工控协议数据分析

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 ， 湖州站
Challenge | 2020 | 工业信息安全技能大赛 | 湖州站 | 工控协议数据分析

点击此处获得更好的阅读体验

WriteUp来源

转自https://www.hyluz.cn/?id=98

题目描述

> *运维人员在某工控环境内网发现内网控制系统被攻破,附件为从现场抓取的报文, 请通过分析报文,得出黑客都获取到了哪些信息?flag格式为:flag{}。*

题目考点

- *流量分析*
- *S7Comm协议分析*

解题思路

Wireshark打开

发现部分S7COMM请求是带data的，data中含有bin数据，分析之后发现所有的`Job`中`Write Var`是含有flag的二进制的，把所有bin数据提取出来


```
01100110
01101100
01100001
01100111
01111011
01100110
01101100
01100001
01100111
01011111
01101001
01110011
01011111
01101000
01100101
01110010
01100101
01111101
```

bin转ascii即可

Flag

```
flag{flag_is_here}
```

- ***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/湖州站/eNzz47uvuhE3bBjVN1jyuy.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 # 湖州站

IEC
S7ccoomm