Lab - Perform a Vulnerability Scan Using OpenVAS

**Overview**

Once we’ve enumerated our target using Nmap, we can perform a more comprehensive scan for vulnerabilities using the Open Vulnerability Assessment Scanner (OpenVAS).

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and 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 scanner obtains the tests for detecting vulnerabilities from a feed with a long history and daily updates.

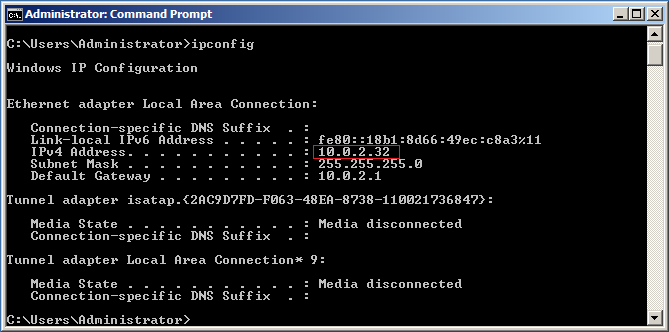
**Lab Requirements**

* One installation of VirtualBox with Extension Pack.
* One virtual install of Kali Linux
* On virtual install of Metasploitable3 Win2k8.
* One virtual install of the OVA file of the Greenbone Enterprise TRIAL.
* All VirtualBox network adapters should be configured for NAT network.

**Find your target’s IP address.**

Log on to your Win2k8 target machine as an administrator using the password **vagrant**.

Once you have a desktop, open a command prompt, and at the prompt, type **ipconfig**. Next, find the IP address for the local area connection.

****

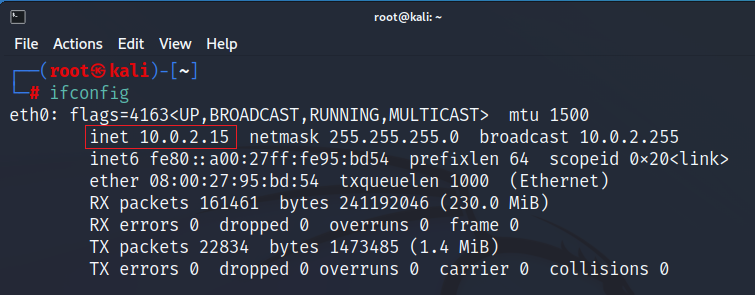
This is the IP address for my Metasploitable3 target. Yours may differ.

**Find the IP address of your Kali machine**

Open a new terminal on your Kali machine. At the prompt and type, **ifconfig**.

Press enter.

Find the IP address for your eth0 adapter.



This is the IP address for my Kali machine. Yours may differ.

**Check for Connectivity**

From your Kali desktop, open a new terminal. At the prompt type, ping <target IP address>.

Text

Description automatically generated with low confidence

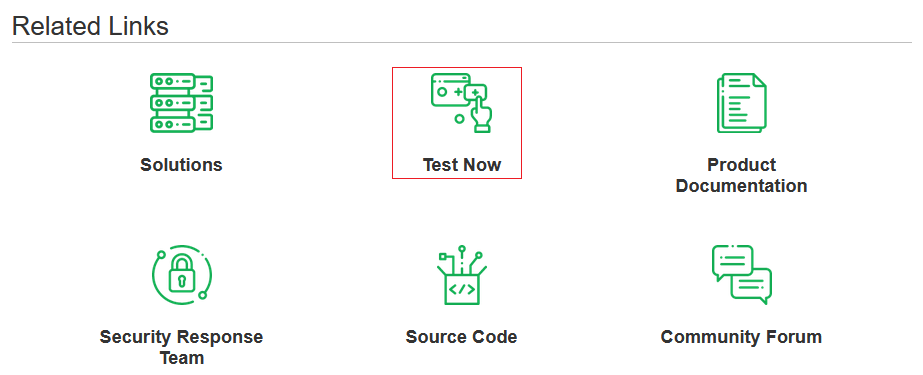
You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to NAT Network adapters and try again.

