OPEN VAS

Open VAS (Open Vulnerability Assessment System) est une solution open-source pour l'analyse de vulnérabilités et la gestion des failles de sécurité. Elle fait partie de la suite **Greenbone Vulnerability Management (GVM)** et est utilisée pour identifier les vulnérabilités sur des systèmes et réseaux.

// Fonctionnalité

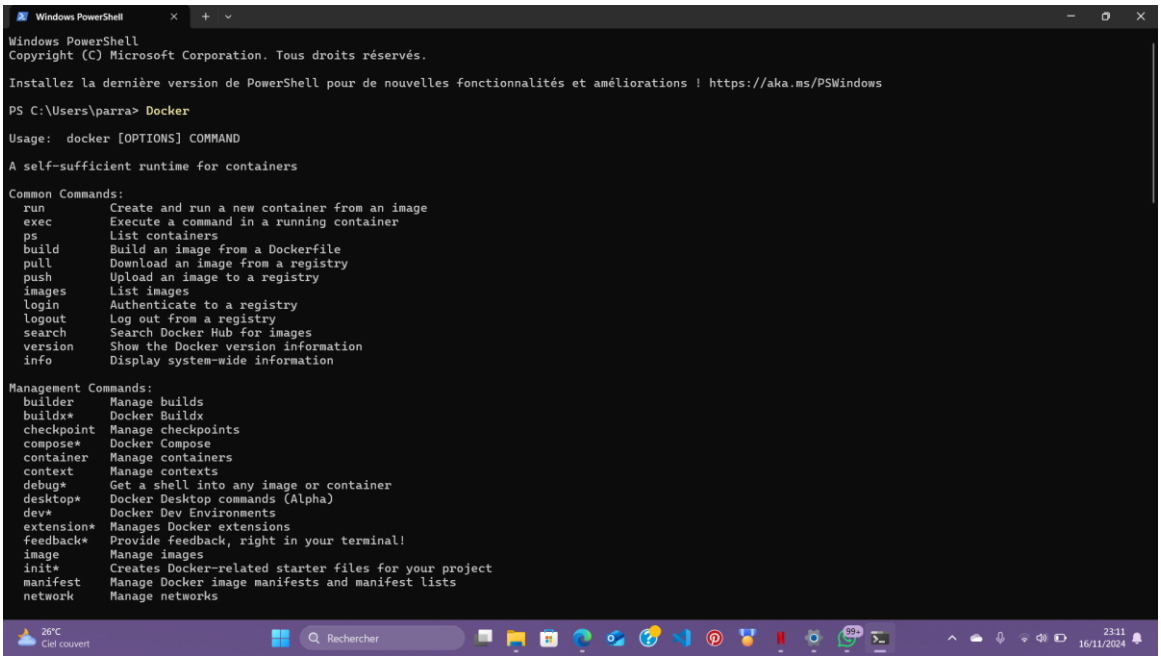
- **Analyse de vulnérabilités** :
- Open VAS scanne les systèmes pour détecter les failles potentielles (comme les logiciels obsolètes, les mauvaises configurations ou les services exposés).
- Il s'appuie sur une base de données de tests (via le *Greenbone Community Feed*) pour identifier les vulnérabilités connues.
- **Prévention des cyberattaques** :
- En identifiant les failles avant qu'elles ne soient exploitées par des attaquants, Open VAS permet de protéger les infrastructures critiques.
- **Audit de sécurité** :
- Les entreprises peuvent l'utiliser pour effectuer des audits réguliers de leurs réseaux et applications, et garantir leur conformité aux normes de sécurité (comme le RGPD ou ISO 27001).
- **Rapports détaillés** :
- Génération de rapports sur les vulnérabilités détectées, avec des recommandations sur la manière de les corriger.
- **Surveillance continue** :
- Permet de surveiller en permanence les réseaux pour repérer rapidement de nouvelles failles ou modifications de la configuration.

1. Télécharger

2. D'abord pour télécharger open vas va falloir ouvrir sa machine virtuelle dans Windows avant toute chose pour pouvoir télécharger normalement . Nous allons utiliser ubuntu pour commencé

3.
4. Ensuite , **Mettre à jour votre système** : Assurer que les paquets de notre système sont à jour.

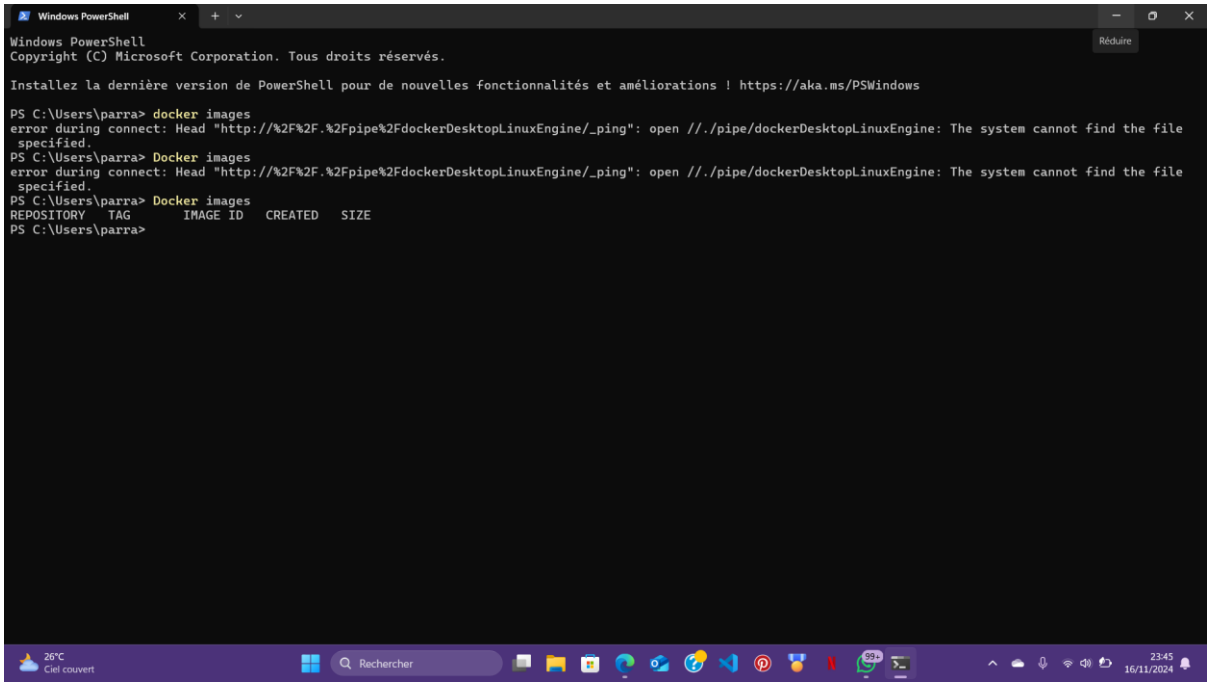
- 3 . i**nstaller Open VAS** : Open VAS fait partie de la suite. Sur Ubuntu, l'installation peut être faite via le gestionnaire de paquets.



- Après le téléchargement nous allons vérifier cela sur notre Power Shell en tapant la commande DOCKER

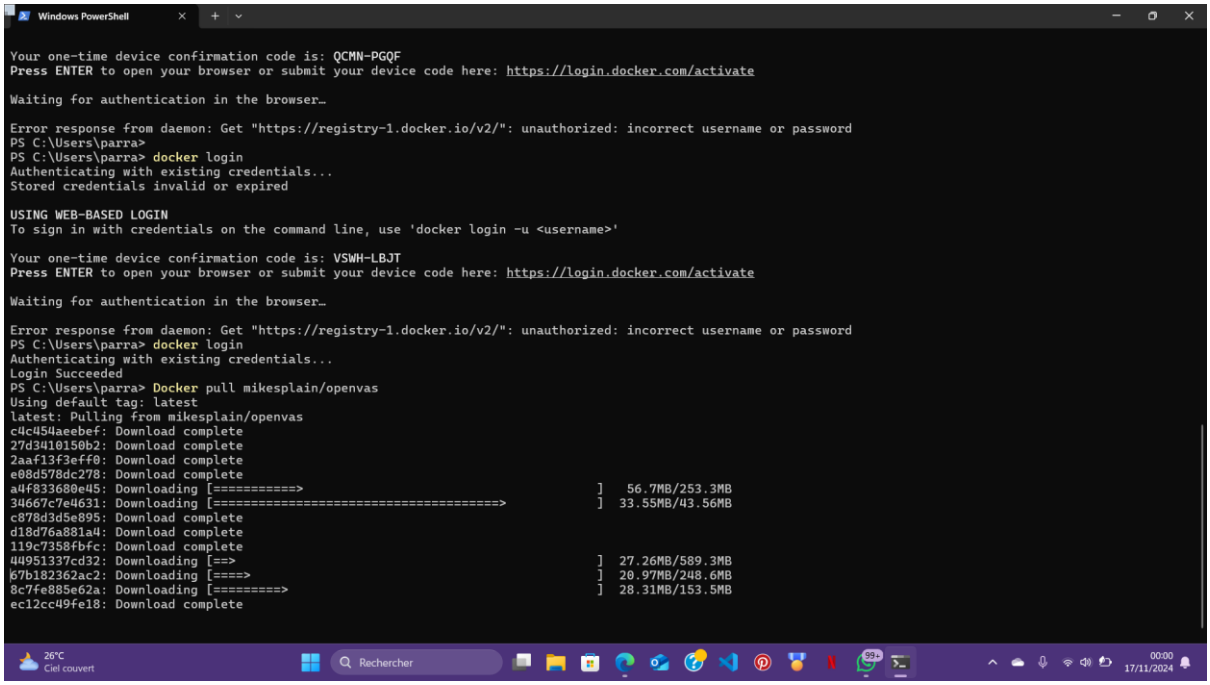
2 -TELECHARGEMENT DE DOCKER IMAGE

Ce telechargement nous permettre de savoir si le setep up a été bien telecharger



Voilà l'image de docker a été bien installé

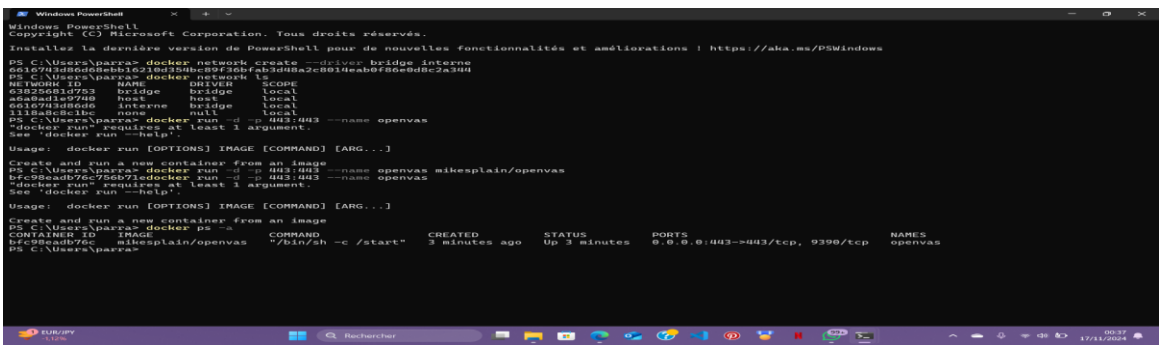
Ensuite nous allons passé tape la commande DOCKER LOGIN cette commande nou permet de verifier si nous avons ouvert un compte dans le DOCKER cela est à verifier dans le email pour pouvoir continuer



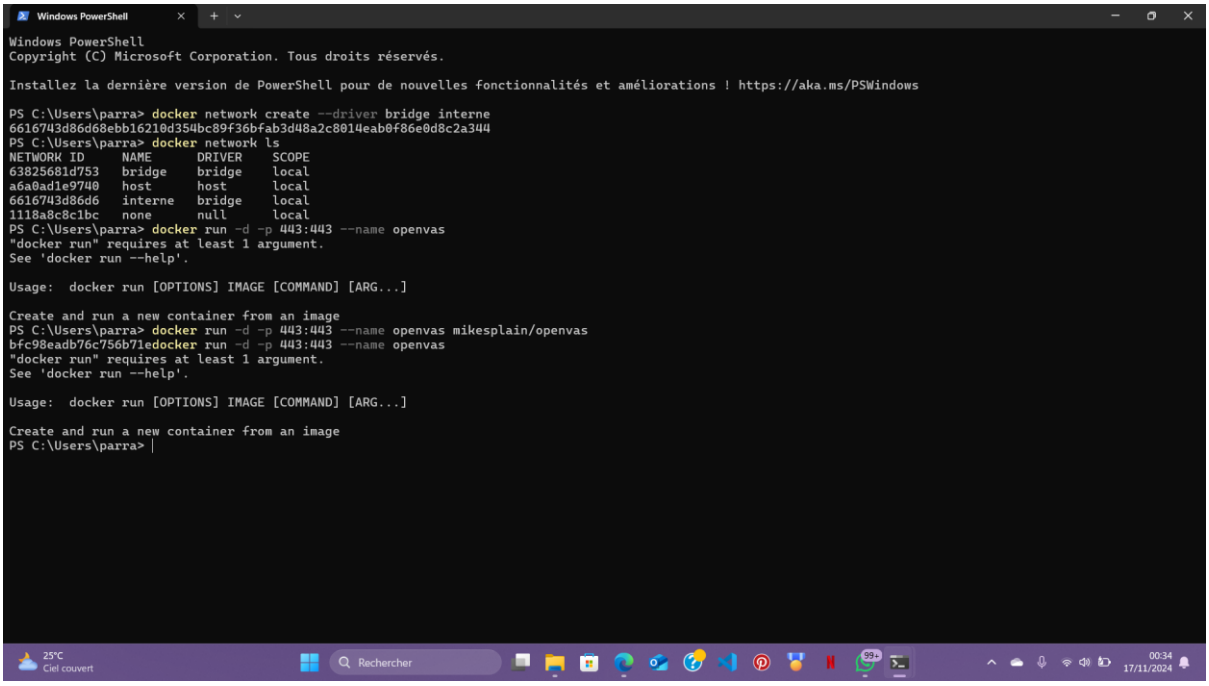
Apres la verification de cela ,nous allons continué avec la commande DOCKER PULLMIKESPLAIN/OPNEVAS La commande **`docker pull mikesplain/openvas:latest`** permet de télécharger une image Docker spécifique depuis un registre Docker (par défaut, Docker Hub). Voici ce qu'elle fait précisément :

C'est une image qui contient une version de **OpenVAS** (Open Vulnerability Assessment System), un outil open-source utilisé pour effectuer des analyses de vulnérabilités sur des systèmes informatiques.

UTILISATION DE POWER SHELL

1. Utilisation de Docker network create --driver bridge interne
    1. Cette commande crée un nouveau réseau Docker nommé **`interne`**.
    2. Les conteneurs attachés à ce réseau pourront communiquer entre eux directement en utilisant leurs noms ou adresses IP.
    3. Les conteneurs ne seront pas accessibles depuis l'extérieur, sauf si des ports sont explicitement exposés.
4. 

5. **docker run -d -p 443:443 --name open vas**

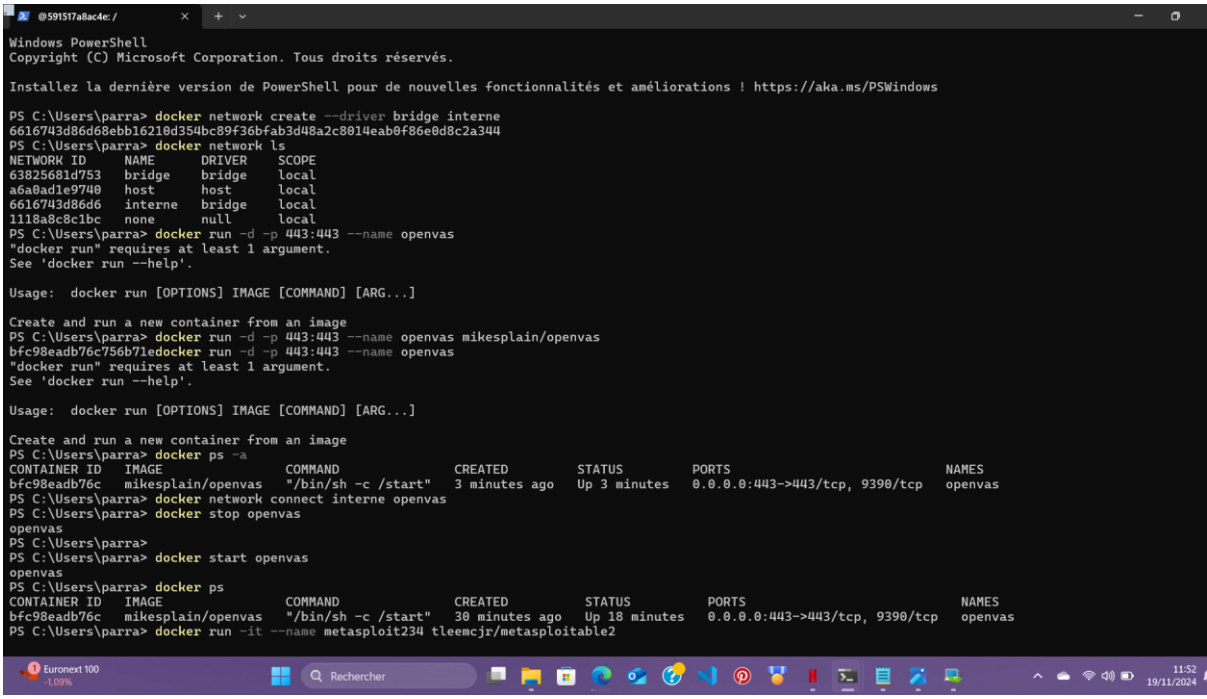


Téléchargement et Exécution :

- Si l'image Docker **`mikesplain/openvas`** n'est pas encore présente sur votre machine, elle sera automatiquement téléchargée depuis Docker Hub.
- Un conteneur basé sur cette image sera ensuite lancé.
  `-p 443:443` : Mappe le port **443** (HTTPS) de l'hôte au port **443** du conteneur, permettant d'accéder à l'interface web d'OpenVAS via HTTPS.

