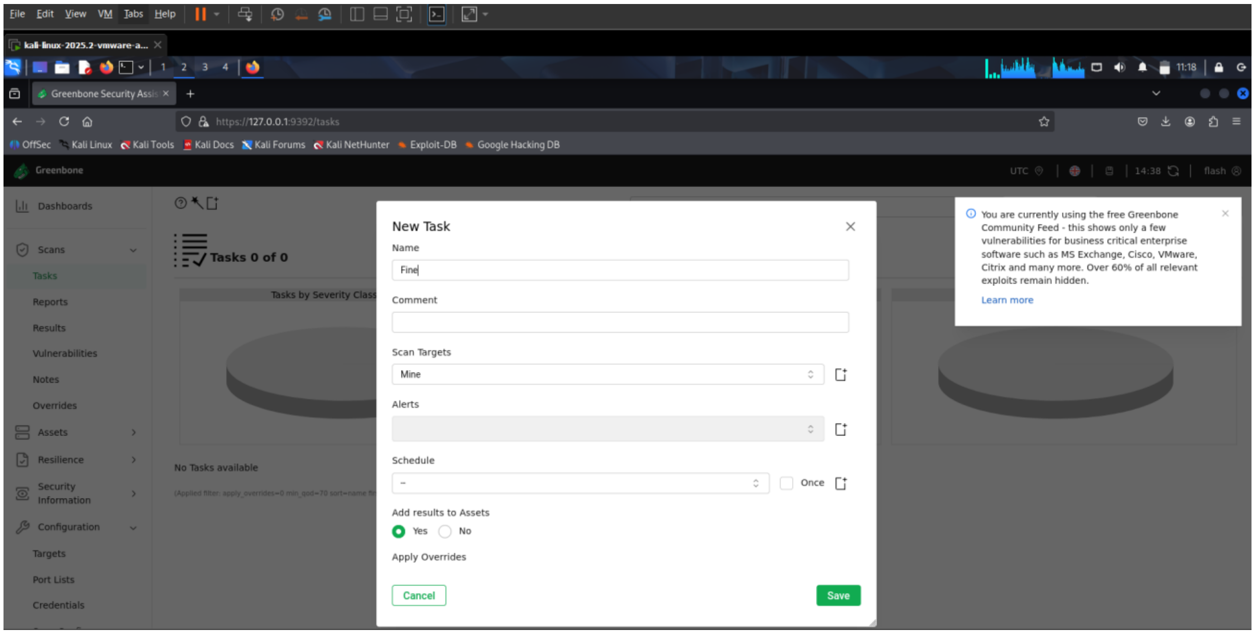


Tasks 0 of 0

No Tasks available

New Task

Name: Fine

Comment:

Scan Targets: Mine

Alerts:

Schedule: – □ Once

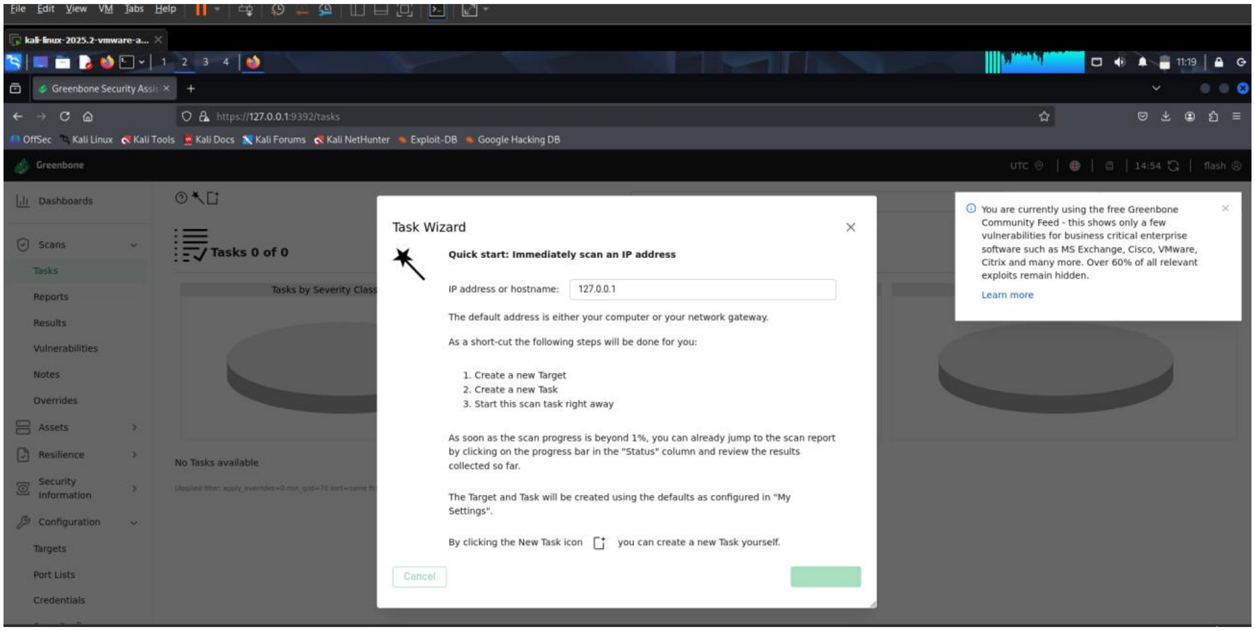
Add results to Assets: ● Yes ○ No

Apply Overrides

Cancel Save

You are currently using the free Greenbone Community Feed - this shows only a few vulnerabilities for business critical enterprise software such as MS Exchange, Cisco, VMware, Citrix and many more. Over 60% of all relevant exploits remain hidden.

