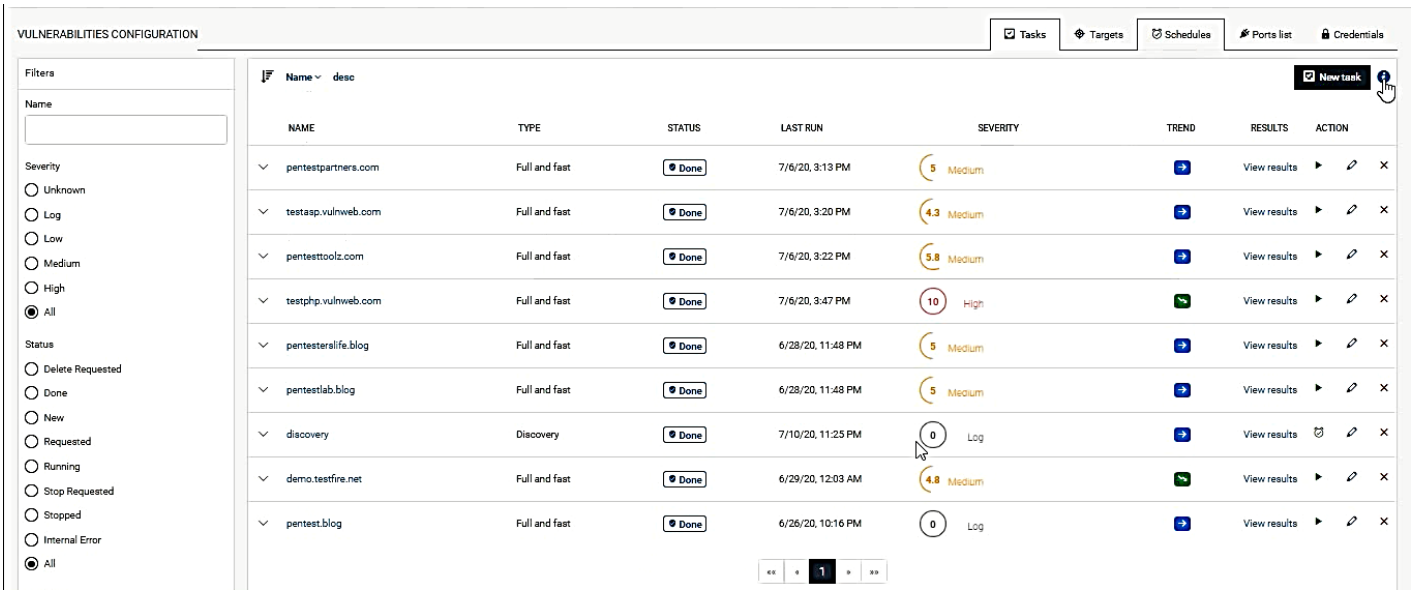
Scan results

Scan results

1. **Scan results.**

In this section, you can configure and manage the scans.

Clicking on scan results displays the vulnerabilities configuration view.



This view shows a table listing the scans. The list can be sorted in ascending or descending order and displays the following columns:

- **Name**: Definition of the name
- **Type**: UTMStack comes with eight preconfigured scan configurations.
- **Status**: Status of the corresponding task.
- **Last run**: Last time run
- **Severity**: Highest severity found by the scan
- **Trend:** The trend describes the change of vulnerabilities between the newest and the second newest report.
- **Result:** Number of results found for this vulnerability. By clicking on the number of results the page Results is opened.
- **Action:** You can perform three tasks: Run, Edit, or Delete.

3.1 The following scan configurations are already available:

- **Empty:** This is an empty template.
- **Discovery**: Only NVTs that provide information of the target system are used. No vulnerabilities are being detected.
- **Host Discovery**: Only NVTs that discover target systems are used. This scan only reports the list of systems discovered.
- **System Discovery**: Only NVTs that discover target systems including installed operating systems and hardware in use are used.
- **Full and fast**: For many environments this is the best option to start with. This scan configuration is based on the information gathered in the previous port scan and uses almost all NVTs. Only NVTs that will not damage the target system are used. NVTs are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value in rare cases but with much higher effort.
- **Full and fast ultimate**: This scan configuration expands the scan configuration Full and fast with NVTs that could disrupt services or systems or even cause shutdowns.
- **Full and very deep**: This scan configuration is based on the scan configuration Full and fast but the results of the port scan or the application/service detection do not have an impact on the selection of the NVTs. Therefore, NVTs that wait for a timeout or test for vulnerabilities of an application/service, which were not detected previously, are used. A scan with this scan configuration is very slow.

3.2 Trends

The following trends are possible:

- In the newest report the highest severity is higher than the highest severity in the second newest report.
- The highest severity is the same for both reports. However, the newest report contains more security issues of this severity than the second newest report.
- The highest severity and the amount of security issues are the same for both reports.
- The highest severity is the same for both reports. However, the newest report contains less security issues of this severity than the second newest report.
- In the newest report the highest severity is lower than the highest severity in the second newest report.

3.3 View Results

This page shows the results for a task. It displays three graphs and a table.

Graphs

- **A pie chart** showing the vulnerabilities by severity class: high, log, low, and medium. Click on any pie slide to display an Asset Discovery dashboard providing exhaustive info: hostname and IP, host OS. Location, date, QOD, and Vulnerabilities word cloud. You can filter by time.
- **Vulnerabilities Word Cloud:** This visualization is generated by calculating the frequency of words that were part of the vulnerability summary description. Hovering over a word shows a tooltip that contains the word and the total number of times the term was found in the vulnerability summary descriptions. Mouse over to see a preview.
- **A bar chart** showing the results by **CVSS**. To support the interpretation of a vulnerability, the Common Vulnerability Scoring System (CVSS) was invented. The CVSS is an industry standard for describing the severity of security risks in computer systems.

Table

For every result, the following information is displayed:

VULNERABILITY	Name of the found vulnerability. By clicking on the Name, details of the vulnerability are shown
SEVERITY	The severity of the vulnerability
QOD	Quality of Detection and shows the reliability of the detection of a vulnerability.

LOCATION	Port number and protocol type used to find the vulnerability on the host. By clicking on the Name, details of the vulnerability are shown
DATE	Date and time of the report creation

ASSET	Asset for which the result was found. The IP address is displayed. Click on **Asset** to view the asset detail

3.4 Filters

The user can employ the filters to display only the most significant results.

UTMStack provides the following filter parameters:

- **Name:** Name of the task
- **Severity:** Highest severity found by a scan of the task
- **Status:** Current status of the task
- **Created at:** A time filtering

3.5 Status

Delete requested: The task was deleted. The actual deletion process can take some time, as reports need to be deleted as well.

Done: The task has been completed successfully

New: The task has not been run since it was created.

Requested: The task was just started.

Running: The task is currently running

Stop requested: The task was requested to stop recently. However, the scan engine has not yet reacted to this request.

Stopped: The task was stopped. The latest report is possibly not yet complete. After restarting the scanner, the task will be resumed automatically.

Internal error: An error has occurred, and the task was interrupted. The latest report is possibly not complete yet or is missing entirely.

All: All tasks

3.6 Targets

This view shows a table with the list of targets. The next columns are displayed:

Name	A descriptive name should be chosen if possible.

Hosts	Manual entry of the hosts that should be scanned, separated by commas,
Port list	Port list used if the target is used for a scan
Action	Three available options: **task using the target, edit schedule,** and **target in use**

Schedules

3.7 Schedules.

Select a previously configured schedule from the tabular list. The following details are displayed:

- **Name** Definition of the Name. The Name can be chosen freely.
- **Comment:** An optional comment can contain additional information.
- **First Run**: Definition of the date and time for the first scan to start.
- **Next Run:** Definition of the date and time for the next scan to start
- **Period**: a period after which the task should run again: hour, day, week, or month.
- **Duration**: Definition of the maximum duration a task can take for its execution: hour, day, week, or month. The duration depends on the given start and ends time. If an end time is defined and the assigned time is expired, the task is aborted and will be suspended until the next scheduled time slot becomes available. This way, it can be ensured that the scan will always run with a specific (maintenance) time window.

Action: You can execute the following actions:

- **Task(s) using this schedule:** The Name of the tasks using the schedule.
- **Edit schedule:** You can edit the Name, comments, start date, period, and duration.
- **Delete the schedule:** Not possible if the schedule is in use.

You can filter the results by **Name, first run, next run, period,** and **duration**.

Click on the **New schedule** tab to configure a new schedule.

Port List

3.8 Ports list.

Managing Port Lists. All existing port lists can be displayed by clicking on the **Port List tab.**

For all port lists the following information is displayed:

Name Name of the port list. A global port list is marked with**.**

Comment: Associated comments

Last modification: Date and time of the last modification

Total: Total number of ports in the port list.

TCP: Number of TCP ports in the port list**.**

UDP: Number of UDP ports in the port list**.**

You can filter the results by Name, time, and Port Ranges: Manual entry of the TCP, UDP ports ranges. If entering manually, the port ranges are separated by commas.

For all port lists, the following actions are available**:**

- **Delete the port list.** Only port lists, which are currently not used, can be deleted**.**
- **Edit the port list.** Only port lists, which are currently not used, can be edited

3.8.1 A new port list can be created as follows:

1. Click on **New Port List** to display a popup window
2. The following details of the port list can be defined**:**

Name Definition of the Name. The Name can be chosen freely.

Comment: An optional comment can contain additional information.

TCP: Number of TCP ports in the port list**.**

UDP: Number of UDP ports in the port list

3. Click **Save.**

Credentials

3.9 Credentials.

Credentials for local security checks are required to allow NVTs to log into target systems, e.g., for locally checking the presence of all vendor security patches.

An authenticated scan can provide more vulnerability details on the scanned system. The scan requires the prior setup of user credentials. These credentials are used to authenticate to different services on the target system. In some circumstances, the results could be limited by the permissions of the users used.

All existing credentials can be displayed by clicking on the **Credentials** tab.

For all credentials, the following information is displayed:

Name: Name of the credential

Comment: Related comment.

Type: Chosen credential type.

Allow insecure use: Indication whether the GSM can use the credential for unencrypted or otherwise insecure authentication methods.

Login: The user name for the credential if a credential type that requires a user name is chosen.

For all credentials, the following actions are available:

- Delete the credential. Only credentials, which are currently not used, can be deleted.
- Edit the credential.
- Target using the credential

Click on the Name of a credential to display the details of the credential.

Creating a Credential

A new credential can be created as follows:

Click on **New credential** and configure the next parameters:

Name: Definition of the Name. The Name can be chosen freely.

Comment: An optional comment can contain additional information

Allow insecure use: Select whether UTMStack can use the credential for unencrypted or otherwise insecure authentication methods.

Username: Definition of the login name used to authenticate on the scanned target system.

Password: Definition of the password used to authenticate on the scanned target system.