SÉCURITÉ LOGICIEL ET MATÉRIEL

PEINTEST

1 – Test de Vulnérabilité

Lancer KALI et ouvrir une console en mode ROOT

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

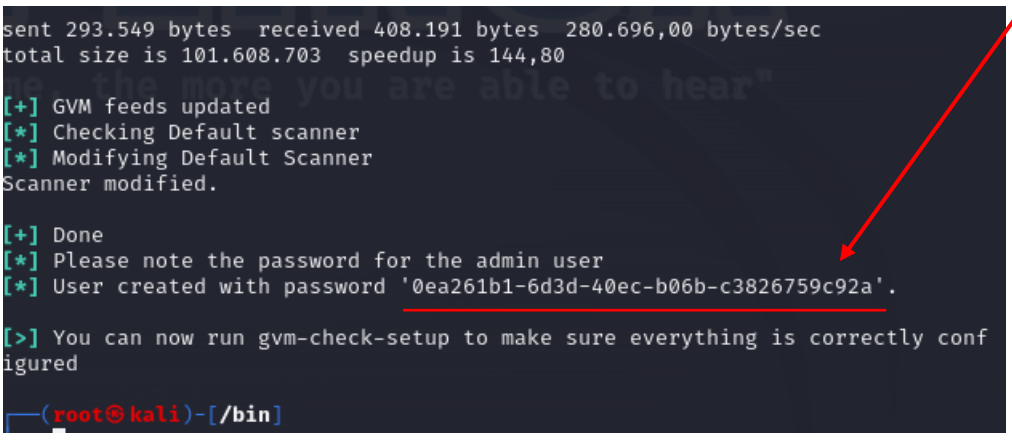
1. Installation du logiciel Libre GVM (Greenbone Vulnerability Manager) ex : OPENVAS (Open source Vulnerability Scanner)

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

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



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

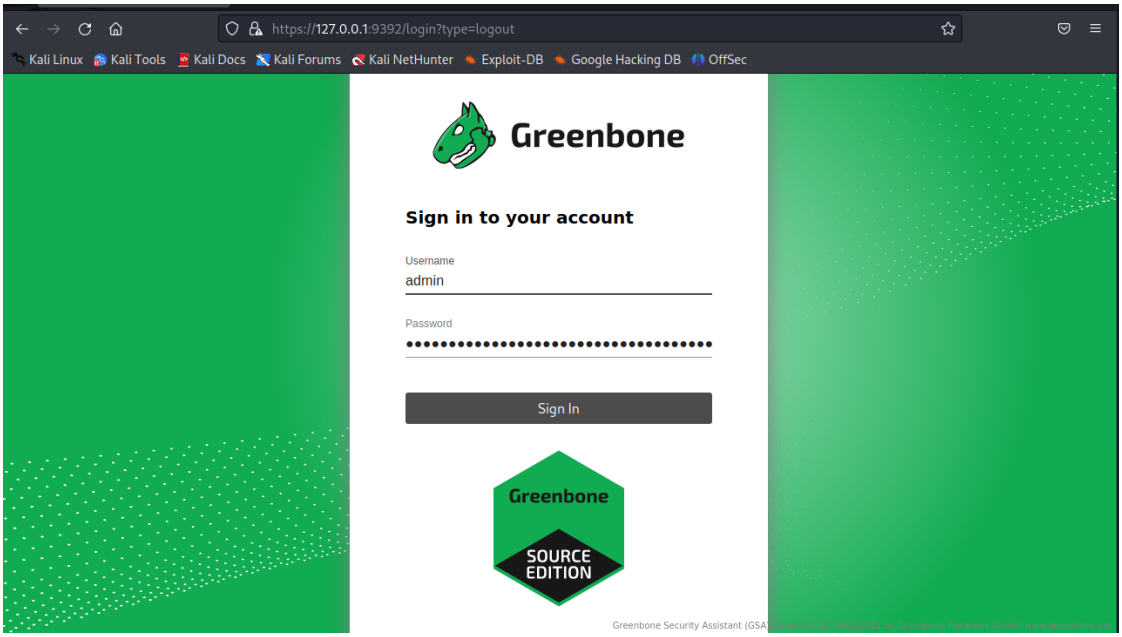
gvm-check-setup

GVM est maintenant fonctionnel.

