

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.

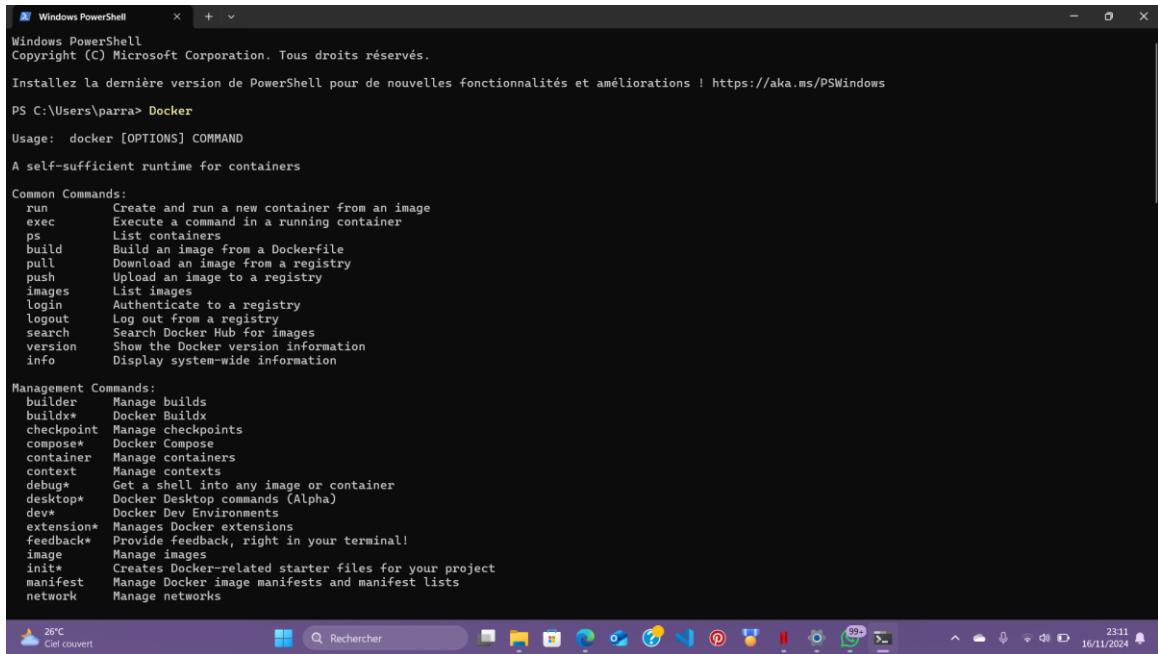
// Fonctionnalité

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



```

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\parra> Docker
Usage: docker [OPTIONS] COMMAND
      A self-sufficient runtime for containers

Common Commands:
  run           Create and run a new container from an image
  exec          Execute a command in a running container
  ps            List containers
  build         Build an image from a Dockerfile
  pull          Download an image from a registry
  push          Upload an image to a registry
  images        List images
  login         Authenticate to a registry
  logout        Log out from a registry
  search        Search Docker Hub for images
  version       Show the Docker version information
  info          Display system-wide information

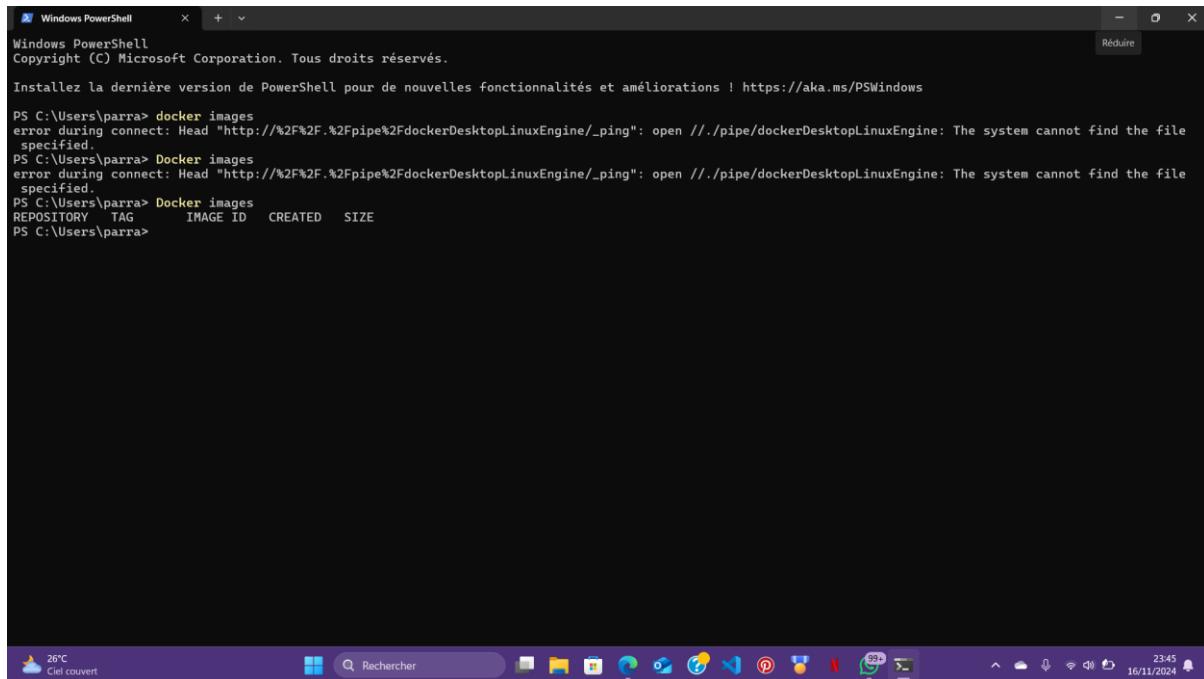
Management Commands:
  builder       Manage builds
  buildx*       Docker Buildx
  checkpoint*   Manage checkpoints
  compose*      Docker Compose
  container*    Manage containers
  context*      Manage contexts
  debug*        Get a shell into any image or container
  desktop*     Docker Desktop commands (Alpha)
  dev*          Docker Dev Environments
  extension*   Manages Docker extensions
  feedback*    Provide feedback, right in your terminal!
  image         Manage images
  init*        Creates Docker-related starter files for your project
  manifest*   Manage Docker image manifests and manifest lists
  network*    Manage networks

```

- 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



```

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\parra> docker images
error during connect: Head "http:///%2F%2Fpipe%2FdockerDesktopLinuxEngine/_ping": open //./pipe/dockerDesktopLinuxEngine: The system cannot find the file specified.
PS C:\Users\parra> Docker images
error during connect: Head "http:///%2F%2Fpipe%2FdockerDesktopLinuxEngine/_ping": open //./pipe/dockerDesktopLinuxEngine: The system cannot find the file specified.
