the bottom of the screen, select the **Contoso Full and Fast** task.

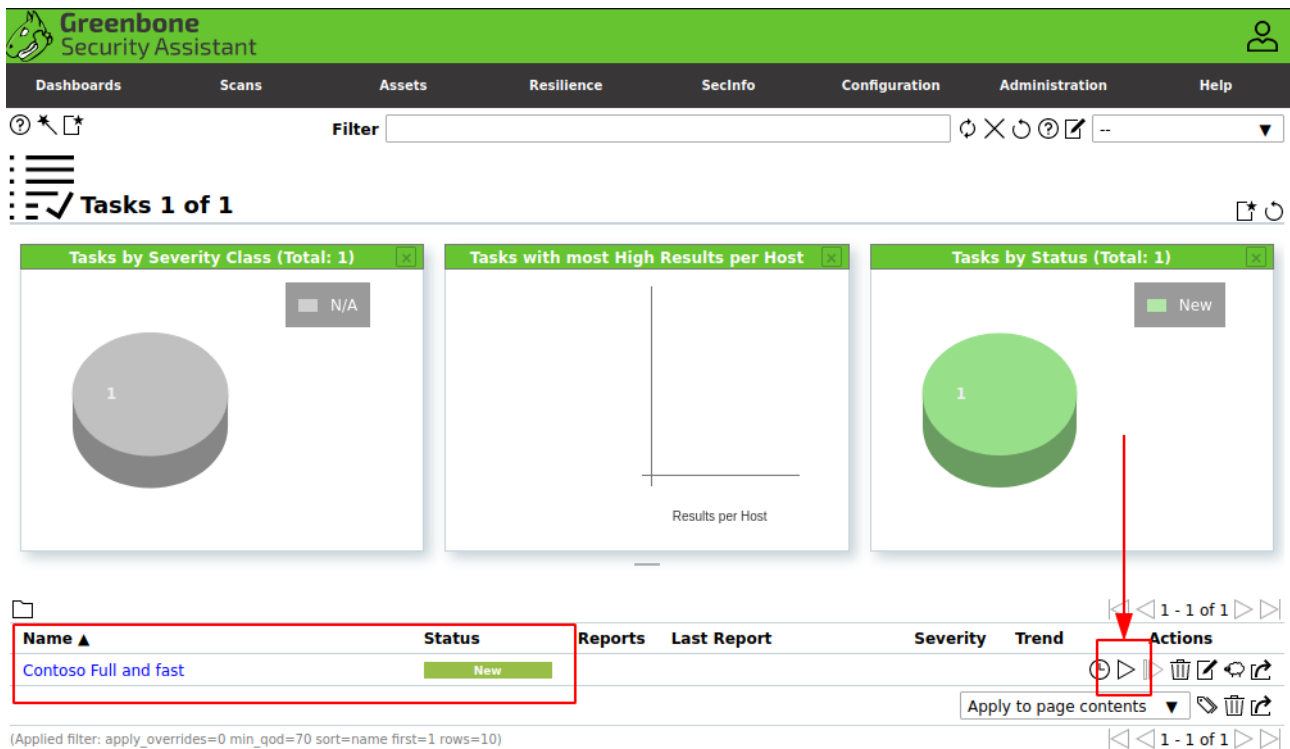


Figure 5.4 – Selecting the New task.

6. Select the **Play** arrow button to **Start** the scan manually.

Task 6

Browse OpenVAS scan report

Now that you have begun a scan, you need to let it run for a three to five minutes. You can open the report results, even if the scan is not complete.

1. Let the scan to execute while you complete the next steps.
2. In the Greenbone web app, select the **Dashboard** link to display current information.

Let it run for **three-five minutes** to begin **generating report entries**.

TIP: Optionally, you may take a few minutes to browse the default scan configurations (select **Configuration** > **Scan Configs**). The scan configuration determines the type of tests and probes that are run. Running more detailed tests take longer, and can carry more risk of crashing the target host.