**Download OVA file for OpenVAS**

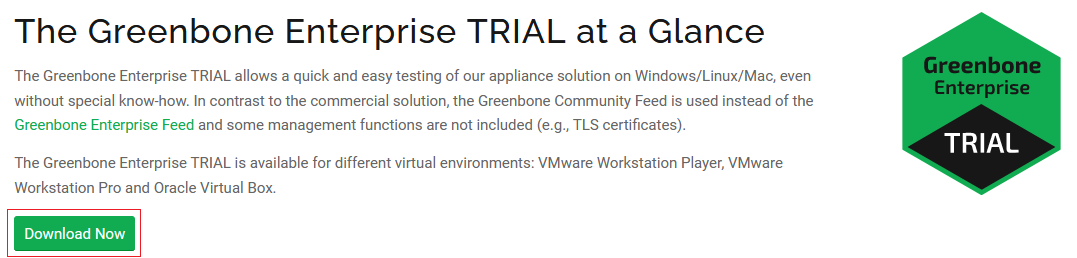
To download the OVA file for OpenVAS, use the following URL.

<https://www.openvas.org/>

Scroll down. Under Related Links, click the icon marked, Test Now.



On the next page, click the link, Download Now.



The page scrolls down. To the right, click on the open for Oracle VirtualBox.

Chart

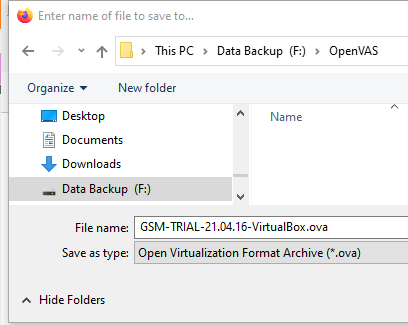
Description automatically generated with low confidence

Click on Instructions. Scroll down until you find the steps for Importing the Greenbone Enterprise TRIAL. Then, click the link marked [Download](https://files.greenbone.net/download/delivery/e56eb22d-360c-48f8-bd44-b701fd834650/GSM-TRIAL-21.04.16-VirtualBox.ova).

Text

Description automatically generated

Save the OVA file to your local machine. I saved y download to a folder labeled OpenVAS situated on my storage drive. Of course, you are free to save yours as you wish.



Once the OVA has been downloaded, find the file and x2 click to import into VirtualBox.

Accept the findings of the Import Appliance Wizard and at the bottom of the screen, click the button labeled **Import**.

Graphical user interface, text, application, email

Description automatically generated

Allow the import to complete.

Graphical user interface, text, application, email

Description automatically generated

Once the import process has been completed, from your left windowpane of VirtualBox, find the virtual disk labeled GSM-TRIAL-21.04.16-VirtualBox.

Text

Description automatically generated with medium confidence

X2 click to launch.

When you start the virtual disk for the first time, you will see the following VirtualBox error. Next, click on the button labeled Change Network Settings.

Graphical user interface, text, application, email

Description automatically generated

Change the adapter to NAT Network and click OK.

Graphical user interface, text, application

Description automatically generated

At the terminal prompt, type in **admin** for both the username and password.

This Linux. You will not see the password being typed in at the prompt.

Text

Description automatically generated

Your screen will be the start of the setup wizard for OpenVAS. Press enter to start the Setup Wizard.

Graphical user interface, text, application, email

Description automatically generated

On the next screen, click Yes to create a web admin account.

Graphical user interface, text, application

Description automatically generated

On the next screen, create your webadmin account. Remember the password!

Use your keyboard up and down arrows to navigate the screen.

Graphical user interface, text, application, email

Description automatically generated

Use your TAB key to highlight the OK button and then press enter.

User created.

Graphical user interface, application, Teams

Description automatically generated

On the next screen, you will be asked for your subscription key. Since we want to use the community edition, use your TAB or arrow key to highlight the Skip button and press enter.

Text

Description automatically generated

The setup performs a Selfcheck.

A picture containing rectangle

Description automatically generated

Ignore any warning and press enter.

