



## **TP : Scan de Vulnérabilité**

Cycle : **ING1**

Auteur : **DA-MATHA Josué**

Module : **Sécurité informatique**

Année Académique : **2022 -2023**

---



## Table des matières

1. Introduction .....	3
2. Détecter les vulnérabilités .....	4
3. Analyser les résultats .....	11
4. Générer les rapports et faire des recommandations .....	14



## 1. Introduction

---

La sécurité informatique est un enjeu crucial pour les organisations, qu'elles soient des entreprises, des organismes gouvernementaux, ou des institutions académiques. Dans ce contexte, la détection des vulnérabilités est une étape clé pour assurer la protection des systèmes informatiques.

OpenVAS (Open Vulnerability Assessment System) est un outil open source de scanner de vulnérabilités qui permet de détecter les failles de sécurité dans les systèmes et applications informatiques. Il est utilisé par les professionnels de la sécurité pour effectuer des analyses de sécurité sur les réseaux et les systèmes d'information, afin d'identifier les vulnérabilités et les risques de sécurité potentiels.

Dans ce contexte, nous procéderons à un scan de la VM Owaps broken Web App en utilisant OpenVAS afin de détecter les vulnérabilités susceptibles d'être exploitées par des attaquants malveillants. Nous analyserons ensuite les résultats obtenus, générerons des rapports détaillés et fournirons des recommandations pour corriger les vulnérabilités identifiées et renforcer la sécurité de la VM Owaps broken Web App.



## 2. Détecter les vulnérabilités

---

Nous utiliserons OpenVAS pour effectuer le scan de la VM Owaps Broken Web App.

## 2.1. Récupérer l'adresse IP de la cible

Ceci ce fait à travers la commande ifconfig.

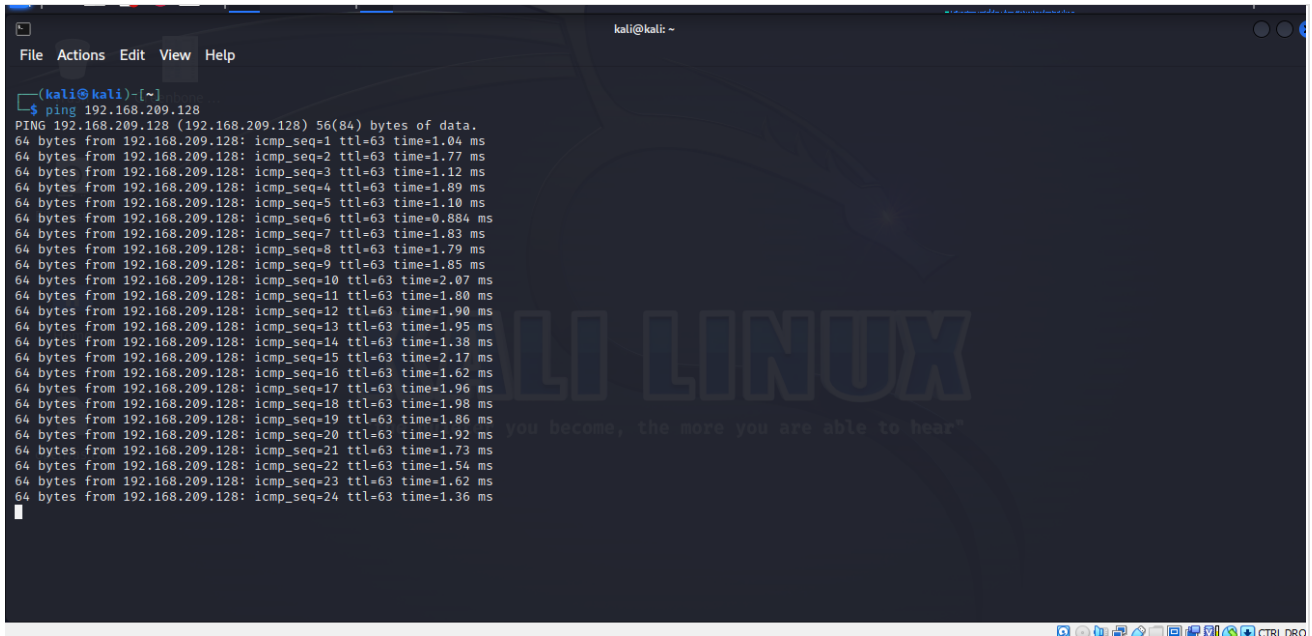
```
OWASP Broken Web Apps VM v1.2 - VMware Workstation 17 Player (Evaluation license)
Player
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:71 errors:0 dropped:0 overruns:0 frame:0
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:18529 (18.5 KB) TX bytes:18529 (18.5 KB)

root@owaspbua:~# ls
root@owaspbua:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:8f:ca:00
          inet addr:192.168.209.128 Bcast:192.168.209.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8f:ca00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3496 (3.4 KB) TX bytes:9722 (9.7 KB)
          Interrupt:18 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18529 (18.5 KB) TX bytes:18529 (18.5 KB)

root@owaspbua:~#
```

## 2.2. Tester la connectivité entre les réseaux



```
kali@kali: ~  
File Actions Edit View Help  
$ ping 192.168.209.128  
PING 192.168.209.128 (192.168.209.128) 56(84) bytes of data:  
64 bytes from 192.168.209.128: icmp_seq=1 ttl=63 time=1.04 ms  
64 bytes from 192.168.209.128: icmp_seq=2 ttl=63 time=1.77 ms  
64 bytes from 192.168.209.128: icmp_seq=3 ttl=63 time=1.12 ms  
64 bytes from 192.168.209.128: icmp_seq=4 ttl=63 time=1.89 ms  
64 bytes from 192.168.209.128: icmp_seq=5 ttl=63 time=1.10 ms  
64 bytes from 192.168.209.128: icmp_seq=6 ttl=63 time=0.884 ms  
64 bytes from 192.168.209.128: icmp_seq=7 ttl=63 time=1.83 ms  
64 bytes from 192.168.209.128: icmp_seq=8 ttl=63 time=1.79 ms  
64 bytes from 192.168.209.128: icmp_seq=9 ttl=63 time=1.85 ms  
64 bytes from 192.168.209.128: icmp_seq=10 ttl=63 time=2.07 ms  
64 bytes from 192.168.209.128: icmp_seq=11 ttl=63 time=1.80 ms  
64 bytes from 192.168.209.128: icmp_seq=12 ttl=63 time=1.90 ms  
64 bytes from 192.168.209.128: icmp_seq=13 ttl=63 time=1.95 ms  
64 bytes from 192.168.209.128: icmp_seq=14 ttl=63 time=1.38 ms  
64 bytes from 192.168.209.128: icmp_seq=15 ttl=63 time=2.17 ms  
64 bytes from 192.168.209.128: icmp_seq=16 ttl=63 time=1.62 ms  
64 bytes from 192.168.209.128: icmp_seq=17 ttl=63 time=1.96 ms  
64 bytes from 192.168.209.128: icmp_seq=18 ttl=63 time=1.98 ms  
64 bytes from 192.168.209.128: icmp_seq=19 ttl=63 time=1.86 ms  
64 bytes from 192.168.209.128: icmp_seq=20 ttl=63 time=1.92 ms  
64 bytes from 192.168.209.128: icmp_seq=21 ttl=63 time=1.73 ms  
64 bytes from 192.168.209.128: icmp_seq=22 ttl=63 time=1.54 ms  
64 bytes from 192.168.209.128: icmp_seq=23 ttl=63 time=1.62 ms  
64 bytes from 192.168.209.128: icmp_seq=24 ttl=63 time=1.36 ms
```

La commande **ping 192.168.209.328** fonctionne en envoyant des paquets de données (appelés « paquets ping ») à l'hôte cible 192.168.209.328 (adresse IP de la VM Owaps Broken Web App) et en mesurant le temps que prend la réponse de l'hôte cible pour revenir à l'émetteur. Ces paquets ping contiennent des informations sur l'heure d'envoi du paquet, la taille du paquet et un numéro de séquence unique.

