S7Common

2021-09-05 | Challenge， 2021， 第七届全国工控系统信息安全攻防竞赛， 四类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 四类 | S7Common

点击此处获得更好的阅读体验

WriteUp来源

来自 毕方安全实验室 战队

题目描述

> 查看工控数据包，获取隐藏的信息。flag格式:flag{xxxxxx}

提示信息

无

题目考点

- 流量分析
- 西门子S7Comm协议

解题思路

下载附件后使用Wireshark打开

过滤出 `s7comm` 包，之后进行TCP follow发现flag字样

使用条件 `s7comm && ip.addr==192.168.1.200 && s7comm.param.func==0x04` 过滤出相关数据

逐一按地址检索得到：

```
45-49flag{
50 U  190
51 2  198
52 F  1a0
53 s  1a8
54 d  1b0
55 _  1b8
56 G  1c0
57 V  1c8
58 k  1d0
59 X  1d8
60 1  1e0
61 9  1e8
62 r  1f0
63 _  1f8
64 2  200
65 7  208
66 h  210
67 E  218
68 Y  220
69 K  228
70 }
```

根据题目提示去掉不可显示字符即可获得flag

Flag

```
flag{U2Fssd_GVkX19r_7hEEYK}
```


Challenge # 2021 # 第七届全国工控系统信息安全攻防竞赛 # 四类

similarPic IEC104