CTFHub

Writeup

Q

S7Common

 □ 2021-09-05 | □ Challenge , 2021 , 第七届全国工控系统信息安全攻防竞赛 , 四类

 Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 四类 | S7Common

点击此处获得更好的阅读体验

WriteUp来源

来自 毕方安全实验室 战队

题目描述

查看工控数据包, 获取隐藏的信息。flag格式:flag{xxxxxx}

提示信息

无

题目考点

- 流量分析
- 西门子S7Comm协议

解题思路

下载附件后使用Wireshark打开

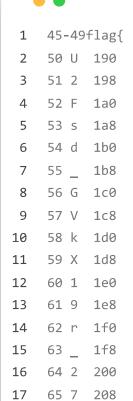
过滤出 s7comm 包, 之后进行TCP follow发现flag字样



使用条件 s7comm && ip.addr==192.168.1.200 && s7comm.param.func==0x04 过滤出相关数据



逐一按地址检索得到:



66 h 210

68 Y 220

69 K 228

19 67 E 218

70 }

18

20

21

22

根据题目提示去掉不可显示字符即可获得flag

Flag



1 flag{U2Fssd_GVkX19r_7hEEYK}

本文作者: CTFHub

本文链接: https://writeup.ctfhub.com/Challenge/2021/第七届全国工控系统信息安全

攻防竞赛/四类/iYGfxF9Cf4chNPy9DTQynb.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 ➡ # 第七届全国工控系统信息安全攻防竞赛

⟨ similarPic | IEC104 ⟩

四类

© 2019 – 2022 **CTFHub**

由 Hexo & NexT.Gemini 强力驱动