Write-up paso a paso – Máquina Pickle Rick

> **Objetivo:** Acceder al sistema mediante enumeración web, autenticarse en el panel administrativo y obtener los tres ingredientes requeridos demostrando impacto de seguridad.

1. Reconocimiento inicial

Se comienza identificando los servicios expuestos por la máquina objetivo.

Acción

```
nmap -p- -open -sS -sC -sV --min-rate=5000 -n -Pn 10.81.147.24 -oN
escaneo
```

Resultado

Se identifican los siguientes servicios:

- **22/tcp** – SSH
- **80/tcp** – Apache HTTP

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 62 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:20:f2:29:3c:3c:b9:09:ed:ad:b9:3a:b2:78:3e:fd (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDU3ydNDbZqHPvGH5faLiHSVk3gZ3xMDotmR6RTlcLp
XV0q2EK3QfZQEesjwHzOzcIVquTj+H+aBZ7ifb9LtxFH03vNY59tSL5d402FTfkKloQYgtT4
jm4FB1taLkxikqzJ76jlGrzUojRtx26lwd5aXWXQf6kQX6Obn3hJjIAeOR2QpyroQvu6PPLV
```

```
kks+tJTeNcV62sR/KtgdiClTlOaTFSud1OLagTFIygv059IDacLHYpbhHVFIOmk8MDSWK5LU
D3E+6c49bV3Gh4c7kB/MyALJPSF8WKd66Co7PM4YqKqDCYfE1D/q1XaevE+7KP/1XavxbxHN
g3PUt+eraPhevMCh2LkI/o+0dfE1cpbmdECpS1lpohtaK8NqxKNxcbsPvDpH2lo0PvfKtbhv
VRVRlEXPg5f2XeTnYoirHrvBVsLDQIXxCLfNj3iv47BwENaFSWRbPw+iUbJ36o8TEQ2rUDvL
JOX/ZgZG3MFXFLDv18bvdRhnaCIIXkd6jayAMdc=
|   256 99:af:18:5a:a3:29:56:ca:32:d3:ce:2e:94:44:61:3d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJsm0SSjxW4LQRODggen
bVjGO+jKLKj0kYtxc0KcaUvFSunaVBh54/sxIIkQlsJ4Aa3aCPCJ7BqCuqqmqJrCyK8=
|   256 3b:21:72:ce:c5:b0:32:a2:c1:c1:22:bd:64:f5:a4:83 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGVOA2hZAjaDwpavCnI1f9vtWxO8DYuxZ8xYz7iW7f0i
80/tcp open  http    syn-ack ttl 62 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
```

2. Enumeración web inicial

Se accede al servicio web para analizar el contenido visible y el código fuente.

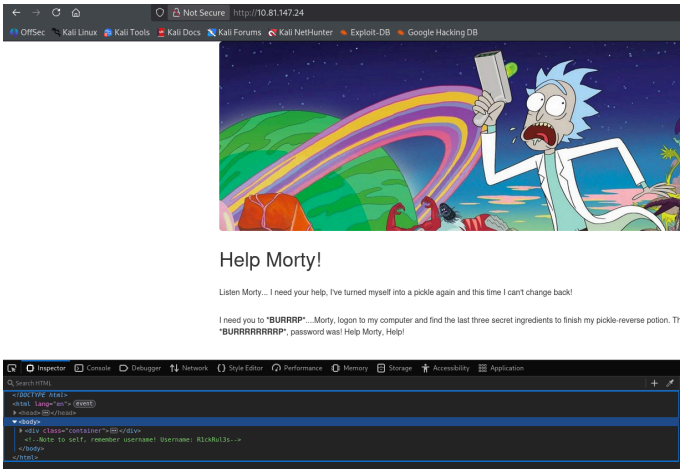
Acción

- Abrir la página principal en el navegador.
- Revisar el código fuente HTML.

Resultado

Se encuentra un comentario HTML con información sensible:

- **Username:** `R1ckRul3s`



3. Enumeración de robots.txt

Como parte de la enumeración básica, se revisa el archivo `robots.txt`.

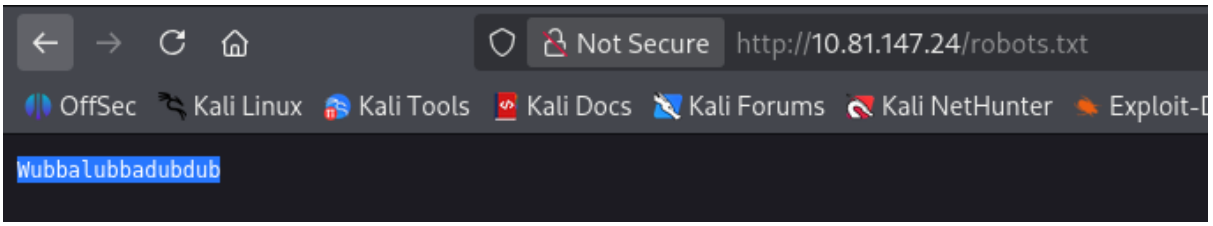
Acción

