


工控CTF之协议分析6——s7comm

原创 Shadow丶S 于 2022-12-20 21:15:54 发布 1737 收藏 6 版权

分类专栏: CTF刷题 工控 文章标签: 安全 网络协议

 CTF刷题 同时被 2 个专栏收录

8 订阅 27 篇文章 订阅专栏

协议分析

流量分析

主要以 **工控** 流量和恶意流量为主，难度较低的题目主要考察Wireshark使用和找规律，难度较高的题目主要考察协议定义和特征
简单只能简单得千篇一律，难可以难得五花八门

常见的工控协议有：Modbus、MMS、IEC60870、MQTT、CoAP、COTP、IEC104、IEC61850、S7comm、OMRON等

由于工控技术起步较早但是统一的协议规范制定较晚，所以许多工业设备都有自己的协议，网上资料数量视其设备普及程度而定，还有部分协议为国家制定，但仅在自己国内使用，网上资料数量视其影响力而定

CTF之协议分析文章合集

- 工控CTF之协议分析1——Modbus
- 工控CTF之协议分析2——MMS
- 工控CTF之协议分析3——IEC60870
- 工控CTF之协议分析4——MQTT
- 工控CTF之协议分析5——COTP
- 工控CTF之协议分析6——s7comm
- 工控CTF之协议分析7——OMRON
- 工控CTF之协议分析8——特殊隧道
- 工控CTF之协议分析9——其他协议

文中题目链接如下

站内下载

网盘下载: <https://pan.baidu.com/s/1vWowLRkd0ldvL8GoMxG-tA?pwd=jkkkg>
提取码: jkkkg

S7comm

西门子设备工控协议，基于COTP实现，是COTP的上层协议，主要由三种类型（ROSCTR）：**Job(1)、Ack_Data(3)/Ack(2)、Userdata(7)**

Job: **下发任务/指令**，机器收到任务/指令后回传数据确认收到，回传的内容就是Ack/Ack_Data

Ack_Data: 带有返回数据，例如指令是查询内容，返回的就有要查询的东西

Ack: 单纯确认，不含有数据

- Job，主要有10种功能（Function）
 - Setup communication (0xf0) 启动、初始化
 - Read Var (0x04) 读参数
 - Write Var (0x05) 写参数
 - 下载
 - Request download (0x



Shadow丶S

关注

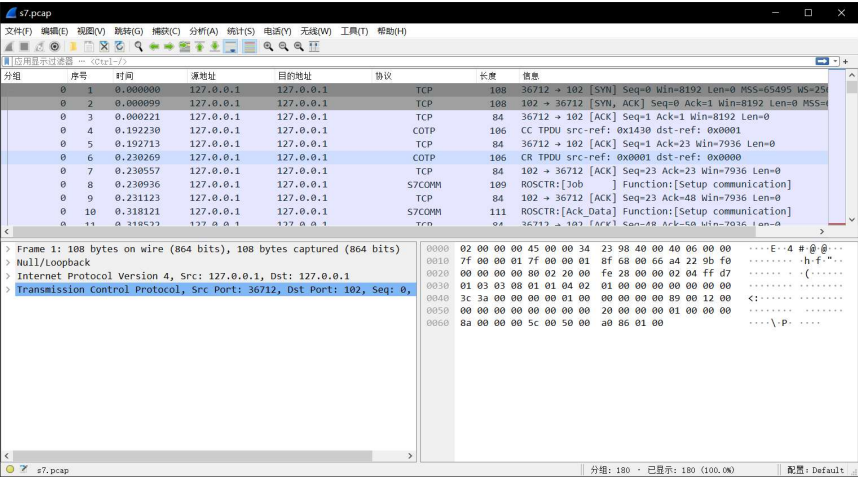
0

0

6

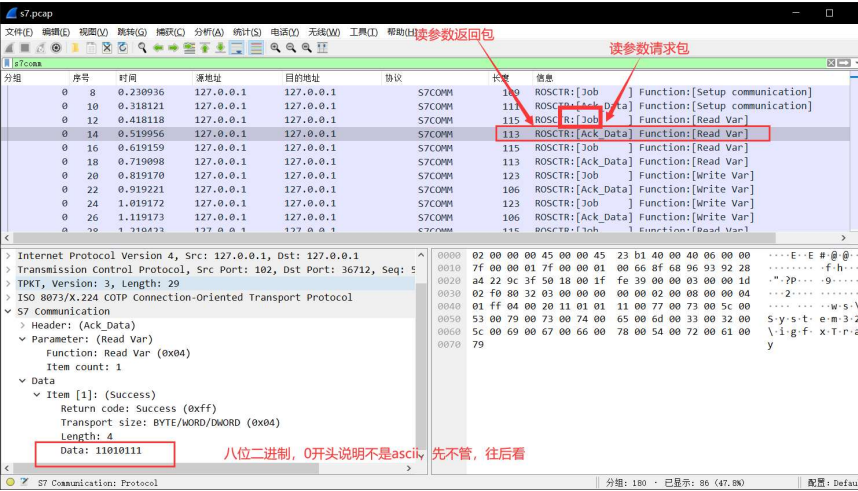
- Download block (0x1b) 要下载的数据，可能出现多次
- Download ended (0x1c) 表示数据已发送完毕
- 上传
 - Start upload (0x1d) 表示要上传东西，读取文件
 - Upload (0x1e) 上传内容
 - End upload (0x1f) 表示上传完成
- PI-Service (0x28) 控制指令，控制一些程序，在题目中很少见
- Userdata, 用户自定义数据区，也包含功能指令，主要有6种功能组（Function group）
 - Mode-transition (0) 模式转换
 - Programmer commands (1) 执行
 - Block functions (3)
 - CPU functions (4)
 - Security (5) 安全相关
 - Time functions (7) 定时任务相关

