

## PEINTEST

### 1 – Test de Vulnérabilité

Lancer KALI et ouvrir une console en mode ROOT

**sudo -i** (puis saisir le mot de passe root)

1. Installation du logiciel Libre GVM (Greenbone Vulnerability Manager) ex : OPENVAS (Open source Vulnerability Scanner)

**apt install gvm** (puis répondre Oui = o) ou **apt install openvas**

```
root@kali: ~
Fichier Actions Éditer Vue Aide
(root@kali)-[~]
# apt install openvas
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  greenbone-security-assistant gsad gvm gvm-tools libmicrohttpd12
Les NOUVEAUX paquets suivants seront installés :
  greenbone-security-assistant gsad gvm gvm-tools libmicrohttpd12 openvas
0 mis à jour, 6 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 5 211 ko dans les archives.
Après cette opération, 20,6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive-4.kali.org/kali kali-rolling/non-free amd64 gr
```

Finalisation de l'installation de GVM

**gvm-setup** (attention c'est très long)

Bien noté le compte admin et le mot de passe de la base créer à la fin de l'installation

```
sent 293.549 bytes received 408.191 bytes 280.696,00 bytes/sec
total size is 101.608.703 speedup is 144,80
[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '0ea261b1-6d3d-40ec-b06b-c3826759c92a'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured

(root@kali)-[/bin]
```

Faire un update de gvm

**Gvm-feed-update** (attention c'est un peu long)

Lancement de gvm

**Gvm-start**

# SÉCURITÉ LOGICIEL ET MATÉRIEL

Vérification que gvm fonctionne

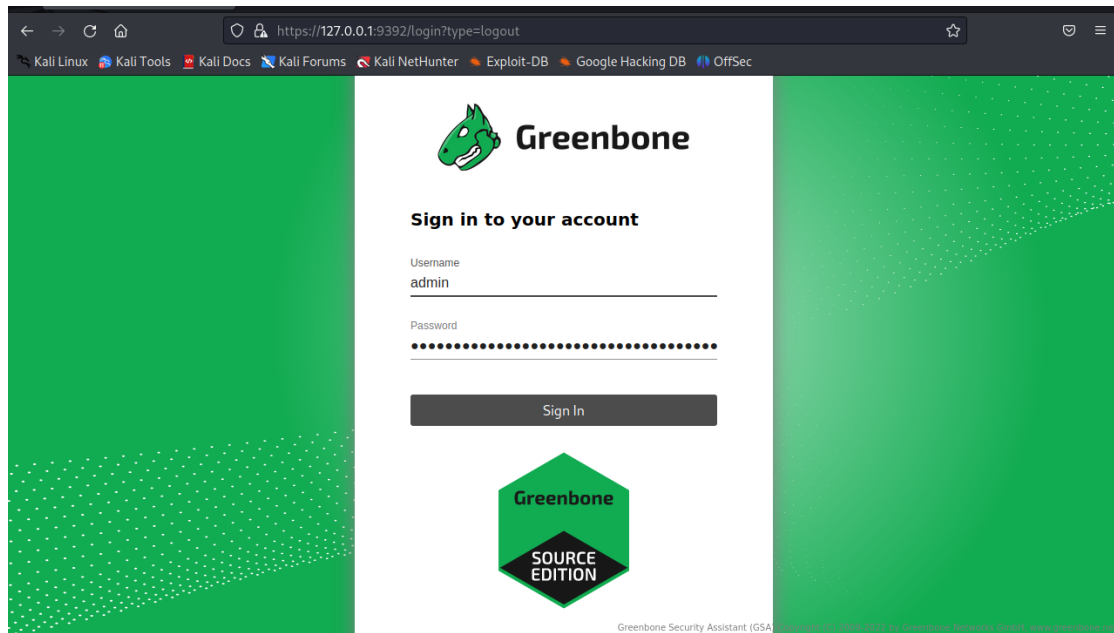
## **gvm-check-setup**

GVM est maintenant fonctionnel.