PS C:\Users\parra> Docker images
REPOSITORY TAG      IMAGE ID      CREATED     SIZE
PS C:\Users\parra>

```

Voilà l'image de docker a été bien installé

Ensuite nous allons passé tape la commande [DOCKER LOGIN](#) cette commande nous permet de vérifier si nous avons ouvert un compte dans le DOCKER cela est à vérifier dans le email pour pouvoir continuer

```
Windows PowerShell x + - 00:00 17/11/2024

Your one-time device confirmation code is: QCMMN-PGQF
Press ENTER to open your browser or submit your device code here: https://login.docker.com/activate

Waiting for authentication in the browser...

Error response from daemon: Get "https://registry-1.docker.io/v2/": unauthorized: incorrect username or password
PS C:\Users\parra>
PS C:\Users\parra> docker login
Authenticating with existing credentials...
Stored credentials invalid or expired

USING WEB-BASED LOGIN
To sign in with credentials on the command line, use 'docker login -u <username>'

Your one-time device confirmation code is: VSWH-LBJT
Press ENTER to open your browser or submit your device code here: https://login.docker.com/activate

Waiting for authentication in the browser...

Error response from daemon: Get "https://registry-1.docker.io/v2/": unauthorized: incorrect username or password
PS C:\Users\parra> docker login
Authenticating with existing credentials...
Login Succeeded
PS C:\Users\parra> Docker pull mikesplain/openvas
Using default tag: latest
latest: Pulling from mikesplain/openvas
c4c454aeeebef: Download complete
27d3410150b2: Download complete
2aaaf12f3e9ff0: Download complete
e88d578dc278: Download complete
a4f833680e45: Downloading [=====] 56.7MB/253.3MB
34667c7e4631: Downloading [=====] 33.55MB/43.56MB
c878d3d5e895: Download complete
d18d76a881a4: Download complete
119c7358fbfc: Download complete
44951337c32: Downloading [==>] 27.26MB/589.3MB
67b182362ac2: Downloading [=-->] 20.97MB/248.6MB
8c7fe885e62a: Downloading [=====] 28.31MB/153.5MB
ec12cc49fe18: Download complete

Ciel couvert 26°C
```

Après la vérification de cela, nous allons continuer avec la commande **DOCKER PULL MIKESPLAIN/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

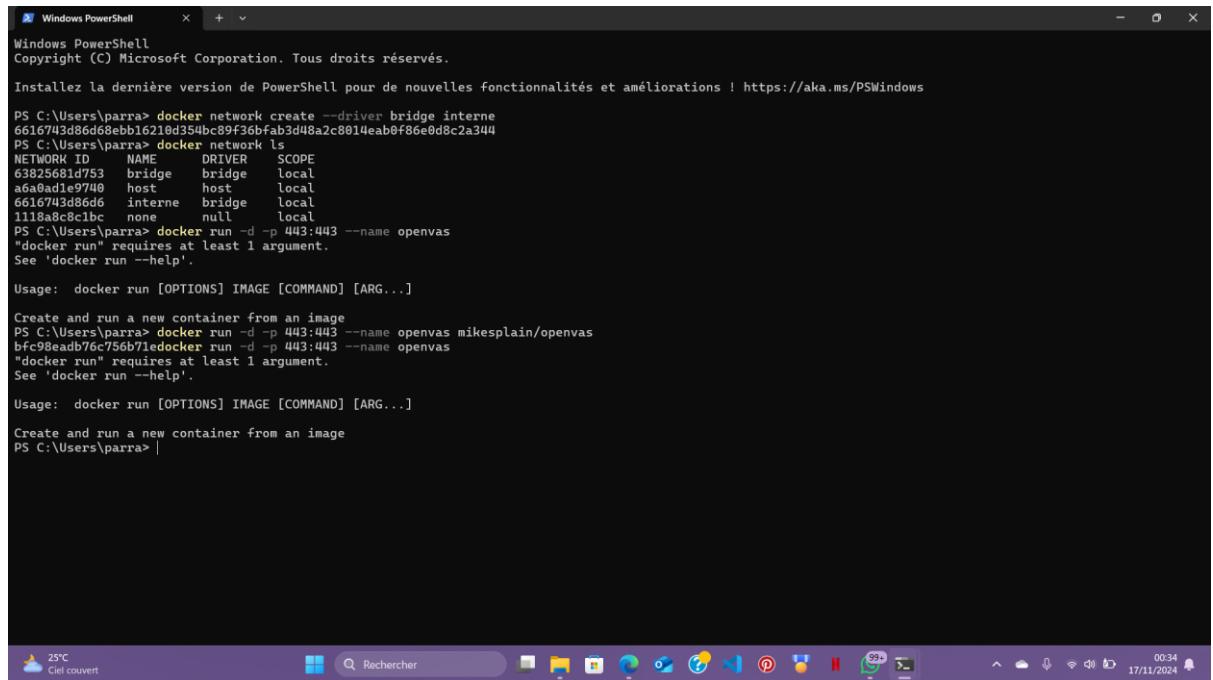
1. Utilisation de Docker network create --driver bridge interne
 1. Cette commande crée un nouveau réseau Docker nommé **interne**.
 2. Les conteneurs attachés à ce réseau pourront communiquer entre eux directement en utilisant leurs noms ou adresses IP.
 3. Les conteneurs ne seront pas accessibles depuis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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations : https://aka.ms/PSWindows

PS C:\Users\parra>\ docker network create --driver bridge interne
PS C:\Users\parra>\ docker network ls
  NAME    ID
  bridge  e8d014eab0e6db2ca2d94
  host    53825681d753
  interne 616174d3d6de
  none   5306f9a8a6c8
PS C:\Users\parra>\ docker run -d -p 443:443 --name openvas
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]
Create and run a new container from an image
Usage: docker run -d -p 443:443 --name openvas mikesplain/openvas
See 'docker run --help'.
PS C:\Users\parra>\ docker run -d -p 443:443 --name openvas
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]
Create and run a new container from an image
Usage: docker run -d -p 443:443 --name openvas mikesplain/openvas
See 'docker run --help'.
PS C:\Users\parra>\ docker run -d -p 443:443 --name openvas
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS              NAMES
openvas            mikesplain/openvas   "/bin/sh -c /start"   3 minutes ago   Up 3 minutes   0.0.0.0:443->443/tcp, 9390/tcp   openvas
PS C:\Users\parra\
```

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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\parra> docker network create --driver bridge interne
6616743d86d68bb16210d354bc89f36bfab3d48a2c8014eab0f86e0d8c2a344
PS C:\Users\parra> docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
63825681d753    bridge    bridge      local
a6a8ad1e9740    host      host       local
6616743d86d6    interne   bridge      local
1118a8c8c1bc    none     null       local
PS C:\Users\parra> docker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> docker run -d -p 443:443 --name openvas mikesplain/openvas
bfc98eadb76c756b71edocker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

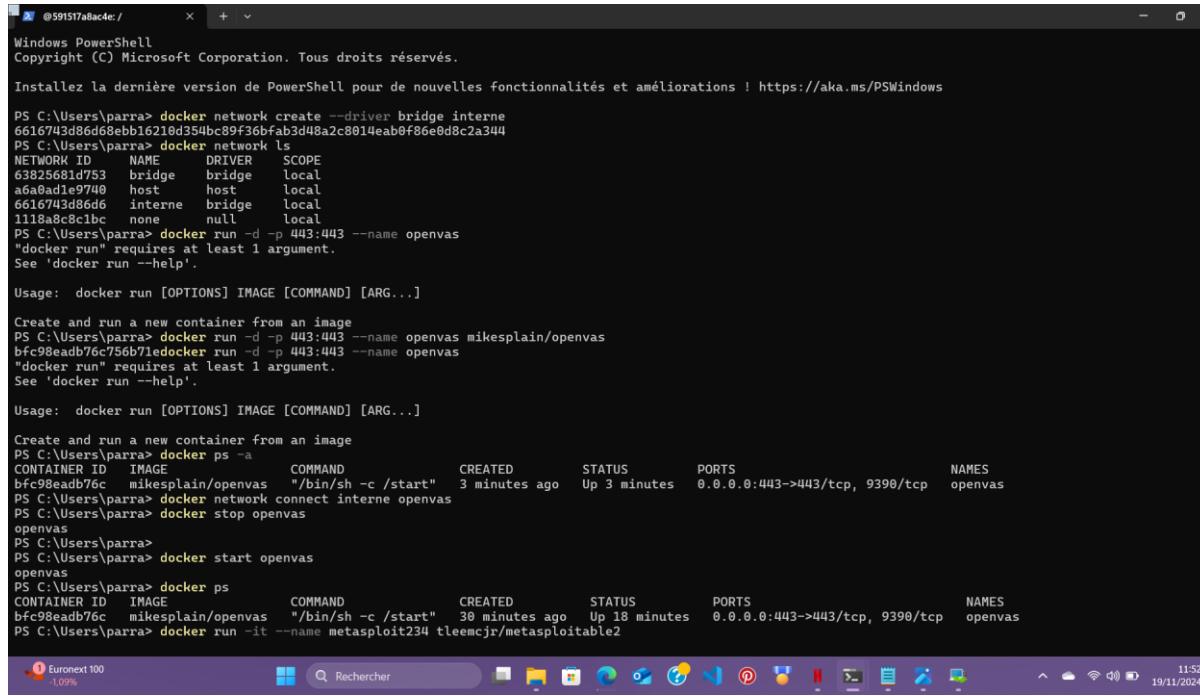
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> |
```

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.



```
PS C:\Users\parra> docker network create --driver bridge interne
6616743d86d68eb16210d354bc89f36fab3d48a2c8014eab0f86e0d8c2a344
PS C:\Users\parra> docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
63825681d753   bridge    bridge      local
a6a0ad1e9740   host      host      local
6616743d86d6   interne   bridge      local
1118a8c8c1bc   none     null      local
PS C:\Users\parra> docker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> docker run -d -p 443:443 --name openvas mikesplain/openvas
bfc98eadb76c756b71edocker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> docker ps -a
CONTAINER ID      IMAGE      COMMAND      CREATED      STATUS      PORTS      NAMES
bfc98eadb76c    mikesplain/openvas  "/bin/sh -c /start"  3 minutes ago  Up 3 minutes  0.0.0.0:443->443/tcp, 9390/tcp  openvas
PS C:\Users\parra> docker network connect interne openvas
PS C:\Users\parra> docker stop openvas
openvas
PS C:\Users\parra>
PS C:\Users\parra> docker start openvas
openvas
PS C:\Users\parra> docker ps
CONTAINER ID      IMAGE      COMMAND      CREATED      STATUS      PORTS      NAMES
bfc98eadb76c    mikesplain/openvas  "/bin/sh -c /start"  30 minutes ago  Up 18 minutes  0.0.0.0:443->443/tcp, 9390/tcp  openvas
PS C:\Users\parra> docker run -it --name metasploit234 tleemcjr/metasploitable2
```

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.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\parra> docker network create --driver bridge interne
6616743d86d68eb16210d354bc89f36fab3d48a2c8014eab0f86e0d8c2a344
PS C:\Users\parra> docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
63825681d753    bridge    bridge      local
a6a0ad1e9740    host      host      local
6616743d86d6    interne   bridge      local
1118a8c8c1bc    none     null      local
PS C:\Users\parra> docker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> docker run -d -p 443:443 --name openvas mikesplain/openvas
bfc98eadb76c756b71edocker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

