

Vulnérabilités – GreenBone



Greenbone
Sustainable Resilience

Sommaire :

1 ./Recherches de vulnérabilités

- Scans > Tasks
- Scans > Reports
- Scans > Results
- Scans > Vulnerabilities

2 ./Gestion des actifs

- Assets > Hosts
- Assets > Operating Systems
- Assets > TLS Certificates

3 ./Résilience

- Resilience > Compliance Policies

4 ./SecInfo

5 ./Gestion des cibles

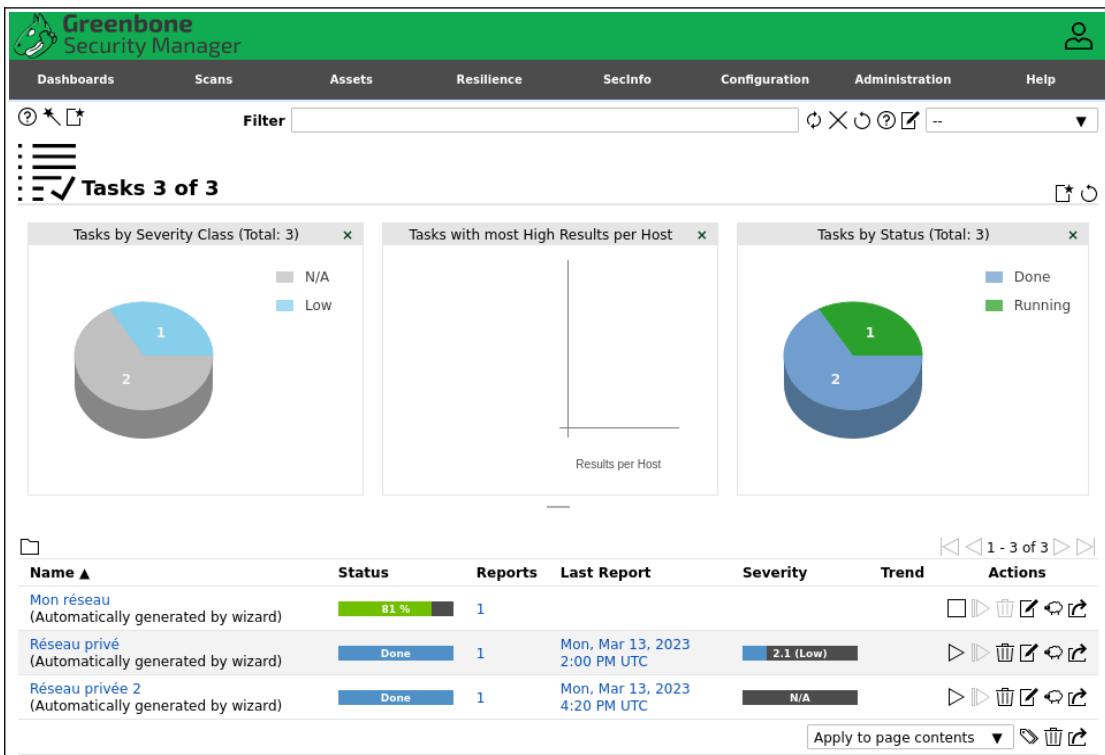
- Configuration > targets

6 ./Définition des identifiants

- Configuration > credentials

1 ./Recherches de vulnérabilités

- Scans > Tasks

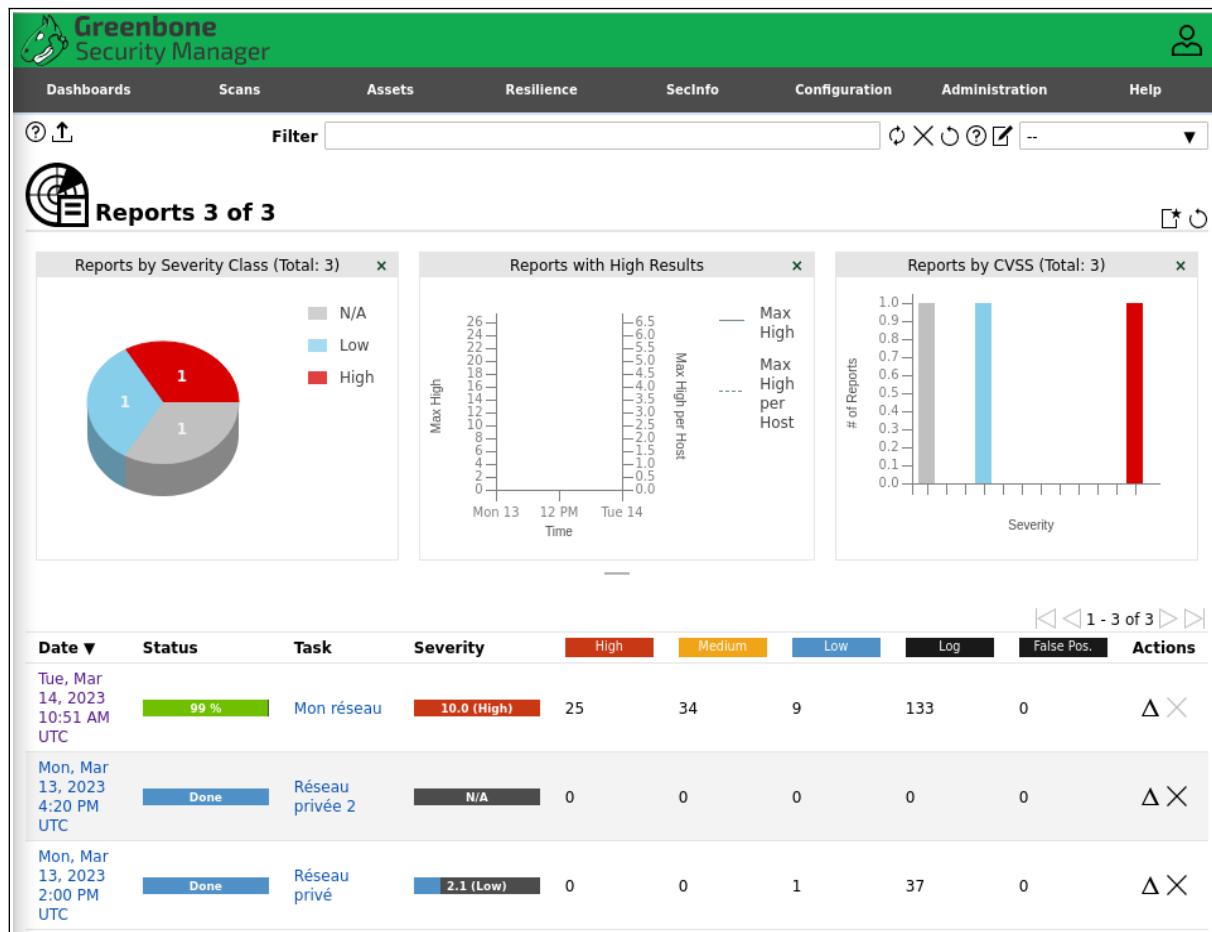


La catégorie **tasks** permet de **gérer les tâches** avec la colonne action ainsi que d'afficher l'**historique des scans** effectuées, les **résultats**, etc. Cette fonctionnalité apporte donc à une entreprise et/ou un administrateur réseau de **répertorier les scans** déjà émis en les datant afin de **garder une chronologie des analyses** sur son réseau.

Indiquant différentes informations tel que :

