

OpenVAS Reporting
Spring 2019

This presentation shows the use of a couple of shell scripts added by Tim Preuss to the kali__spring2019 image. The presentation walks through using OpenVAS.

System Notes:

Kali (Debian 4.19.28-2 Kalil (2019-03-18)

OpenVAS 9



The presentation logs into Kali.

```
root@kali-s2019a: ~/scripts
File Edit View Search Terminal Help
root@kali-s2019a:~# cd scripts/
root@kali-s2019a:~/scripts# ls
cleanup_kali.sh  openvas_notes.txt  setip.sh
feedupdate.sh   openvmtools.sh    update_kali.sh
root@kali-s2019a:~/scripts#
```

The presentation opens a terminal window. The presentation changes the directory as shown. The presentation lists the files in the ~/scripts directory.

```
root@kali-s2019a: ~/scripts
File Edit View Search Terminal Help
root@kali-s2019a:~# cd scripts/
root@kali-s2019a:~/scripts# ls
cleanup_kali.sh  openvas_notes.txt  setip.sh
feedupdate.sh   openvmtools.sh     update_kali.sh
root@kali-s2019a:~/scripts# ./update_kali.sh
```

The presentation runs the `update_kali.sh` script. This will update the software and operating system on Kali. Depending on a number of factors, this may take some time.

If the kernel is updated, please reboot Kali before continuing.



```
root@kali-s2019a: ~/scripts
File Edit View Search Terminal Help
root@kali-s2019a:~# cd scripts/
root@kali-s2019a:~/scripts# ls
cleanup_kali.sh  openvas_notes.txt  setip.sh
feedupdate.sh   openvmtools.sh     update_kali.sh
root@kali-s2019a:~/scripts# ./cleanup_kali.sh
```

The presentation runs the cleanup_kali.sh script. This will remove old files replaced by newer versions. This script is run after the update.




```
root@kali-s2019a: ~/scripts
File Edit View Search Terminal Help
root@kali-s2019a:~# cd scripts/
root@kali-s2019a:~/scripts# ls
cleanup_kali.sh  openvas_notes.txt  setip.sh
feedupdate.sh   openvmtools.sh     update_kali.sh
root@kali-s2019a:~/scripts# ./feedupdate.sh
```

The presentation runs the feedupdate.sh script. This script will update OpenVAS. This script may only be run once a day. This script will take some time to run. The script will report done at the end of the script.




The presentation selects the "show applications" icon (nine dots) . This will open another menu.

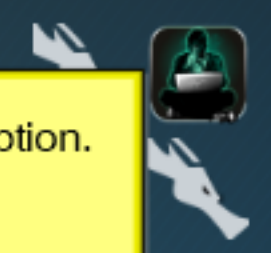
🔍 Type to search...



01-Information



02-Vulnerability



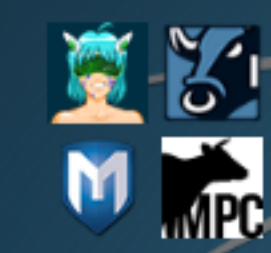
Password




06-Wireless



07-Reversing



08-Exploit




Forensics




12-Reporting

The presentation selects the "02-Vulnerability" option.



13-SETools



14-Services




Advanced Netw...



Archive Manager



Calculator




Characters



CherryTree



Chromium Web...




Contacts



Disk Usage Ana...



Disks



Document View...

🔍 Type to search...

- 01-Information
- 02-Vulnerability**
- 03-WebApps
- 04-Database
- 05-Password
- 06-Wireless

The presentation moves the slider bar down for the next screen.

bed, cisco-auditing-t..., cisco-global-ex..., co..., dhcpig, enumiax, golismero, iaxflood, inviteflood, lynis, merge-router-c..., nikto, nmap, ohrwurm, openvas check s..., openvas feed up...

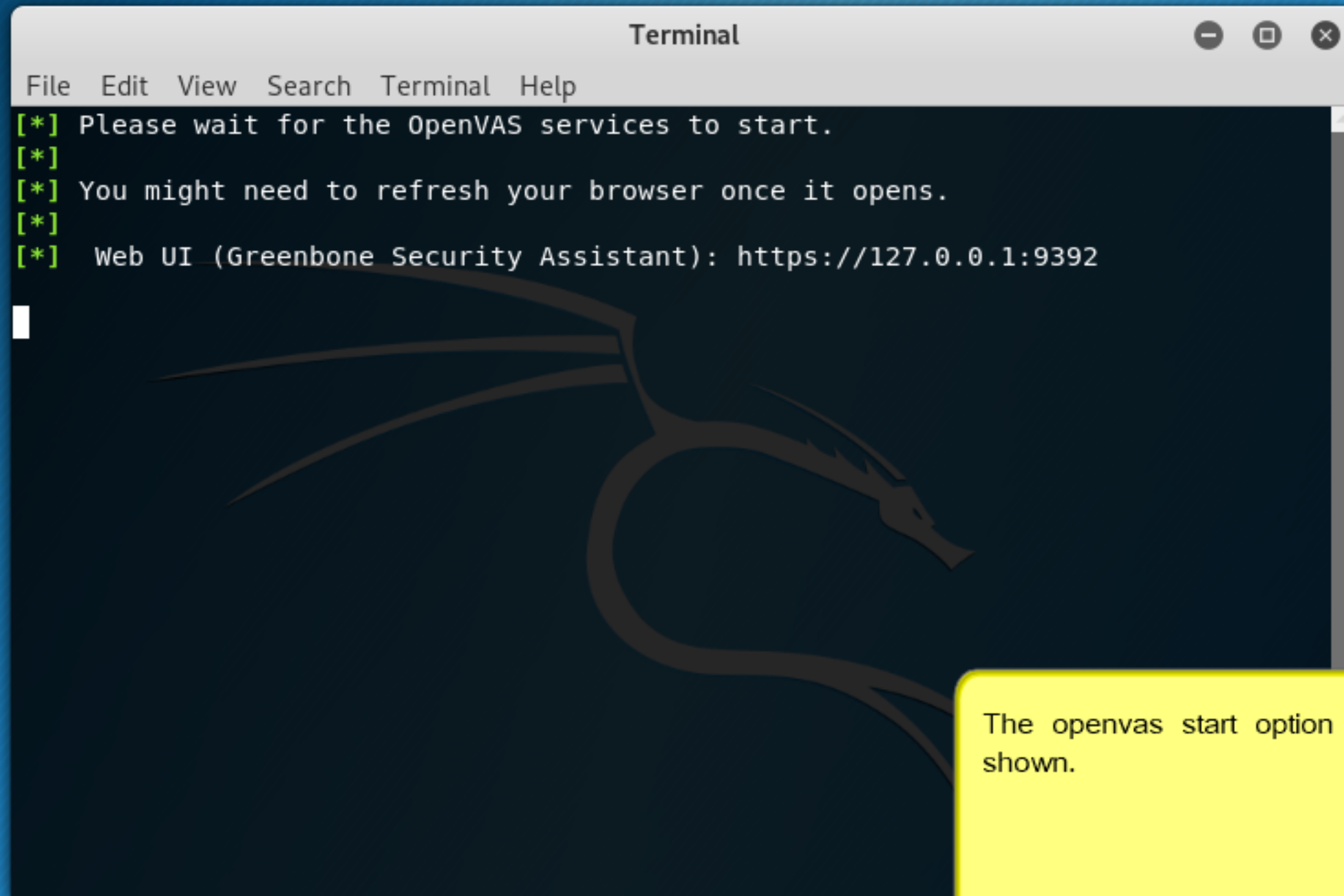
🔍 Type to search...

- 01-Information
- 02-Vulnerability**
- 03-WebApps
- 04-Database
- 05-Password
- 06-Wireless



← The presentation selects "openvas start".

- [Terminal]
- [Folder]
- [Mail]
- [User Avatar]
- [Lightning Bolt]
- [Globe]
- [Terminal]
- [Red Arrow]
- [List Icon]
- [App Grid]



The image shows a terminal window titled "Terminal" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output consists of five lines of asterisk-prefixed messages. The background of the terminal window features a large, faint watermark of a dragon's head. A white cursor is visible on the line following the URL.

```
File Edit View Search Terminal Help
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

The openvas start option opens a terminal window as shown.

Firefox ESR

```
Terminal
File Edit View Search Terminal Help
stem Scanner Daemon.

