Network Penetration Testing Methodology-Internal

6 Hr 37 Min Remaining

Instructions Resources Help  100%

Exercise 16: Vulnerability Analysis with OpenVAS

Scenario

While it is debatable how much a vulnerability scanner can do for a professional security tester, it is an important tool for helping us gather data and identify known vulnerabilities. When doing a penetration test we use a vulnerability scanner to provide us with a quick look at the state of the machines we are building in our target database.  
The objective of this lab is to help students learn how to:

* Perform Vulnerability Assessment with the OpenVAS tool
* Analyze the output of the scan
* Add information to the target database

**Lab Duration**: **25** Minutes

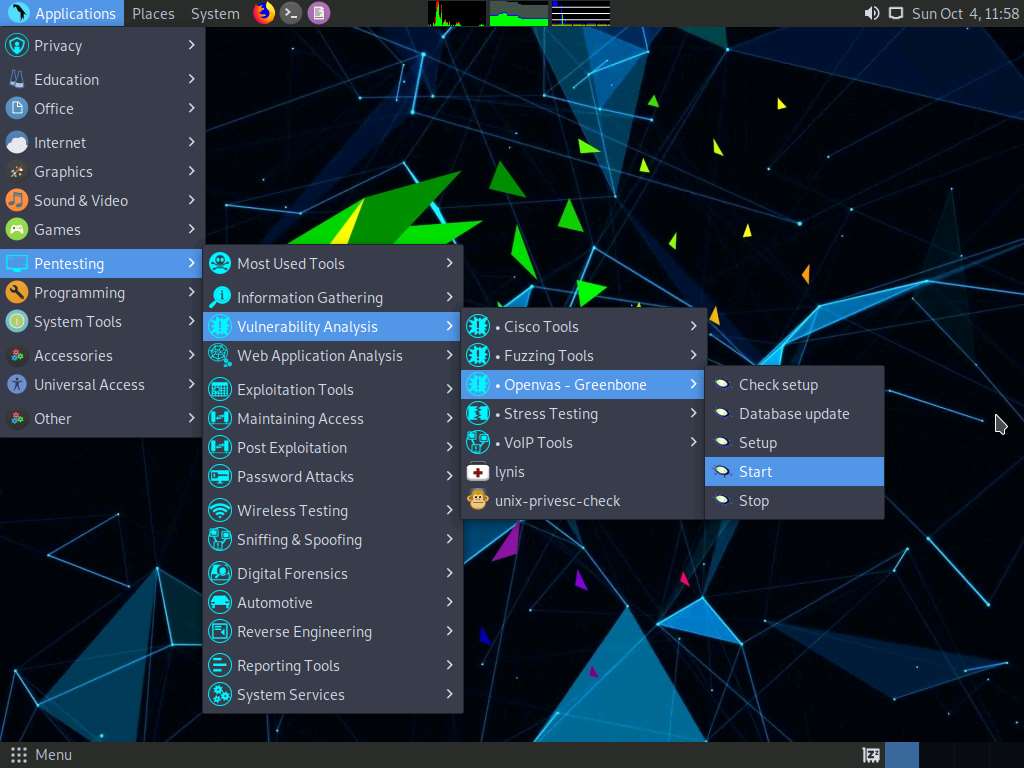
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



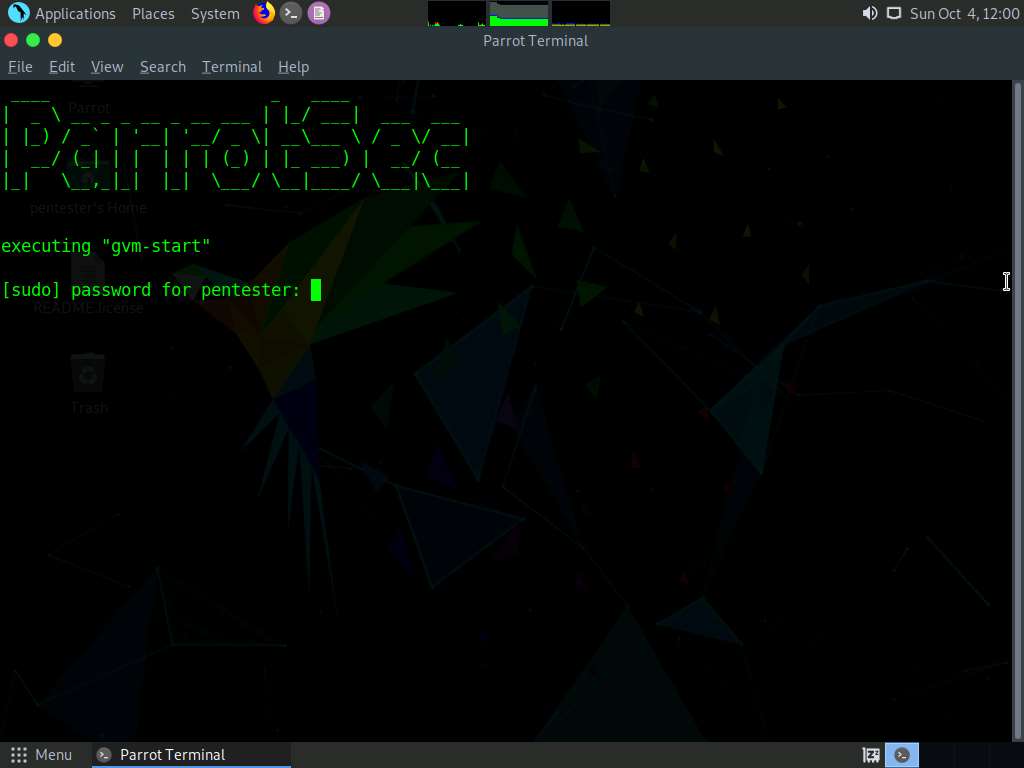
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. Navigate to **Applications** --> **Pentesting** --> **Vulnerability Analysis** --> **OpenVAS - Greenbone** --> **Start**. In this lab, we are going to perform a vulnerability assessment on **172.19.19.15** (Advertisement Dept. machine), which was discovered during ping sweep scan in the previous exercise.

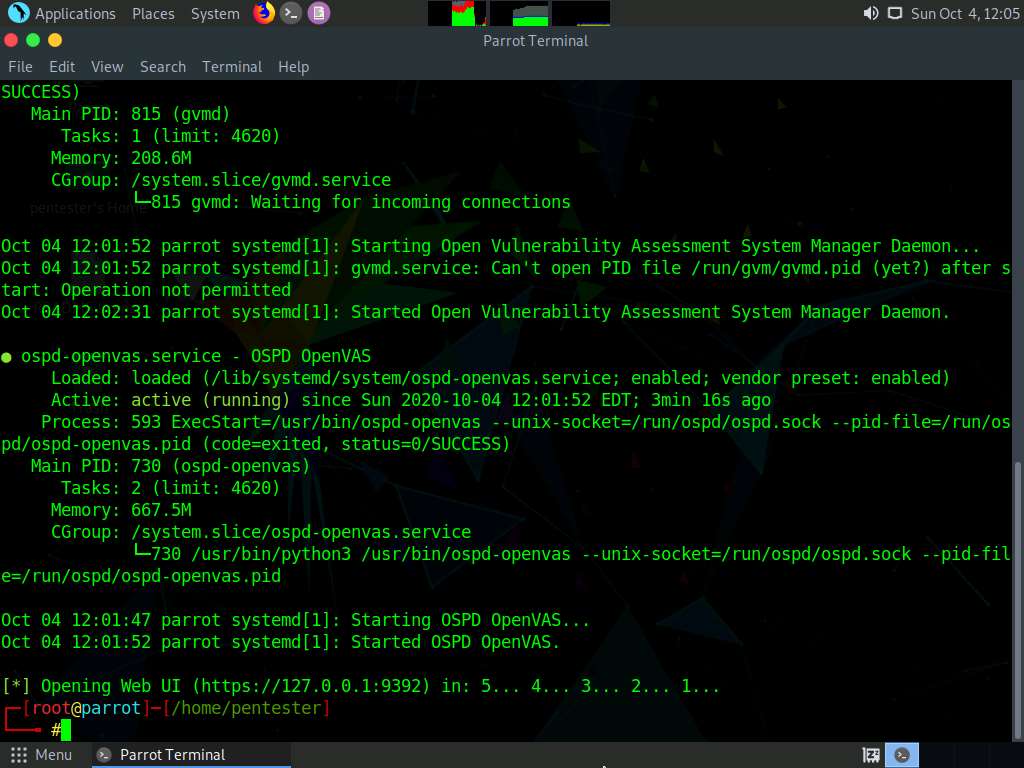


1. You will be prompted to enter password. Enter **toor**.

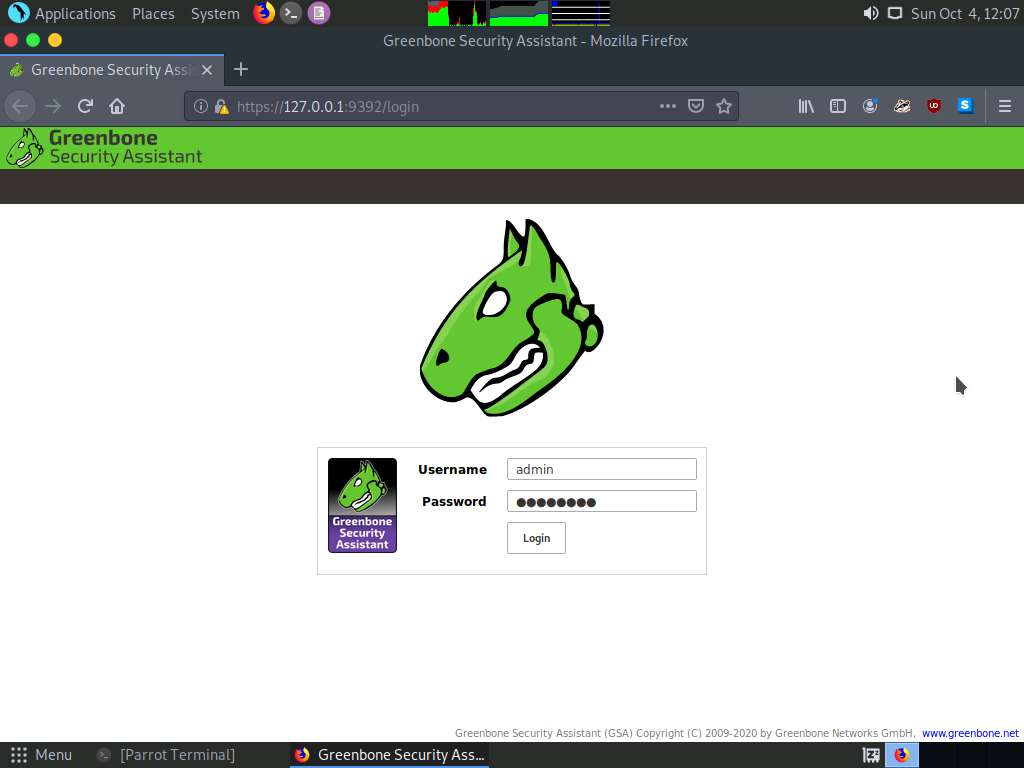


1. Wait until all the services are started. Minimize the command terminal window.

It takes some time for the OpenVas Scanner to start. Ignore any errors returned by OpenVAS Security Manager.

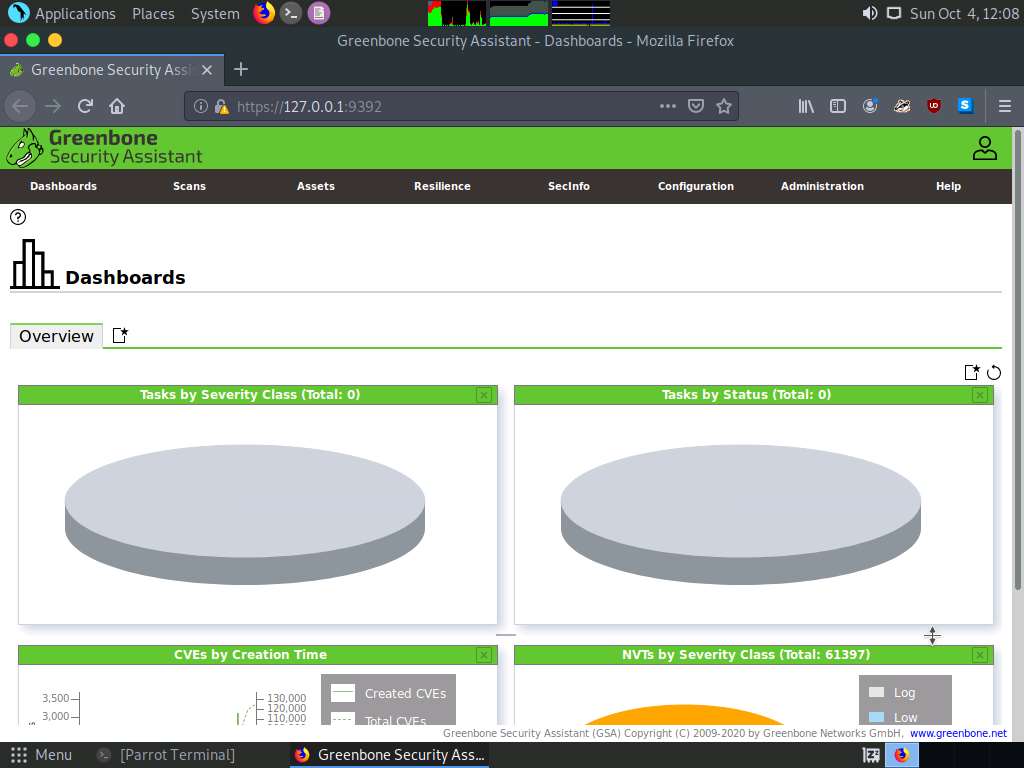


1. Launch Firefox web browser and browser the URL **https:/127.0.0.1:9392**. OpenVAS web GUI login page appears; enter the following credentials and click **Login**:  
   Username: **admin**  
   Password: **password**

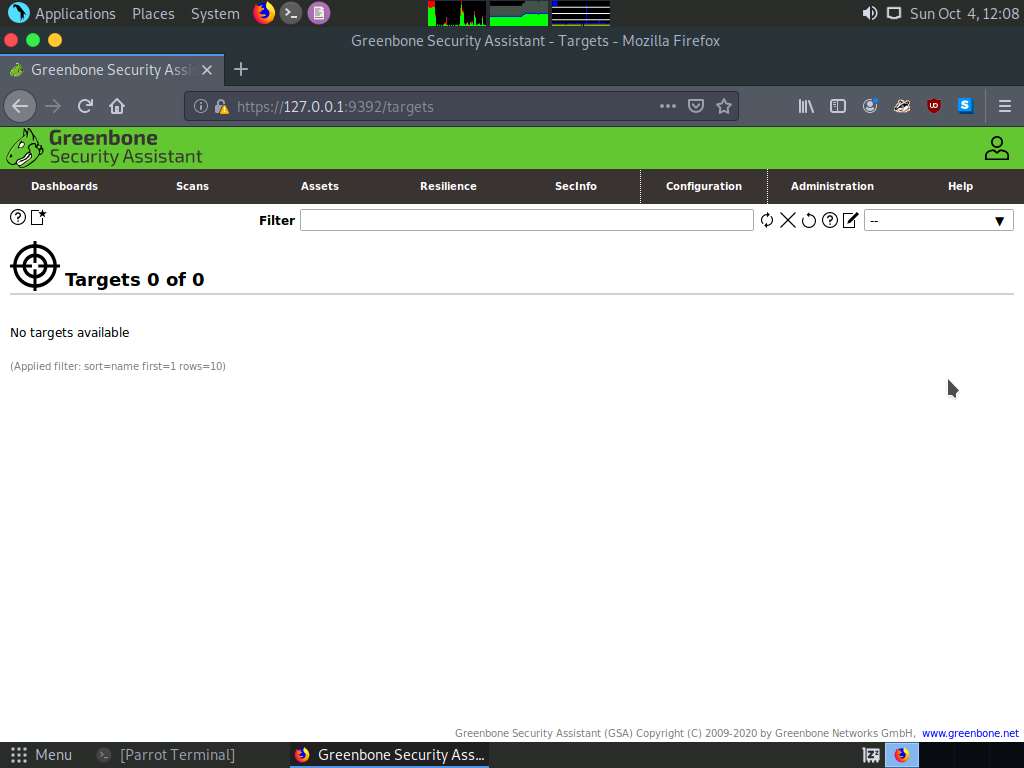


1. OpenVAS Dashboard appears as shown in the screenshot.

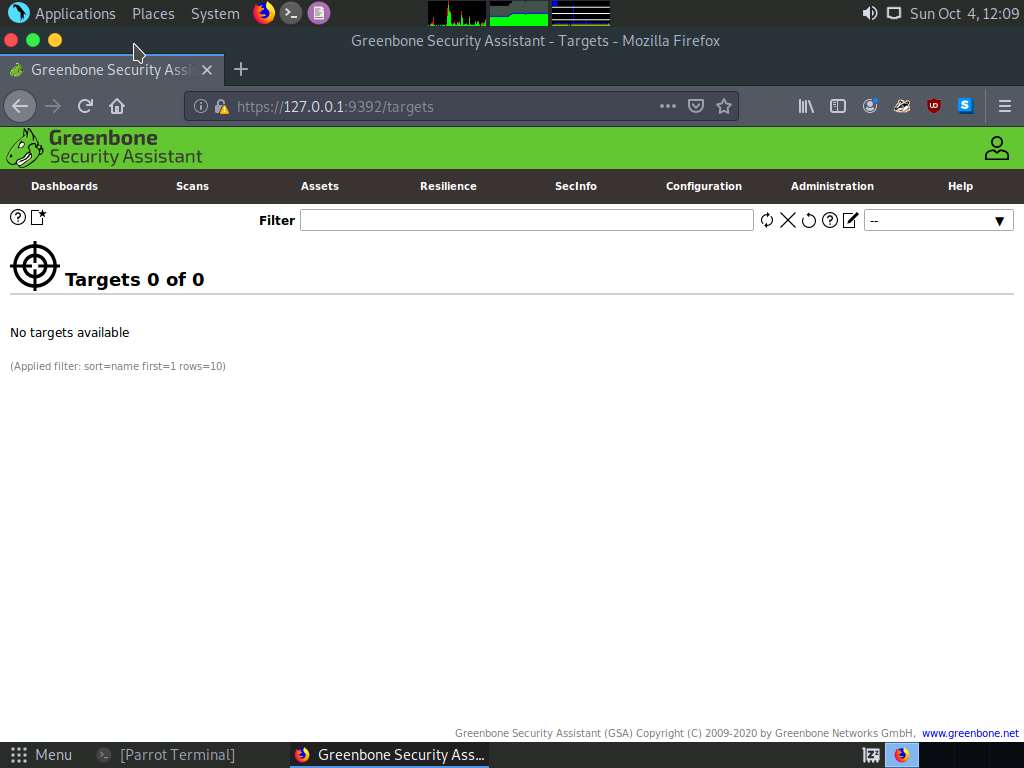
Ignore the password remembering pop-up



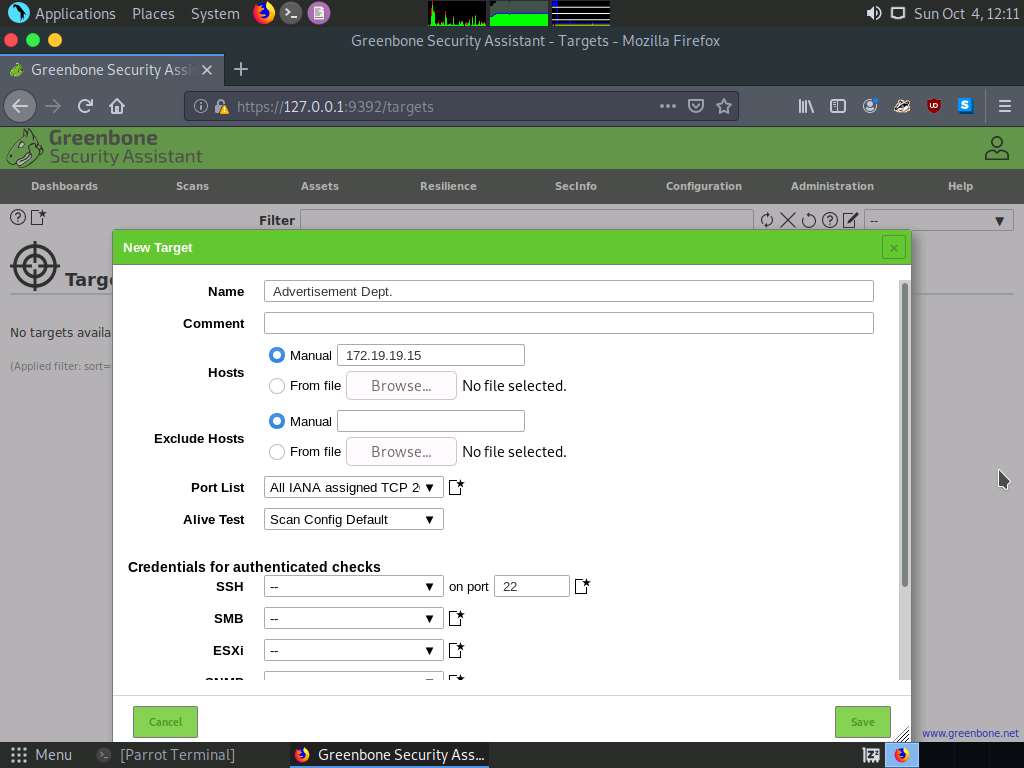
1. Click **Configuration** .



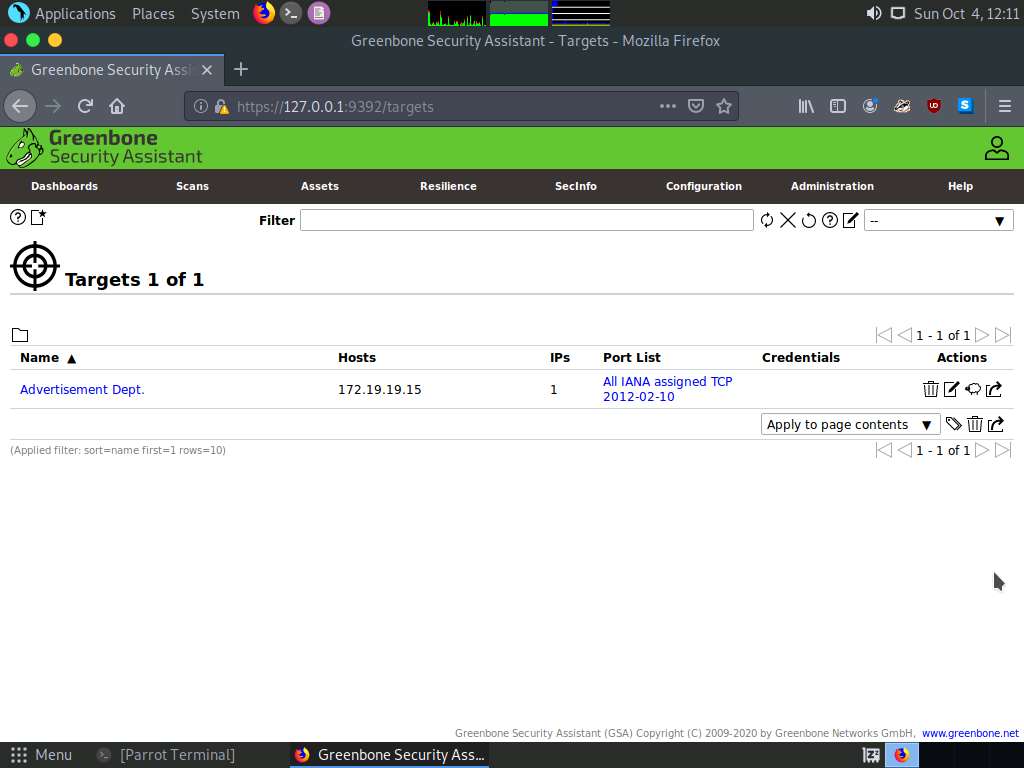
1. Click the **File** icon in the top-left corner of the webpage, in order to add a new target.



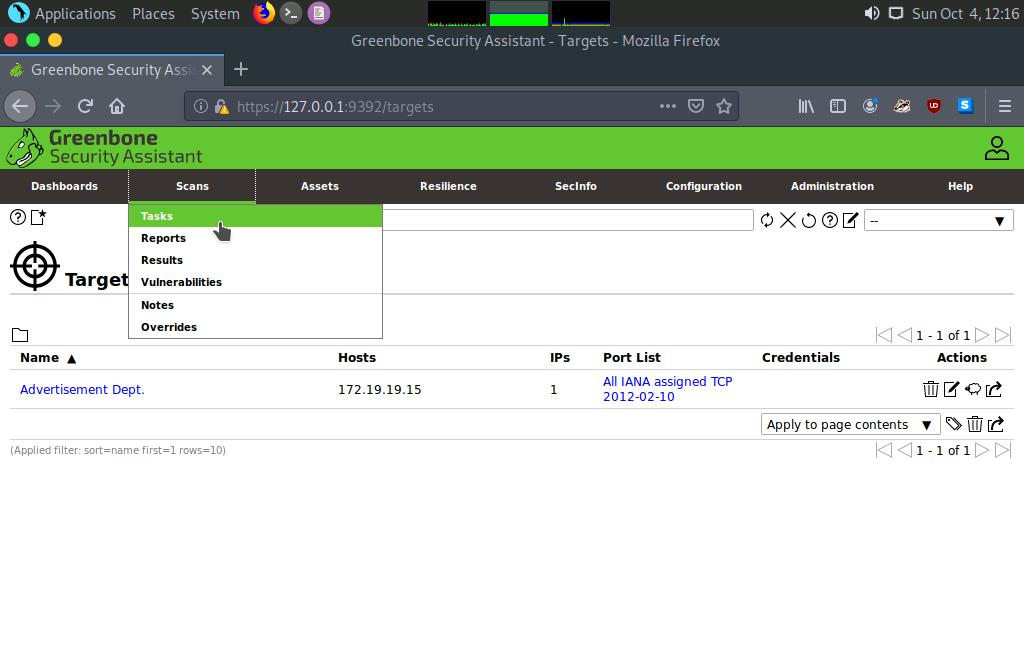
1. **New Target** window appears; enter the target name (**Advertisement Dept.** in this lab) in the **Name** text field, select **Manual** radio button under **hosts** section and enter the IP address of the target machine in the text field adjacent to the Manual radio button. The IP address of Advertisement Dept. is **172.19.19.15**. Select **All IANA assigned TCP 2012-02-10** option from the **Port List** drop-down list. Leave the other options set to default and click **Save**.



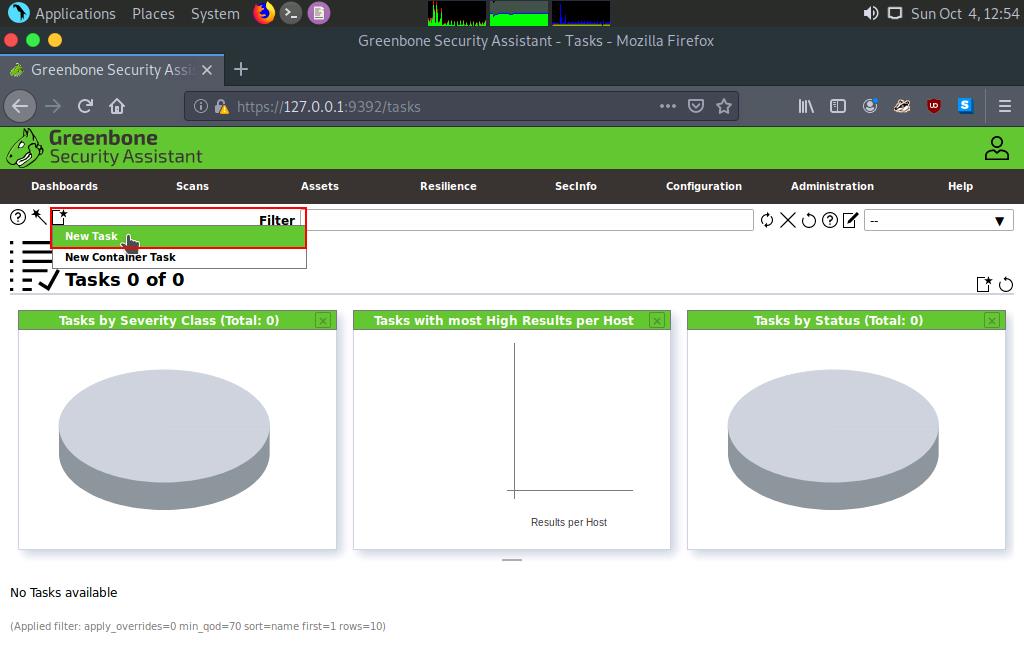
1. Once you click the **Save** button, OpenVas will add the target and it will display the **Target Details** as shown in the screenshot.



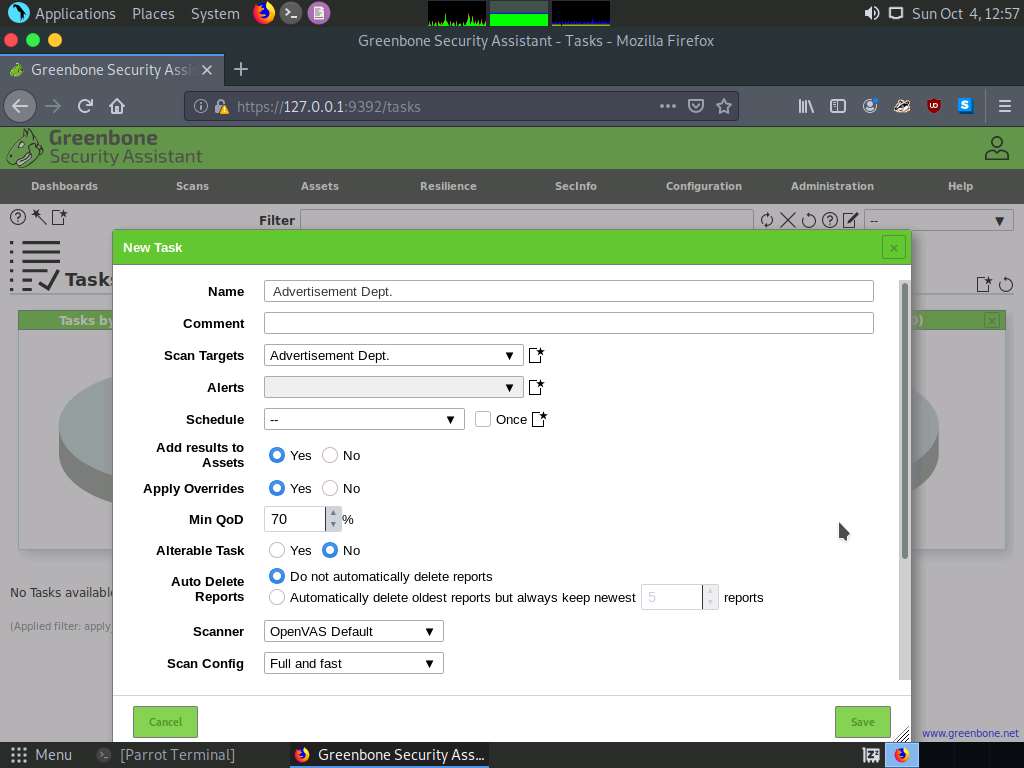
1. Hover the mouse cursor on **Scans** and click **Tasks** to add a new task.



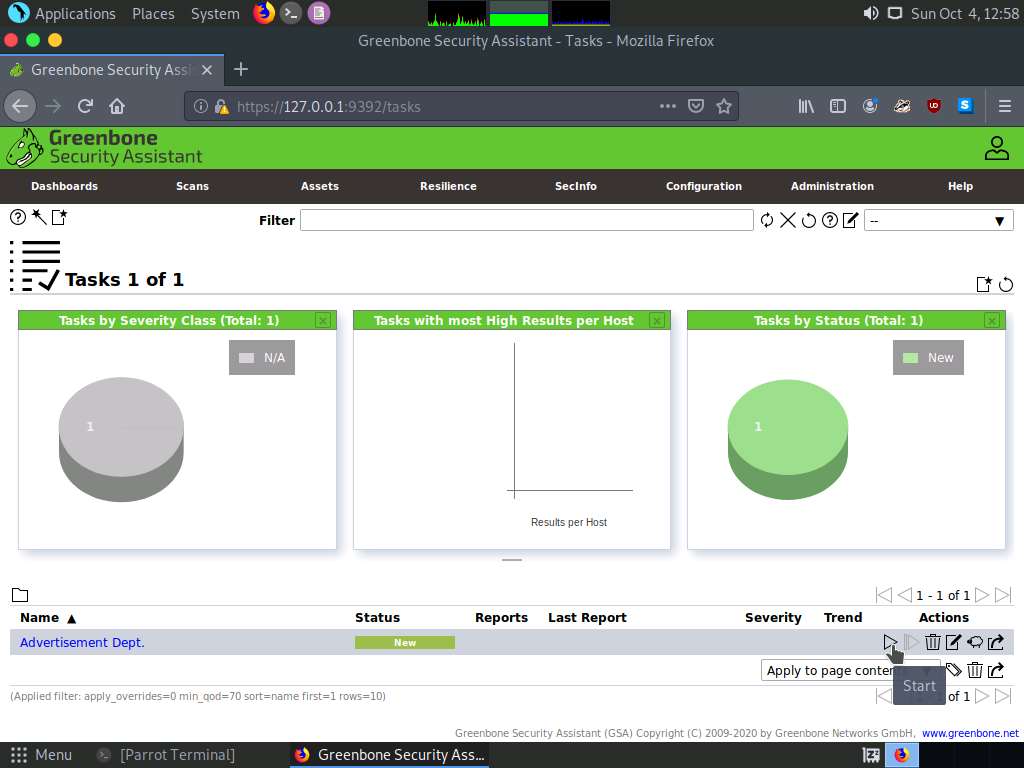
1. **Tasks** wizard appears; since we haven't added any tasks to OpenVas, it will be empty. Now, we need to create a new task. To do this, hover the mouse cursor on the **Task** (File with star icon) on the top-left corner of the browser and click **New Task** in the context menu.



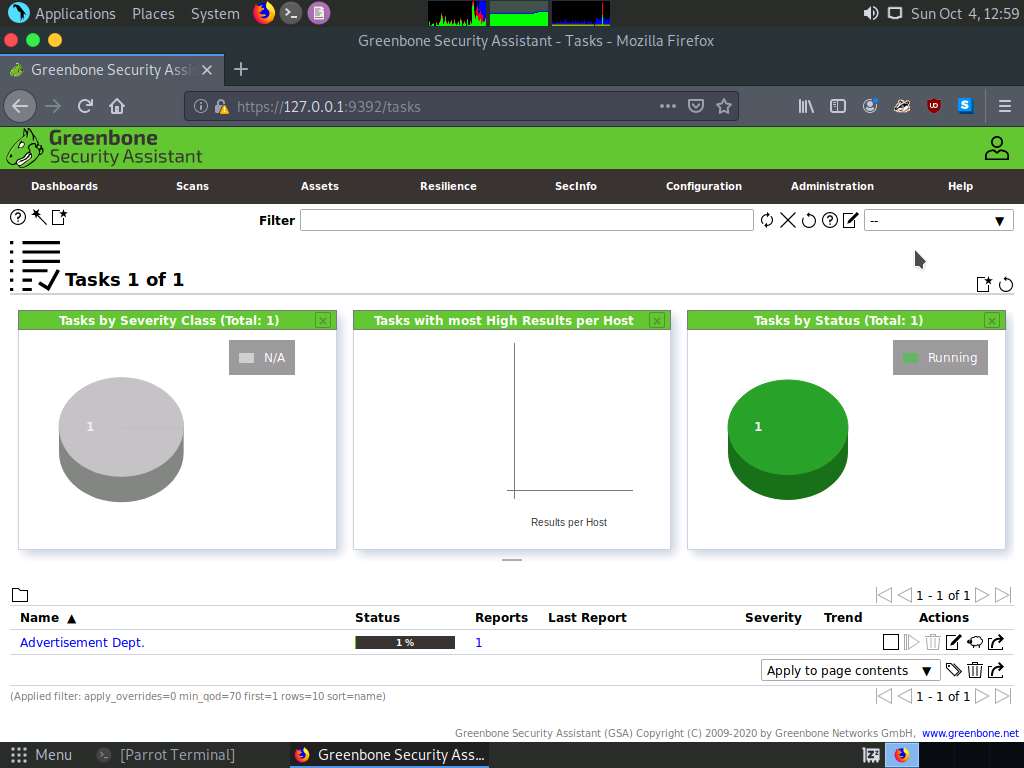
1. **New Task** window appears; enter the name of the task (here, **Advertisement Dept.**), choose **Advertisement Dept.** from the **Scan Targets** drop-down list and choose **Full and fast** scan from the **Scan Config** drop-down list. Set the value of **Maximum concurrently executed NVTs per host** to **4**. Leave the other options set to default, and scroll to down to click **Save**. This creates a task which will be performed in the forthcoming steps.



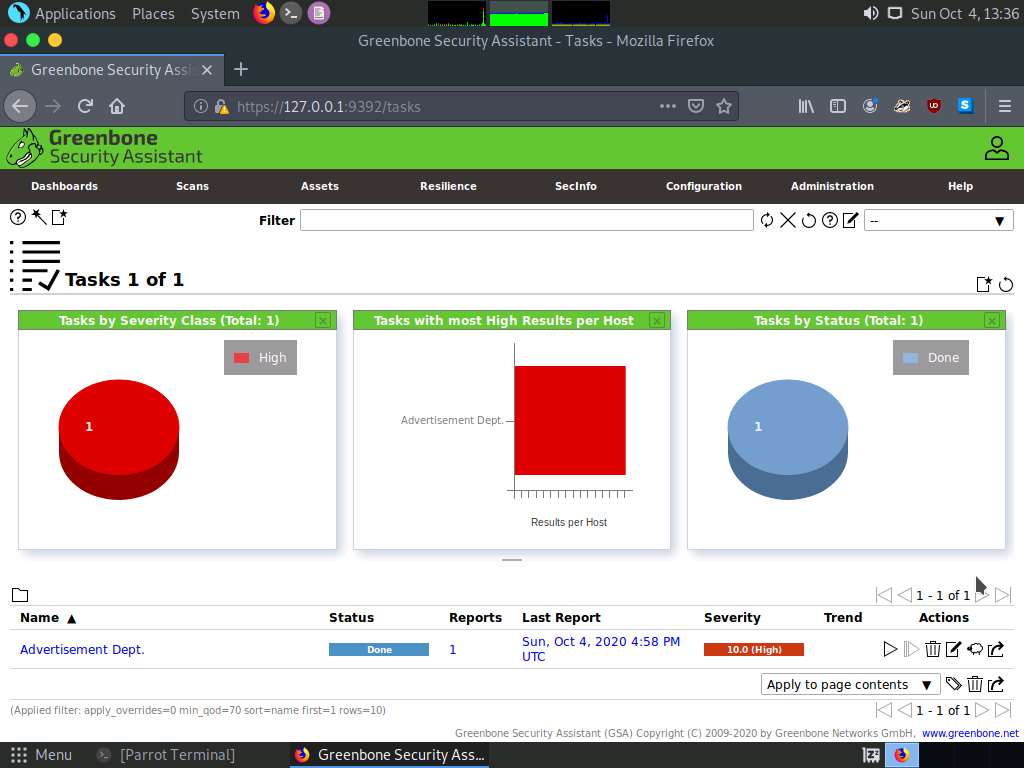
1. The task named **Advertisement Dept.** has been successfully added to OpenVAS as shown in the screenshot. Begin the vulnerability scan by clicking the **Start** (Play) icon in **Task Details**.



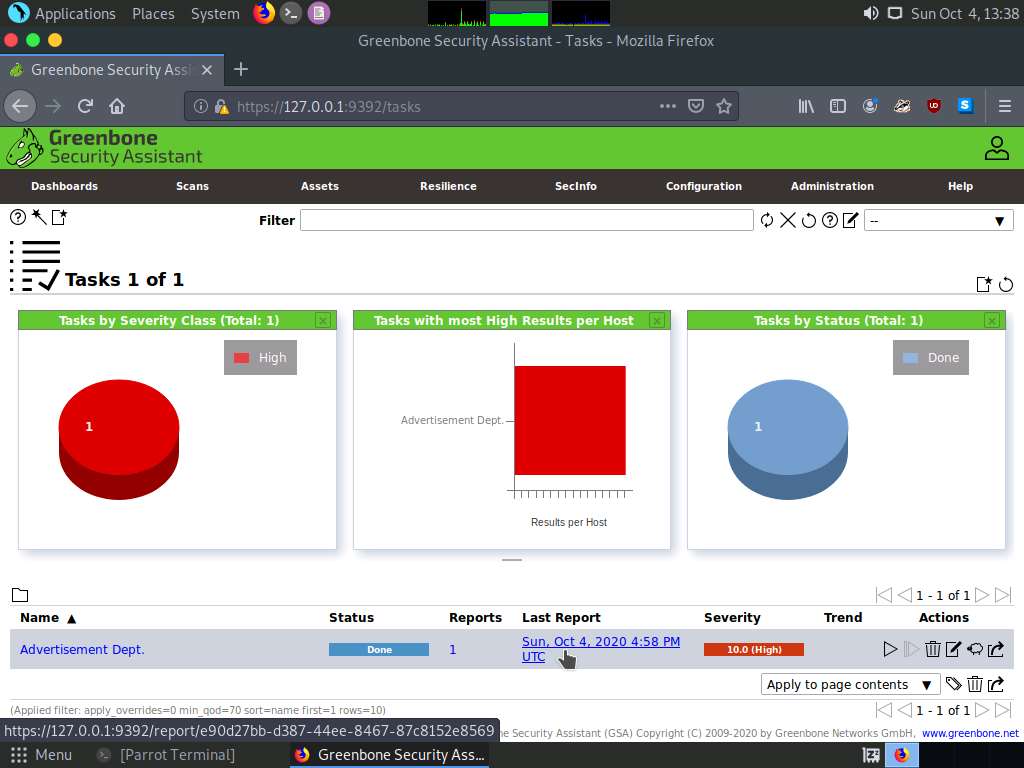
1. A vulnerability scan has been initiated successfully. Wait until the scan is completed. It will take approximately 5 to 10 Minutes to complete the scan.



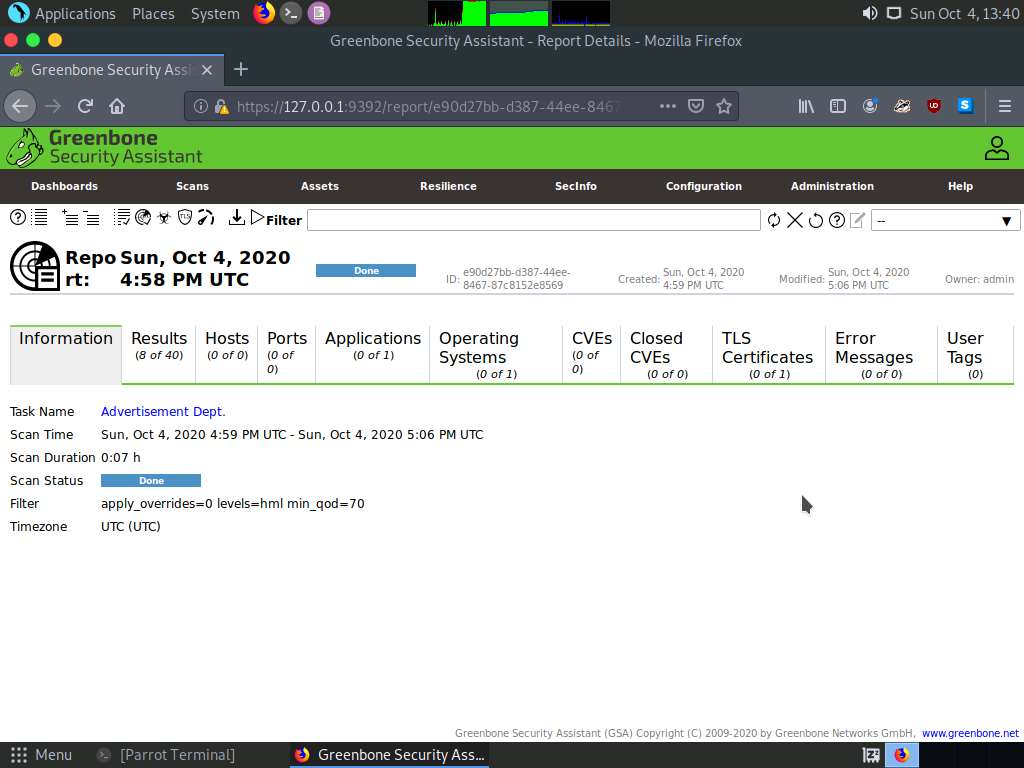
1. On completion of the scan, the status of the scan changes to **Done** as shown in the screenshot.



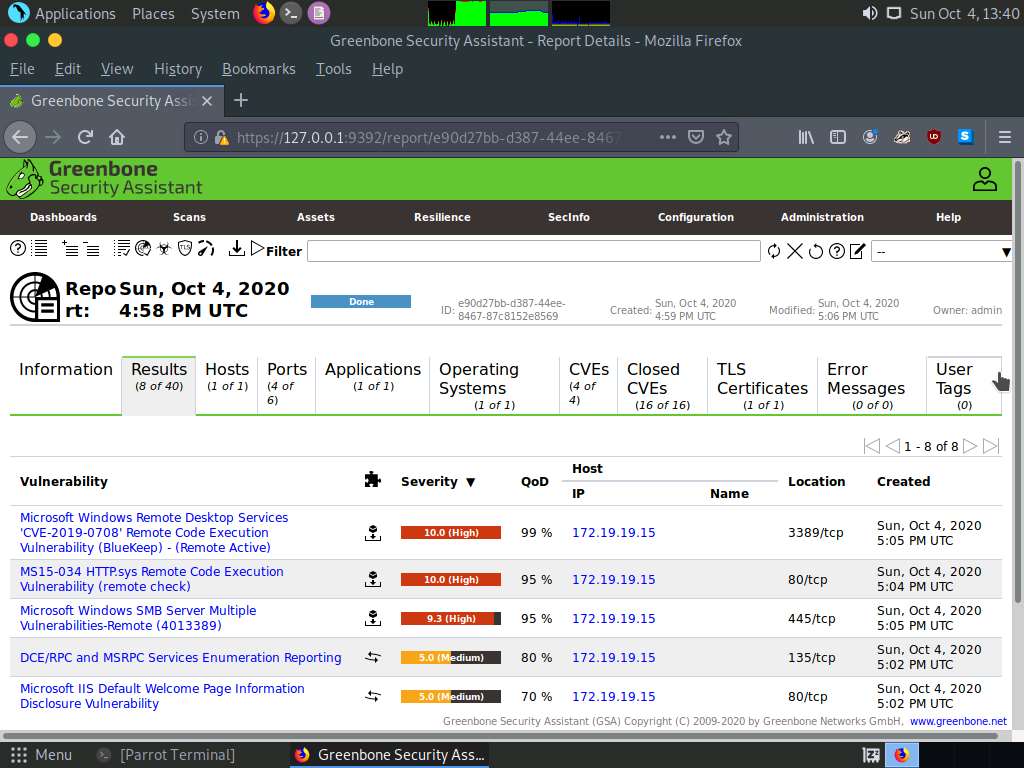
1. Click on the **date** link in the **Last Report** section in Task Details. The date (**Oct 4 2020**) displayed in this lab will vary from your lab environment.



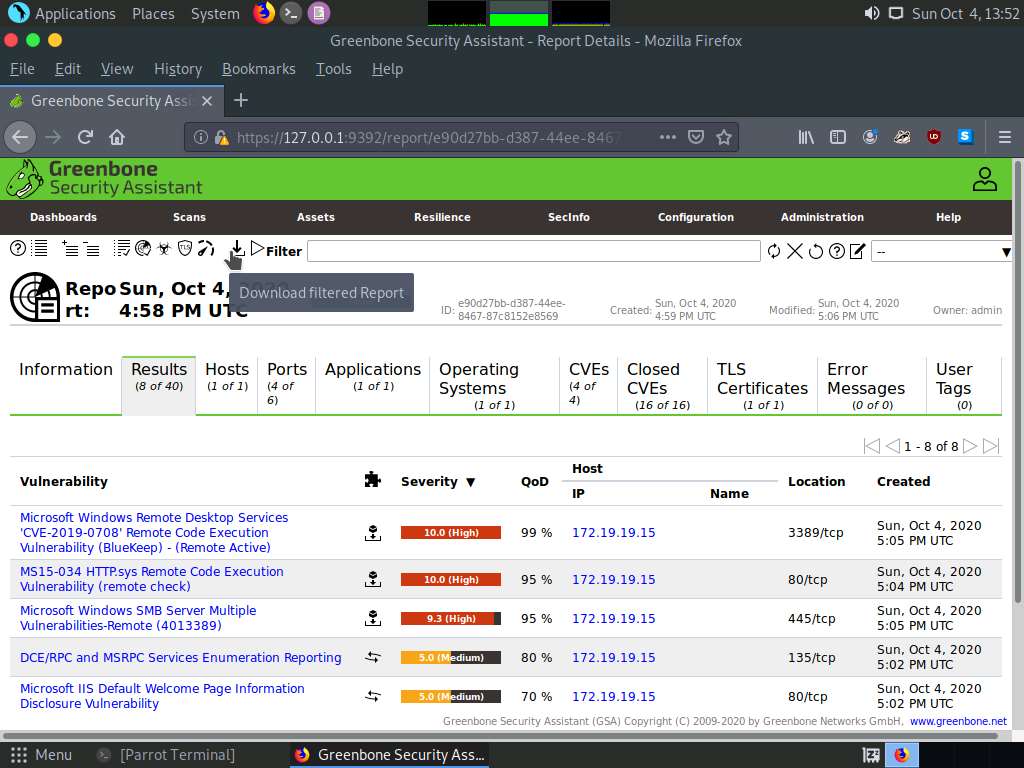
1. The **Report** window appears as shown in the screenshot, click on the Results tab to view the vulnerability information.



