Lab - Perform a Vulnerability Scan Using OpenVAS

Overview

Once we have 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.

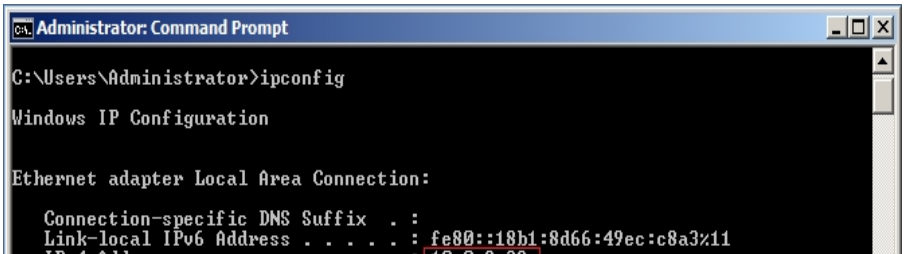
Lab Requirements

- 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 following 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.



```
   IPv4 Address. . . . . . . . . . . : 10.0.2.32
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```

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, type **`ifconfig`**. Press Enter.

Find the IP address for your eth0 adapter.

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 161461  bytes 241192046 (230.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22834  bytes 1473485 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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>:

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ping 10.0.2.32
PING 10.0.2.32 (10.0.2.32) 56(84) bytes of data.
64 bytes from 10.0.2.32: icmp_seq=1 ttl=128 time=0.450 ms
64 bytes from 10.0.2.32: icmp_seq=2 ttl=128 time=0.325 ms
64 bytes from 10.0.2.32: icmp_seq=3 ttl=128 time=0.287 ms
64 bytes from 10.0.2.32: icmp_seq=4 ttl=128 time=0.295 ms
64 bytes from 10.0.2.32: icmp_seq=5 ttl=128 time=0.247 ms
^C
--- 10.0.2.32 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4101ms
rtt min/avg/max/mdev = 0.247/0.320/0.450/0.069 ms
```

```
┌──(root㉿kali)-[~]
└─#
```

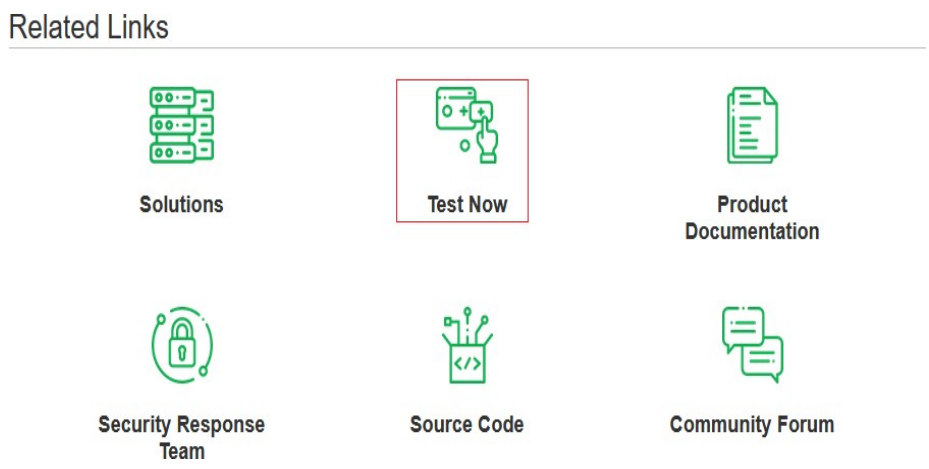
You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to NAT Network adapters and try again.

Download OVA File for OpenVAS

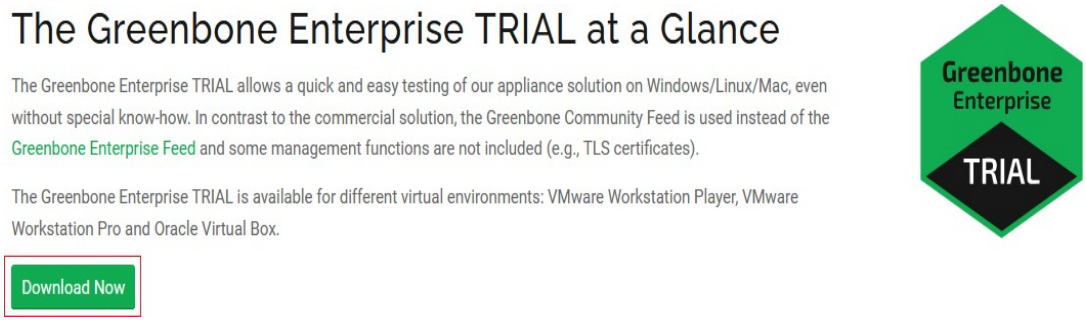
To download the OVA file for OpenVAS, use the following URL:

https://www.openvas.org/

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



On the next page, click the link Download Now:



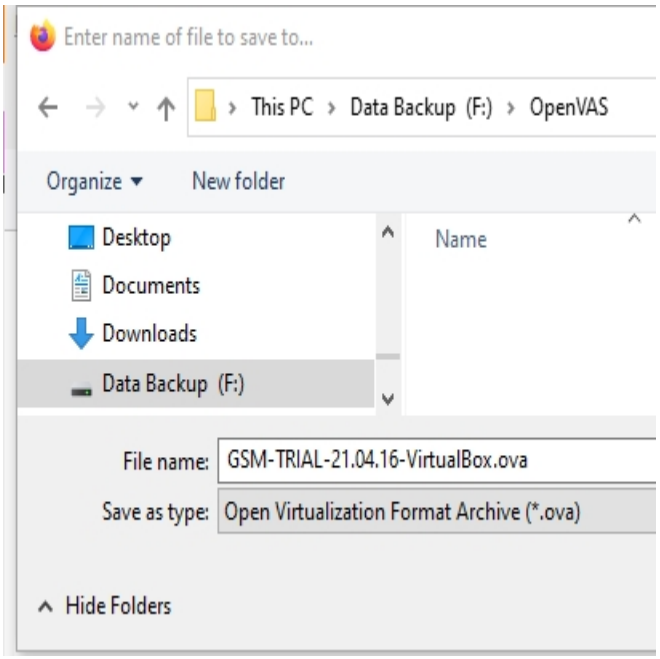
The page scrolls down. To the right, click on the open for Oracle VirtualBox:

Click on Instructions. Scroll down until you find the steps for Importing the Greenbone Enterprise TRIAL. Then, click the link marked Download.

Importing the Greenbone Enterprise TRIAL

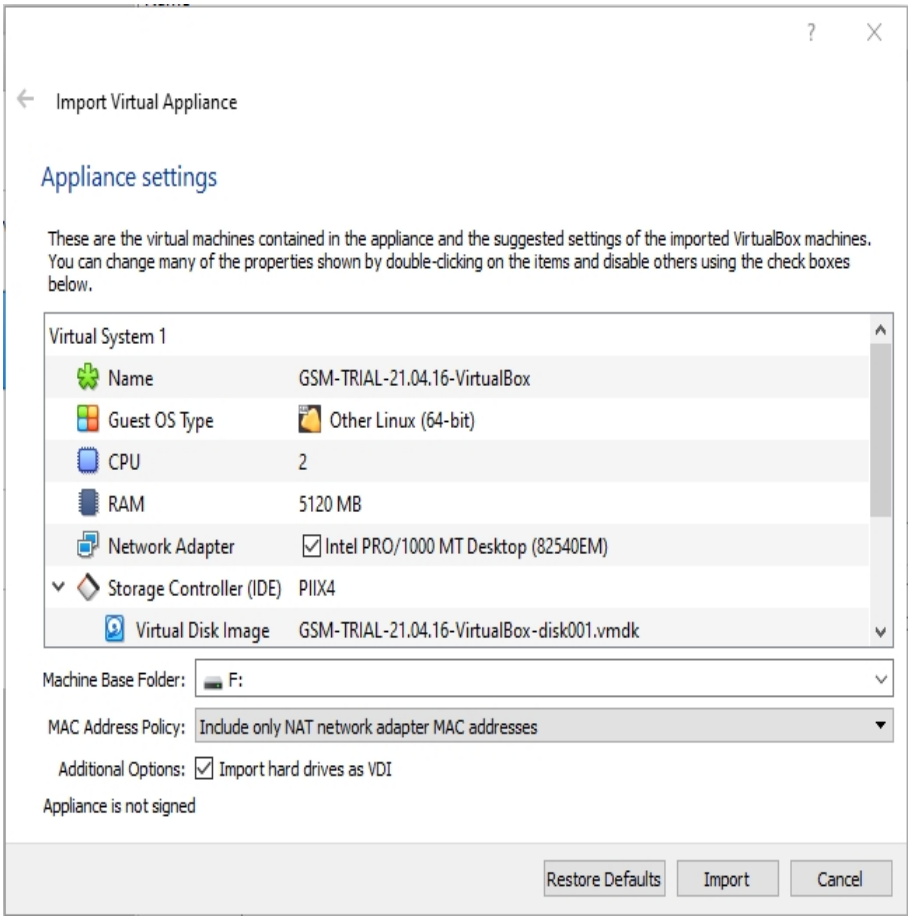
1. Download the OVA file of the Greenbone Enterprise TRIAL.