● openvas-manager.service - Open Vulnerability Assessment System Manager Daemon
  Loaded: loaded (/lib/systemd/system/openvas-manager.service; disabled; vendor
  preset: disabled)
  Active: active (running) since Fri 2019-03-29 15:51:51 CDT; 1min 2s ago
  Docs: man:openvasmd(8)
  http://www.openvas.org/
  Process: 1903 ExecStart=/usr/sbin/openvasmd --listen=127.0.0.1 --port=9390 --d
  atabase=/var/lib/openvas/mgr/tasks.db (code=exited, status=0/SUCCESS)
  Main PID: 1906 (openvasmd)
  Tasks: 1 (limit: 4656)
  Memory: 174.4M
  CGroup: /system.slice/openvas-manager.service
  └─1906 openvasmd

Mar 29 15:51:46 kali-s2019a systemd[1]: Starting Open Vulnerability Assessment S
ystem Manager Daemon...
Mar 29 15:51:46 kali-s2019a systemd[1]: openvas-manager.service: Can't open PID
file /run/openvasmd.pid (yet?) after start: No such file or directory
Mar 29 15:51:51 kali-s2019a systemd[1]: Started Open Vulnerability Assessment Sy
stem Manager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3...
```

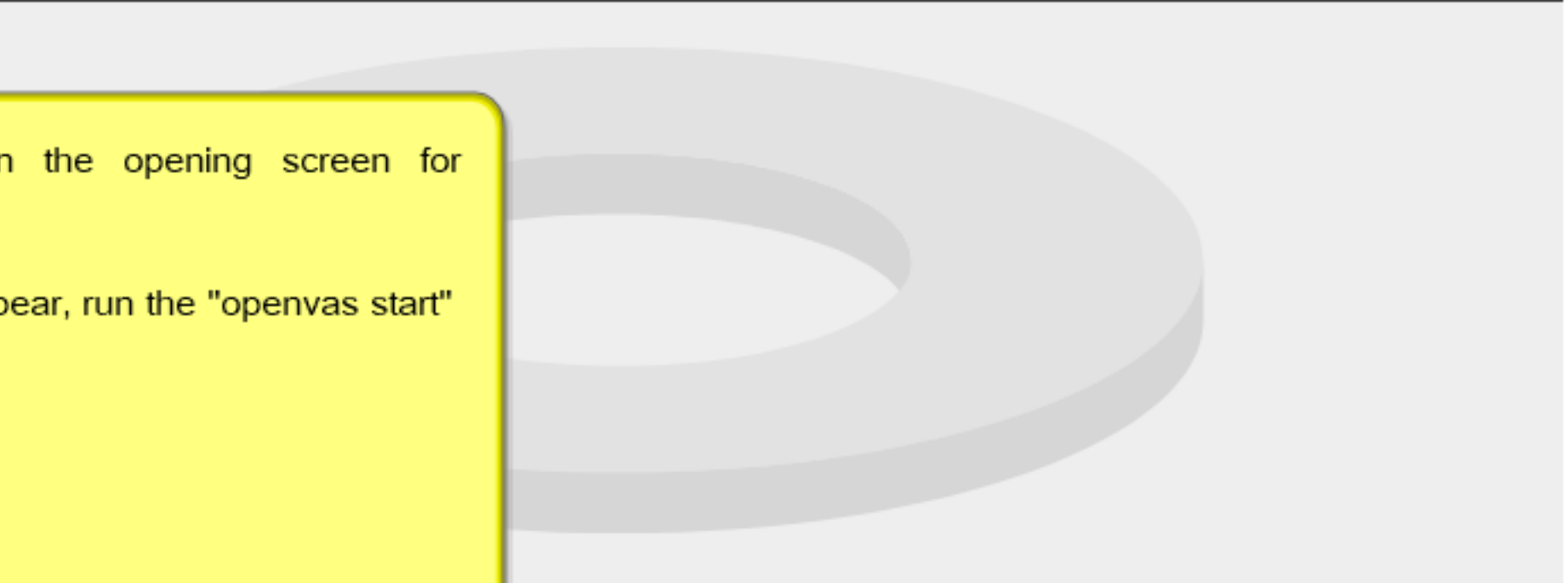
The presentation watches the openvas start screen finish.
The presentation only watches.

 **Dashboard**

Tasks by Severity Class (Total: 0)



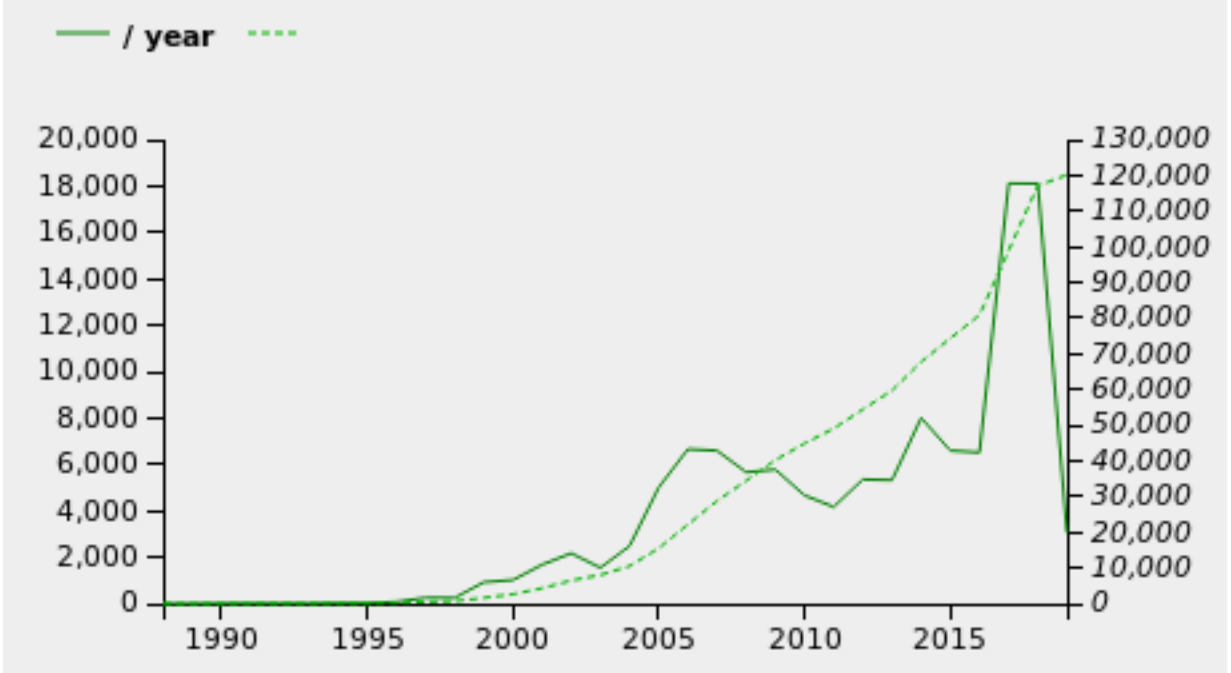
Tasks by status (Total: 0)



The presentation is now on the opening screen for OpenVAS.

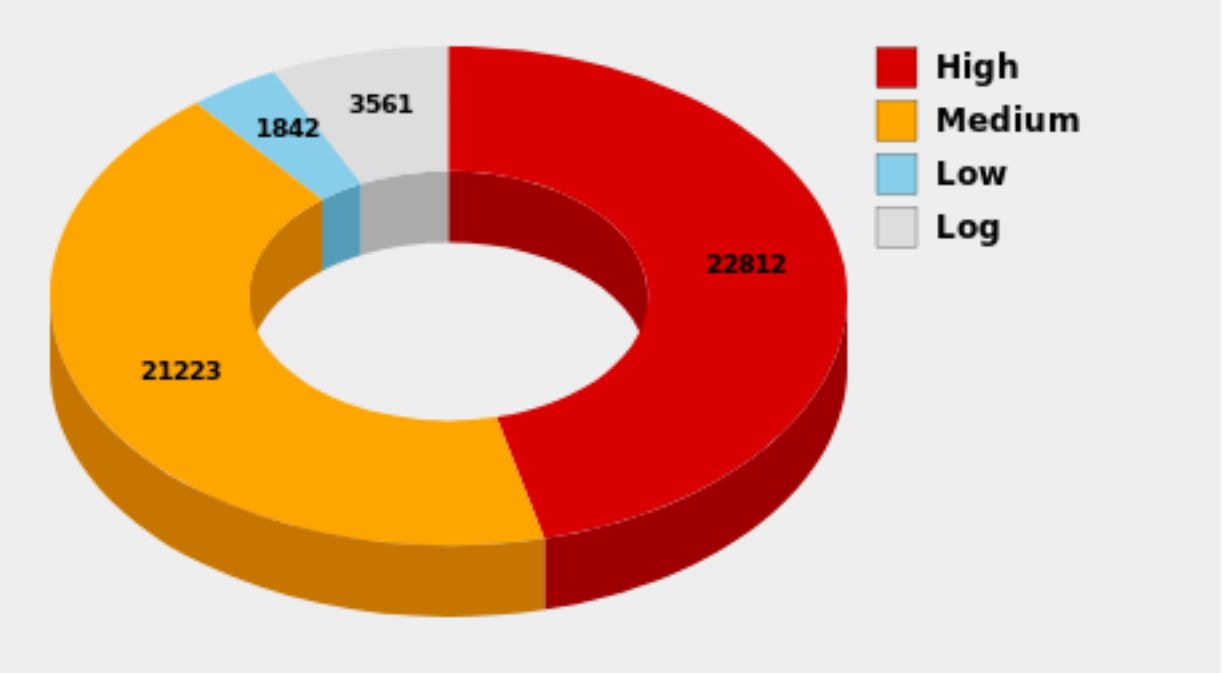
If a similar screen does not appear, run the "openvas start" option again.

CVEs by creation time (Total: 120128)



No hosts with topology selected

NVTs by Severity Class (Total: 49438)



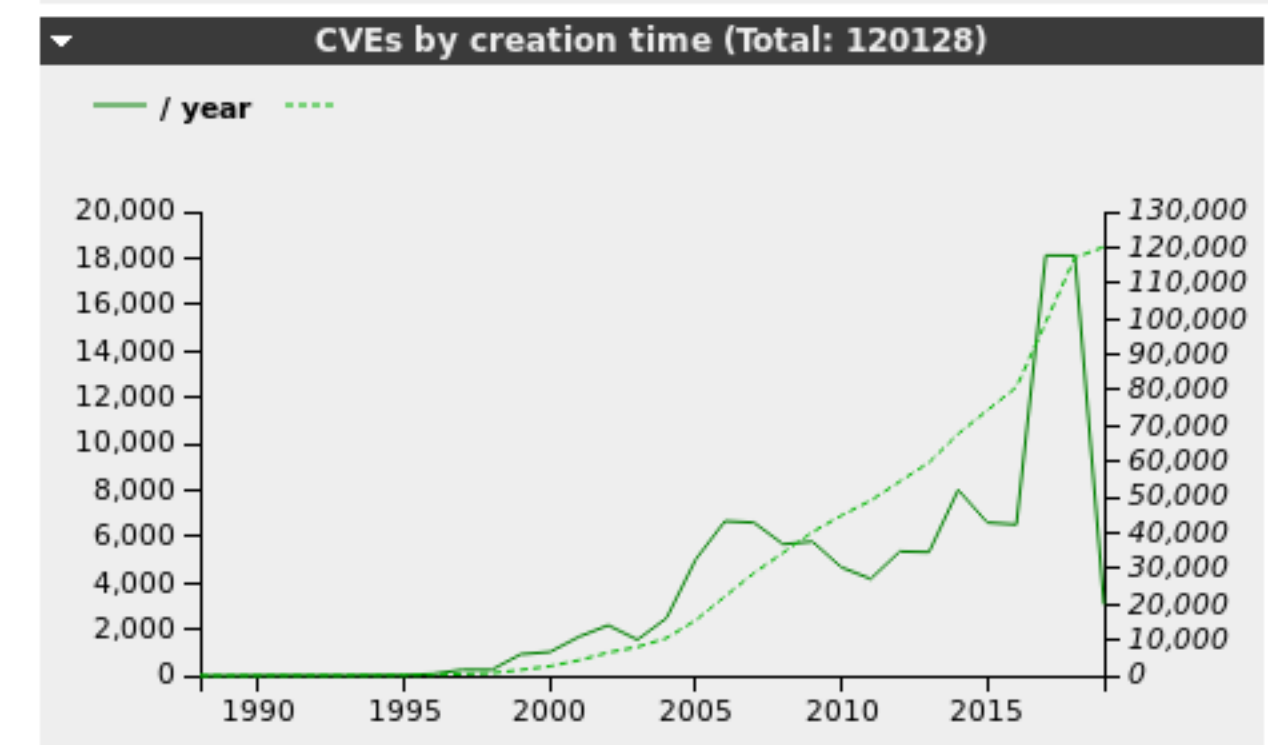
Dashboard

Tasks by Severity Class (Total: 0)

Tasks

