Pickle Rick

Enumeration

TCP

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.36.191
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-03 07:15 EDT
Nmap scan report for 10.10.36.191
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
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 7.73 seconds
```

Podemos observar como cuenta con el puerto 22 (SSH) abierto corriendo OpenSSH 7.2p2
También cuenta con el puerto 80 (HTTP) corriendo el servicio de Apache 2.4.18

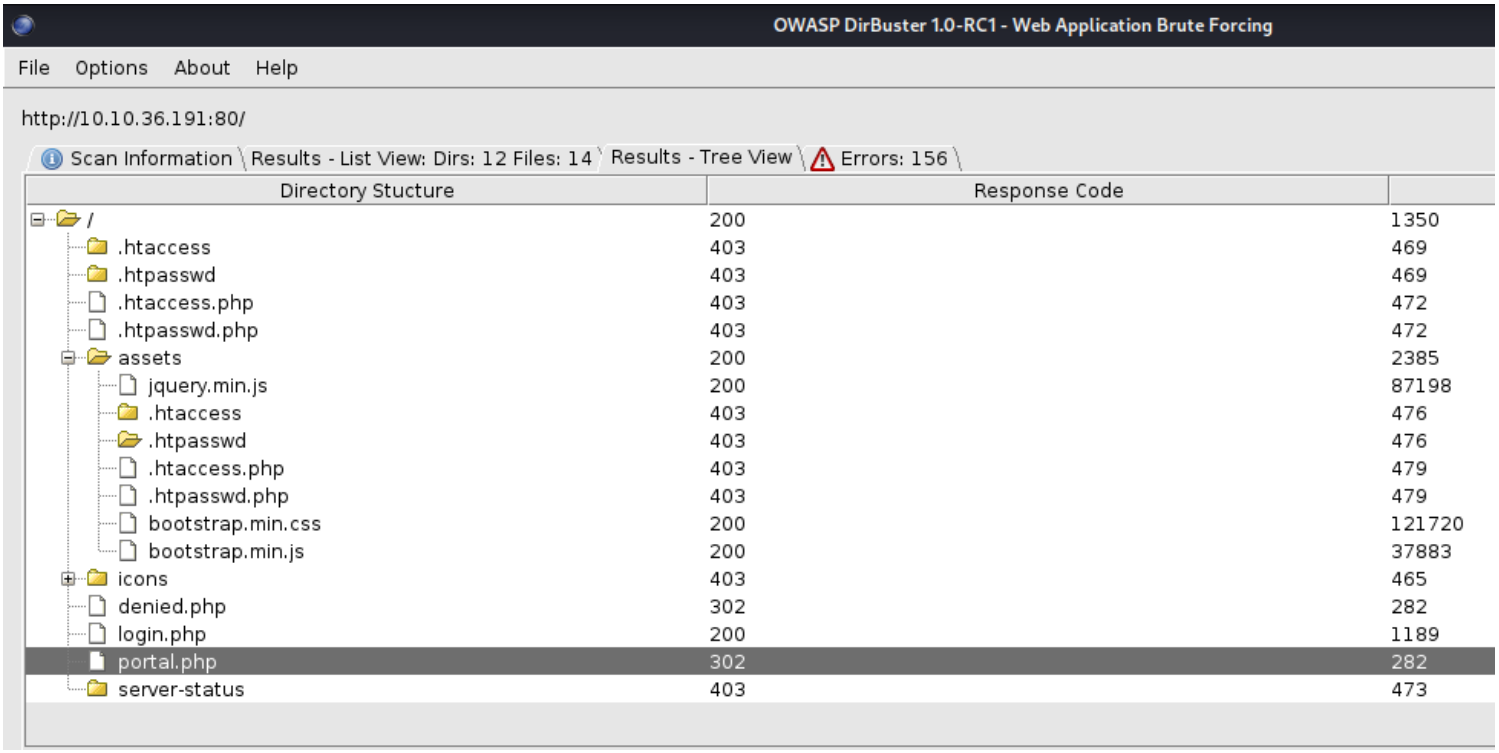
Web Services

Dirb|DirBuster

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.36.191 -w /usr/share/wordlists/dirb/big.txt -R

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

START_TIME: Tue May  3 07:07:25 2022
URL_BASE: http://10.10.36.191/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Interactive Recursion
OPTION: Not Stopping on warning messages

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.36.191/ ----
==> DIRECTORY: http://10.10.36.191/assets/
+ http://10.10.36.191/index.html (CODE:200|SIZE:1062)
+ http://10.10.36.191/robots.txt (CODE:200|SIZE:17)
+ http://10.10.36.191/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.36.191/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
(?) Do you want to scan this directory (y/n)? y

-----------------
END_TIME: Tue May  3 07:15:27 2022
DOWNLOADED: 9224 - FOUND: 3
```

Realizamos el escaneo web de forma recursiva con dirb, conseguimos descubrir que existe robots.txt.

