**Red Team: Summary of Operations**

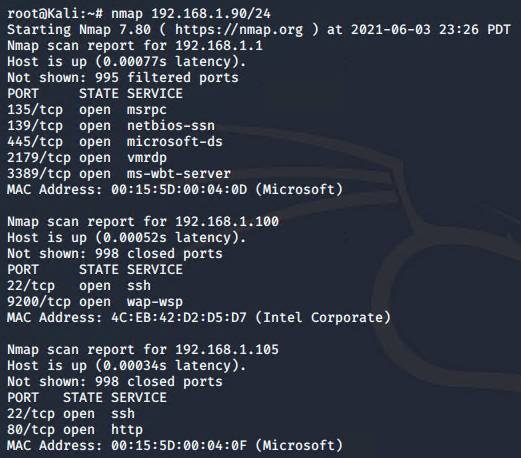
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

**Exposed Services**

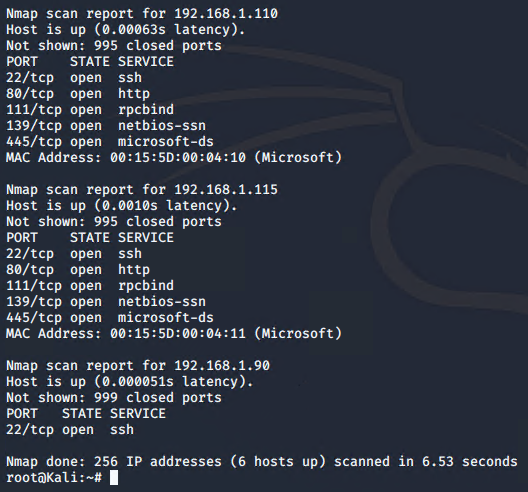
Nmap scan results for each machine reveal the below services and OS details:

$ nmap 192.168.1.90/24



NOTE: Results continue on next page.

**Exposed Services (con’t)**



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

**Target 1**

List of exposed services for Target 1 (192.168.1.110):

* Port 22
  + The ability to remotely connect to a machine.
* Port 80
  + Traffic coming from port 80 can contain attacks such SQL injections, cross-site scripting, cross-site request forgeries.

**Critical Vulnerabilities**

The following vulnerabilities were identified on each target.

**Target 1**

List of critical vulnerabilities:

* Outdated Resources/Software
* Unlimited Authentication
* Sensitive Information Access
* Plaintext Storage of Passwords
* MySQL Server Access
* Brute Force Attacks
* Improper Privilege Management

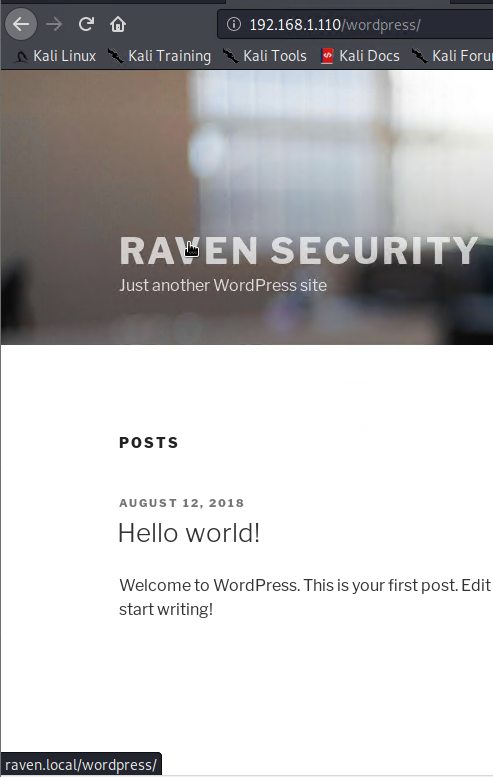
**Exploitation**

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

**Outdated Resources/Software:**

The Red Team was able to enumerate usernames from the WordPress site.

Since Target 1 was a vulnerable WordPress site, it was easy to locate the URL.



* When a cursor was placed over the ‘Raven Security’ name image, the URL for this WordPress site was visible at the bottom, left corner of the website.

URL: http://raven.local/wordpress

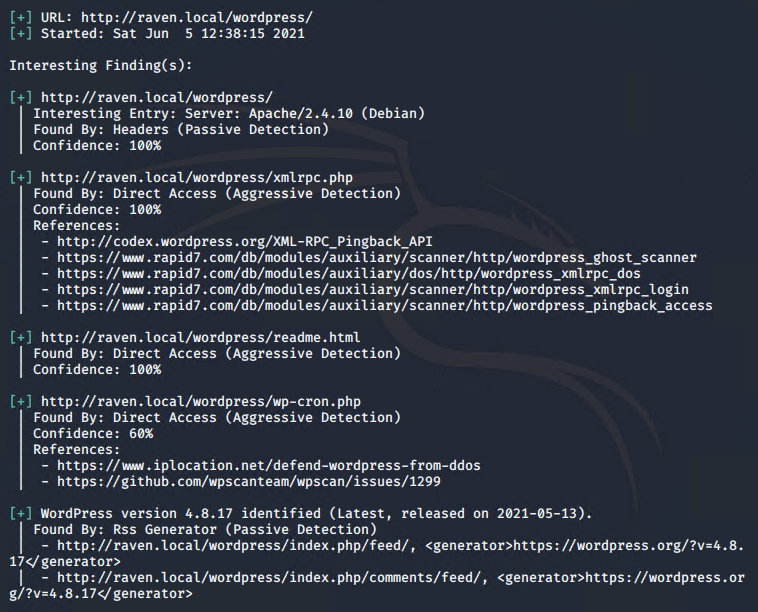
**Exploitation (con’t)**

**Outdated Resources/Software: (con’t)**

Enumerating the WordPress site resulted in the following information:

* Interesting findings.



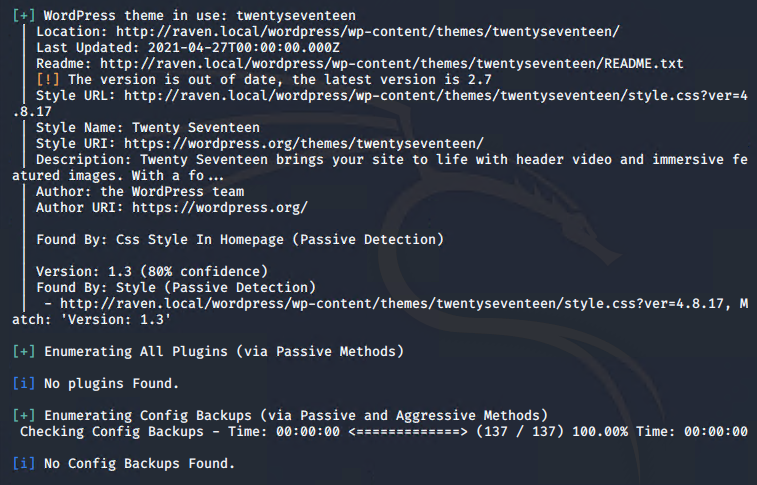


Results of output continues below.

**Exploitation (con’t)**

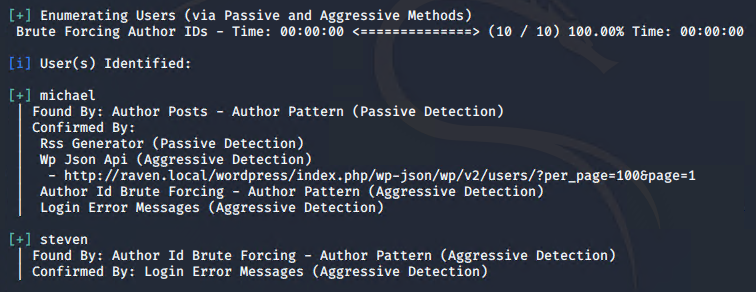
**Outdated Resources/Software: (con’t)**

* Interesting findings. (con’t)



* Identifying usernames.