- Nom
- Status
- Niveau de gravité
- Date

- Scans > Reports



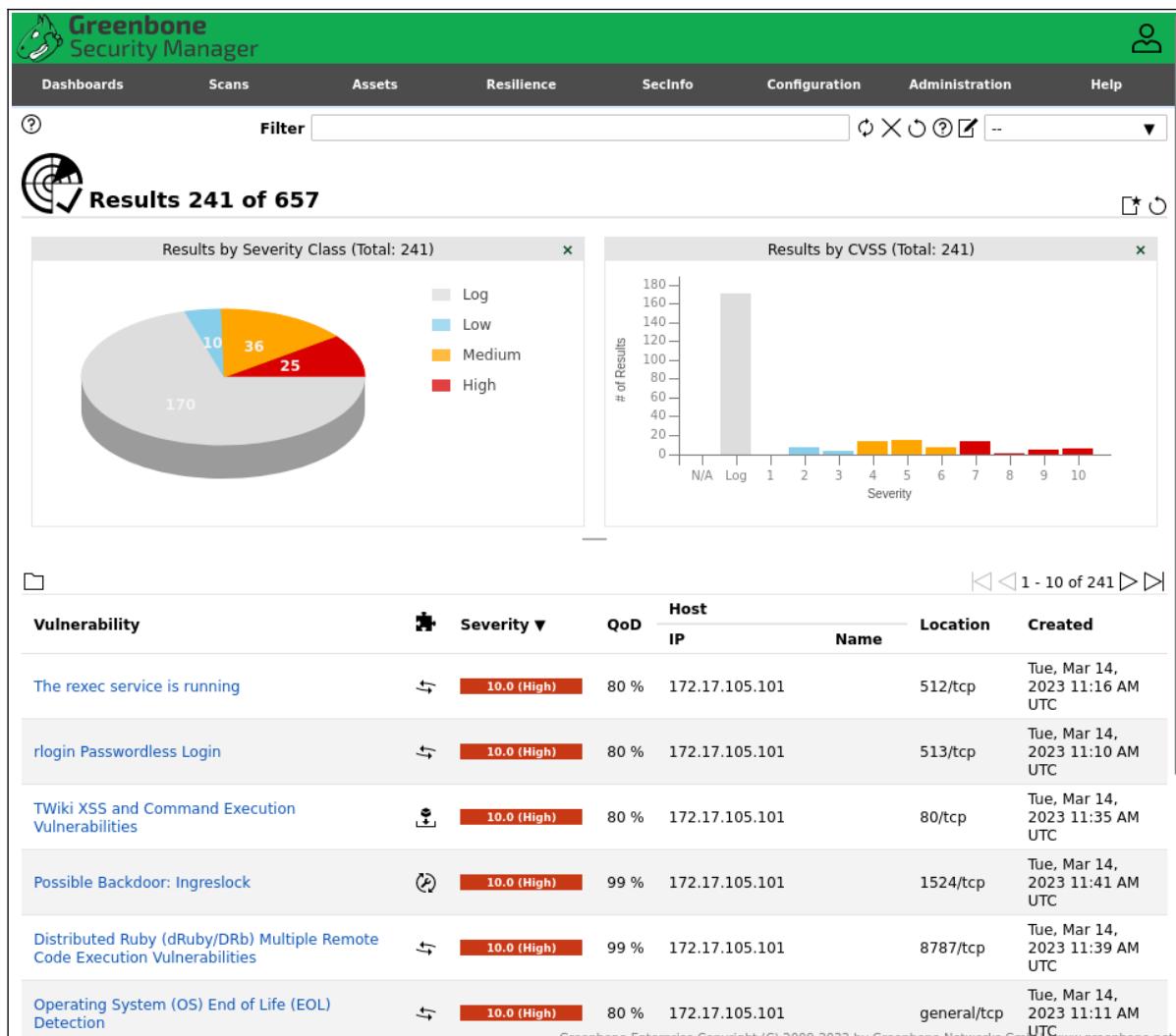
La catégorie **reports** paraît similaire, mais celle-ci offre plus de détails sur les **niveaux de gravité** rencontré concernant les **failles**, par ailleurs un indication du nombre de logs produit par le scan est affiché.

Une entreprise et/ou un administrateur réseau peut donc élaborer un **classement des failles de sécurité** lui permettant de produire un **graphe** classant les soucis rencontrés en fonction de leur **gravité ainsi que la vraisemblance** de ces derniers.

Le niveau de gravité d'une faille est déterminé par trois sections distinctes :

- High
- Medium
- Low

- Scans > Results



La catégorie **results** détaille l'ensemble des services et protocoles scannés sur vos machines en informant sur le **niveau de vulnérabilités**.

Ainsi, cette fonctionnalité guide l'administrateur en indiquant approximativement le **chemin** sur lequel vous orientez si vous souhaitez **investiguer** sur la faille ou bien **sécurisé** celle-ci.

Des colonnes informatives sont disponibles tel que :

- QoD (Pourcentage de fiabilité sur le scan effectué)
- Host IP
- Location (localisation de la possible faille)

- Scans > Vulnerabilities

Vulnerabilities 130 of 545

Name	Oldest Result	Newest Result	Severity ▾	QoD	Results	Hosts
Possible Backdoor: Ingreslock	Tue, Mar 14, 2023 11:41 AM UTC	Tue, Mar 14, 2023 11:41 AM UTC	10.0 (High)	99 %	1	1
The rexec service is running	Tue, Mar 14, 2023 11:16 AM UTC	Tue, Mar 14, 2023 11:16 AM UTC	10.0 (High)	80 %	1	1
rlogin Passwordless Login	Tue, Mar 14, 2023 11:10 AM UTC	Tue, Mar 14, 2023 11:10 AM UTC	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Tue, Mar 14, 2023 11:39 AM UTC	Tue, Mar 14, 2023 11:39 AM UTC	10.0 (High)	99 %	1	1
Operating System (OS) End of Life (EOL) Detection	Tue, Mar 14, 2023 11:11 AM UTC	Tue, Mar 14, 2023 11:11 AM UTC	10.0 (High)	80 %	1	1
TViki XSS and Command Execution Vulnerabilities	Tue, Mar 14, 2023 11:35 AM UTC	Tue, Mar 14, 2023 11:35 AM UTC	10.0 (High)	80 %	1	1
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Tue, Mar 14, 2023 11:45 AM UTC	Tue, Mar 14, 2023 11:45 AM UTC	9.8 (High)	99 %	1	1
DistCC RCE Vulnerability (CVE-2004-2687)	Tue, Mar 14, 2023 11:39 AM UTC	Tue, Mar 14, 2023 11:39 AM UTC	9.3 (High)	99 %	1	1
PostgreSQL Default Credentials (PostgreSQL Protocol)	Tue, Mar 14, 2023 11:30 AM UTC	Tue, Mar 14, 2023 11:30 AM UTC	9.0 (High)	99 %	1	1

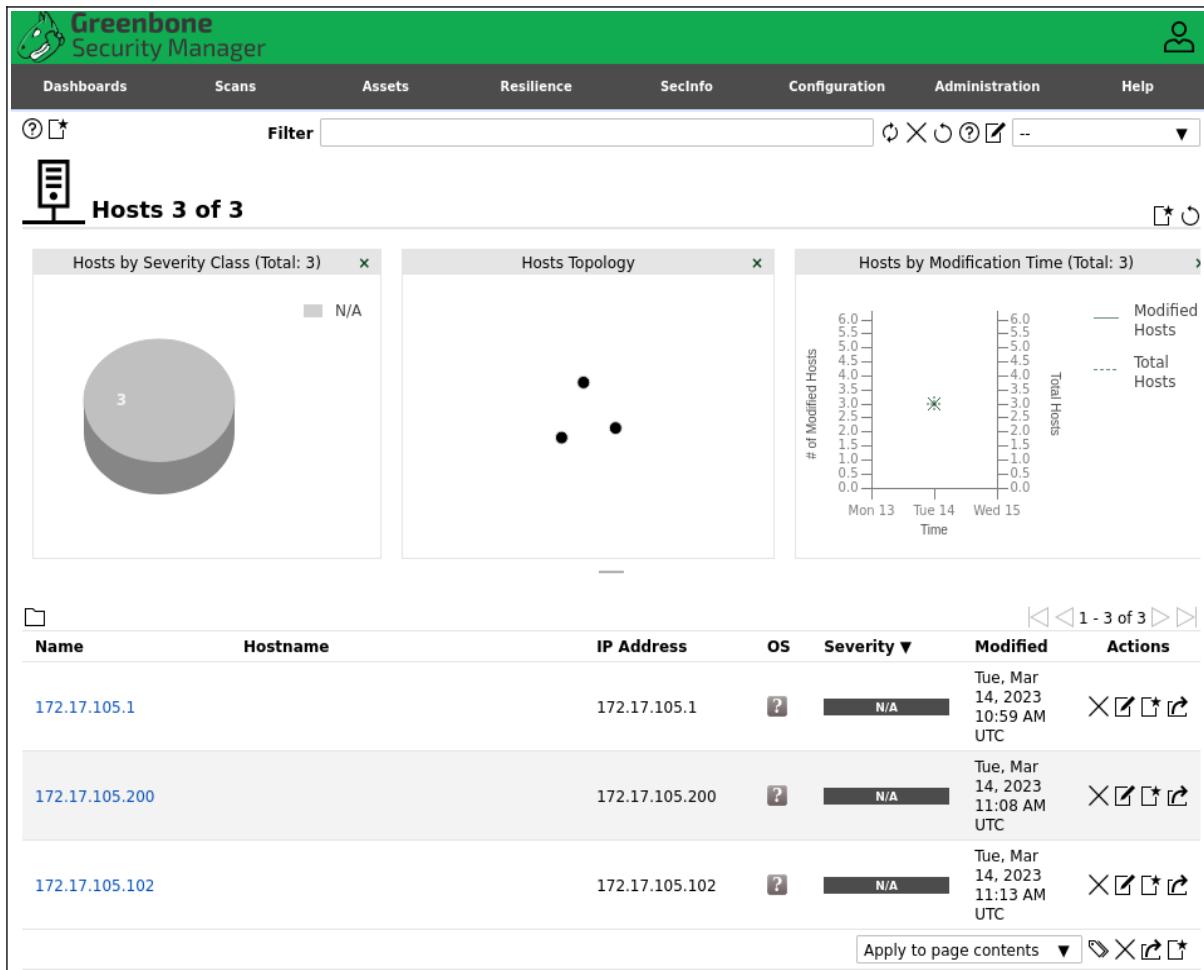
La catégorie **vulnerabilities** n'affiche que l'ensemble des possibles **vulnérabilités présentes sur l'ensemble d'un réseau** indiquant le nom complet de ces dernières. L'administrateur peut donc déterminer quels sont les **domaines touchés par une défaillance de sécurité**, en classant par ordre décroissant le **niveau d'importance**.

