【问鼎杯】3-2关卡writeup

原创

Angel枫丨灬红叶 于 2015-12-03 04:50:21 发布 2308 收藏

分类专栏： CTF 文章标签： ctf writeup 问鼎杯

本文链接：https://blog.csdn.net/yuanyunfeng3/article/details/50155511

0x01序

这题CTF题目是2015/11/28问鼎杯线下的一题题目，当时在这题上卡了好久。。其实主要是因为自己JPG数据格式不熟，并且没有准备相关资料导致的，所幸比赛的最后还是做了出来，这次放这个writeup是因为赛后自己想出了更完美的解题方式，所以记录一下。

0x02题目描述

给出一堆数据，该数据中隐藏着flag信息，请从中提前出flag。

Download it!

0x03 解题思路

首先用binwalk识别一下文件类型

发现偏移0x6000处存在JPG文件。

提取出该文件

```
dd if=3-2 skip=24576 bs=1 of=1.jpg
```

打开文件。。然并软。。

文件似乎有问题，我们用stega查看一下

文件扫描线结束后存在大量垃圾数据。。

首先把之后的垃圾数据去掉，保存至一个文件里面 我这里命名为 1

这边第一个思路的是去掉导致扫描线结束的数据。

如果扫描线遇到ff字节的数据，则判断下一个字节是否为00否则结束扫描线。

写个脚本把垃圾数据中所有导致扫描线结束的字节改过来。。

```
file_hex=''
with open('1','rb') as f:
    file_hex = f.read()
file_hex = list(file_hex)
new_file=[]
i = 0
ko=1
while(i<len(file_hex)):
    if(file_hex[i]=='\xff' and file_hex[i+1]!='\x00'):
        ko=0
    elif(file_hex[i]=='\xff' and file_hex[i+1]=='\x00'):
        ko=1
        new_file.append(file_hex[i])
    elif(ko==1):
        new_file.append(file_hex[i])
    i+=1
new_file = ''.join(new_file)
with open('2','w') as f:
    f.write(new_file)
```

修改图片的长度（JPG数据格式）

FF C0之后3个字节开始是图片高度，占两个字节，然后是图片宽度，占两个字节

然后将处理后的垃圾数据拼接回原图片，希望它能够继续扫描出所有数据

这是什么鬼！？

好吧，换另一个思路，模糊测试。脚本如下

```
file_hex=''
file_old = ''
with open('0.jpg','r') as f:
        file_old = f.read()
file_old = list(file_old)

with open('1','r') as f:
        file_hex = f.read()
file_hex=list(file_hex)
i=1
while(i<len(file_hex)):
        file = []
        file.extend(file_old)
        with open(str(i)+'.jpg','w') as f:
                file.extend(file_hex[i:len(file_hex)])
                file = ''.join(file)
                f.write(file)
        i+=1
```

在第1740张图发现flag，即偏移1740个字节，这里是此处flag区域刚好全为有效数据。。万一运气不好，遇到里面也存在垃圾数据。那该怎么办？（或许我可以先用脚本处理完垃圾数据后，再模糊测试？