2020第六届上海市大学生网安大赛Misc|writeup

原创

lSMidi 于 2020-11-17 18:18:25 发布 199 收藏 1

分类专栏： Misc 文章标签： python

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/wanmiqi/article/details/109748705

版权

Misc 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

2020第六届上海市大学生网安大赛Misc|writeup

Misc

签到


```
{echo,ZmxhZ3t3MzFjMG1lNX0=}|{base64,-d}|{tr,5,6}
```

直接linux下执行

```
$bash -f main.sh
flag{w31c0me6}
```

```
flag{w31c0me6}
```

pcap

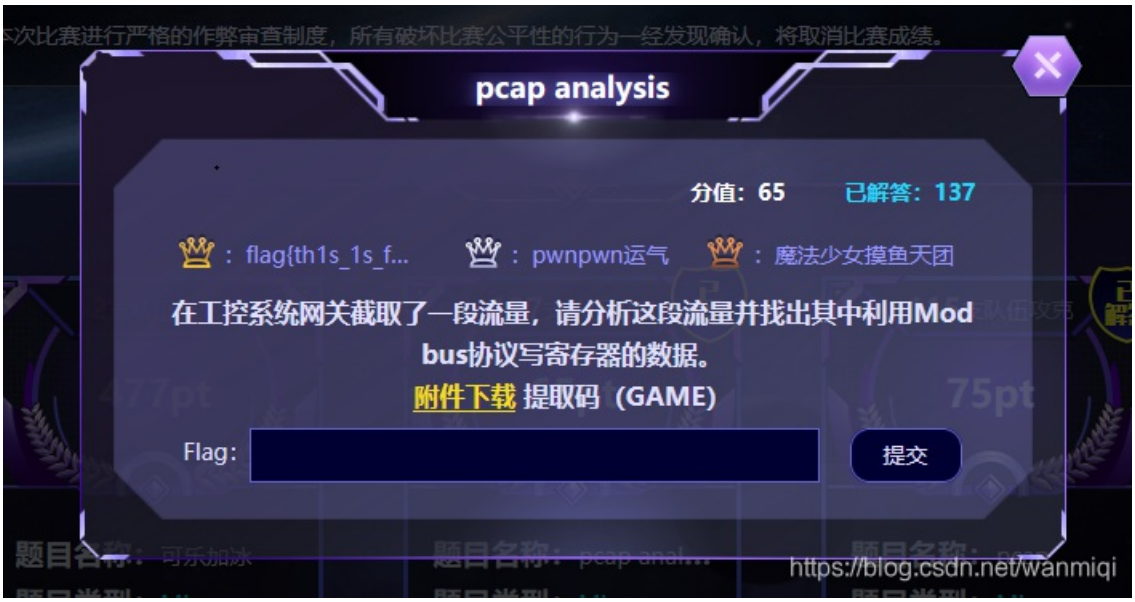
附件: https://pan.baidu.com/s/1BBZKygsXsdpKpIMVOnvYUQ(qu2b)

