

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.

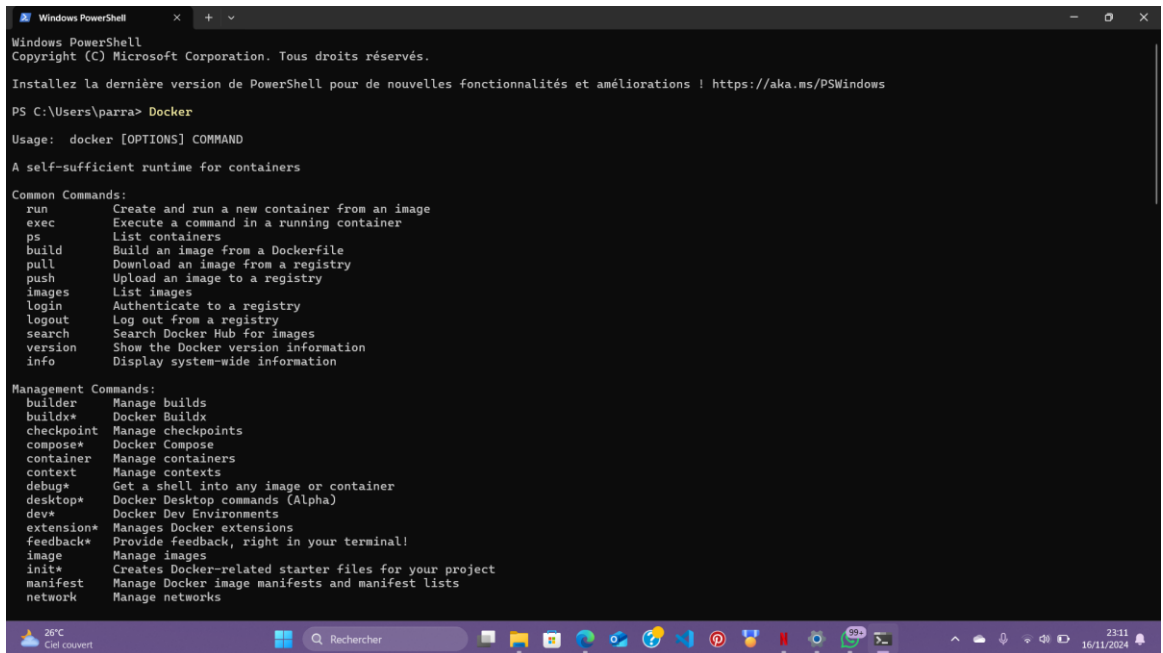
1. Télécharger

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

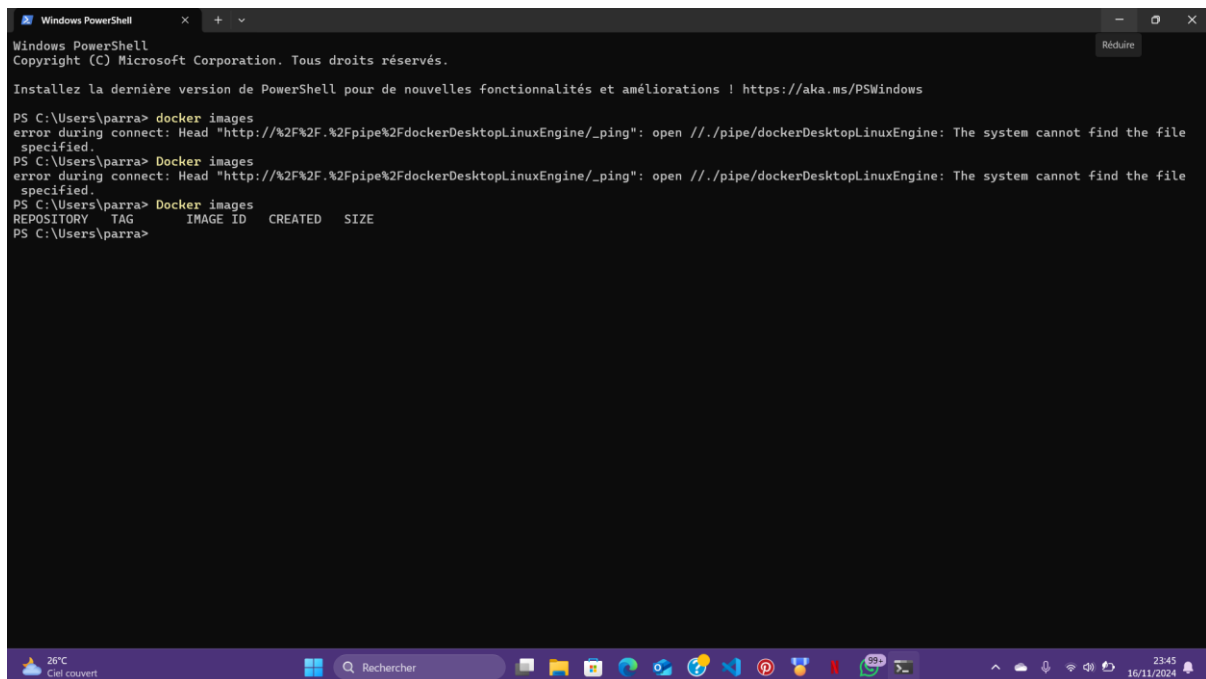
Common Commands:
run          Create and run a new container from an image
exec         Execute a command in a running container
ps           List containers
build        Build an image from a Dockerfile
pull         Download an image from a registry
push         Upload an image to a registry
images       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 téléchargement nous permet 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%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%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

```
Windows PowerShell
Your one-time device confirmation code is: QCMN-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
c4c454aebef: Download complete
27d3410150b2: Download complete
2aaf13f3eff0: Download complete
e08d578dc278: Download complete
a4f833680e45: Downloading [=====] 56.7MB/253.3MB
34667c7e4631: Downloading [=====] 33.55MB/43.56MB
c878d3d5e895: Download complete
d18d76e881a4: Download complete
110c7338fbfc: Download complete
44951337cd32: Downloading [==] 27.26MB/589.3MB
67b182362ac2: Downloading [====] 20.97MB/248.6MB
8c7fe885e62a: Downloading [=====] 28.31MB/153.5MB
ec12cc49fe18: Download complete
```

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.

