



## CySA+ Lab Series

### Lab 05: Vulnerability Scanning

Document Version: **2022-10-10**

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.1 - Explain the importance of threat data and intelligence 1.2 - Given a scenario, utilize threat intelligence to support organizational security 1.3 - Given a scenario, perform vulnerability management activities 1.4 - Given a scenario, analyze the output from vulnerability tools 1.6 - Explain the threats and vulnerabilities associated with operating in the cloud 1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities 3.3 - Explain the importance of proactive threat hunting
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	1: The Importance of Threat Data and Intelligence 2: Threat Intelligence in Support of Organizational Security 3: Vulnerability Management Activities 4: Vulnerability Assessment Tools 6: Threats and Vulnerabilities Associated with Operating in the Cloud 7: Mitigating Controls for Attacks and Software Vulnerabilities 13: The Importance of Proactive Threat Hunting

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.  
KALI LINUX™ is a trademark of Offensive Security.  
ALIEN VAULT OSSIM V is a trademark of AlienVault, Inc.  
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.  
Greenbone is a trademark of Greenbone Networks GmbH.  
SECURITY ONION is a trademark of Security Onion Solutions LLC.  
Android is a trademark of Google LLC.  
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").  
All trademarks, logos, and brand names are the property of their respective owners.

## Contents

Introduction .....	3
Objective .....	3
Lab Topology .....	4
Lab Settings .....	5
1    Enable OpenVAS Services .....	6
2    Configure and Run a Vulnerability Task.....	8
3    Review the Vulnerability Scan Results.....	16
4    Compile a Report on Scan Results .....	24

## Introduction

Scanning a network for vulnerabilities is a major part of a security analyst's job. According to Rapid7, which provides cybersecurity tools and services:

*"Network vulnerability scanning is the process of identifying weaknesses on a computer, network, or other IT asset that are potential targets for exploitation by threat actors. Scanning your environment for vulnerabilities informs you of your current risk posture, the effectiveness of your security measures, and opportunities to improve your defenses through vulnerability remediation."*

*"To face modern attackers, it's no longer enough to build high walls and wait out a siege; modern security programs have to identify the holes that they could exploit and seal them up before threat actors can take advantage."* <https://www.rapid7.com/solutions/network-vulnerability-scanner/>

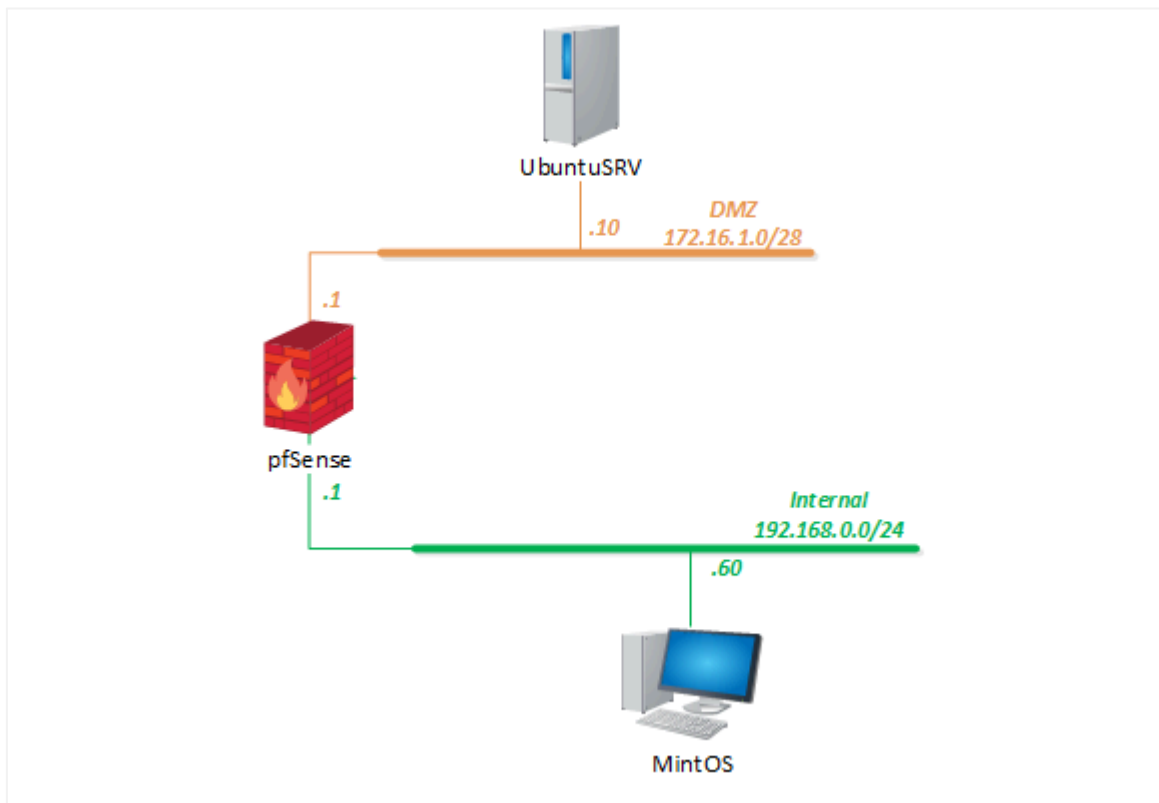
There are many tools, both commercial and open source, that can perform vulnerability scanning. In this lab, you will be using OpenVAS (Open Vulnerability Assessment Scanner) to perform security assessments. OpenVAS uses Network Vulnerability Tests (NVTs) to check for existing security issues on end devices and network devices. These NVTs are based on Common Vulnerabilities and Exposures (CVEs), which is a public listing of known computer security issues. Each CVE is assigned an identification number which allows the data to be shared across different vulnerability tools, such as OpenVAS and Nessus, and are associated with the Common Vulnerability Scoring System (CVSS). The CVSS provides a method for capturing the characteristics of the vulnerability and produces a score that reflects the severity of the vulnerability.

In this lab, you will use OpenVAS to walk through the steps in identifying vulnerabilities found within a network and identify the severity of each of the vulnerabilities while at the same time being able to produce a report on the findings.

## Objective

- Scanning with OpenVAS
- Analyze CVSS Vector
- Remediate the Vulnerability
- Compiling a Report

## Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	192.168.0.50	Administrator	NDGlabpass123!
MintOS (Linux Mint)	192.168.0.60	sysadmin	NDGlabpass123!
OSSIM (Alien Vault)	172.16.1.2	root	NDGlabpass123!
UbuntuSRV (Ubuntu Server)	172.16.1.10	sysadmin	NDGlabpass123!
Kali	203.0.113.2	sysadmin	NDGlabpass123!
pfSense	203.0.113.1 172.16.1.1 192.168.0.1	admin	NDGlabpass123!

## 1 Enable OpenVAS Services



*OpenVAS* has already been installed on the *UbuntuSRV* computer. The *OpenVAS* installation is complex, time consuming, and requires internet access.

1. Set the focus to the **UbuntuSRV** and log in as **sysadmin** with the password: **NDGlabpass123!**

```
Ubuntu 20.04.3 LTS ubuntu:~$ ssh sysadmin@ubuntusrv
ubuntusrv login: sysadmin
Password: _
```

2. Enter the following commands to start the *OpenVAS Scanner* daemon **osspd-openvas**.

```
sudo systemctl start ospd-openvas
```

If asked for the **[sudo]** password for **sysadmin**, enter: **NDGlabpass123!**

```
sysadmin@ubuntusrv:~$ sudo systemctl start ospd-openvas
```

3. Check the status of the **osspd-openvas** service with the following command:

```
sudo systemctl status ospd-openvas
```

Look for the **Active** status. If it says **active (running)** then the service started correctly.

```
sysadmin@ubuntusrv:~$ sudo systemctl status ospd-openvas
• ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (osspd-openvas)
   Loaded: loaded (/etc/systemd/system/ospd-openvas.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-03-01 18:43:59 UTC; 9min ago
     Docs: man:ospd-openvas(8)
           man:openvas(8)
   Process: 1404 ExecStart=/usr/local/bin/ospd-openvas --unix-socket /run/ospd/ospd-openvas.sock
   Main PID: 1422 (osspd-openvas)
    Tasks: 4 (limit: 4612)
   Memory: 778.3M
   CGroup: /system.slice/ospd-openvas.service
           └─1422 /usr/bin/python3 /usr/local/bin/ospd-openvas --unix-socket /run/ospd/ospd-openvas.sock
             └─1424 /usr/bin/python3 /usr/local/bin/ospd-openvas --unix-socket /run/ospd/ospd-openvas.sock

Mar 01 18:43:59 ubuntu:~$ systemctl status ospd-openvas
Mar 01 18:43:59 ubuntu:~$
```

4. Press **Q** to exit the status list.
5. Enter the following commands to start the *Greenbone Vulnerability Manager* daemon **gvmd**.

```
sudo systemctl start gvmd
```

```
sysadmin@ubuntusrv:~$ sudo systemctl start gvmd
```

6. Check the status of the **gvmd** service with the following command:

```
sudo systemctl status gvmd
```

Look for the **Active** status. If it says **active (running)** then the service started correctly.

```
sysadmin@ubuntusrv:~$ sudo systemctl status gvmd
• gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/etc/systemd/system/gvmd.service; disabled; vendor preset: enabled)
  Active: active (running) since Tue 2022-03-01 18:44:07 UTC; 14s ago
    Docs: man:gvmd(8)
  Process: 1434 ExecStart=/usr/local/sbin/gvmd --osp-vt-update=/run/ospd/ospd-openvas.sock --li
 Main PID: 1445 (gvmd)
    Tasks: 1 (limit: 4612)
   Memory: 127.8M
    CGroup: /system.slice/gvmd.service
           └─1445 gvmd: Waiting for incoming connections

Mar 01 18:44:05 ubuntusrv systemd[1]: Starting Greenbone Vulnerability Manager daemon (gvmd)...
Mar 01 18:44:05 ubuntusrv systemd[1]: gvmd.service: Can't open PID file /run/gvm/gvmd.pid (yet?)
Mar 01 18:44:07 ubuntusrv systemd[1]: Started Greenbone Vulnerability Manager daemon (gvmd).
```

7. Press Q to exit the status list.  
8. Enter the following commands to start the *Greenbone Vulnerability Assistant WebUI* service **gsad**.

```
sudo systemctl start gsad
```

```
sysadmin@ubuntusrv:~$ sudo systemctl start gsad
```

9. Check the status of the **gvmd** service with the following command:

```
sudo systemctl status gsad
```

Look for the **Active** status. If it says **active (running)** then the service started correctly.