```
http://10.81.147.24/robots.txt
```

Resultado

Se obtiene una posible contraseña:

- **Wubbalubbadubdub**



4. Acceso al panel de login

Se prueba el acceso a páginas comunes de autenticación.

Acción

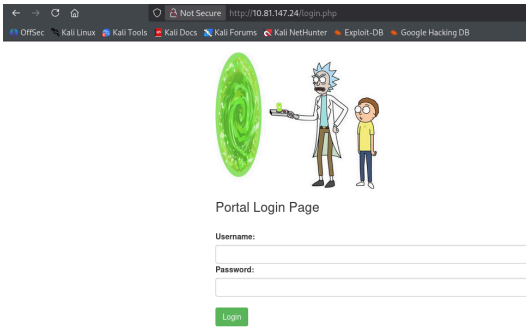
```
http://10.81.147.24/login.php
```

Se utilizan las credenciales descubiertas:

- Usuario: `R1ckRul3s`
- Contraseña: `Wubbalubbadubdub`

Resultado

Acceso exitoso al portal administrativo.



5. Identificación del panel de comandos

Una vez autenticado, se accede a un panel que permite ejecutar comandos del sistema.

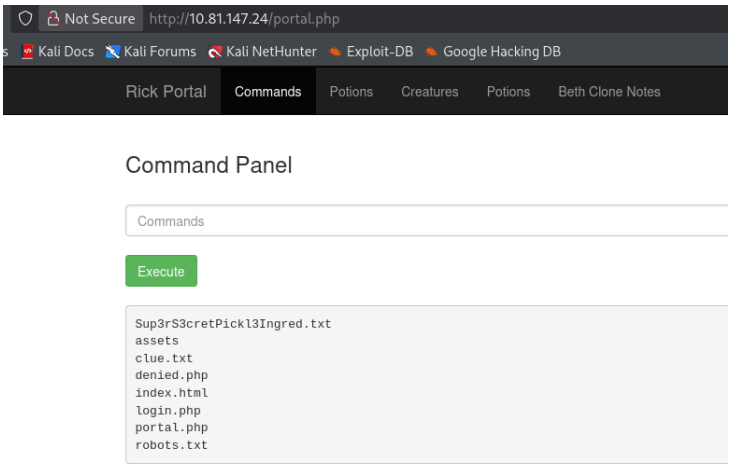
Acción

- Ejecutar comandos básicos como `ls`.

Resultado

Se identifican archivos interesantes:

- `Sup3rS3cretPickl3Ingred.txt`
- `clue.txt`



6. Obtención del primer ingrediente

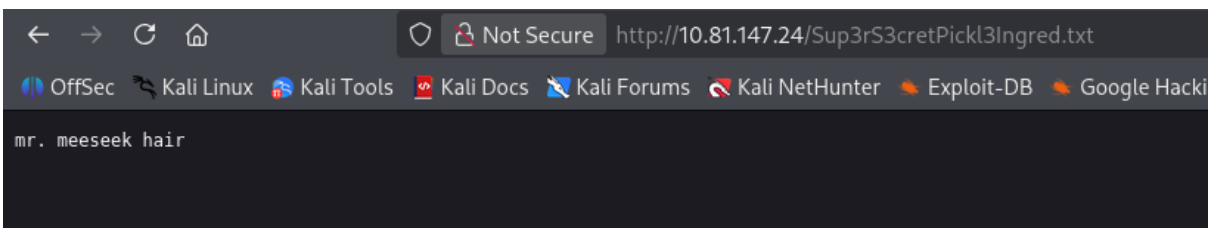
Se accede directamente al archivo desde el navegador.

Acción

```
http://10.81.147.24/Sup3rS3cretPickl3Ingred.txt
```

Resultado

Primer ingrediente: `mr. meeseek hair`



7. Obtención del segundo ingrediente

El archivo `clue.txt` sugiere buscar en el sistema de archivos.

Acción

En el panel de comandos:

```
ls /home/rick
```

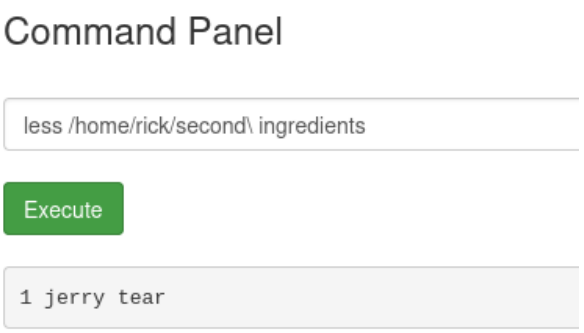
Se encuentra el archivo `second ingredients`.

Debido a restricciones con `cat`, se utiliza `less`.

```
less /home/rick/second\ ingredients
```

Resultado

Segundo ingrediente: `1 jerry tear`



8. Enumeración de privilegios sudo

Se comprueba si el usuario tiene permisos elevados.

Acción

```
sudo -l
```

Resultado

Se confirma que es posible ejecutar comandos como root sin contraseña.

9. Obtención del tercer ingrediente

Con permisos sudo, se accede al directorio `/root`.

Acción

```
sudo ls /root
sudo less /root/3rdingredient.txt
```

Resultado

Tercer ingrediente: `fleeb juice`

Conclusión

La máquina Pickle Rick fue comprometida completamente mediante:

- Exposición de credenciales en código fuente y archivos públicos.
- Panel web con capacidad de ejecución de comandos.
- Uso indebido de privilegios sudo.

Este laboratorio demuestra cómo errores básicos de configuración pueden permitir a un atacante comprometer información sensible sin necesidad de exploits avanzados.