1. Utilisation de Docker network create --driver bridge interne

- ```
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\parras> docker network create --driver bridge interne
6382943d8dbd8e371e6133dc8f9238b43d0a2c8034eab6f86e8dd8c2a3441
PS C:\Users\parras> docker network ls
NETWORK ID NAME DRIVER SCOPE
6382943d8dbd8e371e6133dc8f9238b43d0a2c8034eab6f86e8dd8c2a3441 interne bridge local
6382943d8dbd8e371e6133dc8f9238b43d0a2c8034eab6f86e8dd8c2a3441 none null local
6316783d8d8d6 interne bridge local
1138538c38c none null local
PS C:\Users\parras> docker run -d --name m443 --name openvas
docker run requires at least 1 argument.
See 'docker run --help'.

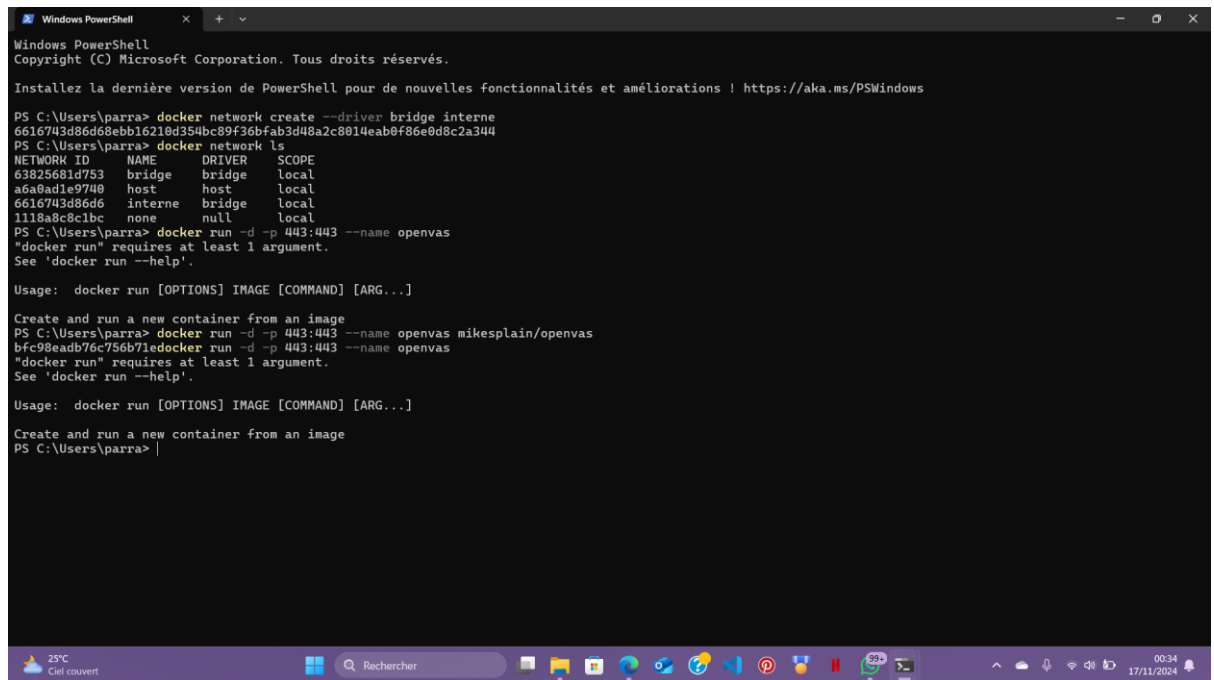
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Create and run a new container from an image
PS C:\Users\parras> docker run --name openvas mikesplain/openvas
6f6c9eabd76c7766b71edocker 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\parras> docker ps -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
6f6c9eabd76c mikesplain/openvas "/bin/sh -c -- start" 3 minutes ago Up 3 minutes 0.0.0.0:443->443/tcp, 9390/tcp
PS C:\Users\parras>
```

## 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
6616743d86d68ebb16210d354bc89f36bfab3d48a2c8014eab0f86e0d8c2a344
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.

```
@ 591517a8ac4e /
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
6616743d86d68ebb16210d354bc89f36bfab3d48a2c8014eab0f86e0d8c2a344
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
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.

```
@591917a8ac4e /
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
6616743d86d68ebb16210d354bc89f36bfab3d48a2c8014eab0f86e0d8c2a344
PS C:\Users\parra> docker network ls
NETWORK ID NAME DRIVER SCOPE
63825681d753 bridge bridge local
a6a0ad1e9740 host host local
6616743d86d6 interne bridge local
1118a8c0c1bc 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...]

