

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.

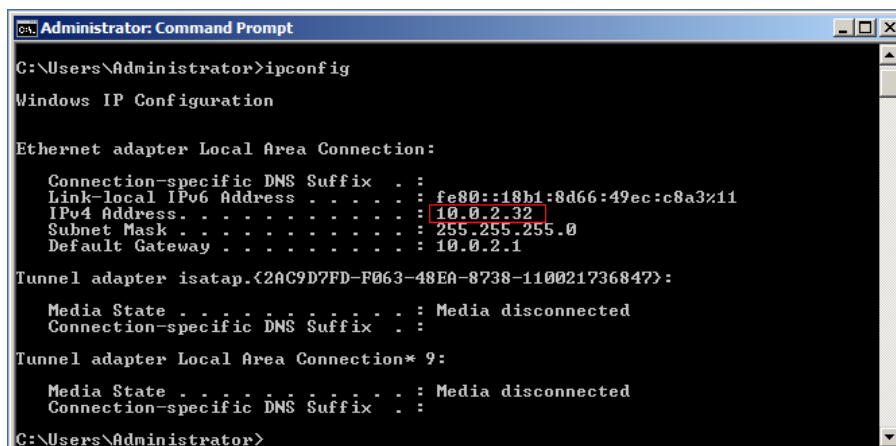
Lab Requirements

- 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.



```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::18b1:8d66:49ec:c8a3%11
    IPv4 Address. . . . . : 10.0.2.32
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter {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 and 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.

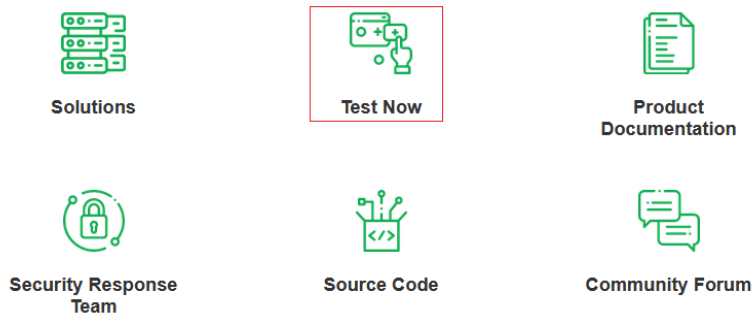
Download OVA file for OpenVAS

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.

Related Links



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

The Greenbone Enterprise TRIAL at a Glance

The Greenbone Enterprise TRIAL allows a quick and easy testing of our appliance solution on Windows/Linux/Mac, even without special know-how. In contrast to the commercial solution, the Greenbone Community Feed is used instead of the [Greenbone Enterprise Feed](#) and some management functions are not included (e.g., TLS certificates).

The Greenbone Enterprise TRIAL is available for different virtual environments: VMware Workstation Player, VMware Workstation Pro and Oracle Virtual Box.

[Download Now](#)



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

Oracle VirtualBox

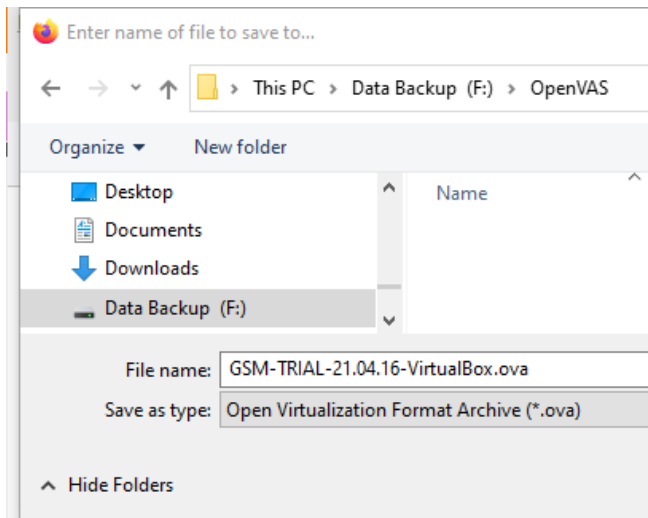
1. Instruction
2. Note
3. Download

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

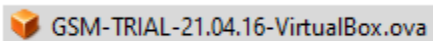
Importing the Greenbone Enterprise TRIAL

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

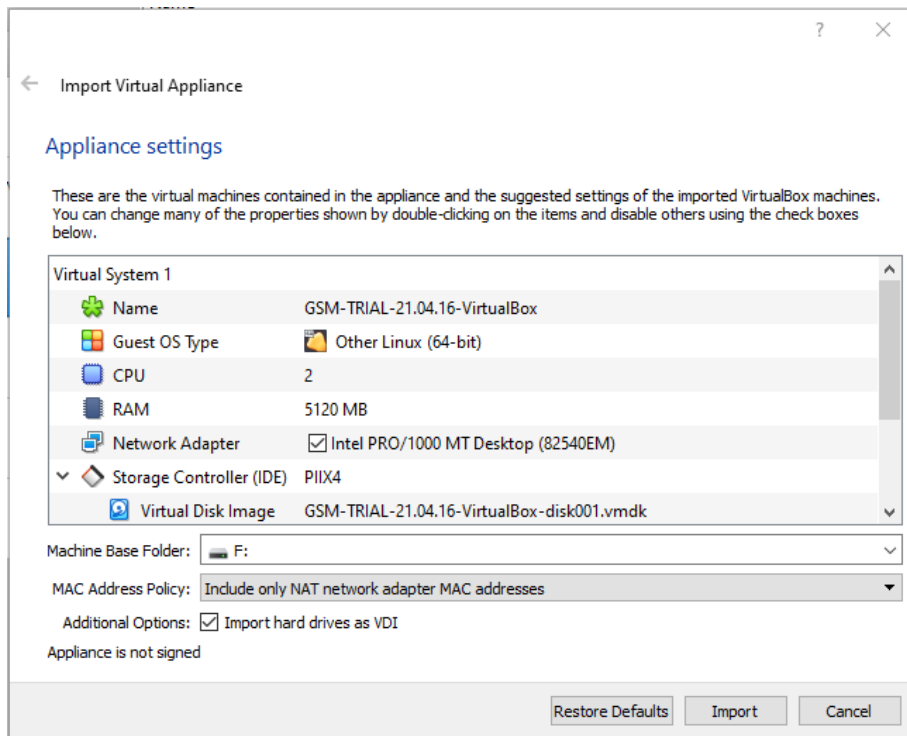
Save the OVA file to your local machine. I saved y download to a folder labeled OpenVAS situated on my storage drive. Of course, you are free to save yours as you wish.



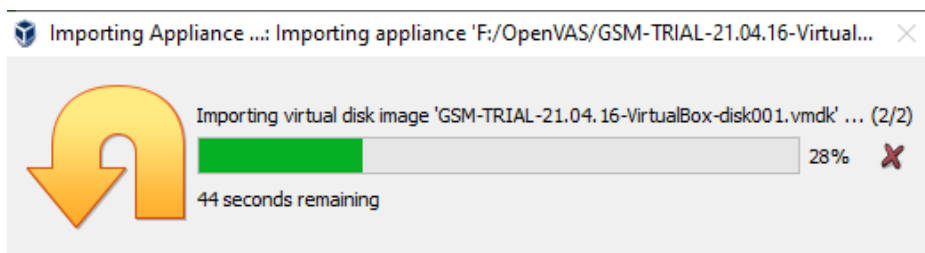
Once the OVA has been downloaded, find the file and x2 click to import into VirtualBox.



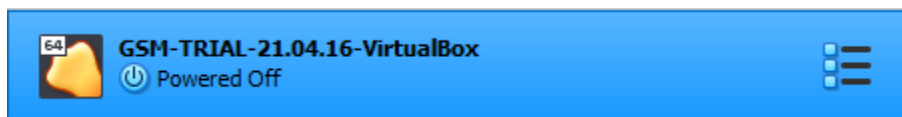
Accept the findings of the Import Appliance Wizard and at the bottom of the screen, click the button labeled **Import**.



Allow the import to complete.

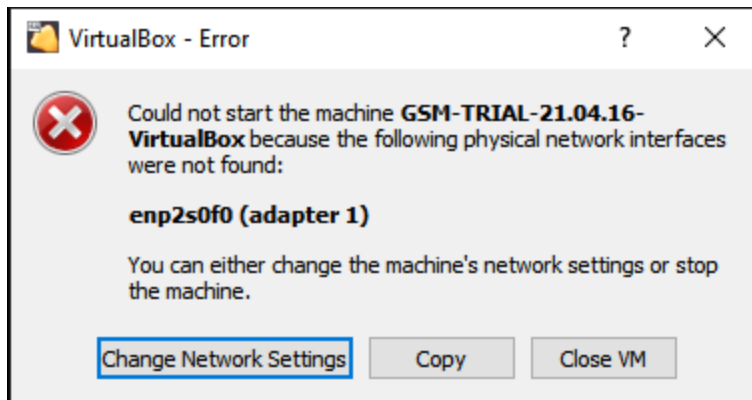


Once the import process has been completed, from your left windowpane of VirtualBox, find the virtual disk labeled GSM-TRIAL-21.04.16-VirtualBox.

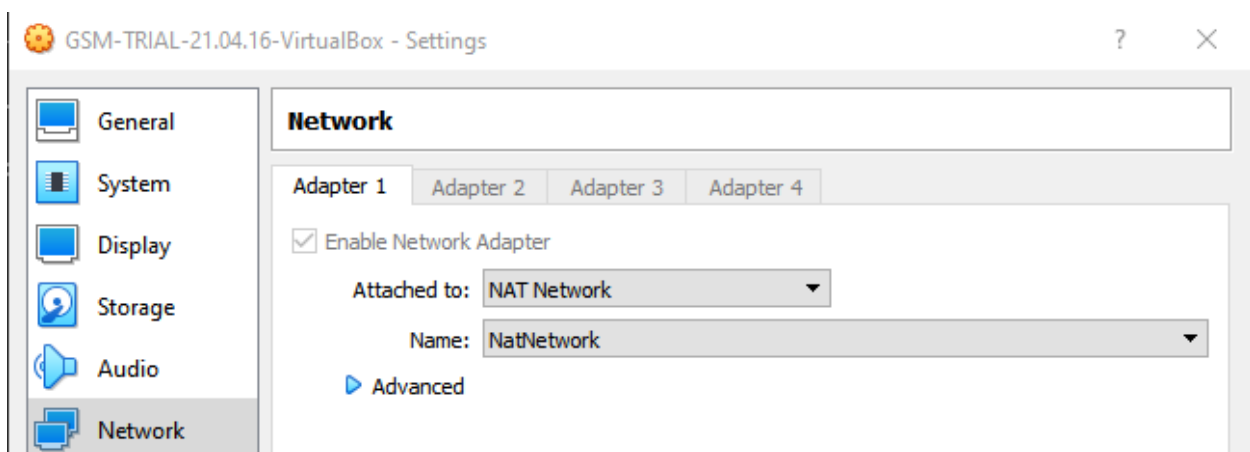


X2 click to launch.

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.

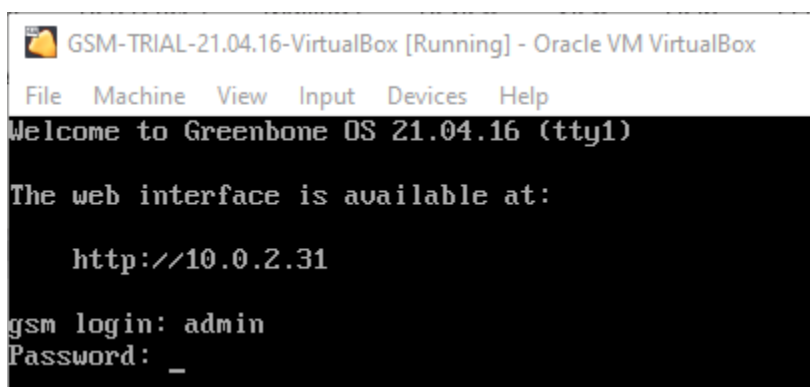


Change the adapter to NAT Network and click OK.

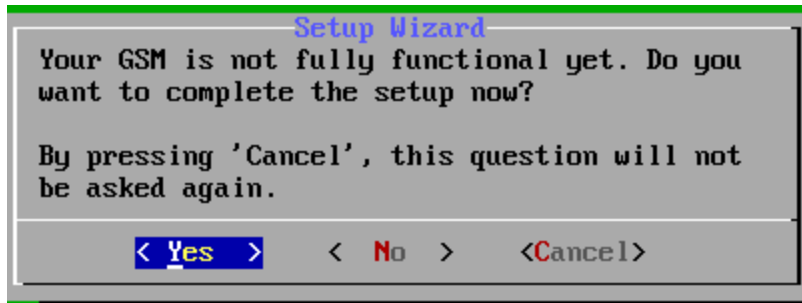


At the terminal prompt, type in **admin** for both the username and password.

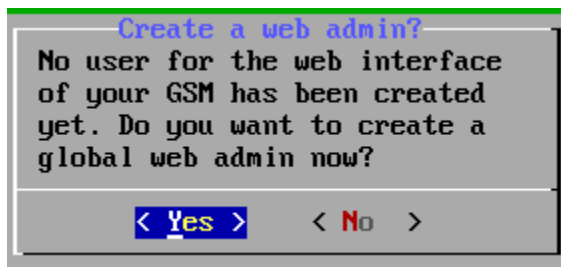
This Linux. You will not see the password being typed in at the prompt.



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

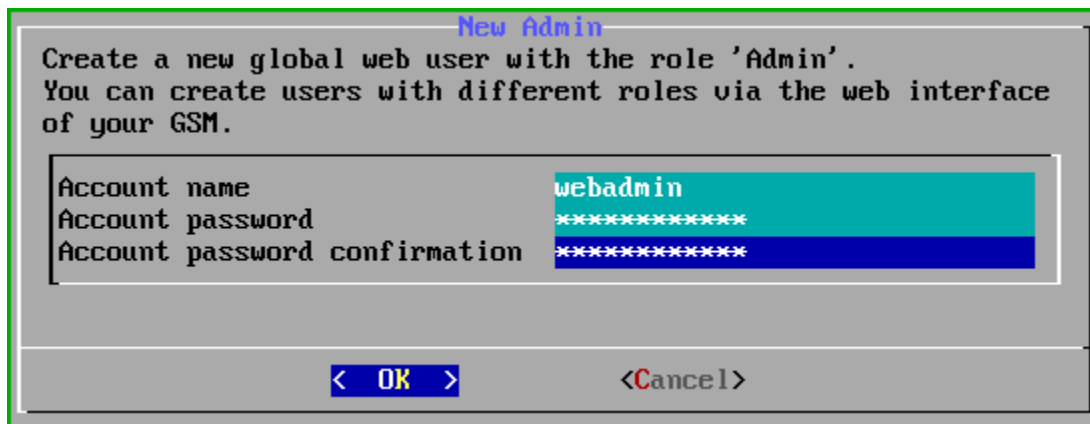


On the next screen, click Yes to create a web admin account.



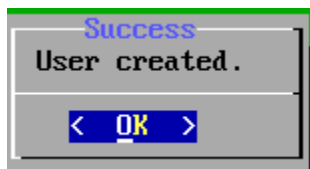
On the next screen, create your webadmin account. Remember the password!