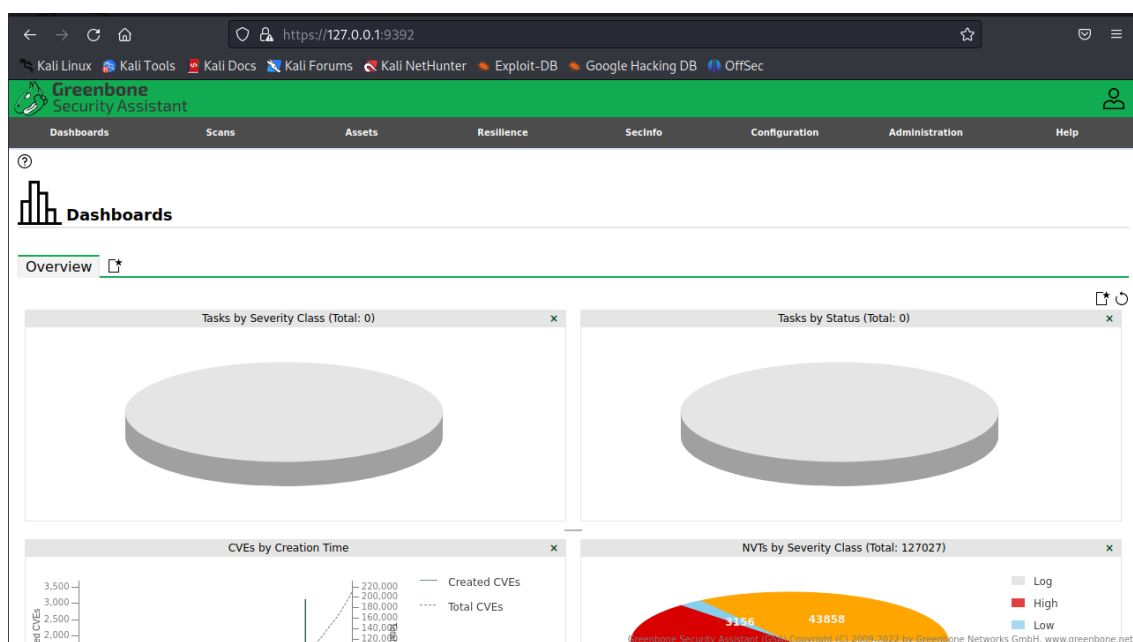
Vous pouvez vous connecter à son interface Web via un navigateur (Firefox) pour kali à l'adresse :

<https://127.0.0.1:9392> il faudra valider le certificat autosigné puis entrer le login admin et le mot de passe

Récupéré dans la phase précédente.



BRAVO vous venez d'installer GVM (anciennement openvas)



# SÉCURITÉ LOGICIEL ET MATÉRIEL

## 2. Analyse de vulnérabilité avec GVM

Création de la machine cible – menu configuration puis TARGET puis new TARGET

The screenshot shows the 'New Target' form in the Greenbone Security Assistant. The form is titled 'New Target' and has a close button 'x'. The fields and their values are:

- Name:** MACHINE-CIBLE
- Comment:** (empty)
- Hosts:** Manual (selected), 192.168.1.51
- Exclude Hosts:** Manual (selected), (empty)
- Allow simultaneous scanning via multiple IPs:** Yes (selected), No (unselected)
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:** SSH (selected), on port 22
- SMB:** (selected)

Red arrows point to the following fields with annotations:

- On nomme la cible (points to Name)
- Puis on ajoute son IP (points to Hosts)
- On choisit le type de protocole (points to Port List)
- On choisit le type de test (points to Alive Test)
- Puis on sauve (points to Save button)

Puis on créer une tache pour lancer l'analyse

On as dans le menu SCAN puis dans le menu TASK puis on créer une nouvelle tache

The screenshot shows the 'New Task' form in the Greenbone Security Assistant. The form is titled 'New Task' and has a close button 'x'. The fields and their values are:

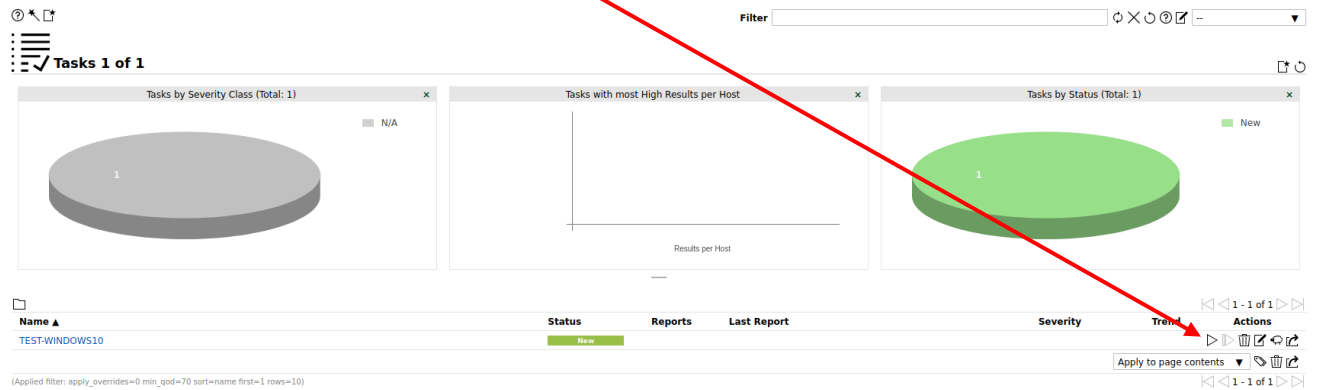
- Name:** TEST-WINDOWS10
- Comment:** (empty)
- Scan Targets:** MACHINE-CIBLE
- Alerts:** (empty)
- Schedule:** --
- Add results to Assets:** Yes (selected), No (unselected)
- Apply Overrides:** Yes (selected), No (unselected)
- Min QoD:** 70
- Alterable Task:** No (selected), Yes (unselected)
- Auto Delete Reports:** Do not automatically delete reports (selected), Automatically delete oldest reports but always keep newest (unselected)
- Scanner:** OpenVAS Default
- Scan Config:** Full and fast

Red arrows point to the following fields with annotations:

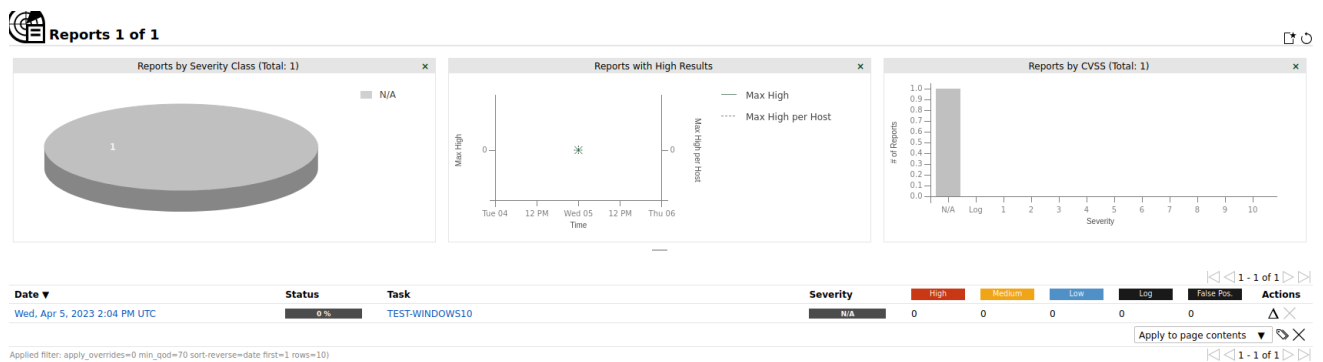
- On donne un nom à la tache (points to Name)
- Puis on choisit la machine cible (points to Scan Targets)
- et on sauve (points to Save button)

