隐信道数据安全分析

发表于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 隐信道数据安全分析

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/5960

题目描述

> *安全分析人员截获间谍发出的秘密邮件，该邮件只有一个mp3文件，安全人员怀疑间谍通过某种private的方式将信息传递出去，尝试分析该文件，获取藏在文件中的数据？*

题目考点

解题思路

题目提示文件使用了private加密信息，在010Editor中打开mp3文件，发现存在private bit，因此，只需要提取每一个mf组中的该字节，组合起来，就是答案。可以从图中看到 ms 开始位为1 C1B8H，即第115128字节，如图所示：，如图所示：


```
uint32 frame_sync : 12
    uint32 mpeg_id : 1
    uint32 layer_id : 2
    uint32 protection_bit : 1
    uint32 bitrate_index : 4
    uint32 frequency_index : 2
    uint32 padding_bit : 1
    uint32 private_bit : 1
    uint32 channel_mode : 2
    uint32 mode_extension : 2
    uint32 copyright : 1
    uint32 original : 1
    uint32 emphasis : 2
```

12+1+2+1+4+2+1+1+2+2+1+1+2=32，即总共4字节，private_bit 为24，所在的字节为第3个字节因此要从前一个，即第二个字节开始提取内容，该字节对应的地址为 115130观察每一个mf组，大小都为414h，即1044字节，因此可以得到以下脚本：

```
# coding:utf-8
import re
import binascii
n = 115130
result = ''
fina = ''
file = open('flag-woody.mp3','rb')
while n < 2222222 :
    file.seek(n,0)
    n += 1044
    file_read_result = file.read(1)
    read_content = bin(ord(file_read_result))[-1]
    result = result + read_content
textArr = re.findall('.{'+str(8)+'}', result)
textArr.append(result[(len(textArr)*8):])
for i in textArr:
    fina = fina + hex(int(i,2))[2:].strip('\n')
fina = fina#.decode('hex')
print (fina)
```

将得到的字符串464c41477b70723176347433356f6269377d25a1cedc3e69888894dac4dd3a87c5e1c5276fa6d626832148d39288a0c596c95abaac3f09f9f524647595ae4894f9b82b3f4c1b47537c365d8d69d84a353c1a93ae436761d430
换对应的ASCII码，得到Flag

Flag

```
flag{pr1v4t3_bi7}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/MvdxB1ZbFWM212UVKZUeW.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2019 # 工业信息安全技能大赛 # 深圳站
工业网络设备逆向
工控蜜罐日志分析