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

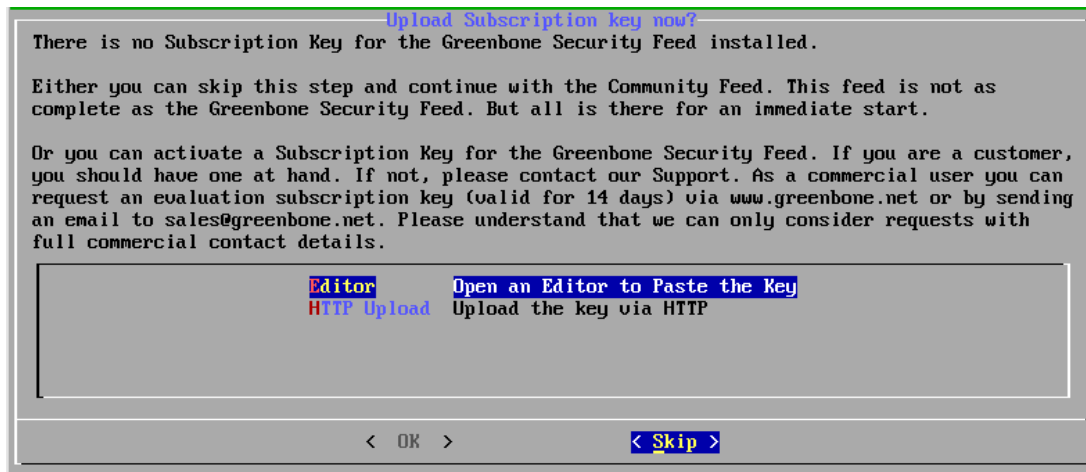


Use your TAB key to highlight the OK button and then press enter.

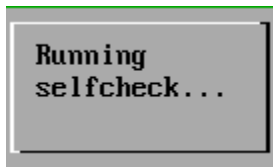
User created.



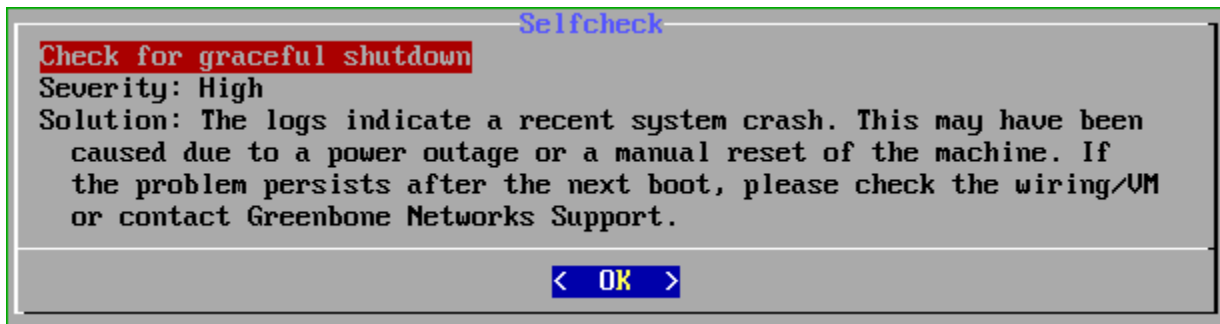
On the next screen, you will be asked for your subscription key. Since we want to use the community edition, use your TAB or arrow key to highlight the Skip button and press enter.



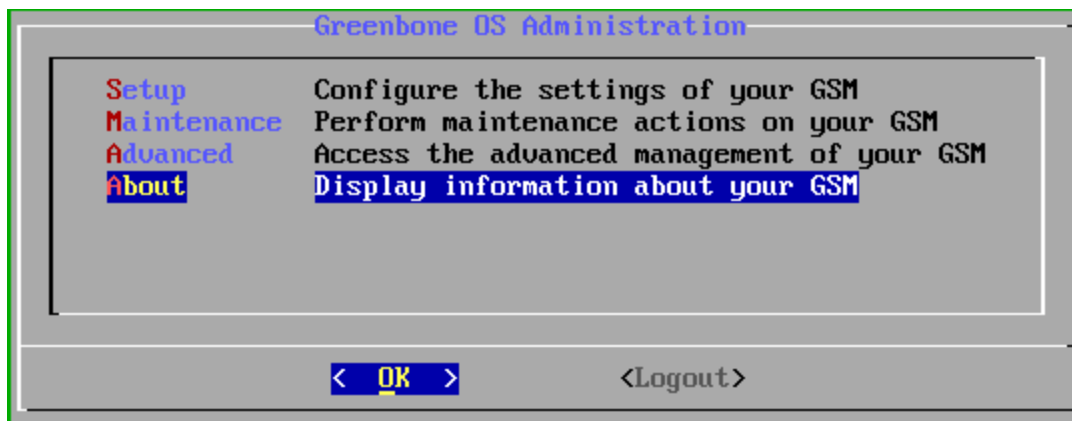
The setup performs a Selfcheck.



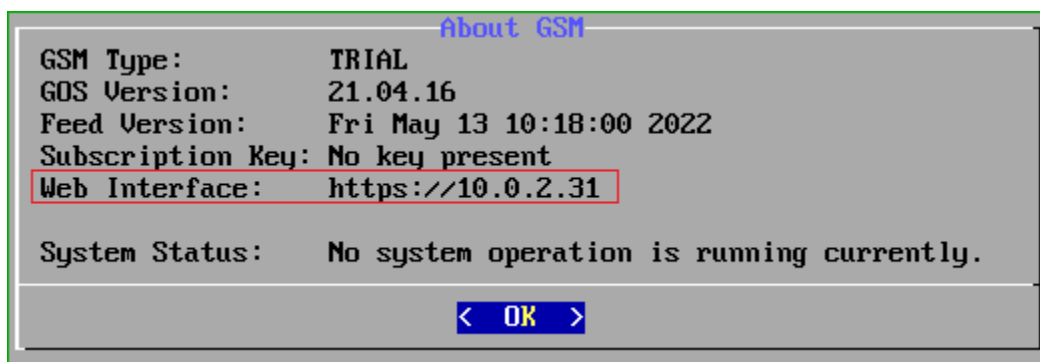
Ignore any warning and press enter.



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

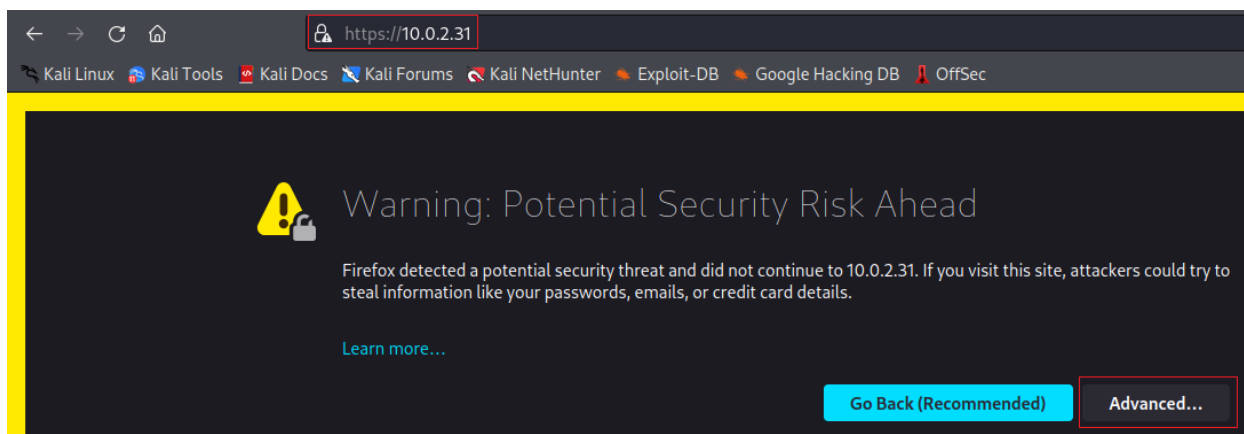


Find the web interface information you need to access OpenVAs using a web browser on the next screen.

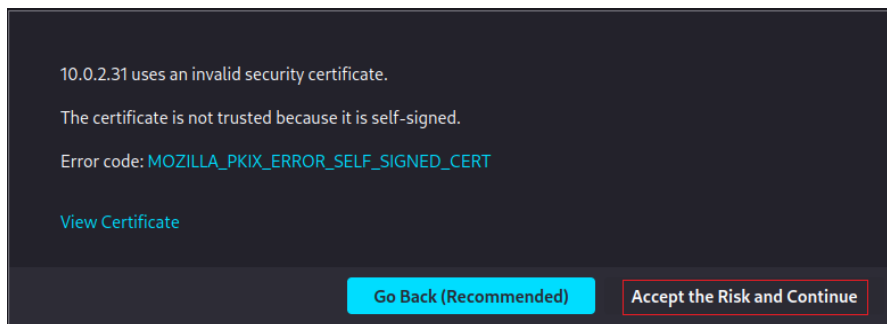


Open a browser on your Kali machine. Then, in the address bar, type the address just as displayed in the About GSM window.

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.

Sign in to your account

Username
webadmin

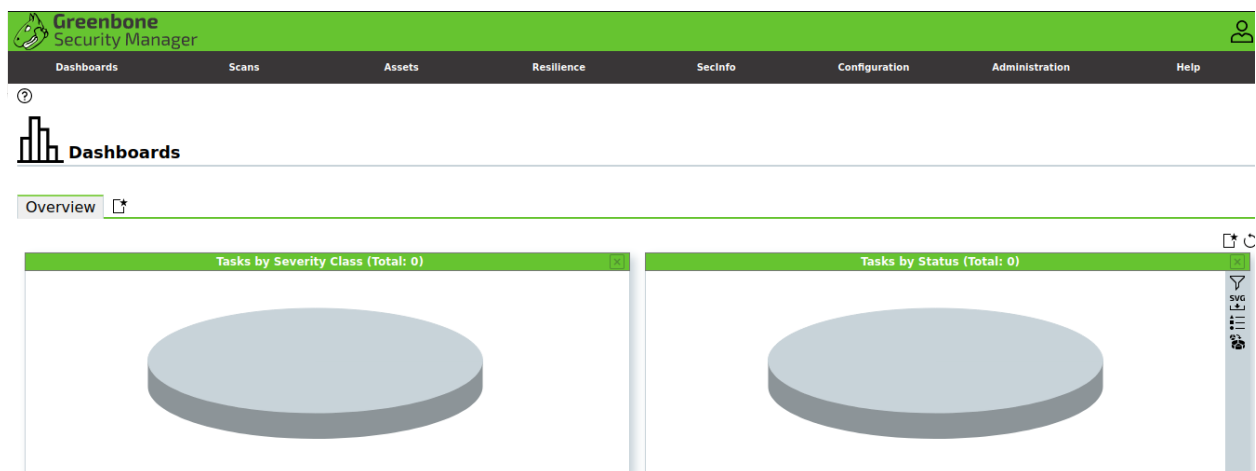
Password
●●●●●●●●

Sign In

Powered by
Greenbone

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

This opens your OpenVAS dashboard.



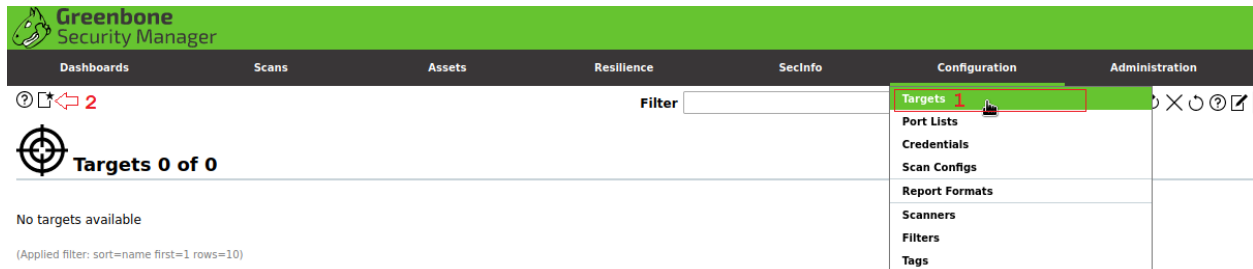
Creating a target in OpenVAS

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.

The screenshot shows the 'New Target' dialog box in Greenbone Security Manager. The dialog has a green header with the title 'New Target' and a close button. The form contains the following fields and options:

- Name:** A text input field containing 'Metasploitable3' with a red number '1' next to it.
- Comment:** An empty text input field.
- Hosts:** A section with two radio buttons: 'Manual' (selected) and 'From file'. The 'Manual' option has a text input field containing '10.0.2.32' with a red number '2' next to it. The 'From file' option has a 'Browse...' button and the text 'No file selected.'
- Exclude Hosts:** A section with two radio buttons: 'Manual' (selected) and 'From file'. The 'Manual' option has an empty text input field. The 'From file' option has a 'Browse...' button and the text 'No file selected.'
- Allow simultaneous scanning via multiple IPs:** A section with two radio buttons: 'Yes' (selected) and 'No'.
- Port List:** A dropdown menu showing 'All IANA assigned TCP' with a star icon to its right.
- Alive Test:** A dropdown menu showing 'Scan Config Default'.
- Credentials for authenticated checks:** A section with two rows: 'SSH' and 'SMB'. Each row has a dropdown menu showing '--' and a text input field for the port. The 'SSH' row has a port of '22' and a star icon to its right.

At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save'. The 'Save' button is highlighted with a red number '3' next to it.

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

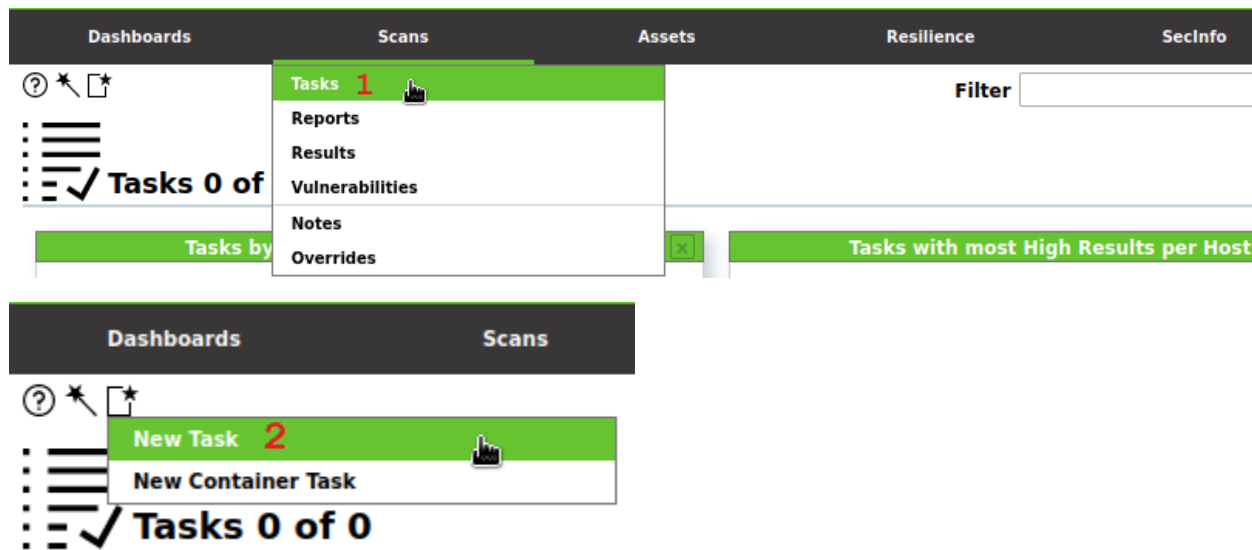


Name ▲	Hosts	IPs	Port List
Metasploitable3	10.0.2.32	1	All IANA assigned TCP

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.

New Task

Name

Scan Metasploitable3 1

Comment

Scan Targets

Metasploitable3 2

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

Cancel

3 Save

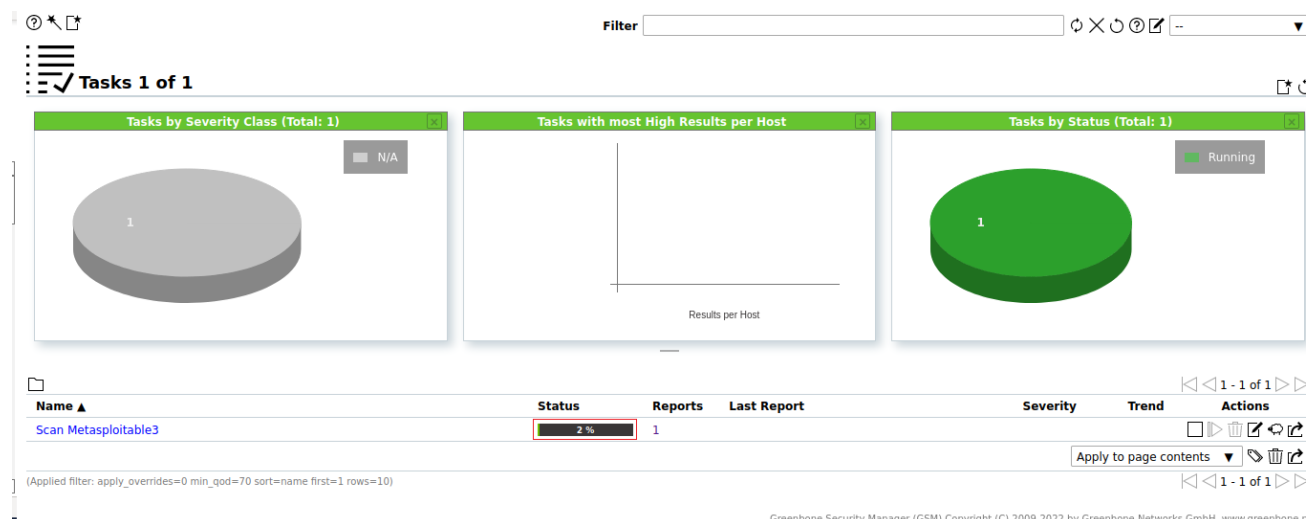
The newly created task will now appear at the bottom of the task list.

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

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan Metasploitable3	New					▶▶▶▶▶▶

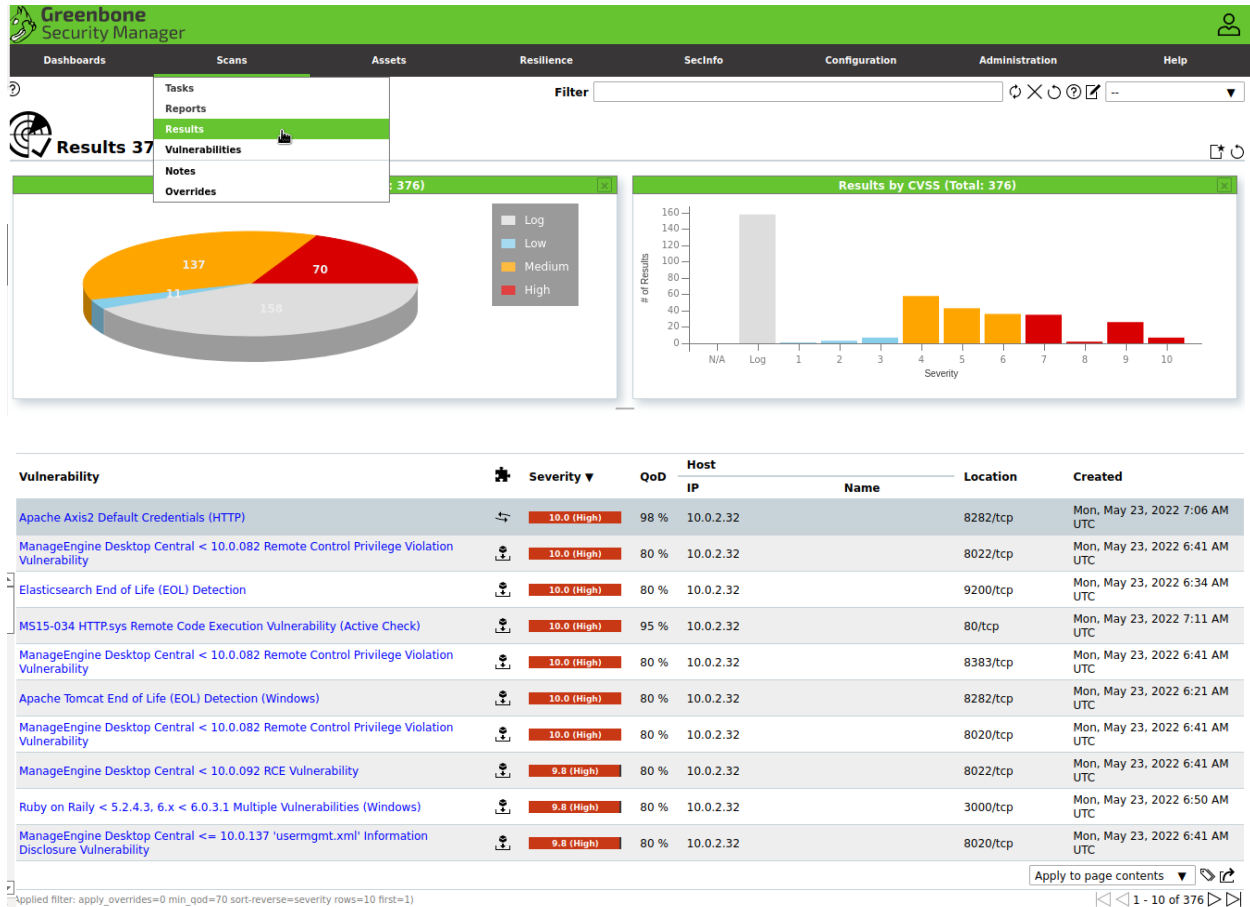
The scan task will now execute against the selected target. Please note that a full scan may take a while to complete. When you refresh the tasks page, you will be able to check the progress of the executed task:

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.