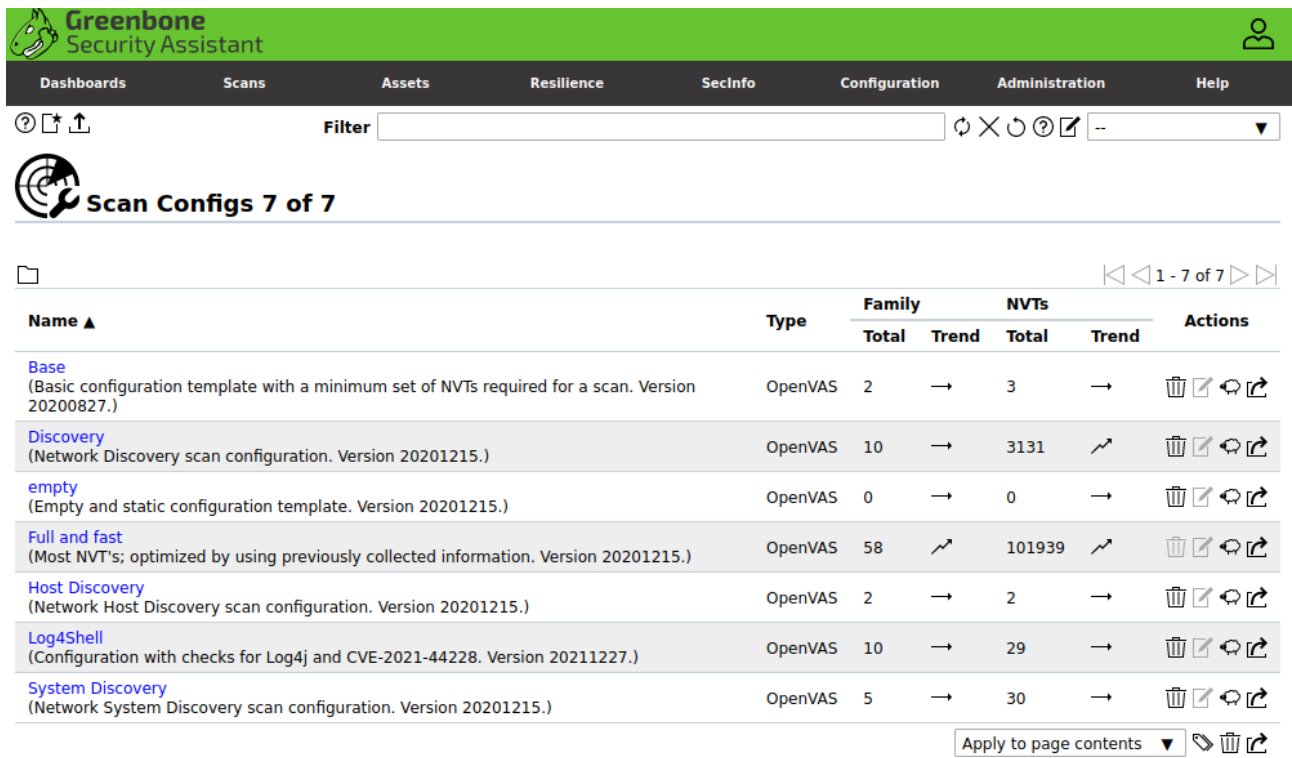


Figure 6.1 – OpenVAS Scan Configs.

3. Select Scans > Reports.

You can use this screen to monitor the status of tasks and preview scan results even if the task is not complete.