## 2.3. Lancer OpenVAS

On utilise la commande « **gvm-start** ».

```
(kali@kali)~$ sudo su
[sudo] password for kali:
(kali@kali)~$ gvm-start
[>] Please wait for the GVM services to start.
[>] You might need to refresh your browser once it opens.
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

• gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-05-26 11:56:13 EDT; 15ms ago
  Docs: man:gsad(8)
        https://www.greenbone.net
  Main PID: 8830 (gsad)
  Tasks: 1 (limit: 2255)
  Memory: 296.0K
  CPU: 2ms
  CGroup: /system.slice/gsad.service
          └─8830 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

May 26 11:56:13 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad) ...
May 26 11:56:13 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

• gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-05-26 11:56:07 EDT; 5s ago
  Docs: man:gvmd(8)
  Process: 8659 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=gvm (code=exited, status=0/SUCCESS)
  Main PID: 8661 (gvmd)
  Tasks: 1 (limit: 2255)
  Memory: 178.5M
  CPU: 1.163s
  CGroup: /system.slice/gvmd.service
          └─8661 "gvmd: gvmd: Wa" --osp-vt-update=/run/ospd/ospd.sock --listen-group=gvm

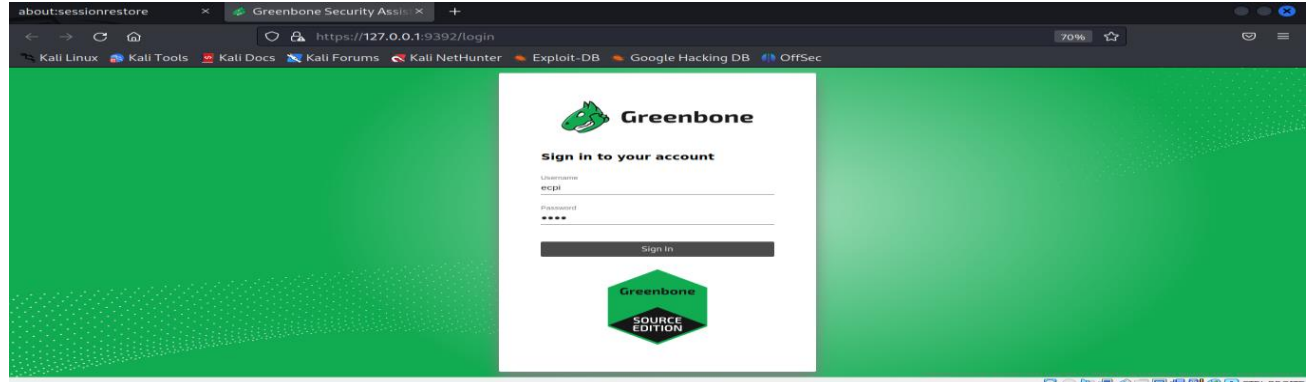
May 26 11:55:56 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd) ...
May 26 11:55:56 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: Operation not permitted
May 26 11:56:07 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

• ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
  Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-05-26 11:55:52 EDT; 20s ago
  Docs: man:ospd-openvas(8)
        man:openvas(8)
  Process: 8531 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
  Main PID: 8601 (ospd-openvas)
  Tasks: 5 (limit: 2255)
  Memory: 227.0M
  CPU: 8.161s
  CGroup: /system.slice/ospd-openvas.service
          └─8601 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
             └─8605 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf

May 26 11:55:44 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas) ...
May 26 11:55:52 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).

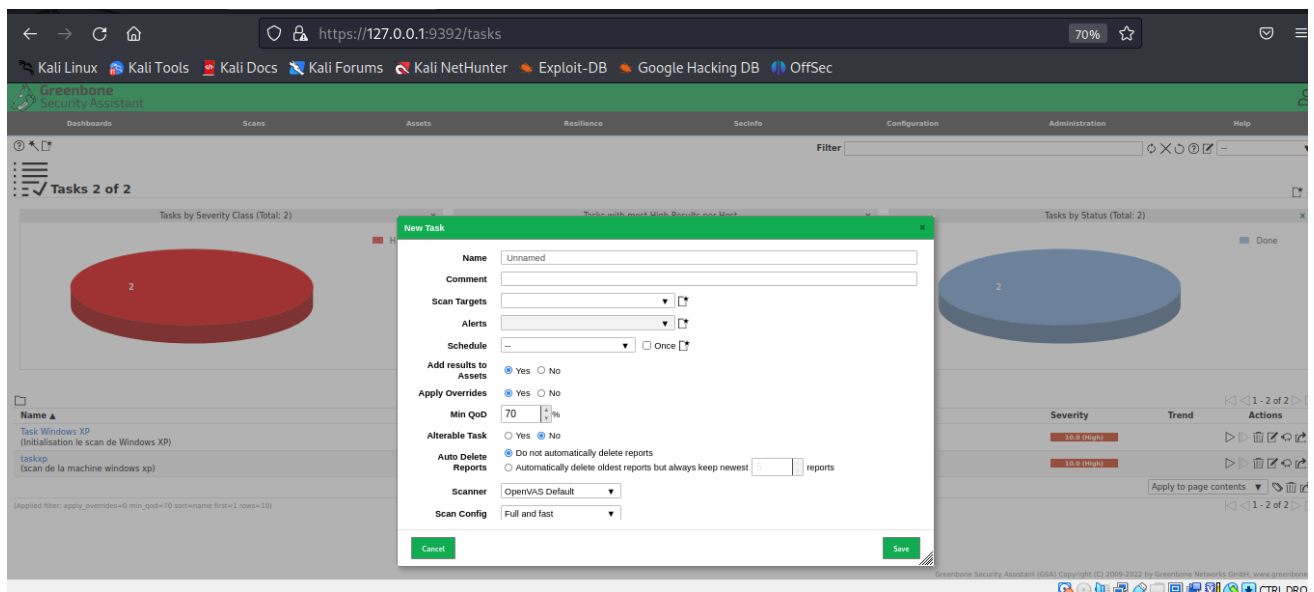
[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

(kali@kali)~$
```

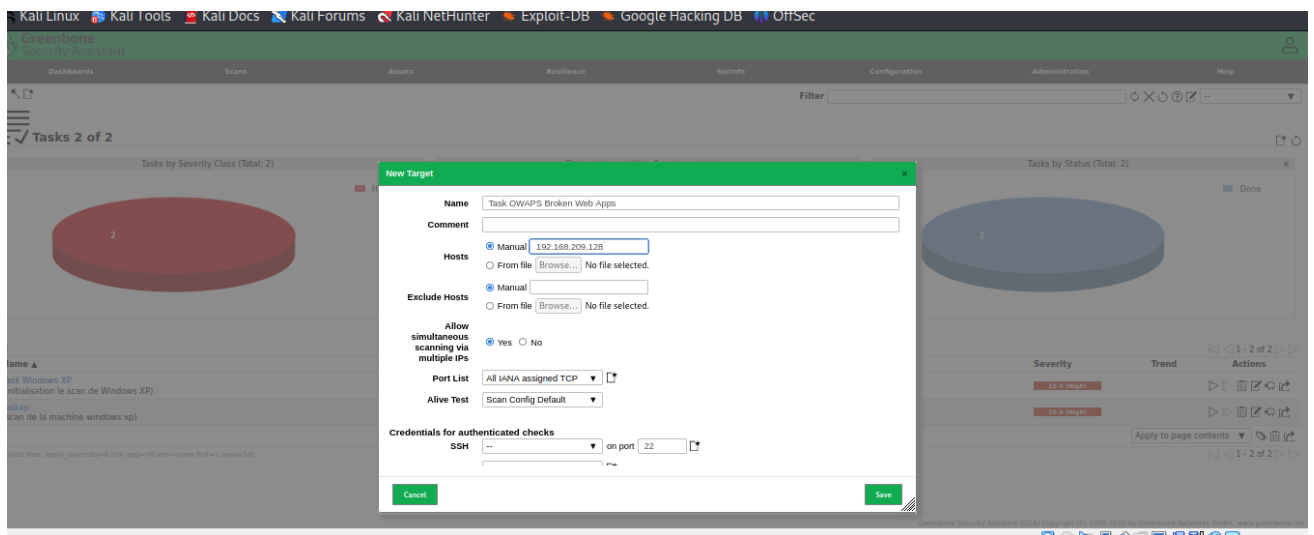


## 2.4. Créer et configurer la tâche

### ◆ Entrer dans le volet Scan puis New Task



### ◆ Entrer le nom du Task ensuite entrer dans Scan Targets pour définir la nouvelle cible puis Save







Security Assistant

Task 2 of 2

Tasks by Severity Class (Total: 2)

Tasks by Status (Total: 2)

New Task

Name: Task OWASP Broken Web Apps

Comment:

Scan Targets: Task OWASP Broken Web Apps

Alerts:

Schedule: --

Add results to Assets: Yes

Apply Overrides: Yes

Min QoD: 70

Alterable Task: No

Auto Delete Reports: Do not automatically delete reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Save

## Visualisation de la nouvelle Task

Security Assistant

Task 3 of 3

Tasks by Severity Class (Total: 3)

Tasks with most High Results per Host

Tasks by Status (Total: 3)

Name	Status	Reports	Last Report	Severity	Trend	Actions
Task OWASP Broken Web Apps	0 %	1				
Task Windows XP (Initialisation le scan de Windows XP)	Done	1	Wed, May 10, 2023 11:46 AM UTC	10.0 (High)		
taskxp (scan de la machine windows xp)	Done	1	Wed, May 17, 2023 11:29 AM UTC	10.0 (High)		

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Greenbone Security Assistant

Task 3 of 3

Tasks by Severity Class (Total: 3)

Tasks with most High Results per Host

Tasks by Status (Total: 3)

Name	Status	Reports	Last Report	Severity	Trend	Actions
Task OWASP Broken Web Apps	100 %	1				
Task Windows XP (Initialisation le scan de Windows XP)	Done	1	Wed, May 10, 2023 11:46 AM UTC	10.0 (High)		
taskxp (scan de la machine windows xp)	Done	1	Wed, May 17, 2023 11:29 AM UTC	10.0 (High)		



## ◆ Résultats du Scan

The screenshot displays the Greenbone Security Assistant (GSA) interface. The top navigation bar includes links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. A filter bar is present on the right. The main content area shows a report for a task named "Task OWASP Broken Web Apps" completed on Friday, May 26, 2023, at 4:08 PM UTC. The report summary indicates 112 results, 1 host, 5 ports, 26 applications, 0 operating systems, 44 CVEs, 0 closed CVEs, 1 TLS certificate, 3 error messages, and 0 user tags. Below the summary, a table lists the vulnerabilities found:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:38 PM UTC
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:38 PM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.209.128	192.168.209.128	general/tcp	Fri, May 26, 2023 4:25 PM UTC
Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.9.7 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.8.12 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.8.12 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! Core LDAP Information Disclosure Vulnerability Nov17	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.9.7 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! Core LDAP Information Disclosure Vulnerability Nov17	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.9.5 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.9.5 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Joomla! < 3.9.13 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:34 PM UTC
Tiki Wiki < 2.2 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	80tcp	Fri, May 26, 2023 4:38 PM UTC
Tiki Wiki < 2.2 Multiple Vulnerabilities	9.8 (High)	80 %	192.168.209.128	192.168.209.128	443tcp	Fri, May 26, 2023 4:38 PM UTC

Le scan nous donne un aperçu de toutes les vulnérabilités découvertes sur la machine VM Owaps Broken Web App.



### 3. Analyser les résultats

<

On constate que les résultats sont classés par taux de gravité par défaut.