Graphical user interface, text, application

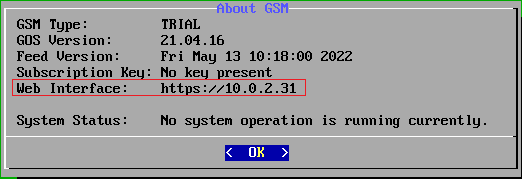
Description automatically generated

Use your up and down arrows on the next screen to select, About.

Graphical user interface, text, application, email

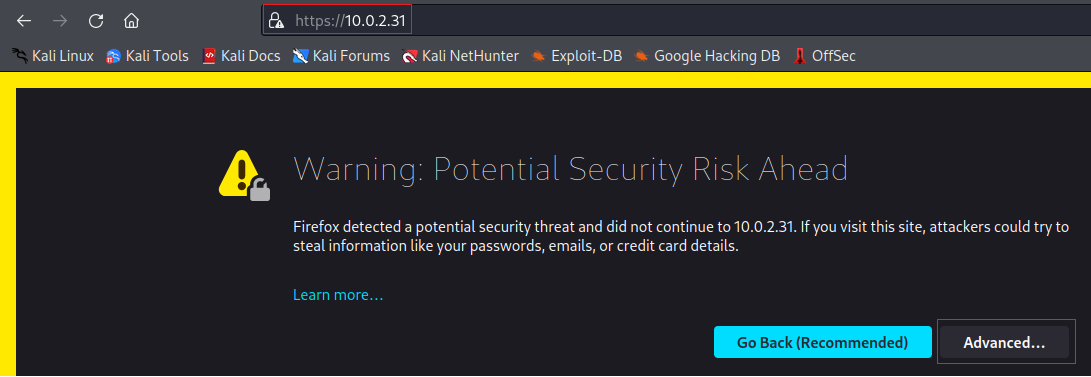
Description automatically generated

Find the web interface information you need to access OpenVAs using a web browser on the next screen.

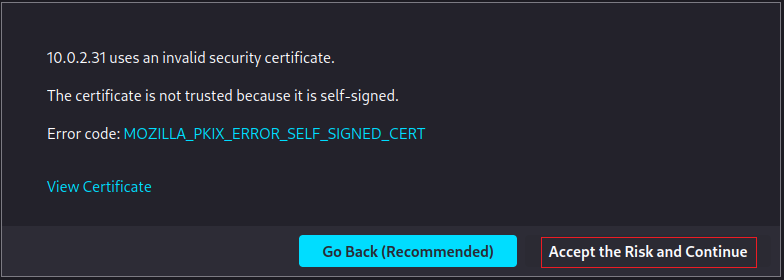


Open a browser on your Kali machine. Then, in the address bar, type the address just as displayed in the About GSM window.

You receive a certificate warning. Then, click on the button labeled, Advanced from the main windows.



Scroll to the bottom of the screen, click the button labeled, **Accept the Risk and Continue.**



On the login page, type in your webadmin account name and password.

Graphical user interface, text

Description automatically generated

You can cache your credentials with your Kali browser if you want to.

This opens your OpenVAS dashboard.

Graphical user interface, application

Description automatically generated with medium confidence

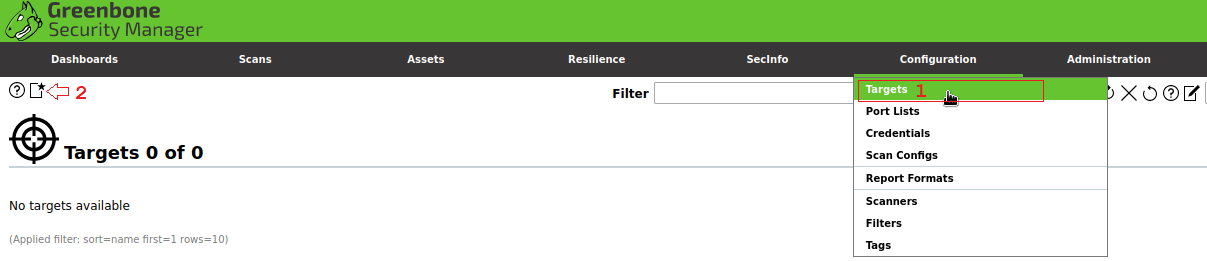
**Creating a target in OpenVAS**

The first step is to create and configure a target using the OpenVAS/Greenbone Security Assistant web interface.