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

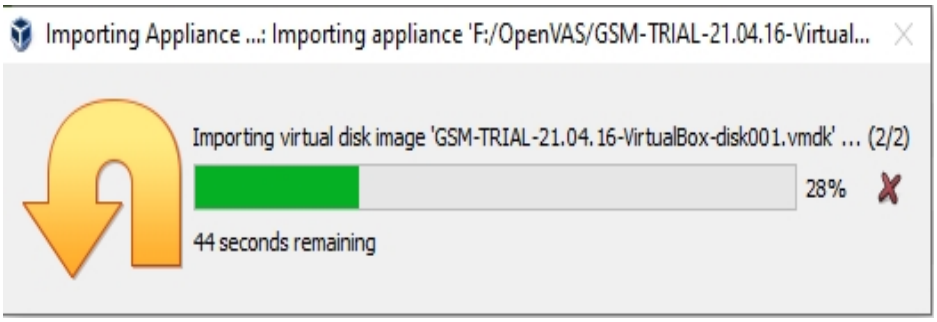


Once the OVA has been downloaded, find the file and x2 click to import into VirtualBox.

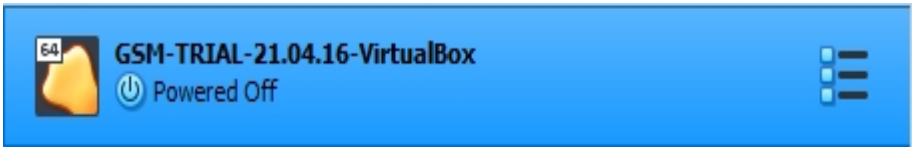
Accept the findings of the Import Appliance Wizard and at the bottom of the screen, click the button labeled **Import**:



Allow the import to complete.

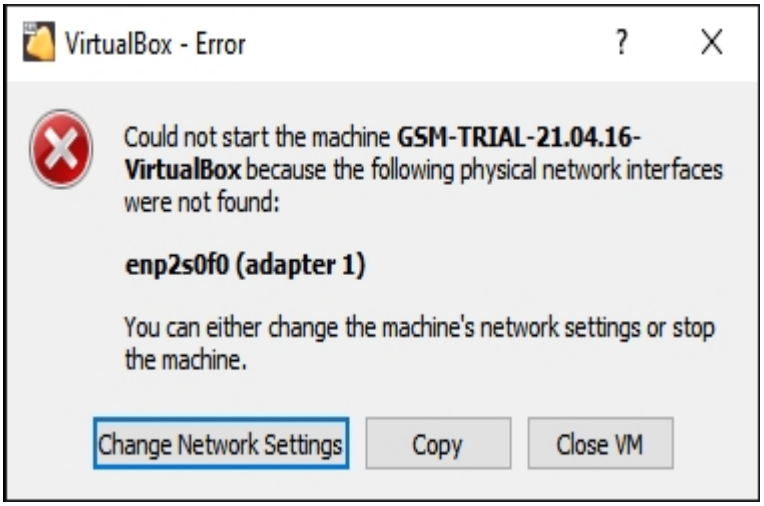


Once the import process has been completed, from your left windowpane of VirtualBox, find the virtual disk labeled GSM-TRIAL-21.04.16-VirtualBox.

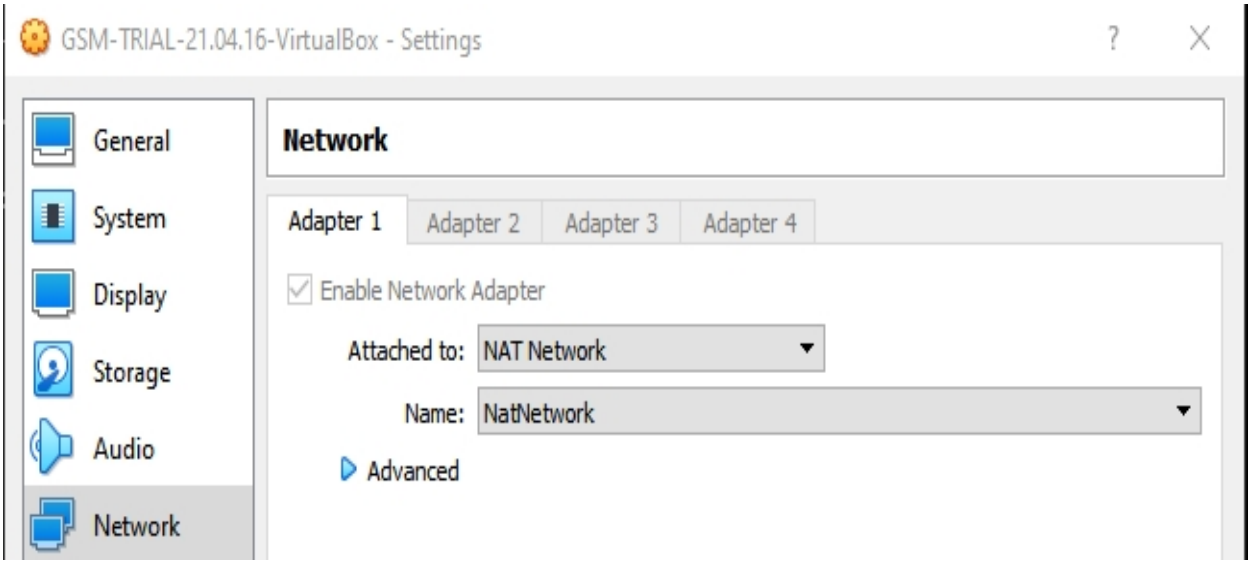


X2 click to launch.

