Exploration

Analyse de vulnérabilités avec Kali et GSM OpenVAS

Rédigé par

David ROUMANET
Professeur BTS SIO

Changement

Date	Révision
16/12/2023	Correction symlink pour édition fichier (accès distant web possible)

Sommaire

A Introduction....1
A.1 Présentation....1
A.2 Prérequis....1
B Analyses de vulnérabilités....2
B.1 Les vulnérabilités....2
B.1.1 définition....2
B.1.2 Histoire des vulnérabilités....2
B.1.3 CVE : Common Vulnerabilites and Exposures....3
B.1.4 CVSS : Common Vulnerability Scoring System....3
C Installation Kali....5
C.1 Téléchargement....5
C.2 Installation....5
C.3 Configuration....5
D Installation OpenVAS (GVM)....6
D.1 Fonctionnement OpenVAS....6
D.2 Installation OpenVAS....6
D.2.1 Préparation base de données....6
D.2.2 Installation OpenVAS....7
D.2.3 Lancement d'OpenVAS....8
D.2.4 Modification d'accès web distant à OpenVAS....9
D.2.5 Observation des menus....10
D.2.5.a CVE (Common Vulnerabilites and Exposures)....10
D.2.5.b NVT (Network Vulnerabilities Tests)....10
D.3 Gestion d'une analyse OpenVAS....11
D.3.1 Analyse rapide d'une machine....11
D.3.2 Lecture des résultats et des rapports....12
D.4 Configuration d'audits réguliers....13
D.4.1 Création de groupes d'utilisateurs....14
D.4.2 Création d'utilisateurs....14
D.4.3 Usage des rôles....15
E Annexes....16
E.1 Sources....16
E.2 Autres....16
E.2.1 Trace d'attaque depuis un parefeu....16
E.3 Commandes de diagnostic pour kali....16
E.4 Perte du mot de passe....17
E.5 Problème avec pg-gvm....17
E.6 Architecture technique de Greenbone OpenVAS :....17

Nomenclature :

- **Assimiler** : cours pur. Explication théorique et détaillée (globalement supérieur à 4 pages).
- **Décoder** : fiche de cours, généralement inférieure à 5 pages.

- **Découvrir** : Travaux dirigés. Faisable sans matériel.
- **Explorer** : Travaux pratiques. Nécessite du matériel ou des logiciels.
- **Mission** : Projet encadré ou partie d'un projet.
- **Voyager** : Projet en autonomie totale. Environnement ouvert : Vous êtes le capitaine !

A Introduction

Les systèmes d'information sont un enjeu capital dans le fonctionnement de l'économie actuel. Aucune organisation ne peut se passer des outils informatiques.

La complexité des ordinateurs et des systèmes d'exploitation est telle, qu'il est impossible d'en garantir la sécurité : au mieux, on peut limiter les risques.

Les DSI et les RSSI ont donc pour mission de s'assurer que leurs systèmes d'information sont à jour, correctement configurés et protégés au maximum. Si la protection via des équipements spécialisés tel que les parefeux semble évidente, le contrôle de la protection est rarement évoqué, sinon par l'intermédiaire d'audit via des sociétés spécialisées.

A.1 Présentation

L'analyse de vulnérabilité est une mission que devrait réaliser tous les services informatiques, une fois par semestre.

Contrairement à une tentative d'accès frauduleuse, l'analyse de vulnérabilité est très transparente : il est recommandé d'utiliser des outils spécialisés (comme OpenVAS, Nessus ou Qualys) et de fournir les identifiants d'accès aux systèmes à évaluer.

Ce n'est donc pas une recherche de faille, au sens d'une enquête pour trouver comment rentrer dans un SI, mais un inventaire des équipements sensibles aux vulnérabilités connues.

Pour cela, il faut comprendre que l'ensemble des vulnérabilités informatiques sont inventoriées et classées. Cette activité a pour but de présenter ce classement, puis de proposer la mise en œuvre de l'outil d'analyse OpenVAS pour en comprendre le fonctionnement et l'intérêt.

A.2 Prérequis

Pour réussir correctement cette activité il est préférable de…

- Connaître les commandes Linux
- Savoir installer la distribution Kali
- Comprendre les notions réseaux de ports, services, adresses...
- Avoir une cible sans risque (un faux serveur)
- Un accès Internet performant (téléchargement des bases de vulnérabilités)

B Analyses de vulnérabilités

Comme tout système, nul ne peut être garant qu'il n'y a pas de failles dans le sien.

La plupart du temps, la mise à jour de ses équipements permettent de lutter contre différentes attaques, mais il peut arriver que certains patchs introduisent (involontairement) des erreurs, dont un pirate pourrait tirer parti.

B.1 Les vulnérabilités

B.1.1 définition

Une **vulnérabilité** est une faiblesse dans un système informatique, permettant à une personne malveillante ou non, d'obtenir des informations ou des droits qu'elle n'est pas autorisée à avoir.

Connaître le défaut d'un système permet de cibler des **attaques** et parfois trouver une **exploitation** de la faille.

B.1.2 Histoire des vulnérabilités

Historiquement, en informatique, de multiples acteurs de la sécurité, référençaient les vulnérabilités avec plus ou moins d'objectivité et de connaissances. Les échanges étaient peu nombreux : une partie de la sécurité reposait sur le secret.

Rapidement, les hackers ont profité de ce secret, pour exploiter de nombreux systèmes en toute tranquillité, puisque les vulnérabilités n'étaient pas connues des administrateurs. Il est alors apparu nécessaire de rendre les vulnérabilités publiques, afin que chaque organisation puisse lutter contre celles-ci (soit par des mises à jour de l'éditeur/constructeur, soit par une protection en amont, comme les parefeux, les antivirus, les WAF ou les IPS).

L'association MITRE et une organisation à but non-lucratif américaine dont l'objectif est de travailler pour l'intérêt public. Ses domaines d'intervention sont l'ingénierie des systèmes, la technologie de l'information, les concepts opérationnels, et la modernisation des entreprises.

En 1999, le bureau du CVE, créé par MITRE, recense et la publie la première liste de toutes les vulnérabilités connues, dans une base de données publique.

Depuis, l'accès à ces bases peuvent donc se faire via différents sites (chacun pouvant développer son moteur web) :

- https://cve.mitre.org 🇺🇸
- https://www.cvedetails.com/ 🇺🇸
- https://www.cert.ssi.gouv.fr/ 🇫🇷

B.1.3 CVE : Common Vulnerabilites and Exposures

Le nombre croissant de vulnérabilités impose l'usage d'une convention de nommage robuste. L'abréviation CVE suivi de l'année puis d'un numéro chronologique permet d'affecter un numéro unique à chaque vulnérabilité recensée.

- Avant 2014, la convention est la suivante : CVE-YYYY-NNNN
- À partir de 2014, la convention change pour : **CVE-YYYY-NNNNN**

En effet, l'augmentation rapide des vulnérabilités nécessite désormais 5 chiffres par années (un million de possibilités).

Cette référence est appelée "enregistrement CVE" (record CVE) ou "identifiant CVE" (**CVE ID**).

La création d'un nouvel enregistrement CVE se fait par un des organismes officiels appelés CVE Numbering Authorities (**CNA**s).

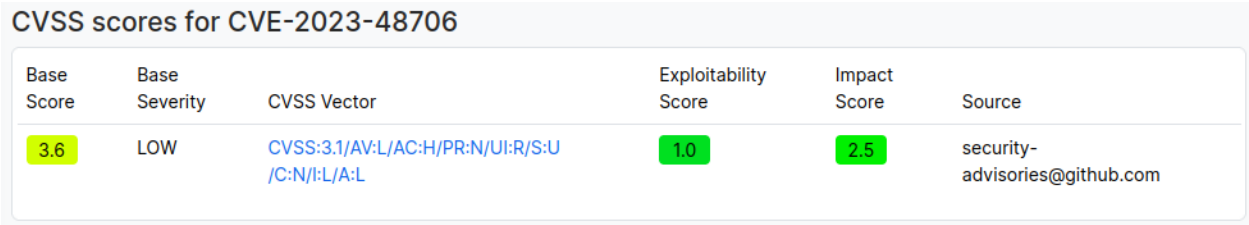
B.1.4 CVSS : Common Vulnerability Scoring System

Chaque vulnérabilité est évaluée pour déterminer sa dangerosité. L'impact et la probabilité ne suffisent pas à créer une échelle correcte. Un outil existe donc pour évaluer de la même manière, l'ensemble des vulnérabilités.

L'outil https://www.first.org/cvss/calculator/4.0 permet de constater les diverses informations nécessaires pour classer une vulnérabilité :

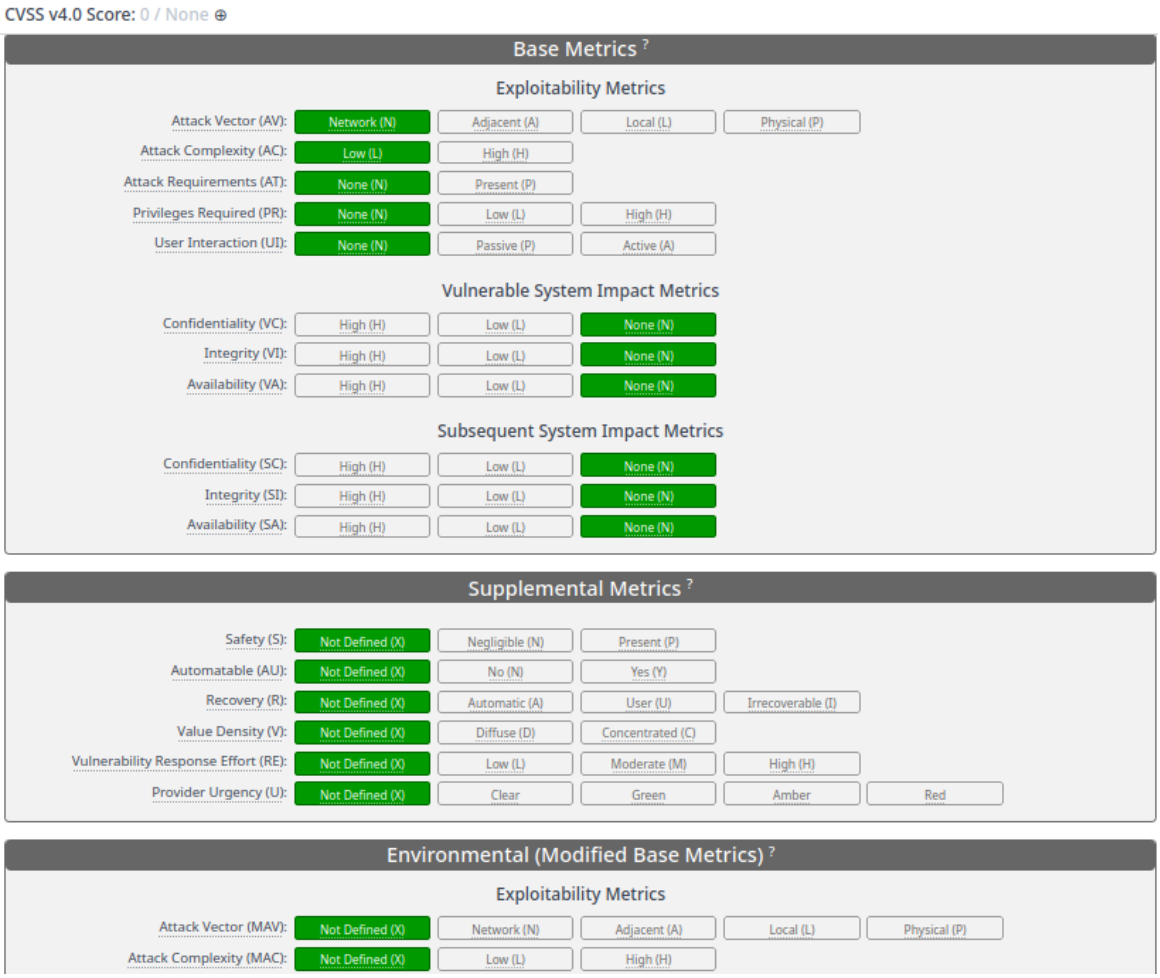
- Indicateurs d'exploitabilité
- Indicateurs supplémentaires
- Indicateurs liés à l'environnement
- Indicateurs de menace (exemple, la maturité de l'exploitation)

L'évaluation des différents indicateurs permet alors de fournir une évaluation des risques qui sont indiqués dans la fiche de la CVE.


CVSS scores for CVE-2023-48706

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
3.6	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L	1.0	2.5	security-advisories@github.com

Capture d'écran d'une partie des indicateurs nécessaires à l'évaluation des risques :



Les différents champs sont enregistrés dans le format JSON, comme dans l'exemple CVSS 3.1 ci-dessous :

```
{
    "version": "3.1",
    "vectorString": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",
    "baseScore": 7.8,
    "baseSeverity": "HIGH"
}
```

Actuellement, la normalisation CVSS est en version 4.0.

Il est possible de télécharger la liste des CVE sur le site https://www.cve.org/Downloads au format JSON 5. En novembre 2023, cette liste fait 300 Mo compressée (soit 1,5 Go décompressée).

C Installation Kali

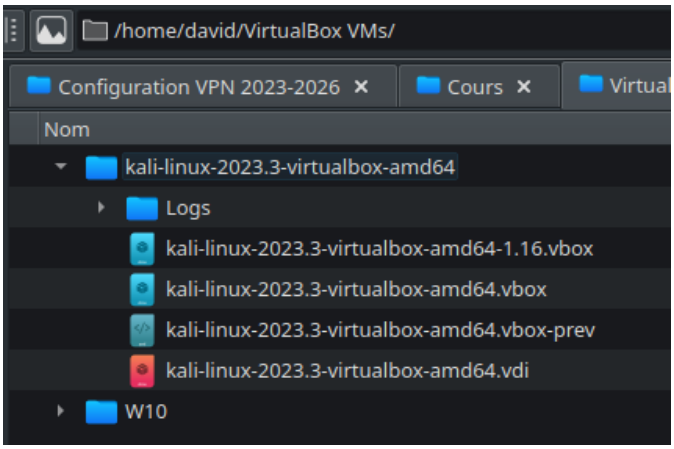
C.1 Téléchargement

Pour les tests, nous utiliserons une machine virtuelle (Virtualbox dans mon cas)

Le lien de téléchargement est donc : https://www.kali.org/get-kali/#kali-virtual-machines

C.2 Installation

Une fois le fichier téléchargé, il faut le décompresser dans un dossier de votre disque, dédié aux machines virtuelles.



C.3 Configuration

Les identifiants d'accès sont :

login : **kali**
mot de passe : **kali**

Toutefois, au démarrage de la machine, le clavier est en format US.

Deux instructions pour y remédier.

La première permet de retrouver rapidement un clavier en français, mais est temporaire : `setxkbmap fr`

La deuxième instruction permet de lancer une configuration du clavier :
`sudo dpkg-reconfigure keyboard-configuration`

Choisir 'other' pour pouvoir installer un clavier français et AZERTY.

Théoriquement, mettre à jour l'OS avec `sudo apt update` et `sudo apt upgrade` (souvent très long).

⚠ Si ce n'est déjà fait, configurer l'interface réseau de la machine virtuelle en mode `pont` (dans Virtualbox, VM éteinte).

La machine est désormais opérationnelle.

D Installation OpenVAS (GVM)

D.1 Fonctionnement OpenVAS

OpenVAS est un outil capable d'analyser un ensemble de machines (une plage, un subnet ou une liste) et de lire les informations transmises sur les ports ouverts.

Il ne s'agit pas d'un outil d'attaque, dans la mesure ou l'auditeur qui emploie cet outil, doit renseigner les identifiants des machines et des services.

Pour réaliser ces taches d'analyses, il faut installer OpenVAS, puis télécharger les listes de CVE à jour et lancer une analyse avec les paramètres voulus. Bien qu'il soit possible d'utiliser cet outil de manière ponctuelle, un administrateur réseau et sécurité prendra soin de lancer régulièrement des analyses sur son réseau.

Il est possible de créer des rôles, afin que chaque responsable puisse lancer un audit sur les machines ou les services dont il a la charge.

À la fin de l'audit, OpenVAS fournit un compte-rendu exhaustif des vulnérabilités potentielles.

D.2 Installation OpenVAS

à l'origine, OpenVAS est un produit de GSM. Il s'agit d'un ensemble de services qui utilisent une base PostgreSQL.

D.2.1 Préparation base de données

Saisir les instructions suivantes :

```
sudo apt-get install postgresql-16
sudo apt-get install postgresql-client-16
sudo vi /etc/postgresql/15/main/postgresql.conf
```

Changez le port en 5433 (placer le curseur sur le 2, taper `R` puis `3` puis `:wq`)

Note : pour ceux qui lisent correctement les phrases, vous pouvez aussi utiliser **nano** à la place de **vi**. vi est un éditeur de texte très connu et très puissant, mais aux commandes difficiles à apprendre.

Faire l'opération inverse pour l'autre fichier :

```
sudo vi /etc/postgresql/16/main/postgresql.conf
```

Changez le port en 5432 (placer le curseur sur le 3, taper `R` puis `2` puis `:wq`)

Enfin, redémarrez votre kali (il serait plus simple de stopper et redémarrer le service PostgreSQL, pour ceux que ça tente…)

D.2.2 Installation OpenVAS

Une fois la base de données modifiée, installer GSM (attention, la mise à jour apt-get upgrade est très longue, essayer d'abord d'installer sans cette phase) :

```
sudo apt-get install openvas gvm
sudo gvm-setup
```

Note : l'opération nécessite le téléchargement de bases de données très importantes et volumineuses. Il est probable de devoir se lancer dans une autre activité durant ce temps.

Vous devriez obtenir un écran similaire pendant la synchronisation des bases :

```
[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password 'bc66b418-af77-4be3-9d87-482762f2ebe7'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
| Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-da
ta/notus/ to /var/lib/notus
/ Downloading NASL files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-da
ta/nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
/ Downloading SCAP data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-
data/ to /var/lib/gvm/scap-data
```

Attention : veuillez noter le mot de passe de l'utilisateur pour OpenVAS, car il ne sera pas réaffiché par la suite.

Lorsque l'installation est terminée, vous pouvez vérifier que tout fonctionne avec la commande :

```
sudo gvm-check-setup
```

Les messages d'erreurs peuvent vous aider à résoudre les problèmes. En particulier, la nécessité d'installer pg-gvm :

```
sudo apt-get install postgresql-16-pg-gvm
```

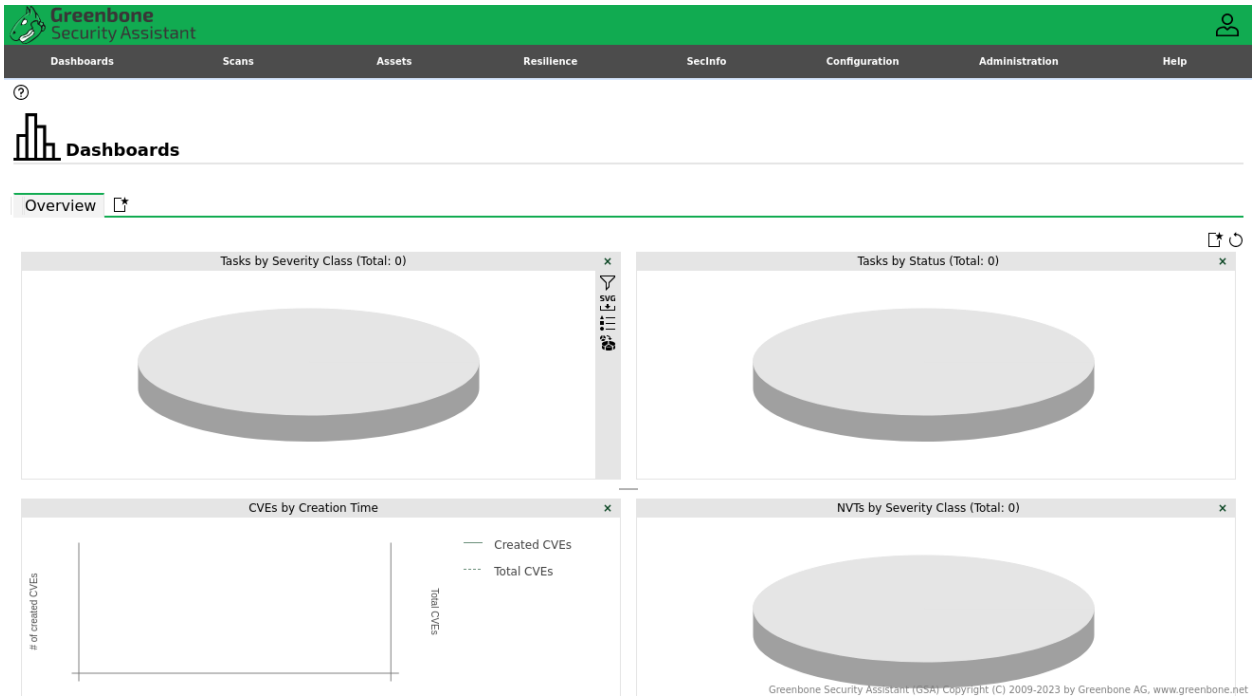
D.2.3 Lancement d'OpenVAS

Le lancement d'OpenVAS se fait avec la commande `sudo gvm-start`.

Il s'agit d'un serveur web, accessible à distance. Copier l'URL et l'ouvrir dans un navigateur.

https://127.0.0.1:9392

admin
(mot de passe copié)



Le problème est qu'il n'est pas possible d'accéder à cette interface d'administration autrement que localement.

Les modifications à apporter sont sur les fichiers `greenbone-security-assistant.service`.

Nous utiliserons `sed`[1] (**s**tream **ed**itor) qui est – pour simplifier – un éditeur de fichier programmable.

1 https://www.ionos.fr/digitalguide/serveur/configuration/commande-sed-de-linux/

D.2.4 Modification d'accès web distant à OpenVAS

Ce placer dans le répertoire `/lib/systemd/system` puis copier la commande suivante :

```
sed --follow-symlinks -i 's/127.0.0.1/0.0.0.0/g' greenbone-security-assistant.service
```

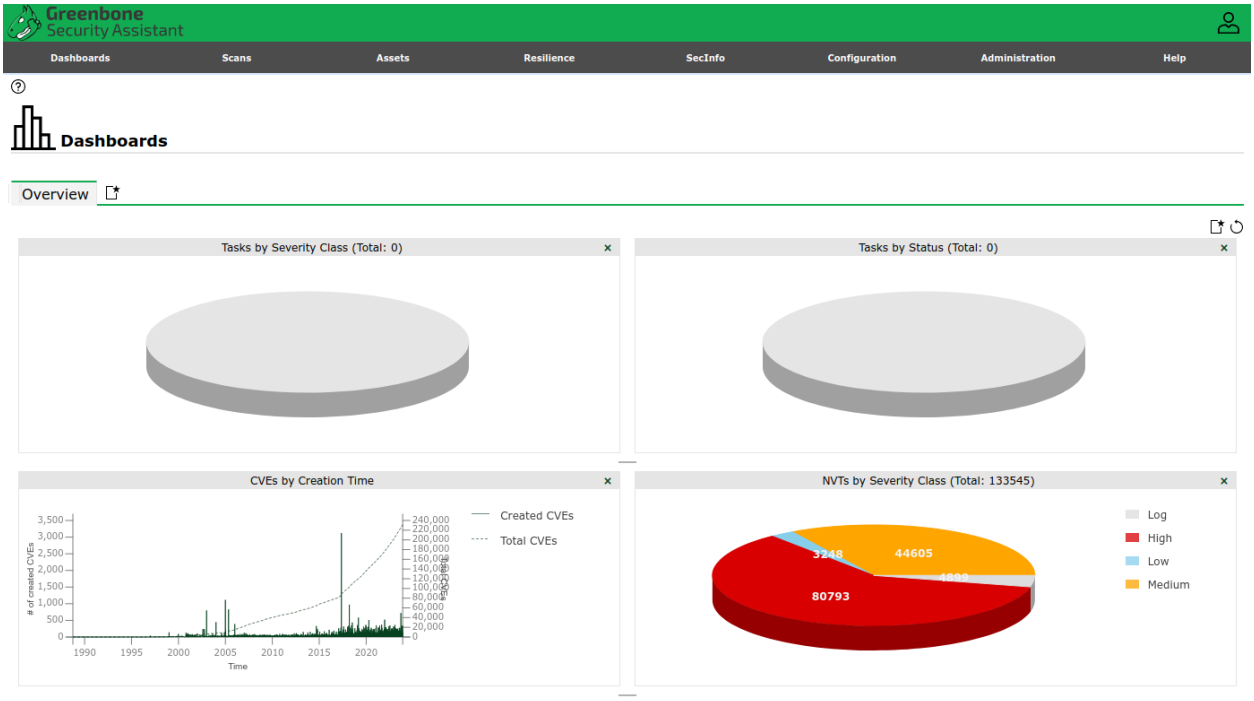
La commande va remplacer automatiquement 127.0.0.1 par 0.0.0.0 dans le fichier. Exemple :

```
ExecStart=/usr/sbin/gsad –foreground --listen 0.0.0.0 --port 9392
```

