攻防世界(MISC)高手进阶

原创

south_1 于 2020-11-25 13:42:18 发布 141 收藏

分类专栏： misc

本文链接：https://blog.csdn.net/doraemon12345/article/details/110120878

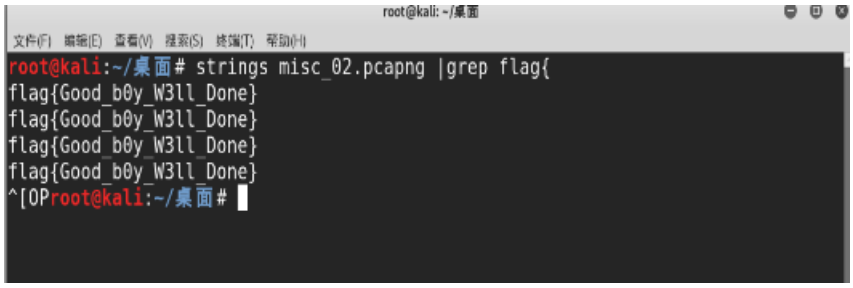
misc 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

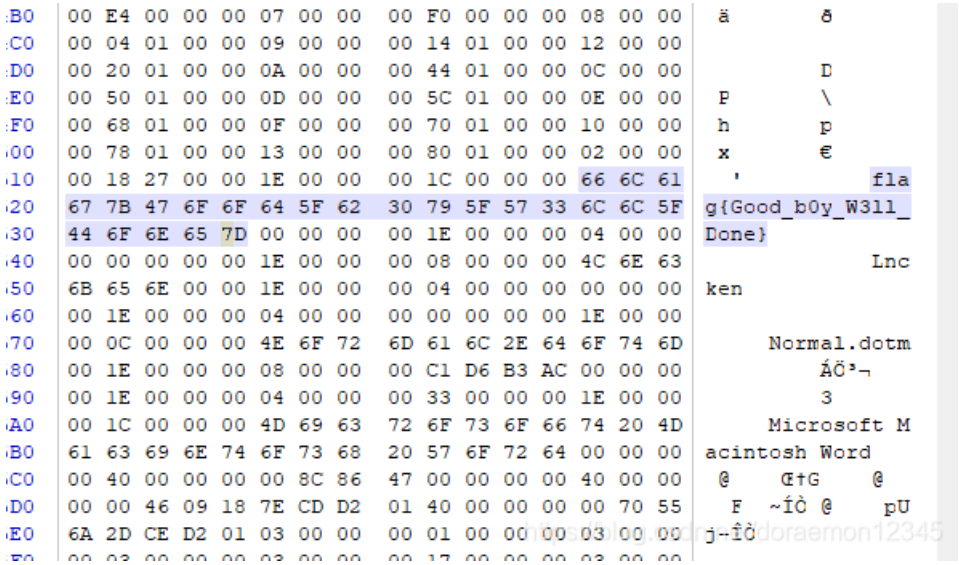
1.embarrass

下载附件是一个流量分析题，还挺大的，这个时候就很难再一个一个看了，借助工具寻找，放入kali里面执行下面一段命令



可以得到flag

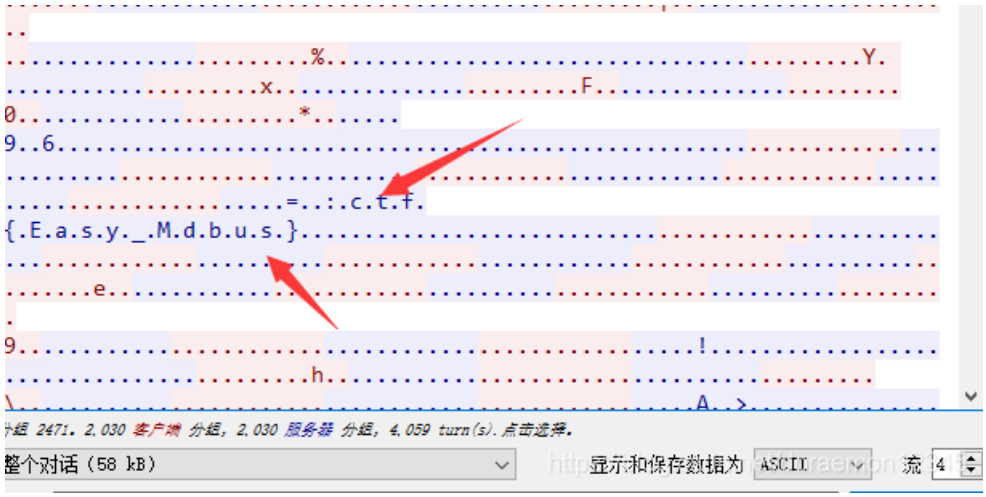
还有一种方法放入winhex里面搜索文本“flag{”



得到flag{Good_b0y_W3ll_Done}

2.神奇的Modbus

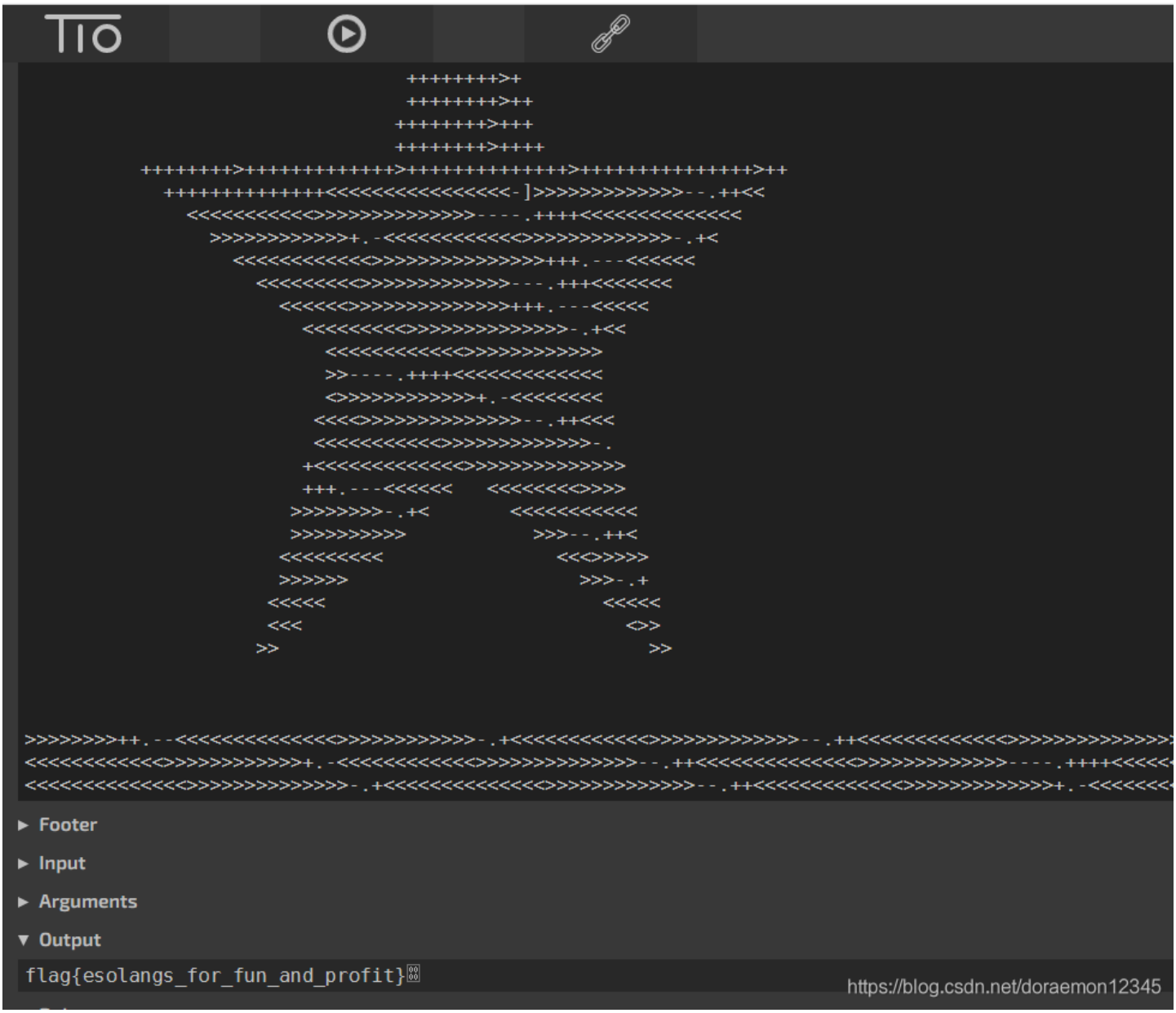
下载附件也是一道流量分析，但是文件比较小，可以先看一下在看到第四个流的时候发现flag



提交flag：ctf{Easy_Mdbus}

3.can_has_stdio?

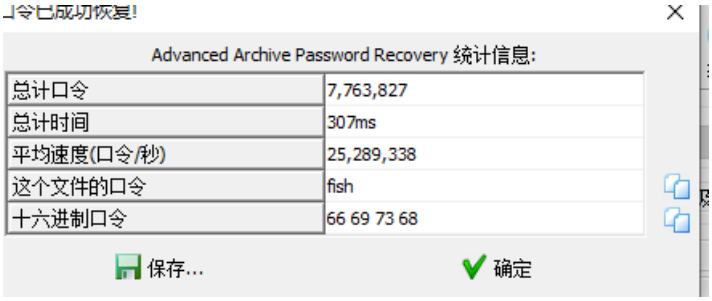
文件是一个用字符组成的五角星，这是一种加密方式brainfuck ， 找到解密网站把字符全部放进去得到flag



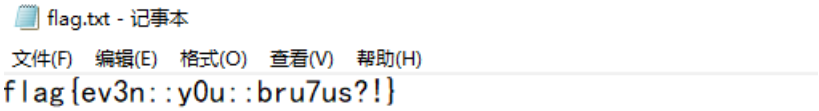
flag{esolangs_for_fun_and_profit}

4.János-the-Ripper

拿到题目放到winhex里看是一个压缩包，改一下后缀，然后发现有密码打不开，有没有提示尝试一下暴力破解，工具直接秒开密码是 fish



打开压缩包得到flag



flag{ev3n::y0u::bru7us?!}

5.Test-flag-please-ignore

下载文件用记事本打开是一串字符，猜测是16进制，拿去网上转换一下，出flag

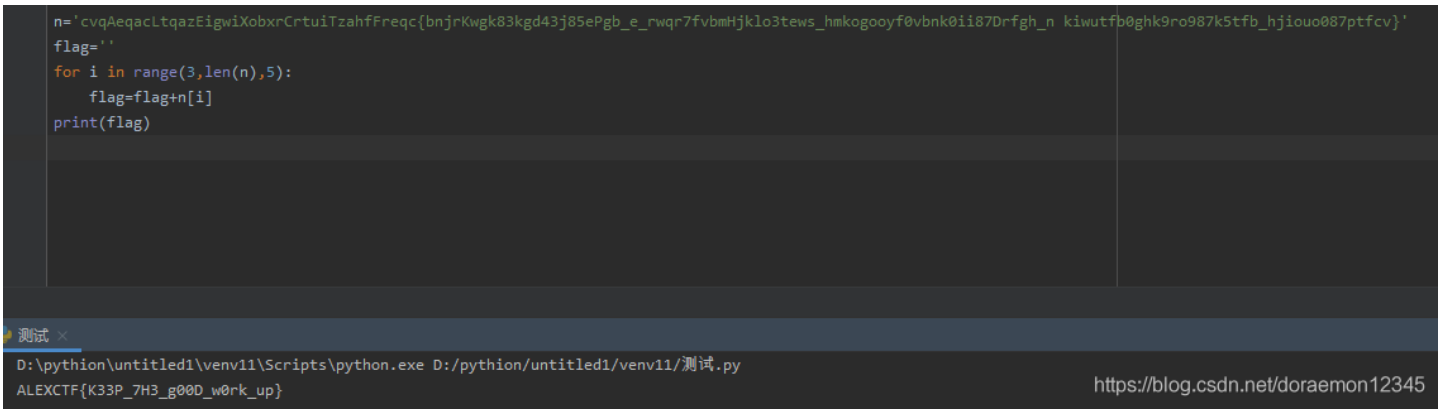
flag{hello_world}

6.hit-the-core

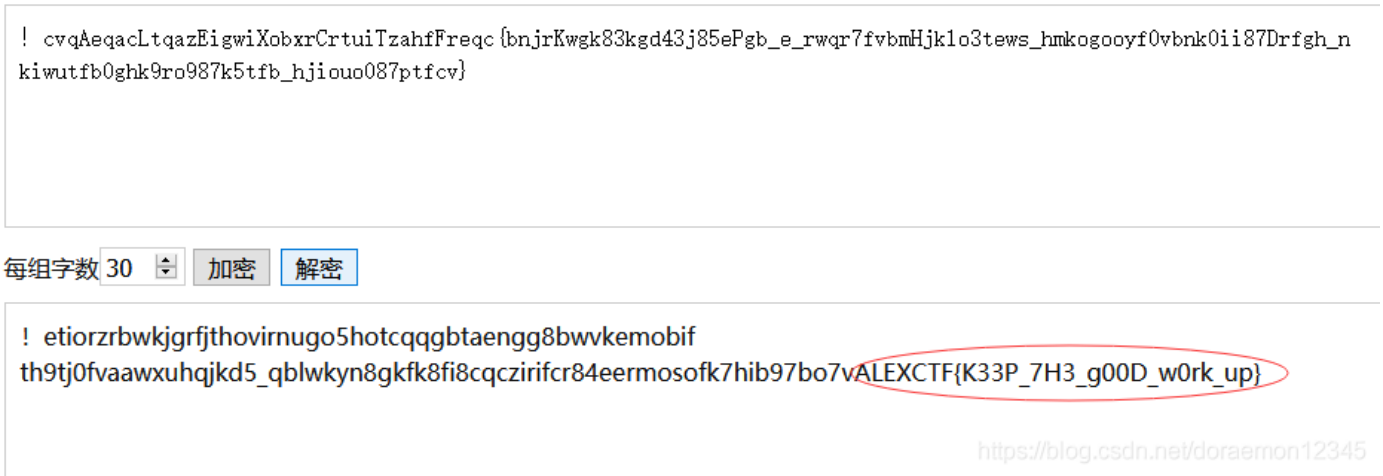
下载文件，发现是core后缀，用linux命令查看

得到一串可疑字符，仔细观察发现从第3个字符开始每过4个字符就会出现一个大写字母刚好是ALEXCTF写python脚本

```
n='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_
n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'
flag=''
for i in range(3,len(n),5):
    flag=flag+n[i]
print(flag)
```



还有一种栅栏的做法，因为得到的字符串有149位，在前面加上一个任意字符变成150位，为了便于区分加的字符可以是一些特殊符号，在网上找工具解密一下在30栏处得到flag



得到flag：ALEXCTF{K33P_7H3_g00D_w0rk_up}