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:

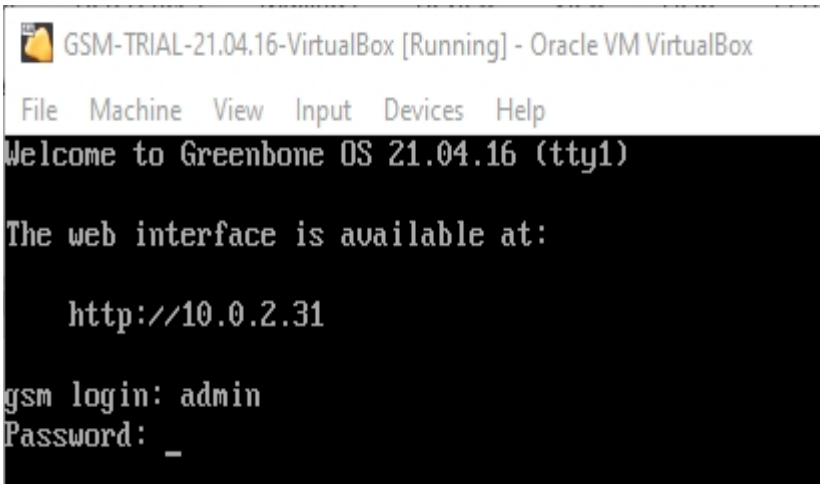


Change the adapter to NAT Network and click on OK:



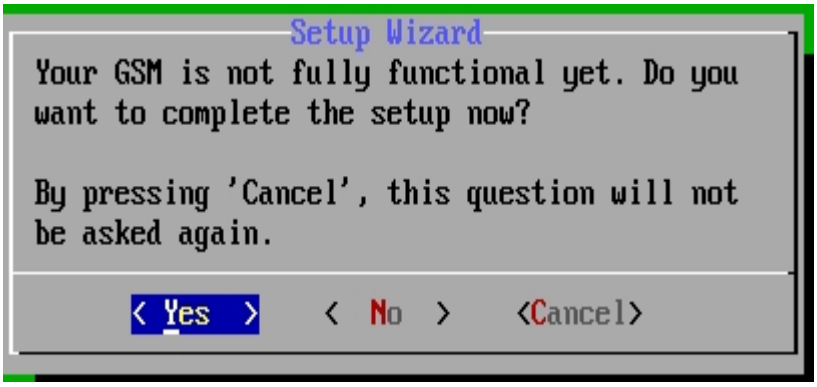
At the terminal prompt, type in **admin** for both the username and password.

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



Your screen will be the start of the setup wizard for OpenVAS. Press Enter to start

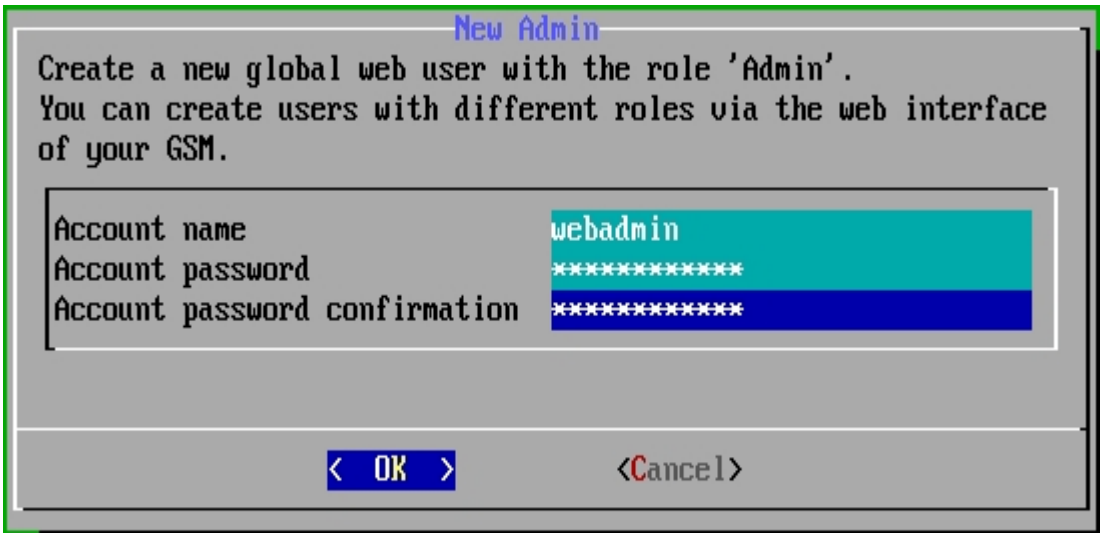
Your screen will be the start of the setup wizard for OpenVAS. Press Enter to start the Setup Wizard.



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

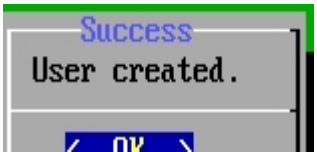
On the next screen, create your webadmin account. Remember the password!

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



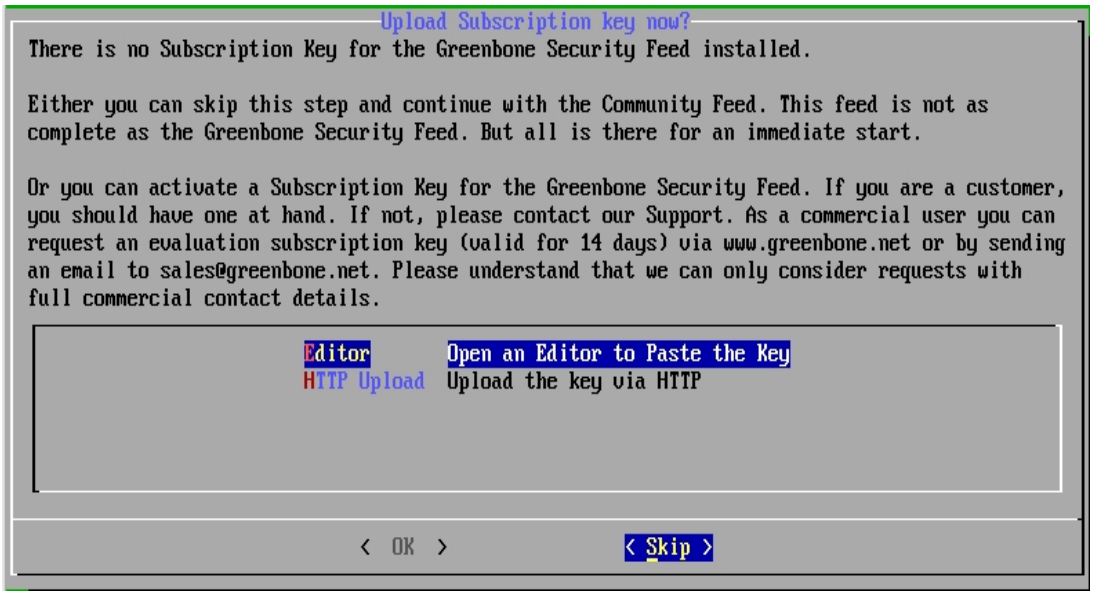
Use your TAB key to highlight the OK button and then press Enter.

User created.

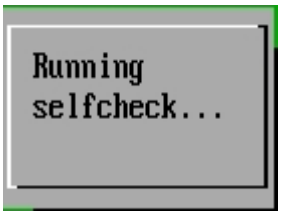



< OK >

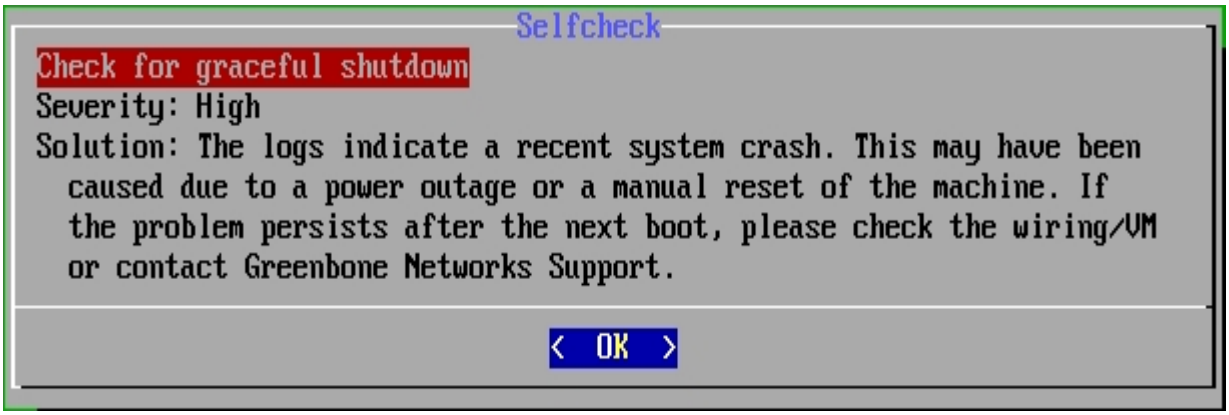
On the next screen, you will be asked for your subscription key. As we want to use the community edition, use your TAB or arrow key to highlight the Skip button and press Enter.



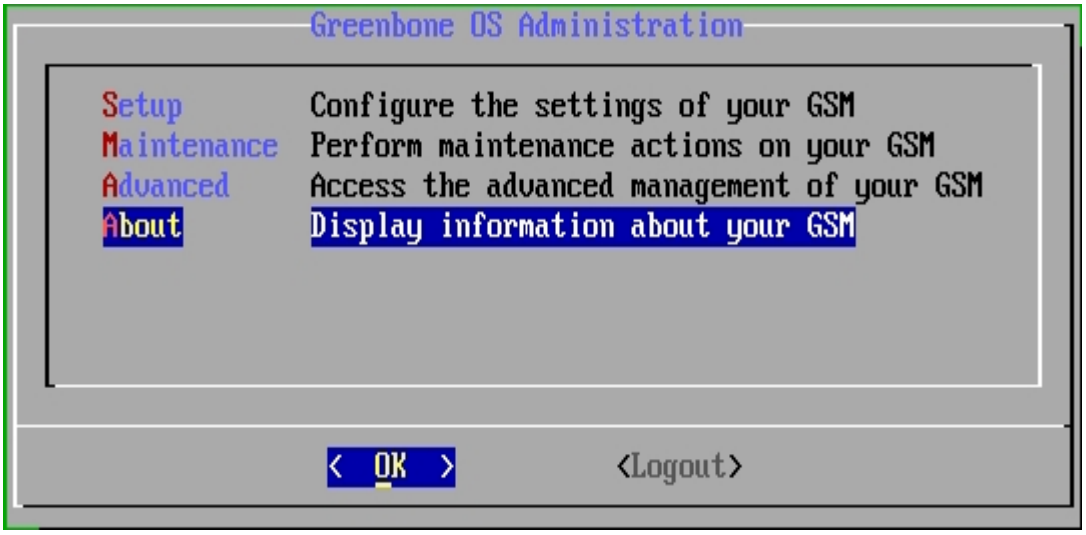
The setup performs a selfcheck.



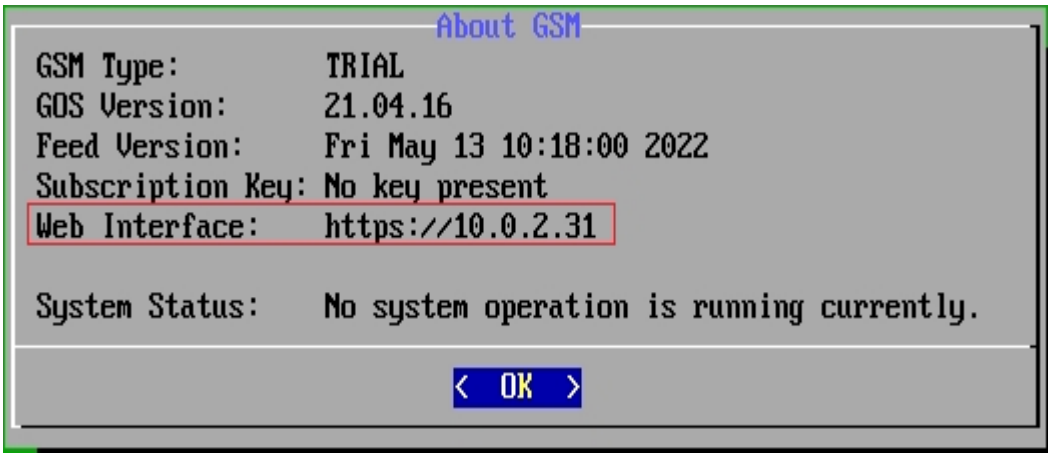
Ignore any warning and press Enter.



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

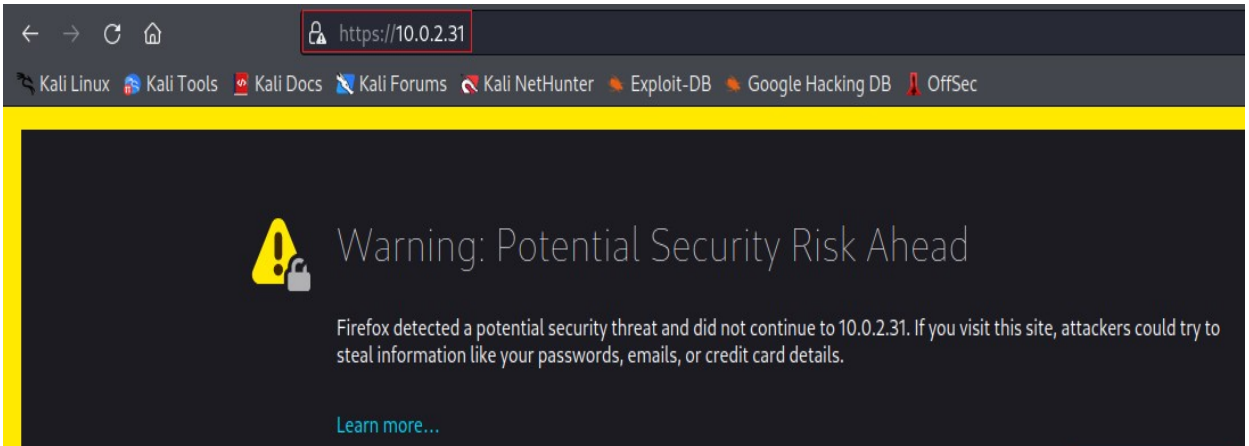


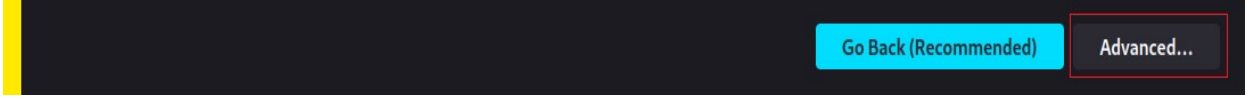
Find the web interface information you need to access OpenVAs using a web browser on the next screen:



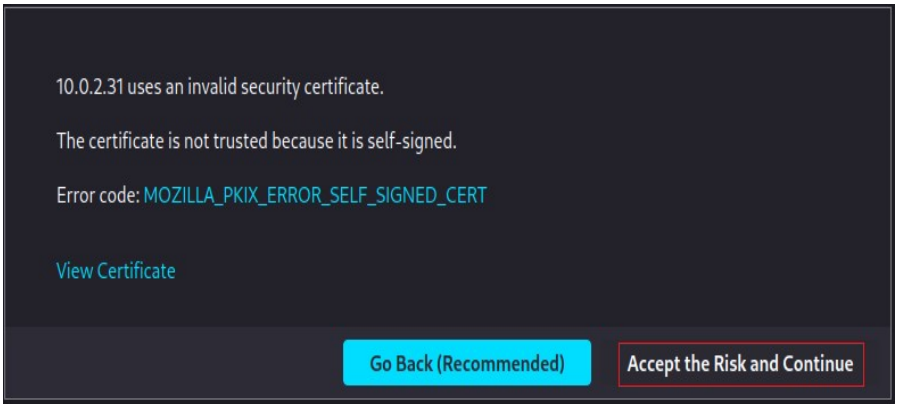
Open a browser on your Kali machine. Then, in the address bar, type the address just as displayed in the About GSM window.