Il faut ensuite redémarrer les services (démons). Dans un premier temps, on recharge la configuration, puis on lance chaque service :

```
systemctl daemon-reload
systemctl restart greenbone-security-assistant.service
```

Il doit maintenant être possible d'accéder à la page d'OpenVAS à distance (en HTTPS sur le port 9392) : pour cela, vérifiez l'adresse de la machine Kali avec l'instruction `ip addr`.



Si l'accès est toujours impossible à distance, le lien symbolique entre le fichier greenbone-security-assistant.service et gsad.service. Dans ce cas, il suffit d'éditer ce dernier :

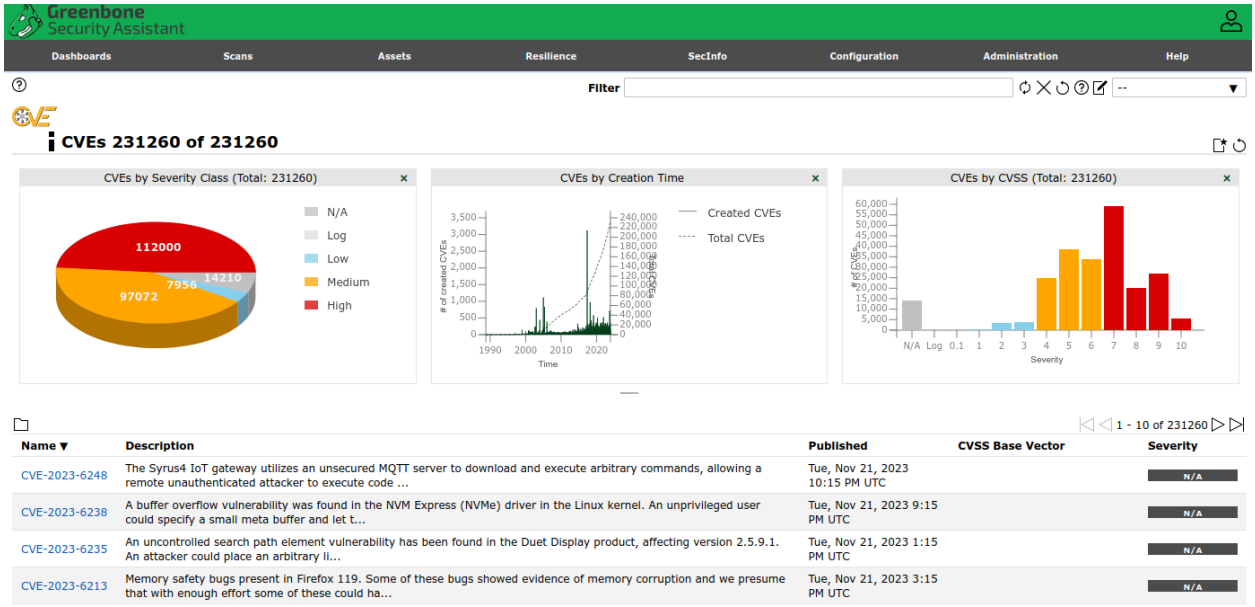
```
sed --follow-symlinks -i 's/127.0.0.1/0.0.0.0/g' gsad.service
```

Puis relancer les services, comme précédemment.

D.2.5 Observation des menus

D.2.5.a CVE (Common Vulnerabilites and Exposures)

Dans le menu d'OpenVAS, cliquer sur **SecInfo** → **CVE's** :



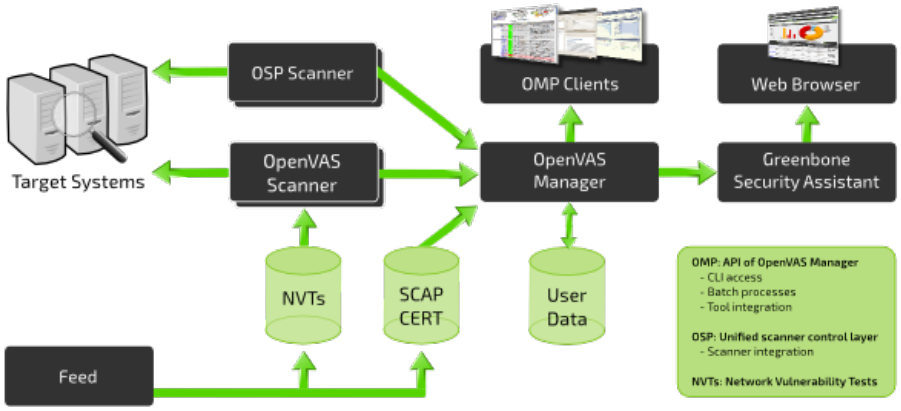
Ce menu permet de voir les CVEs présentes dans la base d'OpenVAS : les graphiques indiquent le nombre de CVE par sévérité, l'évolution des CVEs dans le temps et les CVEs par score CVSS.

Il est possible de filtrer les CVEs pour trouver une marque ou une référence, dans le champ `Filter`.

Tester avec le mot "opnsense".

D.2.5.b NVT (Network Vulnerabilities Tests)

Les NVTs sont des vecteurs d'attaques utilisables par OpenVAS (et des attaquants).



OpenVAS est un produit open-source qui se décline en deux versions :

- Édition Entreprise (GSF = Greenbone Security Feed)
- Édition Communautaire (GCF = Greenbone Communauty Feed)

La première version dispose de beaucoup plus de NVT (notamment les bases pour les produits d'entreprises ainsi que les conformités ISO27001).

D.3 Gestion d'une analyse OpenVAS

Désormais, nous pouvons utiliser et paramétrer OpenVAS pour effectuer des tâches pour nous.

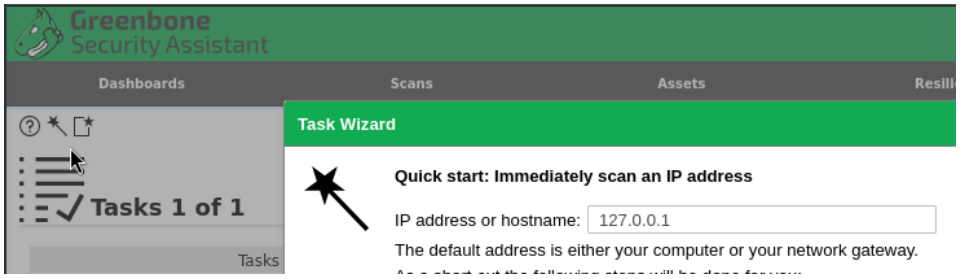
Dans un premier temps, nous allons lancer un scan d'une machine, puis nous verrons ensuite comment utiliser OpenVAS de manière régulière, dans une organisation.

Il s'agit d'un outil à déployer dans le cadre d'analyses régulières de cybersécurité : plusieurs groupes et plusieurs personnes peuvent avoir besoin de tester des périmètres de sécurité différents.

D.3.1 Analyse rapide d'une machine

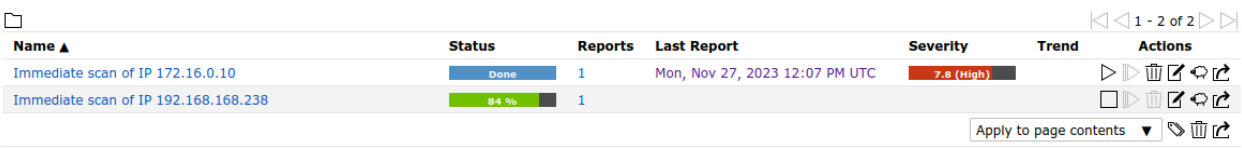
L'analyse la plus rapide et simple peut se faire en quelques clics : aller dans le menu **Scans** → **Tasks** puis cliquer sur l'icône en forme de baguette magique et choisir **Task Wizard**.

Saisir une adresse IP à scanner dans le champ de saisie, cliquer sur **Start Scan** et patienter. La tâche peut prendre plusieurs dizaines de minutes. Sur ma VM, l'audit a duré 2 heures.



Le lancement d'un audit passe par plusieurs états :

Requested	Queued	Running	Error	Done
Création de la tâche	Mise en file d'attente	Exécution	Problème durant le scan	Tâche terminée



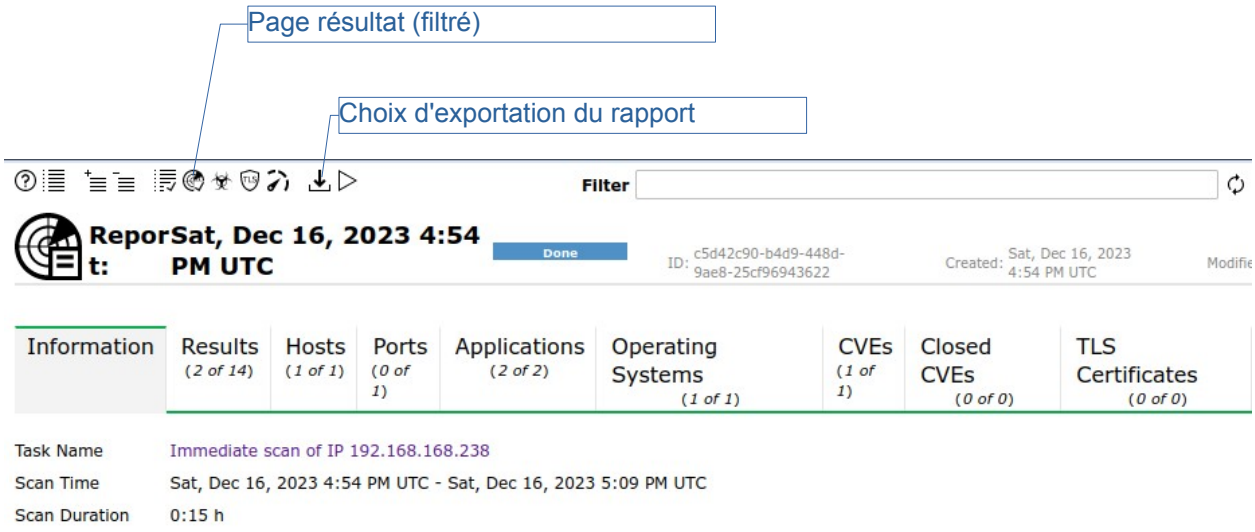
D.3.2 Lecture des résultats et des rapports

L'accès aux résultats et aux rapports se fait dans le menu Scans :

- **Scans → Résults** affiche toutes les vulnérabilités rencontrées, quelles que soient les dates, les tâches et les machines. C'est une vue plutôt statistique.
- **Scans → Reports** affiche les différents rapports (par dates). Cet affichage est plus intéressant, car il permet d'afficher une synthèse d'un audit et même de l'exporter aux formats PDF, XML ou

Dans le cas de l'affichage des rapports, l'interface est un peu particulière, puisqu'un clic sur la date ne renvoie pas sur le même menu qu'un clic sur la machine auditée.

L'affichage du menu lié à la date guide vers une autre page.



D.4 Configuration d'audits réguliers

L'intérêt d'un outil d'analyse de vulnérabilités, n'est pas de réaliser un audit ponctuel : l'administrateur pourra mettre en œuvre les protections recommandées pour sécuriser les services et les équipements, par exemple :

- Mise à jour du firmware ou des patchs
- Fermeture des services inutiles (ports ouverts inutilement) et/ou protéger en amont avec un parefeu
- Modifier la configuration des services pour éviter la prise d'empreinte (reconnaissance d'OS et de services)
- Activation des journaux (logs) pour améliorer la détection d'attaques
- etc.

Cependant, quelques mois après, le contexte n'est déjà plus le même, de nombreuses nouvelles vulnérabilités sont découvertes.

Réflexion : il paraît logique de vouloir mettre à jour ses équipements et serveurs avec les dernières mises à jour, dès leurs publications. Toutefois, il arrive que ces mises à jour contiennent des bogues ou introduisent de nouvelles failles. Il est donc raisonnable d'effectuer les mises à jour à quelques jours d'intervalle, afin de s'assurer de ne pas introduire plus de problèmes que les corrections apportées. De manière générale, la mise en production d'un correctif devrait idéalement être testée sur un environnement de test.

Il est donc intéressant de configurer l'outil pour pouvoir effectuer des audits réguliers (en mettant à jour les bases de vulnérabilités d'abord).

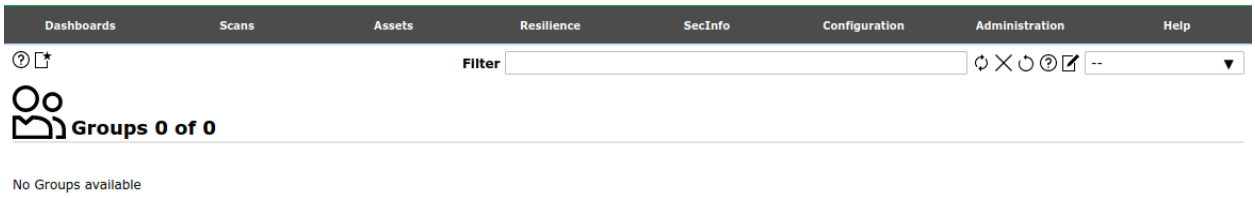
Pour cela, on peut configurer :

- Des groupes d'utilisateurs : les administrateurs de bases de données, les administrateurs réseaux, les administrateurs systèmes… ou par rôle, comme les administrateurs, les personnes avec pouvoir (un responsable qui ne configure pas les systèmes), un utilisateur, etc.
- Des groupes de machines : les serveurs internes, les serveurs en DMZ, les équipements actifs du réseau, etc.
- Des groupes de tâches : des audits rapides hebdomadaires et des audits plus profonds mensuels.

L'ensemble des choix est à définir par la DSI et le RSSI dans un document de politique de sécurité du SI.

D.4.1 Création de groupes d'utilisateurs

Dans le menu Administration → Groups il est possible de créer des groupes, un peu comme dans un annuaire LDAP. L'intérêt est par exemple, de limiter l'accès des rapports à certains groupes. Par exemple, l'audit du serveur de messagerie ne serait pas visible au groupe qui gèrent les serveurs web.



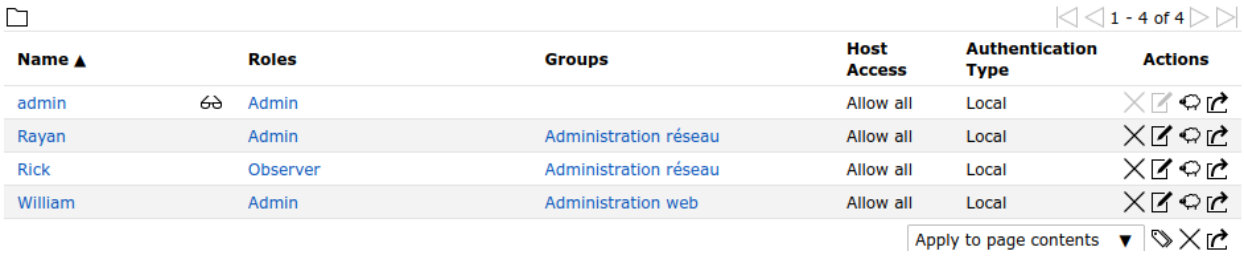
Créez les groupes suivants (en cliquant sur l'icône représentant une feuille avec une étoile) :

- Administration web : administrateurs des services web de l'entreprise
- Administration réseau : administrateurs des équipements de niveau 2 et 3
- Comité de sécurité : Les responsables de services

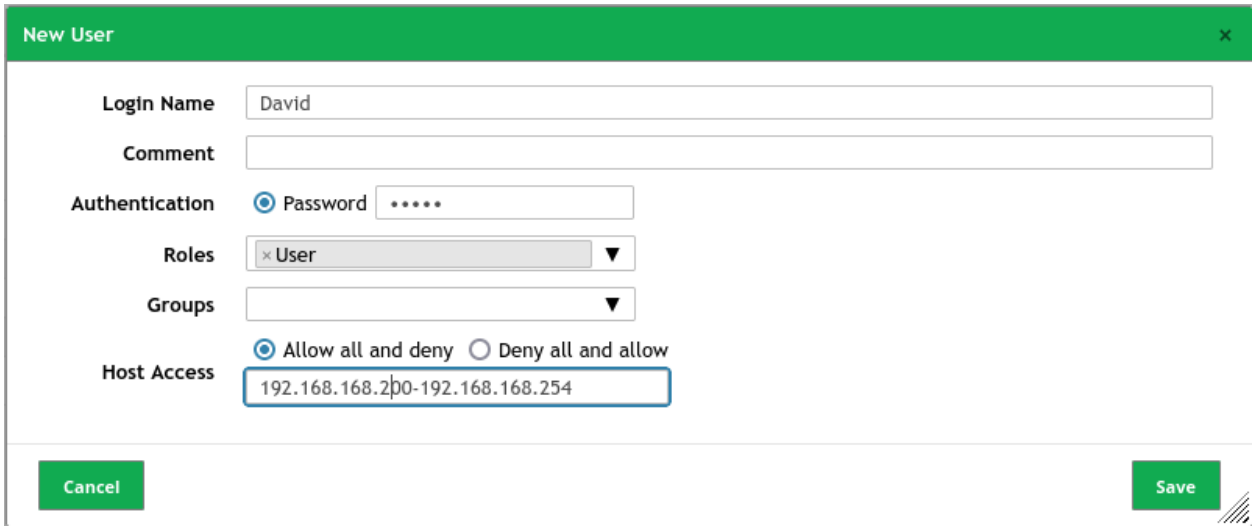
D.4.2 Création d'utilisateurs

Dans le menu Administration → Users créez les utilisateurs suivants :

