压缩包隐写

原创

流浪打浪 于 2019-11-01 17:06:35 发布 1722 收藏 4
分类专栏： 隐写 ctf 文章标签： 隐写 压缩包


隐写 同时被 2 个专栏收录
1 篇文章 0 订阅
订阅专栏


ctf
3 篇文章 1 订阅
订阅专栏

压缩包本身不具备隐藏信息的功能，但CTF中压缩包经常与隐写术结合一起来考查。

压缩包格式：

Rar 有Rar标志 zip 有PK标志 7z 有7z标志

zip 的 无加密 伪加密 真加密

有两个加密标志 数据区和目录区的加密标记

无加密 （偶数（00 00）偶数） 伪加密（偶数 奇数） 真加密（奇数 奇数（09 00））

压缩包+图片

- 压缩包和图片混合，但给出的是压缩包
- 压缩包和图片混合，但给出的是图片

有时候需要先对压缩包文件进行简单的修复

压缩包加密：打开压缩包需要密码

- 密码以注释等其他提示形式出现
- 压缩包伪加密
- 压缩包爆破

CRC32碰撞：

- 加密文件为纯文本文档
- 加密文件大小较小（CTF通常为4）

```
import binascii

crc = 0xDBF9C8F7

for i in range(1000,10000)
    if(binascii.crc32(str(i)&0xffffffff) == crc);
    print i
    exit(0)
```

压缩包已知明文攻击：

- 压缩包为zip格式
- 题目本身给出了压缩包中的某一文件
- 该文件需要和压缩包中的文件的CRC32校验和一致。

通过archpr工具碰撞尽管不能获取其压缩包密码，但能获得其他文件内容（flag.txt）

python解压操作代码：

```
import zlib
import base64
import binascii

a="这里是需要解压的16进制数据".decode('hex')

b = binascii.hexlify(base64.b64decode(zlib.decompress(a)))

print b
```

取每个文件的内容

```
import os,zipfile

directory = os.getcwd() + '/'

for filename in os.listdir(directory):
    fn = filename.split('.')
    if fn[1] = 'zip':
        z =  zipfile.ZipFile(directory + filename)
        print z.namelist()
```

--参考i春秋《隐写术及相关技术分析》