🏴‍☠️ Write-Up: Máquina "Pickle Rick"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

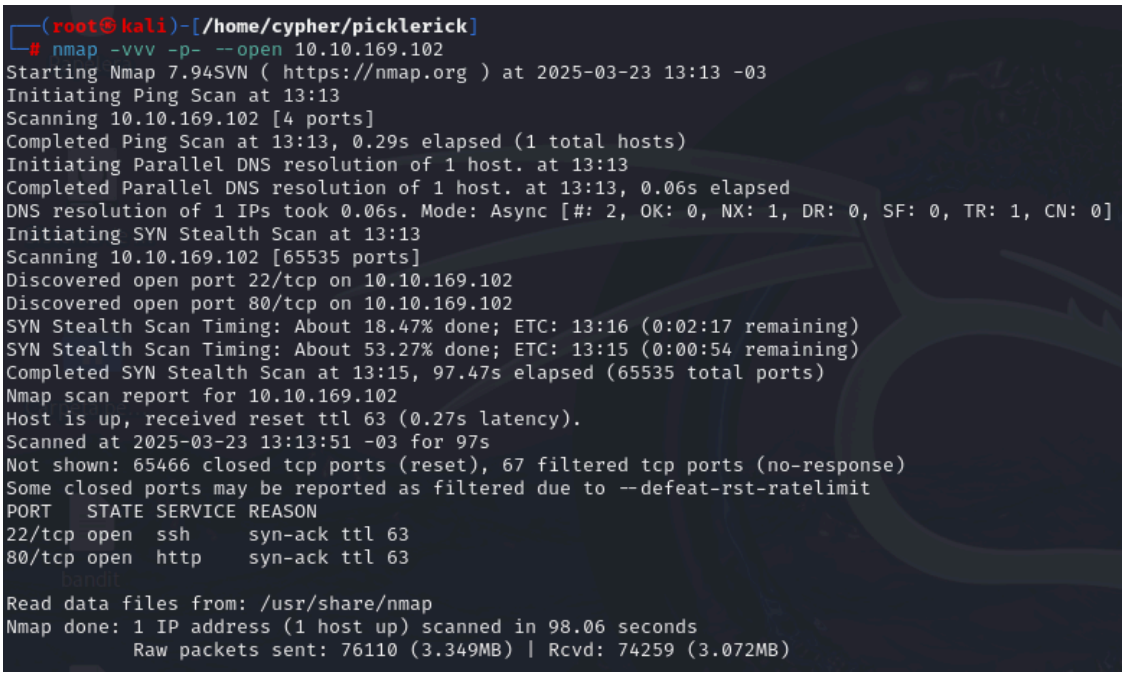
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **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.



🎯 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:f8:79:8c:8e:ed:0a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDW0SKZ3q9WBOku9wumrcqNcldXKrvkw3fxHF2mEKRJMKUdU/AEEAVXvIlNtV4ue+Eb4B/6JzVyXCP0eUuIdxEtNrshgJ7A3mPXDZik5Rri5LU7hTGdh8DzRhqLUrFB
AscmNVFRQRTjSH4QHeIhlXP3xRli4Jw1z6J8qug5g8kUUpMS952AJ56A2WPim2csCUdu8KvhGvf5Sk6Iil5kqvUlz0nM1IVhqA7Uk9phqsKvWGNhFMzCBP3OgT2Jj5pi9AAgL1jUsDyEXhhsxJbuACJ6sUHB6gZnyJwTMt
2+iLqpoKqkRo2mYqbnRfikcjjBAU8cx179pjtAMucWJ1lQZFzdUc9pNI+J4B7d5rtXFXP7xgLW9PjGQZrSFgEp0SEI3OY4FBd+KtSXvxbmtbrtx74Xyn6CavVYPDpK4SEm02rNQMS6Ln6J1OpLfF1ob3GqH09aKDCPbXbf
Iz6Qp/xjnPoknge UpKN17pw/aFv0TGIQYpkuklq59BpaoGBVZD9uFQk=
|   256 1b:6c:d7:e0:77:9b:ad:96:e6:97:60:eb:56:de:b4:a3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDB5cEvLB8vZVzJoDc4i55LGGudaD8pCsi0sHHoA8entKbBV7h7LeTrpovvDOHxoyB27zji7DCqb6o/ct+ObSYE=
|   256 04:89:84:88:b3:b8:35:a7:f4:c7:d3:58:6a:00:eb:50 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMkub0fvLFzfipQj7H+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, Sc