- William (MdP William) dans le groupe Administration web et rôle admin.
- Rayan (MdP Rayan) dans le groupe Administration réseau et rôle admin.
- Rick (MdP Rick) dans le groupe Administration réseau et rôle Observer.



Vous pouvez également créer un utilisateur avec votre nom et limiter la plage réseau que vous serez autorisé à scanner.



La plage peut-être rédigée comme une seule machine, une plage et son masque ou une adresse de début et une adresse de fin.

- 172.16.21.4
- 172.16.21.0-172.16.21.127
- 172.16.21.128/25

D.4.3 Usage des rôles

Il n'est pas recommandé de créer ses propres rôles (bien que ce soit possible) et il est préférable d'utiliser ceux déjà définis :

- **Admin** : toutes les permissions (notamment la gestion des autres utilisateurs).
- **User** : dispose de toutes les permissions, sauf la gestion des utilisateurs.
- **Observer** : peut accéder à toutes les ressources en lecture seulement.
- **Info** : peut consulter les NVT et informations SCAP. Il peut modifier ses informations de profil.
- **Guest** : identique à Info mais ne peut pas modifier son profil.
- **Monitor** : peut accéder aux données de performances de données.
- **Super Admin** : accède à tout et ne peut être administré via l'interface web.

E Annexes

E.1 Sources

Histoire CVE : https://www.tripwire.com/state-of-security/history-common-vulnerabilities-exposures-cve

Enregistrement CVE : https://cve.mitre.org/cve/identifiers/index.html

Score CVSS : https://www.first.org/cvss/data-representations

Problème Postgresql 15 et 16 : https://stackoverflow.com/questions/67203580/installing-openvas-on-kali-debian-problem-with-postgresql-version

Explications générales : https://www.io-expertises.fr/openvas-audit-de-vulnerabilites/

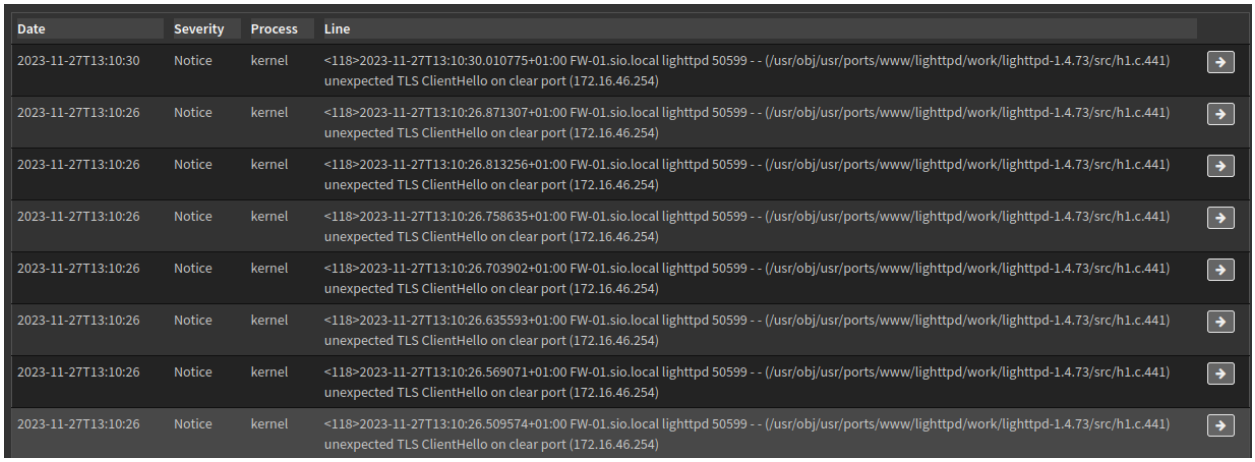
Cours : https://tryhackme.com/room/greenboneappliance

Fonctionnement Kali : https://www.kali.org/tools/gvm/

Installation OpenVAS : https://stacklima.com/installer-openvas-sur-kali-linux/

E.2 Autres

E.2.1 Trace d'attaque depuis un parefeu



Date	Severity	Process	Line
2023-11-27T13:10:30	Notice	kernel	<118>2023-11-27T13:10:30.010775+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.871307+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.813256+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.758635+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.703902+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.635593+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.569071+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)
2023-11-27T13:10:26	Notice	kernel	<118>2023-11-27T13:10:26.509574+01:00 FW-01.sio.local lighttpd 50599 - - (/usr/obj/usr/ports/www/lighttpd/work/lighttpd-1.4.73/src/h1.c.441) unexpected TLS ClientHello on clear port (172.16.46.254)

E.3 Commandes de diagnostic pour kali

Vérifier que GVM écoute sur le port 9392

```
ss -ant | grep:9392
```

E.4 Perte du mot de passe

En cas de perte du mot de passe, il est possible de le réinitialiser avec la commande suivante :

```
gvmd --user=admin --new-password=passwd;
```

E.5 Problème avec pg-gvm

Tenter l'installation séparée du module :

```
sudo apt-get install postgresql-16-pg-gvm
```

Voir bug https://forum.greenbone.net/t/cannot-install-openvas-in-kali-due-to-pg-gvm-extension-error/15796/17

E.6 Architecture technique de Greenbone OpenVAS :

Il y a plusieurs processus actifs dans l'application OpenVAS, voici les liens entre elles :