

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

```
root@kali: ~/桌面
root@kali:~/桌面# strings misc_02.pcapng |grep flag{
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
flag{Good_b0y_W3ll_Done}
^[[OProot@kali:~/桌面#
```

可以得到flag

还有一种方法放入winhex里面搜索文本“flag{”

.B0	00 E4 00 00 00 07 00 00	00 F0 00 00 00 08 00 00	ä	ø
.C0	00 04 01 00 00 09 00 00	00 14 01 00 00 12 00 00		
.D0	00 20 01 00 00 0A 00 00	00 44 01 00 00 0C 00 00	P	D
.E0	00 50 01 00 00 0D 00 00	00 5C 01 00 00 0E 00 00	\	
.F0	00 68 01 00 00 0F 00 00	00 70 01 00 00 10 00 00	h	p
.00	00 78 01 00 00 13 00 00	00 80 01 00 00 02 00 00	x	€
.10	00 18 27 00 00 1E 00 00	00 1C 00 00 00 66 6C 61	'	fla
.20	67 7B 47 6F 6F 64 5F 62	30 79 5F 57 33 6C 6C 5F	g{Good_b0y_W3ll_	
.30	44 6F 6E 65 7D 00 00 00	00 1E 00 00 00 04 00 00	Done}	
.40	00 00 00 00 00 1E 00 00	00 08 00 00 00 4C 6E 63		Inc
.50	6B 65 6E 00 00 1E 00 00	00 04 00 00 00 00 00 00	ken	
.60	00 1E 00 00 00 04 00 00	00 00 00 00 00 1E 00 00		
.70	00 0C 00 00 00 4E 6F 72	6D 61 6C 2E 64 6F 74 6D		Normal.dotm
.80	00 1E 00 00 00 08 00 00	00 C1 D6 B3 AC 00 00 00		ÁÖ³~
.90	00 1E 00 00 00 04 00 00	00 33 00 00 00 1E 00 00		3
.A0	00 1C 00 00 00 4D 69 63	72 6F 73 6F 66 74 20 4D		Microsoft M
.B0	61 63 69 6E 74 6F 73 68	20 57 6F 72 64 00 00 00		acintosh Word
.C0	00 40 00 00 00 00 8C 86	47 00 00 00 00 40 00 00	@	G+G @
.D0	00 00 46 09 18 7E CD D2	01 40 00 00 00 00 70 55	F	~iÖ @ pU
.E0	6A 2D CE D2 01 03 00 00	00 01 00 00 00 03 00 00	j~iÖ	doraemon12345
.F0	00 03 00 00 00 03 00 00	00 17 00 00 00 03 00 00		

得到flag{Good_b0y_W3ll_Done}

2.神奇的Modbus

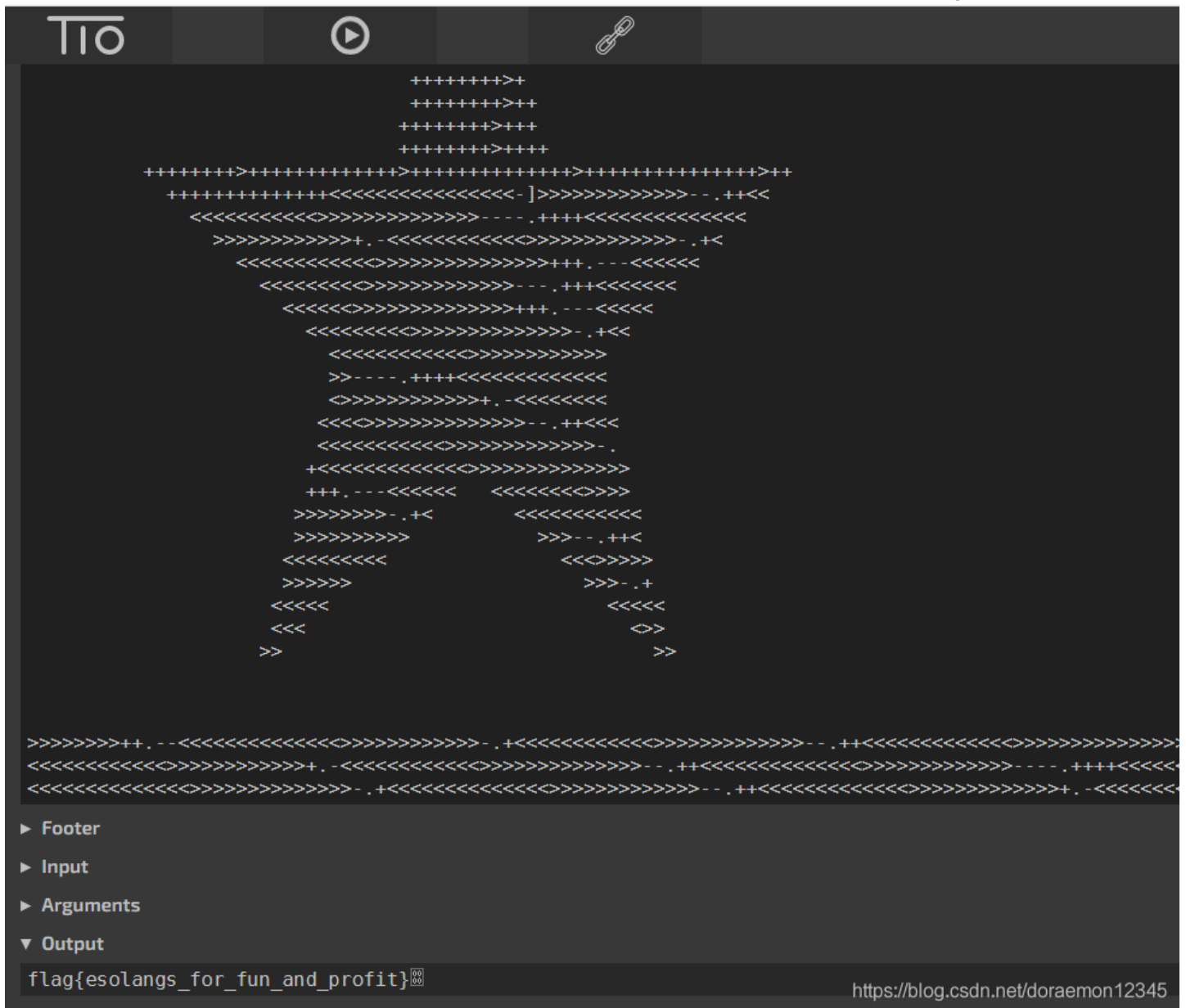
下载附件也是一道流量分析，但是文件比较小，可以先看一下在看到第四个流的时候发现flag



提交flag: ctf{Easy_Mdbus}

3.can_has_stdio?

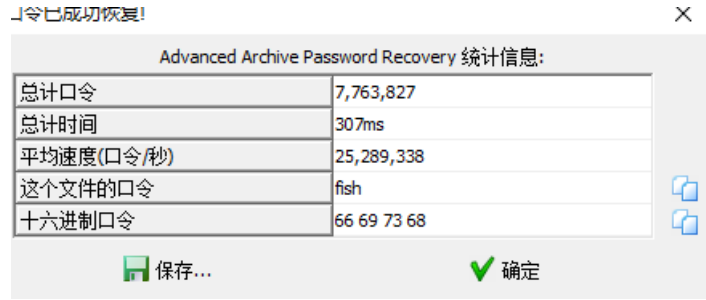
文件是一个用字符组成的五角星，这是一种加密方式brainfuck，找到解密网站把字符全部放进去得到flag



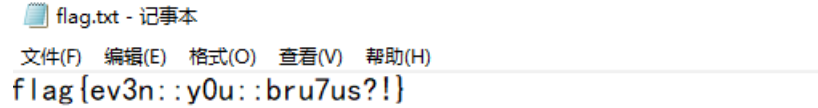
flag{esolangs_for_fun_and_profit}

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

16进制到文本字符串

加密或解密字符串长度不可以超过10M

1	666c61677b68656c6c6f5f776f726c647d
---	------------------------------------

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

 部署无服务器数据

1	flag{hello_world}
---	-------------------

<https://blog.csdn.net/doraemon12345>

flag{hello_world}

6. hit-the-core

下载文件，发现是core后缀，用linux命令查看

```
root@kali:~/桌面# strings 1.core |grep {
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n_kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
h{9e
X{9e
8{9e
0{9e
X{9e
root@kali:~/桌面#
```

<https://blog.csdn.net/doraemon12345>

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_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n_kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'
flag=''
for i in range(3,len(n),5):
    flag=flag+n[i]
print(flag)
```

```
n='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n_kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'
flag=''
for i in range(3,len(n),5):
    flag=flag+n[i]
print(flag)
```

测试 ×
D:\python\untitled1\venv11\Scripts\python.exe D:/python/untitled1/venv11/测试.py
ALEXCTF{K33P_7H3_g00D_w0rk_up}

<https://blog.csdn.net/doraemon12345>

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

```
! cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n_kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
```

每组字数

```
! etiorzrbwkjgrfjthovirnugo5hotcqgqgtaengg8bwwkemobif
th9tj0fvaawxuhqjkd5_qblwkyn8gkfk8fi8cqczirifcr84eermosofk7hib97bo7vALEXCTF{K33P_7H3_g00D_w0rk_up}
```

<https://blog.csdn.net/doraemon12345>

得到flag: ALEXCTF{K33P_7H3_g00D_w0rk_up}