ript, 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]
```

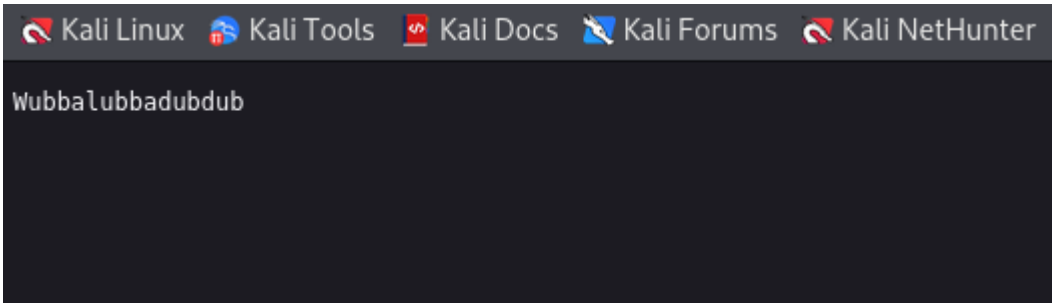
Uso **nikto** para buscar más información relevante en la web.

```
┌──(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: htt
ps://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.

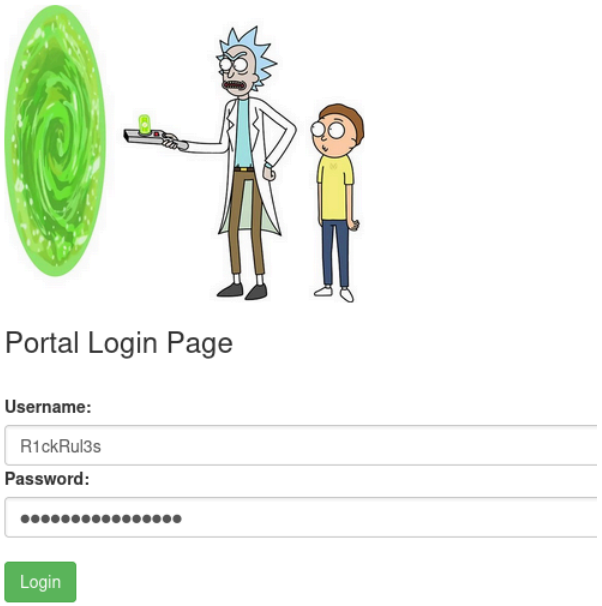
```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <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>
    <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>*BURRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

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

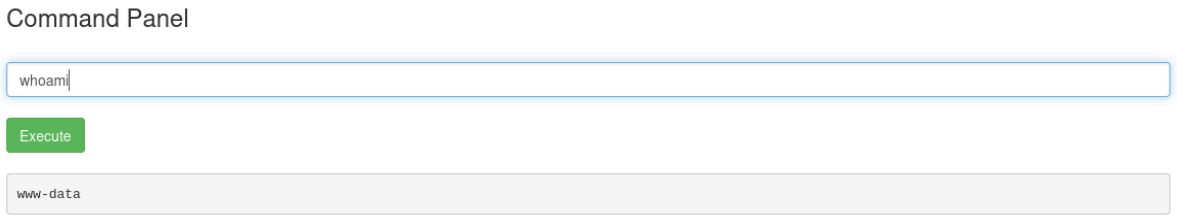


💥 3. Explotación de Vulnerabilidades

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

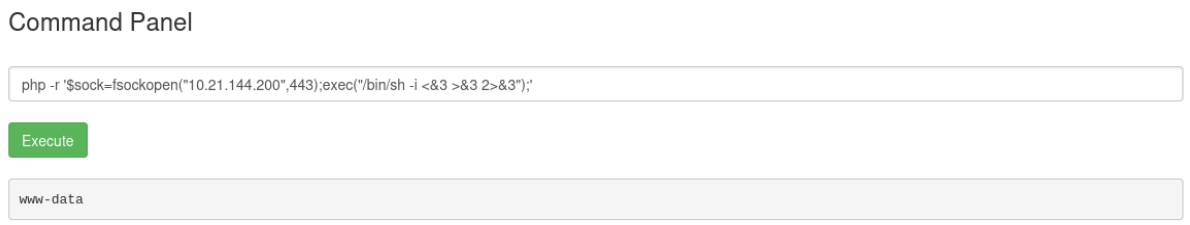


Inicio de sesión exitoso. Ahora busco un panel de comandos. Ingreso whoami para ver si me entrega el usuario actual en la máquina. Y efectivamente, me da el usuario www-data. Puedo usar este panel de comandos para ejecutar algún comando que me sirviese para hacer una reverse shell.