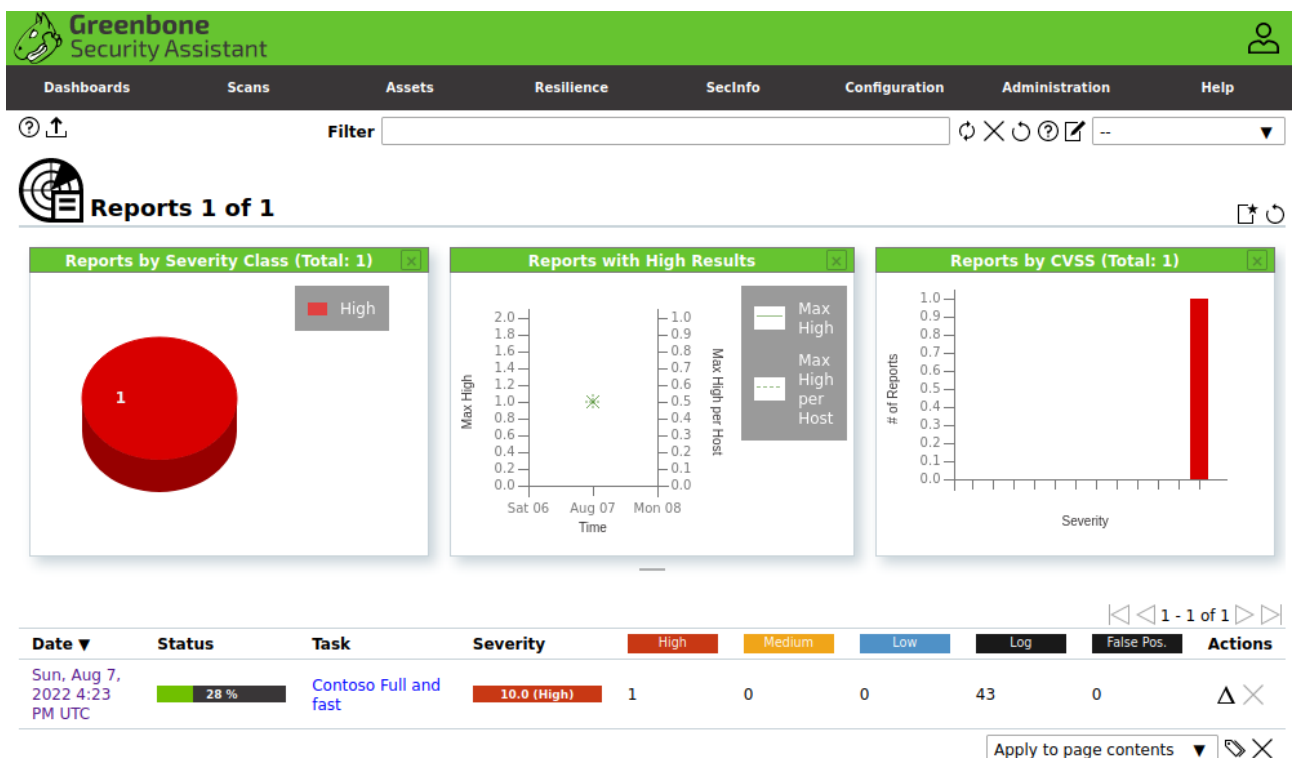


Figure 6.2 – Scan Report windows showing a status of 28% and 1 High Severity.

4. In the **Date** column at the bottom of the Reports page, select the task with today's date to view the results.

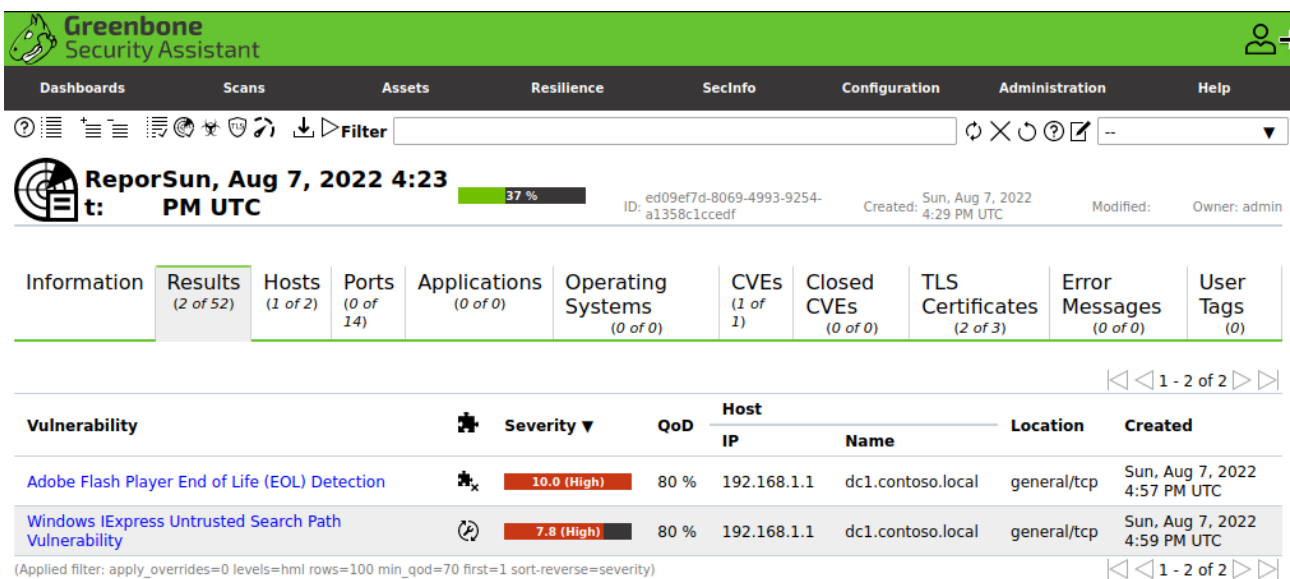


Figure 6.3 – Scan Report in OpenVAS showing the current results while running.

NOTE: If there are no entries in the report yet, wait for a few more minutes. The scan results need to show at least one entry in either High, Medium, or Low Scan Results.

TIP: Refresh the scan's results regularly.

5. Browse the report, and specifically observe the CVEs entries.

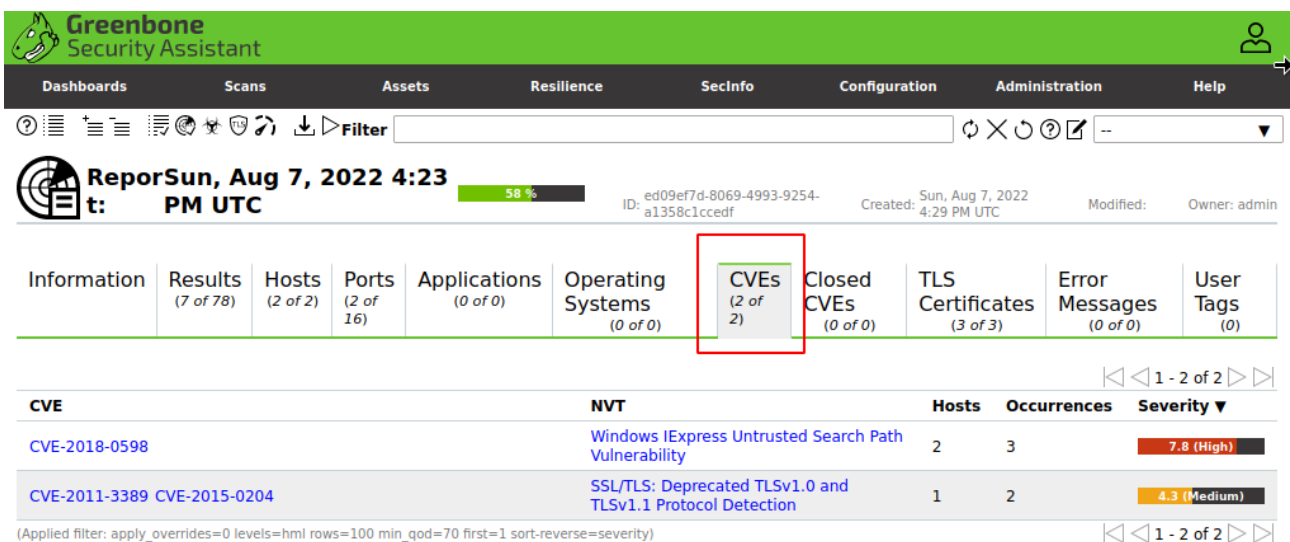


Figure 6.4 – Report CVEs from the current running task.

6. From the tab menu by the **Results** tab, choose **Hosts** to display the discovered hosts and their related vulnerability information.

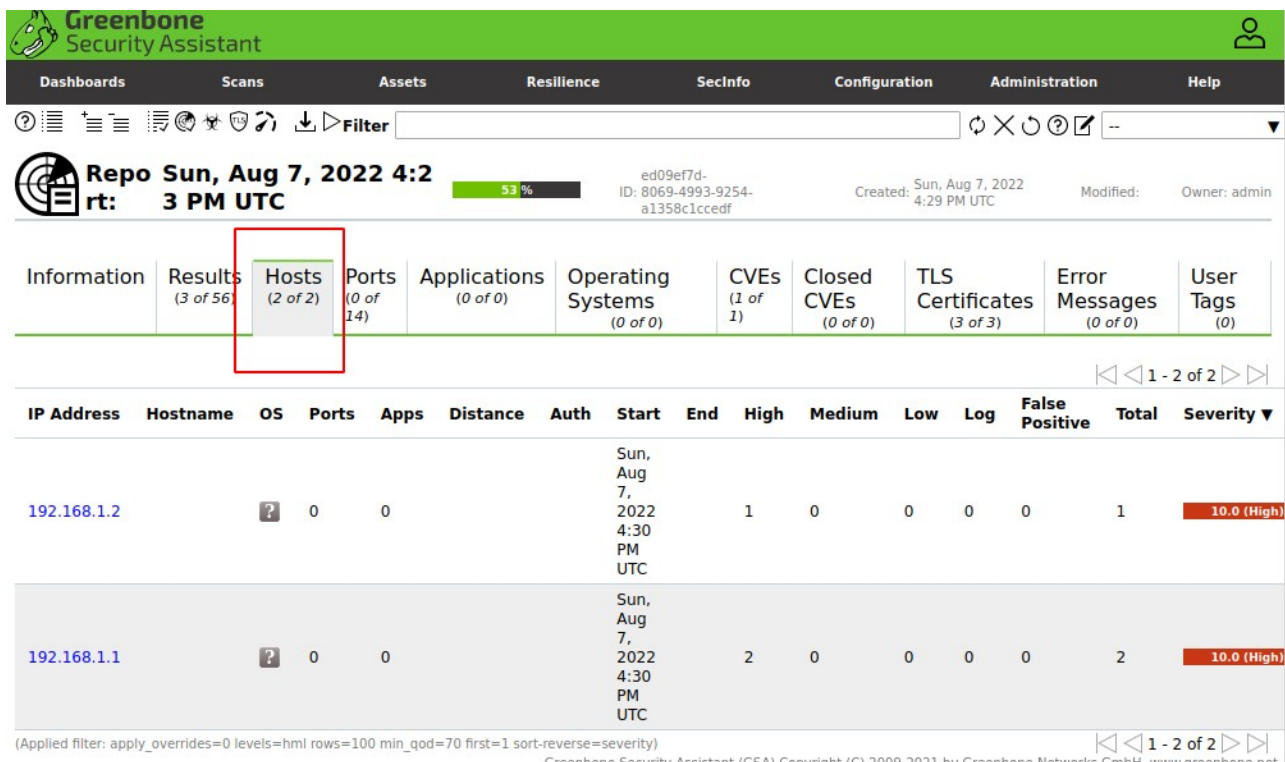


Figure 6.5 – OpenVAS report hosts form the current running task.

Observe that the same hosts you discovered using scanning tools in previous labs were also detected in this activity.

Optionally wait for the scan to complete and Save the scan results as a compliance check report for use as part of the security audit.

NOTE: Waiting for the scan to complete might take 30 minutes.

7. In the pull-down menu at the upper part of the page, select **PDF** (the menu current reads **Anonymous XML**), and then select **OK** button.