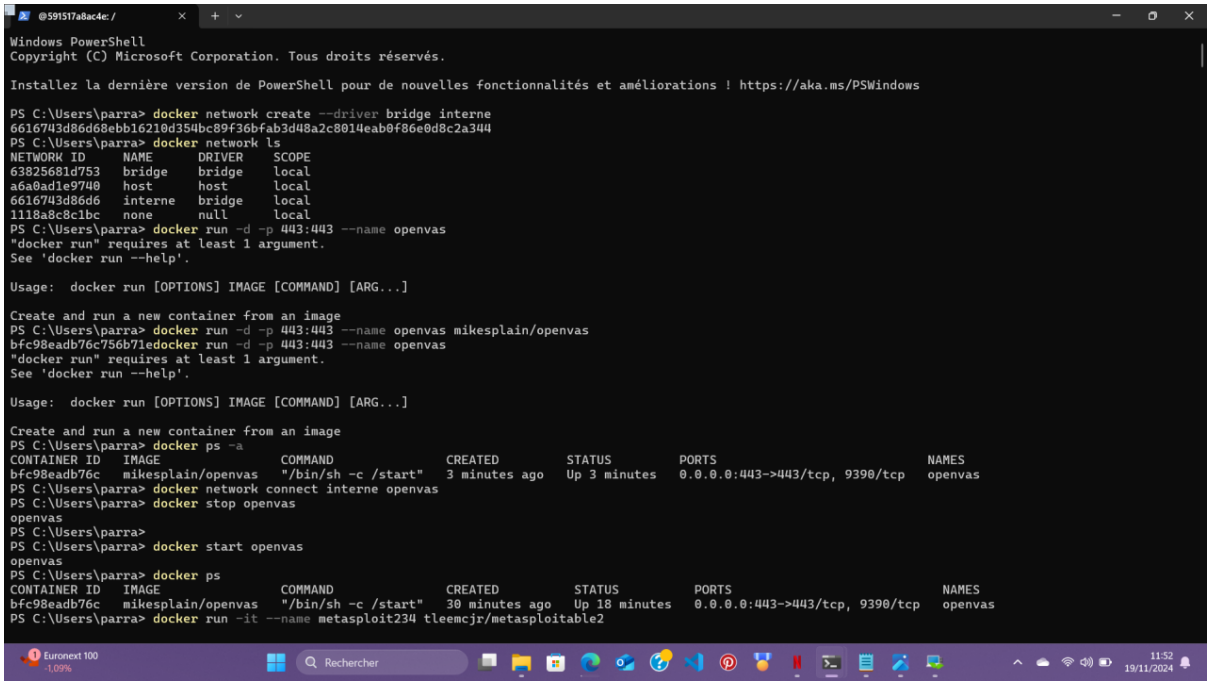
  - **Docker network connect interne open vas**
    Cette commande connecte un conteneur Docker existant (**`openvas`**) à un réseau Docker existant (**`interne`**). Cela permet au conteneur **`openvas`** de communiquer avec d'autres conteneurs attachés au même réseau

interne.



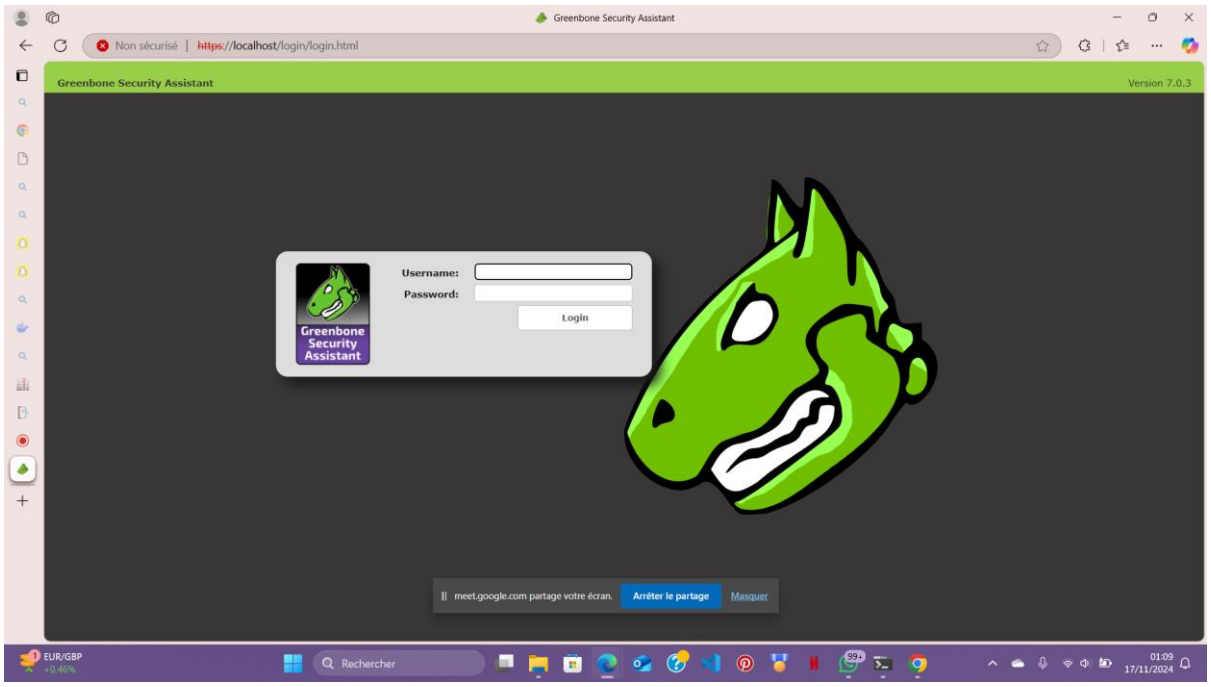
1. **Docker run -it --name metasploit234 tleemcjr/metasploitable2**