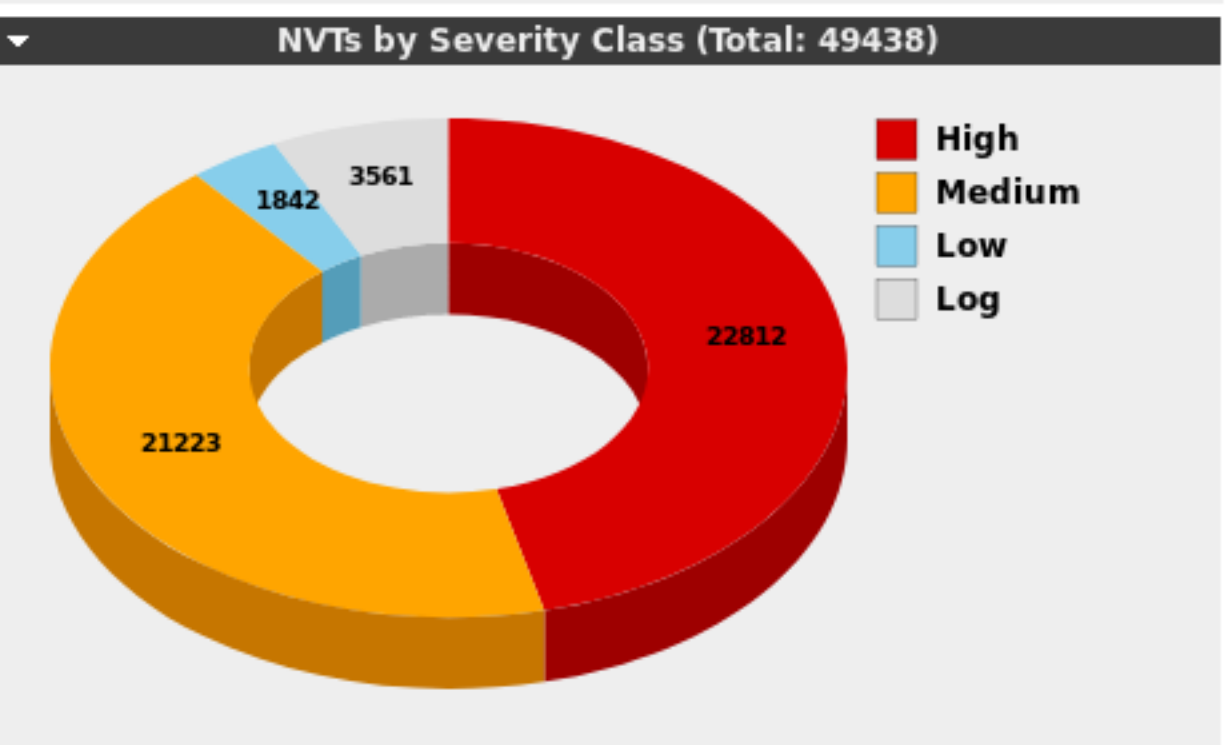
- Targets
- Port Lists
- Credentials
- Scan Configs
- Alerts
- Schedules
- Report Formats
- Agents
- Scanners
- Filters
- Tags
- Permissions

The presentation selects "Configuration | Targets" to begin.



Hosts topology

No hosts with topology selected



? * ← The presentation selects the white star in the blue to create the Target.

Target

Name	Actions
(Applied filter: rows	

Backend operation:

Filter: rows=10 first=1 sort=name

Credentials - sort by: SSH

vApply to page contents

Targets (0 of 0)

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

Backend operation: 0.01s

New Target [X]

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:

ESXi:

SNMP:

The presentation completes the information about the Target as show. The presentation shows changing the "Port List" option.

Targets (0 of 0)

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

Backend operation: 0.01s

New Target x

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 on port ★

SMB ★

ESXi ★

SNMP ★

The presentation shows the Target information before selecting "Create".

Targets (1 of 1)

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
victim01 (Spring 2019 demo)	192.168.74.131	1	All IANA assigned TCP and UDP 2012-02-10		

The presentation sees the Target is prepared.

Targets (1)

- Dashboard
- Tasks
- Reports
- Results
- Notes
- Overrides

The presentation navigates to "Scans | Tasks" as shown.

Name	Hosts	IPs	Pos
victim01 (Spring 2019 demo)	192.168.74.131	1	All

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

Credentials - sort by: SSH

Actions

Apply to page contents

Tasks (0 of 0)

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

Welcome to the scan task management!

If you would like to start your first vulnerability scan, the scan wizard can help you to do so with just one click.

Simply select the wizard icon from the icon bar in the top-left of this page.

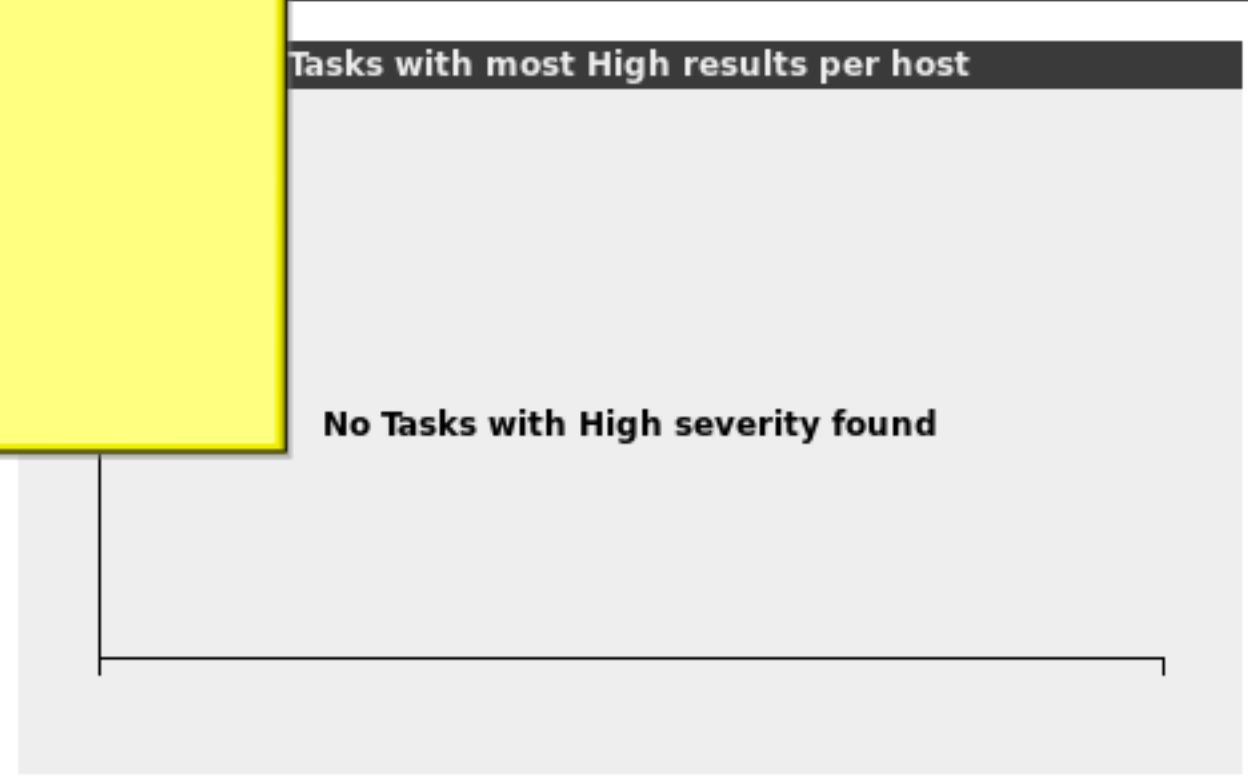
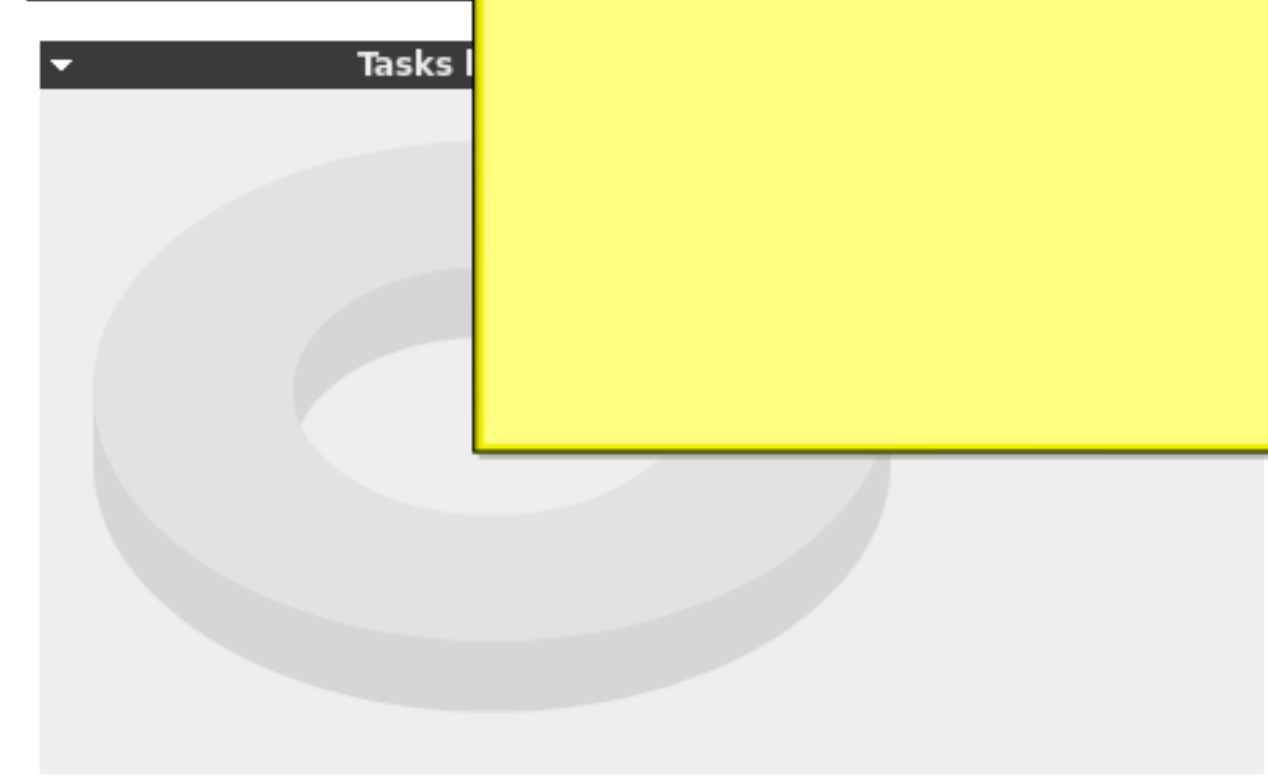
6

The presentations waits for this box to clear before continuing. This will not appear after the first Task is created and saved.

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

The presentation selects the white star in blue, then "New Task". This will begin the Task creation.

New Task New Task Tasks (0 o



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

Tasks (0 of 0)

Tasks by Severity Class (Total: 0)

Tasks by status (Total: 0)

Table with columns Name and Status

New Task

Name: Demonstration Task 01
Comment: Spring 2019 demo
Scan Targets: victim01
Alerts:
Schedule: --
Add results to Assets: yes
Apply Overrides: yes
Min QoD: 0 %
Alterable Task: no
Auto Delete Reports: Do not automatically delete reports
Scanner: OpenVAS Default

- Full and fast
Discovery
Full and fast
Full and fast ultimate
Full and very deep
Full and very deep ultimate
Host Discovery
System Discovery

The presentation configures the Task as shown. The presentation is currently changing the "Scan Config".

Tasks (1 of 1)

Edit Task

Name

Comment

Scan Targets

Alerts

Schedule Once

Add results to Asset Management 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

Scan Config

Network Source Interface

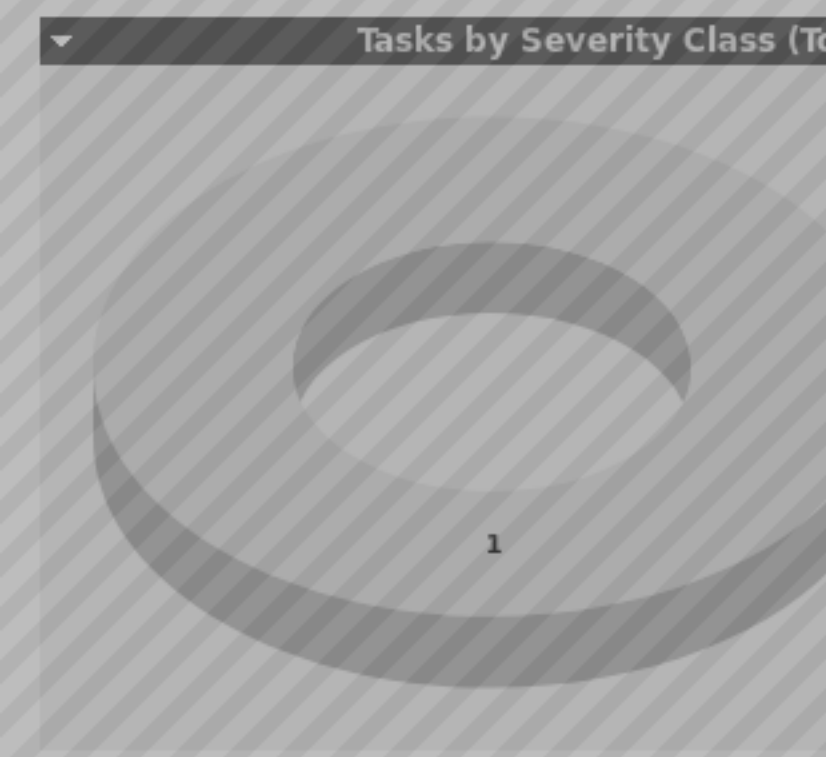
Order for target hosts

Maximum concurrently executed NVTs per host

Maximum concurrently scanned hosts

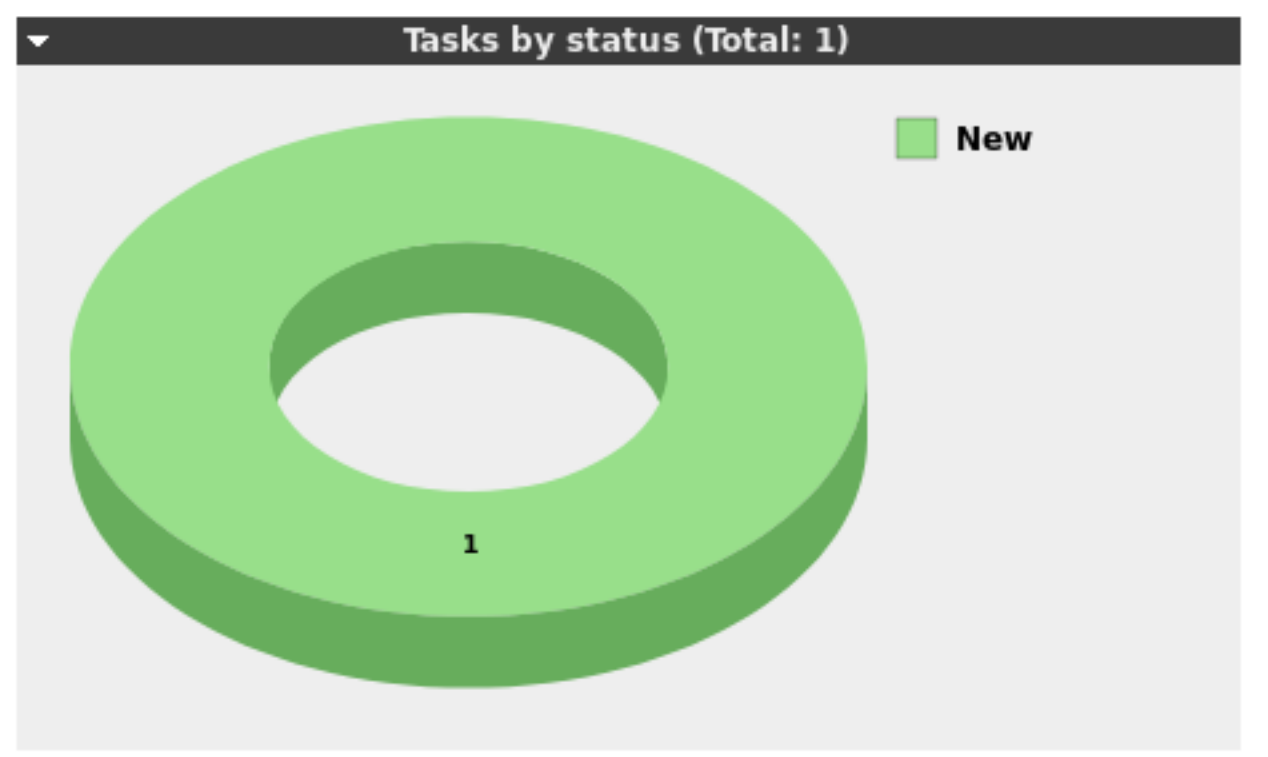
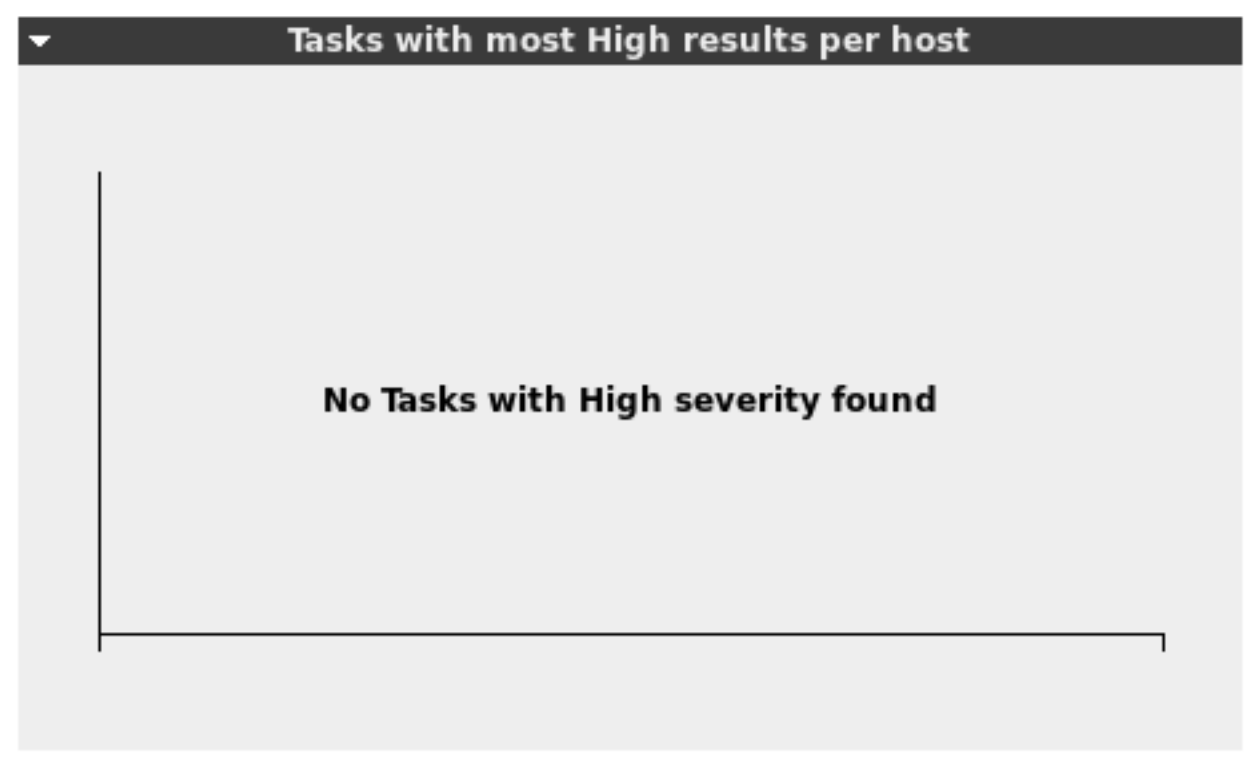
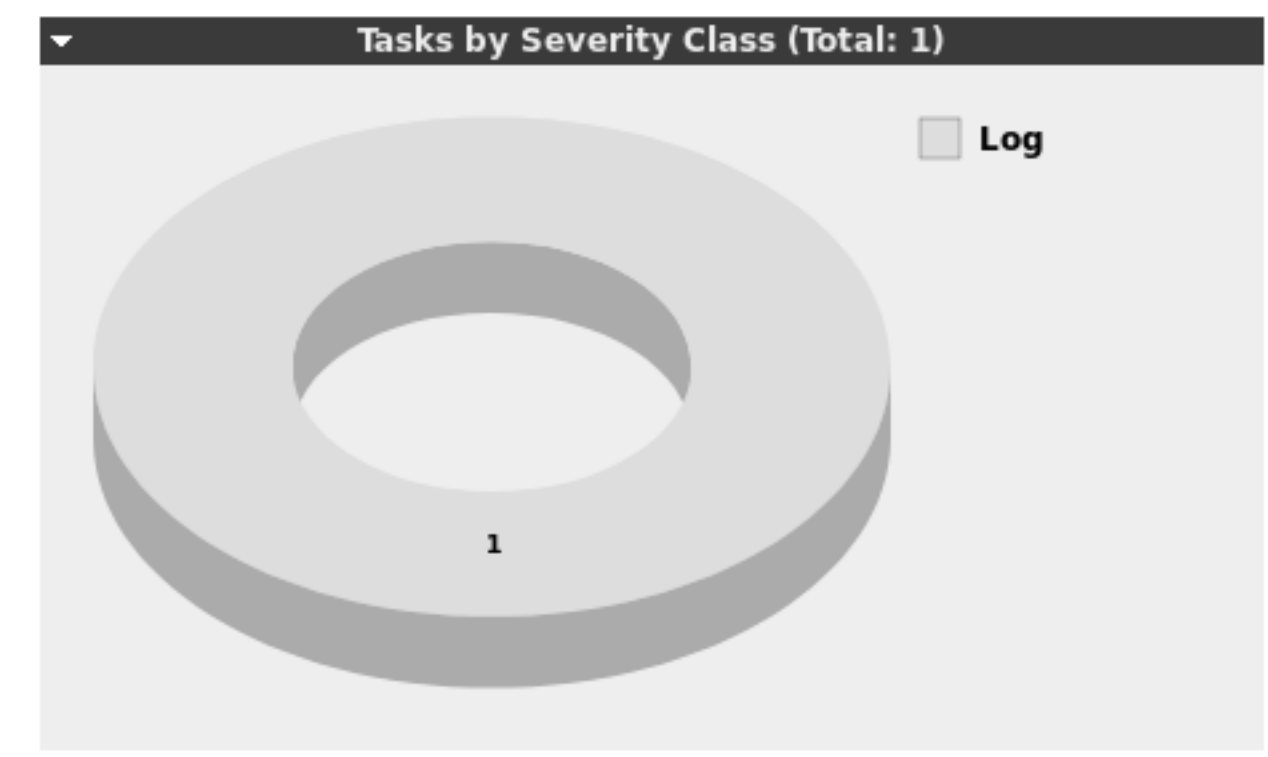
Save

The presentation shows the Task configuration before selecting "Save".



Name
Demonstration Task 01 (Spring 2019 demo)

Tasks (1 of 1)



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

Demonstration Task 01 (Spring 2019 demo)	New					
---	-----	--	--	--	--	--

The presentation sees the Task is ready.

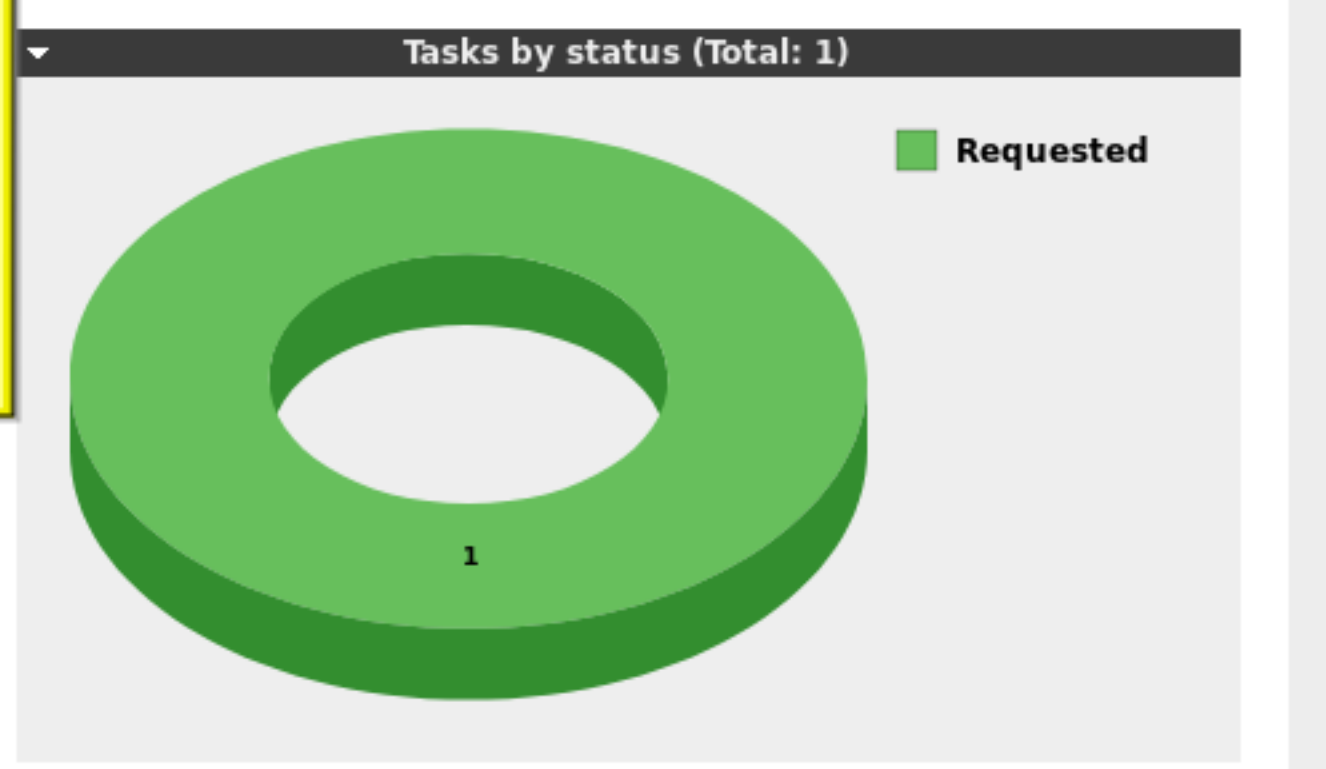
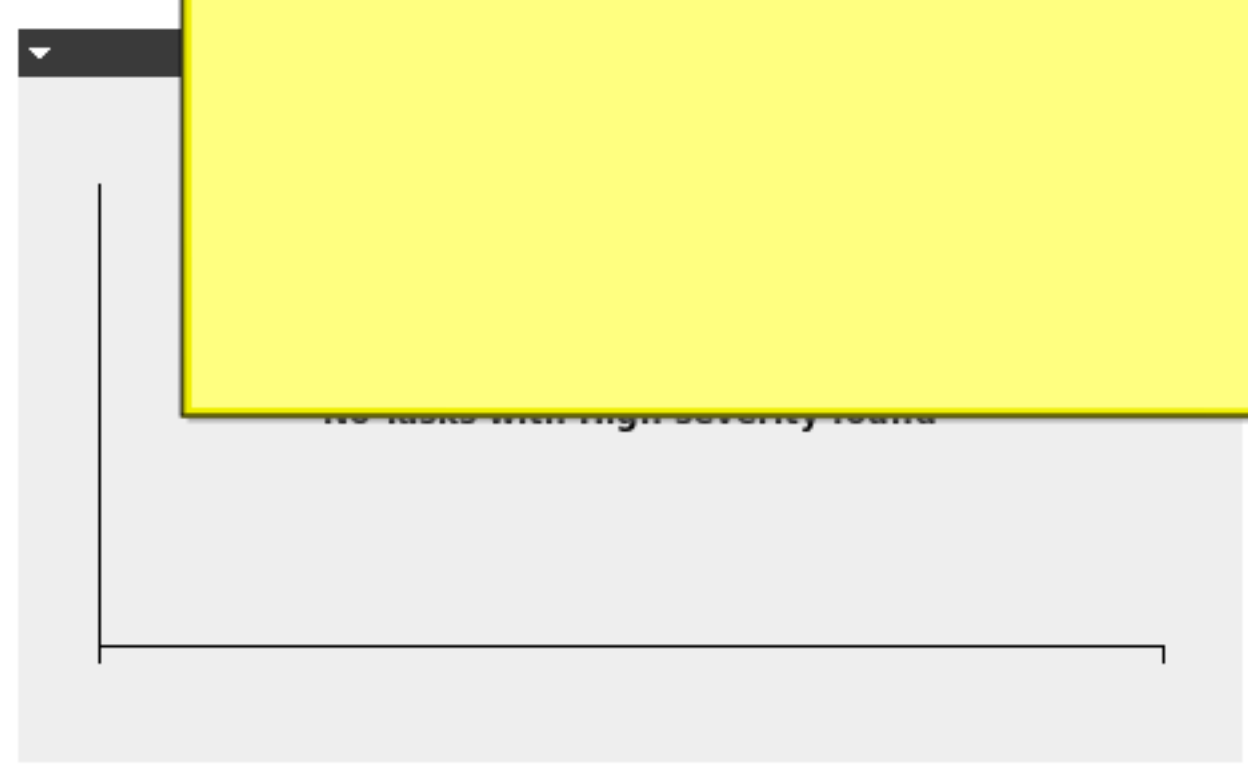
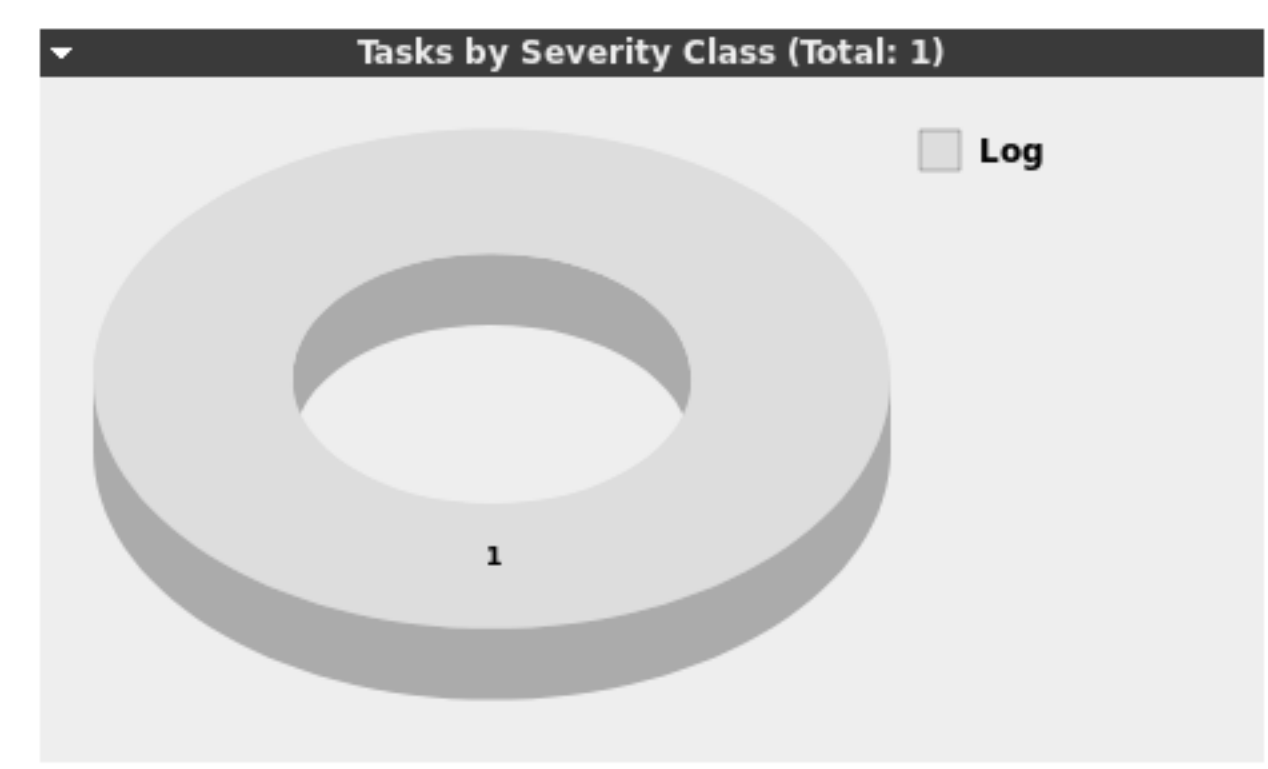
The presentation selects the white arrow to start the scan.

You do have permission to run this scan, correct?

Tasks (1 of 1)

The presentation changes the auto-refresh as shown.

- No auto-refresh
- Refresh every 30 Sec.
- Refresh every 60 Sec.
- Refresh every 2 Min.
- Refresh every 5 Min.

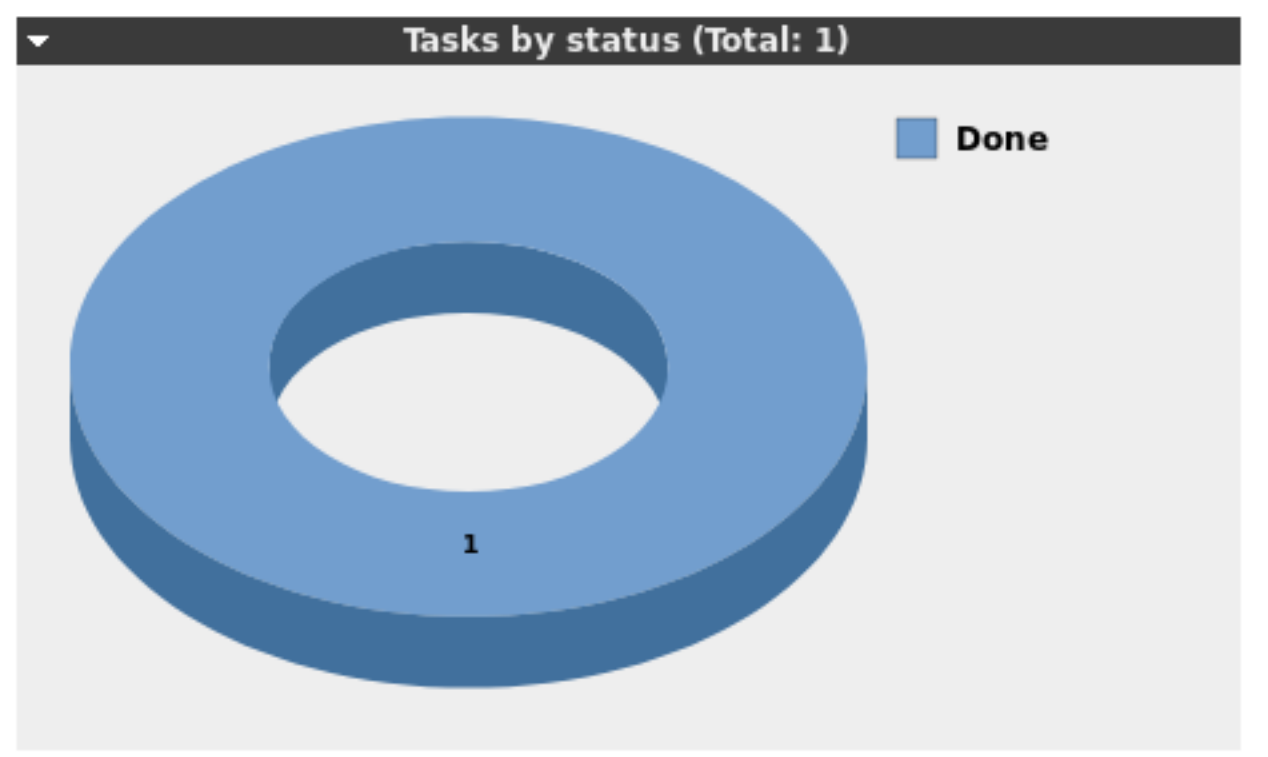
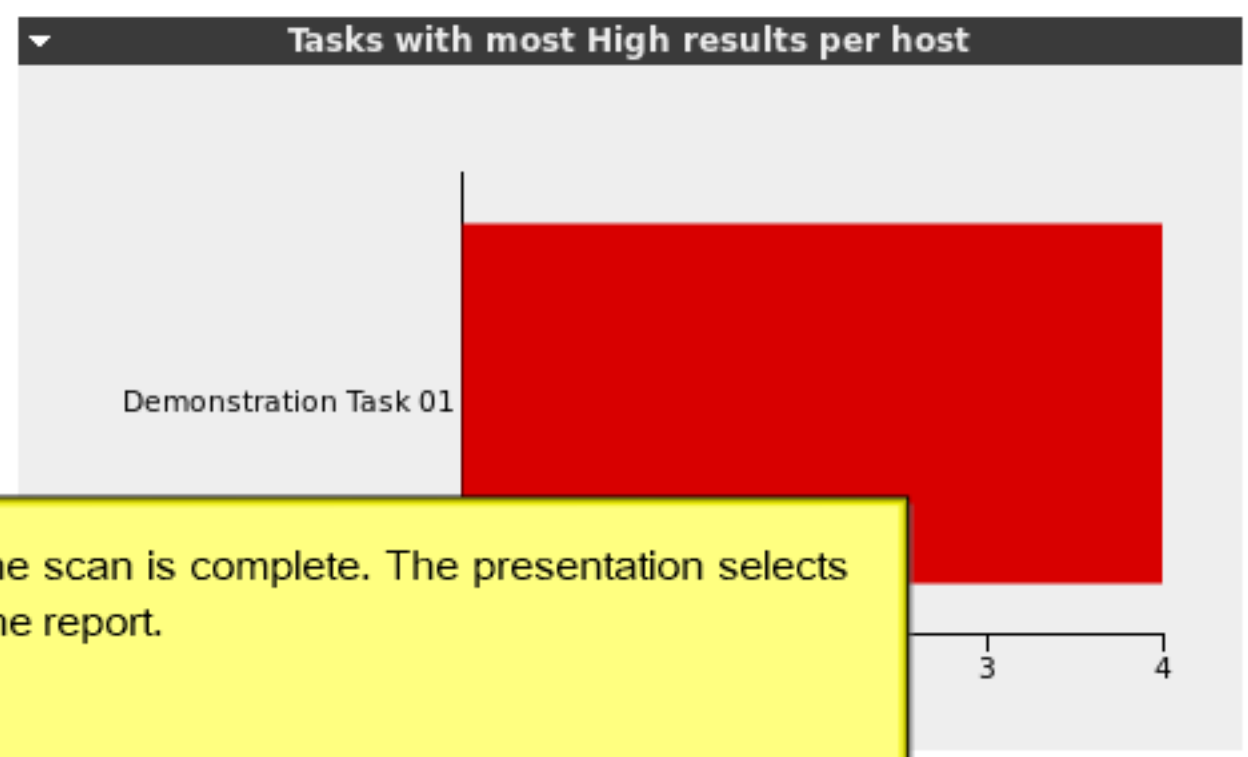
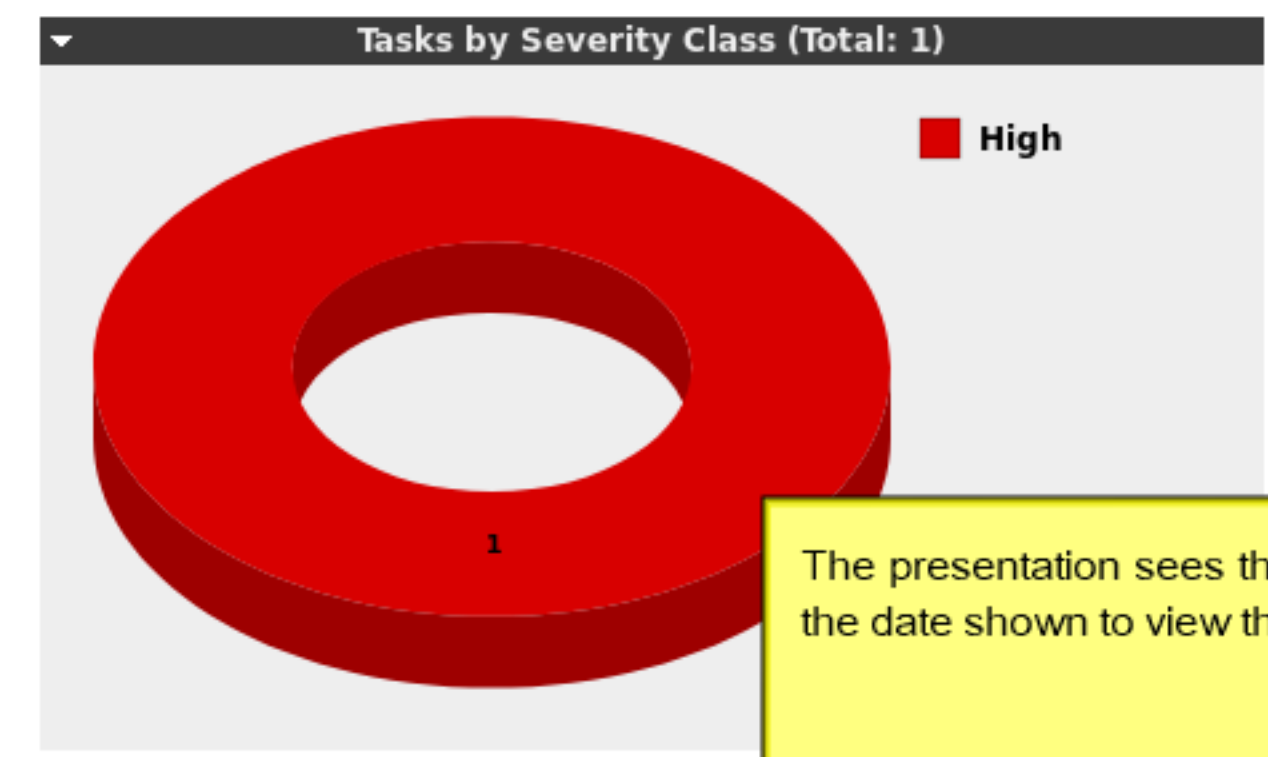


Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Demonstration Task 01 (Spring 2019 demo)	Requested	0 (1)				

Automatic suspend
Computer will suspend very soon because of inactivity.

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

Tasks (1 of 1)



The presentation sees the scan is complete. The presentation selects the date shown to view the report.

Name	Status	Total	Last	Severity	Trend	Actions
Demonstration Task 01 (Spring 2019 demo)	Done	1 (1)	Mar 28 2019	10.0 (High)		[Icons]

View last report for Task Demonstration Task 01

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

Automatic suspend