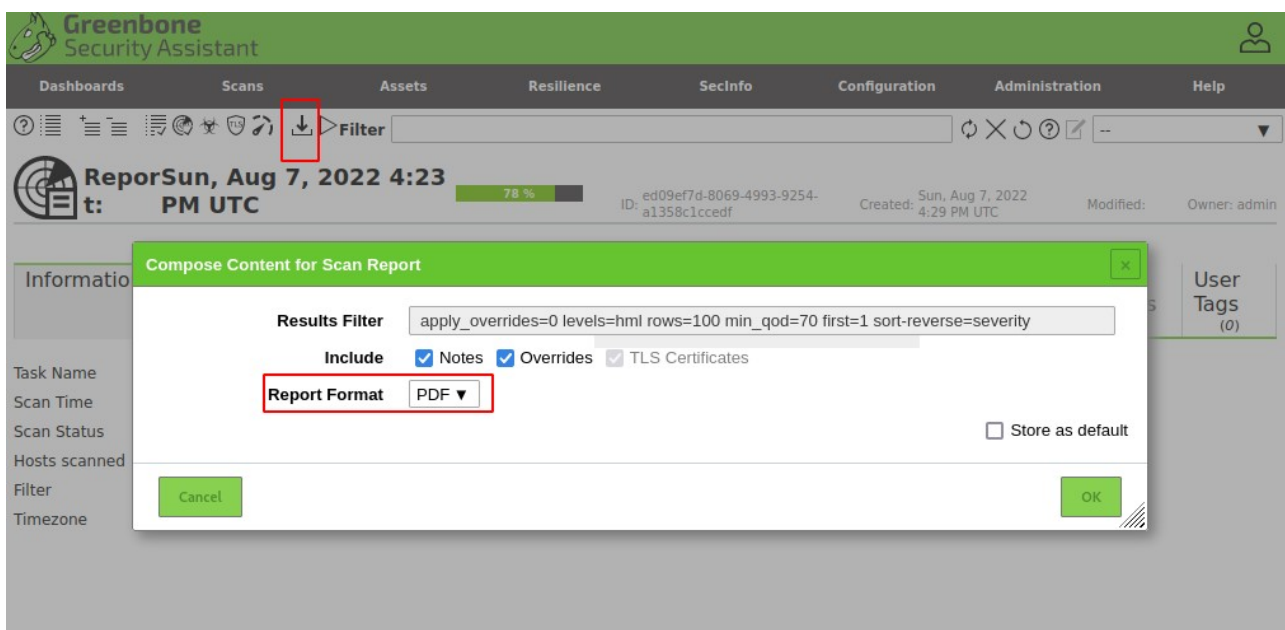


Figure 6.6 – Downloading a Scan Report.

8. When prompted, select **Save File** to download the report to the default **Downloads** folder.

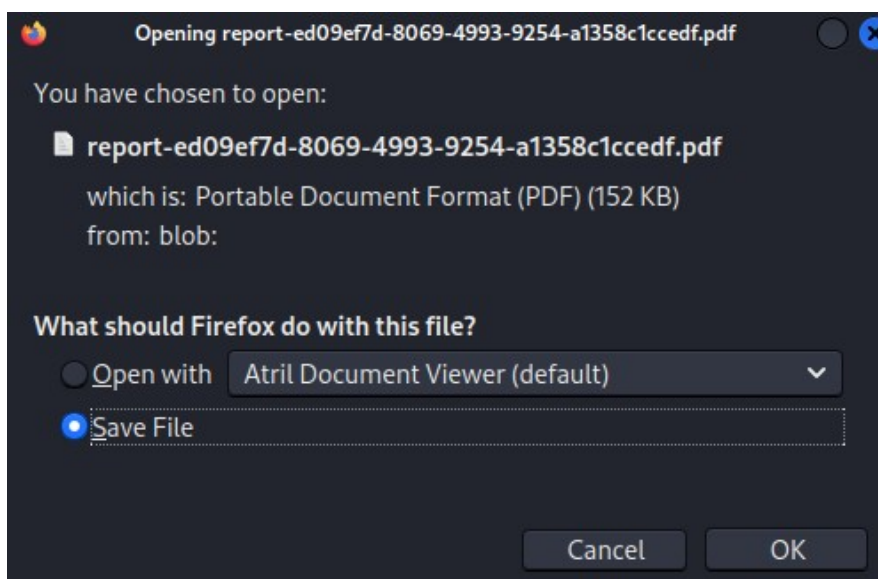


Figure 6.7 – Saving the PDF Report.

