



2

📅 2021-08-30 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-兰州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-兰州站 | 02

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自 M01N 战队

题目描述

某工厂怀疑被黑客入侵，工程人员在分析西门子传输协议时，截获一段报文如下：
0300002402f080320100000009000e00050501120a100100010000830000290003000
101 请解读协议内容，并准确的拿到返回值，返回值即为flag，flag形式为flag{}

题目考点

- 流量分析
- S7Comm协议

解题思路

利用S7Comm协议的脚本将该段报文发送至S7Comm的服务器端（PLC-SIM），wireshark抓取返回报文，报文中的payload即为flag

No.	Time	Source	Destination	Protocol	Length	Info
1002	10.103862	10.65.60.231	10.65.60.102	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
1006	10.106756	10.65.60.102	10.65.60.231	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
1007	10.106882	10.65.60.231	10.65.60.102	S7COMM	90	ROSCTR:[Job] Function:[Write Var]
1009	10.110764	10.65.60.102	10.65.60.231	S7COMM	76	ROSCTR:[Ack_Data] Function:[Write Var]


```

0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window size value: 4096
  [Calculated window size: 4096]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x7e82 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
  TCP payload (22 bytes)
> TPKT, Version: 3, Length: 22
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> S7 Communication
<Wireshark Lua fake item>
0000  00 0e c6 51 49 50 e0 dc a0 fc 7f 67 08 00 45 00  ...QIP... ..g..E.
0010  00 3e 00 1a 00 00 1e 06 0e d2 0a 41 3c 66 0a 41  ->..... ..Ackf.A
0020  3c e7 00 66 d8 45 00 02 f9 92 cd 1b 5c cc 50 18  <..f.E... ..\..P.
0030  10 00 7e 82 00 00 03 00 00 16 02 f0 80 32 03 00  ..... ..-2..
0040  00 00 09 00 02 00 01 00 00 05 01 ff             ..... ..

```



Flag



1 flag{0300001602F0803203000000090002000100000501FF}

本文作者： CTFHub

本文链接： <https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-兰州站/3PPVQd6MGniVb7pGL54CQv.html>

版权声明： 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge](#)
[# 2021](#)
[# 工业信息安全技能大赛](#)
[# 巡回赛-兰州站](#)

< 11

10 >

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动