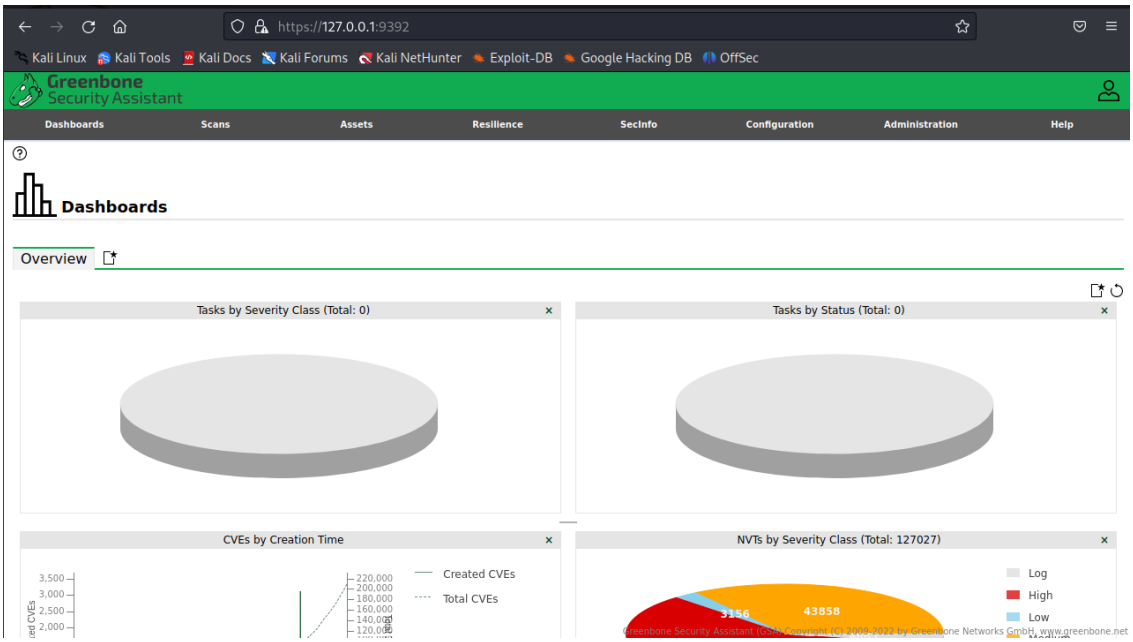
Vous pouvez vous connecter à son interface Web via un navigateur (Firefox) pour kali à l'adresse :

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.

