



# 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

No.	Time	Source	Destination	Protocol	Length	Info
152	19.689204	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 6912; Unit: 1, Func: 6: Write Single Register
225	31.609630	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 9984; Unit: 1, Func: 6: Write Single Register
281	40.053377	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 12544; Unit: 1, Func: 6: Write Single Register
441	48.262204	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 14848; Unit: 1, Func: 6: Write Single Register
706	66.417712	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 19712; Unit: 1, Func: 6: Write Single Register
762	74.864018	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 22016; Unit: 1, Func: 6: Write Single Register
908	93.037062	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 26880; Unit: 1, Func: 6: Write Single Register
1198	103.972041	192.168.3.130	192.168.3.164	Modbus/TCP	66	Query: Trans: 29952; Unit: 1, Func: 6: Write Single Register

  

▶ Frame 706: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_cb:84:a0 (00:0c:29:cb:84:a0), Dst: Vmware\_6d:a1:06 (00:0c:29:6d:a1:06)  
 ▶ Internet Protocol Version 4, Src: 192.168.3.130, Dst: 192.168.3.164  
 ▶ Transmission Control Protocol, Src Port: 12414, Dst Port: 502, Seq: 841, Ack: 1303, Len: 12  
 ▶ Modbus/TCP  
 ▼ Modbus  
 .000 0110 = Function Code: Write Single Register (6)  
 Reference Number: 0  
 Data: 0bb8

0000 00 0c 29 6d a1 06 00 0c 29 cb 84 a0 08 00 45 00 ..)m....).....E.  
 0010 00 34 28 70 40 00 80 06 00 00 c0 a8 03 82 c0 a8 .4(p@....  
 0020 03 a4 30 7e 01 f6 02 07 67 7f b9 7d bb 44 50 18 ..0~...g...}..DP.  
 0030 01 d3 88 9d 00 00 4d 00 00 00 00 06 01 06 00 00 .....M.....  
 0040 0b b8

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

Wireshark - Packet

▶ Frame 706: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_cb:84:a0 (00:0c:29:cb:84:a0), Dst: Vmware\_6d:a1:06 (00:0c:29:6d:a1:06)  
 ▶ Internet Protocol Version 4, Src: 192.168.3.130, Dst: 192.168.3.164  
 ▶ Transmission Control Protocol, Src Port: 12414, Dst Port: 502, Seq: 841, Ack: 1303, Len: 12  
 ▶ Modbus/TCP  
 ▼ Modbus  
 .000 0110 = Function Code: Write Single Register (6)  
 Reference Number: 0  
 Data: 0bb8

0000 00 0c 29 6d a1 06 00 0c 29 cb 84 a0 08 00 45 00 ..)m....).....E.  
 0010 00 34 28 70 40 00 80 06 00 00 c0 a8 03 82 c0 a8 .4(p@....  
 0020 03 a4 30 7e 01 f6 02 07 67 7f b9 7d bb 44 50 18 ..0~...g...}..DP.  
 0030 01 d3 88 9d 00 00 4d 00 00 00 00 06 01 06 00 00 .....M.....  
 0040 0b b8

```

>>> 0x0bb8
3000
>>> 0x012b
299
>>> 0x012b
  
```

# Flag



```
1 flag{4d00000000006010600000bb8}
```

**本文作者：** CTFHub

**本文链接：** <https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/线上赛-第一场/feG6B8GqBJkg3jv7ZHuZjX.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](#)

[# 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 >](#)

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动