

Kali OpenVas Scan 01

This presentation shows configuring and scanning a host using OpenVas in Kali. The presentation will create a target. The presentation will create a task. The presentation will run a scan. The presentation will download a PDF copy of the scan report.

Hardware/Software Used in Presentation

Kali version 2016.2

OpenVAS version 9.0

VMware Player 12.5.5

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?r=1&token=59cc0465-b8d0-417b-a951-de | Search

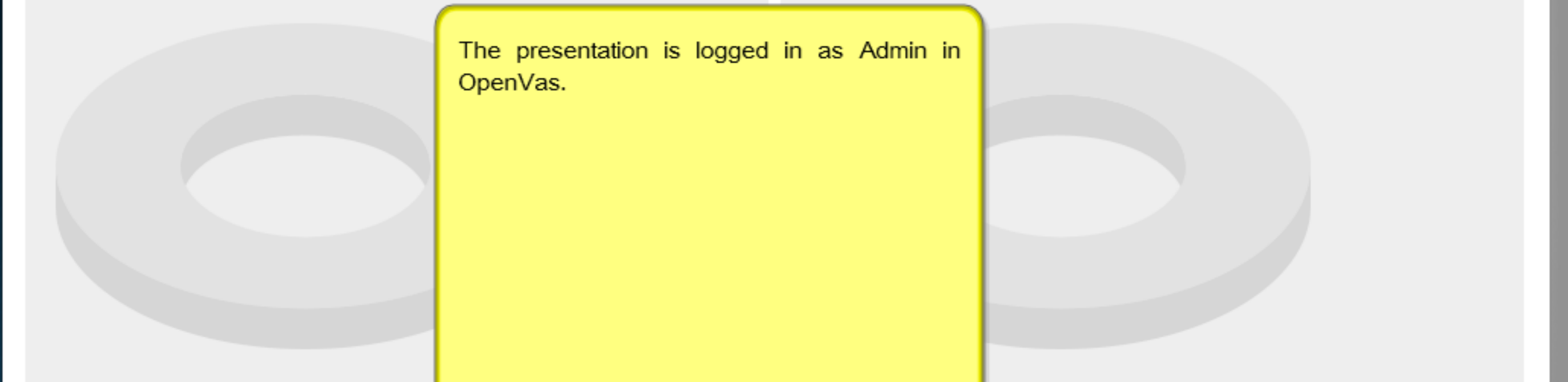
Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant | No auto-refresh | Logged in as Admin **admin** | Logout | Fri Apr 21 15:00:55 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Dashboard

Tasks by Severity Class (Total: 0) | Tasks by status (Total: 0)



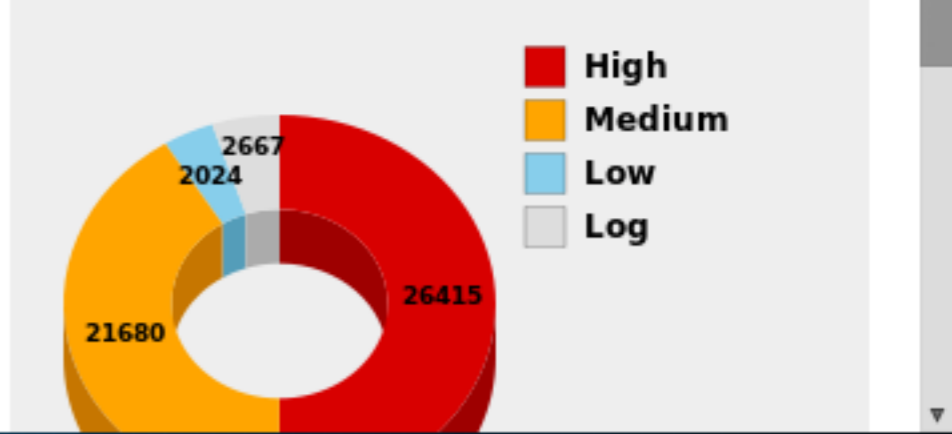
The presentation is logged in as Admin in OpenVas.

