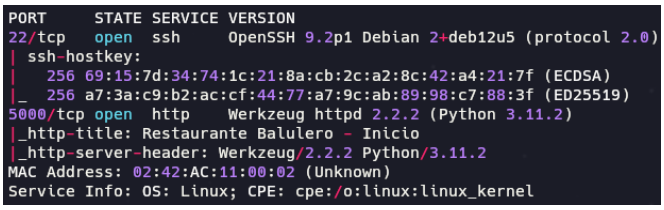
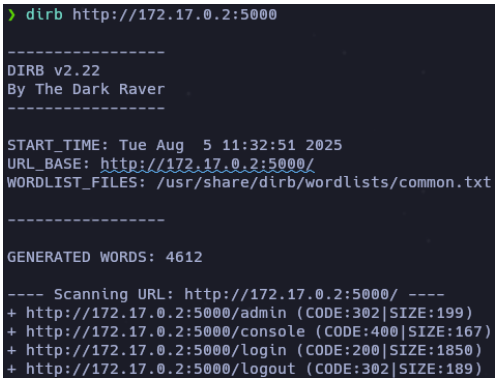
Desplegamos la máquina.

Realimos un nmap para comprobar puertos abiertos y sus servicios.

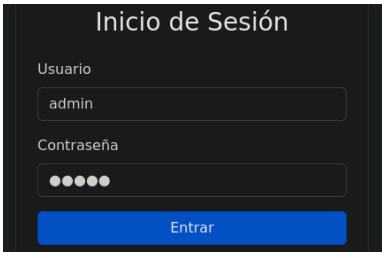


Con whatweb vemos las tecnologías que tiene la página web.

Aplicamos un dirb para comprobar archivos y directorios ocultos.



Tenemos un login y probamos admin:admin.



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 bbdcbc617ee6 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@bbdcbc617ee6:~$ 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@bbdcbc617ee6:~$ 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@bbdcbc617ee6:~$ 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@bbdcbc617ee6:~$ 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@bbdcbc617ee6:~$ su balulero
Password:
balulero@bbdcbc617ee6:/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@bbdcbc617ee6:~$ 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.