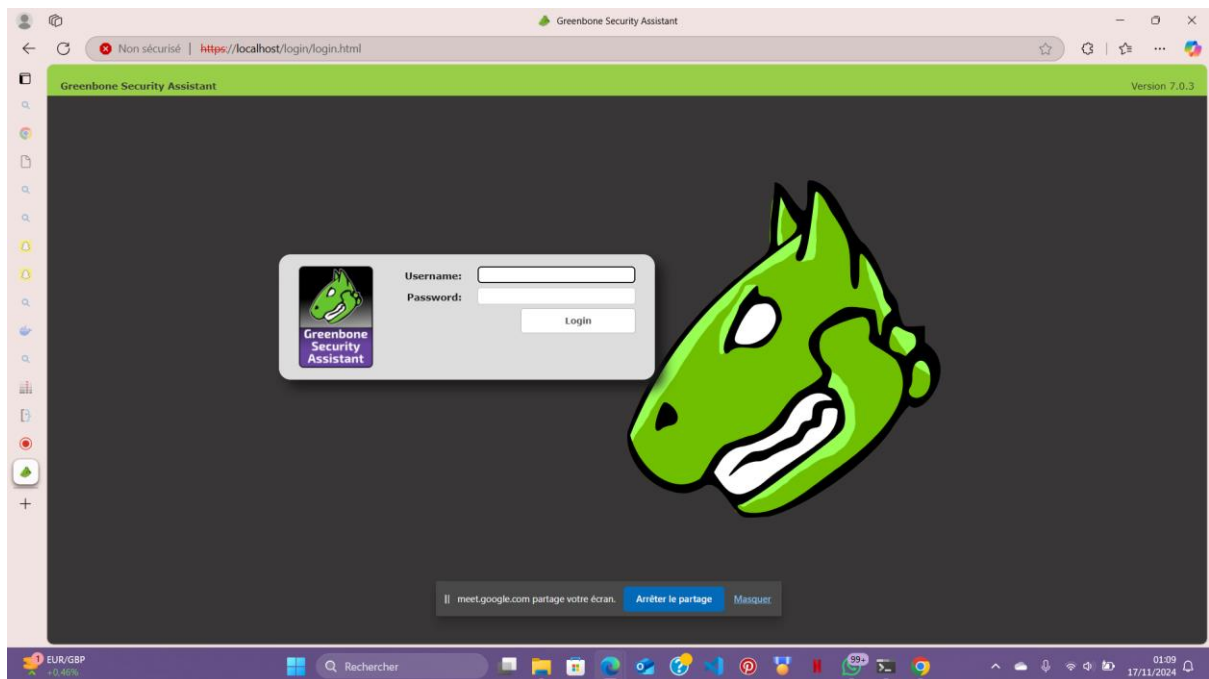
Create and run a new container from an image
PS C:\Users\parra> docker run -d -p 443:443 --name openvas mikesplain/openvas
bfc98eadb76c756b71edocker run -d -p 443:443 --name openvas
"docker run" requires at least 1 argument.
See 'docker run --help'.

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> 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
```

## || GREEN BONE ASSISTANT SECURITY

A



Après 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%20sort=name&token=c5ae2ff...](https://localhost/omp?cmd=get_tasks&filter=sort-reverse=last%20first=1%20min_qod=70%20apply_overrides=1%20rows=10%20sort=name&token=c5ae2ff...)

Greenbone Security Assistant

No auto-refresh

Logged in as Admin admin | Logout

Sun Nov 17 02:54:04 2024 UTC

DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp

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

1

Tasks with most High results per host

scann 1

0 1 2 3 4 5 6

Tasks by status (Total: 1)

Done

1

| Name                    | Status | Reports | Severity    | Trend       | Actions     |
|-------------------------|--------|---------|-------------|-------------|-------------|
|                         |        | Total   | Last        |             |             |
| scann 1 (metasploit234) | Done   | 1 (1)   | Nov 17 2024 | 10.0 (High) | <div></div> |

(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

99%

02:54 17/11/2024

## IV/ VULNÉRABILITÉS

The screenshot shows the Greenbone Security Assistant (GSA) interface. The top navigation bar includes Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area displays a report titled "Report: Results (61 of 400)". The report lists various vulnerabilities with columns for Vulnerability, Severity, QoD, Host, Location, and Actions. The vulnerabilities listed include OpenVAS / Greenbone Vulnerability Manager Default Credentials, OS End Of Life Detection, TWiki XSS and Command Execution Vulnerabilities, rexex Passwordless / Unencrypted Cleartext Login, Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities, Possible Backdoor: Ingreslock, DistCC Remote Code Execution Vulnerability, PostgreSQL weak password, MySQL / MariaDB weak password, rsync Unencrypted Cleartext Login, phpinfo() output Reporting, Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities, rlogin Passwordless / Unencrypted Cleartext Login, vsftpd Compromised Source Packages Backdoor Vulnerability, vsftpd Compromised Source Packages Backdoor Vulnerability, Test HTTP dangerous methods, Check for Backdoor in UnrealIRCd, PHP-CGI-based setups vulnerability when parsing query string parameters from php files, and SSH Brute Force Logins With Default Credentials Reporting.

| Vulnerability                                                                          | Severity    | QoD  | Host                               | Location    | Actions |
|----------------------------------------------------------------------------------------|-------------|------|------------------------------------|-------------|---------|
| OpenVAS / Greenbone Vulnerability Manager Default Credentials                          | 10.0 (High) | 100% | 172.18.0.2 (b/c98eadb76c)          | 9390/tcp    | [Icons] |
| OS End Of Life Detection                                                               | 10.0 (High) | 80%  | 172.18.0.3 (metasploit234.interne) | general/tcp | [Icons] |
| TWiki XSS and Command Execution Vulnerabilities                                        | 10.0 (High) | 80%  | 172.18.0.3 (metasploit234.interne) | 80/tcp      | [Icons] |
| rexex Passwordless / Unencrypted Cleartext Login                                       | 10.0 (High) | 80%  | 172.18.0.3 (metasploit234.interne) | 512/tcp     | [Icons] |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities            | 10.0 (High) | 99%  | 172.18.0.3 (metasploit234.interne) | 8787/tcp    | [Icons] |