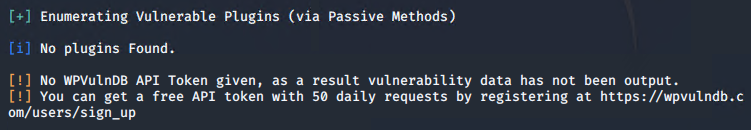


**Exploitation (con’t)**

**Outdated Resources/Software: (con’t)**

* Identifying plugins.

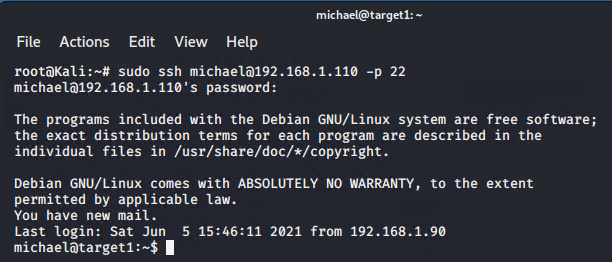




**Unlimited Authentication:**

The Red Team had unauthorized access to a remote host.

Ability to SSH into the Target 1 machine by guessing user Michael’s password.



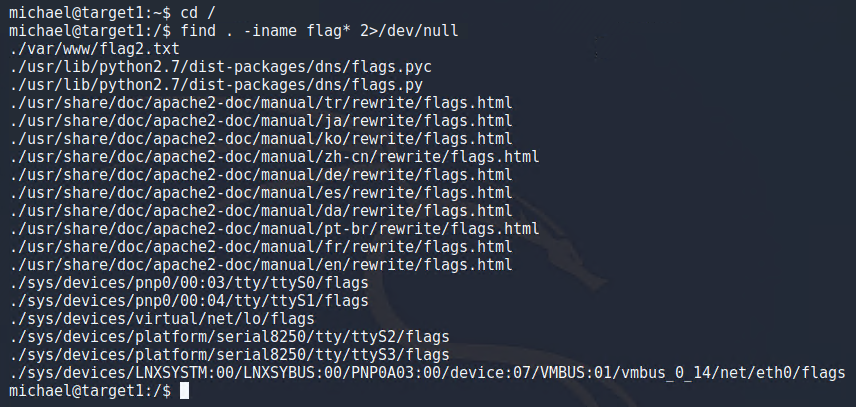
* The Read Team guessed Michael’s password to be ‘michael’.

**Exploitation (con’t)**

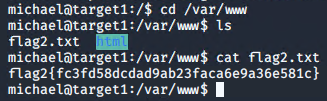
**Sensitive Information Access:**

After logging into Michael’s account, the Red Team had the ability to access sensitive information.

To find the ‘flag2.txt’ file:



Contents of ‘flag2.txt’:

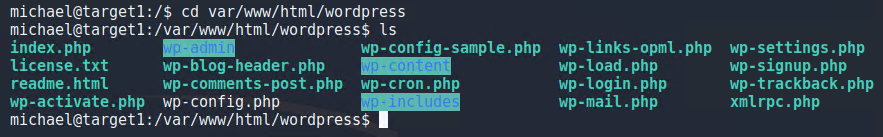


**Exploitation (con’t)**

**Plaintext Storage of Passwords:**

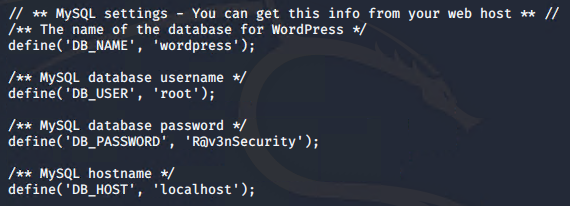
While still logged in as Michael, the Red Team was able to retrieve the WordPress user password hashes to log into a MySQL server.

Finding the MySQL database username and password:



Contents of the wp-config.php file which contained the plaintext password of the MySQL database:

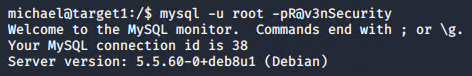




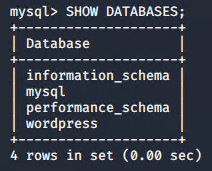
**Exploitation (con’t)**

**MySQL Server Access:**

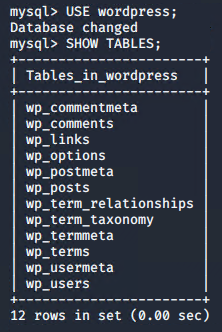
The Red Team was able to successfully log into a MySQL server.



Queried what databases were stored in this server:



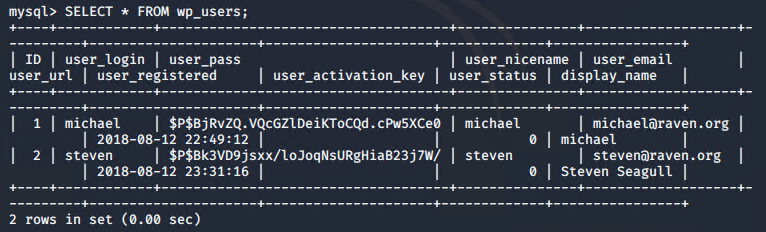
Accessed ‘wordpress’ database to query available tables:



**Exploitation (con’t)**

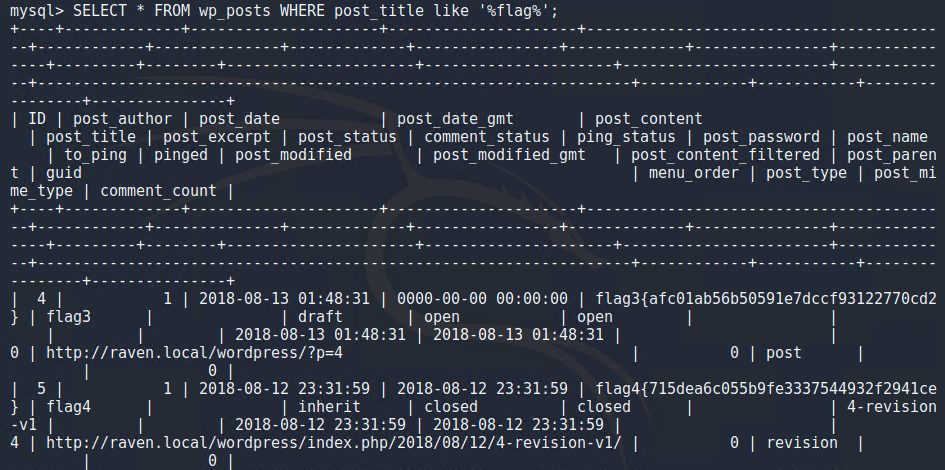
**MySQL Server Access: (con’t)**

Queried ‘wp\_users’ table to retrieve WordPress user password hashes:



Since the Red Team had access to the MySQL server, they viewed the contents of some of the tables from the ‘wordpress’ database to see if they could find other sensitive information.

From the ‘post\_title’ column of the ‘wp\_posts’ table, two flags were found.



Contents of ‘flag3’ and ‘flag4’:

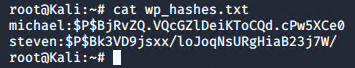
* flag3{afc01ab56b50591e7dccf93122770cd2}
* flag4{715dea6c055b9fe3337544932f2941ce}

**Exploitation (con’t)**

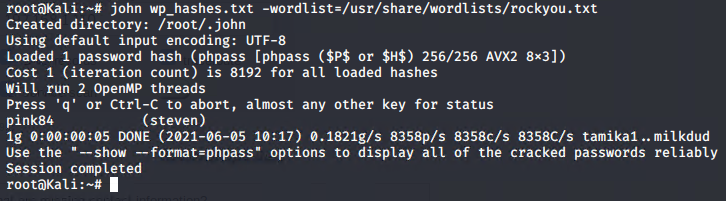
**Brute Force Attacks:**

The Red Team performed a brute force attack on the WordPress password hash values using ‘John The Ripper’.