观察dnp3协议response包，在长度为91的前几个包的layer messages中看到flag{字样，顺序拼接所有包同位置上的字符得到flag。

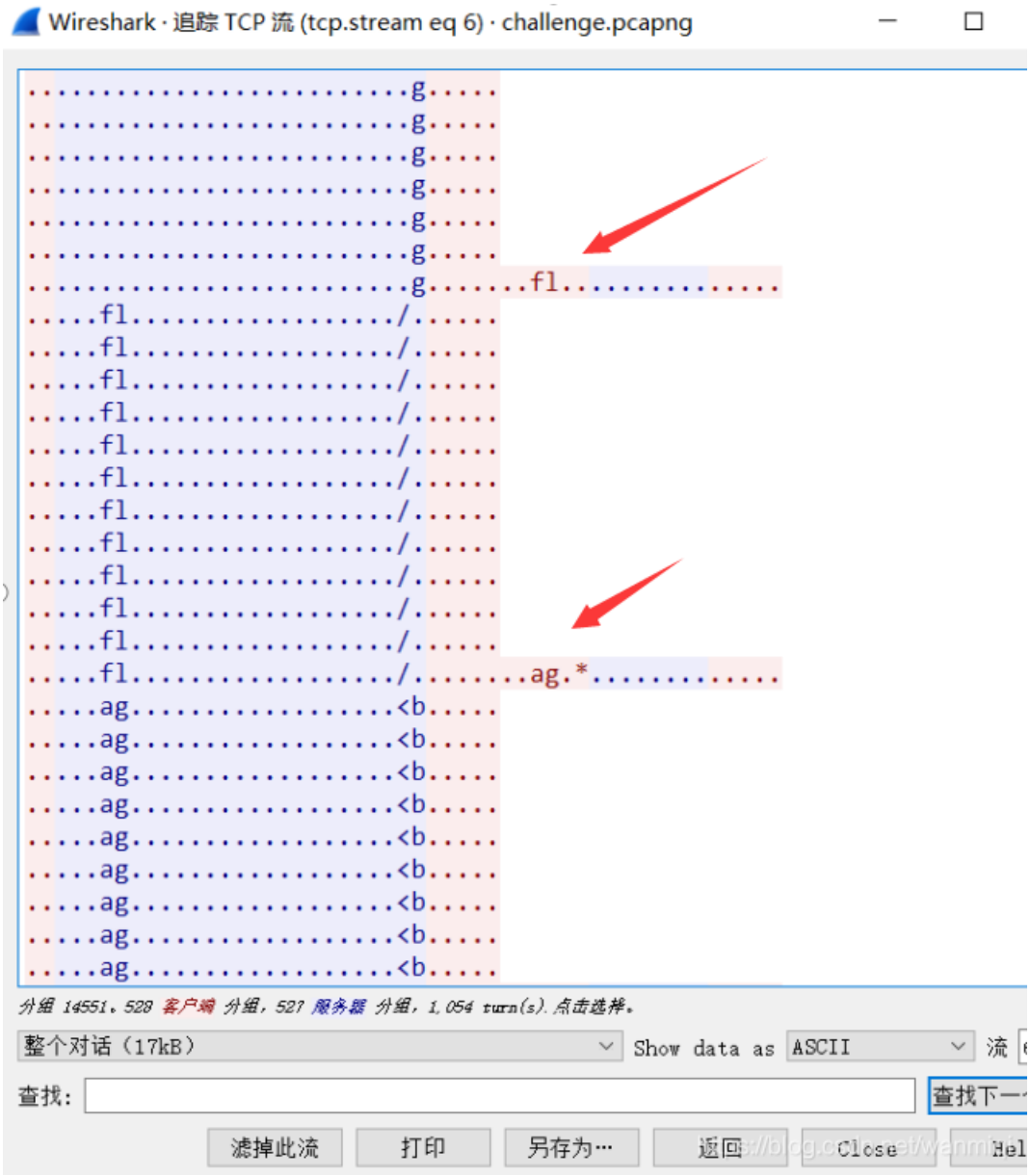
```
flag{d989e2b92ea671f5d30efb8956eab1427625c}
```

pcap analysis

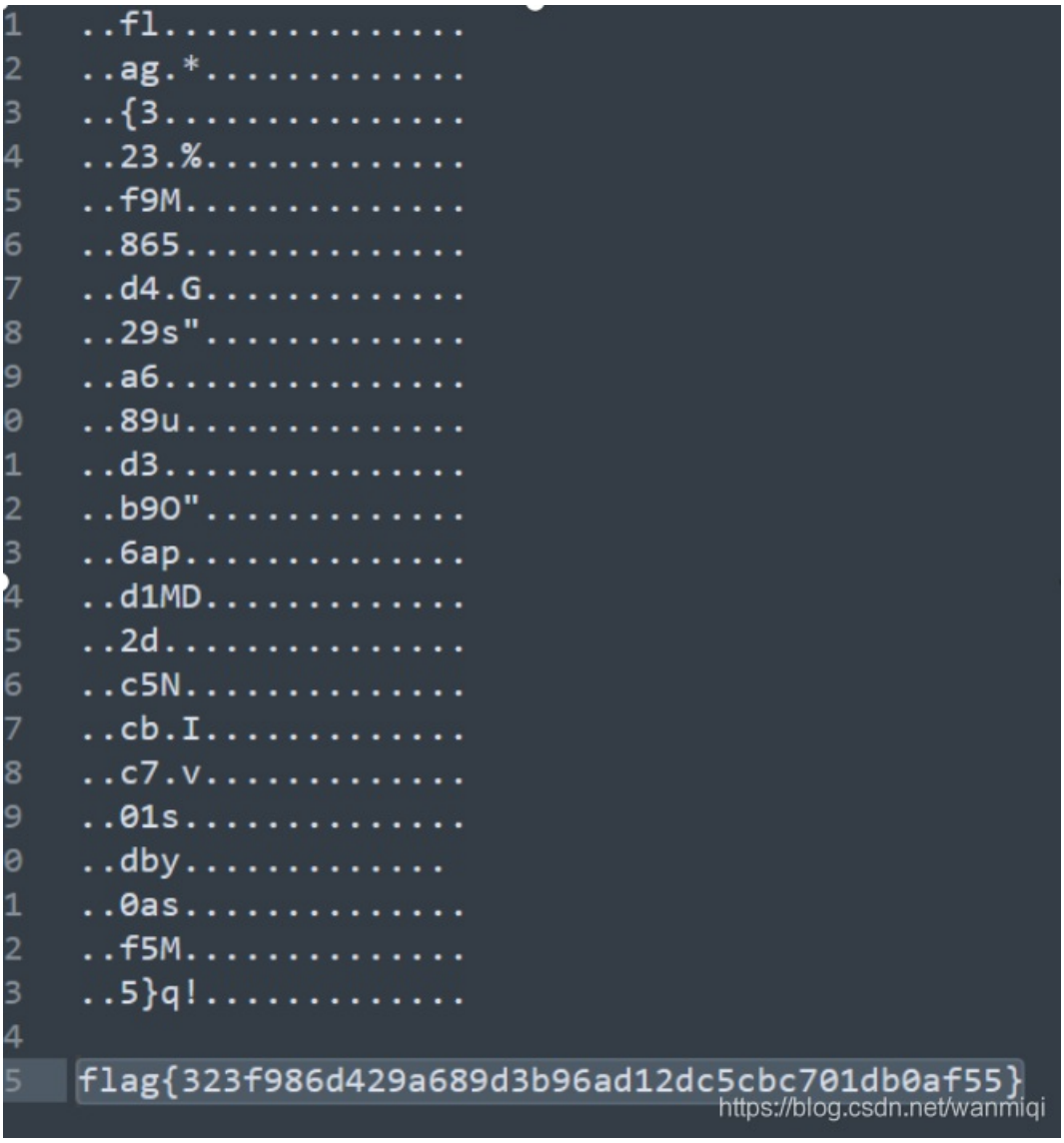
附件:https://pan.baidu.com/s/1N8fOQP2cYC1cUxEMs5yhaA(0weo)



追踪任一ProtocolModbus/TCP的TCP流



发现flag字样 然后拼接第三位第四位下就好了




```
flag{323f986d429a689d3b96ad12dc5cbc701db0af55}
```

可乐加冰

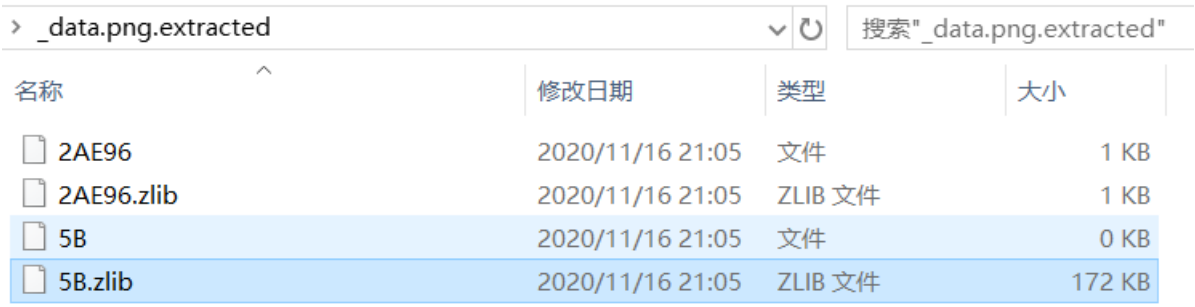
附件: https://pan.baidu.com/s/1qFK1qiXAnFv6ebDXlVxrQg(kqg1)

附件下一张图片 data.png

图片隐写 拿binwalk分析下

```
PS C:\Users\HP\Desktop\CTF> python C:\python\Scripts\binwalk .\data.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 498 x 887, 8-bit/color RGBA, non-interlaced
91            0x5B            Zlib compressed data, compressed
175766        0x2AE96         Zlib compressed data, default compression
```

binwalk -e 来分离下文件



https://blog.csdn.net/wanmiqi

hexdump看下十六进制

```
hexdump 2AE96
```

```
000000  83 46 36 36 36 95 43 83 46 36 95 95 36 43 83 46
000010  95 95 95 43 83 46 95 95 36 43 83 46 36 36 36 36
000020  43 83 46 36 36 36 95 43 83 46 36 95 95 36 43 83
000030  46 95 95 36 43 34 45 34 43 83 46 36 95 36 36 43
000040  83 46 36 95 36 95 43 83 46 36 36 95 36 43 83 46
000050  36 36 95 43 34 45 34 43 83 46 36 95 95 43 83 46
000060  36 95 36 95 43 83 46 36 36 36 36 43 83 46 36 36
000070  36 43 34 45 34 43 83 46 36 95 95 36 43 83 46 36
000080  95 95 36 43 83 46 36 36 95 43 83 46 95 36 36 43
000090  34 45 34 43 83 46 36 36 95 36 43 83 46 36 95 36
0000a0  95 43 83 46 36 36 95 36 43 83 46 36 95 95 95 43
0000b0  83 46 95 95 36 43 83 46 95 36 95 43 83 46 36 36
0000c0  36 36 43 83 46 36 95 36 43 83 46 36 36 95 43 83
0000d0  46 95 36 95 43 83 46 36 95 95 43 83 46 36 36 95
0000e0  36
```

https://blog.csdn.net/wanmiqi

将十六进制数据拿出来转ASCII

```
with open('./test.txt','r') as file:
 line = file.read()
 for i in range(0,len(line),2):
  print(chr(int(line[int(i):int(i+2)])),end="")
```

```
PS C:\Users\HP\Desktop\CTF> python.exe C:\Users\HP\Desktop\CTF\toASCII.py
S.$$$_+S.$__$+S.___+S.__$+S.$$$$+S.$$$_+S.$__$+S.__$+"-"+S.$_$$+S.$_$_+S.$$_$+S.$$_+"-"+S.$__+S.$_$_+S.$$$$+S.$$$+"-"+S.$__$+S.$__$+S.$$_+S._$$+"-"+S.$$_$+S.$_$_+S.$$_$+S.$___+S.__$+S._$_+S.$$$$+S.$_$+S.$$_+S._$_+S.$__+S.$$_$
```

```
S.$$$_+S.$__$+S.___+S.__$+S.$$$$+S.$$$_+S.$__$+S.__$+"-"+S.$_$$+S.$_$_+S.$$_$+S.$$_+"-"+S.$__+S.$_$_+S.$$$$+S.$$$+"-"+S.$__$+S.$__$+S.$$_+S._$$+"-"+S.$$_$+S.$_$_+S.$$_$+S.$___+S.__$+S._$_+S.$$$$+S.$_$+S.$$_+S._$_+S.$__+S.$$_$
```

S. 第一直觉想到了Jquery(.)将所有S改成

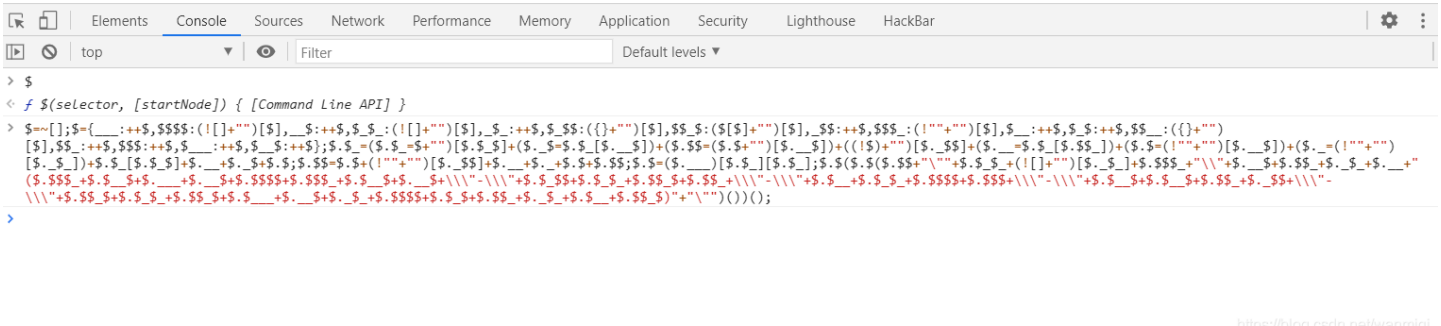
```
s = ''

with open('./test.txt','r') as file:
 line = file.read()
 for i in range(0,len(line),2):
  s += chr(int(line[int(i):int(i+2)]))


s = s.replace("S","$")
print(s)
```

```
$.$$$_+$.$__$+$.___+$.__$+$.$$$$+$.$$$_+$.$__$+$.__$+"-"+$.$_$$+$.$_$_+$.$$_$+$.$$_+"-"+$.$__+$.$_$_+$.$$$$+$.$$$+"-"+$.$__
$+$.$__$+$.$$_+$._$$+"-"+$.$$_$+$.$_$_+$.$$_$+$.$___+$.__$+$._$_+$.$$$$+$.$_$+$.$$_+$._$_+$.$__+$.$$_$
```

只有符号的JS JJEncode 拿去解密下

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$
$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($._
_=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___
)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_$_+(![]+"")[$._$_]+$.$$_+"\\"+$.__$+$.$_+$._$_+$.__+"($.$$_+$.$__$+$.___+$.__$+$.$$$$+$.$$_+
$.$__$+$.__$+\\\"-\\\"+$.$_$$+$.$_$_+$.$$_$+$.$$_+\\\"-\\\"+$.$__+$.$_$_+$.$$$$+$.$$$+\\\"-\\\"+$.$__$+$.$__$+$.$$_+$._$$+\\\"-\\\"+$.$$
_$+$.$_$_+$.$$_$+$.$___+$.__$+$._$_+$.$$$$+$.$_$+$.$$_+$._$_+$.$__+$.$$_$)"+"\"")())();
```

浏览器中直接执行就行了



https://blog.csdn.net/wanmiqi

```
flag{e901fe91-bad6-4af7-9963-dad812f5624d}
```

参考

PNG文件IDAT块隐写：

https://www.cnblogs.com/loo5mity/p/9537911.html

https://blog.csdn.net/qq_29647709/article/details/81876374

Python脚本对zlib的压缩解压详解和一些例子：

https://blog.csdn.net/qq_40574571/article/details/80164981