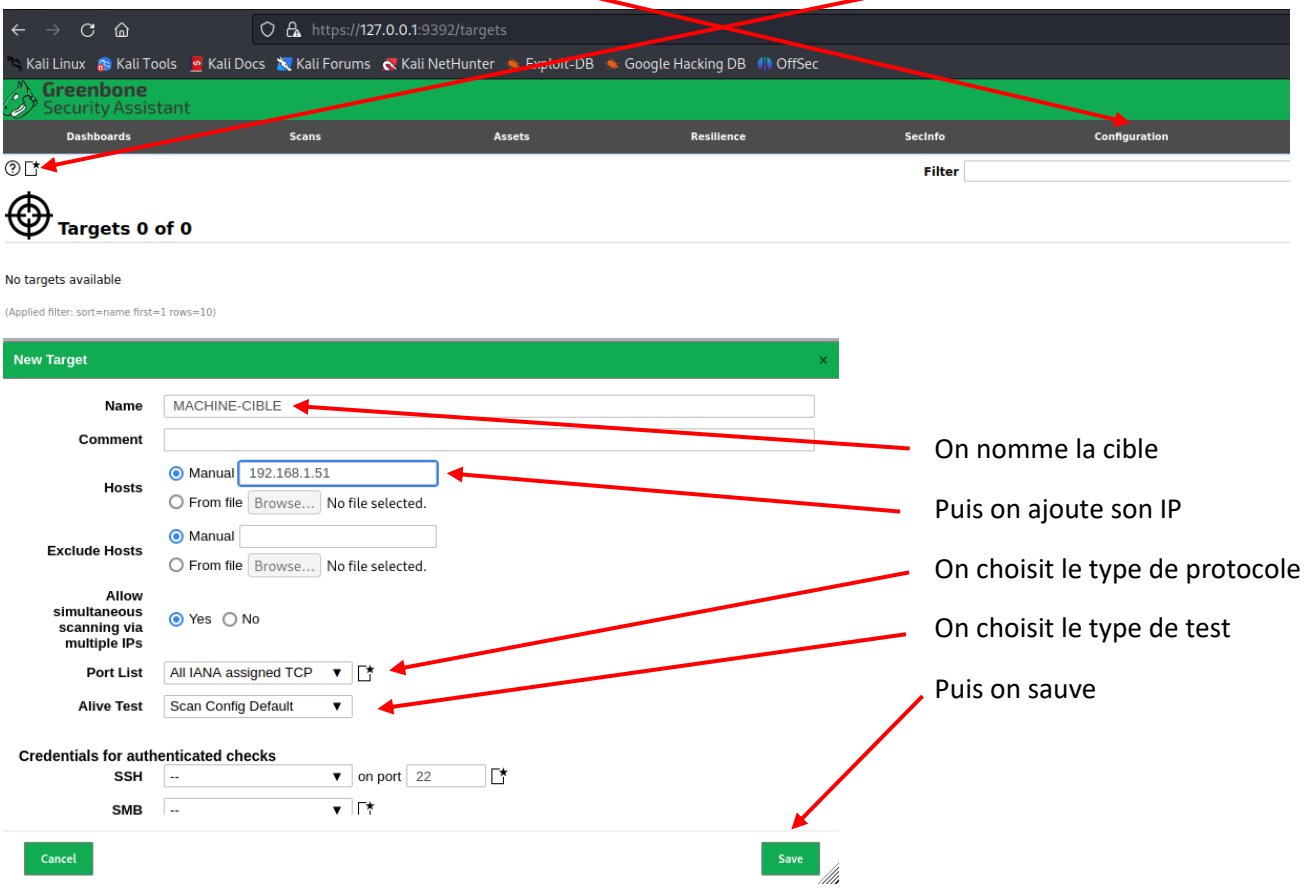


BRAVO vous venez d'installer GVM (anciennement openvas)



2. Analyse de vulnérabilité avec GVM

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



On nomme la cible

Puis on ajoute son IP

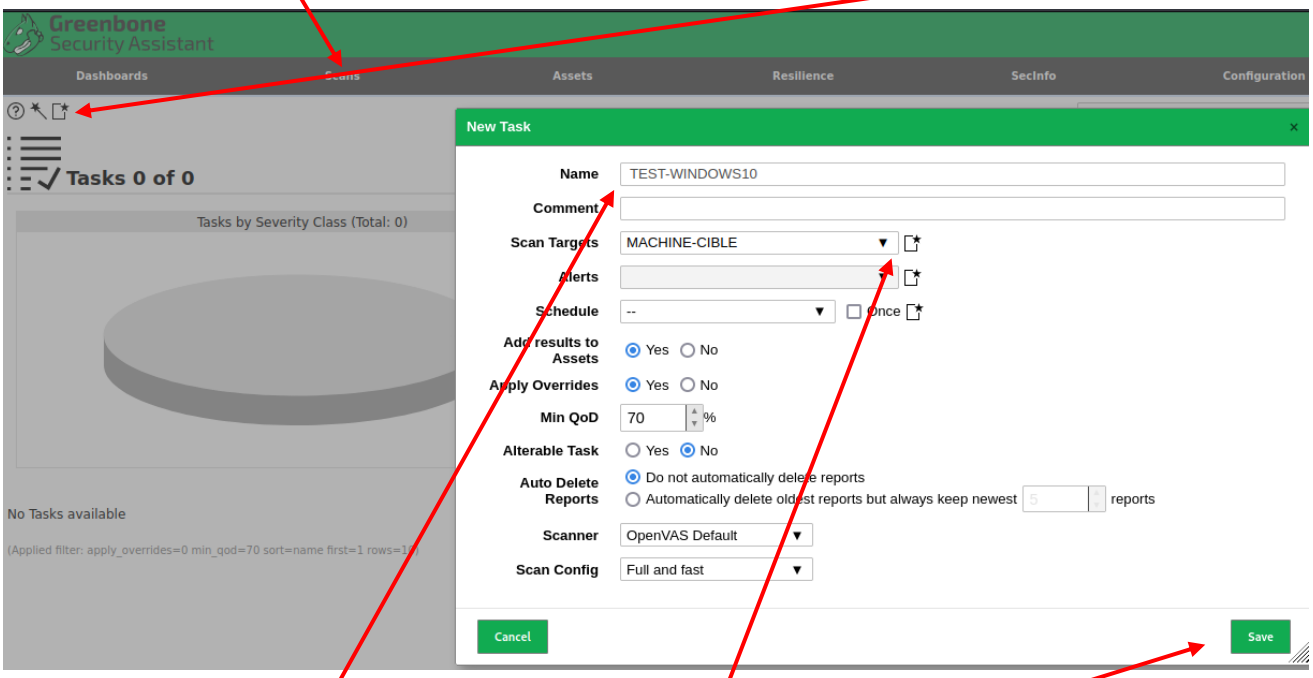
On choisit le type de protocole

On choisit le type de test

Puis on sauve

Puis on créer une tache pour lancer l'analyse

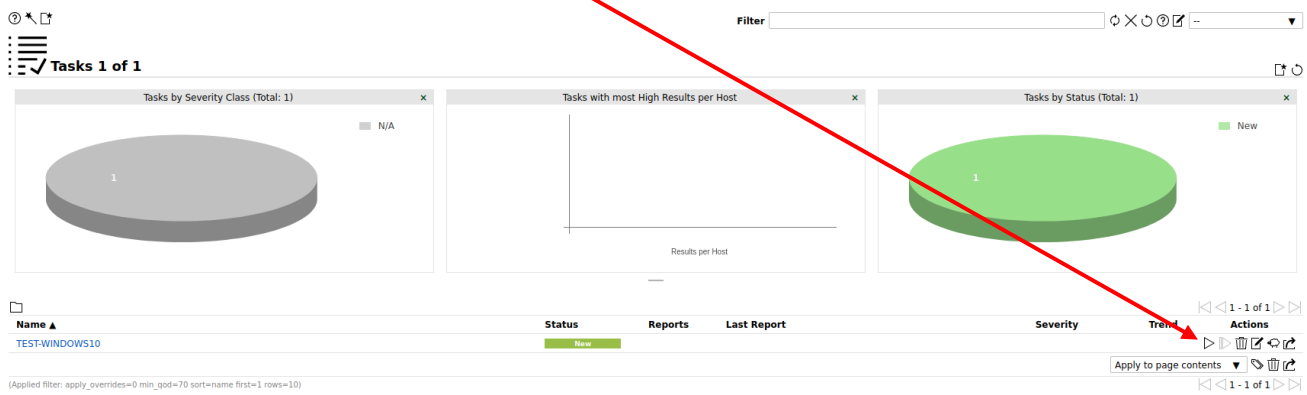
On as dans le menu SCAN puis dans le menu TASK puis on créer une nouvelle tache



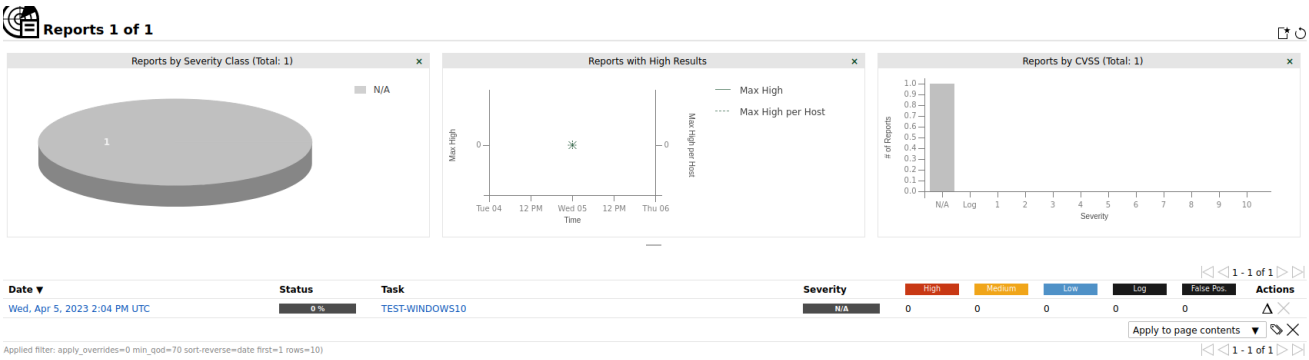
On donne un nom à la tache puis on choisit la machine cible et on sauve