CVEs by creation time (Total: 8548)



No hosts with topology selected

NVTs by Severity Class (Total: 52786)



Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant

Refresh every 30 Sec. | Logged in as Admin **admin** | Logout | Fri Apr 21 15:17:32 2017 UTC

- Dashboard
- Scans
- Assets
- SecInfo
- Configuration**
- Extras
- Administration
- Help

- Targets**
- Port Lists
- Credentials
- Configs
- es
- Formats
- Scanners
- Filters
- Tags
- Permissions

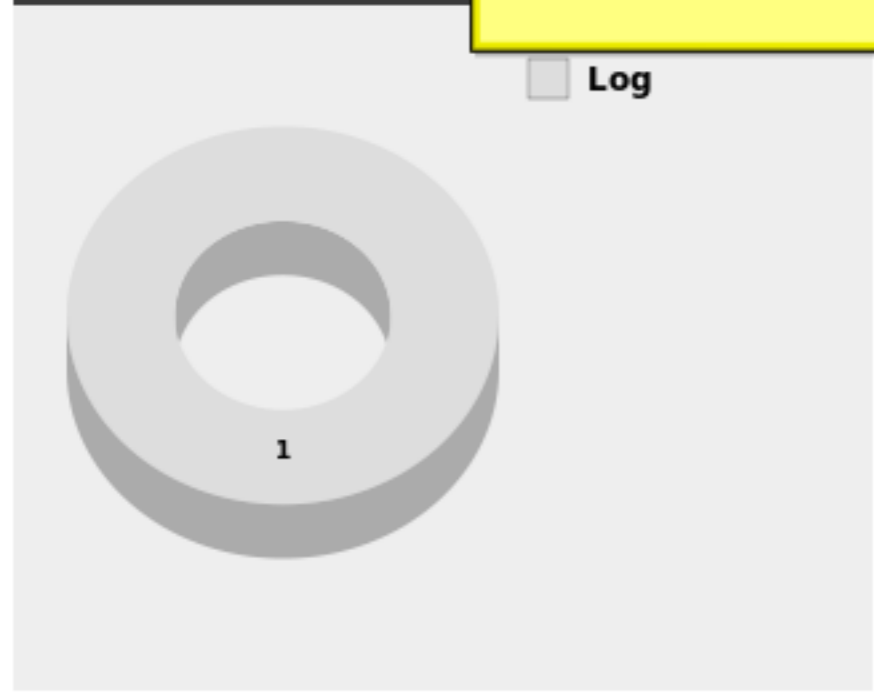
Under the "Configuration" option, the presentation selects "Targets".

Filter:

min_qod=70 app

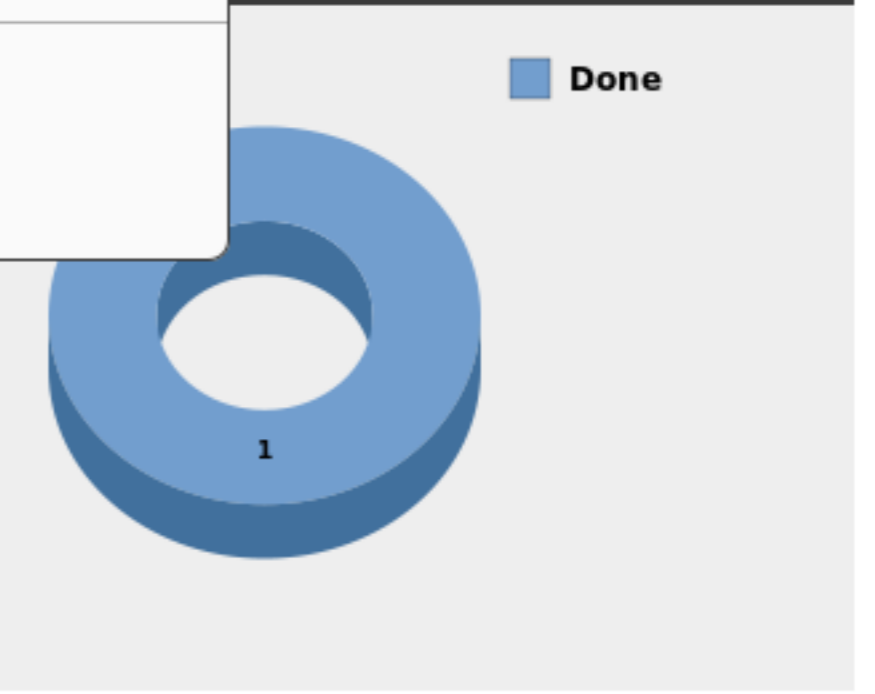
Tasks (1 of 1)

Tasks by Severity



No Tasks with High severity found

Tasks by status (Total: 1)



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampltask01				0.0 (Log)		

1 - 1 of 1

https://127.0.0.1:9392/omp?cmd=get_targets&token=59cc0465-b8d0-417b-a951-dec8e0381962

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x +


https://127.0.0.1:9392/omp?cmd=get_targets&target_id=fc69dc00-75a... | Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant Refresh every 30 Sec. Logged in as Admin **admin** | Logout
Fri Apr 21 15:20:41 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

? * ← The presentation selects the blue box with the white star.