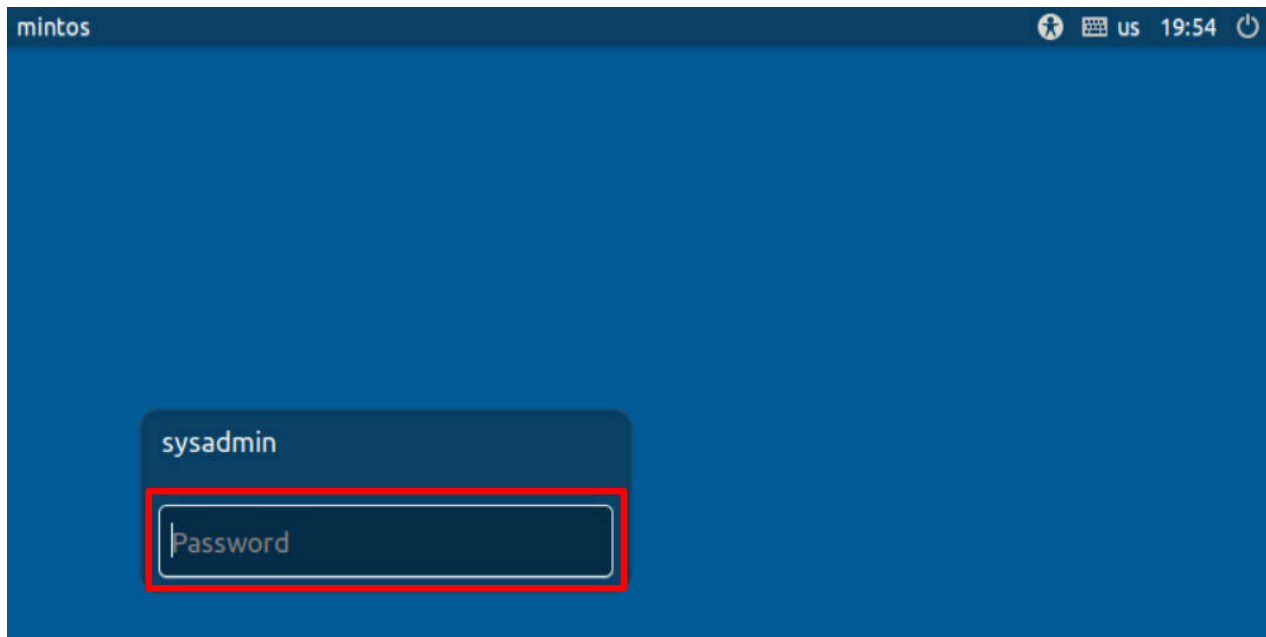
```
sysadmin@ubuntusrv:~$ sudo systemctl status gsad
• gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/etc/systemd/system/gsad.service; disabled; vendor preset: enabled)
  Active: active (running) since Tue 2022-03-01 18:44:45 UTC; 16min ago
    Docs: man:gsad(8)
          https://www.greenbone.net
  Process: 1506 ExecStart=/usr/local/sbin/gsad --listen=172.16.1.10 --port=9392 (code=exited,
 Main PID: 1520 (gsad)
    Tasks: 2 (limit: 4612)
   Memory: 3.3M
    CGroup: /system.slice/gsad.service
           └─1520 /usr/local/sbin/gsad --listen=172.16.1.10 --port=9392

Mar 01 18:44:45 ubuntusrv systemd[1]: Starting Greenbone Security Assistant daemon (gsad)...
Mar 01 18:44:45 ubuntusrv systemd[1]: Started Greenbone Security Assistant daemon (gsad).
```

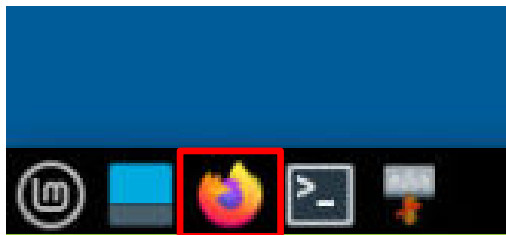
10. Press Q to exit the status list.  
11. The next task will use the **MintOS** computer.

## 2 Configure and Run a Vulnerability Task

1. Change the focus to the **MintOS** computer.
2. Log in as *sysadmin* using the password: NDGLabpass123!



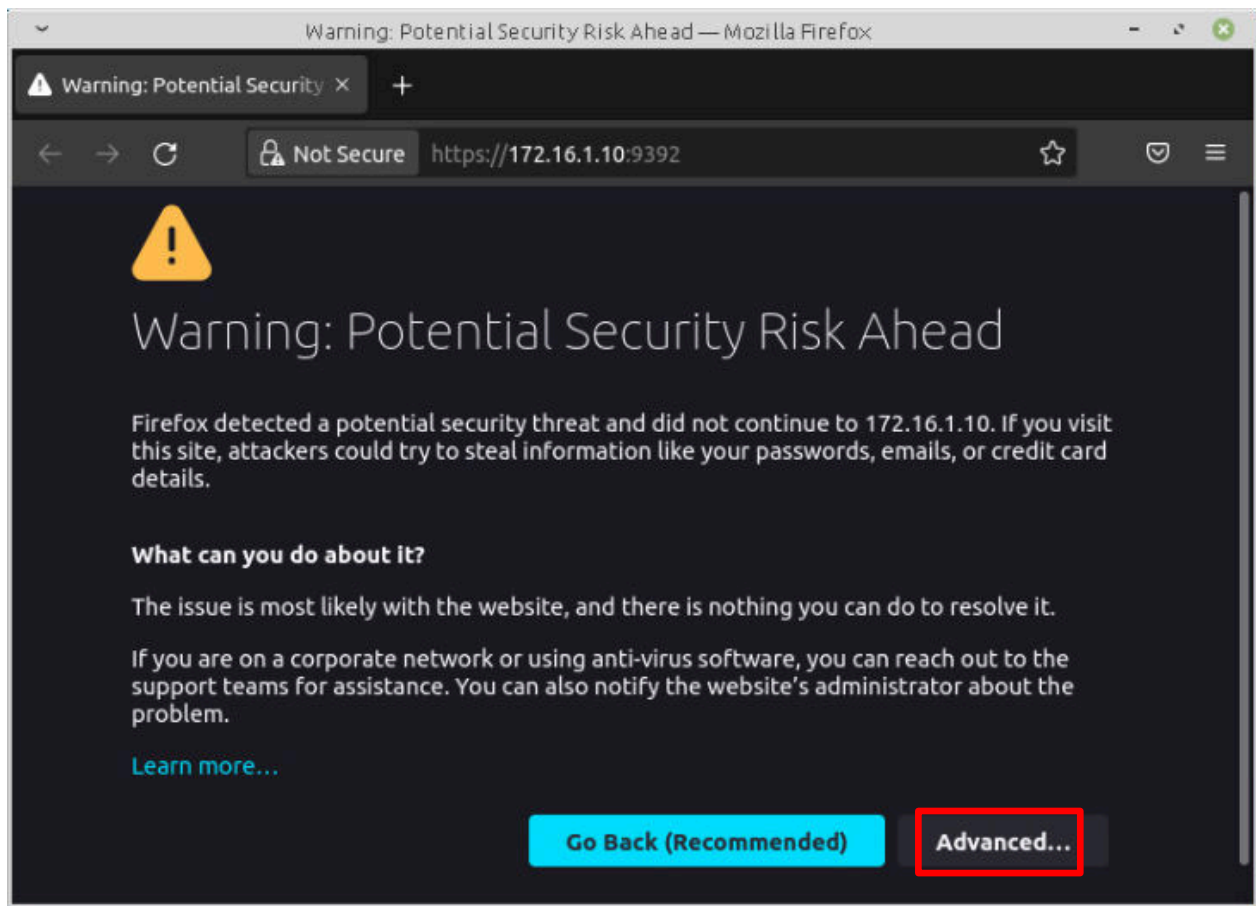
3. Open the browser by clicking on the **Firefox** icon located in the toolbar at the bottom of the window.



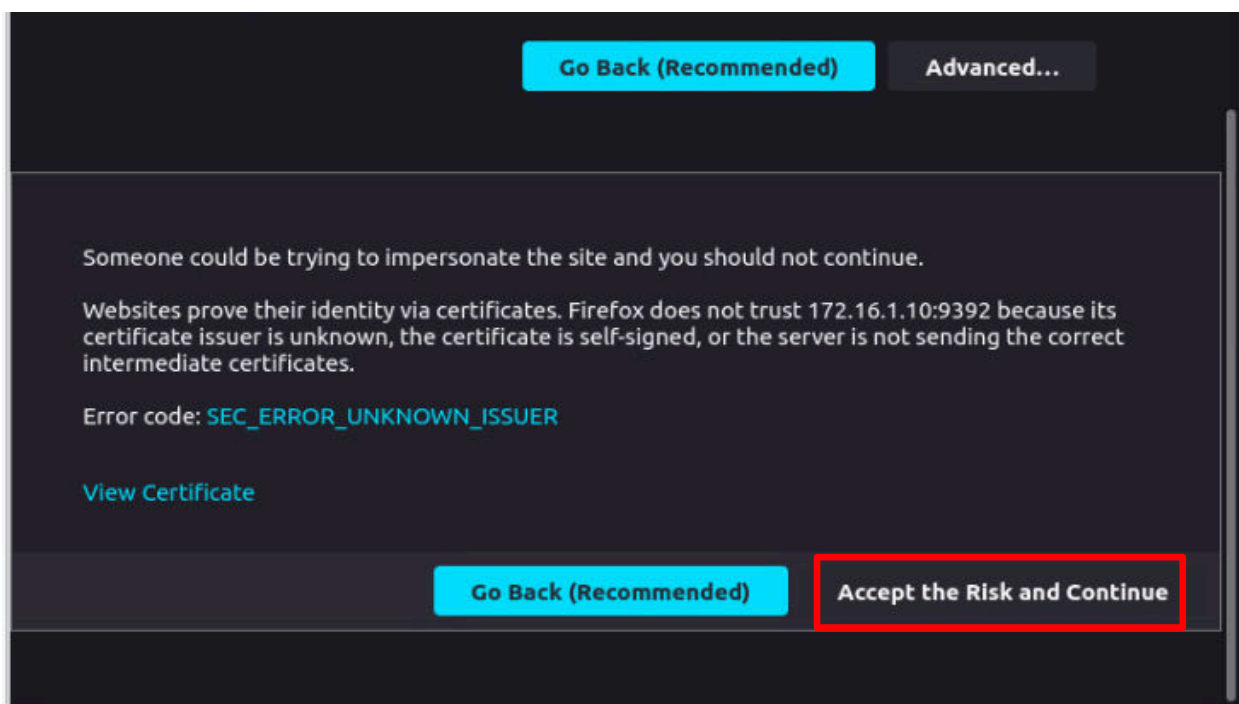
4. In the address bar of the browser, enter `https://172.16.1.10:9392`, which is the IP address of the **OpenVAS** application.



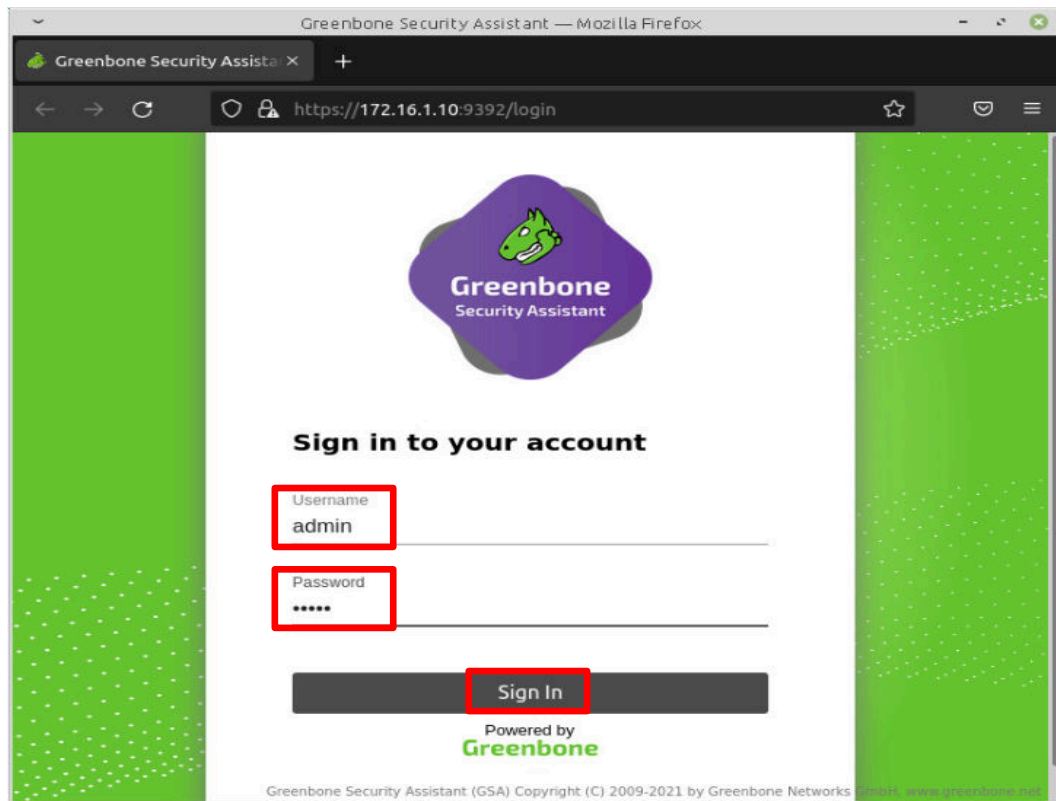
5. Since the web page uses HTTPS: with a self-signed certificate, the browser will warn that there is a security risk. Click on the **Advanced** button.



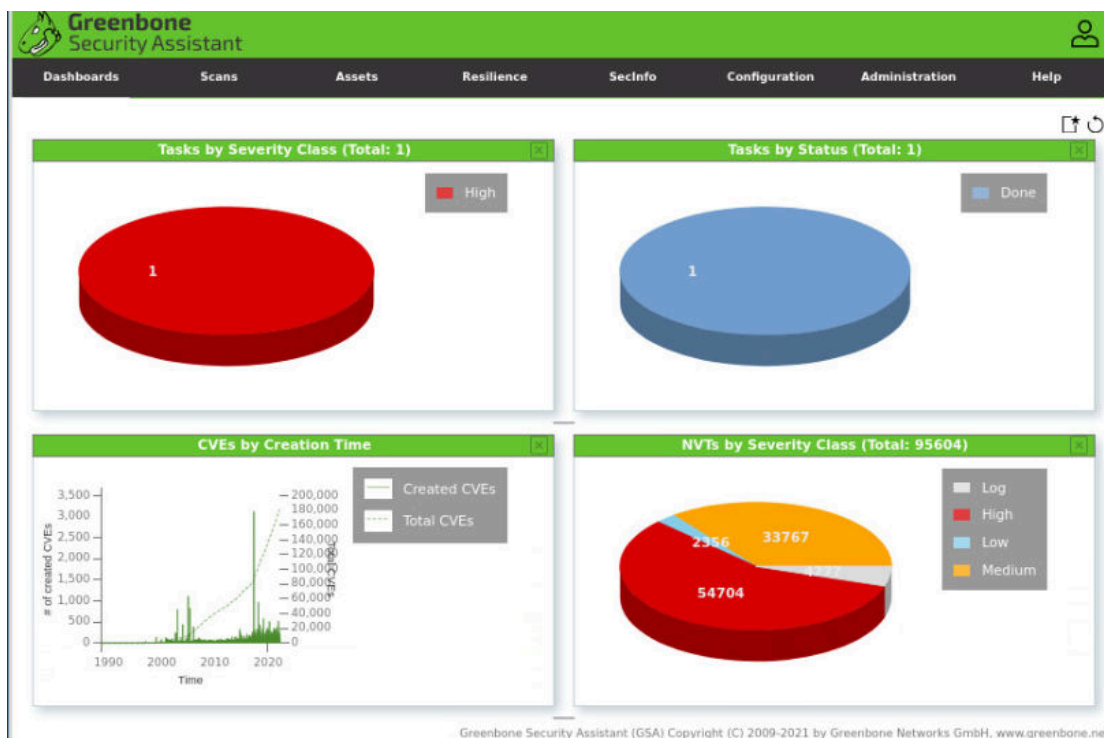
6. Scroll to the bottom of the window and click the **Accept the Risk and Continue** button.



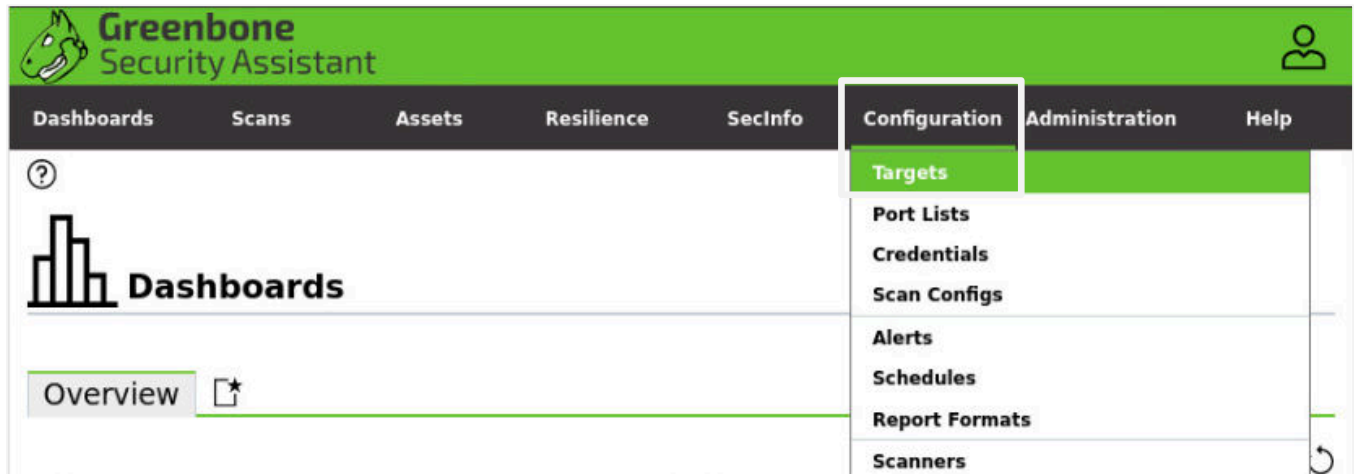
7. Log in as admin using the password admin and click the **Sign In** button.



The opening page shows the *OpenVAS* (which is now called *GVM* (Greenbone Security Assistant) Dashboard. The Dashboard shows different overviews of different tasks; by **Severity Class** and by **Status** and the number of **CVEs** by Creation Time and **NVTs** by Severity Class that are currently loaded.



8. The first step is to select the target host to be scanned. On the menu bar, select **Configuration** and then click on **Targets**.



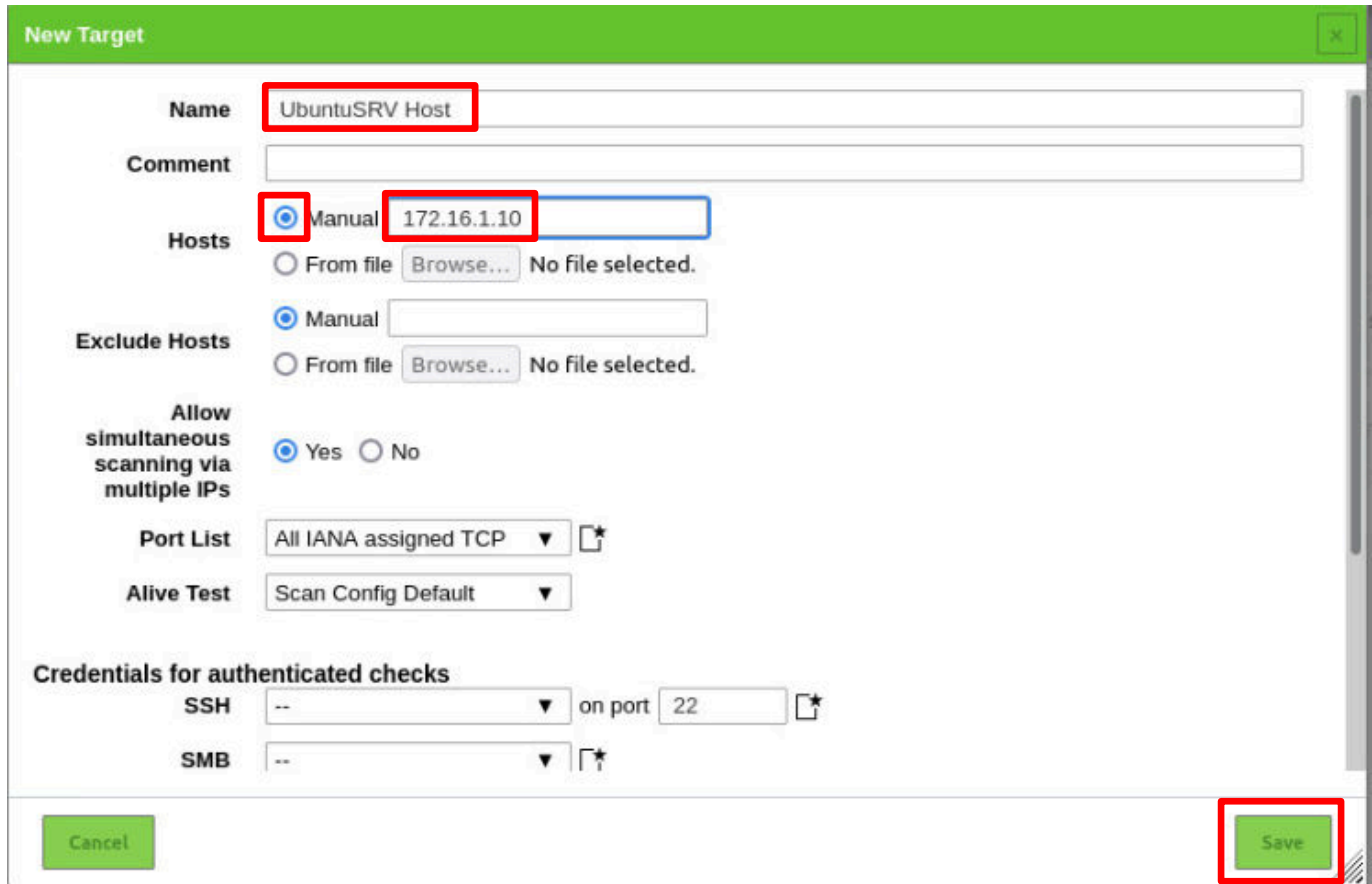
9. Click on the **New Target** icon.



10. In the *New Target* window, enter the following:

Name	UbuntuSRV Host
Hosts	Click on the <b>Manual</b> radio button, then enter 172.16.1.10 (this is the IP Address of the UbuntuSRV computer)

11. Leave all the remaining fields at their defaults and click on the **Save** button.

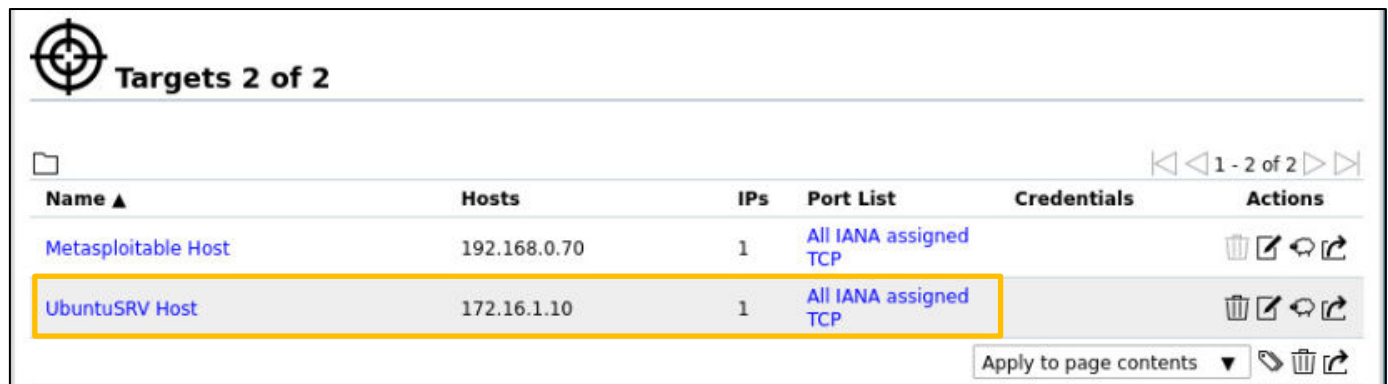


The 'New Target' dialog box is shown with the following fields and values:









- Name:** UbuntuSRV Host
- Comment:** (empty)
- Hosts:** ☒ Manual 172.16.1.10
- Exclude Hosts:** ☒ Manual (empty)
- Allow simultaneous scanning via multiple IPs:** ☒ Yes ☐ No
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:**
  - SSH:** -- on port 22
  - SMB:** --




Buttons: Cancel, Save

You will see the new target added to the list.

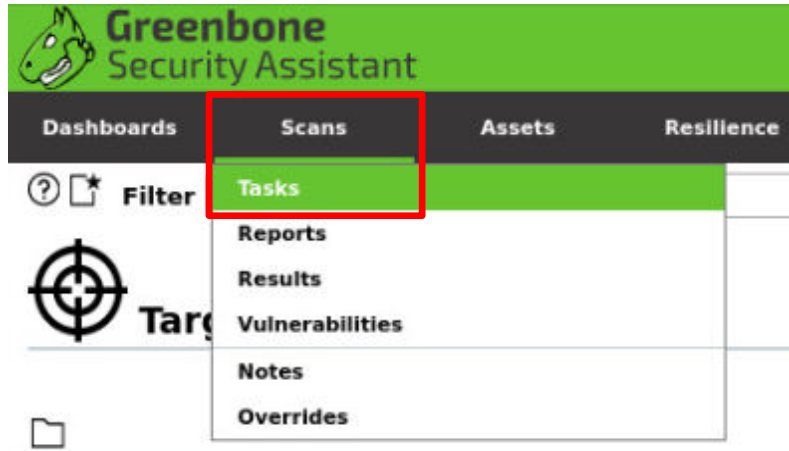


Targets 2 of 2

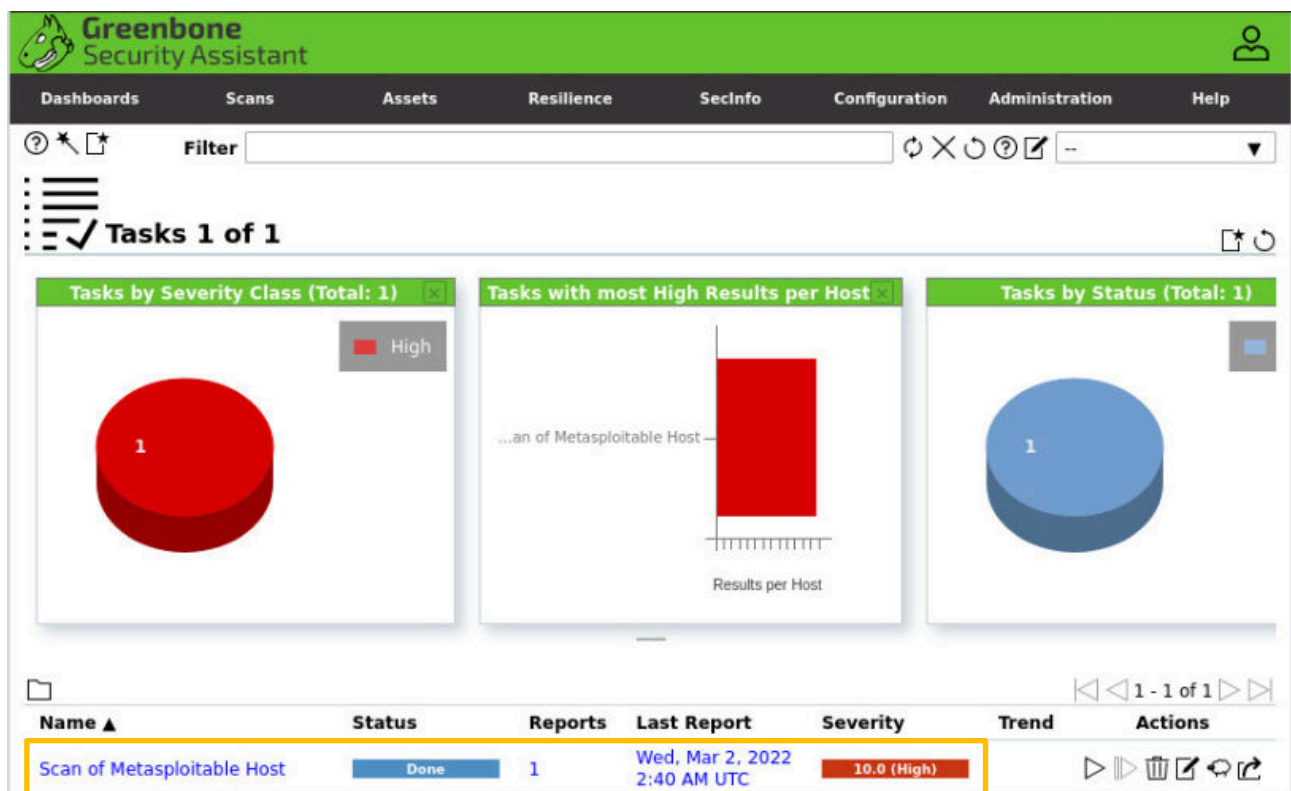
Name ▲	Hosts	IPs	Port List	Credentials	Actions
Metasploitable Host	192.168.0.70	1	All IANA assigned TCP		   
UbuntuSRV Host	172.16.1.10	1	All IANA assigned TCP		   

Apply to page contents ▼   

12. The next step is to create the vulnerability scan task. On the menu bar, select **Scans** and then click on **Tasks**.



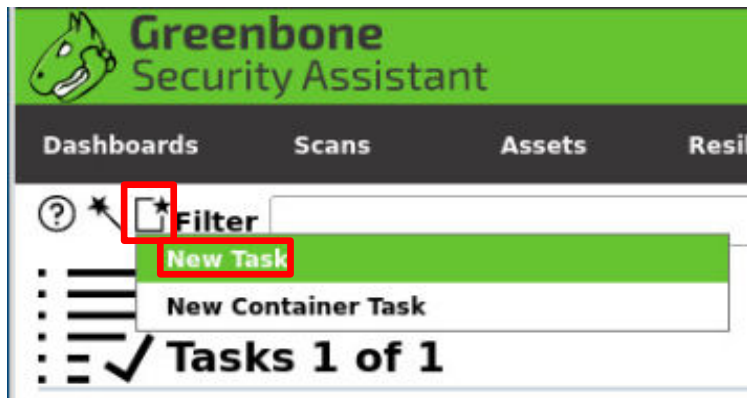
On the *Tasks* page, you will see a summary of tasks that have already been performed (GVM maintains the results of all scans). There is a scan of a **Metasploitable** host already on the list.



*Metasploitable* is a host that has been developed to provide security analysts a vulnerable platform to explore.

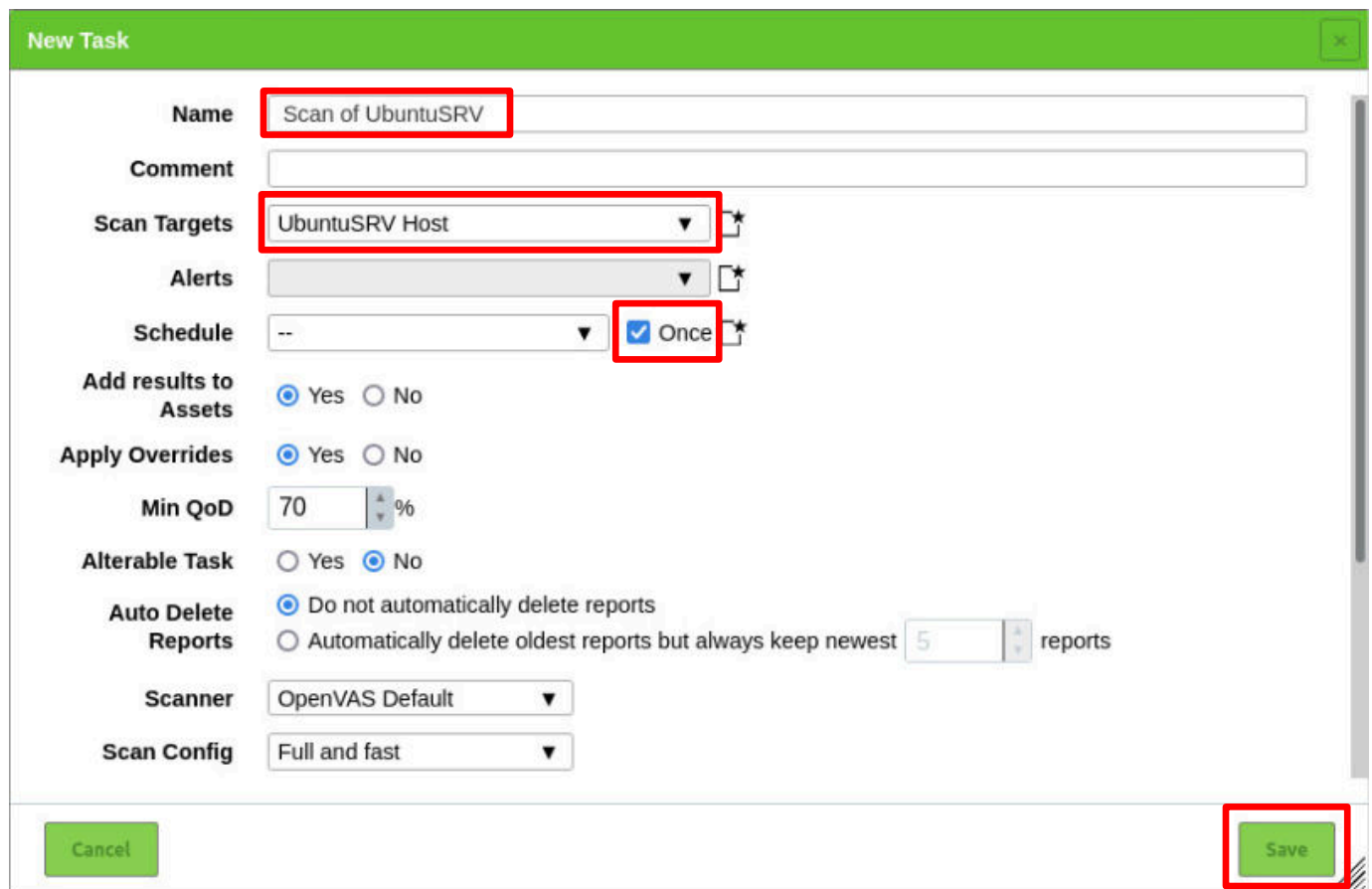
Since the scan of *Metasploitable* takes upwards of an hour to complete, the scan has already been performed and you will be analyzing the results of the scan in the next section.

13. Click on the **New Task** icon and select **New Task**.



14. In the *New Task* window, enter the following, leave all the remaining fields at their defaults and click on the **Save** button.

<i>Name</i>	Scan of UbuntuSRV
<i>Scan Targets</i>	Click on the <b>list arrow</b> and select <b>UbuntuSRV Host</b>
<i>Schedule</i>	Select the <b>Once</b> checkbox



**New Task**

Name: Scan of UbuntuSRV

Comment:

Scan Targets: UbuntuSRV Host

Alerts:

Schedule: -- ☒ 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

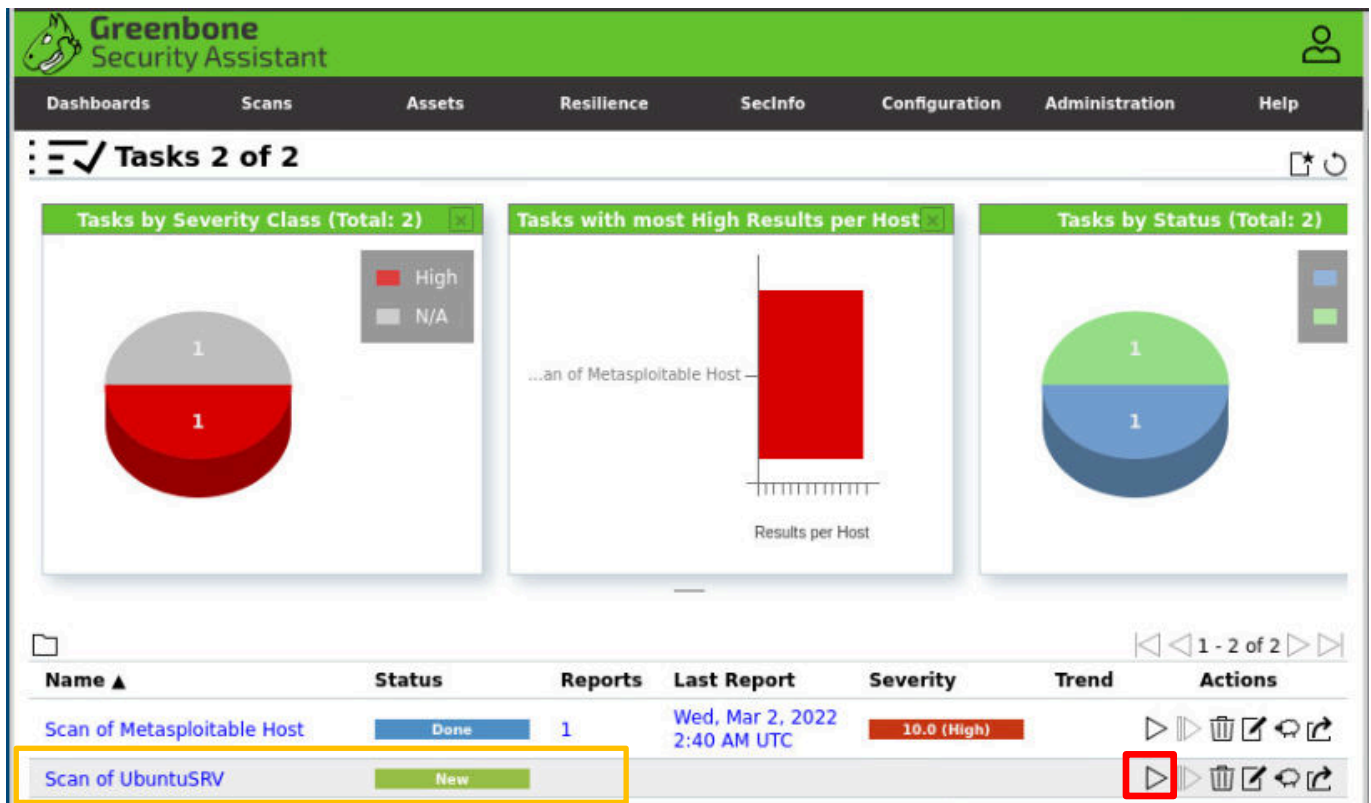
Scanner: OpenVAS Default

Scan Config: Full and fast

Cancel Save



15. An entry will be added for the *UbuntuSRV* scan task you just created. To run the scan, click on the **Play** icon on the right side of the entry.



The scan should take about 15 minutes to complete.

When the Status progress bar gets to at least 1%, you can continue onto the analysis of the previously scanned *Metasploitable* host.

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan of Metasploitable Host	Done	1	Wed, Mar 2, 2022 2:40 AM UTC	10.0 (High)		▶▶🗑️📄🔄🔗
Scan of UbuntuSRV	Done	1	Thu, Mar 3, 2022 4:47 PM UTC	5.3 (Medium)		▶▶🗑️📄🔄🔗

16. Remain in the *MintOS* computer and keep the *Greenbone Security Assistant* web page open, and continue to the next section.

### 3 Review the Vulnerability Scan Results

In this next task, you will be analyzing the vulnerabilities that have been discovered, remediating them, and then compiling a security report.

Because a *Metasploitable* host is full of vulnerabilities (by design), it presents far more interesting results.

1. Under the *Reports* column, click on 1 to open to scan report for the *Metasploitable* host.

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan of Metasploitable Host	Done	1	Wed, Mar 2, 2022 2:40 AM UTC	10.0 (High)		     
Scan of UbuntuSRV	Done	1	Thu, Mar 3, 2022 4:47 PM UTC	5.3 (Medium)		     

*OpenVAS* will show a summary of all the discovered vulnerabilities by severity level. From the descriptions in the *OpenVAS/GAS Tech Doc* user manual, the severity levels are:

Date ▲	Status	Task	Severity	High	Medium	Low	Log	False Pos.
Wed, Mar 2, 2022 2:40 AM UTC	Done	Scan of Metasploitable Host	10.0 (High)	25	33	5	86	0

*"High and Medium: Findings of the severity levels **High** and **Medium** are most important and should be addressed with priority. Before addressing medium level findings, high-level findings should be addressed."*

*"Low and Log: Findings of the severity levels **Low** and **Log** are mostly interesting for detailed understanding. These findings are filtered out by default but can hold very interesting information. Considering them will increase the security of the network and the systems. Typical for a result with the severity **Log** is that a service uses a banner with its name and version number. This could be useful for an attacker when this version has a known vulnerability."*

2. Click on the **Date** entry to open the details of the results.

Date ▲	Status	Task	Severity	High	Medium	Low	Log	False Pos.
Wed, Mar 2, 2022 2:40 AM UTC	Done	Scan of Metasploitable Host	10.0 (High)	25	33	5	86	0



3. Below is the vulnerability scan summary page. From this page, you get a high-level look at how vulnerable the target is. Click on the **Results** tab to see the results of the vulnerability scan.

Rep

Fri, Apr 22, 2022

ort: 2 4:16 PM UTC

Done

0df49af4-

ID: ae23-4f39-a501-

acbe13103de5

Fri, Apr 22,

Created: 2022 4:17 PM

UTC

Fri, Apr 22,

Modified: 2022 5:22 PM

UTC

Owner: admin

Information

Results

(56 of 451)

Hosts

(1 of 1)

Ports

(16 of 23)

Applications

(13 of 13)

Operating Systems

(1 of 1)

CVEs

(25 of 25)

Closed CVEs

(0 of 0)

TLS Certificates

(2 of 2)

Error Messages

(0 of 0)







User Tags

(0)

1 - 56 of 56

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	192.168.0.70		general/tcp	Fri, Apr 22, 2022 4:44 PM UTC
The rexec service is running		10.0 (High)	80 %	192.168.0.70		512/tcp	Fri, Apr 22, 2022 4:47 PM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.0.70		80/tcp	Fri, Apr 22, 2022 4:48 PM UTC
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.0.70		general/tcp	Fri, Apr 22, 2022 4:17 PM UTC
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.0.70		1524/tcp	Fri, Apr 22, 2022 4:56 PM UTC

Description of the columns:

<i>Vulnerability</i>	The name of the vulnerability that has been found. Clicking on the name will show the details page, including recommended solution
<i>(Solution Type)</i>  <ul style="list-style-type: none"> <li> A configuration mitigation is available</li> <li> A workaround is available</li> <li> A patch is available</li> <li> No fix is and will be available</li> <li> No solution exists</li> </ul>	
<i>Severity</i>	A bar graph showing the severity of the vulnerability according to CVSS
<i>QoD</i>	The Quality of Detection, which describes the reliability of the executed vulnerability or product detection (by default, only vulnerability types of 70% or greater are shown)
<i>Host IP</i>	The IP address for the scanned host
<i>Host Name</i>	The name of the scanned host
<i>Location</i>	The port number and protocol type (TCP/UDP) used to find the result
<i>Created</i>	Date and time the vulnerability was discovered during the scan

- Click on the **The rexec service is running** vulnerability.

Vulnerability	Severity ▼	QoD
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %
<b>The rexec service is running</b>	10.0 (High)	80 %

### Summary

This remote host is running a rexec service.

### Detection Result

The rexec service was detected on the target system.

### Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticates by reading the username and password \*unencrypted\* from the socket.

### Detection Method

Checks if a vulnerable version is present on the target host.

Details: [The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111](#)

Version used: 2020-10-01T11:33:30Z

### Solution

**Solution Type:** ↗ Mitigation

Disable the rexec service and use alternatives like SSH instead.

### References



CVE [CVE-1999-0618](#)

The detected vulnerability's detailed page, which includes the solution to remediate the vulnerability, will be shown. In this example, the solution would inform the security analyst that there is a mitigation recommending the *rexec* service be disabled.

- Click on the **Hosts** tab to see the details about the scanned host, then click on the host's **IP address** to show more detailed information about the host.


Information	Results (63 of 531)	Hosts (1 of 1)	Ports (20 of 23)	Applications (15 of 15)	Operating Systems (1 of 1)	CVEs (27 of 27)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)
-------------	------------------------	-------------------	---------------------	----------------------------	-------------------------------	--------------------	-------------------------	------------------------------	----------------------------

1 - 1 of 1

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive
192.168.0.70			20	15			Wed, Mar 2, 2022 2:41 AM UTC	Wed, Mar 2, 2022 3:29 AM UTC	25	33	5	0	0

1 - 1 of 1

(Applied filter: apply\_overrides=0 levels=hml rows=100 min\_qod=70 first=1 sort-reverse=severity)


**Host: 192.168.0.7**


ID: 8d9e7638-be0e-462e-bb0c-be17db0a38a9
Created: Tue, Mar 1, 2022 UTC

Information	User Tags (0)	Permissions (0)
-------------	------------------	--------------------

Hostname

IP Address 192.168.0.70

Comment

OS  Canonical Ubuntu Linux

Route • 172.16.1.10 ► 192.168.0.70

Severity **10.0 (High)**

### Latest Identifiers




Name	Value	Created
ssh-key	22 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TudjgWkIVNdTq6kboEDjteOfc65TII7sRvQBwqAhQjeeyylk8T55gMDkOD0akSISXvLDcmcdYfxelF0ZSuT+nkRhij7XSSA/Oc5QSk3sj/Slnfb78e3anbRHpmkjcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKml78Fo3HjjYucg87JjLeC66i7+dIEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qD	Wed, Mar 2, 2022 3:30 AM UTC

- Click the browser's back arrow to return to the report summary page.

7. Clicking on the **Ports** tab will show the list of open ports and transport protocols that have been discovered as open and the severity of a breach.

Information	Results (63 of 531)	Hosts (1 of 1)	Ports (20 of 23)	Applications (15 of 15)	Operating Systems (1 of 1)	CVEs (27 of 27)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)
<div> <div>1 - 20 of 20</div> </div>									
Port	Hosts			Severity ▼					
80/tcp	1			10.0 (High)					
512/tcp	1			10.0 (High)					
513/tcp	1			10.0 (High)					
1099/tcp	1			10.0 (High)					
1524/tcp	1			10.0 (High)					
8787/tcp	1			10.0 (High)					
8009/tcp	1			9.8 (High)					
3632/tcp	1			9.3 (High)					
3306/tcp	1			9.0 (High)					

8. Clicking on the **Applications** tab will show the *CPE* (Common Platform Enumeration) of the classes of applications, operating systems, and hardware devices.

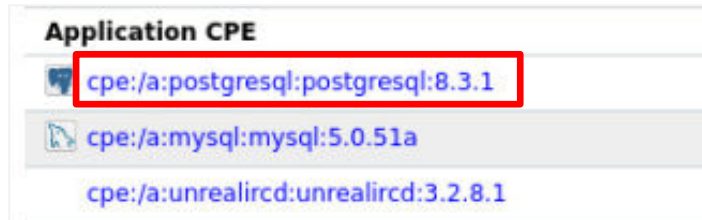
Information	Results (63 of 531)	Hosts (1 of 1)	Ports (20 of 23)	Applications (15 of 15)	Operating Systems (1 of 1)	CVEs (27 of 27)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)
<div> <div>1 - 15 of 15</div> </div>									
Application CPE	Hosts		Occurrences		Severity ▼				
 cpe:/a:postgresql:postgresql:8.3.1	1		1		9.0 (High)				
 cpe:/a:mysql:mysql:5.0.51a	1		1		9.0 (High)				
cpe:/a:unrealircd:unrealircd:3.2.8.1	1		1		8.1 (High)				
cpe:/a:samba:samba:3.0.20	1		1		6.0 (Medium)				
 cpe:/a:apache:http_server:2.2.8	1		1		4.3 (Medium)				
cpe:/a:beasts:vsftpd:2.3.4	1		1		N/A				
cpe:/a:isc:bind:9.4.2	1		1		N/A				



“CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.”

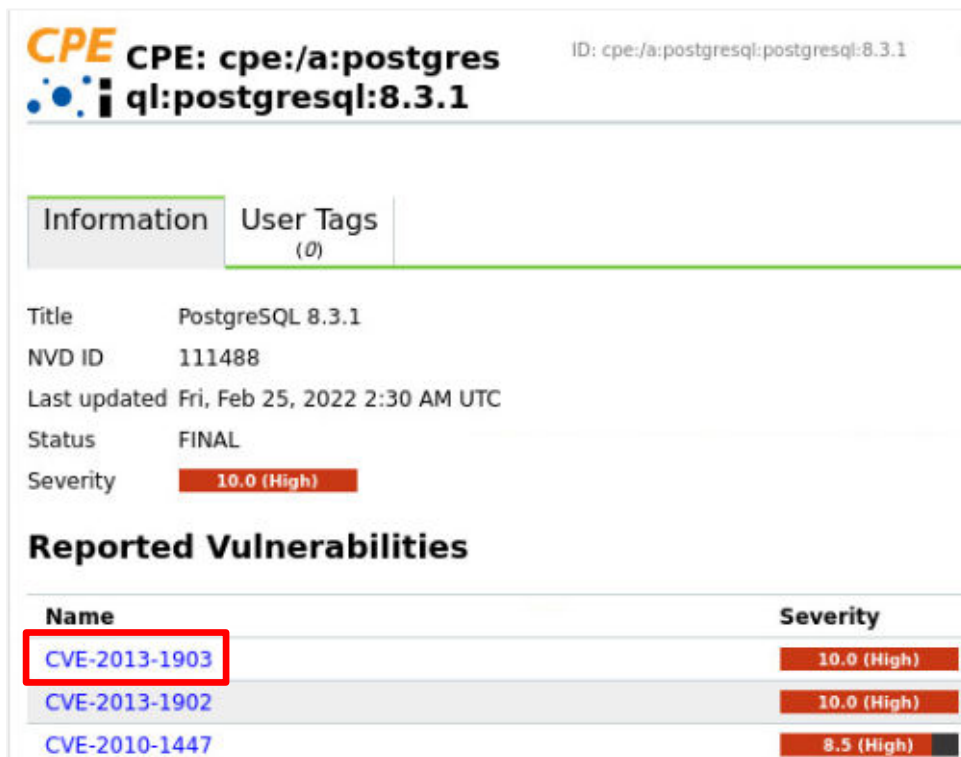
<https://nvd.nist.gov/products/cpe>

9. Clicking on **cpe:/a:postgresql:postgresql:8.3.1** Application CPE will show the reported vulnerabilities by CVE.



It will take about 30 seconds for the CVSS screen to appear.

10. Clicking on the **CVE-2013-1903** CVE entry will show the CVSS information.

A screenshot of a web page showing CVE information for PostgreSQL 8.3.1. The page has a header with the CPE logo and the text "CPE: cpe:/a:postgresql:postgresql:8.3.1" and "ID: cpe:/a:postgresql:postgresql:8.3.1". Below the header is a tabbed interface with "Information" and "User Tags (0)". The "Information" tab is active, showing details: Title (PostgreSQL 8.3.1), NVD ID (111488), Last updated (Fri, Feb 25, 2022 2:30 AM UTC), Status (FINAL), and Severity (10.0 (High)). Below this is a section titled "Reported Vulnerabilities" with a table listing CVEs and their severities. The first entry, "CVE-2013-1903", is highlighted with a red box.

Name	Severity
CVE-2013-1903	10.0 (High)
CVE-2013-1902	10.0 (High)
CVE-2010-1447	8.5 (High)

And most importantly, the *Base Score* and the *Base Vector*.


**CVE: CVE-2013-1903**

ID: CVE-2013-1903
Published: Thu, Apr 4, 2013 5:55 PM UTC
Modified: Fri, Feb 25, 2022 2:30 AM UTC
Last updated: Fri, Oct 20, 2017 1:29 AM UTC

Information
User Tags (0)

### Description

PostgreSQL, possibly 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 incorrectly provides the superuser password to scripts related to "graphical installers for Linux and Mac OS X," which has unspecified impact and attack vectors.

### CVSS

Base Score	10.0 (High)
Base Vector	AV:N/AC:L/Au:N/C/I:C/A:C
Access Vector	NETWORK
Access Complexity	LOW
Authentication	NONE



“The *Common Vulnerability Scoring System* (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.”


<https://www.first.org/cvss/specification-document>




11. Clicking on the **Base Vector** link will display the Base Metric intrinsic characteristics of vulnerabilities that are constant over time across different user environments.

CVSS	
Base Score	10.0 (High)
Base Vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
Access Vector	NETWORK
Access Complexity	LOW
Authentication	NONE

As a security analyst, you will use the CVSS score and vectors to assess the threat level of all of the vulnerabilities and prioritize the mitigation.





**From Metrics:**

Access Vector: Network

Access Complexity: Low

Authentication: None

Confidentiality: Complete

Integrity: Complete

Availability: Complete

**From Vector:**

Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

**Results:**

CVSS Base Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Severity: 10.0 (High)

**From Metrics:**

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Scope: Unchanged

Confidentiality: None

Integrity: None

Availability: None

**From Vector:**

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/U

**Results:**

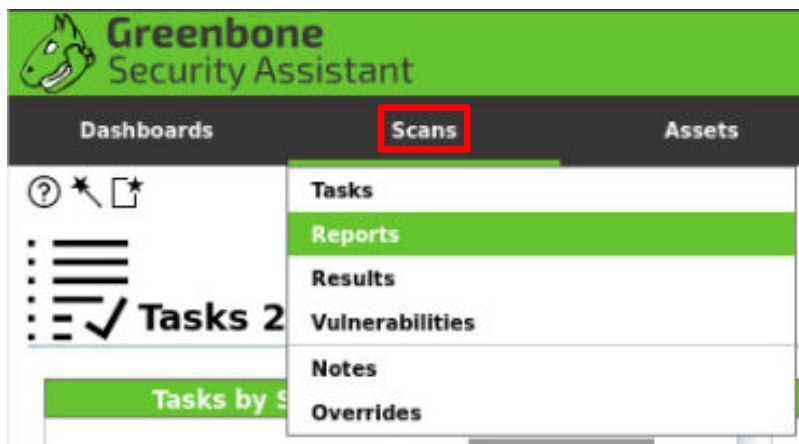
12. Remain on the *Greenbone Security Assistant* web page on the *MintOS* computer and continue to the next task.

## 4 Compile a Report on Scan Results

A Penetration Tester's job is to find vulnerabilities in an organization's IT environment. By contrast, a Security Analyst is tasked with finding the vulnerabilities and reporting the findings to both management and IT (for remediation).

OpenVAS/GSM provides several reporting formats that can be used by the security analyst to prepare the reports. OpenVAS/GSM saves all of the scans that have been done in a local database allowing reviewing of newer scans against past scans to determine if the vulnerabilities have been mitigated.

