Final Report

**Group 7**

Offensive

horizontal line

# Red Team: Summary of Operations

#### Table of Contents:

* Exposed Services
* Critical Vulnerabilities
* Exploitation

## Exposed Services

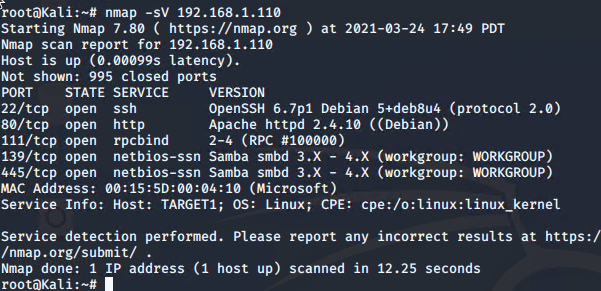
Nmap scan results for each machine reveal the below services and OS details:

```bash

$ nmap -sV 192.168.1.0/24

```

Output:



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

- Target 1

- Port 22 (SSH)

- Port 80 (HTTP)

The following vulnerabilities were identified on each target:

- Target 1

- Wordpress scan identified users

- User “michael” has the same password as his user name

- Mysql log in for root was listed in plain text in “wp\_config.php” file

- Port 22 was listening to any IP address

- SSH with password capable

- Steven can run python with sudo privileges without needing a password

## Exploitation

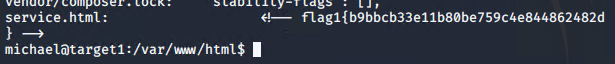
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Flag 1 {b9bbcb33e11b80be759c4e844B62482d}

Exploit used: Grep -ER flag

Since Apache by default saves to “/var/www/html”, running the above

command will show flag 1. (See below screenshot)



- Flag 2 {fc3fd58dcdad9ab23faca6e9a36e581c}

Exploit used: find /var/ -type f -iname “flag2”

Following a similar train of thought as finding flag 1, flag 2 was found 1

One directory higher. (See below screenshot)

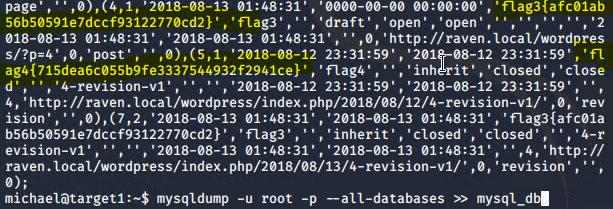


- Flag 3 and 4

Exploits used: There are 2 ways to get these at the same time using the “mysql”

database.

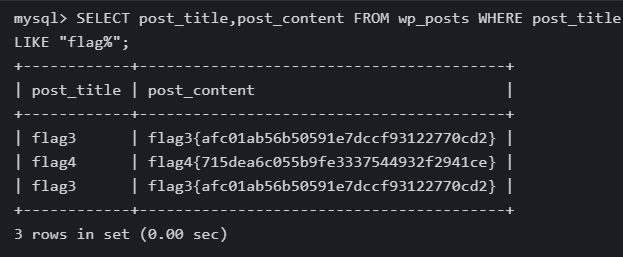
Method 1: mysqldump -u root -p --all-databases >> mysql\_db.txt (enter password when prompted. Password was obtained through the “wp\_config.php” file). Next: cat mysql\_db.txt | grep flag (See below screenshot)



Method 2: mysql> SELECT post\_title,post\_content FROM wp\_posts WHERE

post\_title LIKE “flag%”; (This is done from a “mysql” interface. See below

screenshot.)



This concludes the collection of sensitive files on the Target 1 machine.