#### ◆ Hosts

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Report: 

Fri, May 26, 2023 4:08 PM UTC

Done

ID: 012b02a4-d844-45a3-9c03-561259d70eb7

Created: Fri, May 26, 2023 4:08 PM UTC

Modified: Fri, May 26, 2023 5:17 PM UTC

Owner: ecpi

Information

Results

(112 of 1023)

Hosts

(1 of 1)

Ports

(5 of 9)

Applications

(26 of 26)

Operating Systems

(0 of 0)

CVEs

(44 of 44)

Closed CVEs

(0 of 0)

TLS Certificates

(1 of 1)

Error Messages

(3 of 3)

User Tags

(0)

1 - 1 of 1

IP Address

Hostname

OS

Ports

Apps

Distance

Auth

Start

End

High

Medium

Low

Log

False Positive

Total

Severity ▼

192.168.209.128

?

5

28

✓

Fri, May 26, 2023 4:11 PM UTC

35

74

3

0

0

112

10.0 (High)

Active

Windows

<

#### ◆ Ports

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

--

Report

Fri, May 26, 2023 4:08 PM UT

Done

ID: 012b02a4-d844-45a3-9c03-561259d70eb7

Created: Fri, May 26, 2023 4:08 PM UTC

Modified: Fri, May 26, 2023 5:17 PM UTC

Owner: ecpi

Information

Results

(112 of 1023)

Hosts

(1 of 1)

Ports

(5 of 9)

Applications

(26 of 26)

Operating Systems

(0 of 0)

CVEs

(44 of 44)

Closed CVEs

(0 of 0)

TLS Certificates

(1 of 1)

Error Messages

(3 of 3)

User Tags

(0)

Port

Hosts

Severity

80/tcp

1

10.0 (High)

443/tcp

1

10.0 (High)

8080/tcp

1

6.8 (Medium)

8081/tcp

1

6.1 (Medium)

22/tcp

1

5.3 (Medium)

(Applied filter: apply overrides=0 levels=hml rows=100 min.qod=70 first=1 sort=reverse=severity)

1 - 5 of 5



- ◆ CVEs

- ◆ Closed CVEs

- ◆ TLS Certificates

DashboardsScansAssetsResilienceSecInfoConfigurationAdministrationHelp

**Report:**Fri, May 26, 2023 4:08 PM UTC
 Done

ID: 012b02a4-d844-45a3-9c03-561259d70eb7
Created: Fri, May 26, 2023 4:08 PM UTC
Modified: Fri, May 26, 2023 5:17 PM UTC
Owner: erpi

Information	Results <small>(122 of 1023)</small>	Hosts <small>(1 of 1)</small>	Ports <small>(5 of 9)</small>	Applications <small>(26 of 26)</small>	Operating Systems <small>(0 of 0)</small>	CVEs <small>(44 of 44)</small>	Closed CVEs <small>(0 of 0)</small>	TLS Certificates <small>(1 of 1)</small>	Error Messages <small>(3 of 3)</small>	User Tags <small>(0)</small>
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 30%;"> <p><b>Issuer DN ▲</b></p> <p>CN=owaspbwa</p> </div> <div style="width: 30%;"> <p><b>Serial</b></p> <p>00E6870D0D7C2B9E7</p> </div> <div style="width: 15%;"> <p><b>Activates</b></p> <p>Thu, Jan 3, 2013 2:12 AM UTC</p> </div> <div style="width: 15%;"> <p><b>Expires</b></p> <p>Sun, Jan 1, 2023 2:12 AM UTC</p> </div> <div style="width: 15%;"> <p><b>IP</b></p> <p>192.168.209.128</p> </div> <div style="width: 15%;"> <p><b>Hostname</b></p> </div> <div style="width: 10%;"> <p><b>Port</b></p> <p>443</p> </div> <div style="width: 10%; text-align: right;"> <p><b>Actions</b></p> <p></p> </div> </div>										

(Applied filter: apply overrides=0 levels=<html rows>=100 min=<io first>=1 sort=reverse-severity)