1. On the menu ribbon, select **Scans** and click on **Reports**.

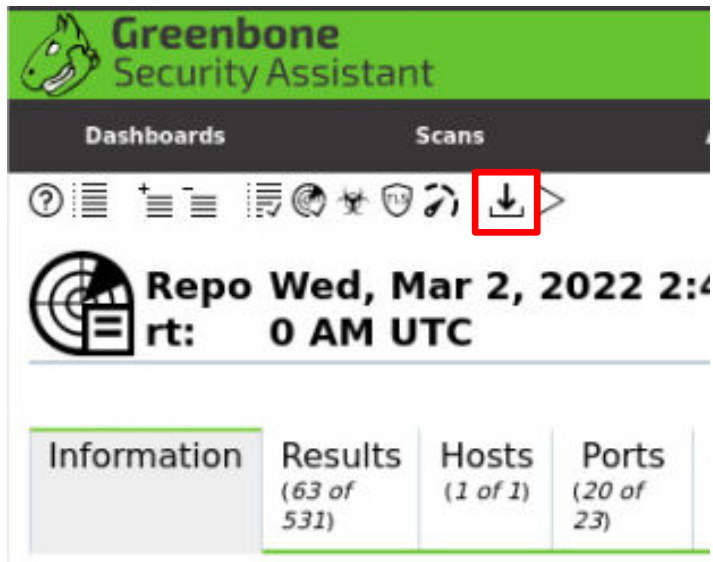


2. Click on the **Date** link in the *Last Report* column for the scan of *Metasploitable Host*.

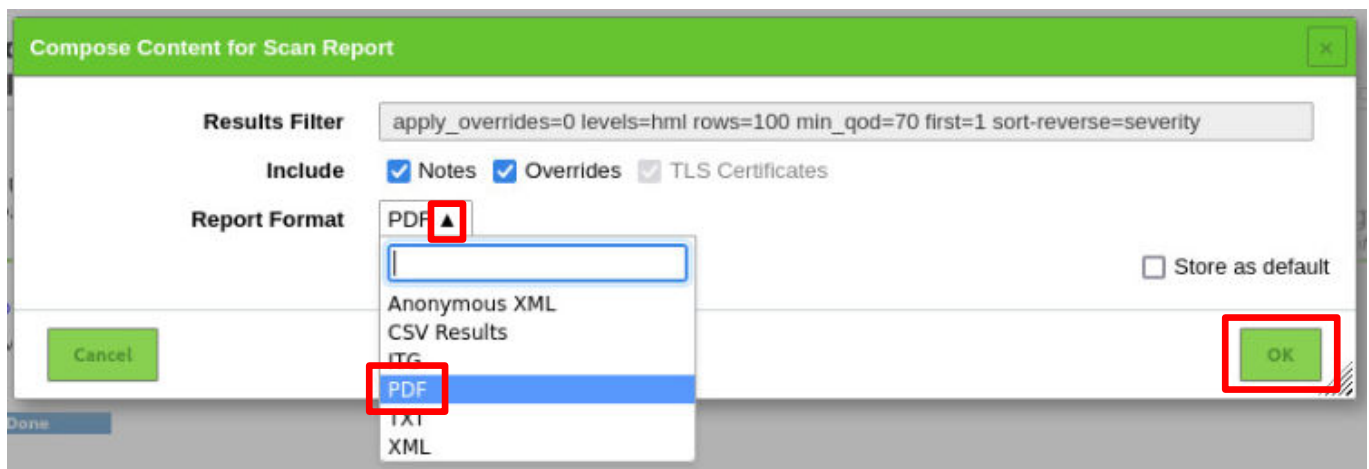
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Apr 22, 2022 4:16 PM UTC	Done	Scan of Metasploitable Host	10.0 (High)	19	32	5	82	0	△ ×



- Just below the menu ribbon, there will be a set of icons that can apply to the report. Click on the 10th icon from the left, which is the **Download Filtered Report** icon.

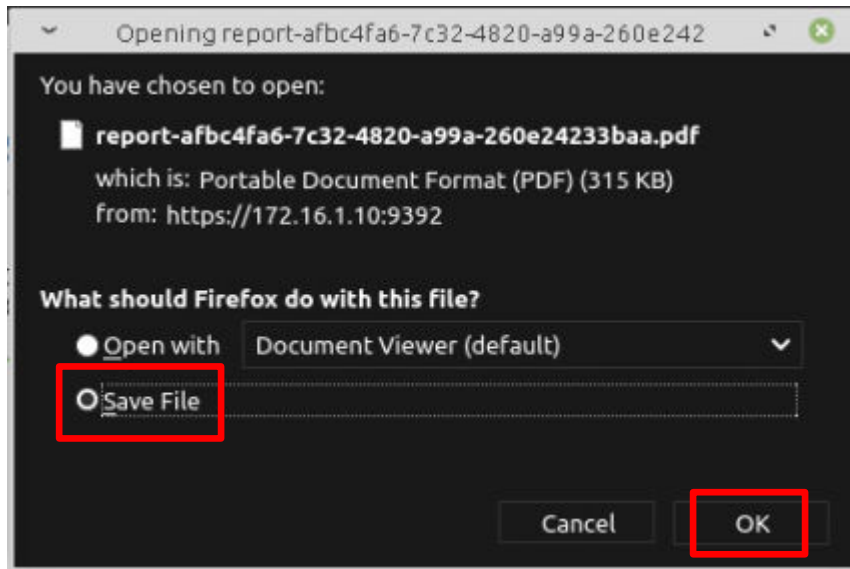


- In the *Compose Content for Scan Report* window, click the **Report Format** list arrow and select **PDF**.



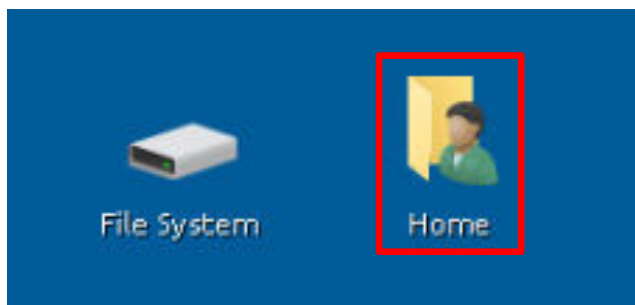
- Click on **OK** to create the report.

6. The report will be compiled, and a window will open asking to either save or open the PDF report. The default option is to save the file. Leave the **Save File** radio button selected and click **OK**.

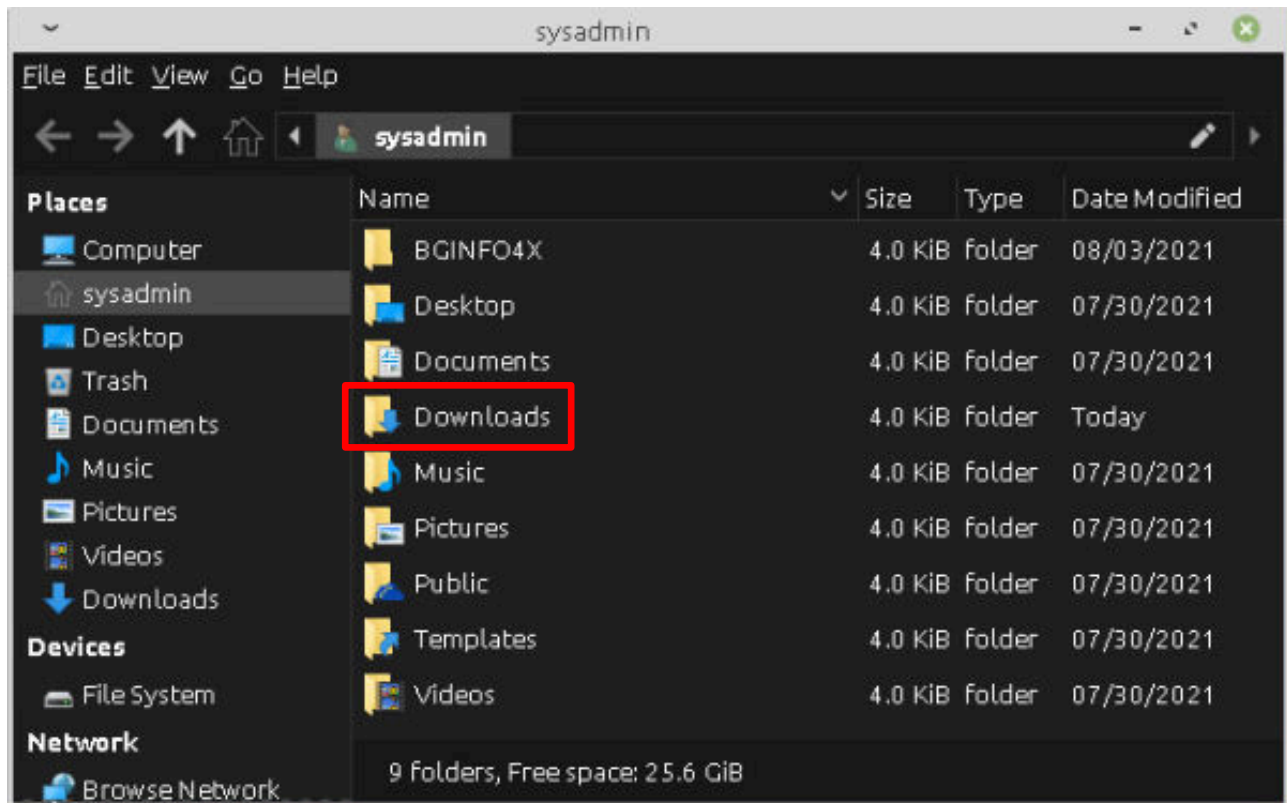


The other report formats; XML, TXT, etc. can be used for additional use cases. More information can be found in the User's Guide, under the Help menu option.

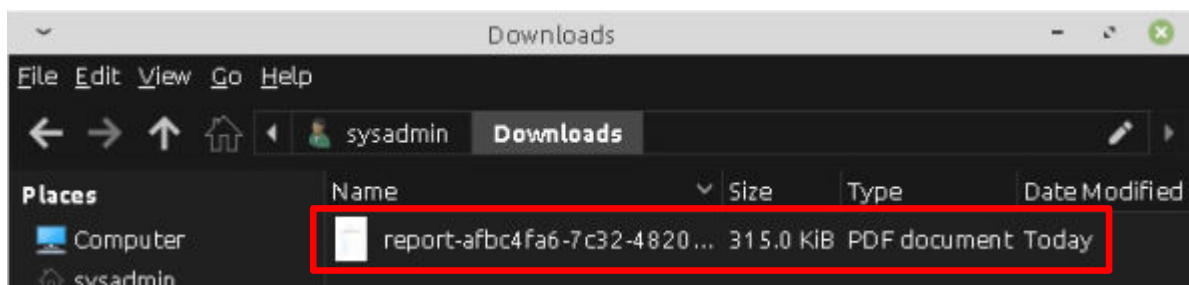
7. Minimize the **Greenbone Security Assistant** web page.
8. Double-click on the **Home** folder on the *MintOS* desktop.



9. Double-click to open the **Downloads** folder.



10. In the **Downloads** folder, double-click on the **report** to open the PDF file.





11. The lab is now finished, and you can end the reservation.