Web

没..没做出来…光第一题的 LFI(大概…)就拦了我三天…

以后本菜鸡签完到就研究上周的 WP 了…

RE

Pro 的 python 教室（二）

pyc 文件找工具反编译掉，得到 py 文件看源码

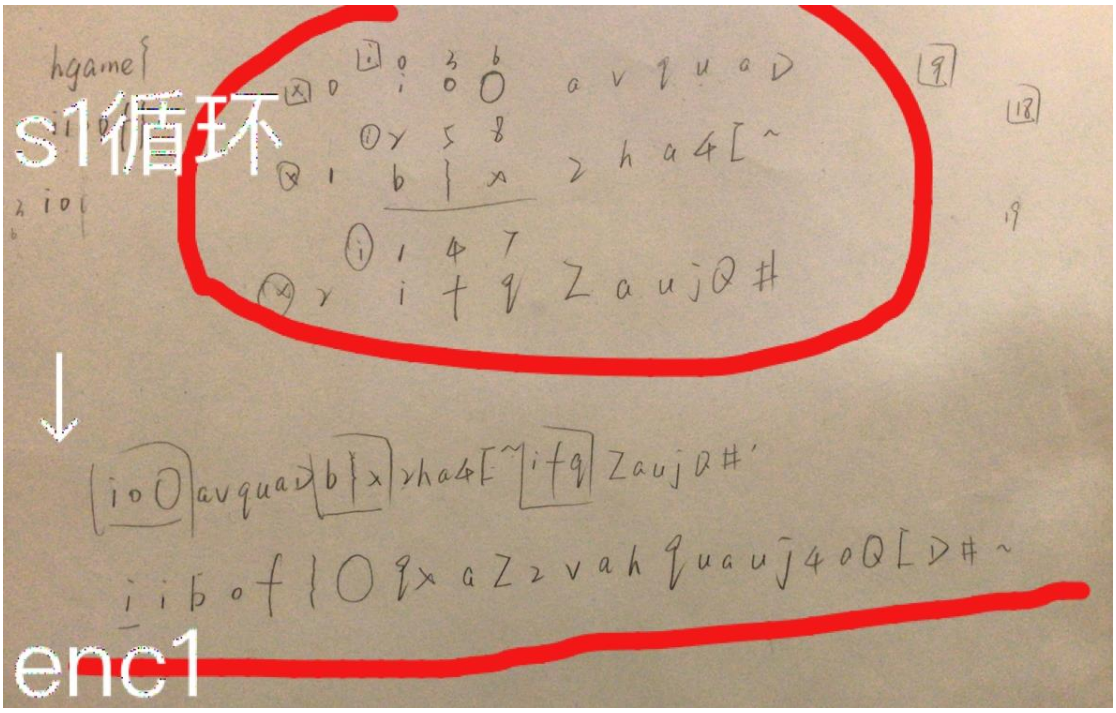
```
enc = input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))  # 奇数位 ascll 码+1 加入 enc1
        continue
    enc1.append(chr(ord(enc[i]) + 2))  # 偶数位 ascll 码+1 加入 enc1
                                        ↑得到 enc1 长度与输入的 flag，即 enc 相同
s1 = []
for x in range(3):  # 外循环三次
    for i in range(len):  # 内循环长度次
        if (i + x) % 3 == 0:
            s1.append(enc1[i])  # 得到 s1
            continue

enc2 = enc2.join(s1)  # 似乎就是 enc2 = s1
if enc2 in aaa: # 得到的 s1 字符串含于 aaa 中
    print ("You 're Right!")
else:
    print ("You're Wrong!")
    exit(0)
```

代码之外，输入的 enc 知道前五位 hgame{

从第一个循环入手，得出 enc1 的前五位 iibof}

代入 s1 的循环，

不大好说…上个草稿截图吧…



然后根据第一个循环用 ascll 码推出 flag

PWN

我..念旧，今年和去年一样…没..没做出来。

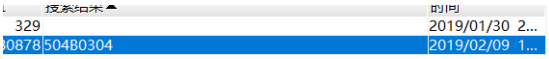
MISC

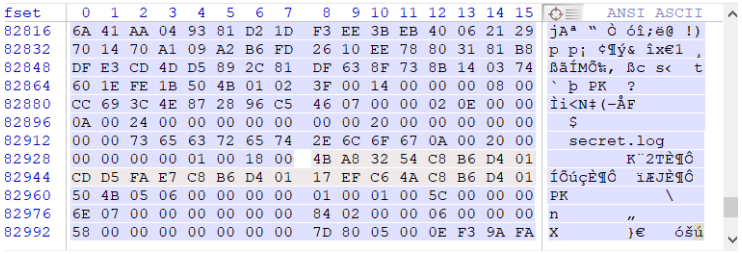
1. Are you familiar with DNS Recoders?

DNS 记录，cmd 中 nslookup 查看，从 A 查到 TXT，在 TXT 记录中找到 flag。

2. 找得到我嘛？小火汁

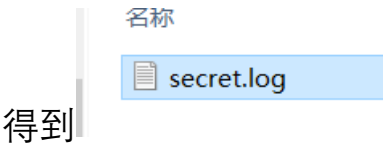
pcapng 文件 winhex 打开

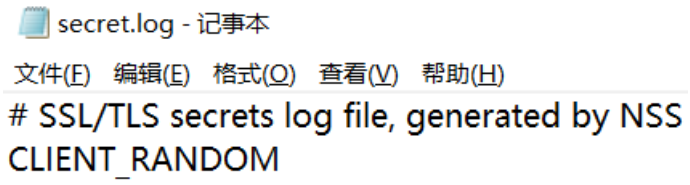




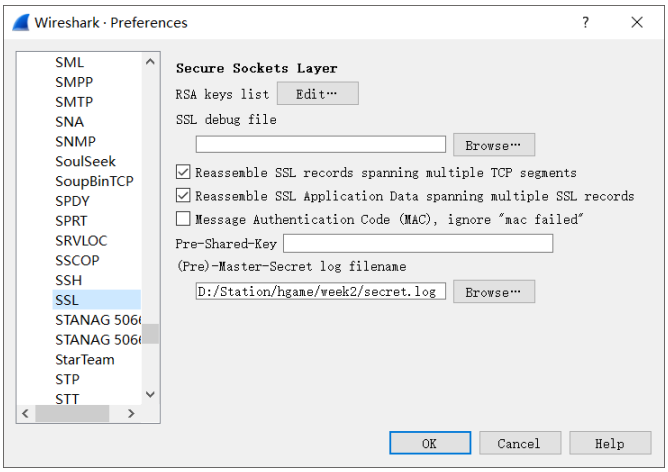
藏了个 zip，扒出来

得到

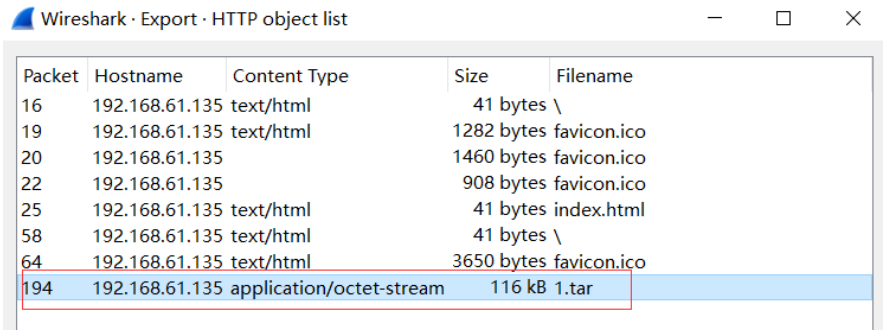




Wireshark 配置

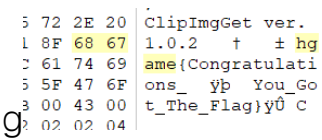


导入文件再找 http 对象



1.tar 解压得 flag.jpg

Winhex 打开得 flag



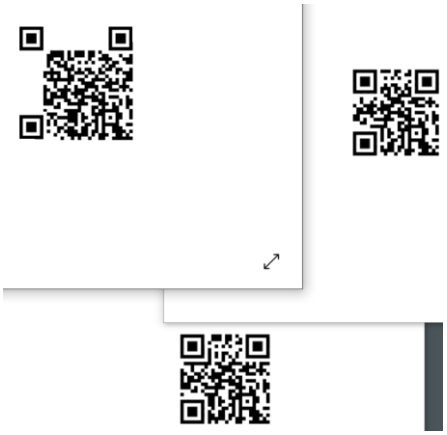
3. 初识二维码

首先呢，强调两点…一是三个“回”字的识别区，二是二维码尺寸。

题干说二维码缺损，那就尺寸往大了整…我呢…整了好久才意识到尺寸问题, 25x25 的根本啥也扫不出来嘛…

最后 ps 一共做了三张二维码,

25 的 29 的 33 的…嗯，33 的才是答案



CRYPTO

1. 浪漫的足球圣地

百度一下，嗯，曼彻斯特。

也就是曼彻斯特编码了，一共两种编码规则

1. 0x5(0101)表 00

   0x9(1001)表 10

   0x6(0110)表 01

   0xA(1010)表 11

2. 0x5(0101)表 11

   0x9(1001)表 01

   0x6(0110)表 10

   0xA(1010)表 00

本题为第一种加密方法，将文本转化后二进制转文本即可。

2. Vigener~

维吉尼亚密码，找工具复制粘贴。

由工具得出密匙 guess，flag 在明文。