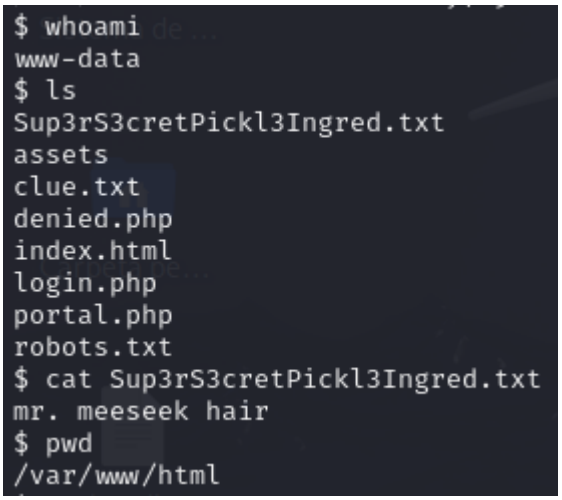
En mi máquina me pongo a la escucha en el puerto 443 para recibir la conexión.

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.

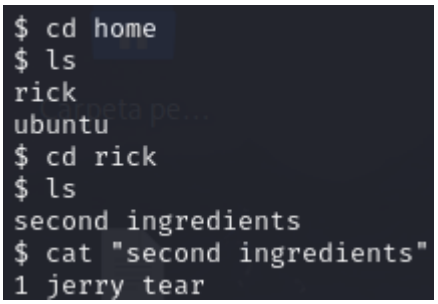


🔐 4. Escalada de Privilegios y Post-explotación

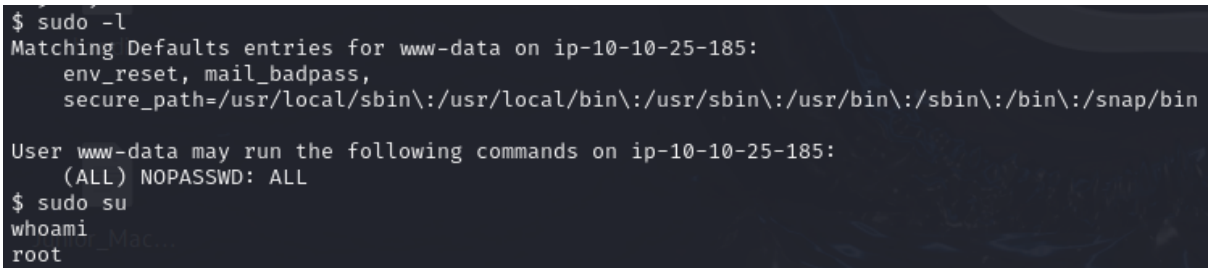
Luego de la ejecución del comando anterior, se recibe la conexión en el puerto 443 de mi máquina, lo cual me da acceso a una terminal simple. Busco el ingrediente.



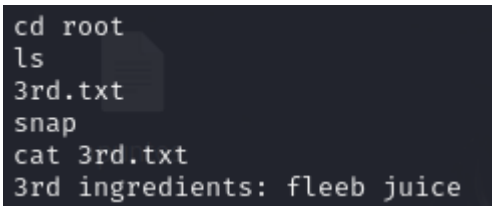
Busco el segundo ingrediente



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.



Busco la última bandera.



🏆 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.