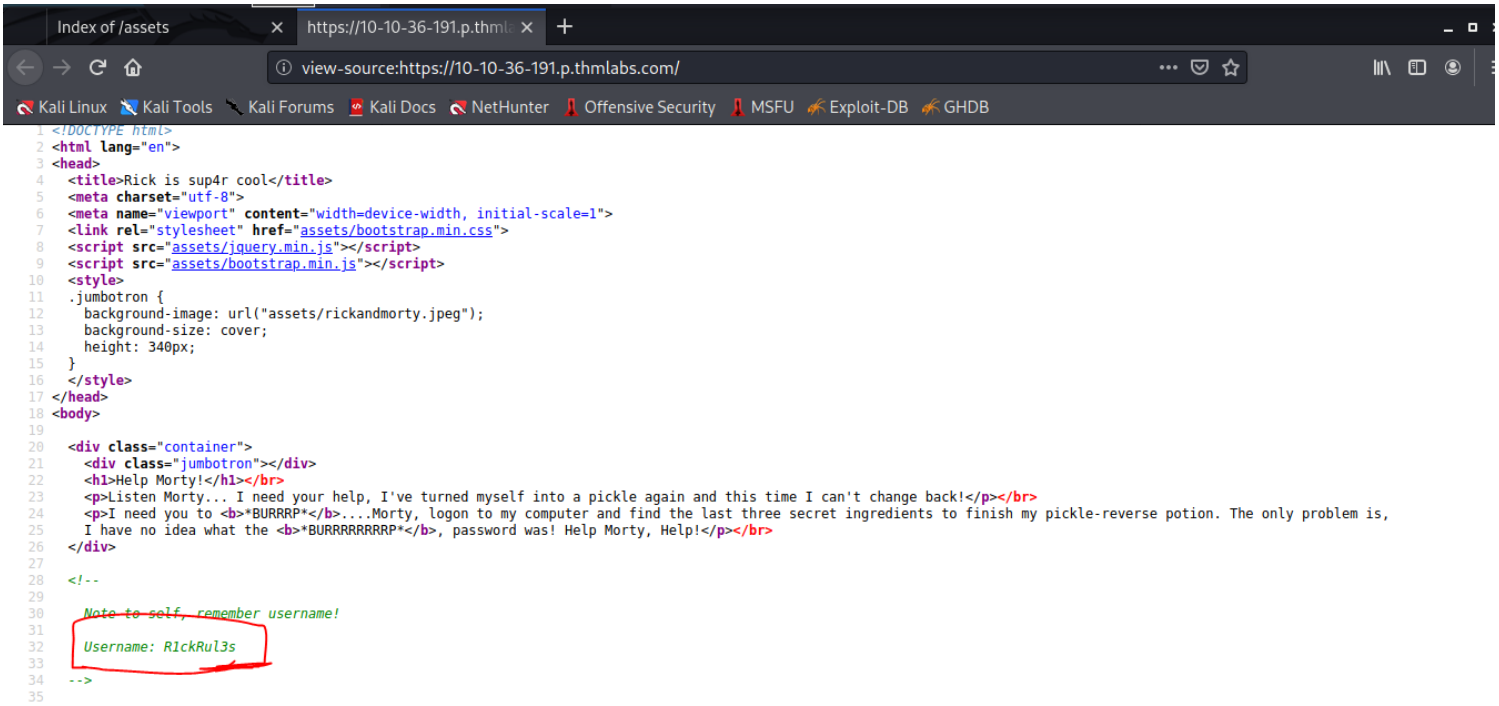
Ahora ejecutamos DirBuster en su versión gráfica para obtener los resultdamos de forma más clara:



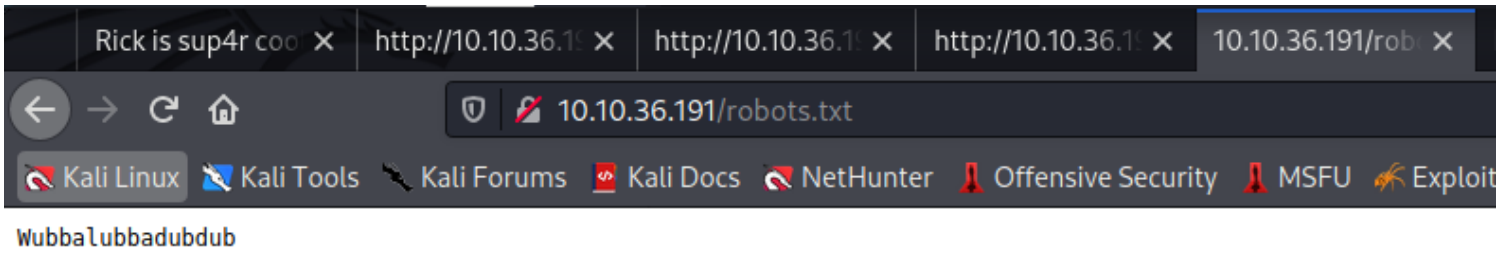
Obtenemos login.php y portal.php que pueden ser interesantes para la explotación de la máquina.

Exploitation

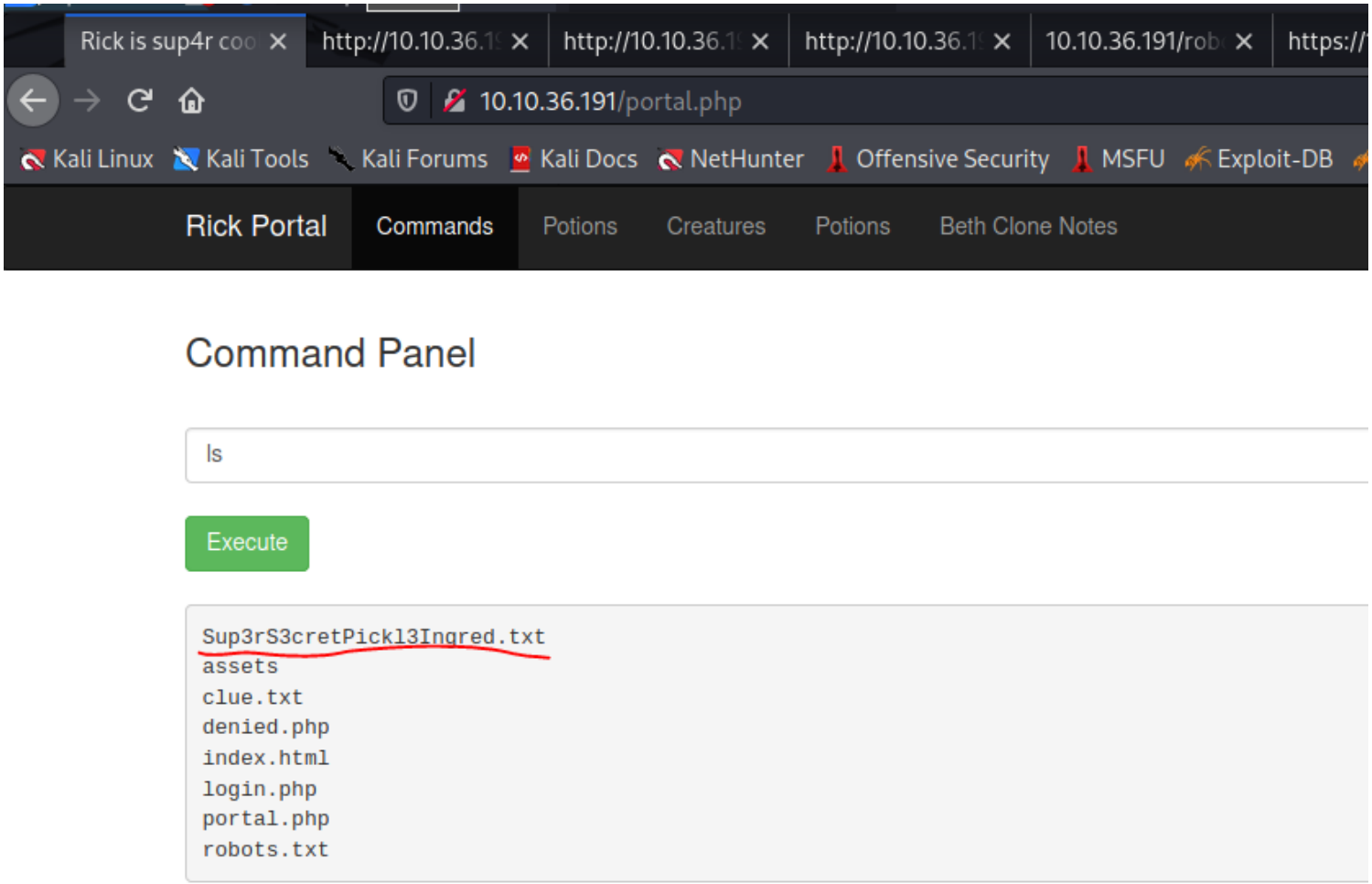
Si analizamos el código fuente de la página encontramos un username:



