base64stego

原创

站立蛋 于 2020-03-20 21:10:54 发布 1200 收藏 4

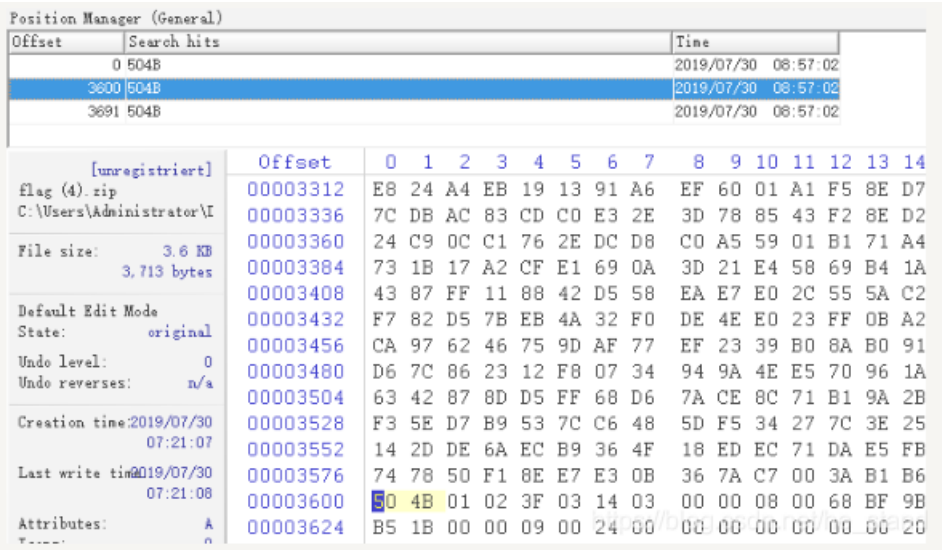
WriteUp

1.题目

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=0&id=5107

2.解题步骤

首先打开文件发现有密码，看了没其他提示之后猜测可能是伪加密。winhex打开文件，搜索16进制504B会有3个结果，定位到第二个之后将09 00修改为00 00 然后保存。



解压得到一个内容全是base64编码的文件，发现是base64文件隐写，python2环境下直接利用脚本即可解出flag.

```
# base64文件隐写脚本
#!/user/bin/env python
# -*-coding:utf-8 -*-
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s1)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res

def solve_stego():

    with open('E://stego.txt', 'rb') as f:
        file_lines = f.readlines()

    bin_str = ''
    for line in file_lines:
        steg_line = line.replace('\n', '')
        norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
        diff = get_base64_diff_value(steg_line, norm_line)
        pads_num = steg_line.count('=')
        if diff:
            bin_str += bin(diff)[2:].zfill(pads_num * 2)
        else:
            bin_str += '0' * pads_num * 2

    res_str = ''

    for i in xrange(0, len(bin_str), 8):

        res_str += chr(int(bin_str[i:i+8], 2))
    print res_str

solve_stego()
```

3.flag值

flag{Base_sixty_four_point_five}

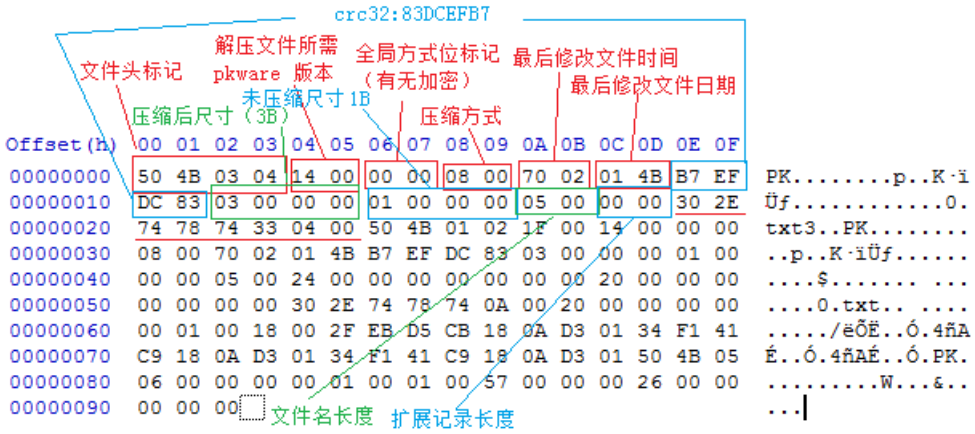
4.涉及的知识点

zip伪加密

原理：在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包。

zip = 压缩源文件数据区 + 压缩源文件目录区 + 压缩源文件目录结束标志

https://blog.csdn.net/wclxyn/article/details/7288994



压缩源文件数据区

c、数据描述符

组成	长度
CRC-32校验	4 bytes
压缩后尺寸	4 bytes
未压缩尺寸	4 bytes

这个数据描述符只在全局方式位标记的第3位设为1时才存在（见后详解），紧接在压缩数据的最后一个字节后。这个数据描述符只用在不能对输出的 ZIP 文件进行检索时使用。例如，在一个不能检索的驱动器（如，磁带机上）上的 ZIP 文件中。如果是磁盘上的ZIP文件一般没有这个数据描述符。

2、压缩源文件目录区

在这个数据区中每一条纪录对应在压缩源文件数据区中的一条数据

组成	长度
目录中文件文件头标记	4 bytes (0x02014b50)
压缩使用的 pkware 版本	2 bytes
解压文件所需 pkware 版本	2 bytes
全局方式位标记	2 bytes
压缩方式	2 bytes
最后修改文件时间	2 bytes
最后修改文件日期	2 bytes
CRC-32校验	4 bytes
压缩后尺寸	4 bytes
未压缩尺寸	4 bytes
文件名长度	2 bytes
扩展字段长度	2 bytes
文件注释长度	2 bytes
磁盘开始号	2 bytes
内部文件属性	2 bytes
外部文件属性	4 bytes
局部头部偏移量	4 bytes
文件名	(不定长度)
扩展字段	(不定长度)
文件注释	(不定长度)

3、压缩源文件目录结束标志

组成	长度
目录结束标记	4 bytes (0x02014b50)
当前磁盘编号	2 bytes
目录区开始磁盘编号	2 bytes
本磁盘上纪录总数	2 bytes
目录区中纪录总数	2 bytes
目录区尺寸大小	4 bytes
目录区对第一张磁盘的偏移量	4 bytes
ZIP 文件注释长度	2 bytes
ZIP 文件注释	(不定长度)

有三个头标志：压缩源文件数据区 50 4B 03 04

压缩源文件目录区 50 4B 01 02

压缩源文件目录结束标记 50 4B 05 06

真假加密

无加密

压缩源文件数据区的全局加密应为00 00

且压缩源文件目录区的全局方式标记应当为00 00

假加密

压缩源文件数据区的全局加密应为00 00

且压缩源文件目录区的全局方式标记应当为09 00

真加密

压缩源文件数据区的全局加密应为09 00

且压缩源文件目录区的全局方式标记应当为09 00

base64隐写

- https://www.tr0y.wang/2017/06/14/Base64steg/
- base64解码：把base64字符串去掉等号，转为二进制，然后从左到右8个一组，多余位扔掉，转为对应得ASCII码。（而多余位即等号数*2反正是要被扔掉的，所以修改它也不会影响原来的字符）
  e64steg/
- base64解码：把base64字符串去掉等号，转为二进制，然后从左到右8个一组，多余位扔掉，转为对应得ASCII码。（而多余位即等号数*2反正是要被扔掉的，所以修改它也不会影响原来的字符）
- 一行 base64 顶多能有 2 个等号, 也就是有 2*2 位的可隐写位. 所以得弄很多行, 才能隐藏一个字符串