 **Targets**

Name	Actions

(Applied filter: row...)

Backend operation

Filter:    

rows=10 first=1 sort=name

Credentials - sort by: SSH   **Actions**

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_targets&token=59cc0465-b8d0- Search

- Most Visited
- Offensive Security
- Kali Linux
- Kali Docs
- Kali Tools
- Exploit-DB
- Aircrack-ng

Green Security

Dashboard

Target

Name

(Applied filter: rows)

Backend operation: 0

New Target

Name:

Comment:

Hosts:

 Manual

 From file No file selected

 From host assets (0 hosts)

Exclude Hosts:

Reverse Lookup Only: Yes No

Reverse Lookup Unify: Yes No

Port List:

Alive Test:

Credentials for authenticated checks:

SSH

SMB

The presentation is scanning only one host. You may put a subnet range in this box.

Remember, you must have permission from the network owner to run a scan.

- All IANA assigned TCP 2012-02-10
- All IANA assigned TCP and UDP 2012-02-10
- All privileged TCP
- All privileged TCP and UDP
- All TCP
- All TCP and Nmap 5.51 top 100 UDP

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_targets&token=59cc0465-b8d0- | Search

- Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Green Security

Dashboard

Target

Name

(Applied filter: rows)

Backend operation: 0

New Target

Manual
 From file No file selected.
 From host assets (0 hosts)

Exclude Hosts

Reverse Lookup Only Yes No

Reverse Lookup Unify Yes No

Port List ★

Alive Test

Credentials for authenticated checks

SSH on port ★

SMB ★

ESXi ★

SNMP ★

Logout

2017 UTC

ns

greenbone.net

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x
https://127.0.0.1:9392/omp?cmd=get_targets&token=59cc0465-b8d0- Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

New Target

Name:

Comment:

Hosts: Manual
 From file No file selected.
 From host assets (0 hosts)

Exclude Hosts:

Reverse Lookup Only: Yes No

Reverse Lookup Unify: Yes No

Port List: ★

Alive Test:

on port ★

★

The presentation selects "Create" to make an OpenVas target.

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_targets&token=59cc0465-b8d0- Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant No auto-refresh Logged in as Admin **admin** | Logout
 Fri Apr 21 15:04:31 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: rows=10 first=1 sort=name

Targets (1 of 1)

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Example01 (Example Scan)	192.168.241.2	1	All IANA assigned TCP 2012-02-10		[Icons]

1 - 1 of 1

√Apply to page contents

(Applied filter: rows=10 first=1 sort=name)

Backend operation: 0.04s

The OpenVas target named "Example01" is ready.

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant | Refresh every 30 Sec. | Logged in as Admin admin | Logout Fri Apr 21 15:17:32 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks with most High results per host

Tasks by status (Total: 1)

1

No Tasks with High severity found

Done

1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampltask01				0.0 (Log)		

1 2017

Under the "Scans" menu, the presentation selects the "Tasks" option.

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&token=59cc0465-b8d0-4...

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant Refresh every 30 Sec. Logged in as Admin **admin** | Logout Fri Apr 21 15:21:01 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

New Task New Container Task

apply_overrides=1 rows=10 first=1 sort=name

The presentation selects the blue box with the white star. The presentation then selects "New Task".

Tasks (0 of 0)

Tasks by Severity High results per host Tasks by status (Total: 0)

High severity found

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
[Empty Row]						

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x
https://127.0.0.1:9392/omp?cmd=get_tasks&token=59cc0465-b8d0-4...

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant | No auto-refresh | Logged in as Admin admin | Logout | Fri Apr 21 15:04:45 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

New Task

Name

Comment

Scan Targets

Alerts

Schedule Once

Add results to Assets yes no

Apply Overrides yes no

Min QoD %

Alterable Task yes no

Auto Delete Reports Do not automatically delete reports
 Automatically delete oldest reports but always keep newest reports

Scanner

Create

The presentation completes the requested information as shown.

Name	Total	Last
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)		

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&token=59cc0465-b8d0-4...

Search

- Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant No auto-refresh Logged in as Admin admin | Logout Fri Apr 21 15:04:45 2017 UTC

- Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

New Task

Assets

Apply Overrides yes no

Min QoD %

Alterable Task yes no

Auto Delete Reports Do not automatically delete reports

Automatically delete oldest reports but always keep newest reports

Scanner

Scan Config

Network Source Interface

Order for target hosts

Maximum concurrently executed NVTs per host

Maximum concurrently scanned hosts

The presentation completes the requested information as shown.