SÉCURITÉ LOGICIEL ET MATÉRIEL

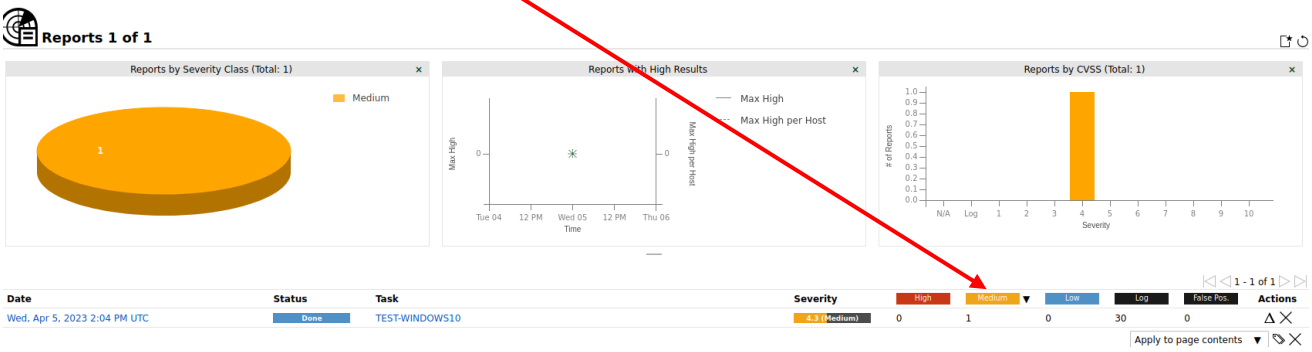
On peut maintenant lancer la tâche d'analyse



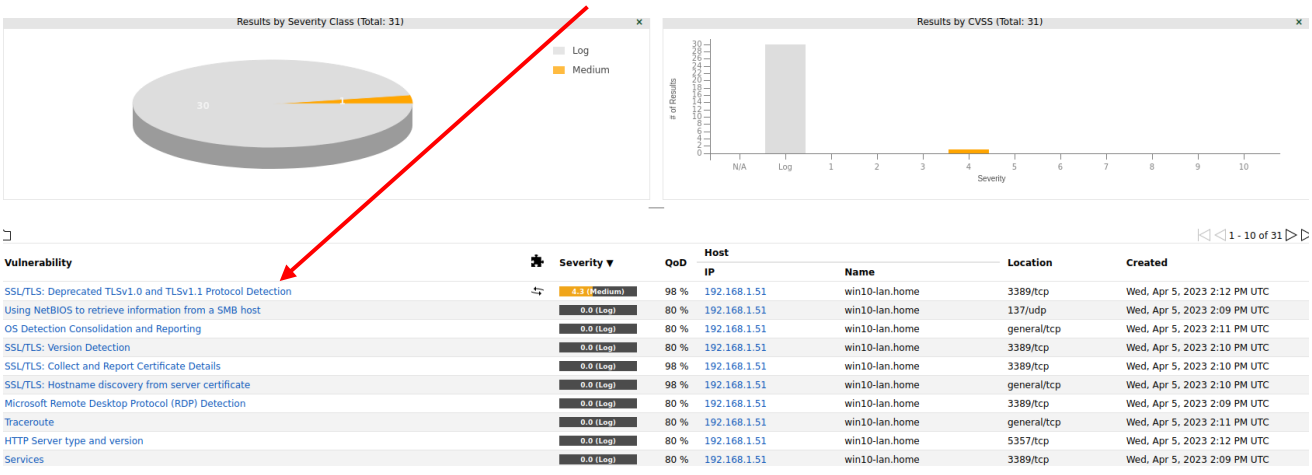
La tâche est en cours … cela peut être un peu long … 😊



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



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.1.51	win10-lan.home	3389/tcp	Wed, Apr 5, 2023 2:12 PM UTC
Using NetBIOS to retrieve information from a SMB host	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	137/udp	Wed, Apr 5, 2023 2:09 PM UTC
OS Detection Consolidation and Reporting	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	general/tcp	Wed, Apr 5, 2023 2:11 PM UTC
SSL/TLS: Version Detection	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	3389/tcp	Wed, Apr 5, 2023 2:10 PM UTC
SSL/TLS: Collect and Report Certificate Details	0.0 (Log)	98 %	192.168.1.51	win10-lan.home	3389/tcp	Wed, Apr 5, 2023 2:10 PM UTC
SSL/TLS: Hostname discovery from server certificate	0.0 (Log)	98 %	192.168.1.51	win10-lan.home	general/tcp	Wed, Apr 5, 2023 2:10 PM UTC
Microsoft Remote Desktop Protocol (RDP) Detection	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	3389/tcp	Wed, Apr 5, 2023 2:09 PM UTC
Traceroute	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	general/tcp	Wed, Apr 5, 2023 2:11 PM UTC
HTTP Server type and version	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	5357/tcp	Wed, Apr 5, 2023 2:12 PM UTC
Services	0.0 (Log)	80 %	192.168.1.51	win10-lan.home	3389/tcp	Wed, Apr 5, 2023 2:09 PM UTC

L'objectif maintenant est de bloquer la vulnérabilité.