

SecPoint[®] Penetrator Vulnerability Scanner V 44
Firmware Release

<https://www.SecPoint.com/penetrator.html>



Penetrator 44 – October 2018

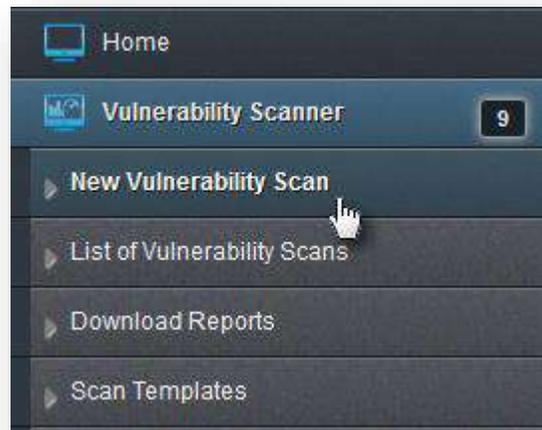
- New GUI for most functions

The migration to the new GUI, started with the previous firmware, has been extended to most functions of the Penetrator. With firmware 44, the new GUI is now available for these menus:

- Vulnerability Scanner
- Schedule
- Statistics
- Tickets
- Cloud Users
- Scan Distribution
- Network Setup

The remaining menus, including all the WiFi functions, will be migrated in the next firmware.

Along with the new GUI, a reorganization of some menus, pages and functions has been carried out. Let's focus on some sample functions:

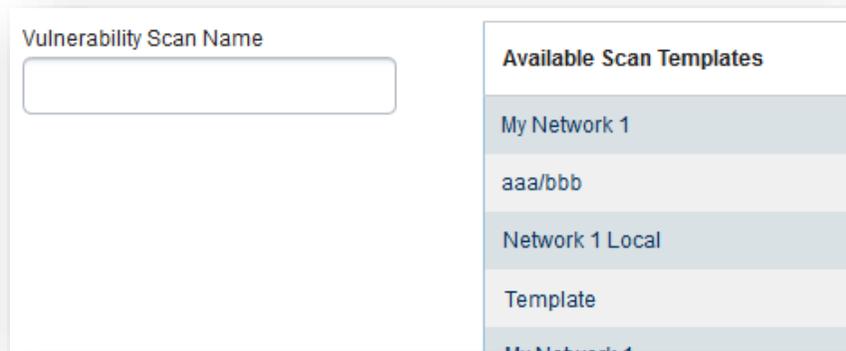


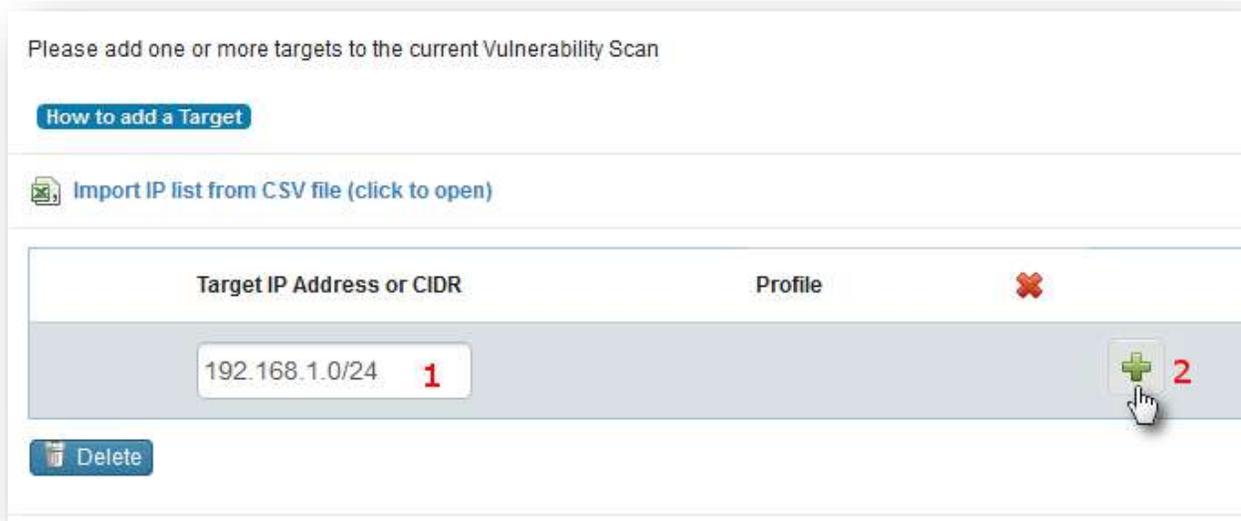
Creating a new scan

Click on the New Vulnerability Scan menu. The next page lets you choose between entering a new scan name or selecting an existing Scan Template.