To create a target:

Go to ‘Configuration’ in the top menu and select ’Targets.’

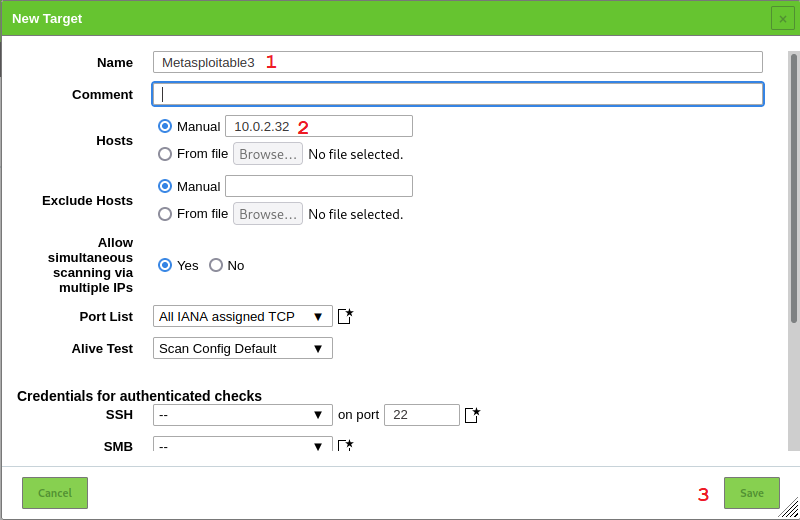
Click the black icon in the top left corner to create a new target.



After hitting the new target button, a dialog screen appears where we have to enter the following information:

* Target name, I have named this target Metasploitable3.
* The target IP host is the IP address for our Metasploitable3 target machine.

Keep all other settings default and click the ‘Save’ button.



The newly created target will now appear in the list of available targets:

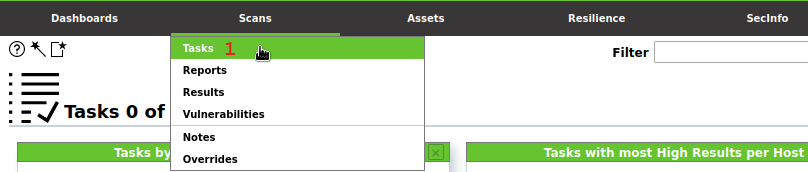
Graphical user interface, text, application

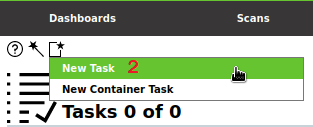
Description automatically generated

We next need to create a scan task that will scan our Metasploitable3 target for vulnerabilities.

To create a new scan task, we must perform the following steps:

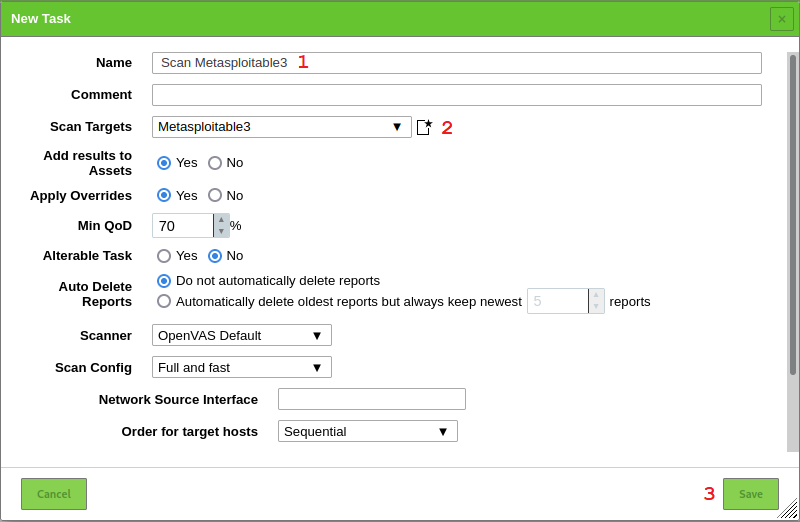
1. Go to ‘Scans’ in the top menu and select ’Tasks.’
2. Point to the black icon in the top left corner and select ‘New Task.’





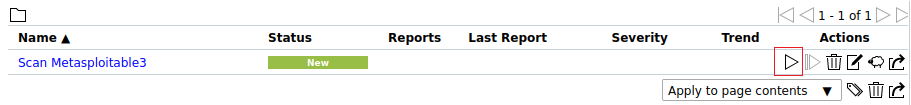
After clicking the new scan option, a dialog screen appears. Enter the following information:

1. Task name, we’ll name it ‘Scan Metasploitable3’.
2. Make sure that the Metasploitable3 target we’ve created earlier is selected.
3. Keep all other settings default and click the ‘Save’ button to create the new task.



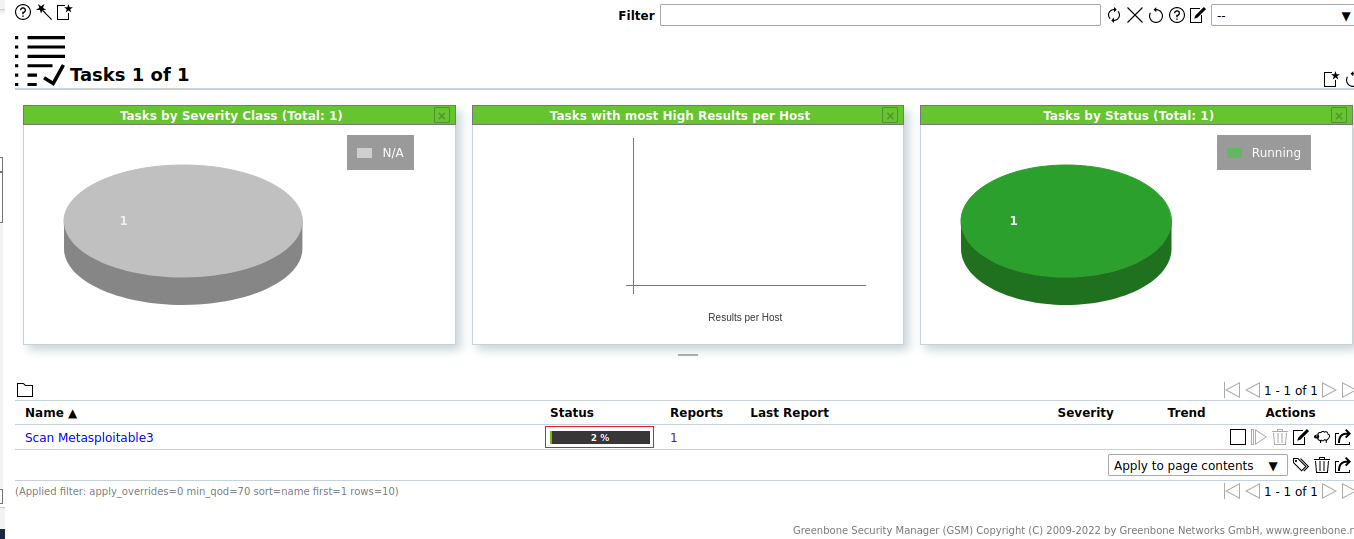
The newly created task will now appear at the bottom of the task list.

To run the newly created task, click the green start button as follows:



The scan task will now execute against the selected target. Please note that a full scan may take a while to complete. When you refresh the tasks page, you will be able to check the progress of the executed task:

1. Reload the page.
2. Check task status/progress. (Press f5)



When the scan task has finished and the status changes to ‘Done’:

To view the scan results, click Scans from the task bar and select Results from the context menu.