## ◆ Error Messages

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

--

Report: Fri, May 26, 2023 4:08 PM UTC

Done

ID: 012b02a4-d844-45a3-9c03-561259d70b67

Created: Fri, May 26, 2023 4:08 PM UTC

Modified: Fri, May 26, 2023 5:17 PM UTC

Owner: ecpi

Information

Results

(122 of 1023)

Hosts

(1 of 1)

Ports

(5 of 9)

Applications

(26 of 26)

Operating Systems

(0 of 0)

CVEs

(44 of 44)

Closed CVEs

(0 of 0)

TLS Certificates

(1 of 1)

Error Messages

(3 of 3)

User Tags

(0)

Error Message

Host

Hostname

NVT

Port

NVT timed out after 320 seconds.

192.168.209.128

CKEditor Detection (HTTP)

general/tcp

NVT timed out after 320 seconds.

192.168.209.128

FCKeditor Detection (HTTP)

general/tcp

NVT timed out after 320 seconds.

192.168.209.128

Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Active Check

general/tcp

(Applied filter: apply\_overrides=0 levels=html rows=100 min\_gd=70 first=1 sort=reverse=severity)

1 - 3 of 3

## ◆ User Tags

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report: Fri, May 26, 2023 4:08 PM UTC

Done

ID: 012b02a4-d844-45a3-9c03-561259d70b67

Created: Fri, May 26, 2023 4:08 PM UTC

Modified: Fri, May 26, 2023 5:17 PM UTC

Owner: ecpi

Information

Results

(122 of 1023)

Hosts

(1 of 1)

Ports

(5 of 9)

Applications

(26 of 26)

Operating Systems

(0 of 0)

CVEs

(44 of 44)

Closed CVEs

(0 of 0)

TLS Certificates

(1 of 1)

Error Messages

(3 of 3)

User Tags

(0)

No user tags available



## 4. Générer les rapports et faire des recommandations

Un rapport complet a été généré pour documenter les résultats du scan. Ce rapport fournit une description détaillée de chaque vulnérabilité détectée, y compris son impact potentiel, sa sévérité et les mesures recommandées pour la corriger.

Intéressons-nous à [Tiki Wiki CMS Groupware End of Life \(EOL\) Detection](#) par exemple.

The screenshot displays the Greenbone Security Assistant (GSA) interface. The top navigation bar includes links for Dashboards, Scans, Assets, Resilience, IP, Security, Name, Configuration, Administration, and Help. The main content area shows the details of a scan titled "Tiki Wiki CMS Groupware End of Life (EOL) Detection". The scan status is "80 %", and the target IP is "192.168.209.128". The scan was performed on "Fri, May 26, 2023 4:38 PM UTC".

**Summary**

The Tiki Wiki CMS Groupware version on the remote host has reached the End of Life (EOL) and should not be used anymore.

**Detection Result**

The "Tiki Wiki CMS Groupware" version on the remote host has reached the end of life.

CPE: cpe:/a:tiki:tikiwiki\_cms/groupware:1.9.5  
Installed version: 1.9.5  
Location/URL: https://192.168.209.128/tikiwiki  
EOL version: 1  
EOL date: unknown  
EOL info: https://tiki.org/versions#Version\_Lifecycle

**Detection Method**

Checks if an EOL version is present on the target host.

Details: Tiki Wiki CMS Groupware End of Life (EOL) Detection OID: 1.3.6.1.4.1.25623.1.0.108622  
Version used: 2020-12-09T14:13:00Z

**Impact**

An EOL version of Tiki Wiki CMS Groupware is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution**

**Solution Type:** Vendorfix  
Update the Tiki Wiki CMS Groupware version on the remote host to a still supported version.

**References**

Other [https://tiki.org/versions#Version\\_Lifecycle](https://tiki.org/versions#Version_Lifecycle)

The bottom of the interface shows a Windows activation watermark: "Activer Windows. Accédez aux paramètres pour activer Windows. 80tcp. Fri, May 26, 2023 4:38 PM UTC".

Lorsqu'on clique sur le nom de la vulnérabilité, nous pouvons obtenir un aperçu des détails concernant la vulnérabilité.