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

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

前言

继续ctf的旅程

攻防世界Misc高手进阶区的6分题

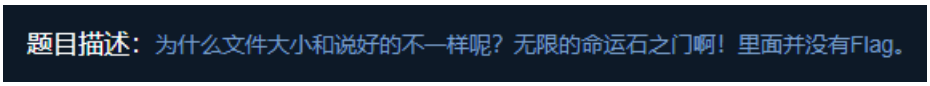
本篇是神奇的压缩文件的writeup

发现攻防世界的题目分数是动态的

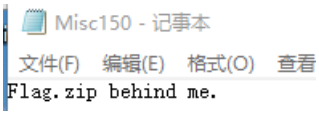
就仅以做题时的分数为准了

解题过程

题目描述



得到的压缩包里有个txt



那肯定是有隐藏什么

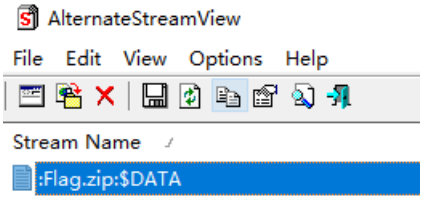
扔进winhex

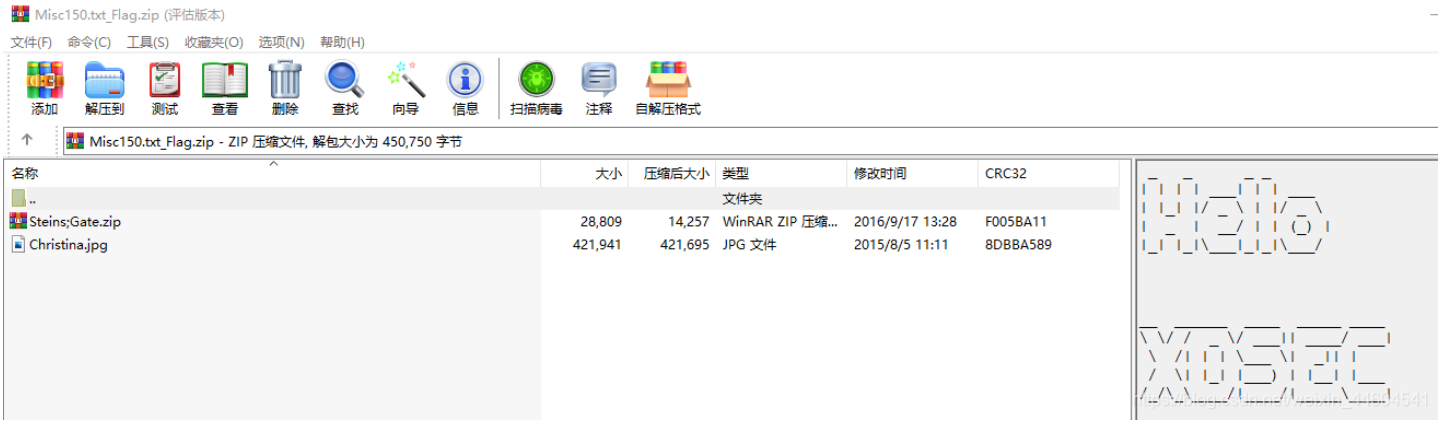
发现PK，即有zip文件隐藏

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

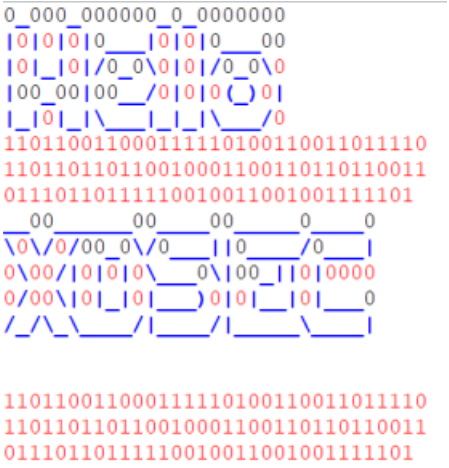
卡了好久

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



```
1101100110001111101001100110111101101100110001100100011001101100111001001100100111110
```

得到`1101100110001111101001100110111101101100110001100100011001101100111001001100100111110`

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