

攻防世界 Misc高手进阶区 6分题 神奇的压缩文件

原创

思源湖的鱼  于 2021-01-10 14:53:11 发布  624  收藏 3

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [misc](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44604541/article/details/112427198

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的6分题

本篇是神奇的压缩文件的writeup

发现攻防世界的题目分数是动态的

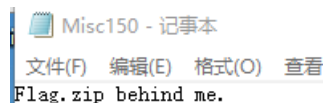
就仅以做题时的分数为准了

解题过程

题目描述

题目描述: 为什么文件大小和说好的不一样呢? 无限的命运石之门啊! 里面并没有Flag。

得到的压缩包里有有个txt



```
Misc150 - 记事本
文件(F) 编辑(E) 格式(O) 查看
Flag.zip behind me.
```

那肯定是有隐藏什么

扔进winhex

发现PK, 即有zip文件隐藏

用foremost和binwalk都失败

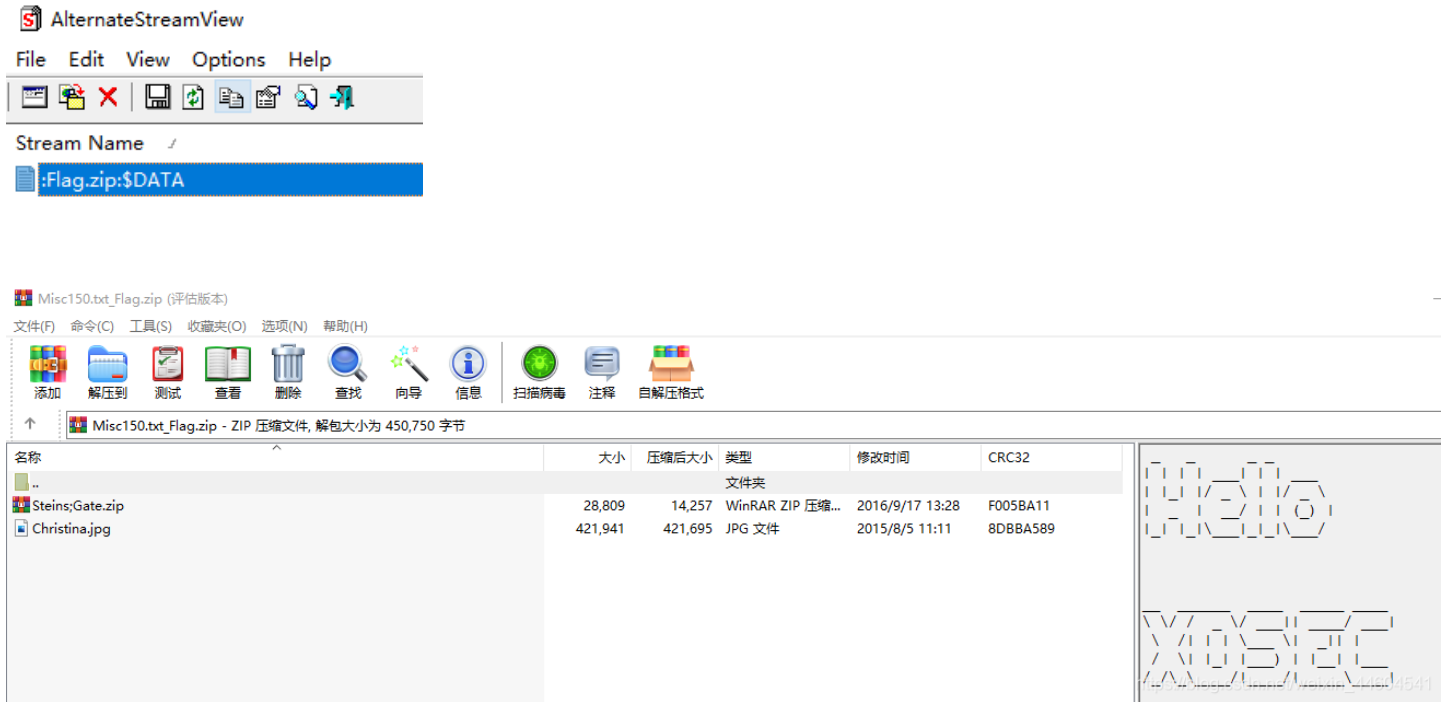
查了查

可能是NTFS流隐藏

谈谈NTFS数据流文件

利用NTFS交换数据流隐藏文件

使用AlternateStreamView扫描得到flag.zip



然后开始套娃了

压缩包里套压缩包和图片

搞了个脚本解压

但是一堆图片怎么处理都没东西

卡了好久

回头看题目描述

“里面没有flag”

好家伙

那再找找

就感觉最开始扫描出来的压缩包里的注释似乎可疑



这要有隐藏信息
估计也就是二进制了

```

0_000_000000_0_0000000
|0|0|0|0|0_|0|0|0_|00
|0|_|0|0|/0_0\0|0|0|/0_0\0
|00_00|00_|0|0|0|0|0|
|_|0|_|0|_|0|_|0|_|0|_|
110110011000111110100110011011110
110110110110010001100110110110011
01110110111110010011001001111101
_00_00_00_00_0_0
|0\0/00_0\0_|0_|0_|0_|0_|
0\00/0|0|0|0_|0\00_|0|0000
0/00\0|0|0|0|_|0|0|_|0|_|0
|_|0|_|0|_|0|_|0|_|0|_|0|_|

```

```

110110011000111110100110011011110
110110110110010001100110110110011
01110110111110010011001001111101

```

得到 110110011000111110100110011011110 110110110110010001100110110110011 01110110111110010011001001111101

```

1 1101100 1100011 1110100 1100110 1111011 0110110 1100100 0110011 0110110 0110111 0110111 1100100 1100100 |111101

```

1 lctf{6d3677dd} https://blog.csdn.net/weixin_44604541

得到flag

结语

学习了新知识——NTFS流隐藏
谈谈NTFS数据流文件
利用NTFS交换数据流隐藏文件