神奇的数据

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 哈尔滨站
Challenge | 2019 | 工业信息安全技能大赛 | 哈尔滨站 | 神奇的数据

点击此处获得更好的阅读体验

WriteUp来源

https://www.cnpanda.net/ctf/415.html

题目描述

> *通过网络分析仪器采集的电力传输网络通信数据，请分析出数据中的异常。flag格式{}*

题目考点

解题思路

使用搜索引擎搜了下ETHER没搜出什么有价值的信息，看见一堆ACSII码，不管这么多，先来一发ASCII变成标准字符.

逻辑为提取|0开始的行，然后把后面的ASCII转换为标准的byte。
然后看了下，这包很像MMS的数据包。

联想到第2题。根据MMS的协议规则，有效的数据包都是成对出现的：

而且在其中找到了flag字样，因此把flag转换为66|6c|61|67|

在原始的stream.exe中搜索可见

直接把71769这行flag后面那一节通过转换工具查看

```
1 flag¡? :
2 PL1012{ROT
3 PL1012CTRL     PL1012LD0
4 PL1012MEAS     PL1012RC}
```

看了下结构，然后猜了下，删除掉`PL1012`，flag就出来了

Flag

```
1 flag{ROTCTRLLD0MEASRC}
```

- ***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/哈尔滨站/uVESEDwsXnxNc92y98vM5L.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 # 哈尔滨站
窃取数据的黑客
flag在哪