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 webservises.

Solution

Solution Type: ↔ Mitigation
Change the password.

References

Generating Reports

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

Name ▲	Extension	Content Type	
Anonymous XML (Anonymous version of the raw XML report. Version 20200827.)	xml	text/xml	Yes (05/22/2022)
CSV Results (CSV result list. Version 20210304.)	csv	text/csv	Yes (05/22/2022)
ITG (German "IT-Grundschutz-Kataloge" report. Version 20200827.)	csv	text/csv	Yes (05/22/2022)
PDF (Portable Document Format report. Version 20210122.)	pdf	application/pdf	Yes (05/22/2022)
TXT (Plain text report. Version 20210122.)	txt	text/plain	Yes (05/22/2022)
XML (Raw XML report. Version 20200827.)	xml	text/xml	Yes (05/22/2022)

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.

The screenshot shows the Metasploit Framework interface. At the top, there are tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, and Administration. Below the tabs is a search bar and a filter input. The main content area displays the scan report for 'Mon, May 23, 2022 5:42 AM UTC'. The report is titled 'Report' and has a status of 'Done'. The report ID is '0bda53d3-1f5b-45ab-8daf-2a4e9bac4b46'. The report was created on 'Mon, May 23, 2022 5:42 AM UTC' and modified on 'Mon, May 23, 2022 8:19 AM UTC'. The report is categorized into several sections: Information, Results (221 of 415), Hosts (1 of 1), Ports (18 of 27), Applications (17 of 17), Operating Systems (1 of 1), CVEs (171 of 171), Closed CVEs (16 of 16), TLS Certificates (4 of 4), Error Messages (1 of 1), and User Tags (0). The 'Information' section is expanded, showing details such as Task Name (Scan Metasploitable3), Scan Time (Mon, May 23, 2022 5:42 AM UTC - Mon, May 23, 2022 8:19 AM UTC), Scan Duration (2:37 h), Scan Status (Done), Hosts scanned (1), Filter (apply_overrides=0 levels=hml min_qod=70), and Timezone (Coordinated Universal Time (UTC)).

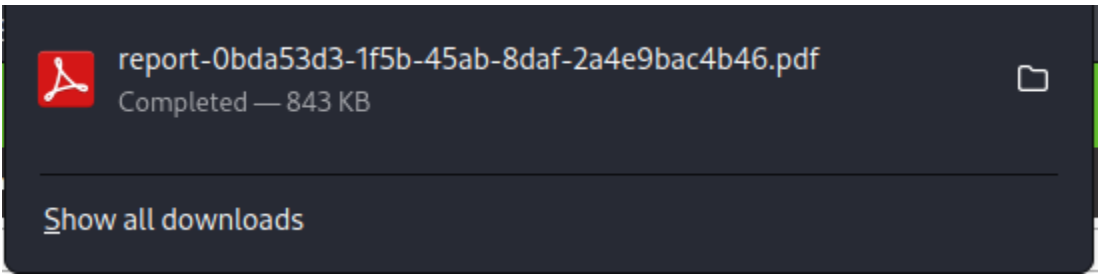
In the top left corner, click on the download icon. Next, choose your format, and finally, click OK.

The screenshot shows the Metasploit Framework interface with the 'Compose Content for Scan Report' dialog box open. The dialog box has a green header and a white body. It contains a 'Results Filter' input field with the value 'apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse=severity'. Below the filter is an 'Include' section with checkboxes for 'Notes', 'Overrides', and 'TLS Certificates', all of which are checked. The 'Report Format' section shows a dropdown menu with 'PDF' selected. Other options in the dropdown are 'Anonymous XML', 'CSV Results', 'ITG', 'TXT', and 'XML'. There is a 'Store as default' checkbox on the right. The dialog box has 'Cancel' and 'OK' buttons at the bottom.

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

The screenshot shows a Firefox file dialog box titled 'Opening report-0bda53d3-1f5b-45ab-8daf-2a4e9bac4b46.pdf'. The dialog box has a dark background and white text. It says 'You have chosen to open:' followed by the file name 'report-0bda53d3-1f5b-45ab-8daf-2a4e9bac4b46.pdf' and its details 'which is: Portable Document Format (PDF) (843 KB) from: blob:'. Below this is a section titled 'What should Firefox do with this file?' with two radio button options: 'Open with' (selected) and 'Save File'. The 'Open with' option has a dropdown menu showing 'Atril Document Viewer (default)'. The 'Save File' option is highlighted with a red box. At the bottom are 'Cancel' and 'OK' buttons.

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	
1	Result Overview 2
2	Results per Host 2
2.1	10.0.2.32 2
2.1.1	High 80/tcp 3
2.1.2	High 8019/tcp 4
2.1.3	High 8282/tcp 11
2.1.4	High 8022/tcp 29
2.1.5	High 8383/tcp 33
2.1.6	High 8020/tcp 43
2.1.7	High 8181/tcp 50

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.

