**Red Team: Summary of Operations**

**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation
* References

**Exposed Services**

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

$ nmap -sV 192.168.1.\*

Target 1 IP determined to be 192.168.1.110.

A screen shot of a computer

Description automatically generated with low confidence

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

* Target 1
  + Port 22 – SSH access
  + Port 80 – HTTP access
  + Port 111 – RPC (Remote server access)
  + Ports 139 & 445 – NetBIOS (LAN access)

**Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

* Target 1
  + Lack of updated software
    - The version of OpenSSH found on the target is vulnerable to numerous exploits including Username Enumeration (CVE-2018-15473)1
    - Apache server is running older version of the software vulnerable to significant exploits including2:
      * CVE-2019-0217: Access control bypass, allowing for alternate username authentication and overriding access controls
      * CVE-2017-9788: Memory pool leak, potentially exposing critical data
      * CVE-2017-3167: Authentication bypass
    - Wordpress server was also running out of date software vulnerable to detailed site enumeration via wpscan

A picture containing text, plaque

Description automatically generated

* + Weak passwords
    - The user account “michael” had a very weak password capable of being exploited through manual brute force attack
    - The user account “steven” also had a fairly weak password that was subject to an automated brute force attack
  + Unsalted SQL credentials
    - The SQL credentials were found through an unencrypted file listed in /var/www/html/wp-config.php

A picture containing text, screen, screenshot

Description automatically generated

* + Unsalted hashed passwords
    - When the SQL database was breached user passwords were found with an unsalted hash, leaving them subject to cracking through tools such as John

Graphical user interface, text

Description automatically generated

* + Privilege escalation
    - Once logged into the system through the ‘steven’ username, escalation to root privileges was performed via a python script

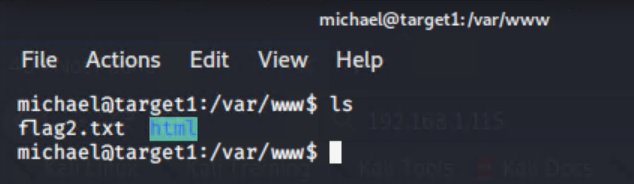
**Exploitation**

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

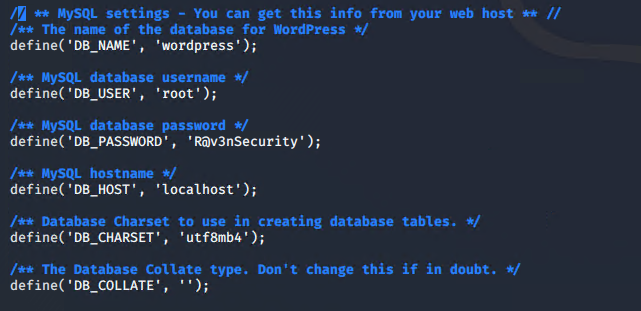
* Target 1
  + flag1.txt: b9bbcb33e11b80be759c43844862482d
    - **Exploit Used**
      * Utilizing wpscan, we enumerated the wordpress site containing the usernames for the computer, exposing “michael” and “steven”
      * Michael’s password was brute force guessed manually (password: michael) and allowed access to the file structure of the system
      * Flag1 was found among a file called “setup.html”



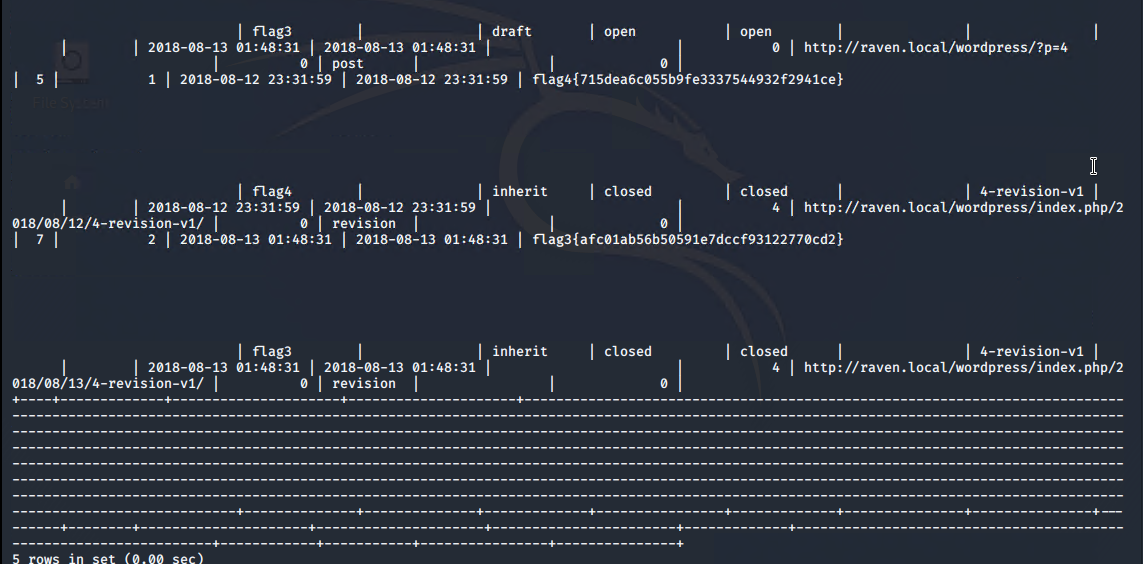
* + - * ssh michael@192.168.1.110
  + flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
    - **Exploit Used**
      * Through directory traversal via the “michael” username, flag2 was found in the /var/www/html directory

**

* + Flag3.txt: afc01ab56b50591e7dccf93122770cd2
    - **Exploit Used**
      * While doing directory traversal, the file “wp-config.php” listed unencrypted SQL credentials
      * Using these credentials, the database was accessed and a file containing the flag 3 information was found



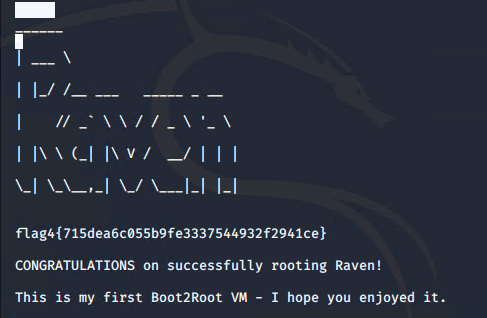
* + - * 1. $mysql -u root -p
        2. Mysql > show databases;
        3. Mysql > use wordpress;
        4. Mysql > show tables;
        5. Mysql > select \* from wp\_users;



* + Flag4.txt: 715dea6c055b9fe3337544932f2941ce
    - **Exploit Used**
      * After finding flag 3, the user account ‘steven’ was logged into



* + - * Account permissions revealed the user could execute python scripts, including ones that escalated to the root user
        1. sudo python -c ‘import pty;pty.spawn(“/bin/bash”)



**References**

* + - * 1. <https://nvd.nist.gov/vuln/detail/CVE-2018-15473#vulnCurrentDescriptionTitle>
        2. <https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=apache+server&search_type=all&isCpeNameSearch=false>