Computer will suspend very soon because of inactivity.

Anonymous XML Done

Filter: [input field] [refresh] [clear] [help] [share] [star] [dropdown]

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



Report: Results (5 of 19)

ID: fa5abdd6-9d41-482c-b90f-a5d2c4bd529c
Modified: Thu Mar 28 18:35:55 2019
Created: Thu Mar 28 18:26:10 2019
Owner: admin

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
OS End Of Life Detection	10.0 (High)	80%	192.168.74.131	general/tcp	[refresh] [star]
Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)	98%	192.168.74.131	445/tcp	[refresh] [star]
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	192.168.74.131	445/tcp	[refresh] [star]
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.74.131	445/tcp	[refresh] [star]
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.74.131	135/tcp	[refresh] [star]

(Applied 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)

1 - 5 of 5

Backend operation: 0.26s

The presentation sees a partial list of results.

Report: Results (5 of 19) ID: fa5abdd6-9d41-482c-b90f-a5d2c4bd529c Modified: Thu Mar 28 18:35:55 2019 Created: Thu Mar 28 18:26:10 2019 Owner: admin

- Report: Summary and Download
- Report: Results (19)
- Report: Vulnerabilities (18)
- Report: Hosts (1)
- Report: Ports (3)
- Report: Applications (0)
- Report: Operating Systems (1)
- Report: CVEs
- Report: Closed CVEs (2)
- Report: SSL Certificates (0)
- Report: Error Messages (0)

The presentation selects the down arrow found to the left of the word Report.

The presentation selects "Report: Summary and Download".

Severity	QoD	Host	Location	Actions
10.0 (High)	80%	192.168.74.131	general/tcp	
10.0 (High)	98%	192.168.74.131	445/tcp	
10.0 (High)	98%	192.168.74.131	445/tcp	
9.3 (High)	95%	192.168.74.131	445/tcp	
5.0 (Medium)	80%	192.168.74.131	135/tcp	

Anonymous XML Done 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

Report: Summary and Download ID: fa5abdd6-9d41-482c-b90f-a5d2c4bd529c Modified: Thu Mar 28 18:35:55 2019 Created: Thu Mar 28 18:26:10 2019 Owner: admin

Result of Task: Demonstration Task 01
Scan initiated: Thu Mar 28 18:26:01 2019 UTC
Scan started: Thu Mar 28 18:26:10 2019 UTC
Scan ended: Thu Mar 28 18:35:55 2019 UTC
Scan duration: 9 minutes 45 seconds
Scan status: Done

Table with columns: High, Medium, Low, Log, False Pos., Total, Run Alert, Download. Rows: Full report, Filtered report.

User Tags (none)

The presentation sees the "Report:Summary and Download" page.

Report: Summary and Download ID: fa5abdd6-9d41-482c-b90f-a5d2c4bd529c Modified: Thu Mar 28 18:35:55 2019 Created: Thu Mar 28 18:26:10 2019 Owner: admin

Result of Task: Demonstration Task 01
Scan initiated: Thu Mar 28 18:26:01 2019 UTC
Scan started: Thu Mar 28 18:26:10 2019 UTC
Scan ended: Thu Mar 28 18:35:55 2019 UTC
Scan duration: 9 minutes 45 seconds
Scan status: Done

Table with columns: High, Medium, Low, Log, False Pos., Total, Run Alert, Download. Rows: Full report, Filtered report.

User Tags (none)

Backend operation: 0.18s

The presentation selects the "Download" box on the "Full report". As shown, the presentation changes the report to PDF.

- Anonymous ...
ITG
LaTeX
NBE
PDF
Topology SVG
TXT
Verinice ISM

Report: Summary and Download

Result of Task: [Demonstration Task 01](#)

Scan initiated: **Thu Mar 28 18:26:01 2019 UTC**