9. Confirm the PDF report file exists by viewing it.

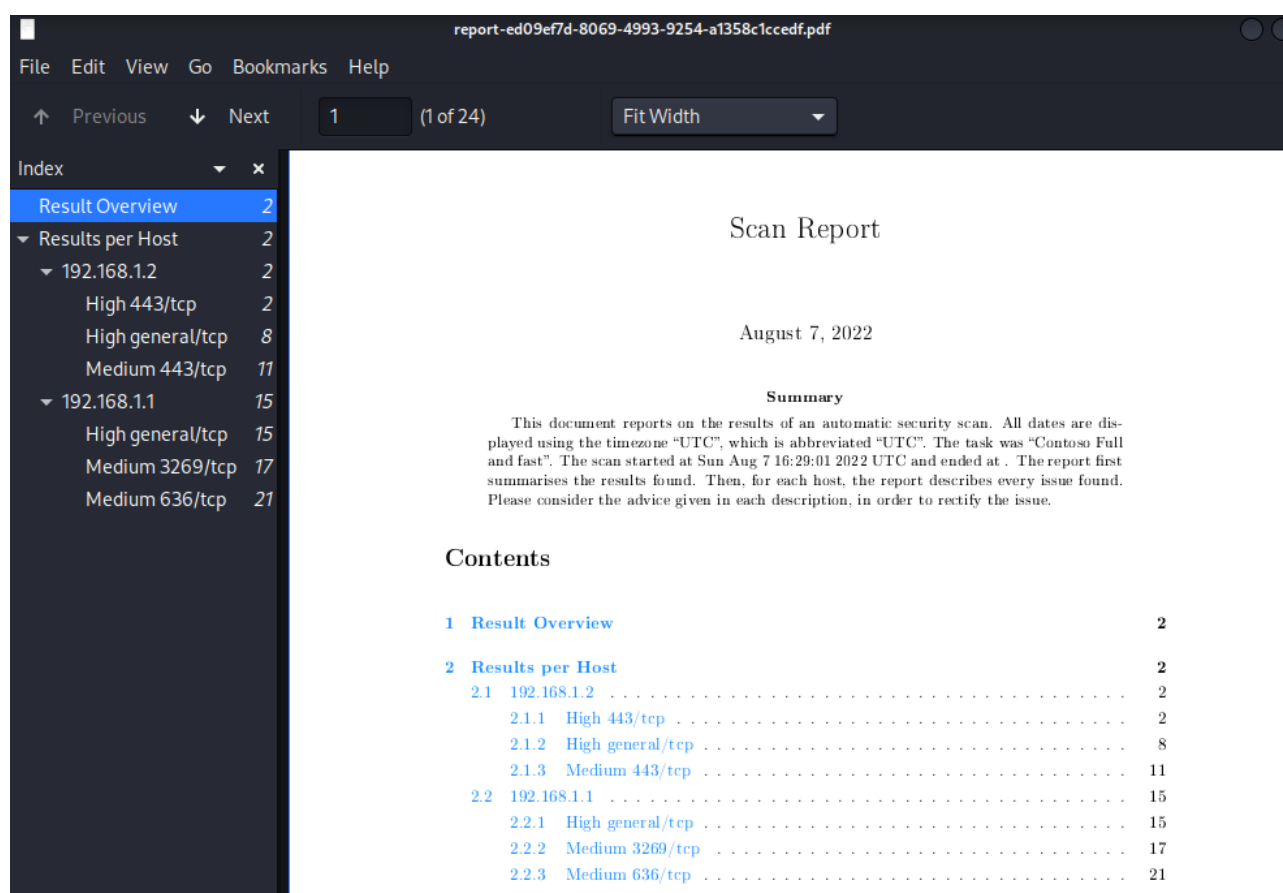


Figure 6.8 – Viewing the OpenVAS PDF Report.