EXPERIMENT -3

OpenVAS

Open Vulnerability Assessment Scanner

Introduction

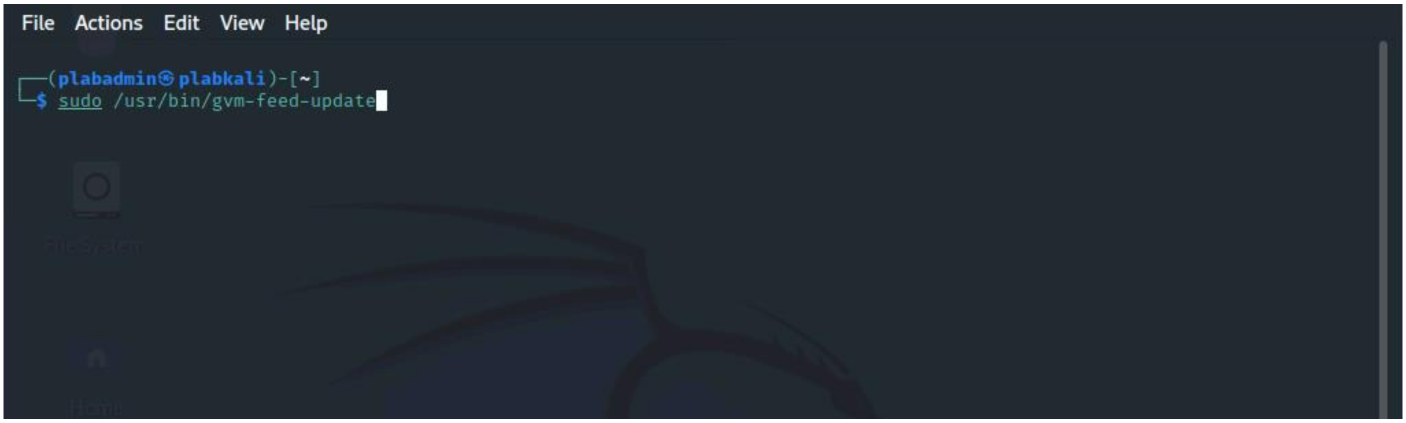
Open Vulnerability Assessment System (OpenVAS) is a tool in Kali Linux for vulnerability scanning of the system on a network. OpenVAS is a framework consisting of multiple services and tools and requires Python binaries

Perform Vulnerability Scanning using OpenVAS.

In the **Terminal** window, type the following and press Enter:

```
sudo /usr/bin/gvm-feed-update
```

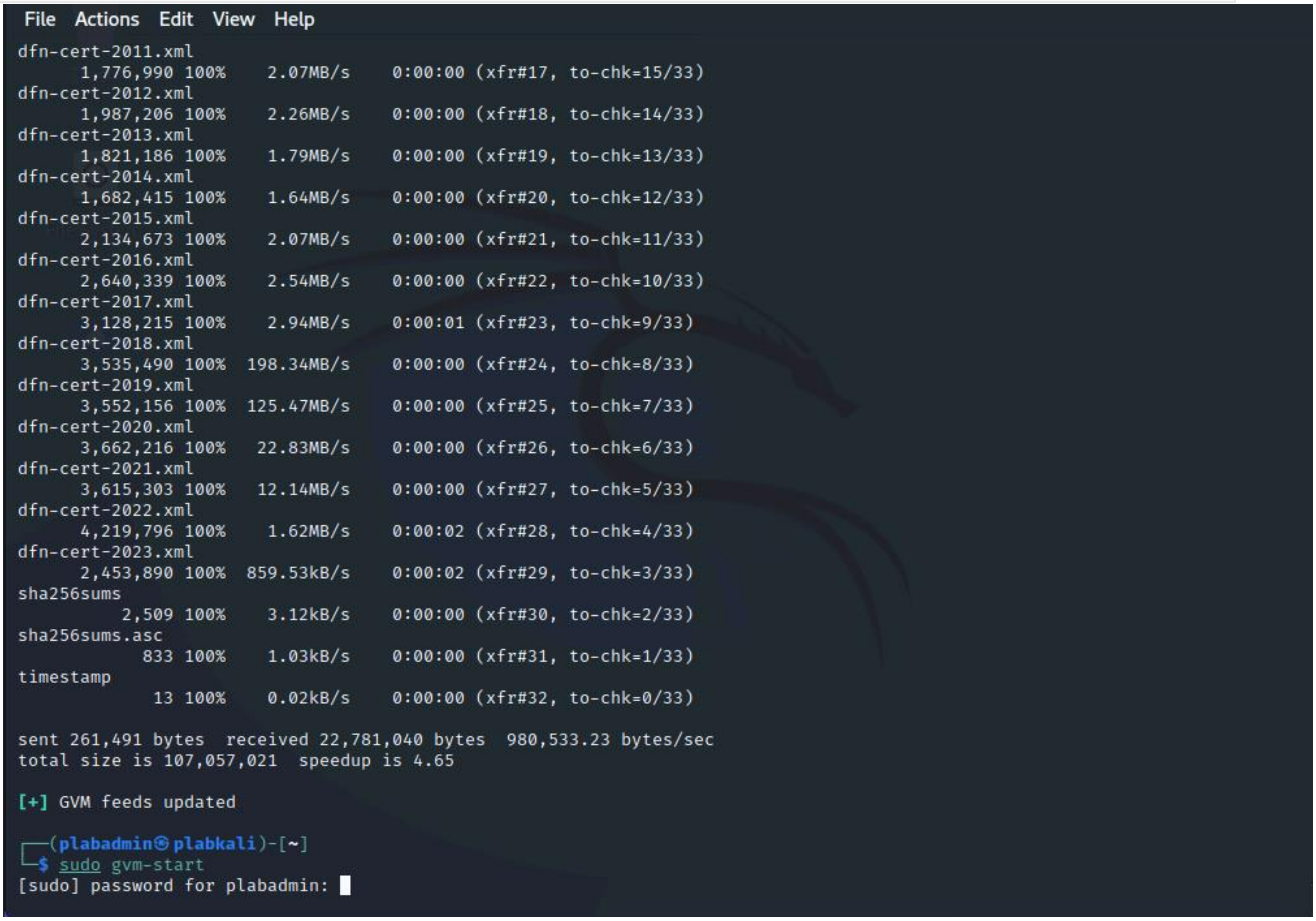
Executing this command will update the Greenbone database. This process will take up to 15 minutes to complete.



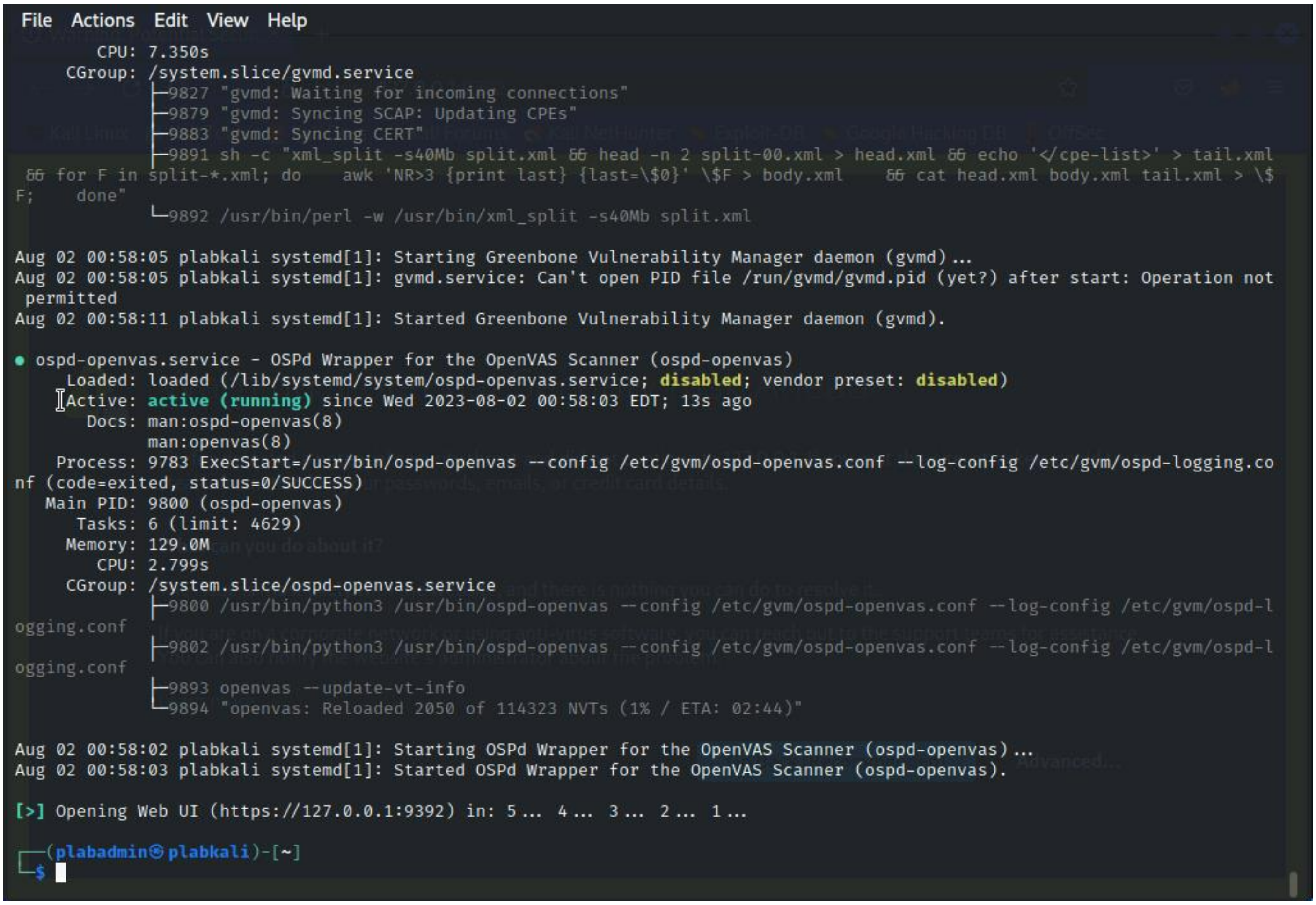
```
┌──(plabadmin㉿plabkali)-[~]
└─$ sudo /usr/bin/gvm-feed-update
```