A text file containing the hash passwords for Michael and Steven were first created.



Brute forced the passwords using ‘John the Ripper’.

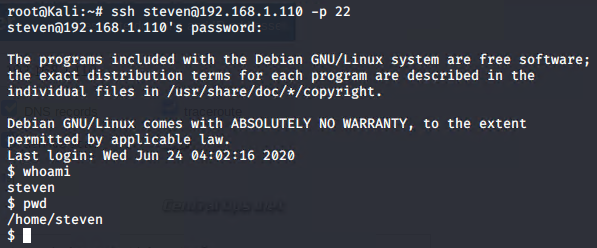


* The password for Steven was cracked.

**Improper Privilege Management:**

The Red team had the ability to elevate a user’s privilege to ‘root’.

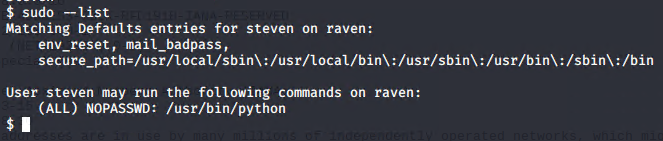
After cracking the password for Steven, they ssh’d into the Target 1 machine as Steven.



**Exploitation (con’t)**

**Improper Privilege Management: (con’t)**

Steven had the following ‘sudo’ privileges:

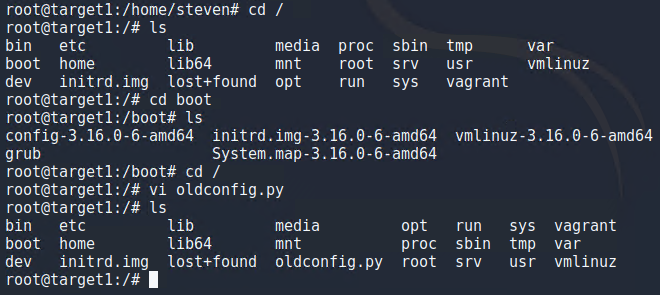


* Steven has access to Python.

To escalate access as ‘root’, the Read Team spawned a shell by creating a bidirectional communication channel through a pseudoterminal (pty) to execute the ‘/bin/bash’ command.



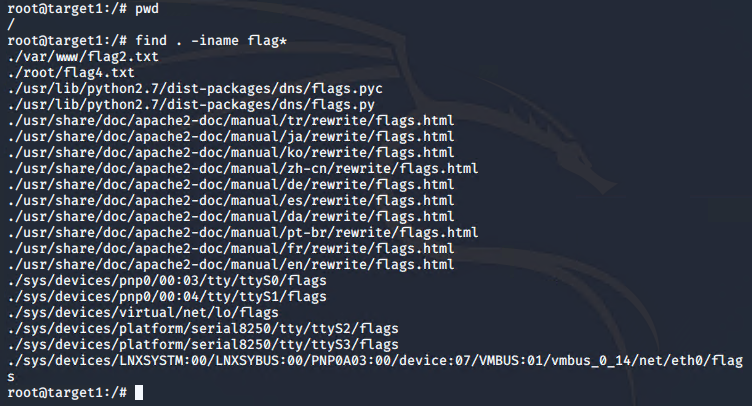
As ‘root’, they were able to move around the system, list contents of directories and even create a malicious script.



**Exploitation (con’t)**

**Improper Privilege Management: (con’t)**

The location of the ‘flag4.txt’ file was found:



**Exploitation (con’t)**

**Improper Privilege Management: (con’t)**

Contents of ‘flag4.txt’.

