Amor

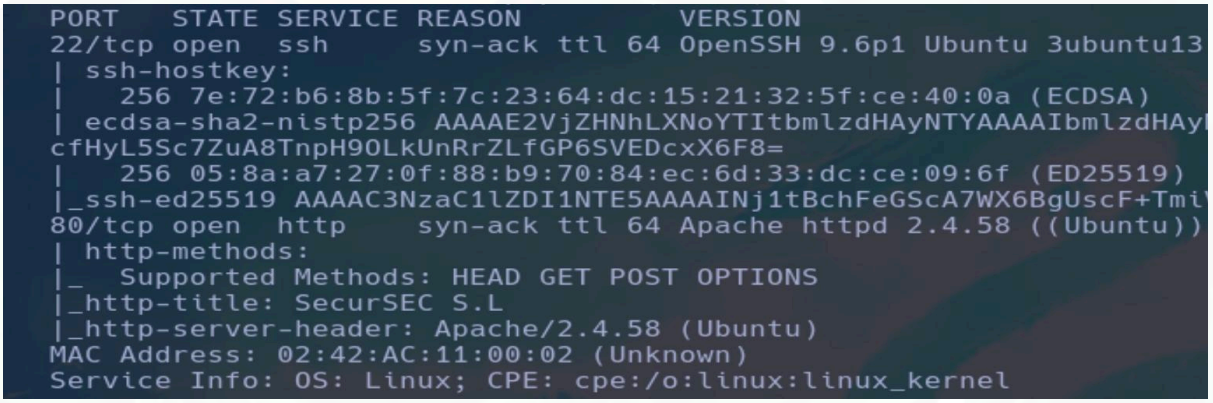
Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

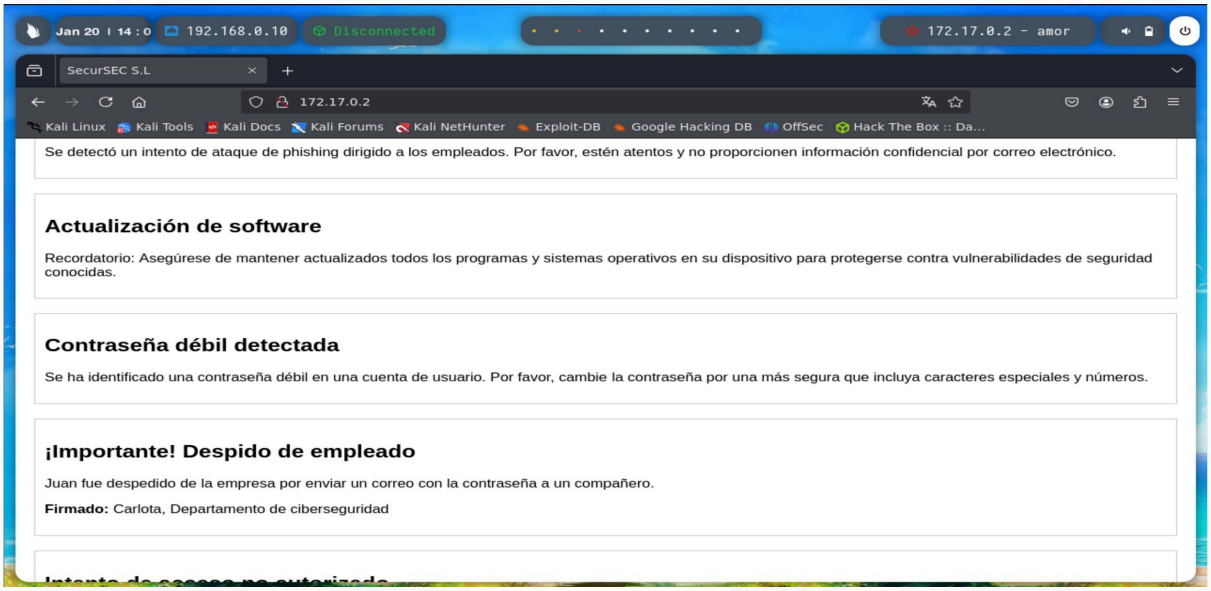
- **-p-**: Escanea todos los puertos .
- **-sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- **-sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- **-sV**: Detecta las versiones de los servicios en ejecución.
- **--min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- **-n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- **-vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- **-Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos



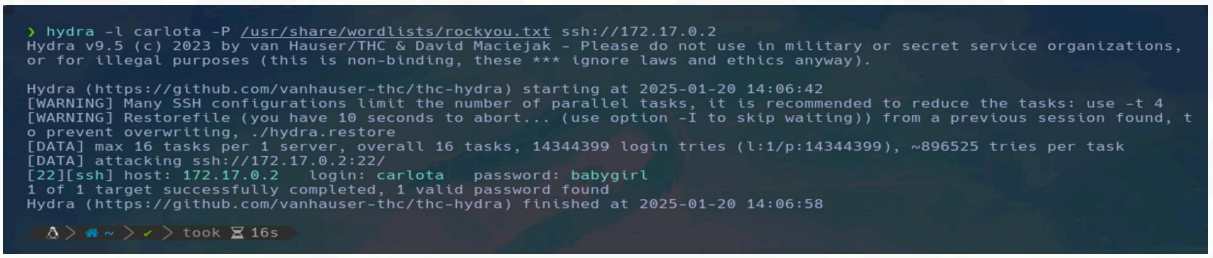
El puerto 22 tiene SSH, pero como su versión es alta, nos enfocaremos en el puerto 80, que tiene HTTP.

Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.

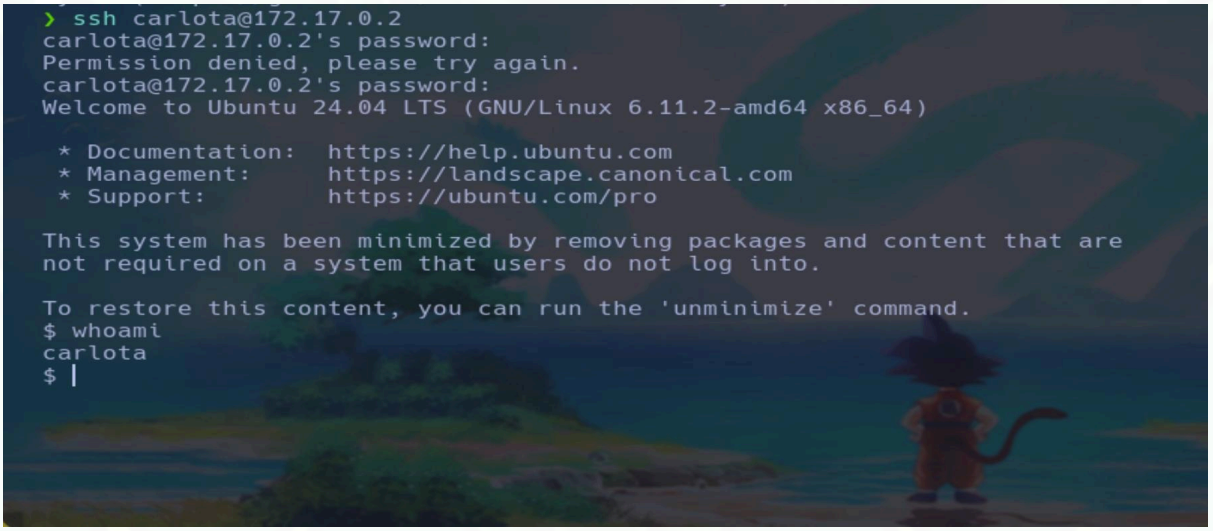


Nos aparecen dos posibles usuarios, Juan y Carlota así que probaremos un con un ataque de fuerza bruta con hydra para obtener su contraseña

