BorazuwarahCTF

Primero comprobamos si tenemos conexión con la máquina:

```
❯ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.117 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.117/0.117/0.117/0.000 ms
```

La ttl es de 64, por lo que probablemente estamos frente a una máquina **Linux**.

Ahora vamos a ver los puertos abiertos:

```
❯ sudo nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
[sudo] contraseña para romy:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 19:47 CEST
Initiating ARP Ping Scan at 19:47
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:47, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:47
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:47, 1.12s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-06-03 19:47:34 CEST for 2s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Ahora vamos a realizar un escaneo más en profundidad:

```
❯ nmap -sCV -p22,80 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 19:48 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00015s 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-server-header: Apache/2.4.59 (Debian)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora vamos a explorar la web.

Vamos a descargar la imagen para analizarla:

Y ahora la analizamos:

```
❯ steghide extract -sf huevo.jpeg
Anotar salvoconducto:
anot◆los datos extra◆dos e/"secreto.txt".
```

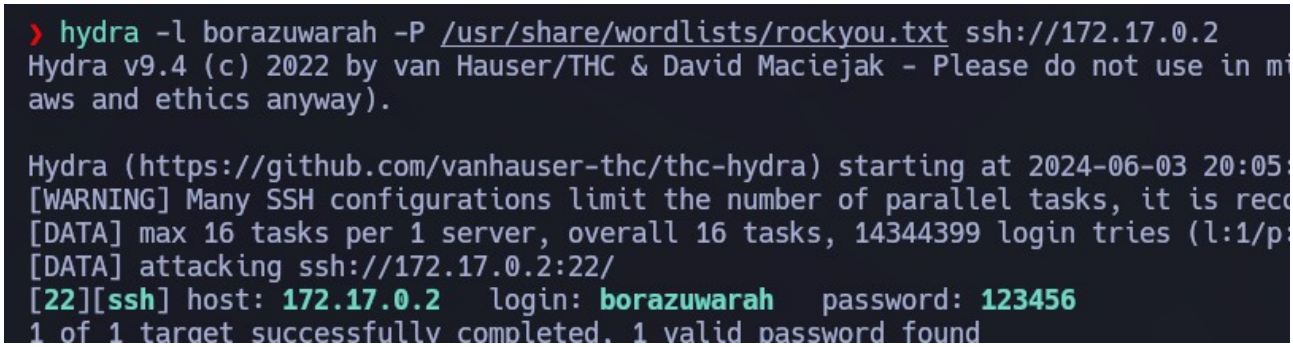
Y el txt contiene lo siguiente:

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

Ahora vamos a ver los metadatos que contiene la imagen:

```
❯ exiftool huevo.jpeg
ExifTool Version Number         : 12.57
File Name                       : huevo.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2024:06:03 19:55:58+02:00
File Access Date/Time           : 2024:06:03 19:55:58+02:00
File Inode Change Date/Time     : 2024:06:03 19:56:09+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 vemos, sale el usuario para acceder por ssh pero no la contraseña, vamos a intentar conseguir la contraseña por fuerza bruta:



Y ya tenemos la contraseña para acceder por ssh:

Ahora accedemos a root: