异常的S7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 | 异常的S7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

> *这是一个S7comm协议的数据包。但是流量中存在一条异常写入的数据。找出异常流量的ascii数据流。flag格式为flag{ascii数据流}*

题目考点

- *流量分析*
- *S7Comm协议分析*

解题思路

下载题目所给的flag.pcapng，发现有57万个包，还是蛮多的。

在过滤器中输入s7comm

过滤后数量没什么变化，还是57万多个

然后观察包内容，使用过滤语句

```
1 s7comm.header.rosctr == 3 & s7comm.data.returncode == 0xff
```

发现包数量为288305

然后加上初始化通信的包，刚好占一半，说明所有发送都是成功接收的。

因此就不需要看Ack_Data。使用s7comm.header.rosctr == 1过滤语句，查看ROSCTR为Job的Write Var的数据包，发现写的数据长度均为10。基于这些信息，开始进入写代码筛选阶段。

编写了下面的筛选代码：对所有长度113的包进行过滤，最开始走了不少弯路，以为是把后面变化的字节过滤出来，进行合并，然后还原flag的。

从过滤出来的数据中还真看到和flag字样有关的信息，在这浪费了不少时间。

没看出个所以然后，突然灵光一现，是不是前面的0xffff会有不同的呢，于是写了下面的代码：

经过验证，只有一个包符合这个条件。

flag即为这串数据

Flag

```
flag{FFAD28A0CE69DB34751F}
```


 # Challenge # 2019 # 工业信息安全技能大赛 # 哈尔滨站
恶意软件样本分析
IoT