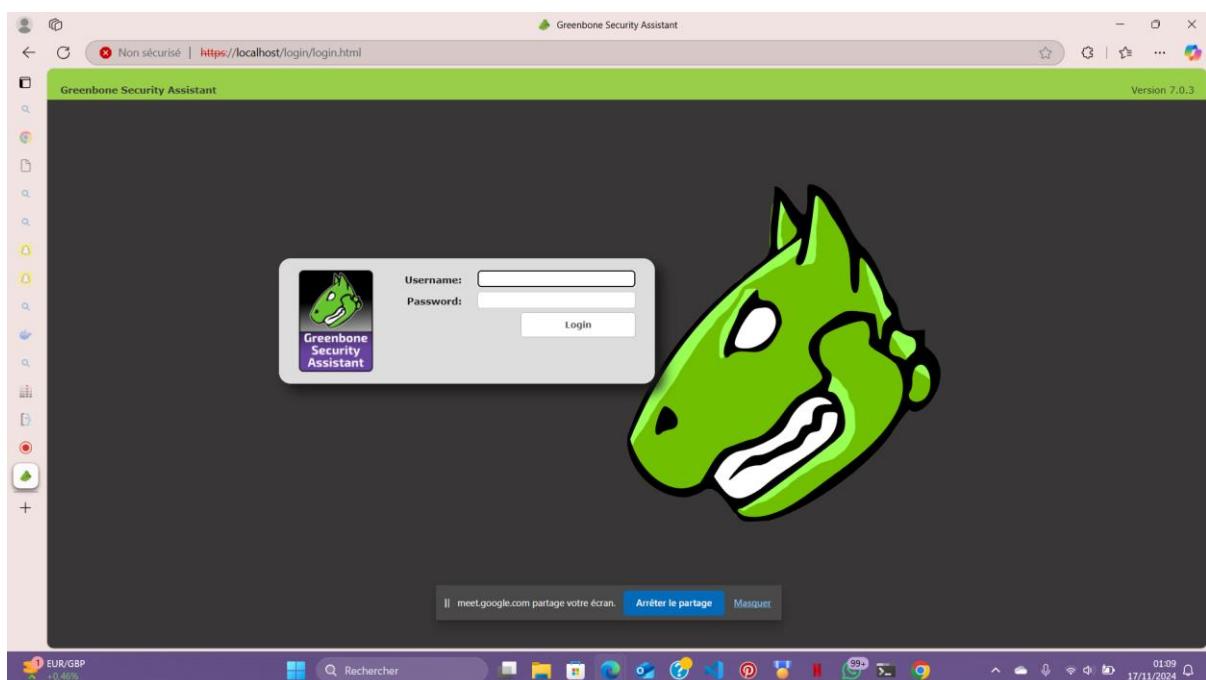
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parra> docker ps -a
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
bfc98eadb76c        mikesplain/openvas   "/bin/sh -c /start"   3 minutes ago    Up 3 minutes      0.0.0.0:443->443/tcp, 9390/tcp   openvas
PS C:\Users\parra> docker network connect interne openvas
openvas
PS C:\Users\parra>
PS C:\Users\parra> docker stop openvas
openvas
PS C:\Users\parra> docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
bfc98eadb76c        mikesplain/openvas   "/bin/sh -c /start"   30 minutes ago   Up 18 minutes     0.0.0.0:443->443/tcp, 9390/tcp   openvas
PS C:\Users\parra> docker run -it --name metasploit234 tleemcjr/metasploitable2

```

|| 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

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...

Logged in as Admin admin | Logout Sun Nov 17 02:54:04 2024 UTC

Greenbone Security Assistant

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

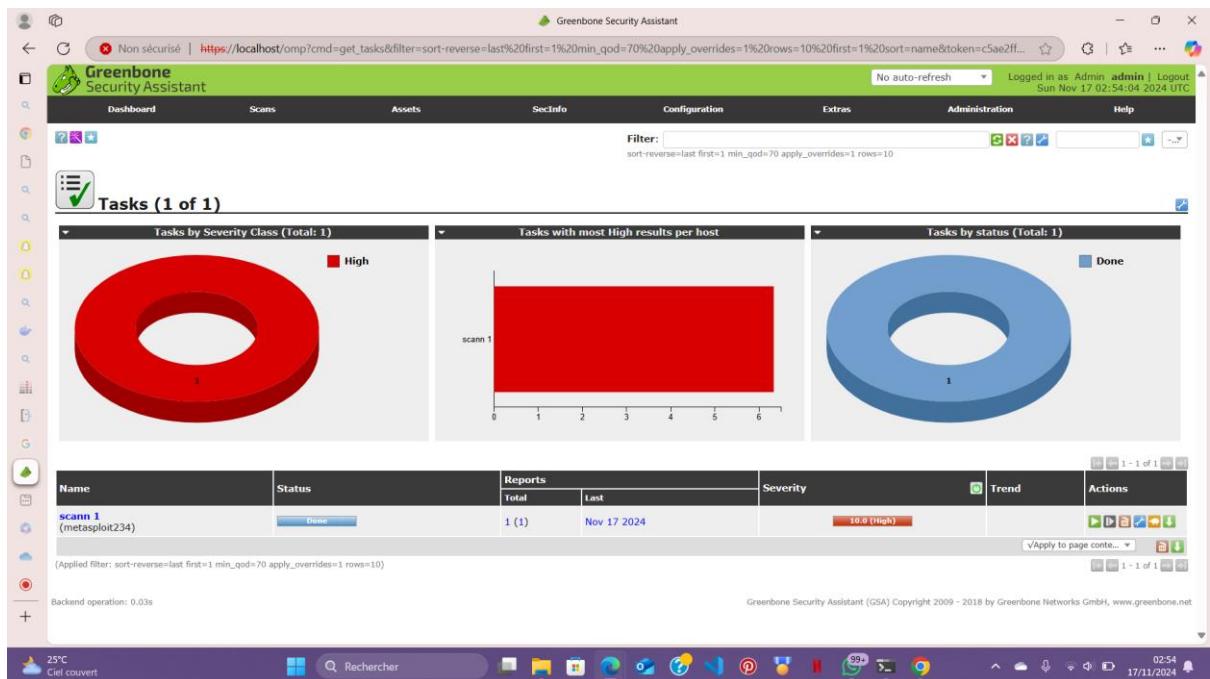
Name	Status	Reports	Severity	Trend	Actions
scann 1 (metasploit234)	Done	1 (1)	Nov 17 2024	10.0 (High)	

(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 02:54 17/11/2024



IV/ VULNÉRABILITÉS

The screenshot shows the Greenbone Security Assistant interface with a list of detected vulnerabilities. The table includes columns for Severity (e.g., 10.0 (High), 9.0 (High)), QoD (Quality of Detection), Host (IP address like 172.18.0.2 or 172.18.0.3), Location (TCP port like 9390/tcp or 80/tcp), and Actions (button icons). The list includes various types of vulnerabilities such as OpenVAS / Greenbone Vulnerability Manager Default Credentials, OS End Of Life Detection, TWiki XSS and Command Execution Vulnerabilities, and vsftpd Compromised Source Packages Backdoor Vulnerability.

Vulnerability	Severity	QoD	Host	Location	Actions			
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	172.18.0.2 (bfc98eadb76c)	9390/tcp				
OS End Of Life Detection	10.0 (High)	80%	172.18.0.3 (metasploit234.interne)	general/tcp				
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	172.18.0.3 (metasploit234.interne)	80/tcp				
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	80%	172.18.0.3 (metasploit234.interne)	512/tcp				