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

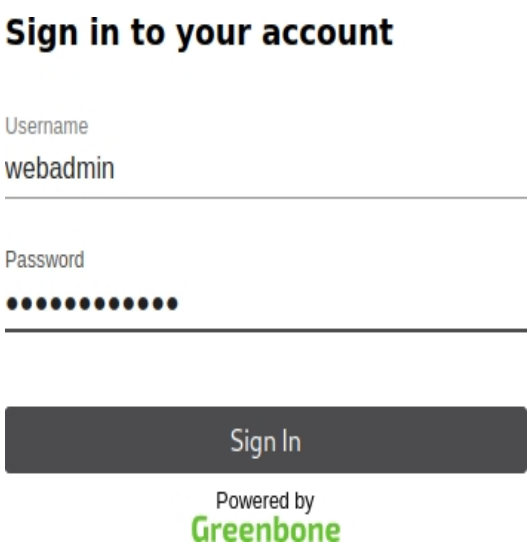




Scroll to the bottom of the screen; click the button labeled **Accept the Risk and Continue.**

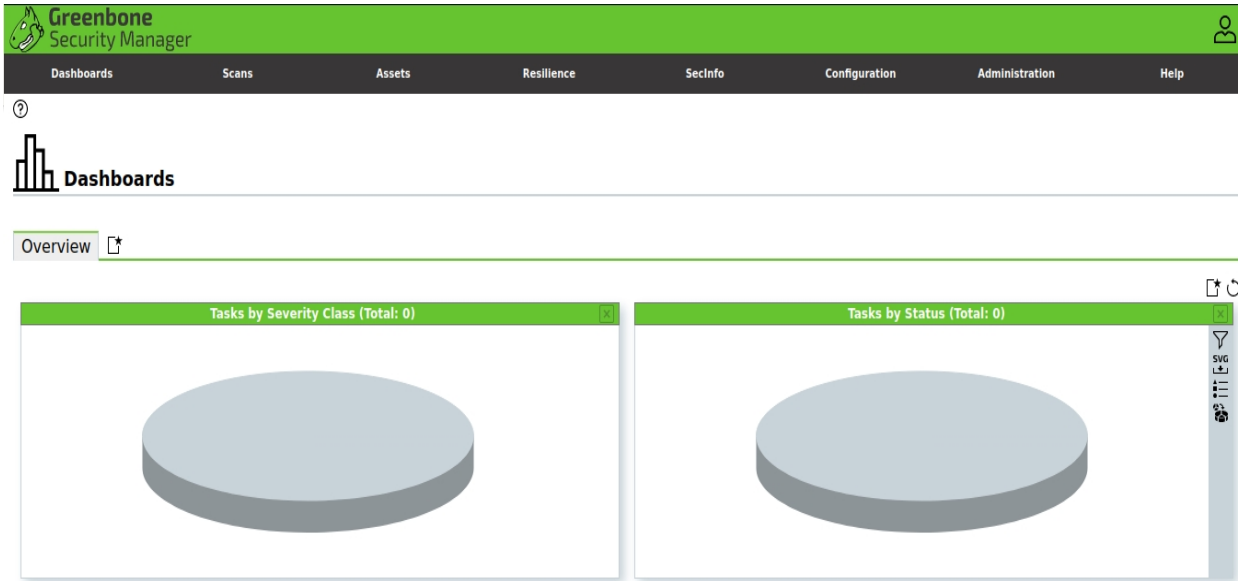


On the login page, type in your webadmin account name and password.



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

This opens your OpenVAS dashboard.



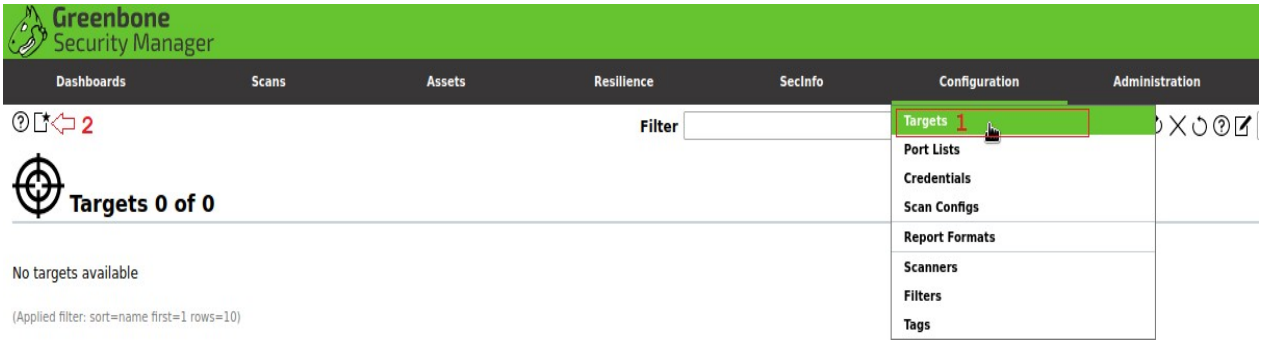
Creating a Target in OpenVAS

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’.

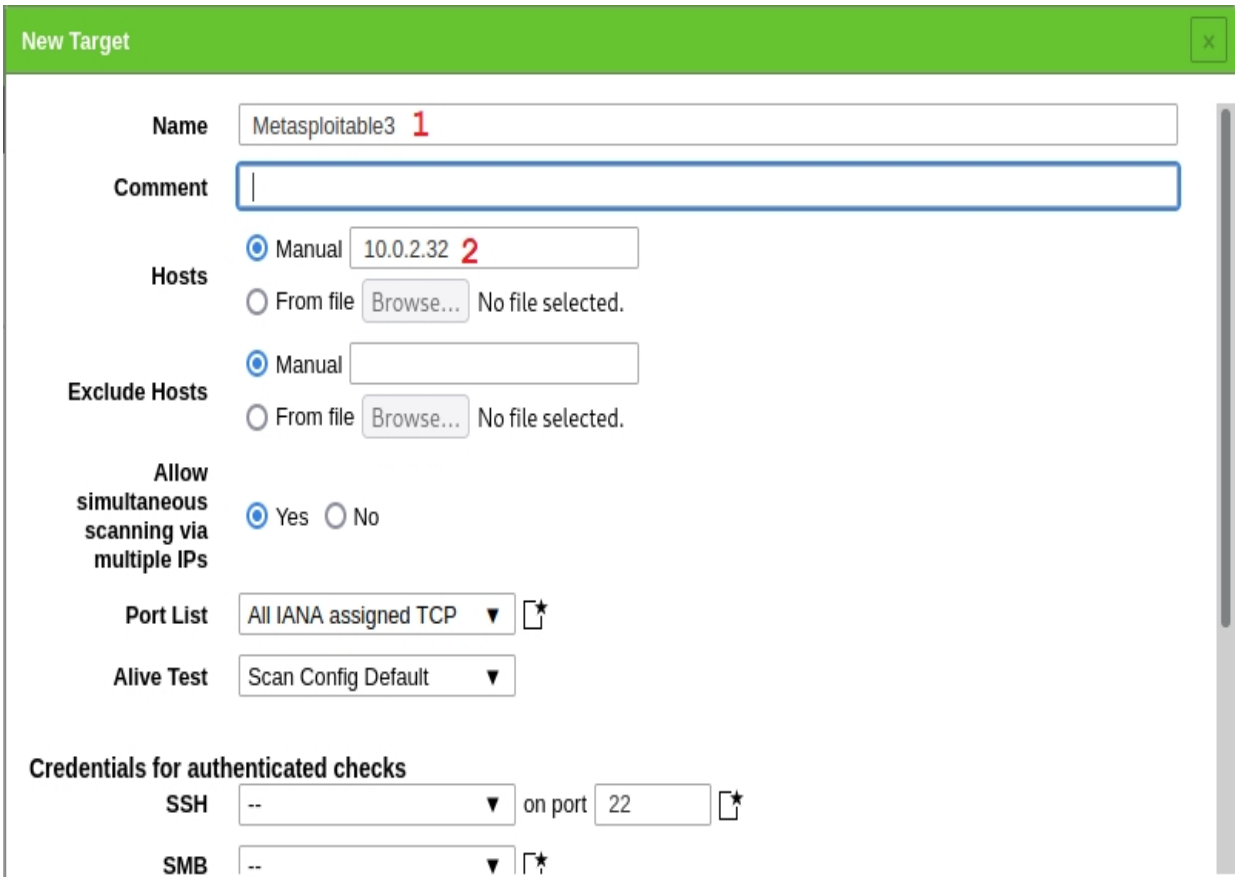
Click the black icon in the top left corner to create a new target.



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.



