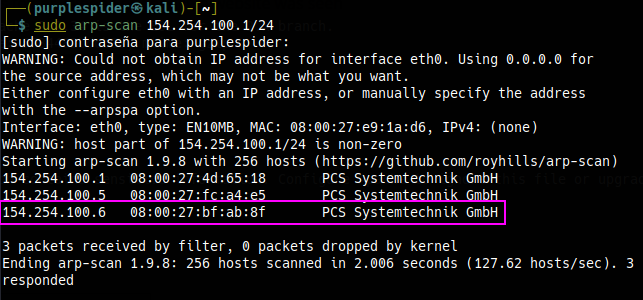
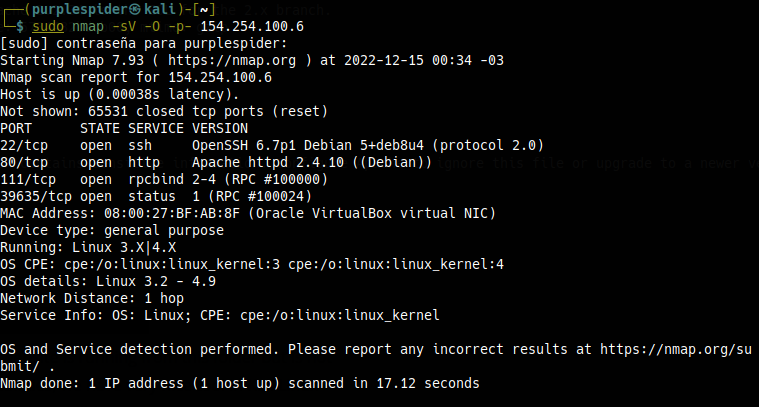
**Raven1 Walktrought CTF**

Como primer paso realizamos un escaneo a nuestro rango de red mediante la herramienta arp-scan al gateway de la red, en este caso 154.254.100.1/24

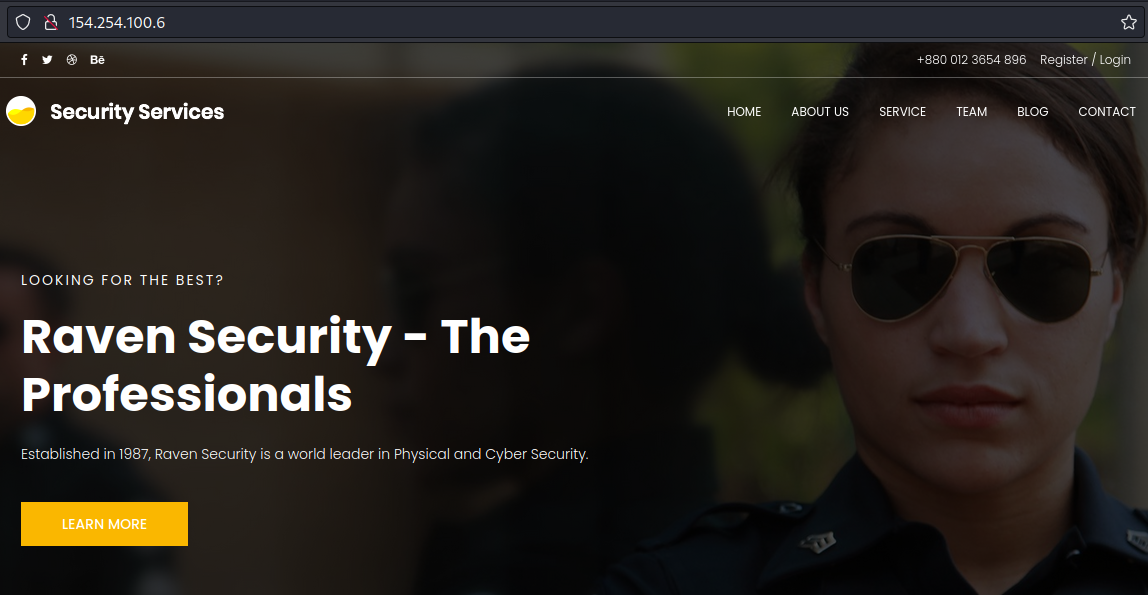


Una vez identificadas los distintos dispositivos, encontramos una IP nueva.