Create

Name	Total	Last
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)		

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

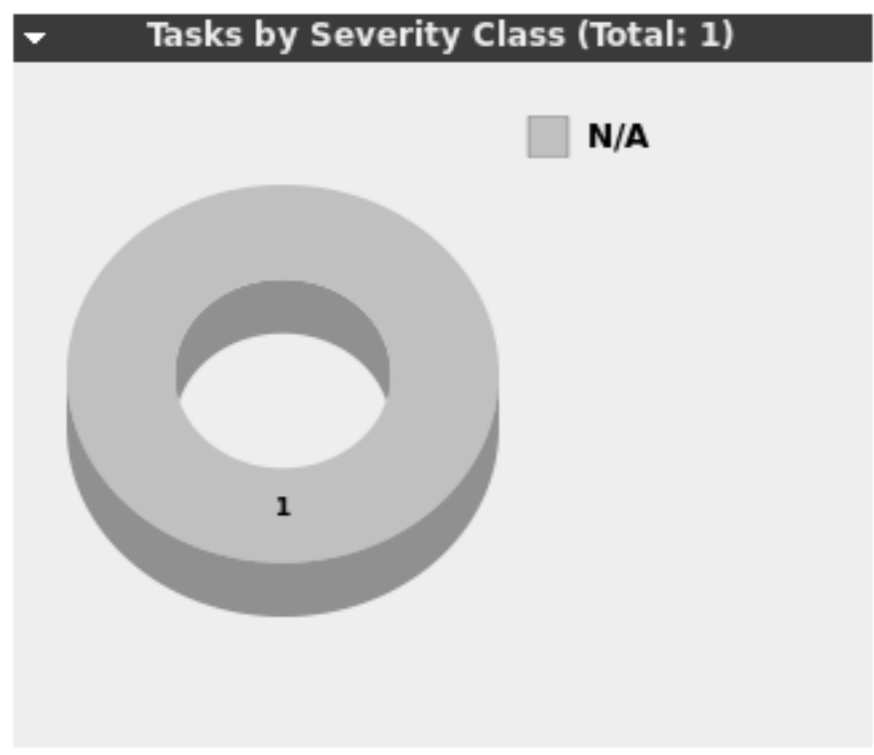
https://127.0.0.1:9392/omp?cmd=get_tasks&token=59cc0465-b8d0-4...

Search

- Most Visited
- Offensive Security
- Kali Linux
- Kali Docs
- Kali Tools
- Exploit-DB
- Aircrack-ng

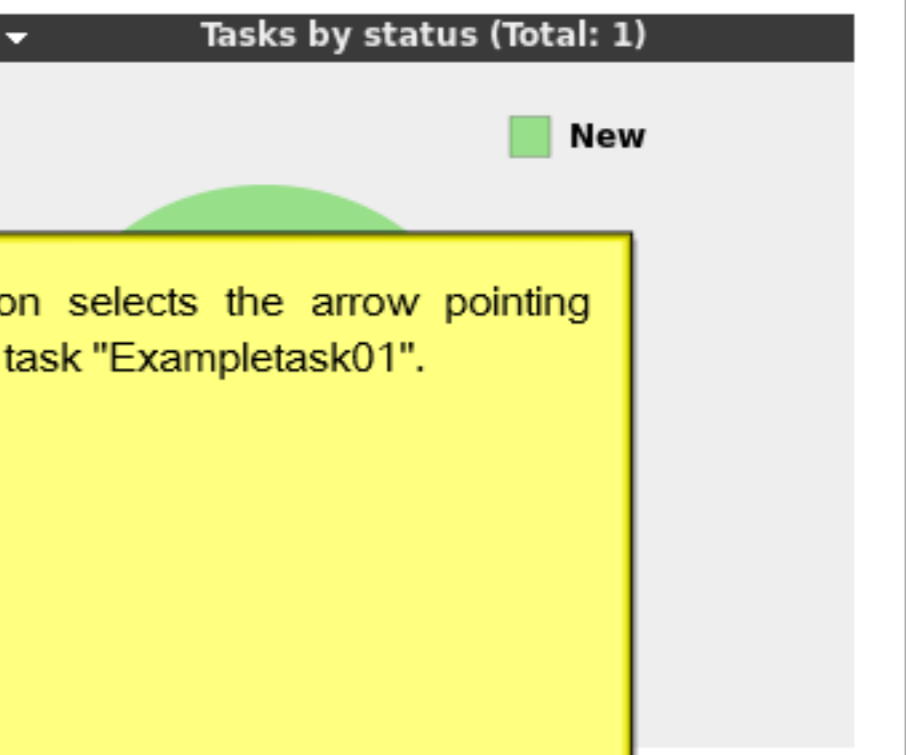
- Dashboard
- Scans
- Assets
- SecInfo
- Configuration
- Extras
- Administration
- Help

Tasks (1 of 1)



Tasks with most High results per host

No Tasks with High severity



The presentation selects the arrow pointing right to start the task "Exampletask01".

Name	Status	Total		Severity	Trend	Actions
		Total	Last			
Exampletask01 (This is an example task using the example target 01)	New					

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

1 - 1 of 1

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant No auto-refresh Logged in as Admin **admin** | Logout Fri Apr 21 15:06:36 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks (1 of 1)

Tasks by Severity Class (Total: 1)

N/A

1

Tasks with most High results per host

Severity found

Tasks by status (Total: 1)

Requested

1

The task "Exampletask01" is preparing to start.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampletask01 (This is an example task using the example target 01)	Requested	0	(1)			[Icons]

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant

Refresh every 30 Sec. | Logged in as Admin **admin** | Logout | Fri Apr 21 15:06:36 2017 UTC

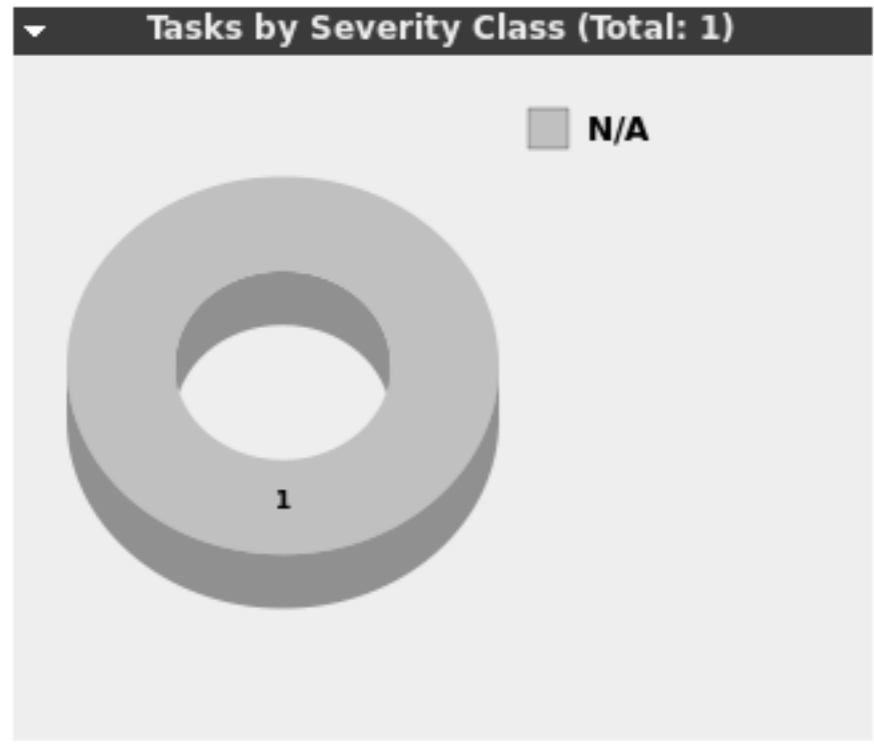
- Dashboard
- Scans
- Assets
- SecInfo
- Configuration
- Tasks
- Administration
- Help

Tasks (1 of 1)