After choosing either options, on the next page you can add targets to the scan. To do this, enter a target

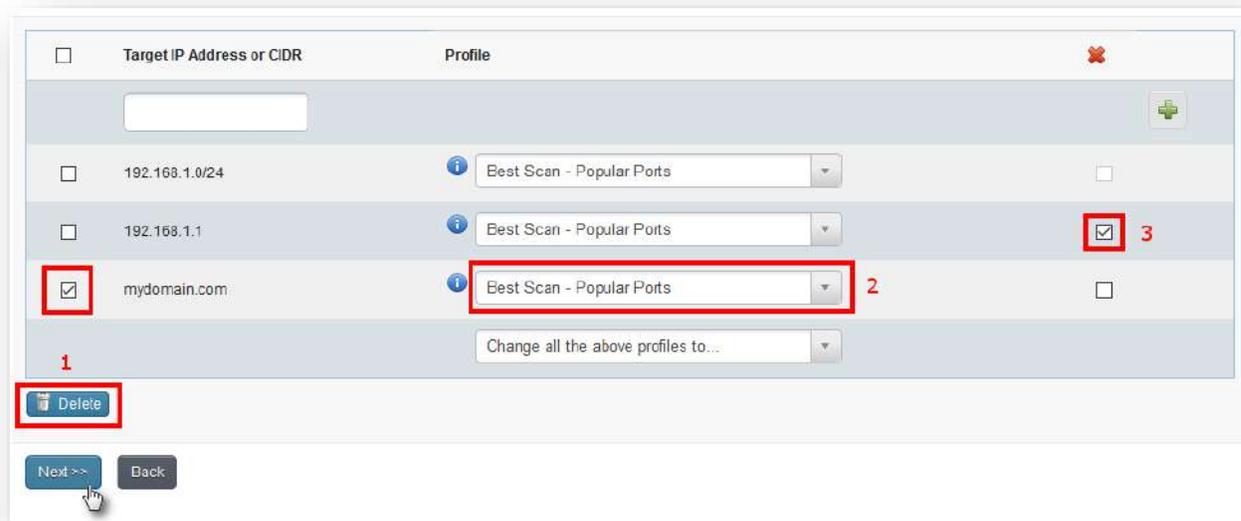
IP/CIDR or hostname in the entry field (1) and click  (2).

A screenshot of the 'New Vulnerability Scan' form. It features a text input field labeled 'Vulnerability Scan Name'. To the right, there is a section titled 'Available Scan Templates' with a list of options: 'My Network 1', 'aaa/bbb', 'Network 1 Local', and 'Template'. The 'My Network 1' option is currently selected.



Online instructions are available clicking on the button [How to add a Target](#). It's also possible to click on to import a CSV list from an external file.

When the targets have been added, it is possible to delete one or more items from the list (1), change the scan profile for one or more targets (2), exclude a target from a previously added CIDR (3).



In the next page, you can see a summary of the scan that is about to be launched and it is possible to click on [Advanced Setup](#) and enter the Advanced Settings page for more detailed settings.

IP or CIDR	Reverse DNS	Host Name	Advanced
192.168.1.0/24			Advanced Setup
192.168.1.1	192.168.1.1		
<i>(excluded)</i>			
65.254.242.180	mydomain.com	mydomain.com	Advanced Setup
Scanning vhosts:	mydomain.com		

⚠ WARNING: By clicking "Start Vulnerability Scan", you accept that the SecPoint® Penetrator will try to penetrate the selected Target. Shunning and screening functions must be disabled. All this has also been described in the agreement. If you do not agree to this, do not click on "Start Vulnerability Scan". Make sure your Penetrator's IP address is whitelisted in IPS and Shunning devices.

Back
Start Vulnerability Scan
Cancel

To complete the process, press Start Vulnerability Scan.