Realizamos un escaneo mediante la herramienta nmap a la IP 154.254.100.6 para revelar los puertos que tiene abiertos.



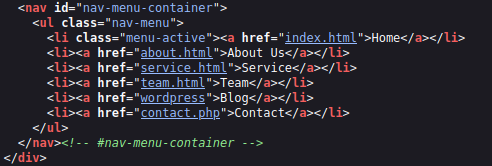
Ya verificados comenzamos a revisar los puertos en el navegador web, partiendo por el puerto 80, que es el que por defecto nos envía a la web del host ingresado.



Al revisar la página nos damos cuenta que posee diversos links de redireccionamiento, por lo que decidimos revisar el código fuente para encontrar posibles vectores de ataques o pistas para lograr nuestra meta. Esto lo realizamos dando click derecho en cualquier posición de la página y seleccionamos la opción “view page source” o “ver código fuente”.



Revisando el código encontramos redireccionamientos que nos llevaran a distintas URLs que podrían ser vectores de ataques.



La más atractiva es la de wordpress, ya que podríamos tener acceso a la administración de la web, por ende a la administración del host.

Bajo esto es que le damos ctrl más click izquierdo del mouse sobre la sentencia “wordpress” para ingresar a la URL que tiene asociada, lo que nos redireccionará a view-source:http://154.254.100.6/wordpress/ pero para ingresar realmente a la web debemos retirarle el view-source:



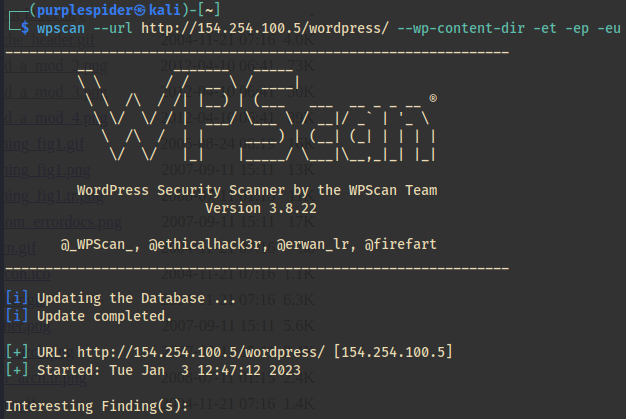
Ahora que tenemos claro que existe un wordpress, buscaremos sus vulnerabilidades con la herramienta wpscanner, la que nos permitirá identificar vectores de ataque para obtener la información que requerimos.

Para esto utilizamos el comando **wpscan --url http://192.168.1.14/wordpress --wp-content-dir -ep -et -eu**

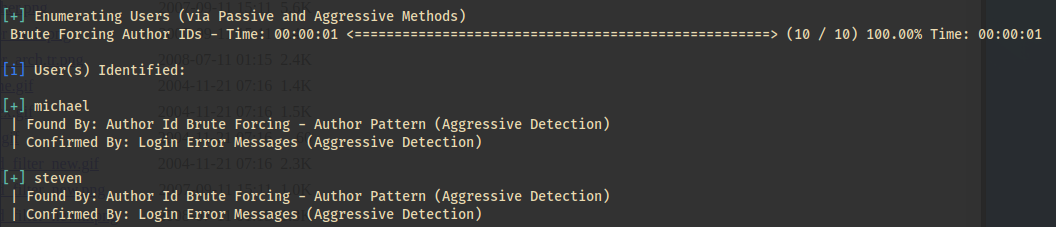
**-ep** nos servirá para enumerar plugins de wordpress que puedan presentarse como vectores de ataque

**-et** nos servirá para enumerar temas de wordpress que puedan presentarse como vectores de ataque

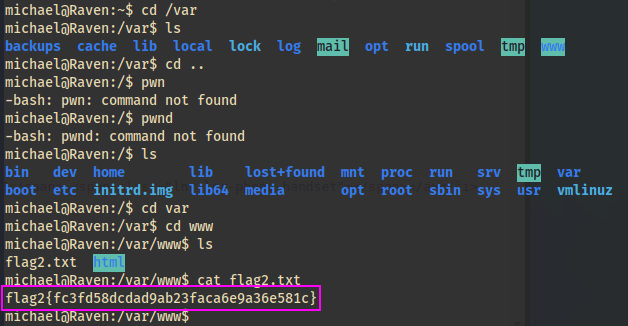
**-eu** nos servirá para enumerar usuarios que tengan algun registro dentro del sitio escaneado



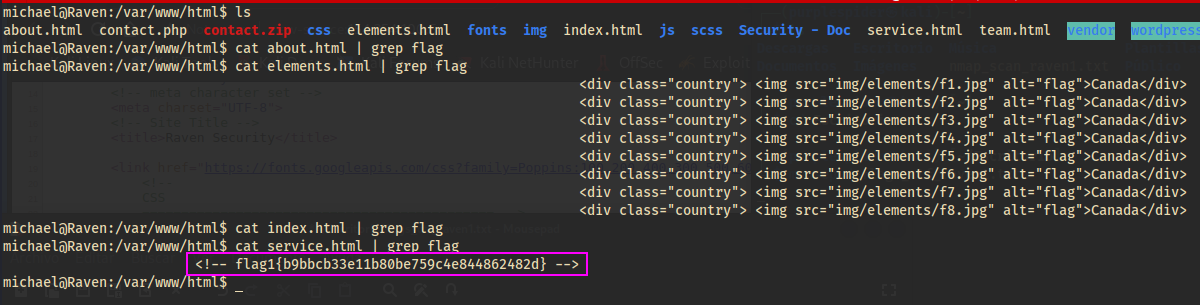
Encontrando dentro de la enumeración de usuarios dos que podemos ocupar para ingresar a sus cuentas ssh mediante fuerza bruta.



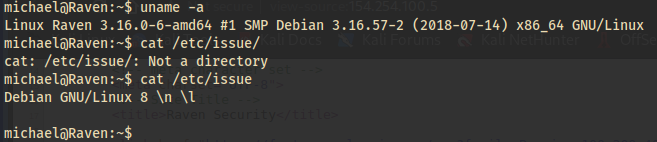
Identificamos los usuarios Steven y Michael, ambos serán nuestros dos vectores más atractivos como vulnerabilidades. Primero utilizo a la cuenta “steven” con la clave “steven” pero no logramos tener acceso, pero al intentar con “michael” y clave “michael” si que logramos tener acceso a los directorios del servidor ssh habilitado para ese usuario. Ya dentro fue cuestión de estar navegando entre los distintos directorios del servidor para dar con una flag, específicamente la flag2



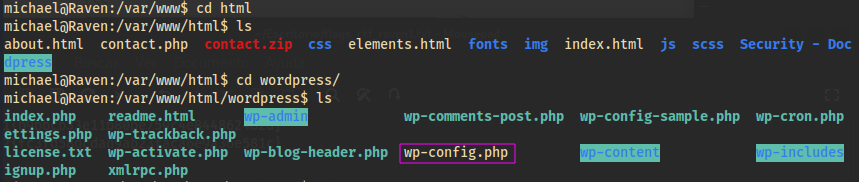
Igualmente, en la misma carpeta /var/www hay un directorio html al cual ingresamos y comenzamos a buscar mediante el comando cat en cada archivo html con un “| grep flag” alguna posible nueva flag, y para nuestra sorpresa encontramos una en el archivo service.html, correspondiente a la flag1

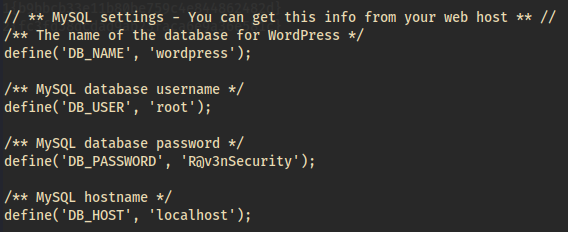


Ahora que ya tenemos 2 de las 4 flag a encontrarse en este desafío es que intentaremos obtener acceso bajo root, para esto primero debemos conocer el sistema operativo y la versión de kernel de la maquina víctima, así podremos averiguar por posibles vulnerabilidades o exploits que pueda llegar a poseer. Para esto corremos un par de comandos. El primero **uname -a** que nos dirá la versión de kernel y **cat /etc/issue** que nos traerá la versión de SO

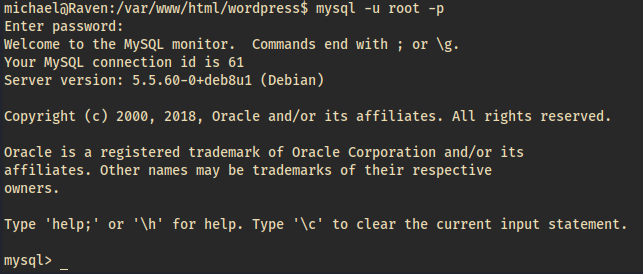


Bajo lo observado en estas consultas es que no encontré ninguna vulnerabilidad o posible exploit relacionadas a estas características, así que decidí volver al directorio /var/www/html y esta vez a ingresar dentro del directorio wordpress, ya que dentro de sus archivos muy posiblemente estén las credenciales de la base de datos del wordpress. Asi que dentro del directorio /var/www/html/wordpress/ encontramos el archivo wp-config.php el que leemos mediante el comando cat y efectivamente encontramos las credenciales de la base de datos.

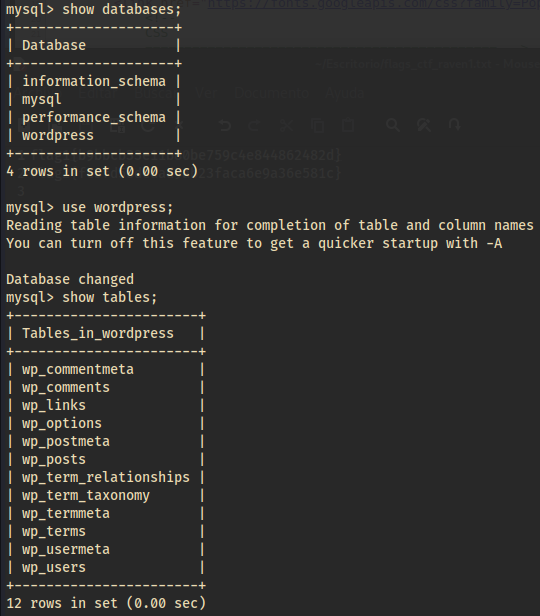




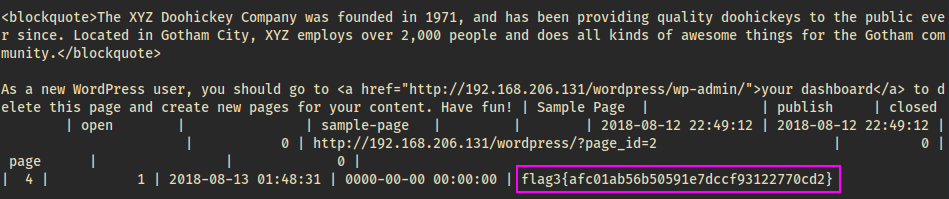
Ya con las credenciales damos ingreso a la base de datos todavía dentro del usuario Michael bajo el comando **mysql -u root -p**



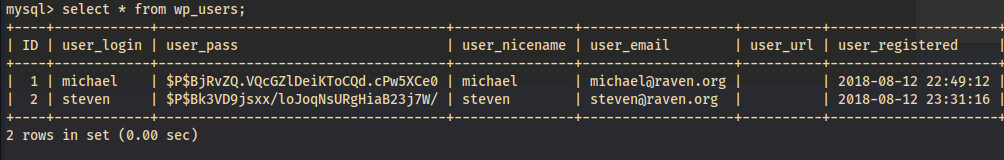
Como siguiente paso identifico las bases que existen, utilizo la base de worpress y veo las tablas que contiene, todo con sentencias SQL.



