Misc bugku(三)

原创

Pito 于 2019-05-20 19:25:56 发布 164 收藏

分类专栏： bugku的writeup 文章标签： bugku

本文链接：https://blog.csdn.net/weixin_42350229/article/details/90380758

神秘文件：

直接下载文件，解压出来看到了看见一个压缩包和一张图片。压缩包里面有那张一模一样的图片。直接明文爆破。（在这里有个注意点，一定要一定要用什么解压出来的就用什么压缩，我这里用的是winrar和7z添加成.zip结果很难受，后来改用了WinRAR才好）

红色是爆破出来的压缩包。

解压得到一个word文档，打开提示没有writeup,后来binwalk分析了一下发现里面还有好多文件，直接分离出来。

里面有个flag.txt文档。里面就是flag的base64加密的字符串

```
1
2   import base64
3   s = 'ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ=='
4   print(base64.b64decode(s))
```

直接python解码。flag{d0cX_1s_ziP_file}

这里再补充一下使用pkcrack进行明文爆破的方法：

Kali下先安装这个工具，通过tar包方式

Wget https://www.unix-ag.uni-kl.de/~conrad/krypto/pkcrack/pkcrack-1.2.2.tar.gz

Tat xzf pkcrack-1.2.2.tar.gz

Cd pkcrack-1.2.2/src

Make

Mkdir -p …/…/pkcrack

Cp pkcrack …/…/pkcrack

Cd …/…/

-C：要破解的目标文件（含路径）

c：破解文件中的明文文件的名字（其路径不包括系统路径，从zip文件一层开始）

P：压缩后的明文文件

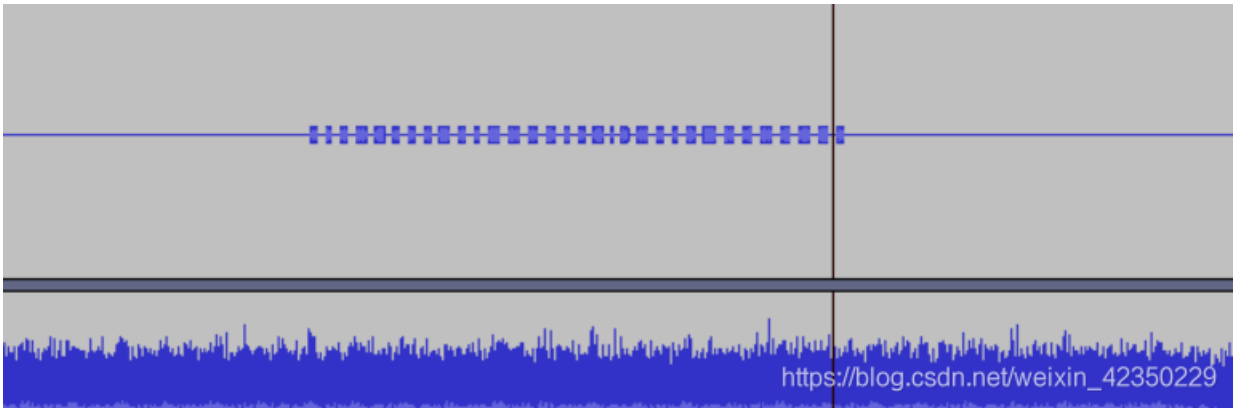
p：压缩的明文文件中明文文件的名字（也就是readme.txt在plain.zip中的位置）

d：最后得到的没有加密的zip文件

```
flag.zip  logo.zip  pkcrack
text@LAPTOP-RRKM786L:~/pkcrack$ ./pkcrack -c 'folder2/logo.png' -p logo.png -C flag.zip  -P logo.zip -d ok.zip
File folder2/logo.png not found in ZIP file
text@LAPTOP-RRKM786L:~/pkcrack$ ./pkcrack -c 'logo.png' -p logo.png -C flag.zip  -P logo.zip -d ok.zip
Files read. Starting stage 1 on Tue May  7 22:09:26 2019
Generating 1st generation of possible key2_27404 values...done.
Found 4194304 possible key2-values.
Now we're trying to reduce these...
Lowest number: 950 values at offset 11229
Lowest number: 938 values at offset 11211
Lowest number: 903 values at offset 11210
Lowest number: 879 values at offset 11206
Lowest number: 783 values at offset 9567
Lowest number: 732 values at offset 9566
Lowest number: 721 values at offset 9555
Lowest number: 714 values at offset 9490
Lowest number: 706 values at offset 9489
Done. Left with 706 possible Values. bestOffset is 9489.
Stage 1 completed. Starting stage 2 on Tue May  7 22:09:48 2019
Strange... had a false hit.
Strange... had a false hit.
Ta-daaaaa! key0= f3b8dbf, key1=bc1ad2b6, key2= 3bd7740
Probabilistic test succeeded for 17920 bytes.
Stage 2 completed. Starting zipdecrypt on Tue May  7 22:10:17 2019
Decrypting 2018[?□障□□riteup.docx (0b0d29973bf3d010d5ad3172)... OK!
Decrypting logo.png (2299aecf189b7a29621dd959)... OK!
Finished on Tue May  7 22:10:17 2019
```


听首音乐：

下载文件，wav结尾直接audacity打开，发现



感觉就是莫斯编码，

… -… -.-. ----. …— … -… …- ----. -.-. -… ----- .---- —… —… …-. … …— . -… .---- --… -… --… ----- ----. …— ----. .---- ----. .---- -.-. 按这个写下来，直接解码

5bc925649cb0188f52e617d70929191c因为我的工具解出来的是小写，以为还要hex解一下解不出来，大佬说直接提交就可以，结果提交不对，后来转换为大写之后提交就对了。

好多数值：

打开文件，全是255，255，255 看了有61366行第61367行是空着的，所以不用考虑，由于是第一次碰见这种题目，所以直接问

了大佬。就是直接用python的PIL库对这些数据做一个图形处理，61366=261503 当然也有其他的分法，我直接选择这种，直接出flag，x,y调换只是图片 横着和竖着的区别，直接上脚本。

RGB_to_image.py 1.txt

```
#-*- coding:utf-8 -*-
from PIL import Image
import re
x = 503 #x坐标  通过txt里的行数进行整数分解
y = 122 #y坐标  x*y = 行数
im = Image.new("RGB",(x,y)) #创建图片
file = open('1.txt')# 打开rbg值文件
# 通过一个个rgb点生成图片.
for i in range(0,x):
    for j in range(0,y):
        line = file.readline()# 获取一行
        rgb = line.split(',')# 分离rgb
        im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))
im.show()
```


由于我使用的是python3所以PIL不支持，所以我直接换了一个和PIL有一样功能的库Pillow。
直接pip install Pillow就可以直接安装了。

散乱的密文：

先按照提示的顺序

```
print(len('lf5{ag024c483549d7fd@@1}'))
```

```
i = 0

while i in range(25):
    print(str('lf5{ag024c483549d7fd@@1}')[i:i+6])
    i += 6


lf5{ag
024c48
3549d7
fd@@1}
```


下面时打印结果，接下来直接栅栏解密flag{52048c453d794df1}@@ 提交的时候直接把后面的@@去掉，这个估计就是来凑数的。

凯撒部长的奖励：

一长串的密文，直接丢进工具解密

```
RXB{gdqd_Hr_xNtq_qDvZqc_dmiNx_Hs_Bzdrzq_nq_bzkk_ghl_uHbsNq_hr_z_Dwbdkkdms_Izm_he_xnt_vzms_sn_fds_ghr_hmenqlzshnmr_xnt_bz
SYC{here_Is_yOur_rEwArd_enjOy_It_Caesar_or_call_him_vIctOr_is_a_Excellent_man_if_you_want_to_get_his_informations_you_ca
```

Here is 直接跑出这个，所以直接提交，本来看着这个还以为还要再解一遍，结果看到题目猜想就是这个了，所以直接提交，正好对了。