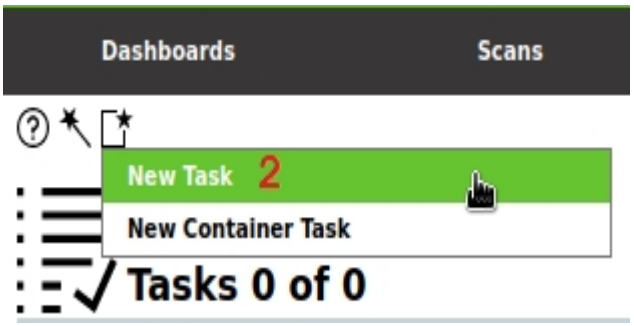

Cancel
3
Save

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

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:

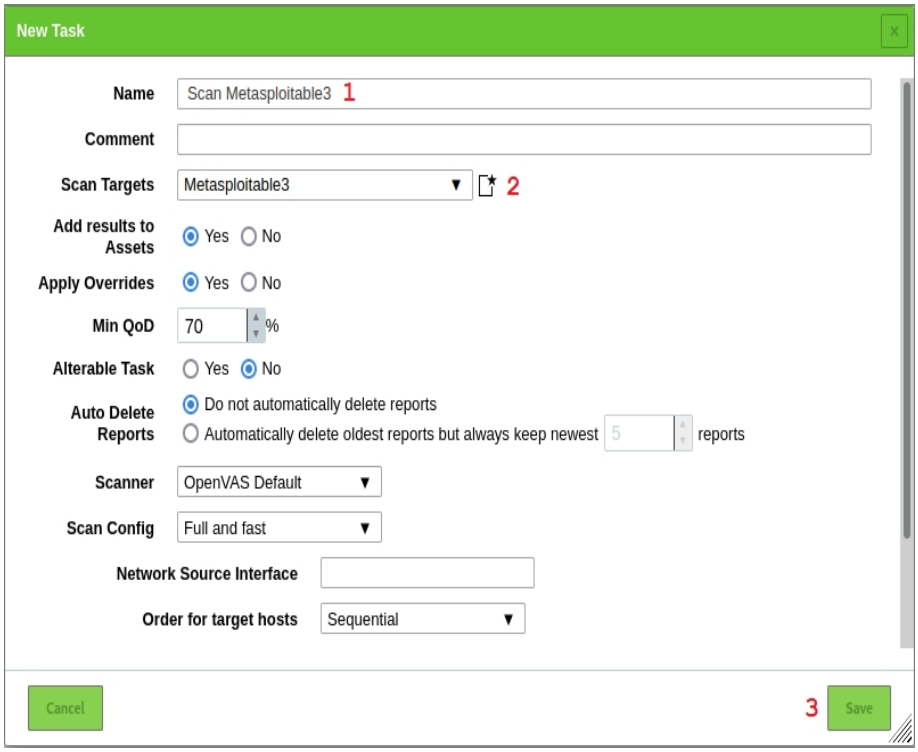
1. Go to 'Scans' in the top menu and select 'Tasks'.
2. Point to the black icon in the top left corner and select 'New Task'.



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

- Task name, we'll name it 'Scan Metasploitable3'
- Make sure that the Metasploitable3 target we have created earlier is selected
- Keep all other settings default and click the 'Save' button to create the new task

tash

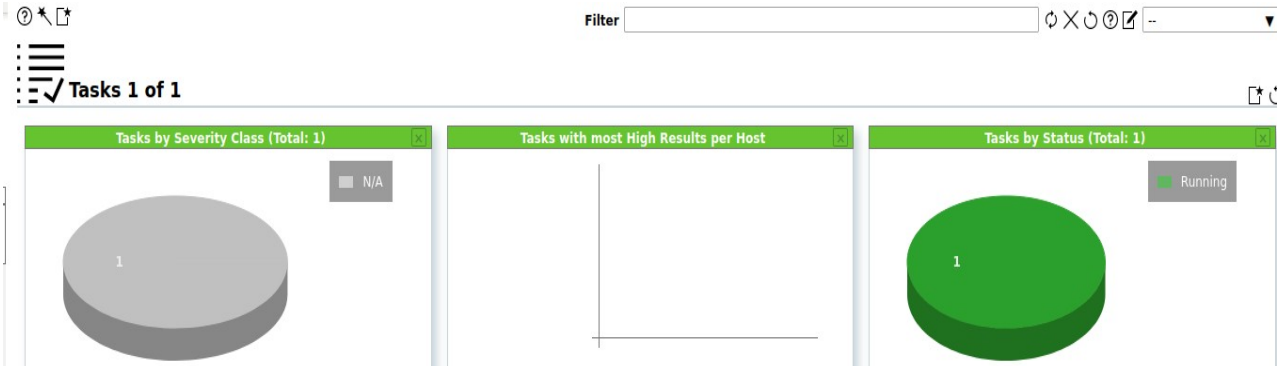


The newly created task will now appear at the bottom of the task list.

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.)



Results per Host

1 - 1 of 1

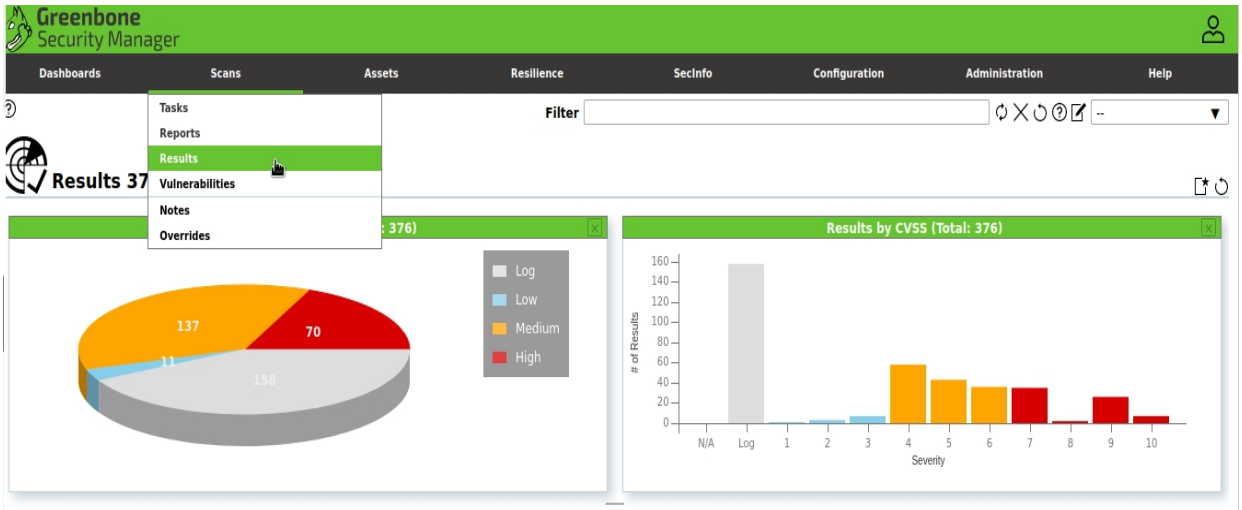
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan Metasploitable3	2 %	1				

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 1 of 1

When the scan task has finished, the status changes to ‘Done’.
To view the scan results, click Scans from the taskbar and select Results from the context menu:



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Apache Axis2 Default Credentials (HTTP)	10.0 (High)	98 %	10.0.2.32		8282/tcp	Mon, May 23, 2022 7:06 AM UTC
ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	10.0.2.32		8022/tcp	Mon, May 23, 2022 6:41 AM UTC
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.32		9200/tcp	Mon, May 23, 2022 6:34 AM UTC
MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)	10.0 (High)	95 %	10.0.2.32		80/tcp	Mon, May 23, 2022 7:11 AM UTC
ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	10.0.2.32		8383/tcp	Mon, May 23, 2022 6:41 AM UTC
Apache Tomcat End of Life (EOL) Detection (Windows)	10.0 (High)	80 %	10.0.2.32		8282/tcp	Mon, May 23, 2022 6:21 AM UTC
ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	10.0.2.32		8020/tcp	Mon, May 23, 2022 6:41 AM UTC
ManageEngine Desktop Central < 10.0.092 RCE Vulnerability	9.8 (High)	80 %	10.0.2.32		8022/tcp	Mon, May 23, 2022 6:41 AM UTC
Ruby on Raily < 5.2.4.3, 6.x < 6.0.3.1 Multiple Vulnerabilities (Windows)	9.8 (High)	80 %	10.0.2.32		3000/tcp	Mon, May 23, 2022 6:50 AM UTC
ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability	9.8 (High)	80 %	10.0.2.32		8020/tcp	Mon, May 23, 2022 6:41 AM UTC

Apply to page contents

Applied filter: apply_overrides=0 min_qod=70 sort-reverse=severity rows=10 first=1)

1 - 10 of 376

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

Summary

The remote Apache Axis2 web interface is using known default credentials.

