不安全的组件

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2020 ， 工业信息安全技能大赛 ， 石家庄站
Challenge | 2020 | 工业信息安全技能大赛 | 石家庄站 | 不安全的组件

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *工控生产环境内网中使用了不安全的组件，致使黑客突破隔离内网进入工控环境，安全员捕获到相关流量，请分析相关流量。flag格式为：flag{}。----本题由恒安嘉新贡献*

题目考点

解题思路

拿到pacp文件后，筛选http流量

将modbus3.pcapng数据包通过winhex还原。

筛选modbus流量，通过modbus的方法4写寄存器1的并且有响应的为黑客写入成功的流量，每四位写入，全部还原成出来为16进制

```
3433
0928
4338
0001
8445
6228
7119
5029
8777
7431
8527
4044
9263
3948
3215
0897
9
```

整串数字拼起来转换为16进制之后转换为字符串即为flag

Flag

```
flag{St0p_all_machine_explosi0ns}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/石家庄站/3XWM6eeB7Px5hbG9CADgaQ.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 # 2020 # 工业信息安全技能大赛 # 石家庄站
奇怪的声音

工厂恶意攻击分析