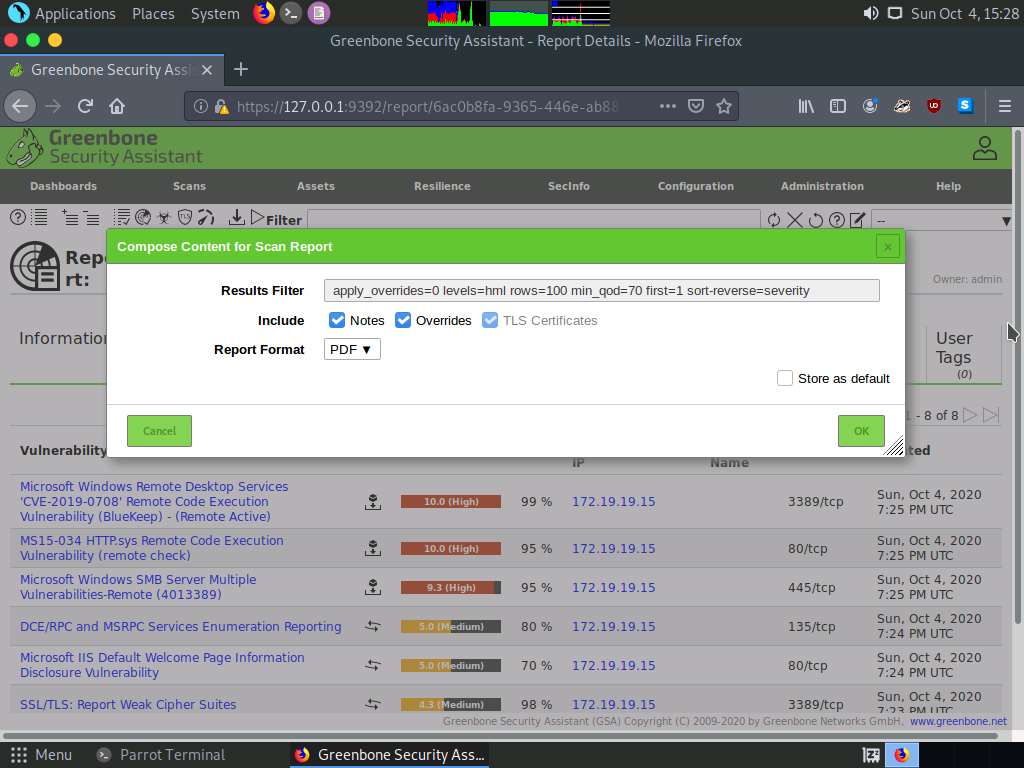
1. The **Results** window appears as shown in the screenshot, where OpenVas will display all the **Vulnerability** list and its **Severity** levels.



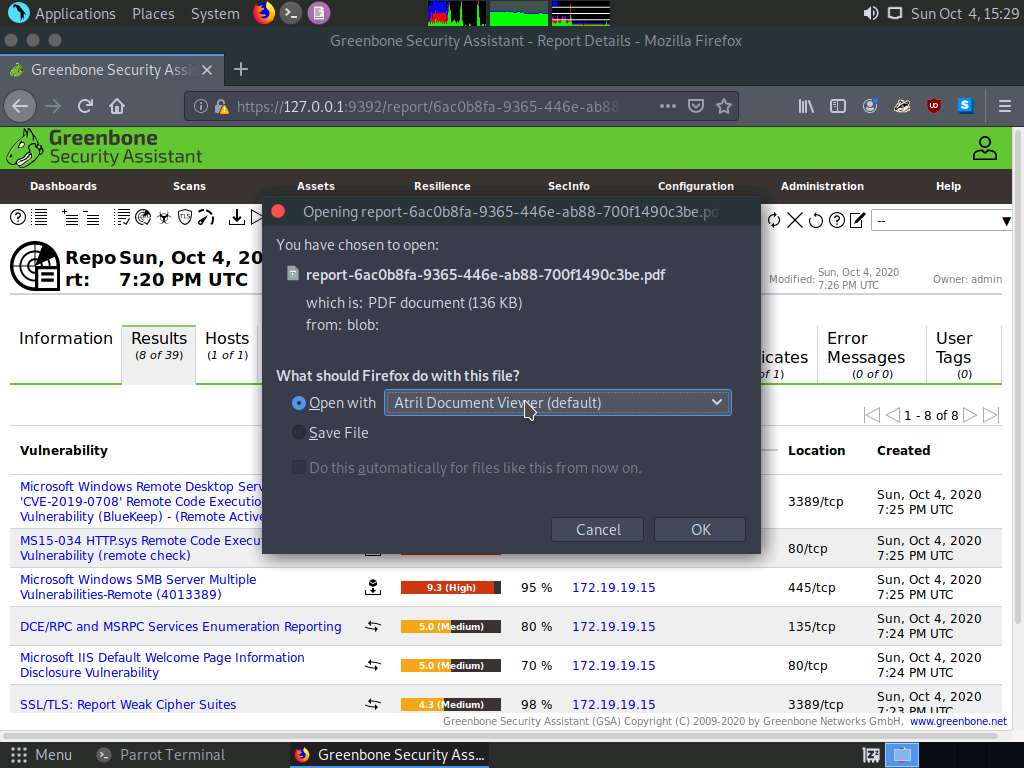
1. Click on Download button on top of the page to download the report.



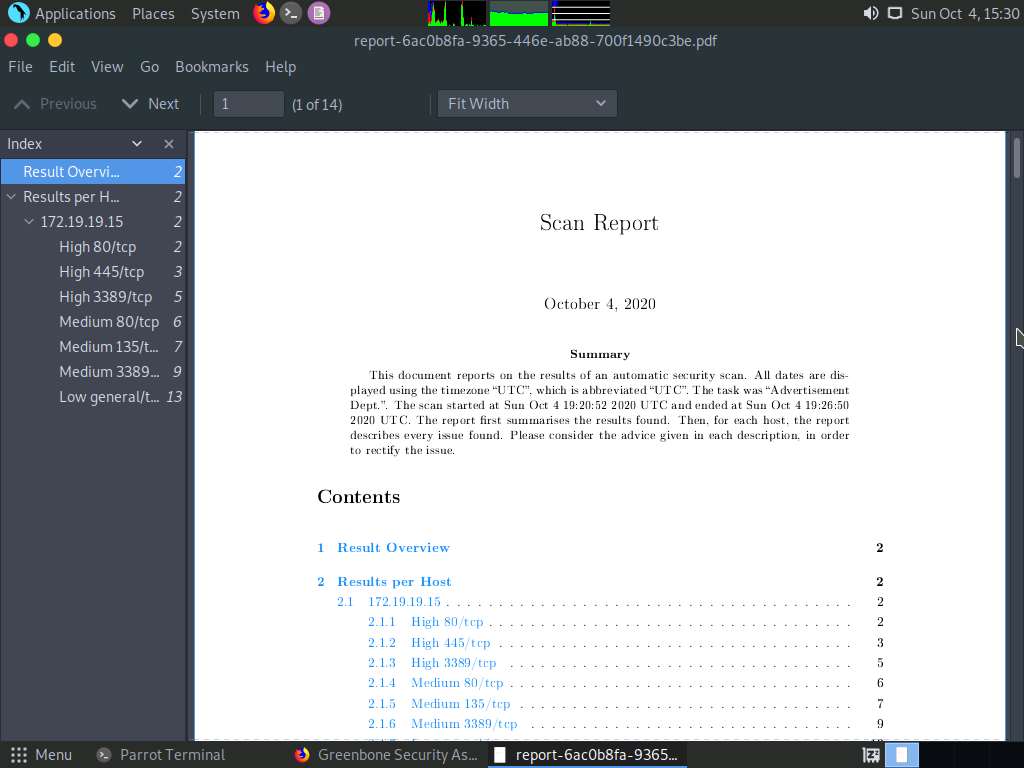
1. **Compose Content for Scan Report** pop-up appears, select **PDF** from the **Report Format** drop-down list and click **OK**.



1. **Opening report** pop-up appears, select **Open with** radio button, choose **Atril Document Viewer** from the drop-down menu and click **OK**.



1. The report appears in the document viewer. Scroll down the report and examine all the vulnerabilities that are detected during the scan.



1. After examining the vulnerability report, logout and close the web browser and all the windows that were opened.