CTF writeup：python脚本爆破zip密码

原创

samohyes 于 2017-07-12 00:18:44 发布 5411 收藏 5
分类专栏： CTF writeup 文章标签： 信息安全 黑帽 python 脚本 密码

整个过程我先后尝试了python的zipfile,gzip模块，用过linux下的unzip，最后发现得用linux下7z指令才行。现在写下整个过程！

首先拿到zip文件，提示在123456附近，那么提示给这么明显，直接用Python写个脚本就好。

首先用的是os模块，用os.system执行‘winrar e -p 密码 ***.rar’这样的，发现网上写的很好，但是自己用了感觉不行！

遂尝试zipfile模块！自编代码奉上！

```
import zipfile

flag = 0

def zipbp(zip_file,passwd):
 try:
  zip_file.extractall(pwd = passwd)
  print("[*] success! password is %s"%passwd)
  global flag
  flag = 1
 except:
  print('Sorry, %s failed'%passwd)

def main():
 zip_file = zipfile.ZipFile('droste.zip')
 for i in range(123000,124000):
  passwd = str(i).encode(encoding = 'utf-8')
  zipbp(zip_file,passwd)
  if flag == 1:
   break

if __name__ == '__main__':
 main()
```

跑起来，有错误！显示这不是一个zip文件！WTF？后缀明明是zip好不好。google得到有人有类似错误，说是zip文件少了某个东西，仿佛尝试，无果。

转而用gzip，可是没有带密码的形式啊！放弃。

那么就用os.system调用Linux下的unzip吧，发现还是不行，依旧显示这不是个zip文件！

```
BadZipfile: File is not a zip file
```

真是伤心！

接着，了解到可以用功能更强的7z指令！奉上代码！

```
import os

for i in range(120000,130000):
 cmd = '7z x -p%d droste.zip'%i
 r = os.system(cmd)
 if r == 0:
  print('[*] success! The key is %d'%i)
  print(r)
  break
 else:
  print('%d is wrong,continuing...'%i)
  print(r)
```

虽然不知道爆破出来的时候那个循环还在执行，中间123465密码的时候虽然r==512但是跳出来一条询问我是否覆盖文件的语句，猜测123465应该就是，尝试，成功，得到一张图片，难道是隐写？明天我再去鼓捣以下！

##############

继续上次的博文，拿到了密码，发现解压后是一个新的zip和一张droste.jpg的图片，用winhex一看，jpg末尾没问题，题目又给出Hint是ntfs文件流，在网上搜索相关资料：

http://www.cnblogs.com/Chesky/p/ALTERNATE_DATA_STREAMS.html

好了，那么直接对着原来的zip操作，mspaint.exe droste.zip:droste.jpg，竟然提示没有这个图片。没办法，解压一次后得到了一个zip和jpg，对这个zip继续操作

mspaint.exe droste.zip:droste.jpg

得到flag!