Différentes informations accompagnent le détaille des vulnérabilités :

- Oldest Result
- Newest Result
- QoD
- Hosts (nombre d'hosts possédant ce service/protocole et possiblement touchés par une faille de sécurité)

2 ./Gestion des actifs

- Assets > Hosts

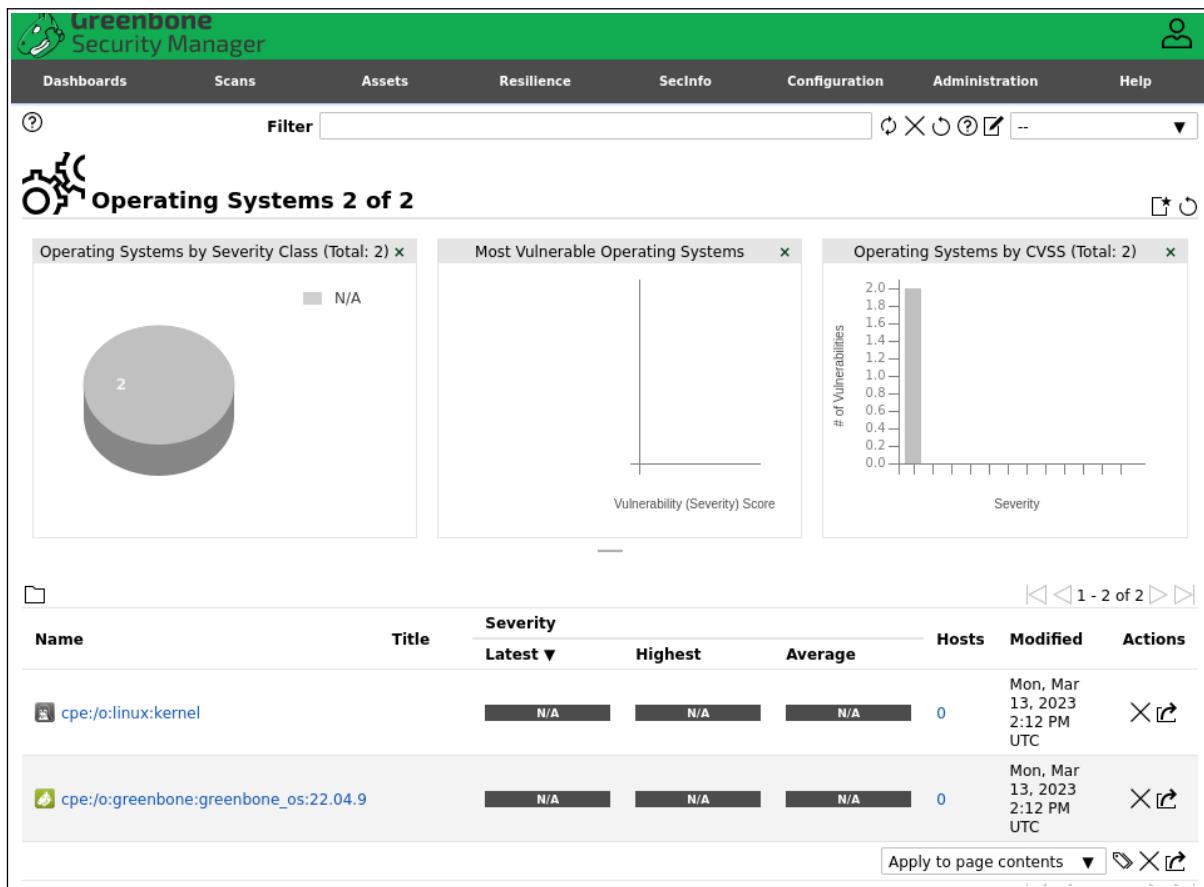


La catégorie **assets** permet de répertorier les **machines présentes sur le réseau** analysé ainsi que les **connexions entre elles**. En indiquant, les **adresses ip** ainsi que **l'OS** présent sur la machine concerné.

Renseignements disponibles sur l'infrastructure :

- Adress IP
- Schéma du réseau
- Connexion des machines
- OS
- Nom

- Assets > Operating Systems

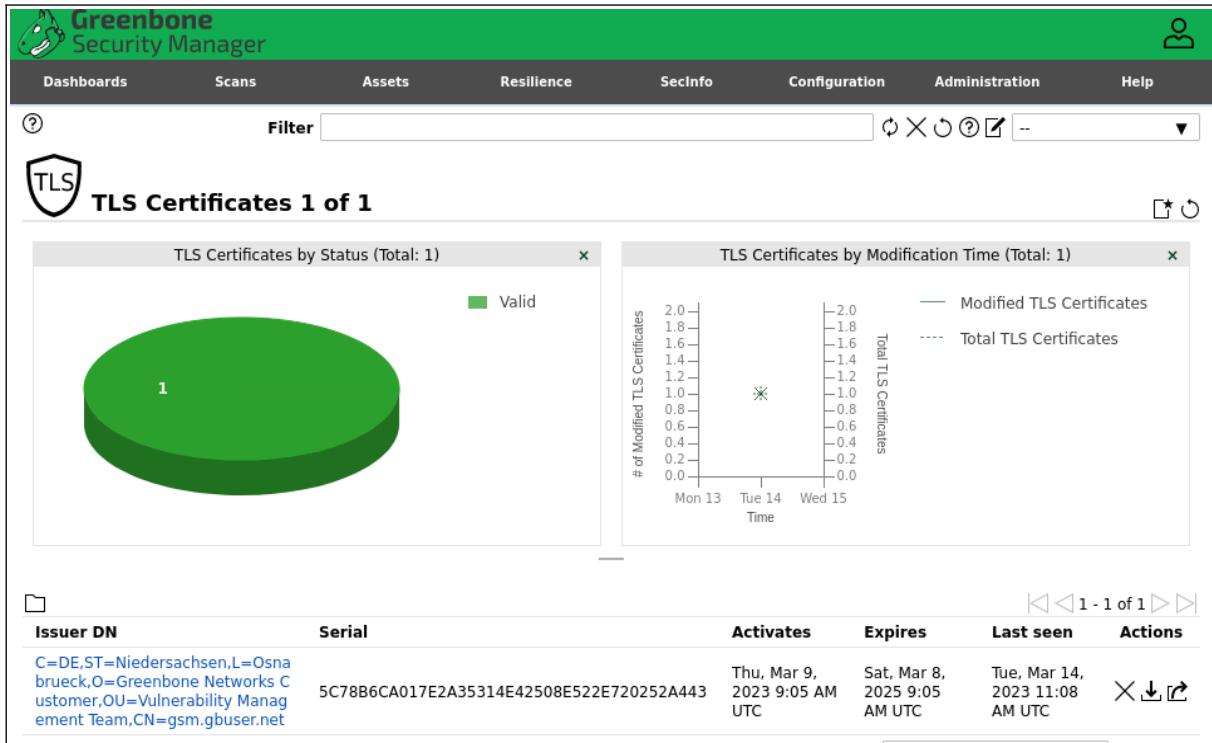


La catégorie **operating systems**, permet de visualiser les **systèmes d'exploitations** fournissant une vue différente sur les **données stockées**. Alors que la vue des hôtes est centrée sur les hôtes individuels, cette vue se concentre sur les systèmes d'exploitation **utilisés**.

Informations complémentaires disponibles :

- Nom de l'OS
- Niveau de sévérité
- Nombre d'hosts
- Date de modification

- Assets > TLS Certificates



Dans la catégorie **TLS Certificates**, tous les certificats TLS existants peuvent être affichés. Vous pouvez cliquez sur le **nom d'un certificat TLS** pour **afficher les détails** du certificat TLS.

Informations complémentaires disponibles :

- Nom distinctif
- Numéro de série
- Date d'activation
- Date d'expiration

3 ./Résilience

- Resilience > Compliance Policies

The screenshot shows the Greenbone Security Manager web interface. The top navigation bar includes links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A user icon is in the top right. Below the header is a toolbar with icons for search, filter, and actions. The main content area is titled 'Policies 6 of 6'. It lists six policy entries with their names, descriptions, and action buttons (Delete, Edit, Copy, etc.). The policies listed are:

- EulerOS Linux Security Configuration (Check compliance status of EulerOS 2.0 SP3/SP5/SP8 installation against above named Policy as distributed by Huawei. Version 20201215.)
- GaussDB 100 V300R001C00 Security Hardening Guide (Standalone) (Check compliance status of GaussDB installation against above named Policy as distributed by Huawei (based on Issue 5). Version 20201215.)
- GaussDB Kernel V500R001C00 Security Hardening Guide (Check compliance status against mentioned policy (based on Issue 01 from 2020-07-21). Version 20201222.)
- Huawei Datacom Product Security Configuration Audit Guide (Check compliance status of Huawei Datacom Device against above named Policy as distributed by Huawei. Version 20211209.)
- IT-Grundschutz Kompendium (Policy für Bausteine: SYS 1.2.2, SYS 2.2.2, SYS 2.2.3, SYS 1.3, SYS 2.3. Version 20210318.)
- openGauss Security Hardening Guide (Check compliance status against mentioned policy (based on Issue 01 from 2020-10-14). Version 20201222.)

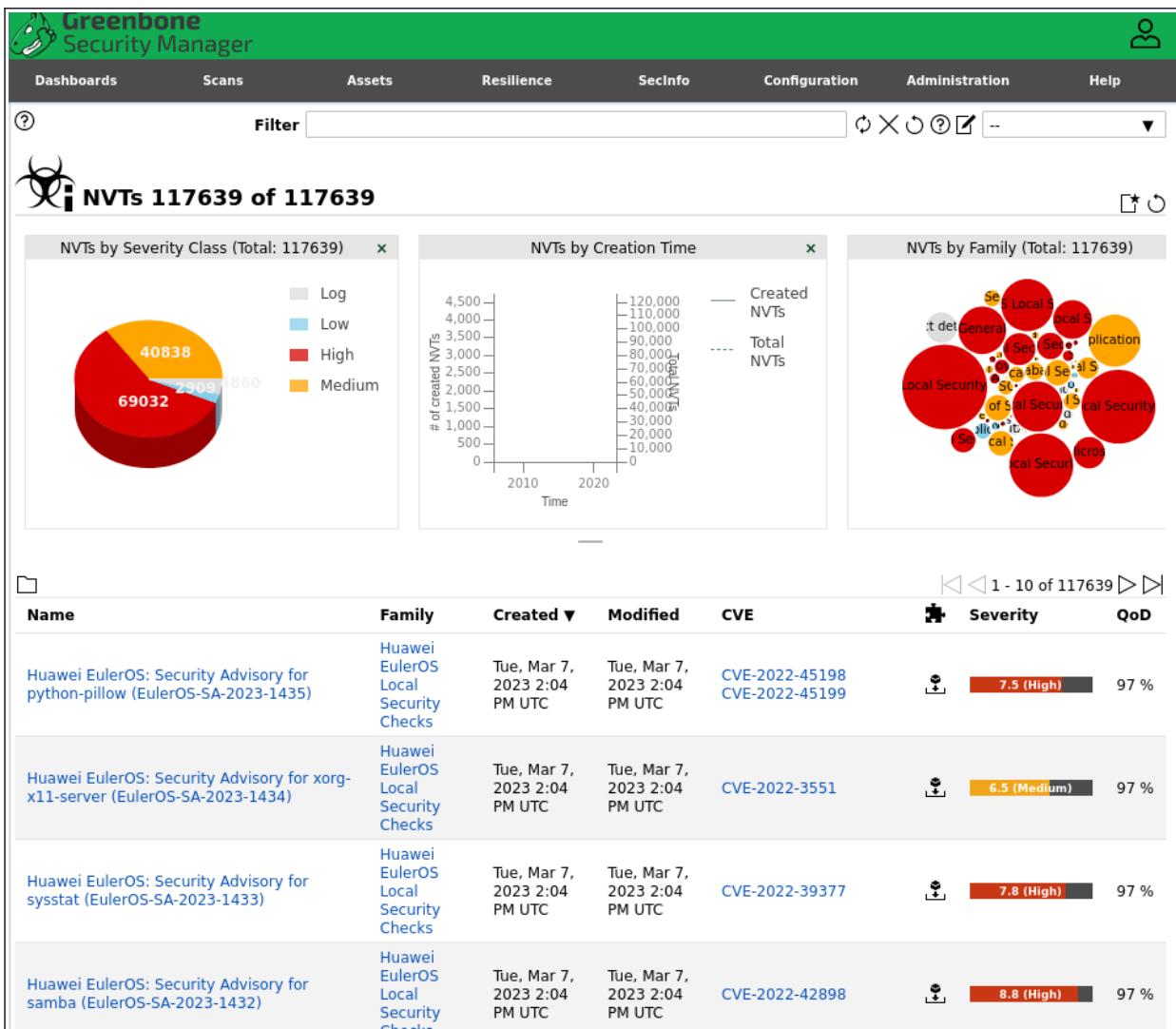
At the bottom right of the list, there are buttons for 'Apply to page contents' and a trash bin icon.

Dans la catégorie **Policies**, les **stratégies de conformité** sont utilisées par les **entreprises**, les **organisations** ou les autorités pour vérifier si tous les produits, applications, systèmes d'exploitation et autres composants utilisés **répondent à certaines spécifications**.

Informations complémentaires disponibles :

Nom complet des polices présentes sur greenbone, celles-ci peuvent être modifiés, cloner ou encore supprimés.

4 ./SecInfo



La gestion **SecInfo** fournit un accès **centralisé** à un large éventail d'informations de sécurité informatique. NVT autrement dit **Network vulnerability tests** répertoriant l'ensemble des vulnérabilités rencontrées.

Informations complémentaires disponibles :

- Nom
- Famille
- Date de création
- Date de modification
- Sévérité

5 ./Gestion des cibles

- Configuration > targets

The screenshot shows the Greenbone Security Manager web interface. At the top, there's a navigation bar with links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. On the far right of the header is a user profile icon. Below the header, there's a search bar with a 'Filter' input field and some advanced search options. The main content area is titled 'Targets 5 of 5'. It features a table with the following columns: Name, Hosts, IPs, Port List, Credentials, and Actions. The table lists five targets, each with a small icon to its left. The first target is 'Target for Mon réseau - 2023-03-14 10:51:54 (Automatically generated by wizard)' with hosts 172.17.105.0/24 and 254 ports. The second is 'Target for Réseau privé - 2023-03-13 14:00:02 (Automatically generated by wizard)' with hosts 192.168.1.0/24 and 254 ports. The third is 'Target for Réseau privée 2 - 2023-03-13 16:20:38 (Automatically generated by wizard)' with host 192.168.1.0 and 1 port. The fourth is 'Target for test - 2023-03-14 08:33:02 (Automatically generated by wizard)' with host 192.168.1.0 and 1 port. The fifth is 'Target for Test Réseau - 2023-03-14 10:41:00 (Automatically generated by wizard)' with hosts 172.17.105.0/24 and 254 ports. The 'Actions' column contains icons for delete, edit, and refresh.

Name	Hosts	IPs	Port List	Credentials	Actions
Target for Mon réseau - 2023-03-14 10:51:54 (Automatically generated by wizard)	172.17.105.0/24	254	All IANA assigned TCP		
Target for Réseau privé - 2023-03-13 14:00:02 (Automatically generated by wizard)	192.168.1.0/24	254	All IANA assigned TCP		
Target for Réseau privée 2 - 2023-03-13 16:20:38 (Automatically generated by wizard)	192.168.1.0	1	All IANA assigned TCP		
Target for test - 2023-03-14 08:33:02 (Automatically generated by wizard)	192.168.1.0	1	All IANA assigned TCP		
Target for Test Réseau - 2023-03-14 10:41:00 (Automatically generated by wizard)	172.17.105.0/24	254	All IANA assigned TCP		

Dans la catégorie **Targets**, toutes les cibles rencontrées lors des différentes analyses sont présentes ici afin d'obtenir un **historique des machines déjà analysées**. Greenbone liste donc via un **journal de log les hosts déjà ciblés** lors d'un scan.

Informations complémentaires disponibles :

- Nom
- Hosts (adresse IP)
- Ips
- Port list

6 ./Définition des identifiants

- Configuration > credentials

The screenshot shows the Greenbone Security Manager web interface. At the top, there is a green header bar with the 'Greenbone Security Manager' logo and a user icon. Below the header is a dark navigation bar with tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. To the left of the main content area is a sidebar with icons for help, star, filter, and a key. The main content area has a title 'Credentials 0 of 0'. Below the title, it says 'No credentials available' and '(Applied filter: sort=name first=1 rows=10)'. There is a search bar labeled 'Filter' with some placeholder text and a dropdown menu.