Creating/Modifying a scheduled scan

Scheduled scans can be created/changed in the Schedule menu, which doesn't have submenus.

The page that opens shows the list of existing schedules and allows editing schedule parameters by clicking on the Schedule Name, or creating a new schedule, clicking on the button



List of Schedules

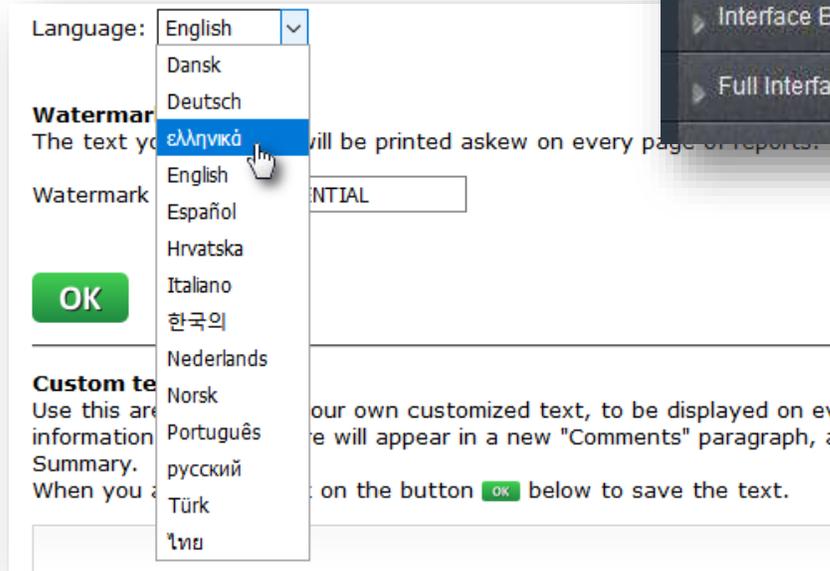
Show entries Search:

<input type="checkbox"/>	Schedule Name	Time	Day of Month	Month	Day of Week	Start Date	Repeated	Pause	Options
<input type="checkbox"/>	My Network	10:08:00	(every)	(every)	Sunday			<input type="checkbox"/>	Start Now
<input type="checkbox"/>	Computer	02:00:00	(every)	(every)	Saturday			<input checked="" type="checkbox"/>	Start Now
<input type="checkbox"/>	Customer	02:00:00	(every)	(every)	Monday			<input checked="" type="checkbox"/>	Start Now
<input type="checkbox"/>	Firewall	10:21:00	(every)	(every)	Sunday			<input type="checkbox"/>	Start Now

Showing 1 to 10 of 15 entries First Previous 1 2 Next Last

- **Greek and Russian Report Languages**

The Greek and the Russian languages are available for the report. The language can be set in the System – Report Branding menu.

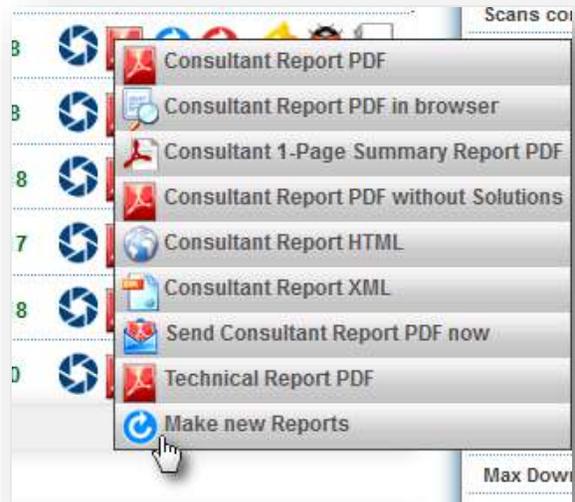


In this page, you can select the language of your choice through the pull-down list, where each choice is displayed in the language and in the alphabet of the language itself.

⚠ When you set a new language, all the reports available on the home page must be created again to be translated into the new language.

It's important to take into account that the reports available on the home page, to be displayed in the new language, must be created again.

To do so, go to the home page and click on the Make New Reports button in the floating menu next to each scan. The reports available in the pages inside a scan, are generated on the fly and do not need to be created in advance.



- **And...**

- In a Master-Client environment, the dialogue between the two units is available through the Http protocol.
- The mail that is sent to warn about a false positive scan contains information about the first 100 vulnerabilities.