# SÉCURITÉ LOGICIEL ET MATÉRIEL

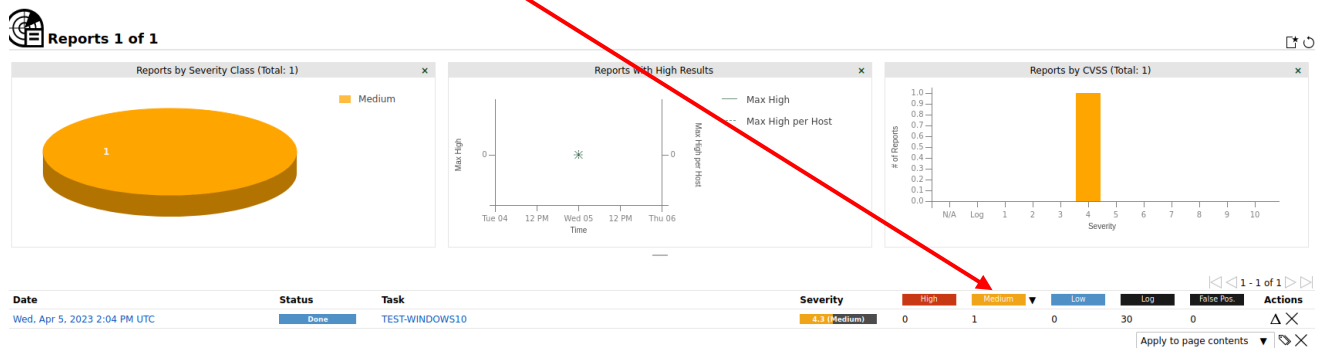
On peut maintenant lancer la tâche d'analyse



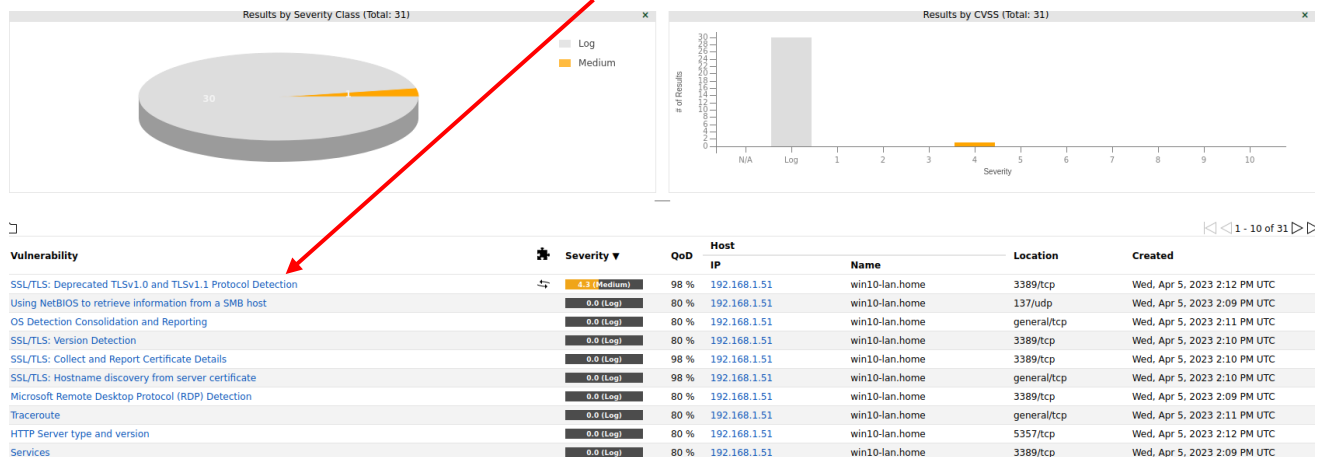
La tâche est en cours ... cela peut être un peu long ... 😊



On a maintenant le résultat de l'analyse, il y a une vulnérabilité médium



Dans le menu Scan et Report on a le détail des logs, pour avoir le détail de la vulnérabilité on click dessus



L'objectif maintenant est de bloquer la vulnérabilité.