Detection Result

Vulnerability was detected according to the Detection Method.

Insight

It was possible to login with default credentials: admin/axis2

Detection Method

Try to login with default credentials.

Details: Apache Axis2 Default Credentials (HTTP) OID: 1.3.6.1.4.1.25623.1.0.111006

Version used: 2022-04-14T06:42:08Z

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration or execute code by uploading malicious webservices.

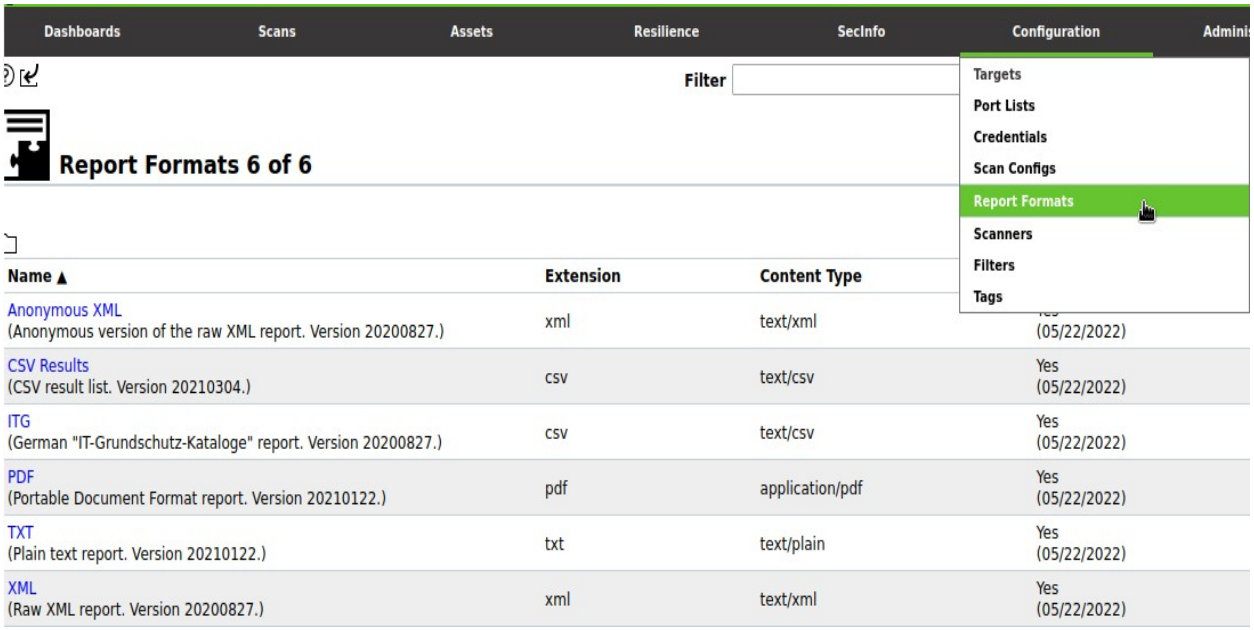
Solution

Solution Type: Mitigation
Change the password.

References

Generating Reports

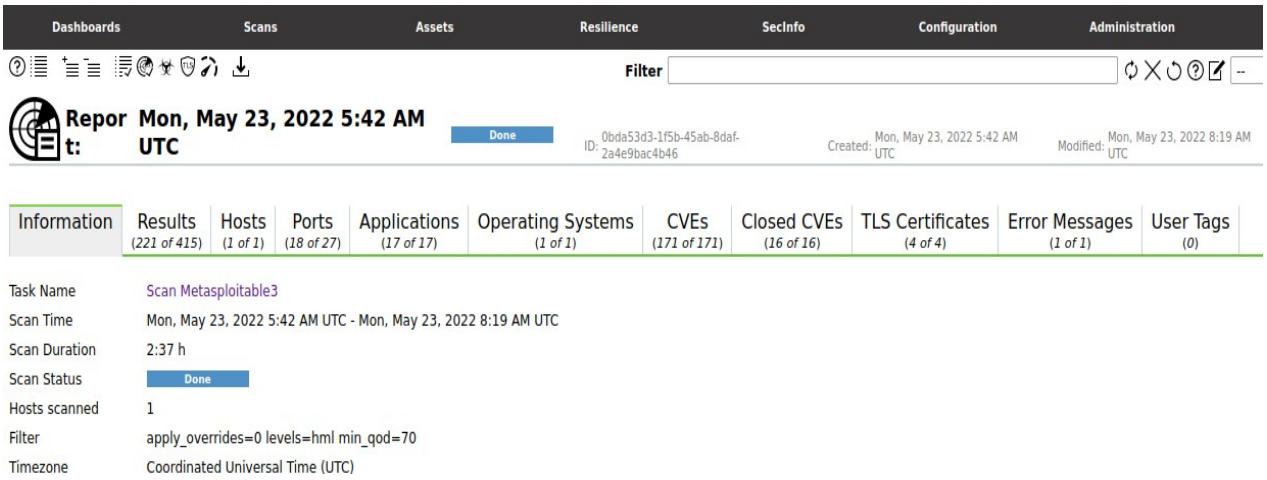
Under Configuration>Report Formats, you can generate one of six formatted scan reports:



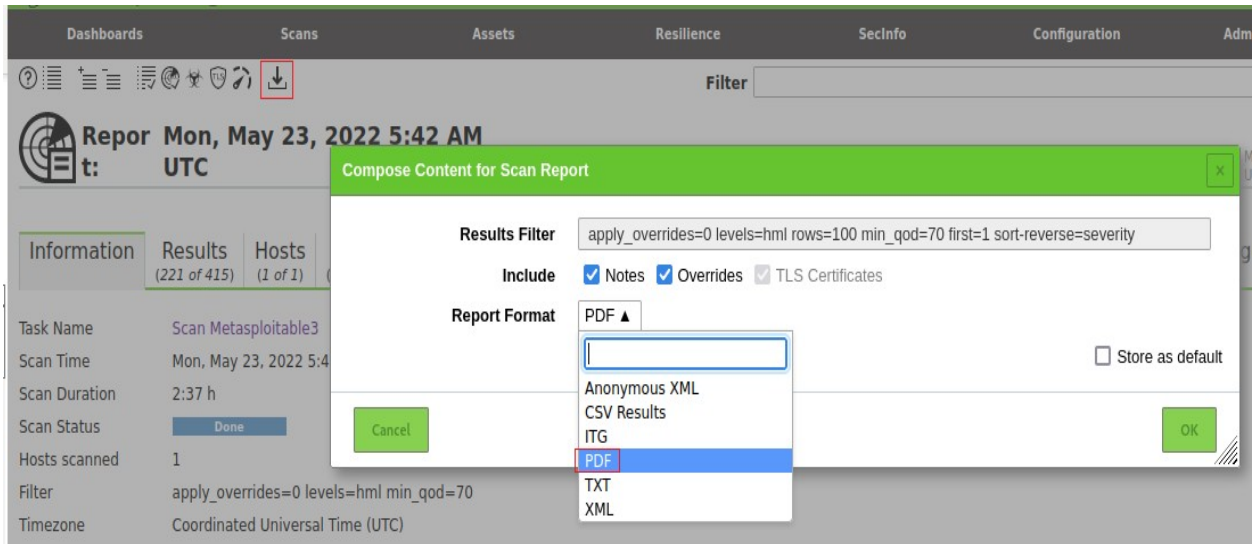
To download your scan results as a report, under Scans>reports, click on the date of the scan:

Date ▼	Status	Task	Severity
Mon, May 23, 2022 5:42 AM UTC	Done	Scan Metasploitable3	10.0 (High)

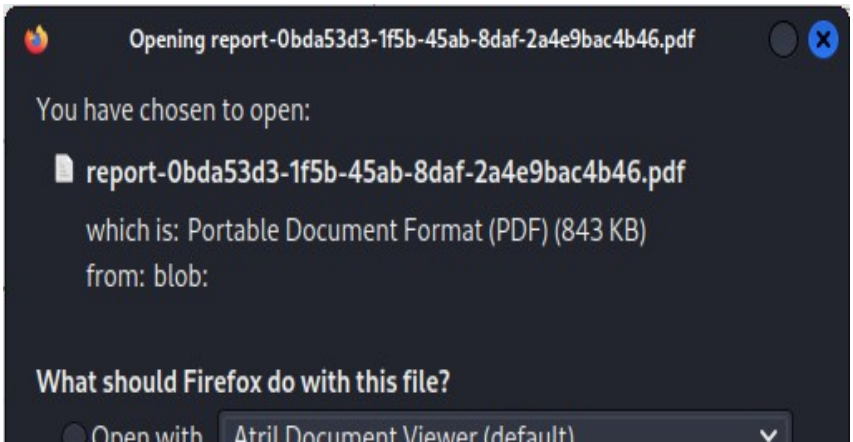
On the next page, you can see all the information included in the scan report.

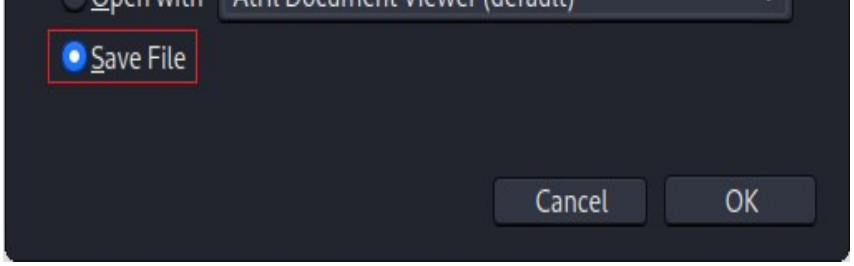


In the top left corner, click on the download icon. Next, choose your format, and finally, click on OK:

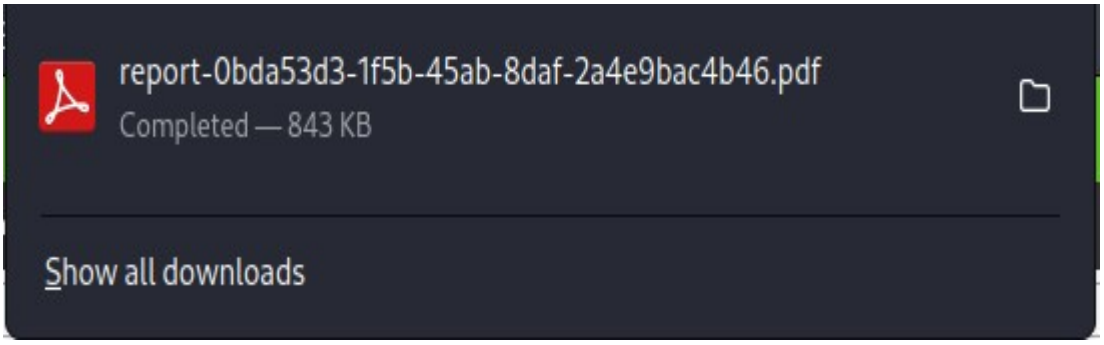


You can choose to open or save the report on the next screen.

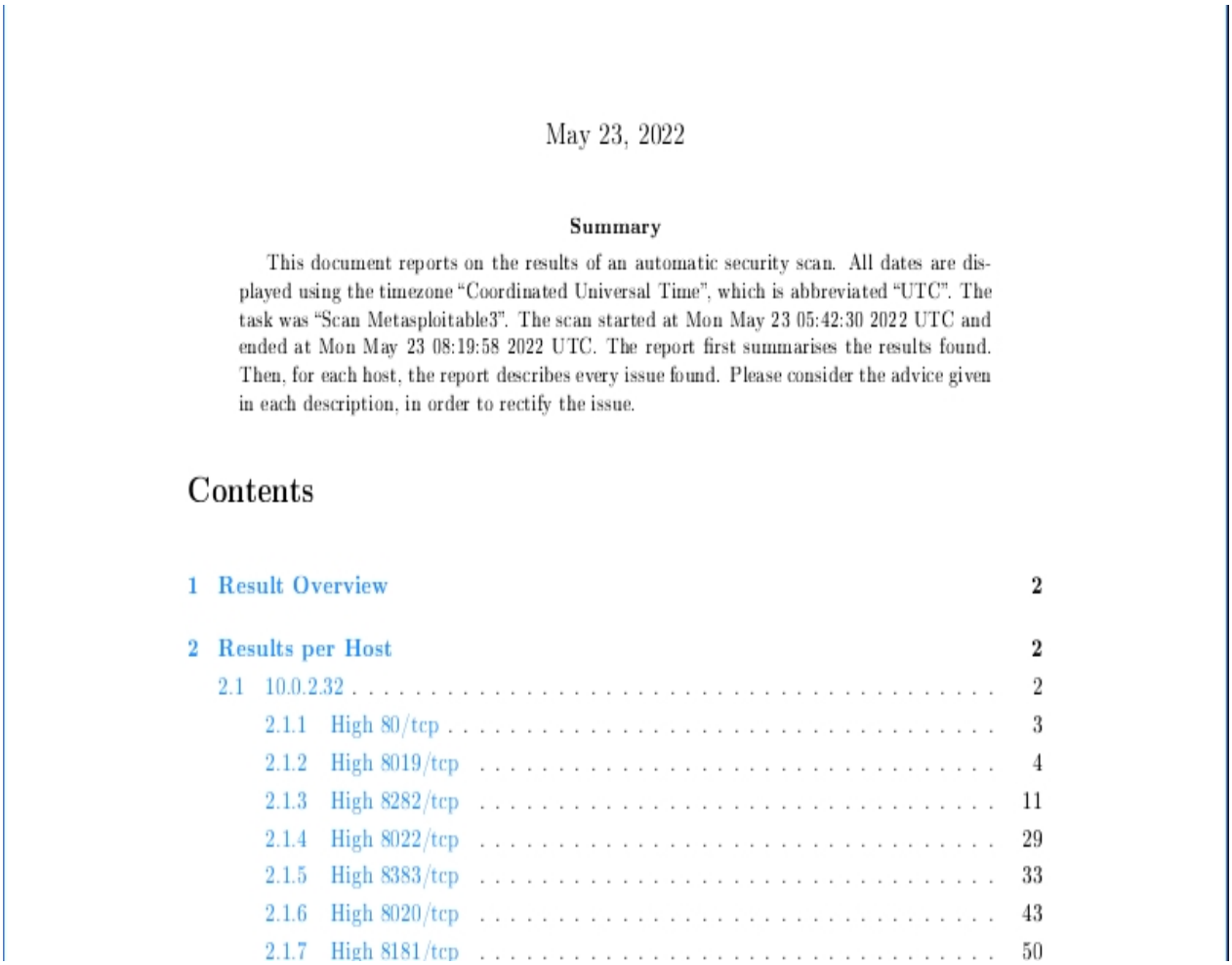



Save File
Cancel
OK

The report is saved to your Downloads.



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.



May 23, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scan Metasploitable3". The scan started at Mon May 23 05:42:30 2022 UTC and ended at Mon May 23 08:19:58 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Summary

OpenVAS is a commercial product that comes with a community edition. OpenVAS may be the

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.