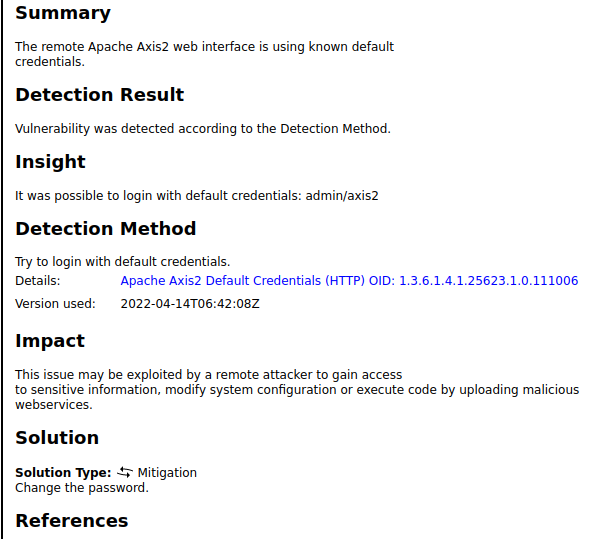
Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

You can click on any found vulnerability and get the information on the vulnerability, how to mitigate the vulnerability, and see the solution.



**Generating Reports**

Under Configuration>Report Formats, you can generate one of six formatted scan reports.

Graphical user interface, application

Description automatically generated

To download your scan results as a report, under Scans>reports, click on the date of the scan.

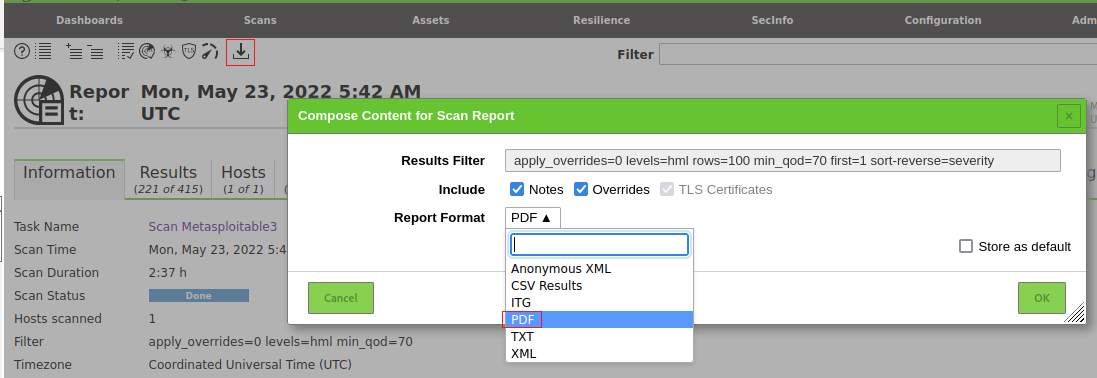


On the next page, you can see all the information included in the scan report.

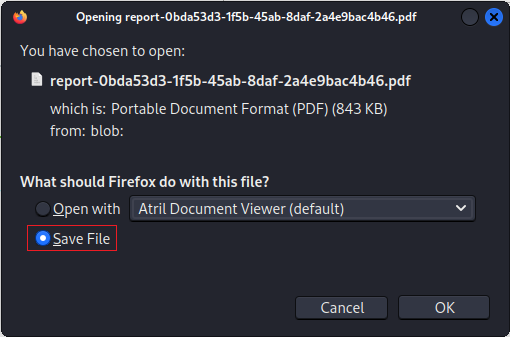
Graphical user interface, text, application

Description automatically generated

In the top left corner, click on the download icon. Next, choose your format, and finally, click OK.



You can choose to open or save the report on the next screen.



The report is saved to your Downloads.

Graphical user interface, text, application

Description automatically generated with medium confidence

You can open the report by clicking the folder icon on the right. When you open the saved PDF file, you are presented with a nicely formatted Scan Report.

Table

Description automatically generated

**Summary**

OpenVAS is a commercial product that comes with a community edition. OpenVAS may be the most popular of all scanners, second only to NESSUS. Using an OVA file and importing the scanner into VirtualBox makes the installation a snap.