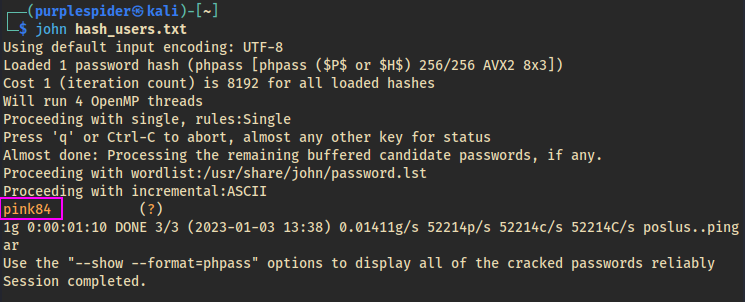
Fui probando las distintas tablas, buscando información hasta que en la tabla wp\_posts se encuentra la flag3.



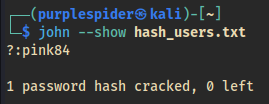
Ya sabiendo que existe la tabla wp\_users dentro de la base de datos de wordpress, entonces procedemos a ver la información que hay dentro de esta tabla mediante la sentencia (query) **select \* from wp\_users;** y gracias a esto conseguimos la clave de ingreso de Steven, pero encriptada



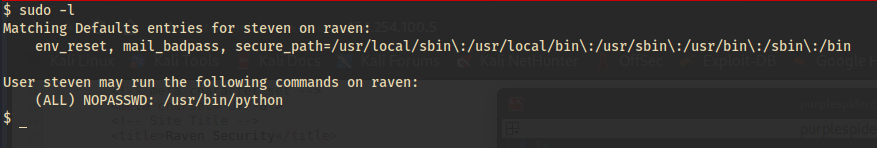
Para desencriptarla procederemos a utilizar la herramienta John The Ripper, primero guardando la clave encriptada en un txt, para luego utilizar la herramienta con el comando **john hash\_users.txt** y una vez ejecutado el comando podemos ver que la clave del usuario Steven es pink84



Esto se puede verificar igualmente con el comando **john --show hash\_users.txt**



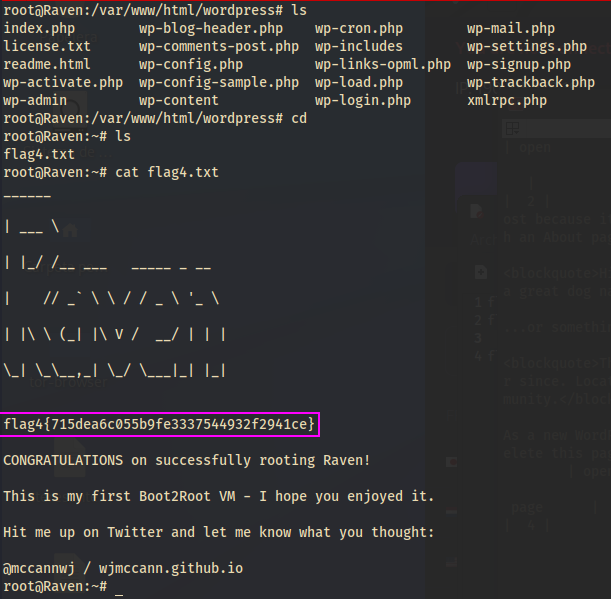
Con toda la información extraída, damos ingreso mediante ssh al usuario steven y ejecutamos el comando sudo -l para ver que utilidades o herramientas podemos utilizar bajo el usuario root, de esta manera descubrimos que se puede correr Python



Sabiendo esto, utilizamos el comando para tomar acceso al usuario root mediante el comando **sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’**



Ahora ya dentro de root, nos movemos al directorio base y descubrimos la última flag que nos faltaba, finalizando así este Capture The Flag.



*FIN*.