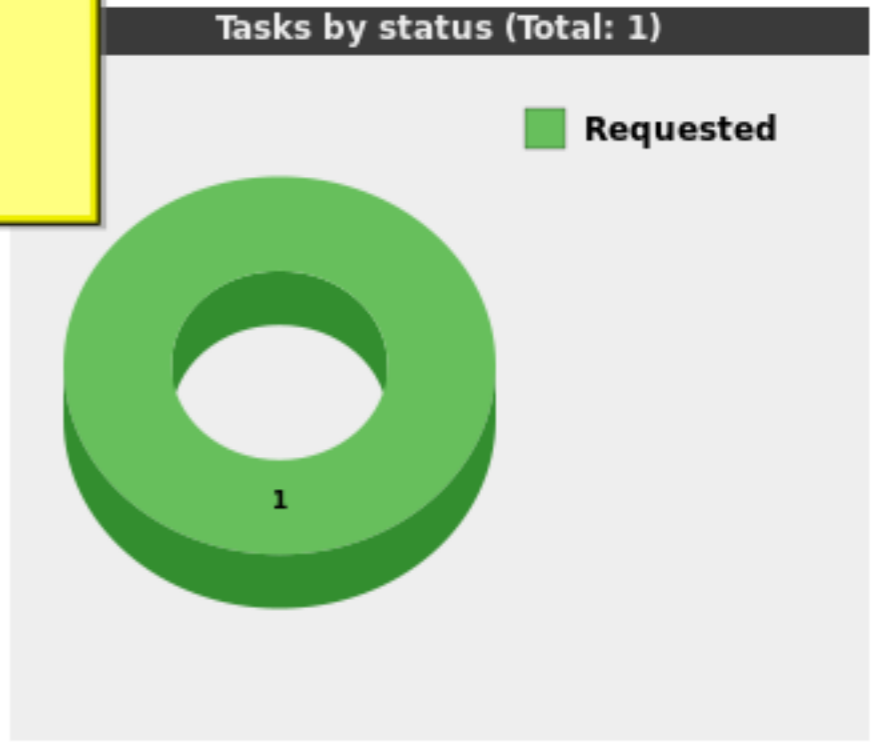
Tasks by Severity Class (Total: 1)

Tasks by status (Total: 1)

OpenVas does not automatically refresh. The presentation sets OpenVas to refresh every 30 seconds by changing the menu as shown.



No Tasks with High severity found



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampletask01 (This is an example task using the example target 01)	Requested	0	(1)			

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant Refresh every 30 Sec. Logged in as Admin **admin** | Logout Fri Apr 21 15:17:01 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks (1 of 1)

Tasks by Severity Class (Total: 1)

Log

Tasks with most High results per host

Tasks by status (Total: 1)

Done

The task "Exampletask01" is complete.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampletask01 (This is an example task using the example target 01)	Done	1 (1)	Apr 21 2017	0.0 (Log)		[Icons]

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_tasks&filt_id=&filter=&task_id=

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant Refresh every 30 Sec. Logged in as Admin **admin** | Logout Fri Apr 21 15:17:32 2017 UTC

- Dashboard
- Scans**
- Assets
- SecInfo
- Configuration
- Extras
- Administration
- Help

- Dashboard
- Tasks
- Reports**
- Results
- Notes

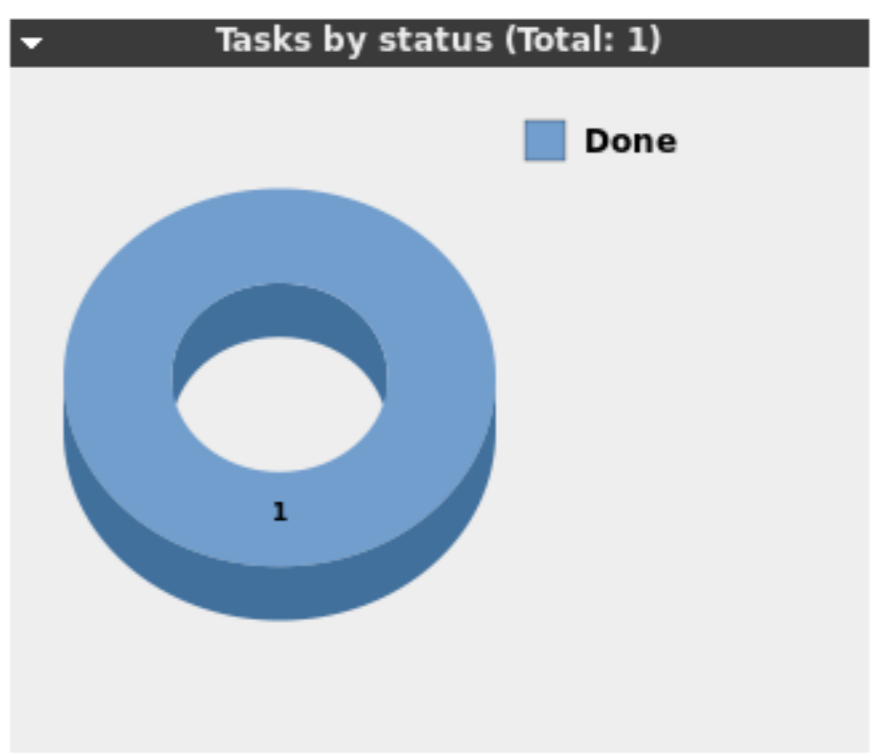
Filter:

min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Under the "Scans" menu, the presentation selects the "Reports" option.

Tasks with most High results per host

No Tasks with High severity found



1 - 1 of 1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Exampltask01				0.0 (Log)		

https://127.0.0.1:9392/omp?cmd=get_reports&token=59cc0465-b8d0-417b-a951-dec8e0381962

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x
https://127.0.0.1:9392/omp?cmd=get_reports&token=59cc0465-b8d0- Search

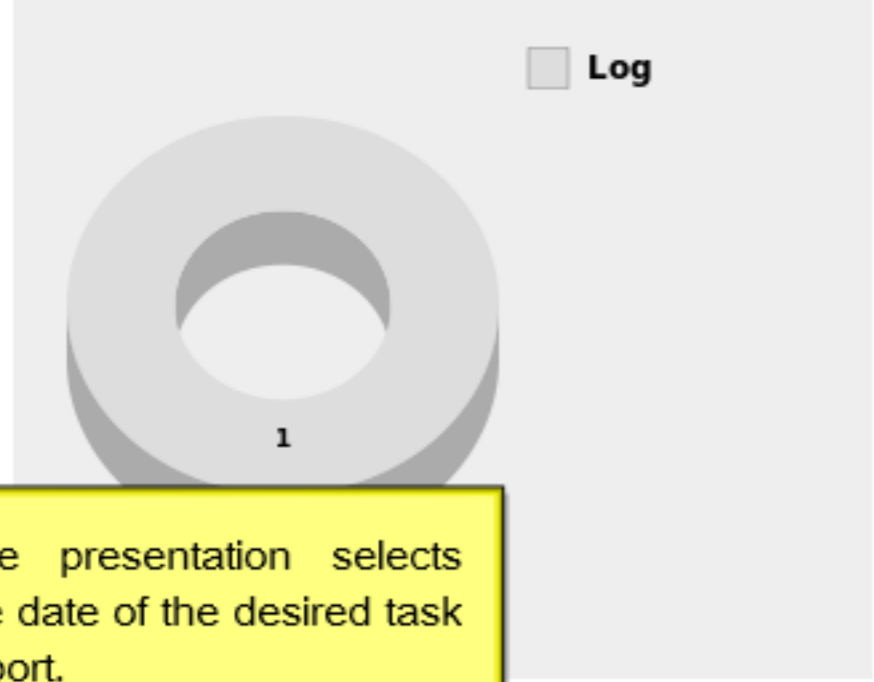
Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

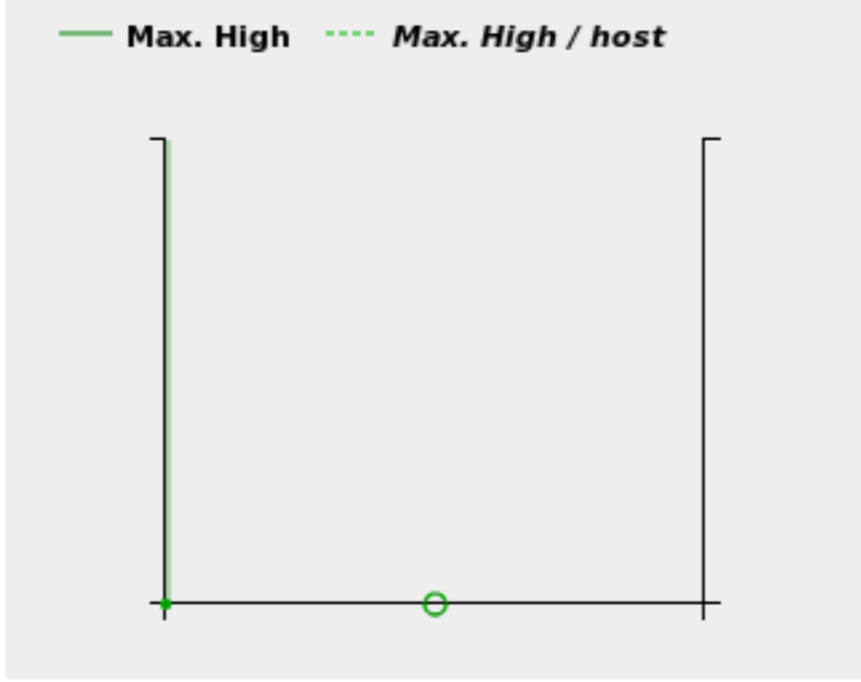


Reports (1 of 1)

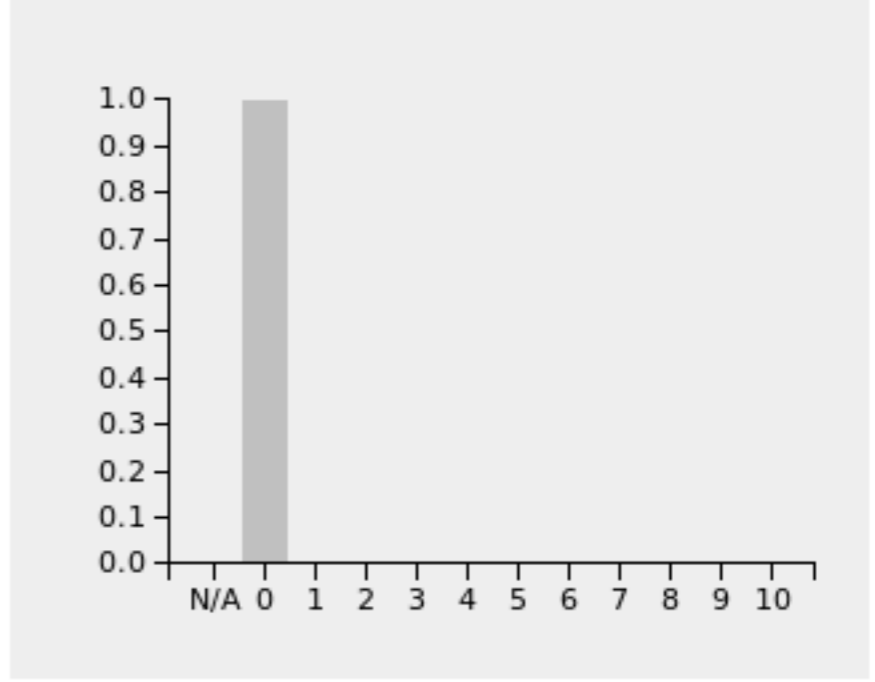
Reports by Severity Class (Total: 1)



Reports: High results timeline



Reports by CVSS (Total: 1)



The presentation selects the date of the desired task report.

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Fri Apr 21 15:06:36 2017	Done	Exampletask01	0.0 (Log)	0	0	0	4	0	[Icons]

(Applied filter: min_qod=70 apply_overrides=1 rows=10 sort-reverse=date first=1)

vApply to page contents

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x
https://127.0.0.1:9392/omp?cmd=get_report&report_id=ac73b0e8-71f

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant | No auto-refresh | Logged in as Admin **admin** | Logout
Fri Apr 21 15:18:23 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Anonymous XML

- ITG
- LaTeX
- NBE
- PDF**
- Topology SVG
- TXT
- Verinice ISM
- Verinice ITG

Filter:

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100
sort-reverse=severity levels=hml min_qod=70

ID: ac73b0e8-71f6-4685-b290-3149d40d47d4
Modified: Fri Apr 21 15:12:43 2017
Created: Fri Apr 21 15:06:45 2017
Owner: admin

Under the file type menu, the presentation selects PDF as the report file type.

Include log messages in your filter setting.

There may be results below the current minimum Quality of Detection level.

Decrease the minimum QoD in the Filter to 30 percent to see those results.

Your filter settings may be too refined.

Adjust and update your filter settings.

Your last filter change may be too restrictive.

Reset the filter settings to the defaults.

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security A... x

https://127.0.0.1:9392/omp?cmd=get_report&report_id=ac73b0e8-71f

Search

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng

Greenbone Security Assistant No auto-refresh Logged in as Admin **admin** | Logout
 Fri Apr 21 15:18:23 2017 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

PDF [Download Icon] The presentation selects the down arrow to download a copy of the scan report.

Done

1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100
 ls=hml min_qod=70

Report: Results (0 of 5)

ID: ac73b0e8-71f6-4685-b290-3149d40d47d4
 Modified: Fri Apr 21 15:12:43 2017
 Created: Fri Apr 21 15:06:45 2017
 Owner: admin

The report is empty. **The filter does not match any of 5 results.**

Log messages are currently excluded.

Include log messages in your filter setting.

There may be results below the current minimum Quality of Detection level.

Decrease the minimum QoD in the Filter to 30 percent to see those results.

Your filter settings may be too refined.

Adjust and update your filter settings.

Your last filter change may be too restrictive.

Reset the filter settings to the defaults.