SSH Tunnel

Server:
Instalamos mysql-server

```
root@debian:/home/chaos# apt-get install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libaio1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18
  libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server-5.5
  mysql-server-core-5.5
Suggested packages:
  libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl
  libipc-sharedcache-perl tinyca
The following NEW packages will be installed:
  libaio1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18
  libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server
  mysql-server-5.5 mysql-server-core-5.5
0 upgraded, 11 newly installed, 0 to remove and 196 not upgraded.
Need to get 8,715 kB of archives.
After this operation, 96.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Nos conectamos a la base:

```
root@debian:/home/chaos# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.54-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

Creamos el usuario y damos privilegios:

```
mysql> CREATE DATABASE becario;
Query OK, 1 row affected (0.00 sec)

mysql> USE becario;
Database changed
mysql> CREATE TABLE calificaciones(nombre VARCHAR(30),calif integer);
Query OK, 0 rows affected (0.14 sec)
```

SSH Tunnel

Creamos la base becario:

```
mysql> CREATE DATABASE becario;
Query OK, 1 row affected (0.00 sec)

mysql> USE becario;
Database changed
mysql> CREATE TABLE calificaciones(nombre VARCHAR(30),calif integer);
Query OK, 0 rows affected (0.14 sec)
```

Cliente:
Instalamos mysql-client

```
root@debian2:/home/chaos# apt-get install mysql-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libdbd-mysql-perl libdbi-perl libmysqlclient18 libterm-readkey-perl
  mysql-client-5.5 mysql-common
Suggested packages:
  libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl
The following NEW packages will be installed:
  libdbd-mysql-perl libdbi-perl libmysqlclient18 libterm-readkey-perl
  mysql-client mysql-client-5.5 mysql-common
0 upgraded, 7 newly installed, 0 to remove and 196 not upgraded.
Need to get 3,457 kB of archives.
After this operation, 43.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Tcp-Dump:

```
root@debian2:/home/chaos# apt-get install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tcpdump
0 upgraded, 1 newly installed, 0 to remove and 196 not upgraded.
Need to get 410 kB of archives.
```

IPServer:

```
root@debian:/home/chaos# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:24:4a
          inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.
0
          inet6 addr: fe80::a00:27ff:fe1f:244a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12032 (11.7 KiB)  TX bytes:9498 (9.2 KiB)
```

SSH Tunnel

IPCliente:

```
root@debian2:/home/chaos# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:52:60
          inet addr:172.28.128.4  Bcast:172.28.128.255  Mask:255.255.255.
0
          inet6 addr: fe80::a00:27ff:fe33:5260/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2984 (2.9 KiB)  TX bytes:12479 (12.1 KiB)
```

En el server, permitimos conexiones remotas;

```
root@debian:/home/chaos# nano /etc/mysql/
conf.d/       debian.cnf    debian-start  my.cnf
root@debian:/home/chaos# nano /etc/mysql/my.cnf
```

```
 GNU nano 2.2.6         File: /etc/mysql/my.cnf                Modified

port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address           = 127.0.0.1
```

Reiniciamos el servicio:

```
root@debian:/home/chaos# /etc/init.d/mysql restart
[ ok ] Restarting mysql (via systemctl): mysql.service.
```

Desde el cliente escuchamos el trafico

```
root@debian2:/home/chaos# tcpdump -Xnni eth0 port 3306
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

SSH Tunnel

Nos conectamos al server:

```
root@debian2:/home/chaos# mysql -u bec -h 172.28.128.3 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.54-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserv
ed.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

Hacemos una peticion:

```
mysql> use becario;
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> DESCRIBE calificaciones;
+--------+-------------+------+-----+---------+-------+
| Field  | Type        | Null | Key | Default | Extra |
+--------+-------------+------+-----+---------+-------+
| nombre | varchar(30) | YES  |     | NULL    |       |
| calif  | int(11)     | YES  |     | NULL    |       |
+--------+-------------+------+-----+---------+-------+
2 rows in set (0.00 sec)
```

SSH Tunnel

Vemos el trafico capturado:

```
21:14:26.492493 IP 172.28.128.4.58010 > 172.28.128.3.3306: Flags [P.], seq 121:143, ac
:h 22
        0x0000:  4508 004a 5a6f 4000 4006 87f6 ac1c 8004  E..JZo@.@.......
        0x0010:  ac1c 8003 e29a 0cea 0648 85c3 5637 6625  .........H..V7f%
        0x0020:  8018 00e5 587d 0000 0101 080a 0002 6aee  ....X}........j.
        0x0030:  0001 e44d 1200 0000 0353 454c 4543 5420  ...M.....SELECT.
        0x0040:  4441 5441 4241 5345 2829                 DATABASE()
21:14:26.492808 IP 172.28.128.3.3306 > 172.28.128.4.58010: Flags [P.], seq 178:242, ac
:h 64
        0x0000:  4508 0074 813c 4000 4006 60ff ac1c 8003  E..t.<@.@.`.....
        0x0010:  ac1c 8004 0cea e29a 5637 6625 0648 85d9  ........V7f%.H..
        0x0020:  8018 00e3 c8d5 0000 0101 080a 0002 7017  ..............p.
        0x0030:  0002 6aee 0100 0001 0120 0000 0203 6465  ..j..........de
        0x0040:  6600 0000 0a44 4154 4142 4153 4528 2900  f....DATABASE().
        0x0050:  0c21 0066 0000 00fd 0000 1f00 0005 0000  .!.f............
        0x0060:  03fe 0000 0200 0100 0004 fb05 0000 05fe  ................
        0x0070:  0000 0200                                ....
21:14:26.492903 IP 172.28.128.4.58010 > 172.28.128.3.3306: Flags [.], ack 242, win 229
        0x0000:  4508 0034 5a70 4000 4006 880b ac1c 8004  E..4Zp@.@.......
        0x0010:  ac1c 8003 e29a 0cea 0648 85d9 5637 6665  .........H..V7fe
        0x0020:  8010 00e5 5867 0000 0101 080a 0002 6aee  ....Xg........j.
        0x0030:  0002 7017                                  p
```

Podemos ver que los datos viajan en claro, para solucionar esto hacemos un tunel ssh.
Donde 6666 es el puerto local (cliente) que hara tunel con el 3306 del servidor chaos@172.28.128.3 son las credenciales del server externo.

```
chaos@debian2:~$ ssh -p 22 chaos@172.28.128.3 -L 6666:127.0.0.1:3306
The authenticity of host '172.28.128.3 (172.28.128.3)' can't be establish
d.
ECDSA key fingerprint is 0b:5b:85:12:59:61:67:19:26:19:6d:84:b3:ae:e3:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.28.128.3' (ECDSA) to the list of known ho
ts.
chaos@172.28.128.3's password:
Permission denied, please try again.
chaos@172.28.128.3's password:

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 Apr 15 21:28:00 2017 from 172.28.128.4
chaos@debian:~$
```

SSH Tunnel

Nos conectamos a la base usando el tunel:

```
root@debian2:/home/chaos# mysql -u bec -h 127.0.0.1 -P 6666 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.5.54-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserv
d.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

Hacemos peticiones y observamos que el trafico ahora va cifrado:

```
        0x0000:  4510 0260 835b 4000 4006 5cec ac1c 8003  E..`.[@.@.\.....
        0x0010:  ac1c 8004 0016 a991 6fac 17e1 7af2 130e  ........o...z...
        0x0020:  8018 012f 81f4 0000 0101 080a 0011 757d  .../..........u}
        0x0030:  0011 6f9b 0000 0220 7f6d 6b7d a265 adaf  ..o.....mk}.e..
        0x0040:  eb6e c800 9979 76d4 089c 09db 6f33 1fb6  .n...yv.....o3..
        0x0050:  6133 512c fdd6 682d fe52 cb25 484b f18b  a3Q,..h-.R.%HK..
        0x0060:  db41 3a2f 6787 4fcc f224 09ad 4914 c70e  .A:/g.O..$..I...
        0x0070:  baf1 8ed7 16fc b766 1d8a 8c28 4fba faa2  .......f...(O...
        0x0080:  b28e b219 c036 7107 b136 92f3 c2c7 8b81  .....6q..6......
        0x0090:  450f 0c07 ba25 7ac3 89c2 65b9 5655 5bfe  E....%z...e.VU[.
        0x00a0:  3fcb 0603 6da9 31ad d315 6a3a 18f0 13e7  ?...m.1...j:....
        0x00b0:  4f2d 7a01 29d1 ff80 22fa b7f6 fb50 a877  O-z.)..."....P.w
        0x00c0:  d6f6 e9c3 d2f4 8eba b8cf 997b 76c8 5d26  ...........{v.]&
        0x00d0:  839c e1fa 052f bc04 49b5 df17 15cb 5cb0  ...../..I.....\.
        0x00e0:  0b6c 4da4 8717 1022 def7 ee5e ce09 8f0d  .lM...."...^....
        0x00f0:  5016 57fd bd4b f3b8 b4f6 bb6b 1de9 e7ba  P.W..K.....k....
        0x0100:  e8f6 73e2 759c b116 12cf 619a f410 e978  ..s.u.....a....x
        0x0110:  b357 d46d 5c57 7465 3326 54b5 605a 2c40  .W.m\Wte3&T.`Z,@
        0x0120:  fb02 41b5 aa3e 27c1 0e16 64b7 060d 3f58  ..A..>'...d...?X
        0x0130:  4716 45af 3aec f883 8a0f 3f18 38b6 1ad5  G.E.:.....?.8...
        0x0140:  f79e b730 61dd 5bfd 2d27 3782 ecf7 a43a  ...0a.[.-'7....:
        0x0150:  f525 4a94 52de ae64 8da3 eb6a 5f4d 2f1c  .%J.R..d...j_M/.
        0x0160:  3329 0d4e f22a 8103 a5d6 996e bdb2 e8e8  3).N.*.....n....
        0x0170:  0b92 3cb7 ea61 4add 63e1 c0ee bd03 c667  ..<..aJ.c......g
        0x0180:  7eb0 a77d a290 8b4a 5c53 1e14 3296 3650  ~..}...J\S..2.6P
```

SSH Tunnel


0x0090: 450f 0c07 ba25 7ac3 89c2 65b9 5655 5bfe E....%z...e.VU[.
0x00a0: 3fcb 0603 6da9 31ad d315 6a3a 18f0 13e7 ?...m.1...j:....
0x00b0: 4f2d 7a01 29d1 ff80 22fa b7f6 fb50 a877 O-z.)..."....P.w
0x00c0: d6f6 e9c3 d2f4 8eba b8cf 997b 76c8 5d26 ....{v.]&
0x00d0: 839c e1fa 052f bc04 49b5 df17 15cb 5cb0 ...../..I.....\.
0x00e0: 0b6c 4da4 8717 1022 def7 ee5e ce09 8f0d .lM...."...^....
0x00f0: 5016 57fd bd4b f3b8 b4f6 bb6b 1de9 e7ba P.W..K.....k....
0x0100: e8f6 73e2 759c b116 12cf 619a f410 e978 ..s.u.....a....x
0x0110: b357 d46d 5c57 7465 3326 54b5 605a 2c40 .W.m\Wte3&T.`Z,@
0x0120: fb02 41b5 aa3e 27c1 0e16 64b7 060d 3f58 ..A..>'...d...?X
0x0130: 4716 45af 3aec f883 8a0f 3f18 38b6 1ad5 G.E.:.....?.8...
0x0140: f79e b730 61dd 5bfd 2d27 3782 ecf7 a43a ...0a.[.-'7....:
0x0150: f525 4a94 52de ae64 8da3 eb6a 5f4d 2f1c .%J.R..d...j_M/.
0x0160: 3329 0d4e f22a 8103 a5d6 996e bdb2 e8e8 3).N.*.....n....
0x0170: 0b92 3cb7 ea61 4add 63e1 c0ee bd03 c667 ..<..aJ.c......g
0x0180: 7eb0 a77d a290 8b4a 5c53 1e14 3296 3650 ~..}...J\S..2.6P
0x0190: 89b0 a326 1b42 0cd4 435f 1258 5035 9aac ...&.B..C_.XP5..
0x01a0: 00aa ae15 60f3 bd82 7f81 3e48 0bae 12b9 ....`.....>H....
0x01b0: 2b93 978f d5c0 bfdd df73 9956 5ca3 8c80 +........s.V\...
0x01c0: ae08 25b0 7d9a 38ab 5886 cc47 4589 1ed7 ..%.}.8.X..GE...
0x01d0: 9ab4 7c0b 8730 009e 588a b09f 05c7 8797 ..|..0..X.......
0x01e0: 242d 246f fdf1 130e 96d9 1faf 6def d32c $-$o........m..,