Type the following in the **Terminal** window and press Enter:

```
sudo gvm-start
```



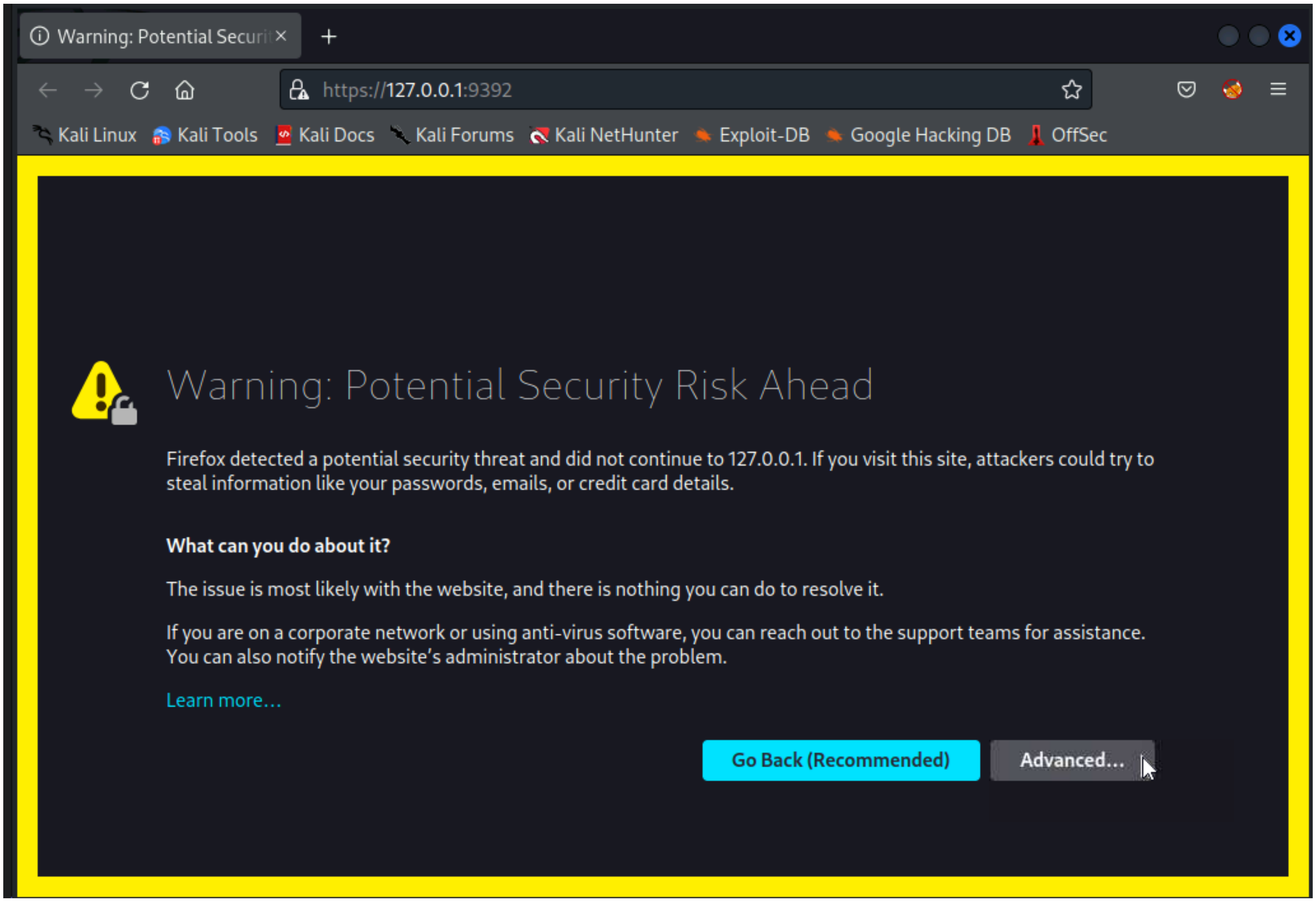
```
dfn-cert-2011.xml
      1,776,990 100%    2.07MB/s    0:00:00 (xfr#17, to-chk=15/33)
dfn-cert-2012.xml
      1,987,206 100%    2.26MB/s    0:00:00 (xfr#18, to-chk=14/33)
dfn-cert-2013.xml
      1,821,186 100%    1.79MB/s    0:00:00 (xfr#19, to-chk=13/33)
dfn-cert-2014.xml
      1,682,415 100%    1.64MB/s    0:00:00 (xfr#20, to-chk=12/33)
dfn-cert-2015.xml
      2,134,673 100%    2.07MB/s    0:00:00 (xfr#21, to-chk=11/33)
dfn-cert-2016.xml
      2,640,339 100%    2.54MB/s    0:00:00 (xfr#22, to-chk=10/33)
dfn-cert-2017.xml
      3,128,215 100%    2.94MB/s    0:00:01 (xfr#23, to-chk=9/33)
dfn-cert-2018.xml
      3,535,490 100%  198.34MB/s    0:00:00 (xfr#24, to-chk=8/33)
dfn-cert-2019.xml
      3,552,156 100%  125.47MB/s    0:00:00 (xfr#25, to-chk=7/33)
dfn-cert-2020.xml
      3,662,216 100%   22.83MB/s    0:00:00 (xfr#26, to-chk=6/33)
dfn-cert-2021.xml
      3,615,303 100%   12.14MB/s    0:00:00 (xfr#27, to-chk=5/33)
dfn-cert-2022.xml
      4,219,796 100%    1.62MB/s    0:00:02 (xfr#28, to-chk=4/33)
dfn-cert-2023.xml
      2,453,890 100%  859.53kB/s    0:00:02 (xfr#29, to-chk=3/33)
sha256sums
          2,509 100%    3.12kB/s    0:00:00 (xfr#30, to-chk=2/33)
sha256sums.asc
            833 100%    1.03kB/s    0:00:00 (xfr#31, to-chk=1/33)
timestamp
             13 100%    0.02kB/s    0:00:00 (xfr#32, to-chk=0/33)

sent 261,491 bytes  received 22,781,040 bytes  980,533.23 bytes/sec
total size is 107,057,021  speedup is 4.65

[+] GVM feeds updated

┌──(plabadmin㉿plabkali)-[~]
└─$ sudo gvm-start
[sudo] password for plabadmin:
```



```
        CPU: 7.350s
     CGroup: /system.slice/gvmd.service
             ├─9827 "gvmd: Waiting for incoming connections"
             ├─9879 "gvmd: Syncing SCAP: Updating CPEs"
             ├─9883 "gvmd: Syncing CERT"
             ├─9891 sh -c "xml_split -s40Mb split.xml && head -n 2 split-00.xml > head.xml && echo '</cpe-list>' > tail.xml
 && for F in split-*.xml; do    awk 'NR>3 {print last} {last=\$0}' \$F > body.xml    && cat head.xml body.xml tail.xml > \$
F;    done"
             └─9892 /usr/bin/perl -w /usr/bin/xml_split -s40Mb split.xml

Aug 02 00:58:05 plabkali systemd[1]: Starting Greenbone Vulnerability Manager daemon (gvmd)...
Aug 02 00:58:05 plabkali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: Operation not
 permitted
Aug 02 00:58:11 plabkali systemd[1]: Started Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2023-08-02 00:58:03 EDT; 13s ago
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 9783 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.co
nf (code=exited, status=0/SUCCESS)
   Main PID: 9800 (ospd-openvas)
      Tasks: 6 (limit: 4629)
     Memory: 129.0M
        CPU: 2.799s
     CGroup: /system.slice/ospd-openvas.service
             ├─9800 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-l
ogging.conf
             ├─9802 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-l
ogging.conf
             ├─9893 openvas --update-vt-info
             └─9894 "openvas: Reloaded 2050 of 114323 NVTs (1% / ETA: 02:44)"

Aug 02 00:58:02 plabkali systemd[1]: Starting OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)...
Aug 02 00:58:03 plabkali systemd[1]: Started OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).

[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

┌──(plabadmin㉿plabkali)-[~]
└─$ 
```

The **Firefox** browser will open automatically.

Click **Advanced**.



Warning: Potential Security Risk Ahead

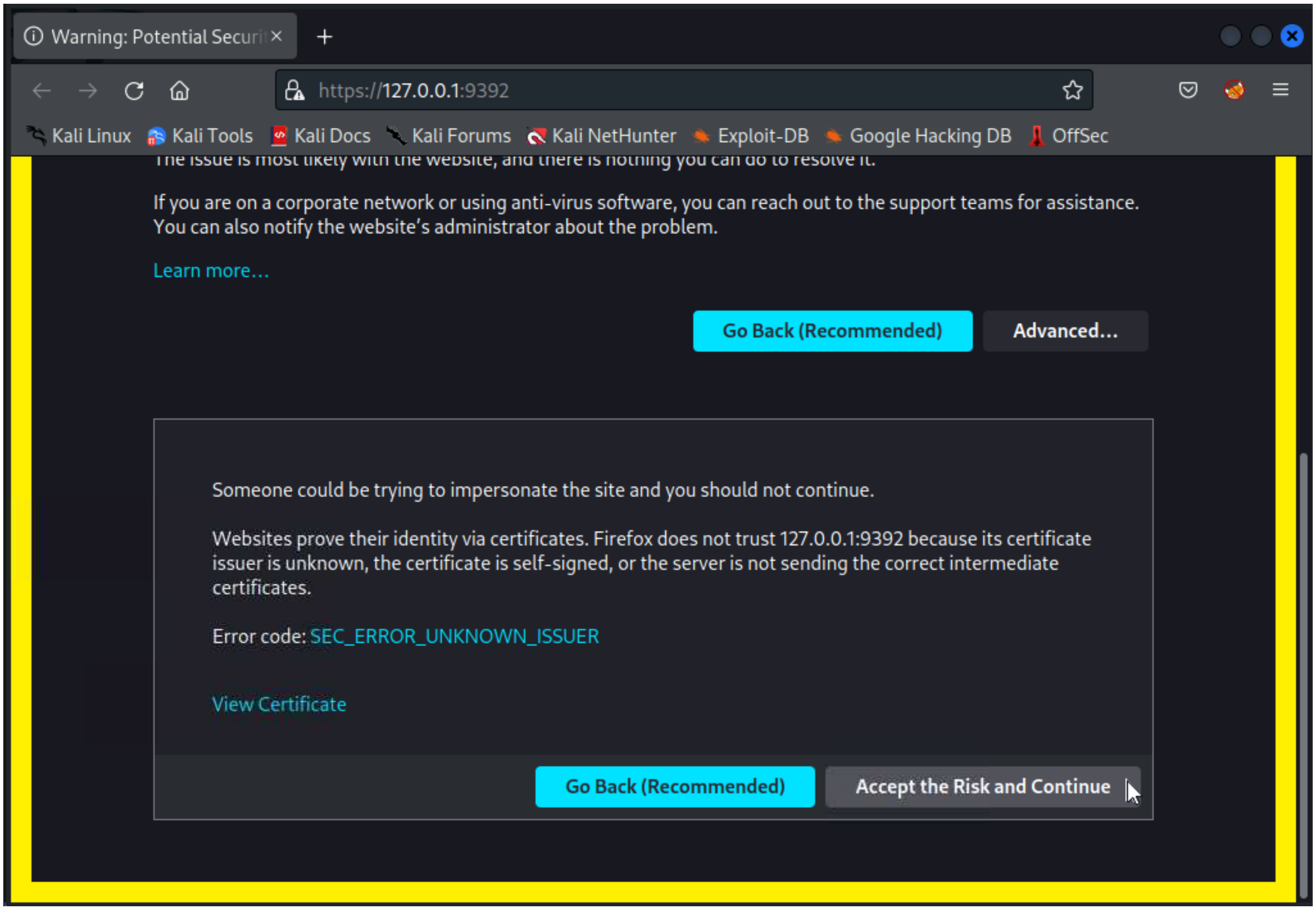
Firefox detected a potential security threat and did not continue to 127.0.0.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Scroll down and click **Accept the Risk and Continue**.



The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

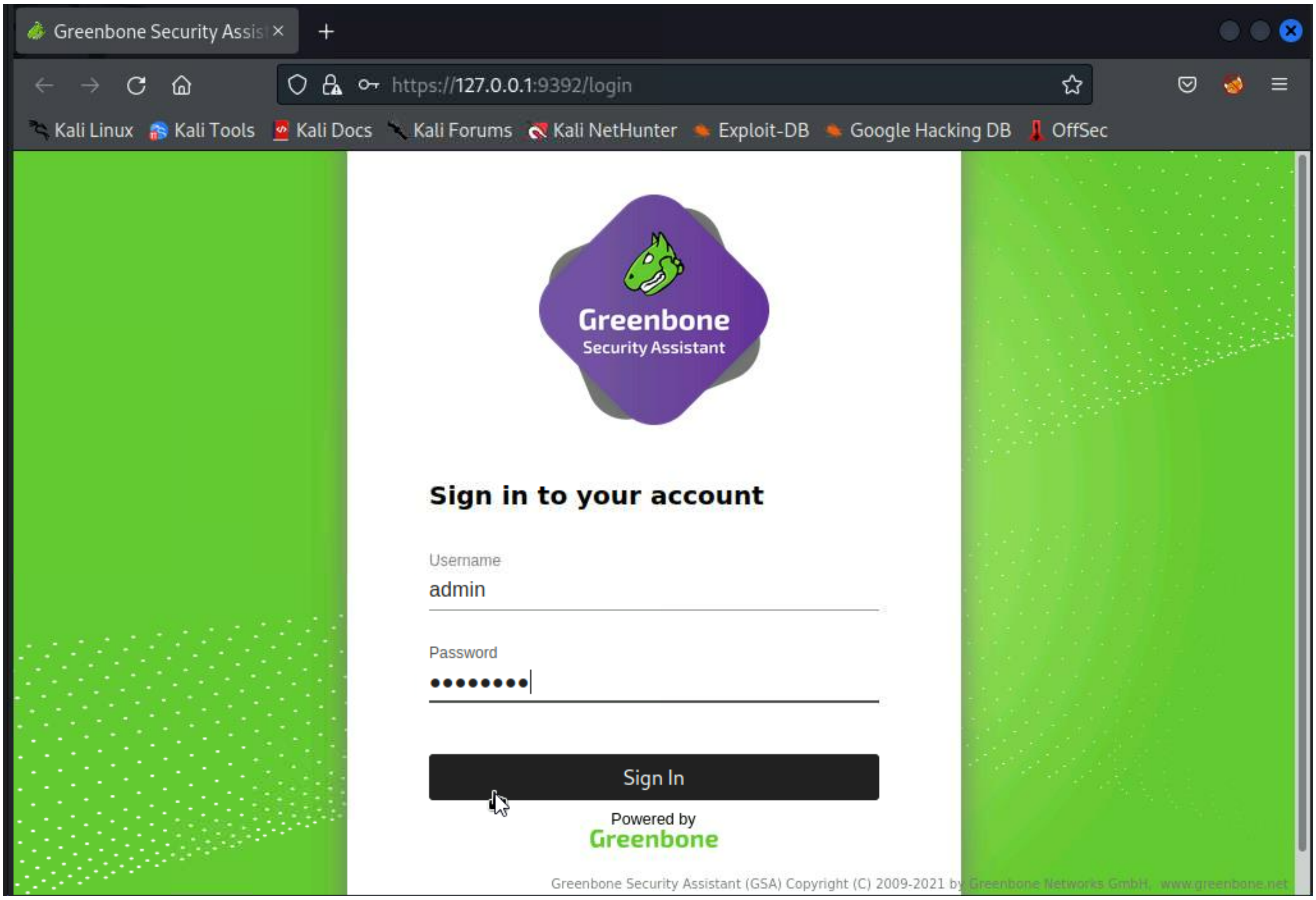
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 127.0.0.1:9392 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

The **Greenbone Security Assistant** login page is displayed.

Type the credentials in the Username and Password text box and click Login.



Sign in to your account

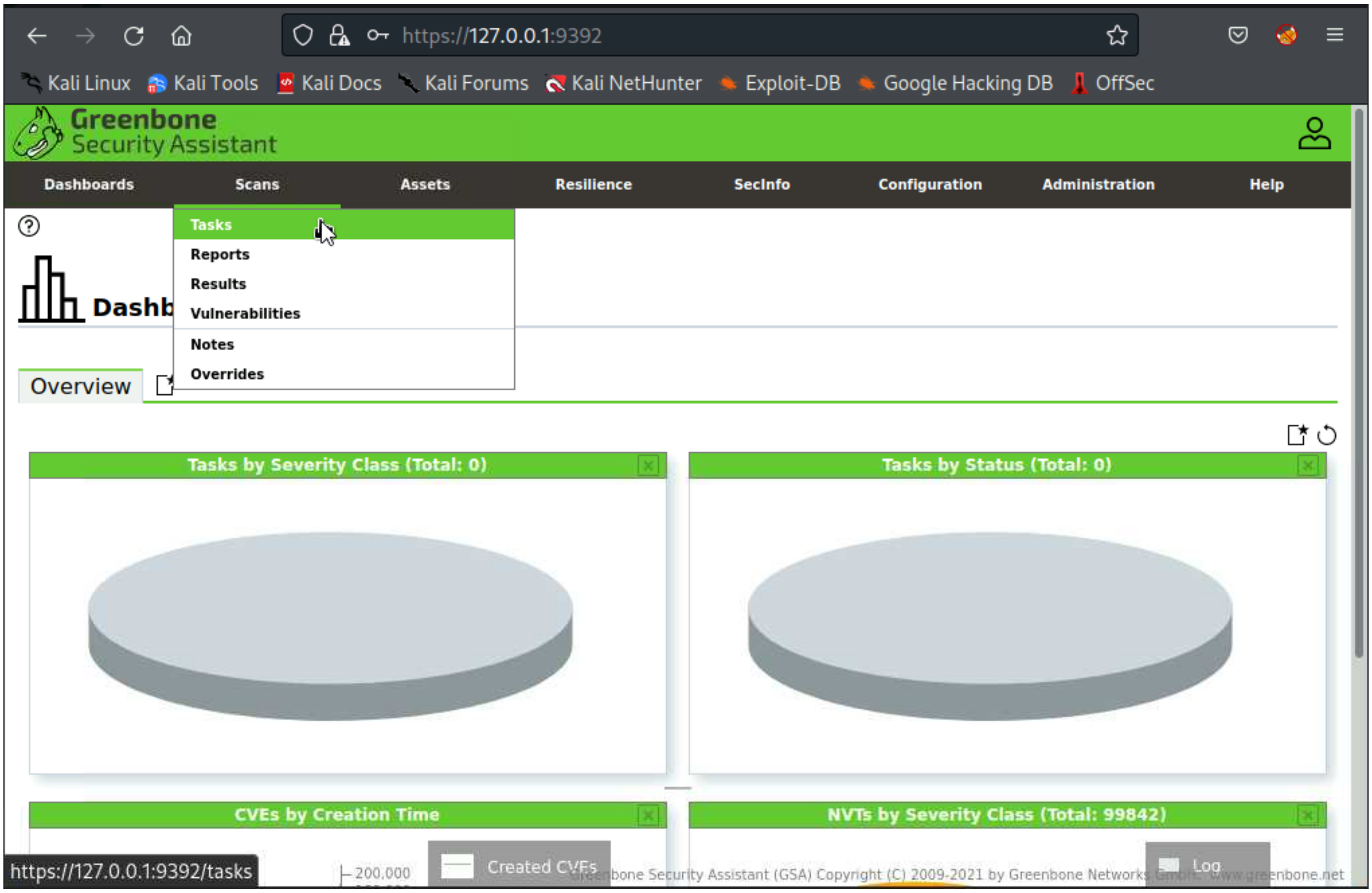
Username
admin

Password
••••••••

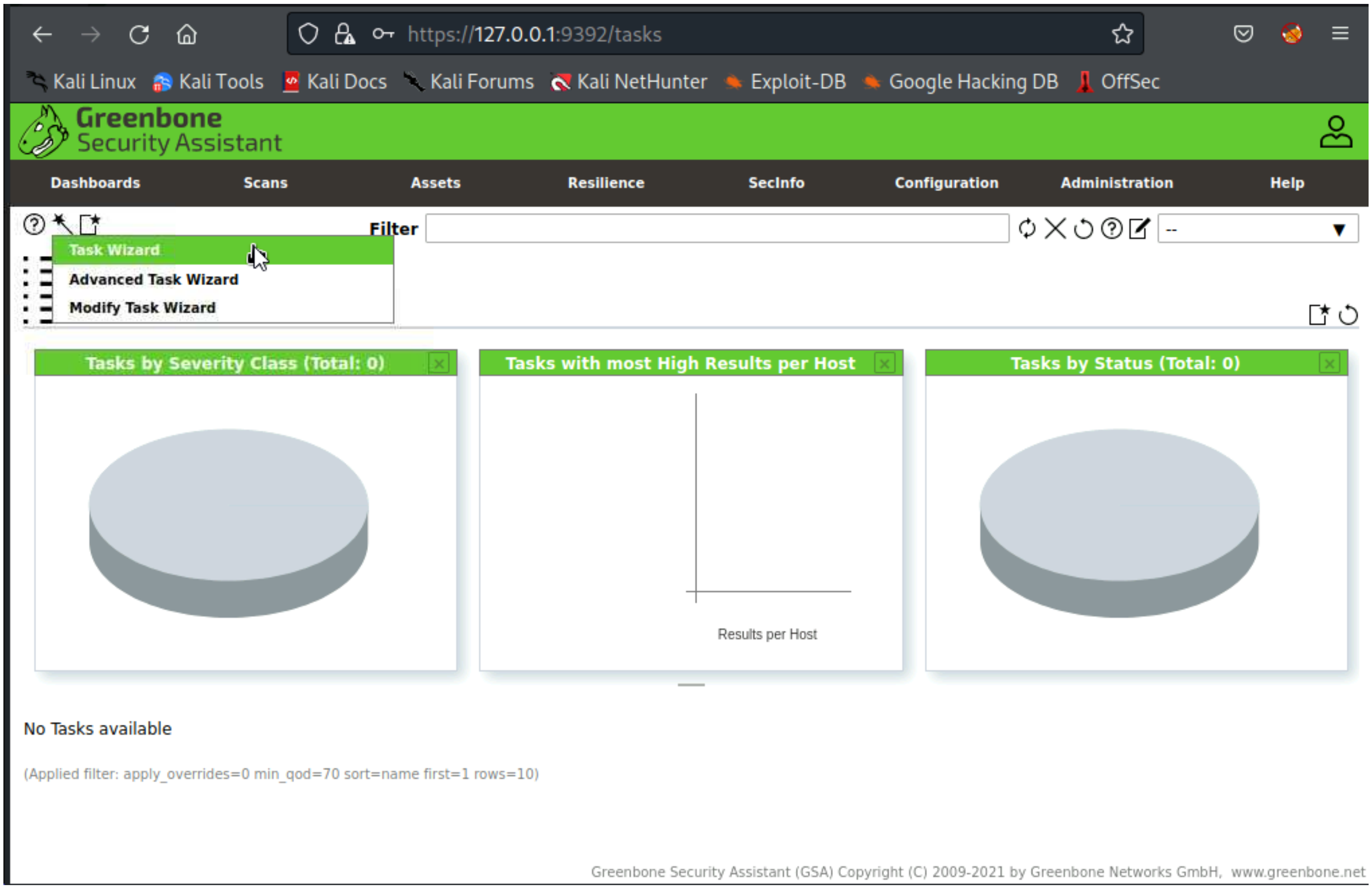
Greenbone Security Assistant
https://127.0.0.1:9392/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Security Assistant
Sign In
Powered by
Greenbone
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

The dashboard for OpenVAS is displayed.

Click **Scans** and select **Tasks**.



The **Tasks** page is displayed. Click **Task Wizard** on the upper left side — just below the menu.



No Tasks available

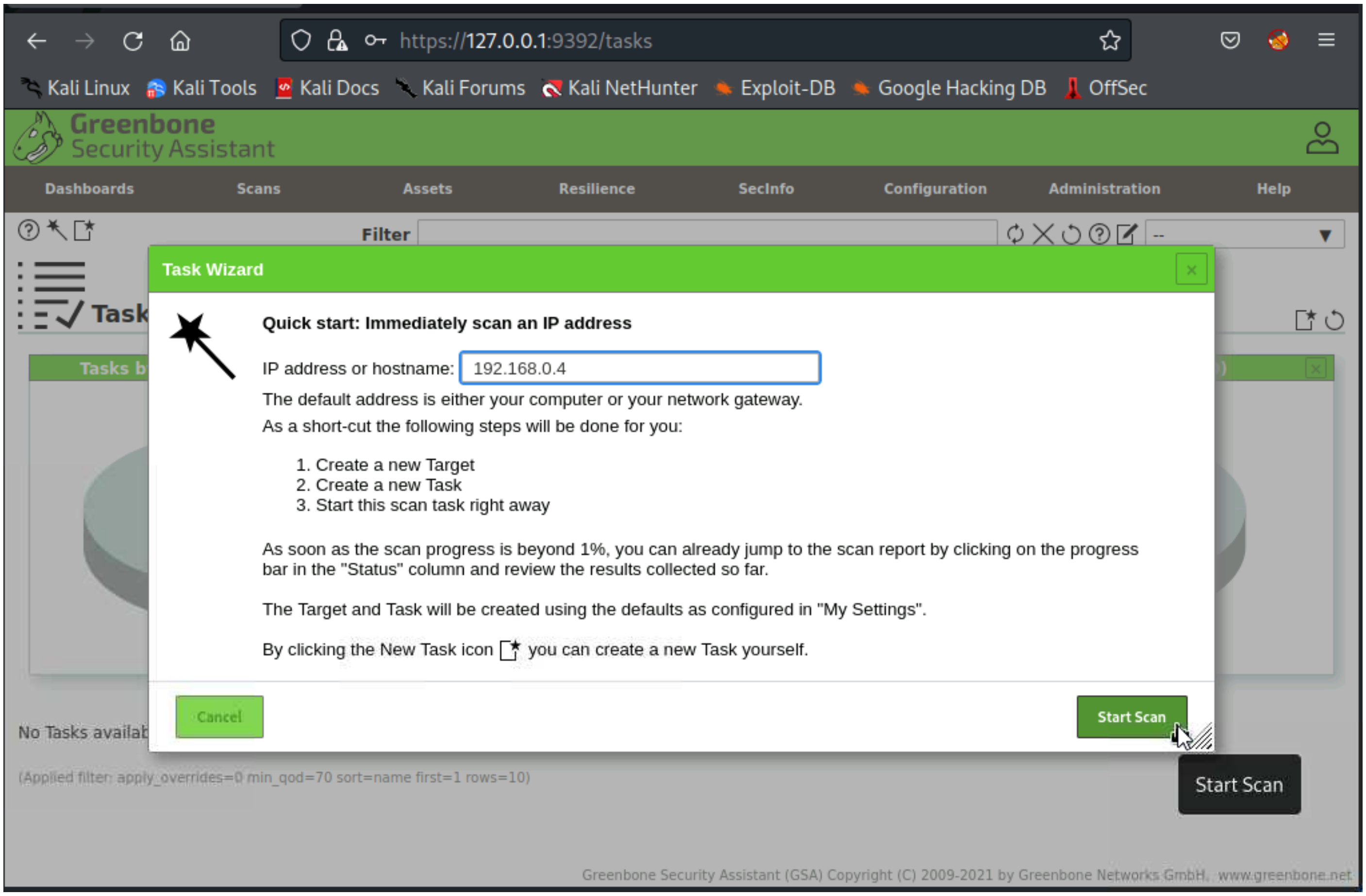
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

In the **Task Wizard** pop-up window, enter the following in the **IP address or hostname** field:

```
192.168.0.4
```

Click **Start Scan**



Quick start: Immediately scan an IP address

IP address or hostname: 192.168.0.4

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

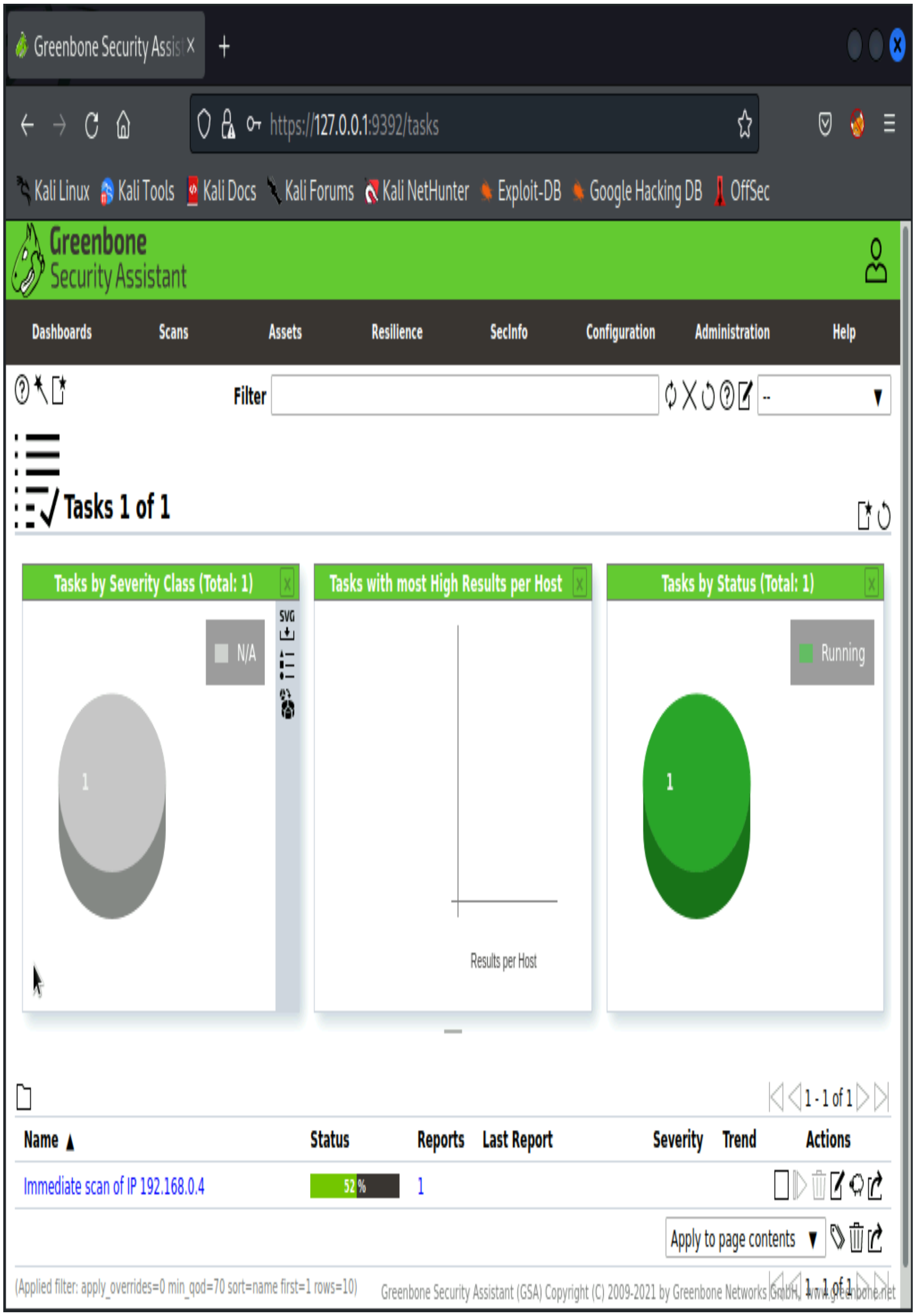
By clicking the New Task icon you can create a new Task yourself.

No Tasks availab

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

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Wait for the scan to complete. This may take up to 10 minutes.

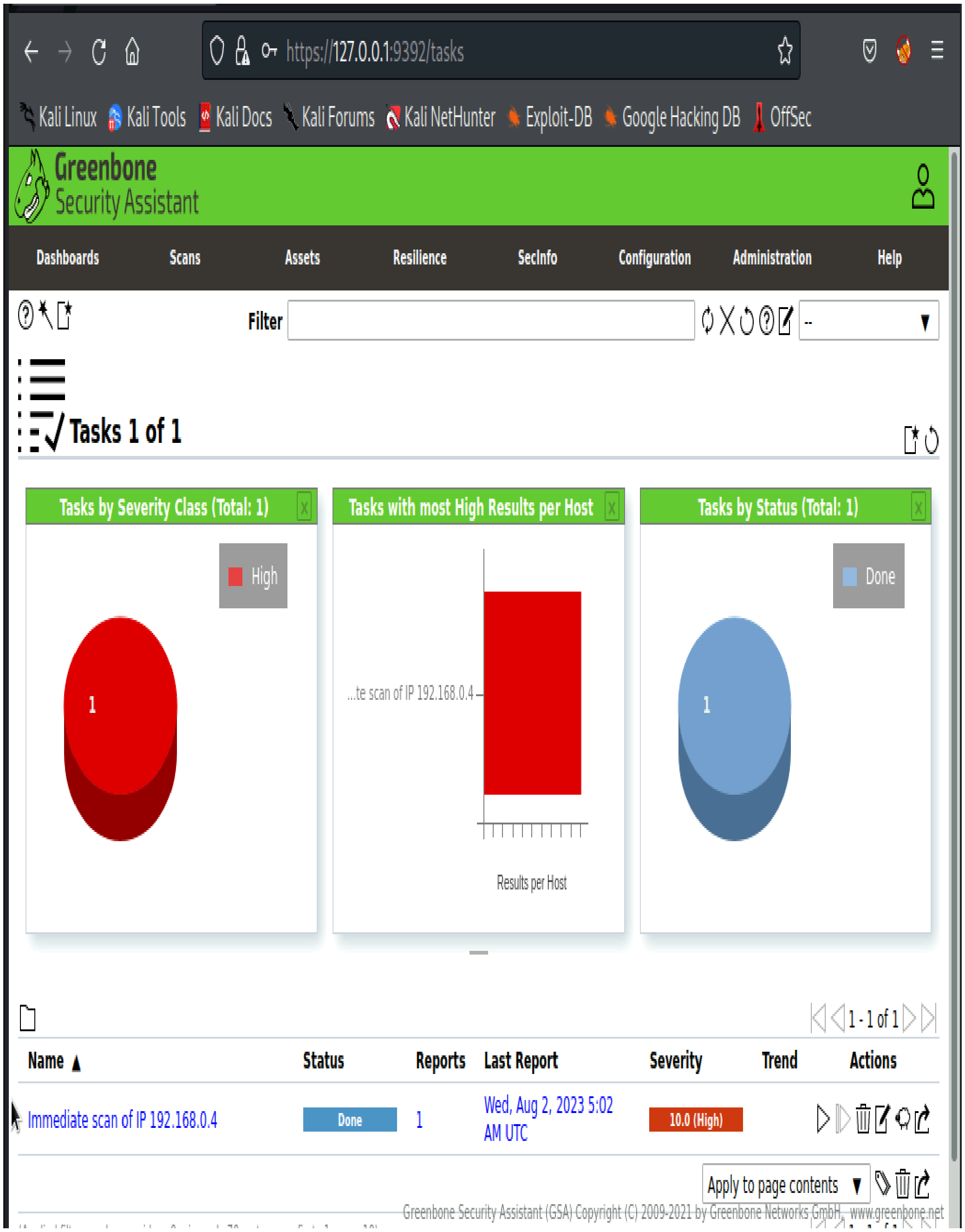


Tasks 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.0.4	52 %	1				

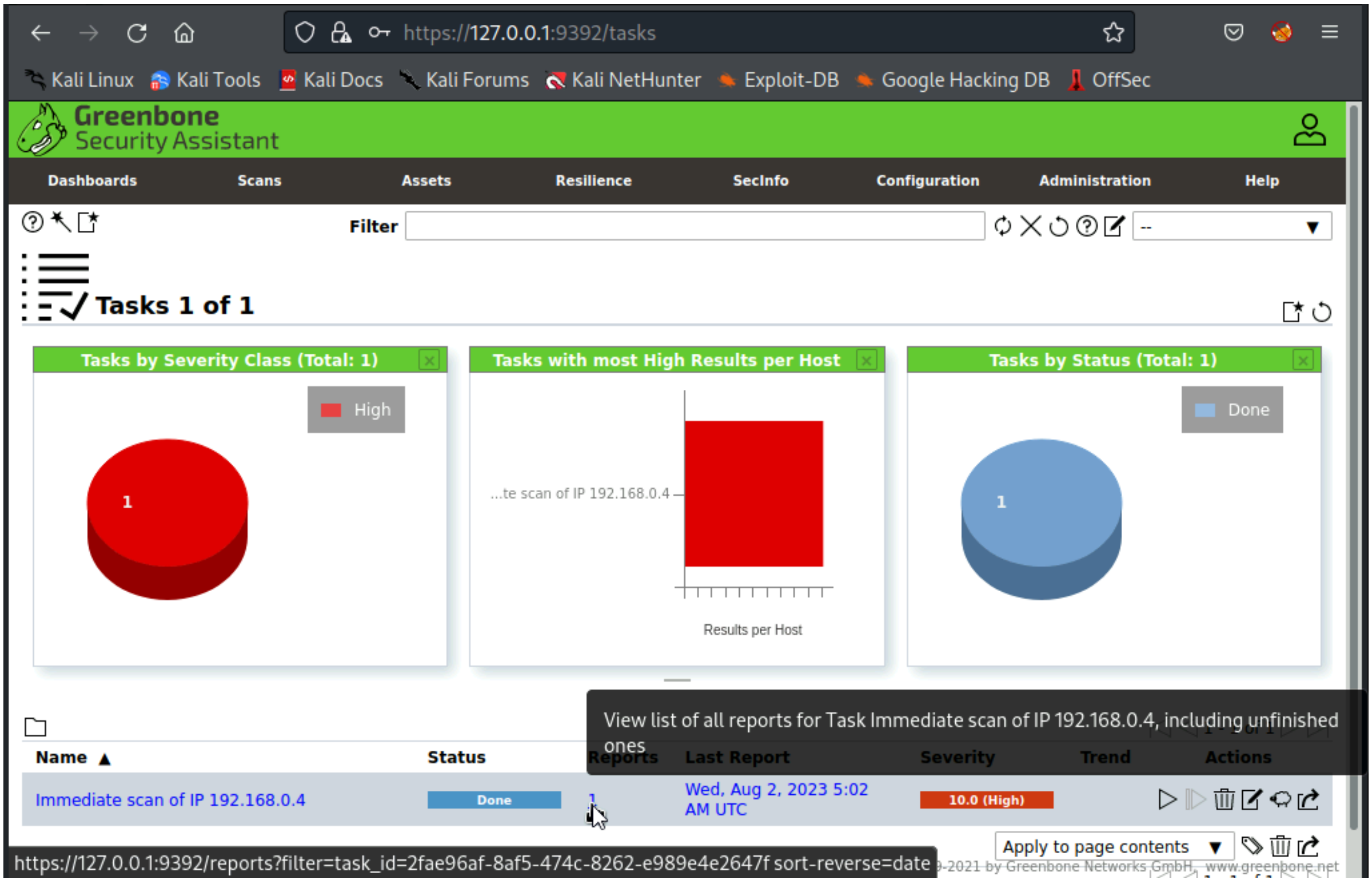
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.0.4	Done	1	Wed, Aug 2, 2023 5:02 AM UTC	10.0 (High)		

On **Task 1 of 1,** click **1** in the **Reports** field.



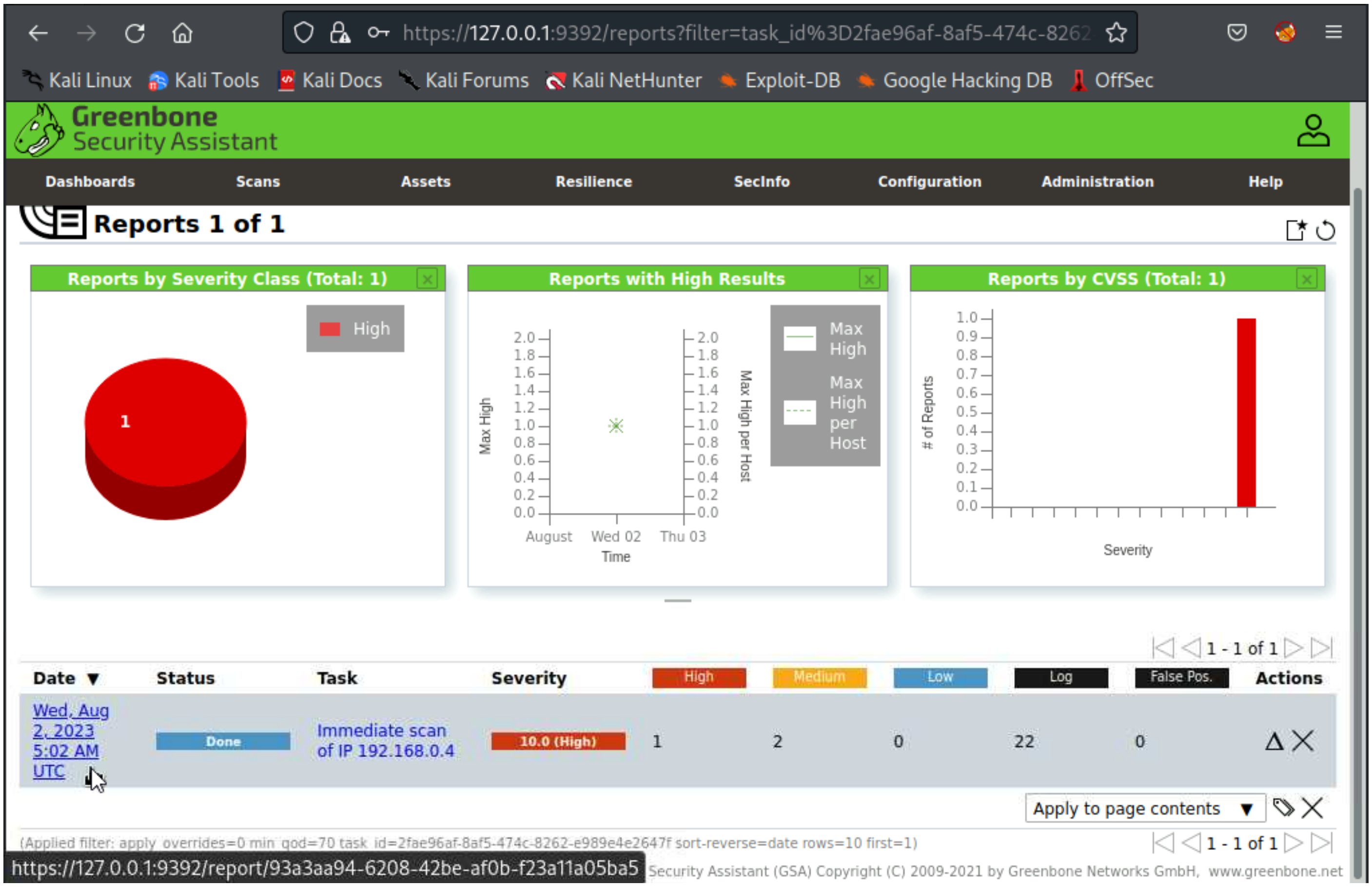
View list of all reports for Task Immediate scan of IP 192.168.0.4, including unfinished ones

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.0.4	Done	1	Wed, Aug 2, 2023 5:02 AM UTC	10.0 (High)		

https://127.0.0.1:9392/reports?filter=task_id=2fae96af-8af5-474c-8262-e989e4e2647f sort-reverse=date

-2021 by Greenbone Networks GmbH, www.greenbone.net

Click the entry in the **Date** field.



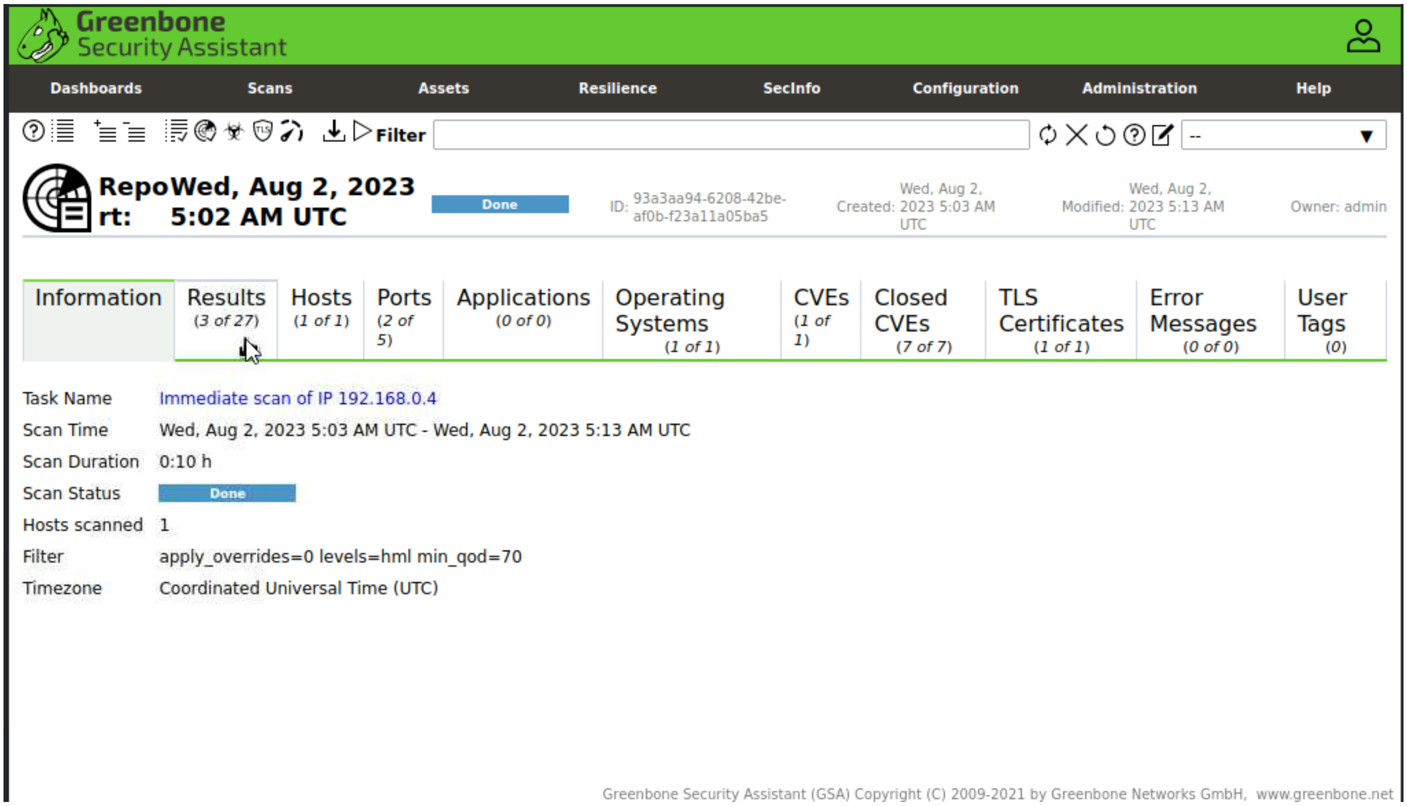
Reports 1 of 1

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Aug 2, 2023 5:02 AM UTC	Done	Immediate scan of IP 192.168.0.4	10.0 (High)	1	2	0	22	0	△ ✕

(Applied filter: apply_overrides=0 min_qod=70 task_id=2fae96af-8af5-474c-8262-e989e4e2647f sort-reverse=date rows=10 first=1)

Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

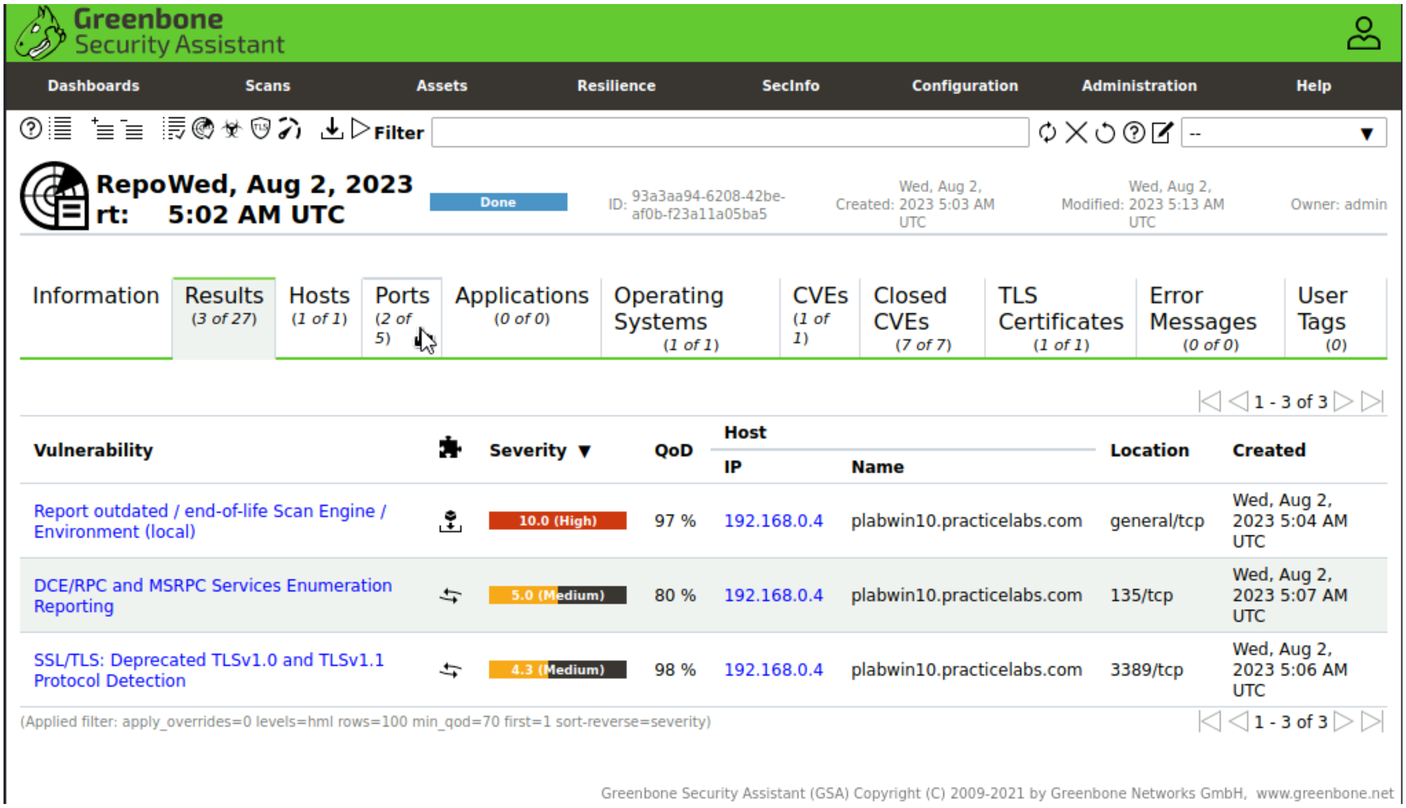
Select the **Results** field on the **Immediate scan of IP 192.168.0.4** task results window.



Task Name	Immediate scan of IP 192.168.0.4
Scan Time	Wed, Aug 2, 2023 5:03 AM UTC - Wed, Aug 2, 2023 5:13 AM UTC
Scan Duration	0:10 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Select **Ports** on the **Immediate scan of IP 192.168.0.4** task results window.



Report: Wed, Aug 2, 2023 5:02 AM UTC

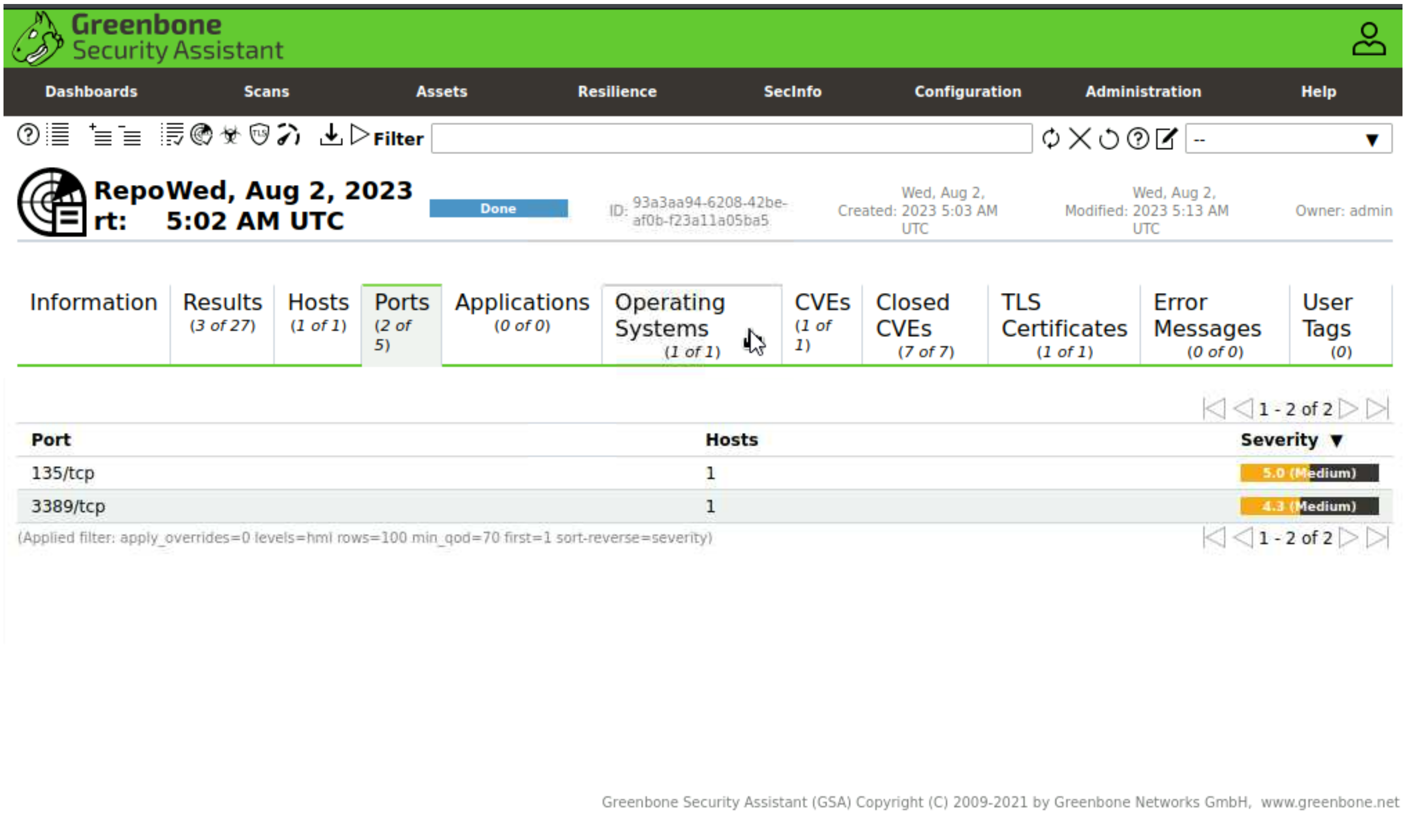
ID: 93a3aa94-6208-42be-af0b-f23a11a05ba5 Created: Wed, Aug 2, 2023 5:03 AM UTC Modified: Wed, Aug 2, 2023 5:13 AM UTC Owner: admin

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.0.4	plabwin10.practicelabs.com	general/tcp	Wed, Aug 2, 2023 5:04 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80 %	192.168.0.4	plabwin10.practicelabs.com	135/tcp	Wed, Aug 2, 2023 5:07 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.3 (Medium)	98 %	192.168.0.4	plabwin10.practicelabs.com	3389/tcp	Wed, Aug 2, 2023 5:06 AM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

In the **Ports** field, the open ports of the scanned host are displayed.



RepoWed, Aug 2, 2023
rt: 5:02 AM UTC

ID: 93a3aa94-6208-42be-af0b-f23a11a05ba5
Created: Wed, Aug 2, 2023 5:03 AM UTC
Modified: Wed, Aug 2, 2023 5:13 AM UTC
Owner: admin

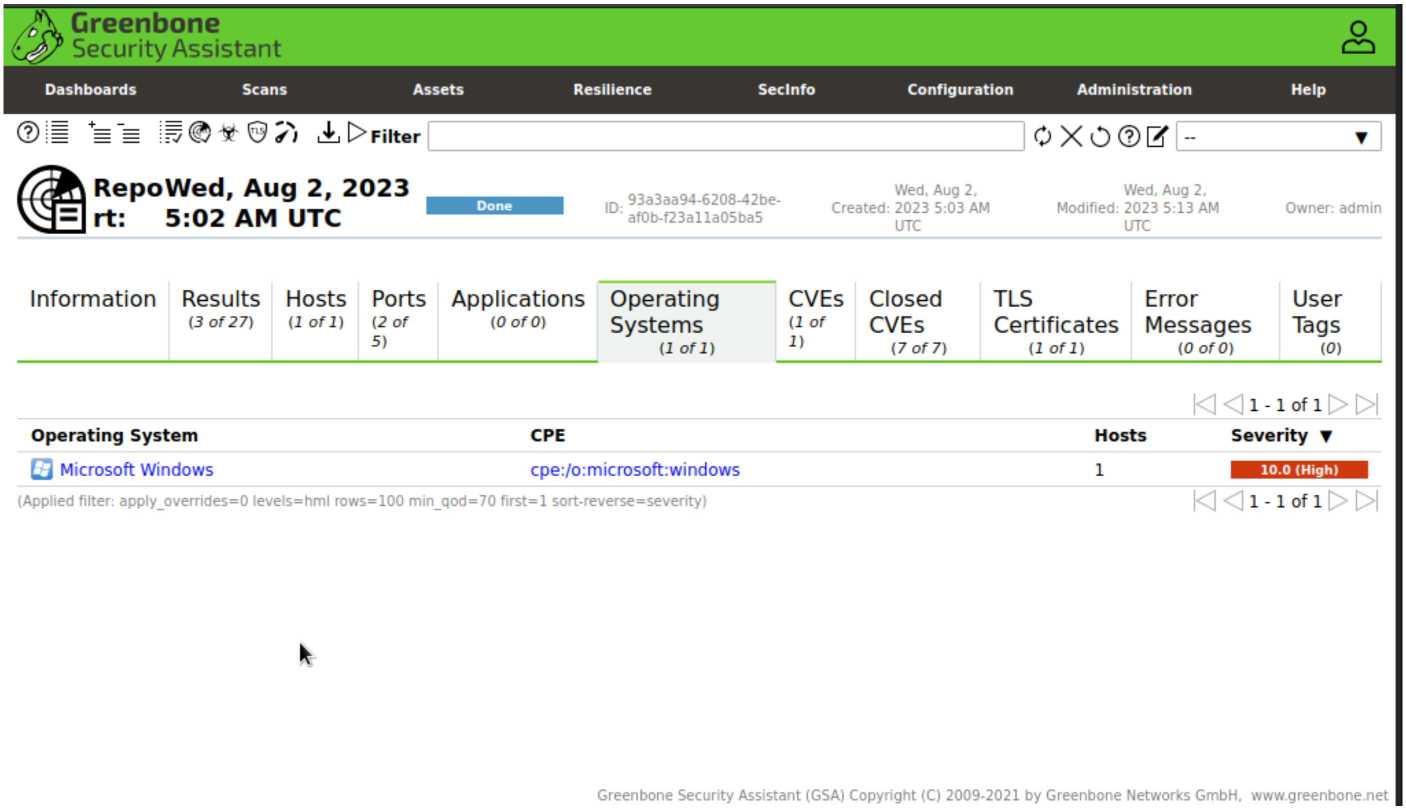
Port	Hosts	Severity ▼
135/tcp	1	5.0 (Medium)
3389/tcp	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Select **Operating Systems** on the **Task** window.

The scanned host’s operating system is identified as Microsoft Windows. Several other fields of information gathered from the scanned host can be explored.



Report: Wed, Aug 2, 2023 5:02 AM UTC

Done

ID: 93a3aa94-6208-42be-af0b-f23a11a05ba5

Created: Wed, Aug 2, 2023 5:03 AM UTC

Modified: Wed, Aug 2, 2023 5:13 AM UTC

Owner: admin

Operating System	CPE	Hosts	Severity ▼
Microsoft Windows	cpe:/o:microsoft:windows	1	10.0 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)