Mongodb-Redis匿名扫描脚本

沦沦 / 2017-01-19 03:20:00 / 浏览数 7090 安全工具 工具 顶(0) 踩(0)

---

mongodb-redis匿名扫描脚本，支持mongodb和redis的匿名扫描，脚本是之前有需求写的，现在分享给大家学习和研究:）

扫描截图：

```
#coding=utf-8
import pymongo
import redis
import time
import sys
import threading
import Queue

q=Queue.Queue()

class myThread (threading.Thread):
   def init(self,func,args1,args2):
       threading.Thread.init(self)
       self.func = func
       self.args1 = args1
       self.args2 = args2
   def run(self):
       self.func(self.args1, self.args2)

def ip2num(ip):
   ip=[int(x) for x in ip.split('.')]
   return ip[0] <<24 | ip[1]<<16 | ip[2]<<8 |ip[3]
def num2ip(num):
   return '%s.%s.%s.%s' %( (num & 0xff000000) >>24,
                           (num & 0x00ff0000) >>16,
                           (num & 0x0000ff00) >>8,
                           num & 0x000000ff )
def get_ip(ip):
   start,end = [ip2num(x) for x in ip.split('-') ]
   return [ num2ip(num) for num in range(start,end+1) if num & 0xff ]

def mongo(q,f):
   while True:
       if not q.empty():
           ip=q.get()
           try:
               print ip.strip()+"\r"
               conn=pymongo.Connection(ip.strip(),27017)
               db = conn.database_names()
               if db:
                   time.sleep(0.1)
                   f.write(ip.replace("\n","\t")+"Login mongodb"+'\n')
                   f.flush()
                   print ip.replace("\n","\t")+"Login mongodb"+'\n'
               else:
                   pass
               r=redis.Redis(host=ip,port=6379,db=0)
               rs=r.info()
               if rs:
                   time.sleep(0.1)
                   f.write(ip.replace("\n","\t")+"Login redis"+'\n')
                   f.flush()
                   print ip.replace("\n","\t")+"Login redis"+'\n'
               else:
                   pass
           except:
               pass

if name == 'main':
```

```
    help_l=u"""
            Mongodbscan■■
               ■■■■■
■■■
■■■■■Mongodbscan.py -m 100 -u ip.txt url.txt
IP■■■■Mongodbscan.py -m 100 -g 192.168.1.1-192.168.1.254 url.txt
    """
    if len(sys.argv)<2:
        print help_l
    else:
        if len(sys.argv)>2:
            if sys.argv[1]=='-m':
                threads = []
                threadList = range(int(sys.argv[2]))
            if sys.argv[3]=='-u':
                ipc=open(sys.argv[4],"r")
                f=open(sys.argv[5],"w")
                for ipcc in ipc:
                    q.put(ipcc)
                for i in threadList:
                    t = myThread(mongo, q, f)
                    t.setDaemon(True)
                    threads.append(t)
                    t.start()
                for t in threads:
                    t.join()
            if sys.argv[3]=='-g':
                users = get_ip(sys.argv[4])
                f=open(sys.argv[5],"w")
                for user in users:
                    q.put(user.strip())
                for i in threadList:
                    t = myThread(mongo, q, f)
                    t.setDaemon(True)
                    threads.append(t)
                    t.start()
                for t in threads:
                    t.join()
```

附件代码脚本
链接: http://pan.baidu.com/s/1qYnRA3q 密码: njrh

上一篇：重大安全事件调查思维导图 下一篇：先知众测向你发出一个新年挑战~

1. 7 条回复


xiaopigfly 2017-01-19 03:22:44

大屌哥~~~

0 回复Ta


aa 2017-01-19 05:26:01

表哥，图片没显示出来

0 回复Ta


沦沦 2017-01-19 05:45:57

社区的BUG，上传了也不行

0 回复Ta


笑然 2017-01-19 06:12:12

这个问题我也发现了，在排查
你试试从图片入口上传图片，在附件那边把图片插到文章中试试

0 回复Ta


沦沦 2017-01-19 06:46:14

从附件这边OK了

0 回复Ta


笑然 2017-01-19 07:31:23

或者先用markwown也行~~

0 回复Ta


风带走故事也 2017-01-28 11:19:43

不错 哈哈哈哈哈

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录