

工控安全取证

发表于 2021-01-25 更新于 2021-02-16 分类于 [Challenge](#) , [2019](#) , [工业信息安全技能大赛](#) , [山东站](#)
[Challenge](#) | [2019](#) | [工业信息安全技能大赛](#) | [山东站](#) | [工控安全取证](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自MOIN战队

题目描述

有黑客入侵工控设备后在内网发起了大量扫描，而且扫描次数不止一次。请分析日志，指出对方第4次发起扫描时的数据包的编号，flag形式为flag{}

题目考点

- 流量分析

解题思路

分割数据包，找到第4个TCP连接，然后提交附近的几个包序号

□

Flag

```
1 flag{155989}
```

- 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/山东站/dwKedf4JDKzqlxyzqDXspad.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](#) [#山东站](#)

[隐藏的黑客](#)

[恶意软件后门分析](#)