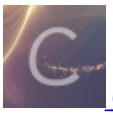
CTF--crypto

原创

本人&ren 于 2020-04-28 12:06:29 发布 642 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_40730029/article/details/105808666



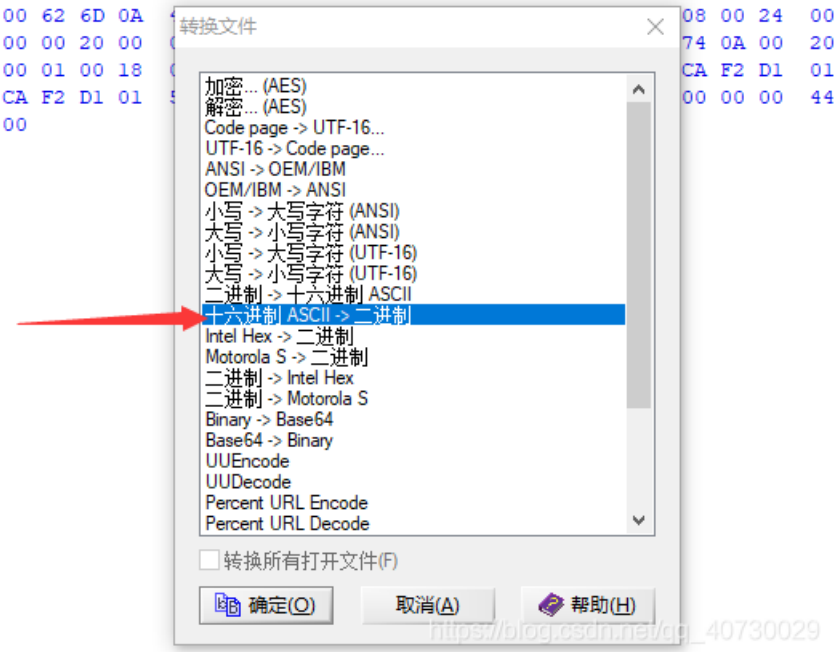
你猜猜

题目：我们刚刚拦截了，敌军的文件传输获取一份机密文件，请君速速破解。

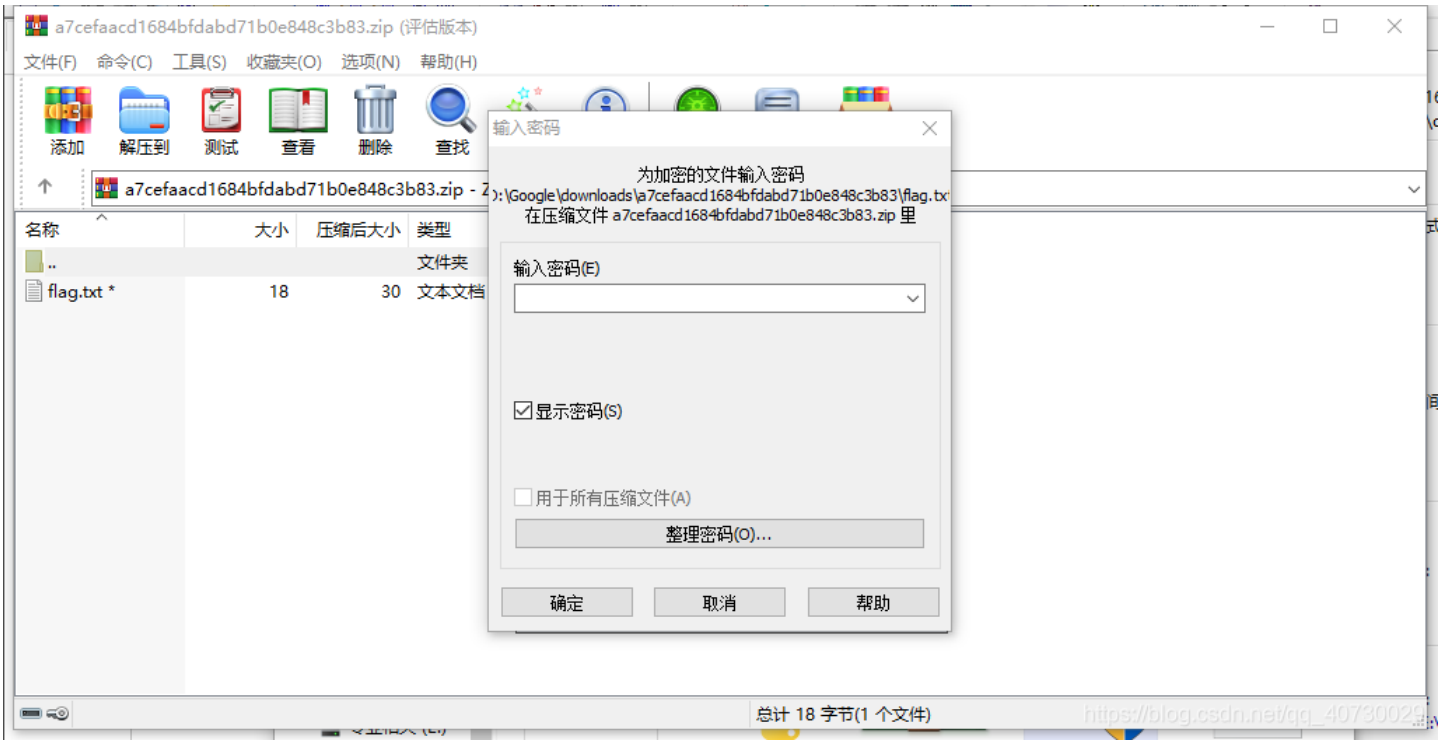
下载附件解压后是一个文本文件，看到**504B**，很明显是压缩文件的文件头

将该文本文件拖到**winhex**打开，将文件格式转为**.zip**格式，右键—>编辑—>转换选块，转好之后保存文件

```
B 03 04 0A 00 01 08   00 00 62 6D 0A 49 F4 B5   09 1F 1E 00 00 00 12 00   00
8 00 00 00 66 6C 61   67 2E 74 78 74 6C 9F 17   0D 35 D0 A4 58 26 A0 3E   16
9 68 70 ED DF C7 C8   9A 11 86 2F 91 99 B4 CD   78 E7 50 4B 01 02 3F 00   0A
1 08 00 00 62 6D 0A                                                08 00 24   00
0 00 00 00 00 20 00                                                74 0A 00   20
0 00 00 00 01 00 18                                                CA F2 D1   01
E AA 05 CA F2 D1 01                                                00 00 00   44
0 00 00 00
```



将文件后缀名改为.zip然后解压，需要密码



将压缩包拖到kali里，在终端输入命令

```
root@kali:~# fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt a7cefaacd1
684bfdabd71b0e848c3b83.zip


PASSWORD FOUND!!!!: pw == 123456
root@kali:~#
```

(相关操作见Fcrackzip解题)

```
crackzip -D -u -p /usr/share/wordlists/rockyou.txt a7cefaacd1684bfdabd71b0e848c3b83.zip
```

成功解压之后打开**flag.txt**，得到**flag**

```
daczcasdqwdcsdzasd
```