攻防世界 Misc高手进阶区 3分题 奇怪的TTL字段

原创

思源湖的鱼 于 2020-11-13 10:39:08 发布 615 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 misc 二维码 ttl

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109669271

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

本篇是奇怪的TTL字段的writeup

发现攻防世界的题目分数是动态的

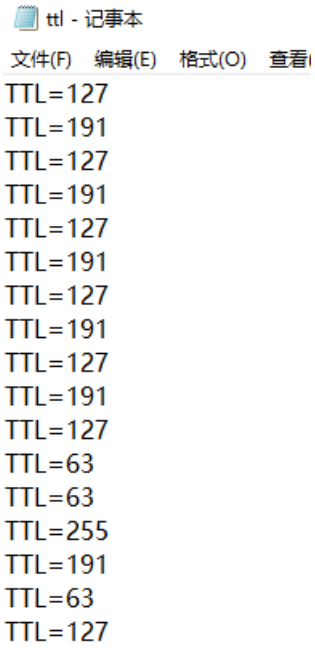
就仅以做题时的分数为准了

解题过程

题目描述

```
我们截获了一些IP数据报，发现报文头中的TTL值特别可疑，怀疑是通信方嵌入了数据到TTL，我们将这些TTL值提取了出来，你能看出什么端倪吗？
```

下下来一个ttl.txt



只有4个值63,127,191,255
有295374行

感觉应该是搞成一张图片
先转为二进制试试
63=00111111
127=01111111
191=10111111
255=11111111

看着是只要前两位就是了

脚本跑下

```
fp = open('ttl.txt','r')
a = fp.readlines()
p = []
for i in a:
    p.append(int(i[4:]))
s = ''
for i in p:
    if i == 63:
        a = '00'
    elif i == 127:
        a = '01'
    elif i == 191:
        a = '10'
    elif i == 255:
        a = '11'
    s += a
# print(s)

import binascii
flag = ''
for i in range(0,len(s),8):
    flag += chr(int(s[i:i+8],2))
flag = binascii.unhexlify(flag)
wp = open('res.jpg','wb')
wp.write(flag)
wp.close()
```

得到

```
ffd8ffe1001845786966000049492a00080000000000000000000000
2b687474703a2f2f6e732e61646f62652e636f6d2f7861702f312e30
222069643d2257354d304d7043656869487a7265537a4e54637a6b
```

以FFD8开头，FFD9结束。所以，是jpeg格式的图片无疑了

winhex构建图片

formost分离

ps拼接

再读取

得到flag

结语

有点绕