工业网络设备逆向

发表于 2021-02-16 分类于 Challenge， 2019， 工业信息安全技能大赛， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 工业网络设备逆向

点击此处获得更好的阅读体验

WriteUp来源

题目描述

> *这是一个工业系统中使用的路由器，系统的tddp协议存在远程代码执行漏洞。请找出并分析tddp协议的执行过程，并回答以下问题：1. 远程执行命令的消息类型为？（格式为CMD_???_???） 2. 在tddp协议中第几个字节等于什么时，可以控制发出远程命令执行的消息 （FLAG格式为16进制）*

题目考点

解题思路

Flag

```
1 1
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/r7NEo8baEUAAUkXekEWW9D.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 # 2019 # 工业信息安全技能大赛 # 深圳站
二次设备固件逆向
隐信道数据安全分析