hydra -l carlota -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2



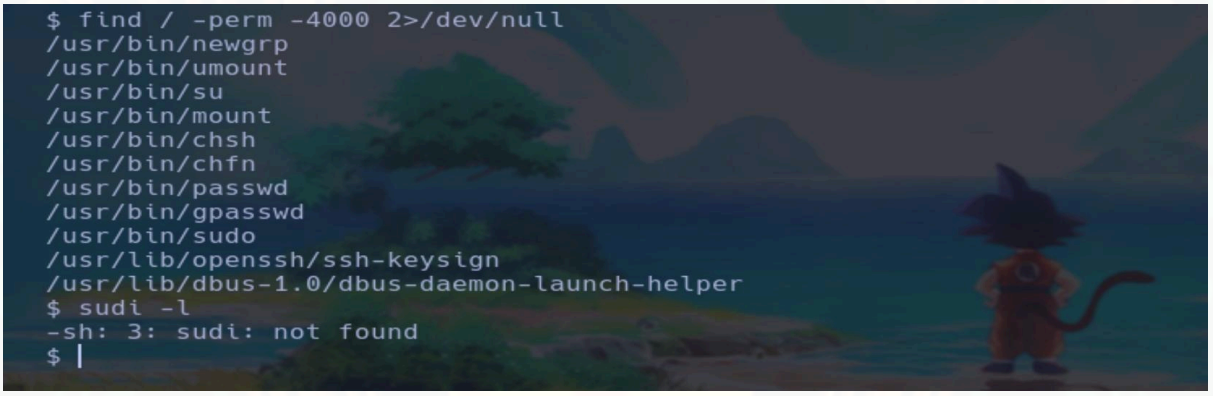
Una vez obtenida, entramos por el puerto ssh con: **ssh carlota@172.17.0.2**



Ya dentro, al no ser usuario root, debemos escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando :
find / -perm -4000 2>/dev/null

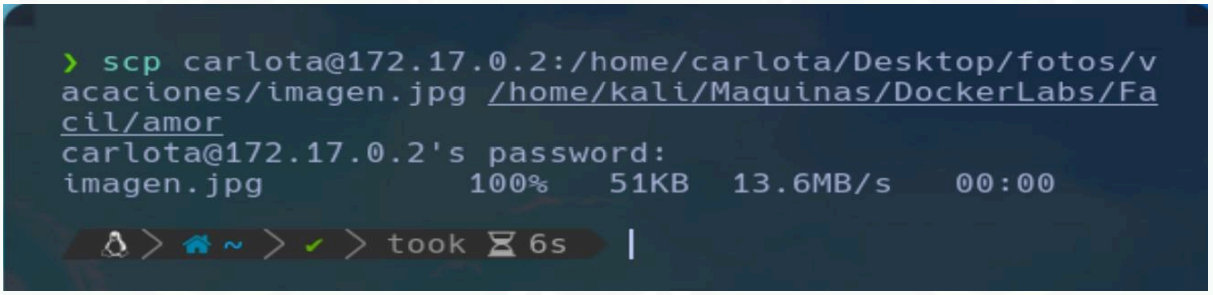
o binarios Sudo con **sudo -l**



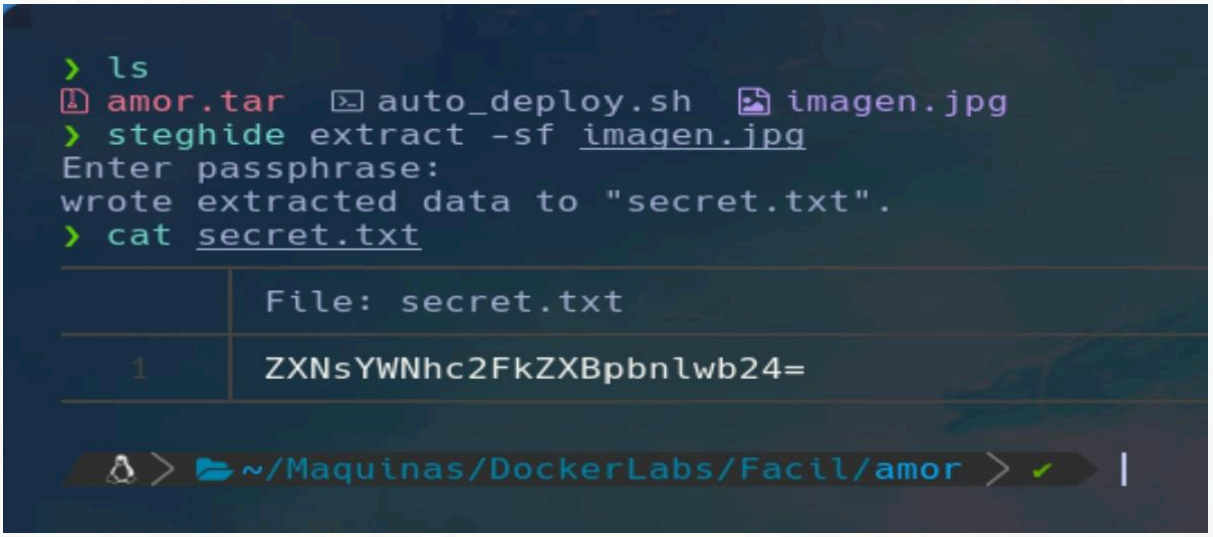
Desafortunadamente no vemos nada que nos pueda ayudar así que navegamos por los directorios en

busca de alguna pista

Hay una imagen, procedemos a descargarla para ver si tiene algún archivo oculto y buscar en sus metadatos
scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg <aqui pon tu directorio>

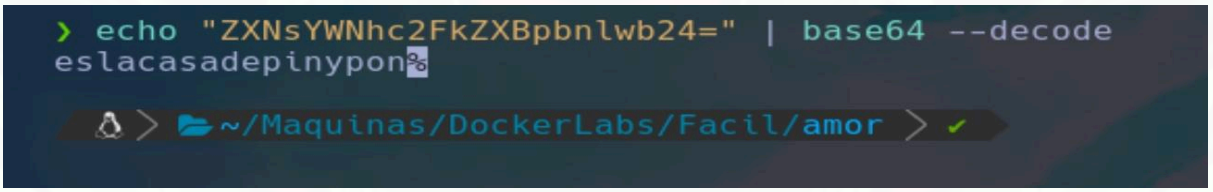


Para comprobar si tiene archivos ocultos utilizamos la herramienta sthegide: **steghide extract -sf imagen.jpg**



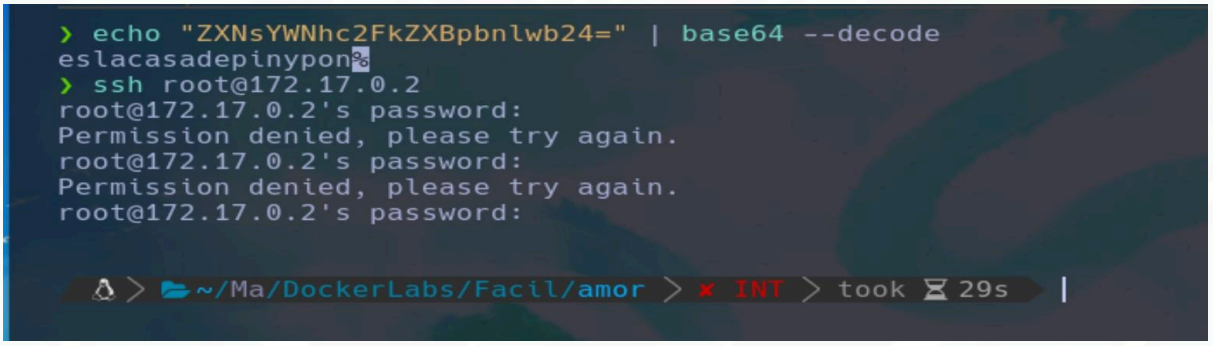
Efectivamente hay un archivo oculto por lo que haremos un cat para ver su contenido y parece estar cifrado

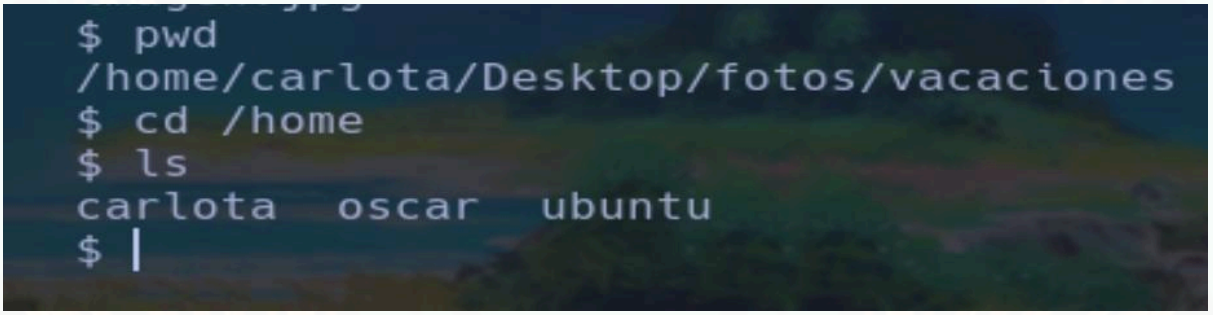
en base64, para descifrarlo ponemos: **echo "ZXNsYWNhc2FkZXBpbnlwb24=" | base64 --decode**



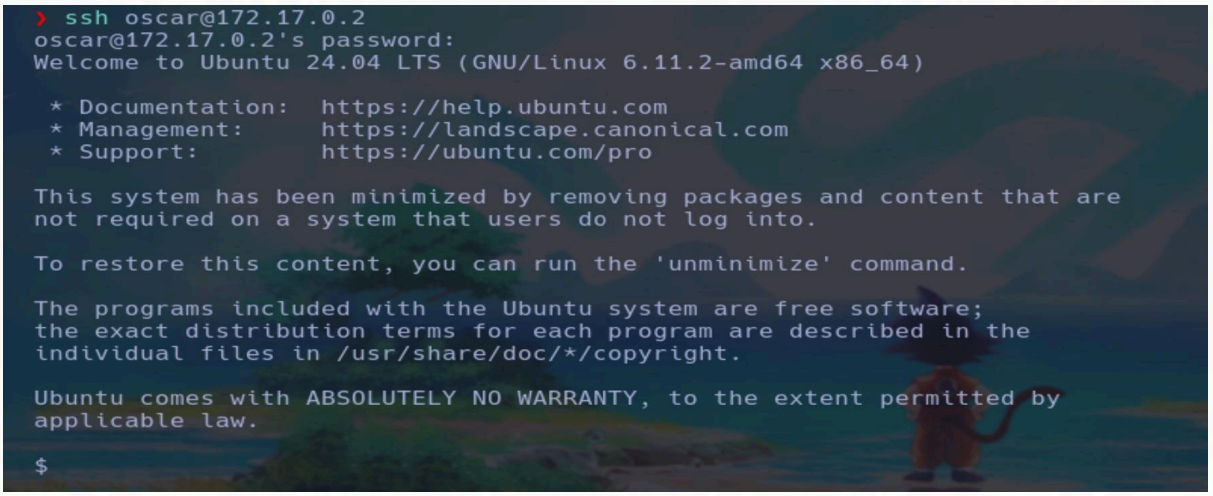
La contraseña es: **eslacasadepinypon**

Intento entrar con el usuario root pero la contraseña no pertenece a ese usuario, así que buscaremos usuarios desde el usuario de carlota

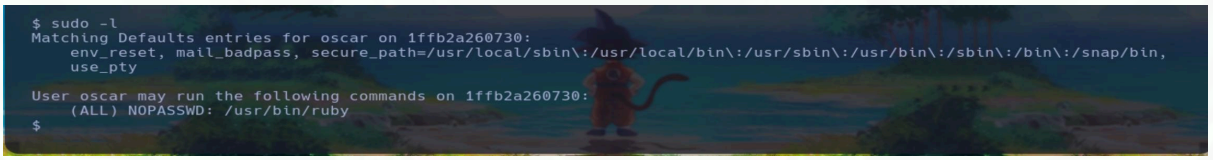




Oscar es un usuario, intentemos entrar por el puerto ssh con ese usuario

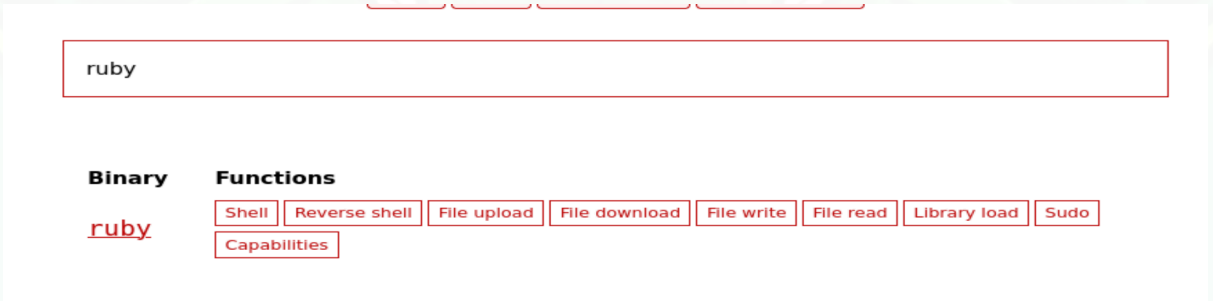


Si ha funcionado, ahora dentro de oscar tenemos que escalar privilegios, busquemos binarios **sudo -l**



Encontramos el binario ruby ,para encontrar las vulnerabilidades recomiendo esta pagina: https://gtfobins.github.io/

En nuestro caso buscamos el binario ruby nos aparece la opción de Sudo

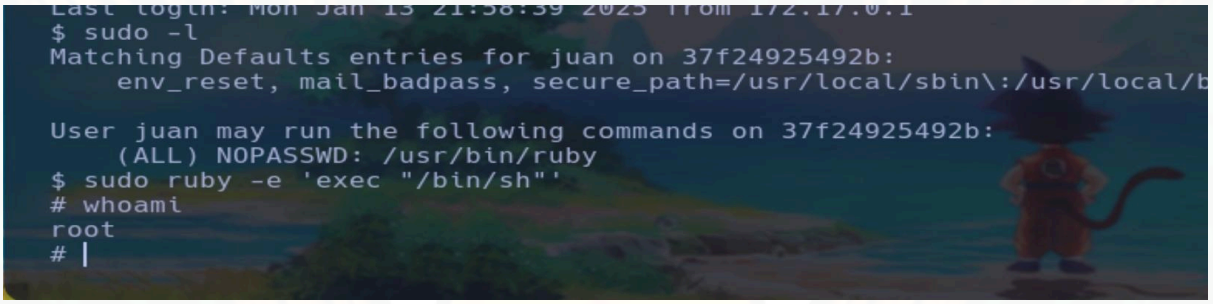


Sudo

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"'
```

Ahora simplemente copiamos y pegamos el comando: **sudo ruby -e 'exec "/bin/sh"'**



Y ya somos usuario root.