| Possible Backdoor: Ingreslock                                                          | 10.0 (High) | 99%  | 172.18.0.3 (metasploit234.interne) | 1524/tcp    | [Icons] |
| DistCC Remote Code Execution Vulnerability                                             | 9.5 (High)  | 99%  | 172.18.0.3 (metasploit234.interne) | 3632/tcp    | [Icons] |
| PostgreSQL weak password                                                               | 9.0 (High)  | 99%  | 172.18.0.3 (metasploit234.interne) | 5432/tcp    | [Icons] |
| MySQL / MariaDB weak password                                                          | 9.0 (High)  | 95%  | 172.18.0.3 (metasploit234.interne) | 3306/tcp    | [Icons] |
| rsync Unencrypted Cleartext Login                                                      | 7.5 (High)  | 80%  | 172.18.0.3 (metasploit234.interne) | 514/tcp     | [Icons] |
| phpinfo() output Reporting                                                             | 7.5 (High)  | 80%  | 172.18.0.3 (metasploit234.interne) | 80/tcp      | [Icons] |
| Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities                     | 7.5 (High)  | 80%  | 172.18.0.3 (metasploit234.interne) | 80/tcp      | [Icons] |
| rlogin Passwordless / Unencrypted Cleartext Login                                      | 7.5 (High)  | 70%  | 172.18.0.3 (metasploit234.interne) | 513/tcp     | [Icons] |
| vsftpd Compromised Source Packages Backdoor Vulnerability                              | 7.5 (High)  | 99%  | 172.18.0.3 (metasploit234.interne) | 6200/tcp    | [Icons] |
| vsftpd Compromised Source Packages Backdoor Vulnerability                              | 7.5 (High)  | 99%  | 172.18.0.3 (metasploit234.interne) | 21/tcp      | [Icons] |
| Test HTTP dangerous methods                                                            | 7.5 (High)  | 99%  | 172.18.0.3 (metasploit234.interne) | 80/tcp      | [Icons] |
| Check for Backdoor in UnrealIRCd                                                       | 7.5 (High)  | 70%  | 172.18.0.3 (metasploit234.interne) | 6667/tcp    | [Icons] |
| 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      | [Icons] |
| SSH Brute Force Logins With Default Credentials Reporting                              | 7.5 (High)  | 95%  | 172.18.0.3 (metasploit234.interne) | 22/tcp      | [Icons] |

## V/ REGARDER LES DIFFÉRENTS CAS DÉTECTE

The screenshot shows the Greenbone Security Assistant (GSA) interface displaying a detailed report for the "vsftpd Compromised Source Packages Backdoor Vulnerability". The report includes a summary, vulnerability detection result, impact, solution, affected software/OS, vulnerability detection method, and references.

**Result: vsftpd Compromised Source Packages Backdoor Vulnerability**

**Vulnerability**

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

**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

The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

**Affected Software/OS**

The vsftpd 2.3.4 source package is affected.

**Vulnerability Detection Method**

Details: vsftpd Compromised Source Packages Backdoor Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103185)  
Version used: \$Revision: 12076 \$

**References**

BID: 48539  
Other: <http://www.securityfocus.com/bid/48539>  
<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>  
<https://security.appspot.com/vsftpd.html>

**User Tags (none)**