Learn more



Tasks 0 of 0

No Tasks available

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1

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.

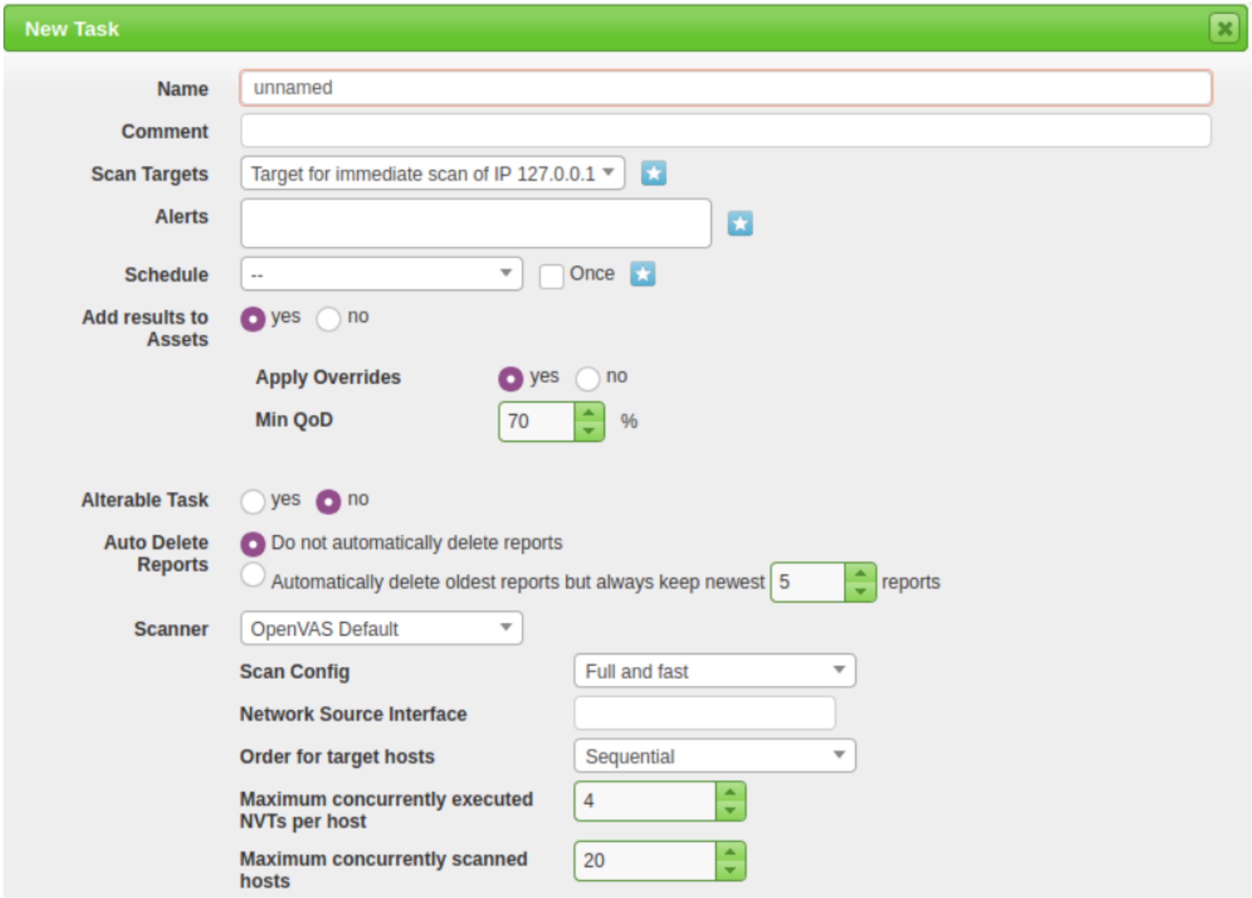
The Target and Task will be created using the defaults as configured in "My Settings".

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

Cancel

You are currently using the free Greenbone Community Feed - this shows only a few vulnerabilities for business critical enterprise software such as MS Exchange, Cisco, VMware, Citrix and many more. Over 60% of all relevant exploits remain hidden.

Learn more



New Task

Name: unnamed

Comment:

Scan Targets: Target for immediate scan of IP 127.0.0.1

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

Network Source Interface:

Order for target hosts: Sequential

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

This report contains all 5 results selected by the filtering described above. Before filtering there were 23 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	**Fri Oct 24 20:04:36 2021 UTC**
Scan ended:	Fri Oct 24 20:21:02 2021 UTC
Task:	Blue

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
10.10.148.71	Oct 24, 20:04:46	Oct 24, 20:21:02	1	3	1	0	0
Total: 1			1	3	1	0	0

Results per Host

Host 10.10.148.71

Scanning of this host started at:	Sun Feb 28 00:04:46 2021 UTC
Number of results:	5

Port Summary for Host 10.10.148.71

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/tcp	Low
445/tcp	High

Security Issues for Host 10.10.148.71

High (CVSS: 9.3) 445/tcp
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID:
1.3.6.1.4.1.25623.1.0.810676)

Summary

This document reports on the results of an automatic security scan. 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.

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

This report contains all 39 results selected by the filtering described above. Before filtering there were 326 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	**Fri Oct 24 20:25:54 2021 UTC**
Scan ended:	Fri Oct 24 20:51:56 2021 UTC
Task:	METASPLOITABLE

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
192.168.1.98	Oct 24, 20:25:54	Oct 24, 20:51:56	9	28	2	0	0
Total: 1			9	28	2	0	0

Host Authentications

Host	Protocol	Result	Port/User
192.168.1.98	SMB	Success	Protocol SMB, Port 445, User

Results per Host