Distributed Ruby (DRuby/DRB) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	172.18.0.3 (metasploit234.interne)	8787/tcp				
Possible Backdoor: Ingreslock	10.0 (High)	99%	172.18.0.3 (metasploit234.interne)	1524/tcp				
DistCC Remote Code Execution Vulnerability	9.0 (High)	99%	172.18.0.3 (metasploit234.interne)	3632/tcp				
PostgreSQL weak password	9.0 (High)	99%	172.18.0.3 (metasploit234.interne)	5432/tcp				
MySQL / MariaDB weak password	9.0 (High)	95%	172.18.0.3 (metasploit234.interne)	3306/tcp				
rsh Unencrypted Cleartext Login	7.5 (High)	80%	172.18.0.3 (metasploit234.interne)	514/tcp				
phpinfo() output Reporting	7.5 (High)	80%	172.18.0.3 (metasploit234.interne)	80/tcp				
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	172.18.0.3 (metasploit234.interne)	80/tcp				
rlogin Passwordless / Unencrypted Cleartext Login	7.5 (High)	70%	172.18.0.3 (metasploit234.interne)	513/tcp				
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	172.18.0.3 (metasploit234.interne)	6200/tcp				
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	172.18.0.3 (metasploit234.interne)	21/tcp				
Test HTTP dangerous methods	7.5 (High)	99%	172.18.0.3 (metasploit234.interne)	80/tcp				
Check for Backdoor in UnrealIRCd	7.0 (High)	70%	172.18.0.3 (metasploit234.interne)	6667/tcp				
+ PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	172.18.0.3 (metasploit234.interne)	80/tcp				
SSH Brutal Force Logins With Default Credentials Reporting	7.5 (High)	95%	172.18.0.3 (metasploit234.interne)	22/tcp				

V/ REGARDER LES DIFFÉRENTS CAS DÉTECTÉ

The screenshot shows a detailed view of a specific vulnerability: "vsftpd Compromised Source Packages Backdoor Vulnerability". The page includes sections for Summary (vsftpd is prone to a backdoor vulnerability), Vulnerability Detection Result (Vulnerability was detected according to the Vulnerability Detection Method), Impact (Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application), Solution (Solution type: VendorFix, repaired package available at the provided link), Affected Software/OS (vsftpd 2.3.4 source package is affected), and References (BID: 48539, other links to security focus and blog posts). A "User Tags (none)" section is also present at the bottom.

Vulnerability	Severity	QoD	Host	Location	Actions			
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	172.18.0.3	6200/tcp				