En robots.txt encontramos lo siguiente:

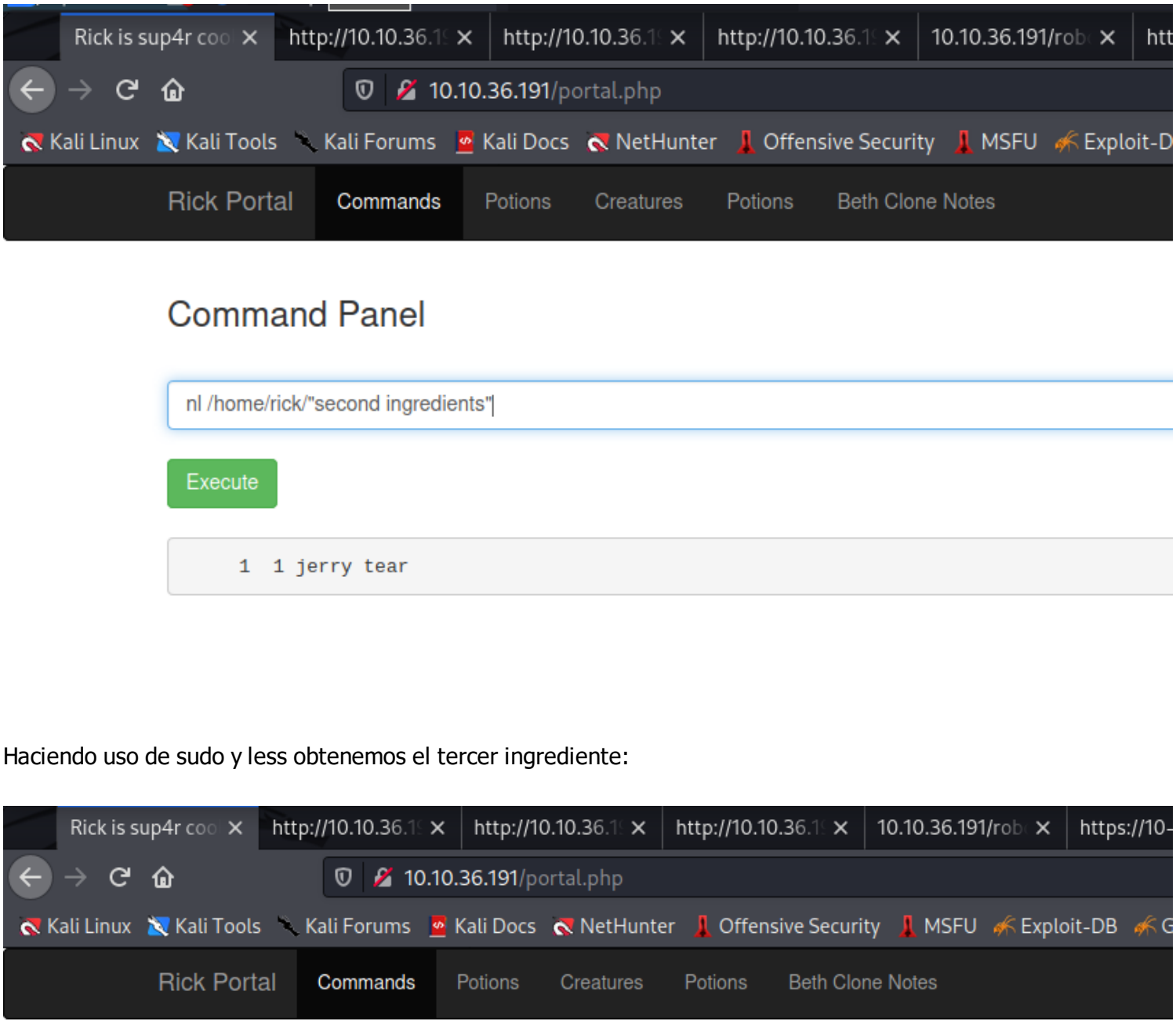


Accediendo a portal.php, tenemos acceso a una terminal que nos permite la ejecución de comandos:



Aquí encontramos el primer ingrediente de la máquina de THM.

Esta terminal no permite la ejecución del comando cat ni otros similares, así que hacemos uso de nl para obtener el segundo ingrediente:



Haciendo uso de sudo y less obtenemos el tercer ingrediente: