损坏的风机

2021-09-01 | Challenge， 2021， 工业信息安全技能大赛， 线上赛-第一场

Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | 损坏的风机

点击此处获得更好的阅读体验

WriteUp来源

来自 Venom 战队

题目描述

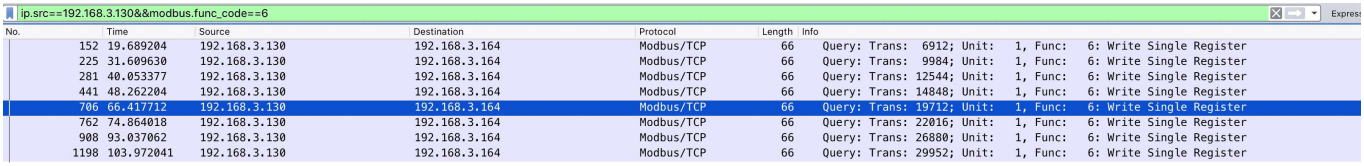
> 小明是一家新能源汽车制造厂的风机操作员，每天的工作是根据工厂的实时温度输入风机的转数，但由于机器的老化，风机最多能接受2000转/分钟的转速，在当天下班后，检修人员发现风机由于转速过快出现了故障，请根据维修人员捕获的流量包分析当天风机的转速达到了多少转才出现的故障，flag为发送高额转速的Data层的HEX数据。flag格式为:flag{}

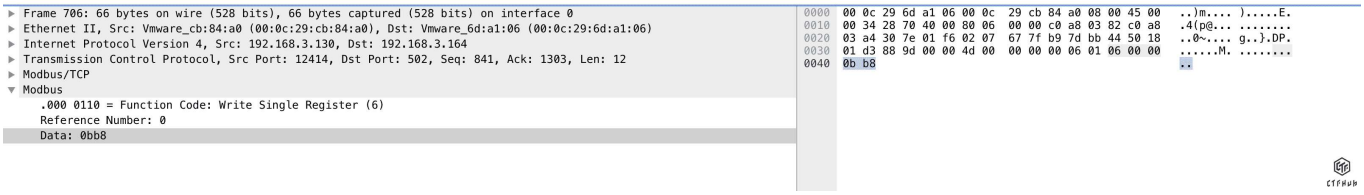
题目考点

- 流量分析
- modbus协议分析

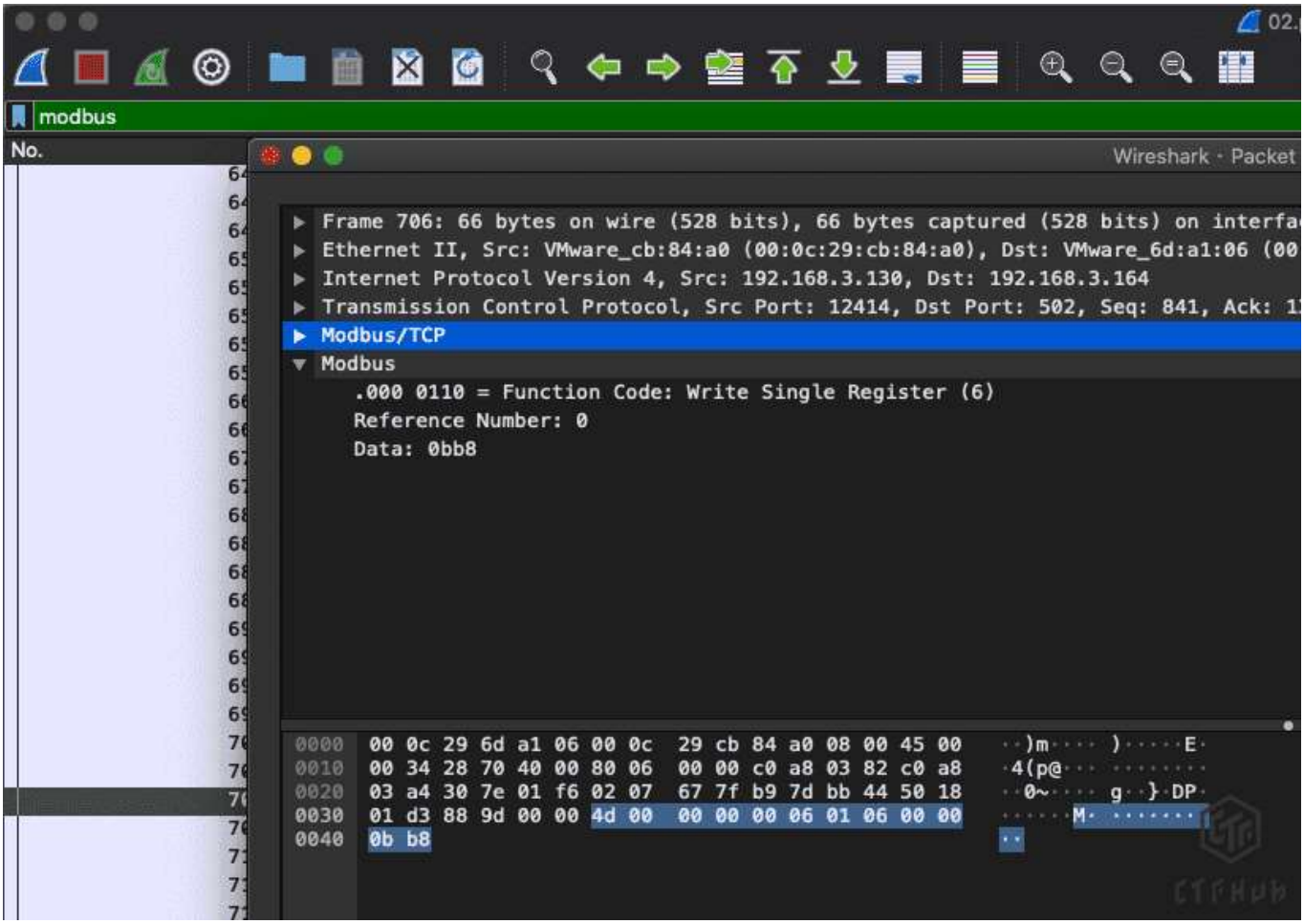
解题思路

打开附件为modbus流量，分析流量找到写入相关数据包





该数据包即为风机转速调整，其中 `0x0bb8` 为 `3000` ， 表示修改转速到3000



Flag

```
1  flag{4d000000000610600000bb8}
```


Challenge # 2021 # 工业信息安全技能大赛 # 线上赛-第一场

简单的梯形图 工控现场里异常的文件