- **-it** : Lance le conteneur en mode interactif avec un terminal attaché, vous permettant d'interagir directement avec le système à l'intérieur du conteneur.
- **--name metasploit234** : Attribue un nom personnalisé (**metasploit234**) au conteneur pour faciliter son identification.
- **tleemcjr/metasploitable2** : Spécifie l'image Docker à utiliser, qui correspond à un système vulnérable conçu pour des tests de sécurité.



|| GREEN BONE ASSISTANT SECURITY

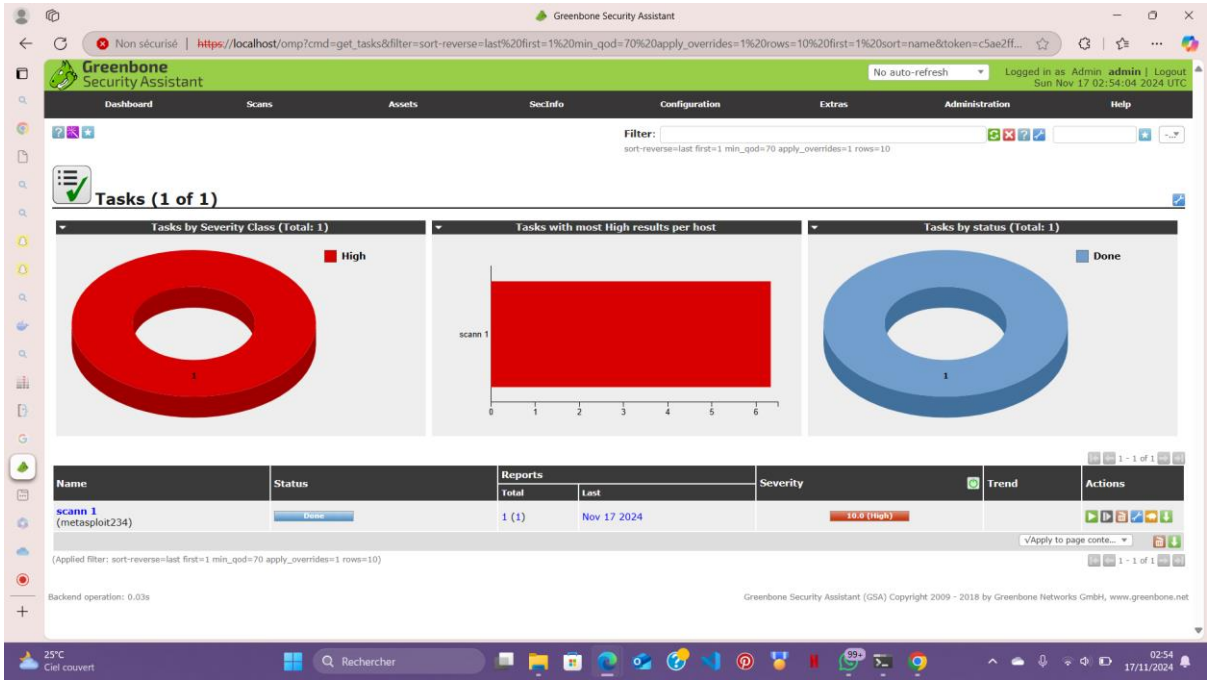
A



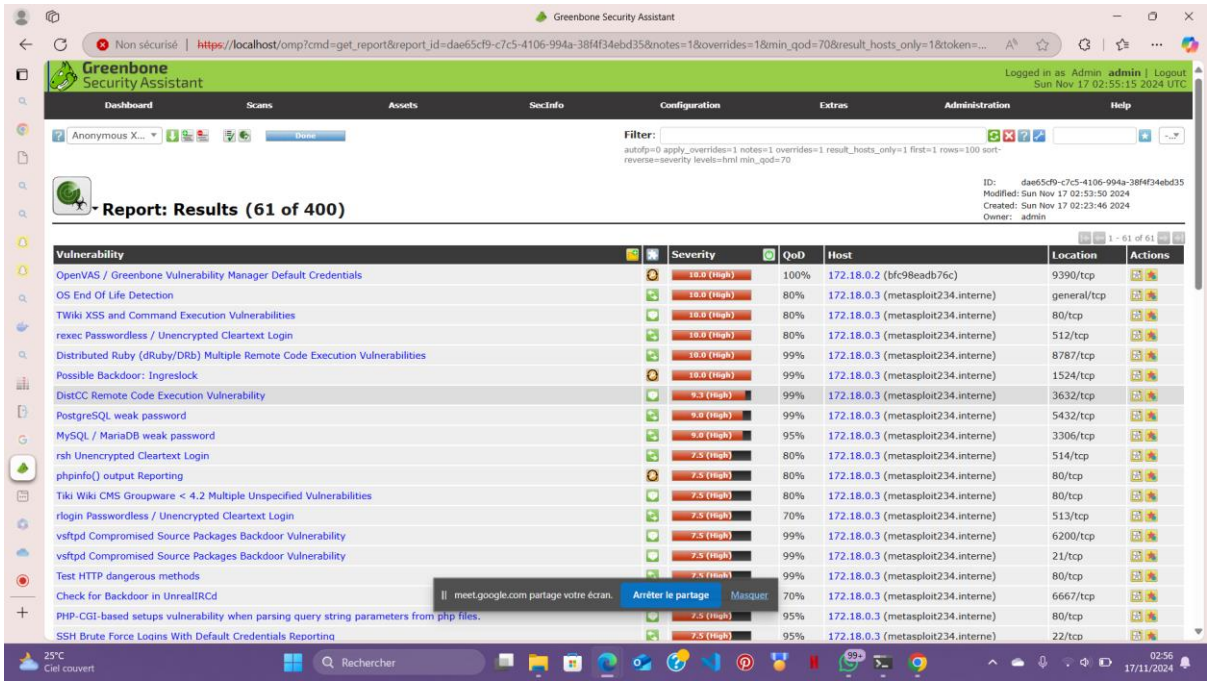
Apres avoir mis notre localhost c’est à dire l’adresse du ip site

On va tape cette commande dans le web sa depend du navigateur qui est à votre disposition

||| TESTE


Greenbone Security Assistant
Non sécurisé | https://localhost/omp?cmd=get_tasks&filter=sort-reverse=last%20first=1%20min_qod=70%20apply_overrides=1%20rows=10%20first=1%20sort=name&token=c5ae2ff...
Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sun Nov 17 02:54:04 2024 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
sort-reverse=last first=1 min_qod=70 apply_overrides=1 rows=10
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
Tasks with most High results per host
scann 1
Tasks by status (Total: 1)
Done
Name
Status
Reports
Total
Last
Severity
Trend
Actions
scann 1
(metasploit234)
Done
1 (1)
Nov 17 2024
10.0 (High)
(Applied filter: sort-reverse=last first=1 min_qod=70 apply_overrides=1 rows=10)
Backend operation: 0.03s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
25°C
Ciel couvert
Rechercher
02:54
17/11/2024

|V/ VULNÉRABILITÉS



V/REGARDER LES DIFFÉRENTS CAS DÉTECTE