Scan started: Thu Mar 28 18:26:10 2019 UTC

Scan ended: Thu Mar 28 18:35:55 2019 UTC

Scan duration: 9 minutes 45 seconds

Scan status: **Done**

Network Source Interface:

	High	Medium
Full report:	4	1
Filtered report:	4	1

User Tags (none)

Backend operation: 0.18s

Opening report-fa5abdd6-9d41-482c-b90f-a5d2c4bd529c.pdf

You have chosen to open:

report-fa5abdd6-9d41-482c-b90f-a5d2c4bd529c.pdf
which is: PDF document (139 KB)
from: https://127.0.0.1:9392

What should Firefox do with this file?

Open with Document Viewer (default)

Save File

Do this automatically for files like this from now on.

Cancel OK

ID: fa5abdd6-9d41-482c-b90f-a5d2c4bd529c
 Modified: Thu Mar 28 18:35:55 2019
 Created: Thu Mar 28 18:26:10 2019
 Owner: admin

Alert Download

PDF

Anonymous ...

The presentation now has the option to download or view the report.

- Result Overv... 2
- ▼ Results per ... 2
- ▼ 192.168.7... 2
 - High g... 2
 - High 4... 3
 - Mediu... 6
 - Low ge... 7
 - Log 10... 8
 - Log ge... 9
 - Log 13... 9
 - Log ge... 10
 - Log 44... 11
 - Log ge... 13
 - Log ge... 13

This is the first page of the presentation task report.

Scan Report

March 29, 2019

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 "Demonstration Task 01". The scan started at Thu Mar 28 18:26:10 2019 UTC and ended at Thu Mar 28 18:35:55 2019 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	192.168.74.131	2
2.1.1	High general/tcp	2
2.1.2	High 445/tcp	3
2.1.3	Medium 135/tcp	6
2.1.4	Low general/tcp	7
2.1.5	Log 1025/tcp	8
2.1.6	Log general/CPE-T	9
2.1.7	Log 135/tcp	9
2.1.8	Log general/tcp	10
2.1.9	Log 445/tcp	11
2.1.10	Log general/SMBClient	13
2.1.11	Log general/icmp	13