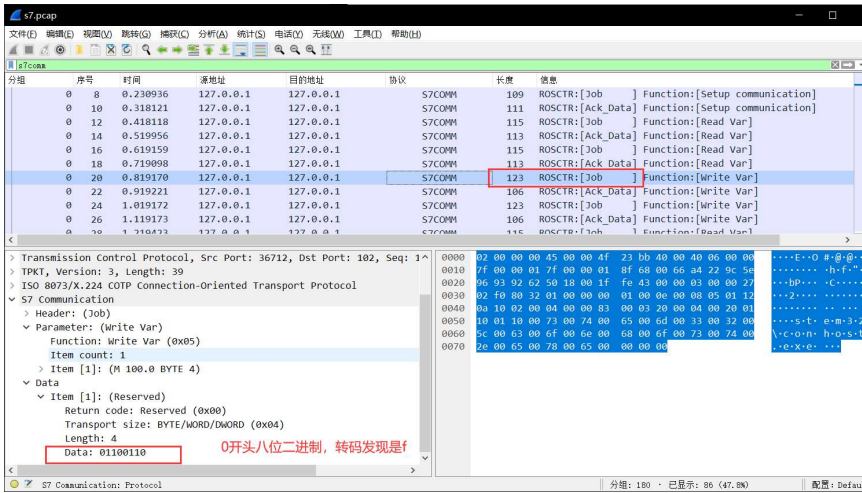
例题1 2020ICSC湖州站—工控协议数据分析



发现不仅有s7，还有很多COTP，因为s7是COTP上层协议，s7数据都是通过COTP传输

筛选s7，读参数的请求内容会在返回数据中，写请求内容一定在发送数据中，根据不同功能分析数据包





看第二个写请求，发现参数转码为l，判断flag藏在写请求中，筛选所有写请求

```
(s7comm) && (s7comm.param.func == 0x05) && (s7comm.header.rosctr == 1)
```

提取所有写请求参数，转码得到flag

例题2 2020ICSC济南站—被篡改的数据

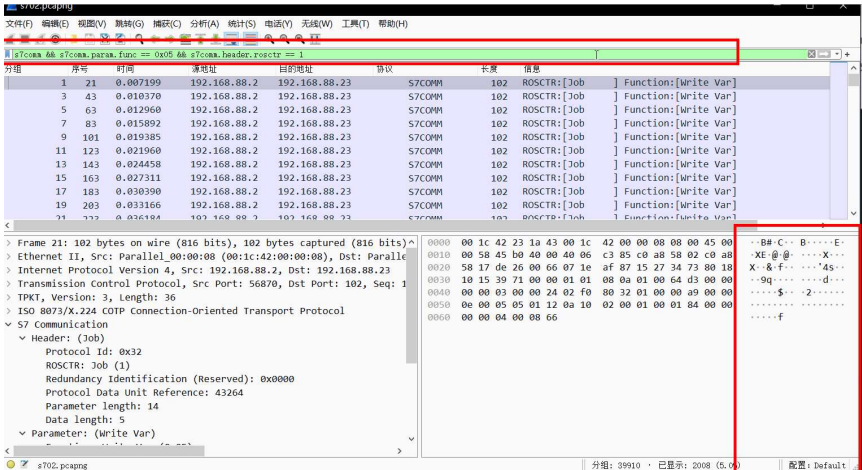
直接筛选s7comm，根据题目提示，篡改的数据，那么优先筛选写参数请求即write var

发现大量数据66，转码为f，猜测可能是flag的字符，但是两千多条，先将其筛选，看剩下的

```
((s7comm) && (s7comm.param.func == 0x05) && (s7comm.header.rosctr == 1)) && !(s7comm.resp.data == 66)
```

剩下的数据可以直接看出就是flag，开头结尾有花括号，但是为了防止flag中含有f，重新筛一遍

直接看序号19987，即刚刚发现的上一条，从这里开始提取得到flag



手动复制或者py脚本提取

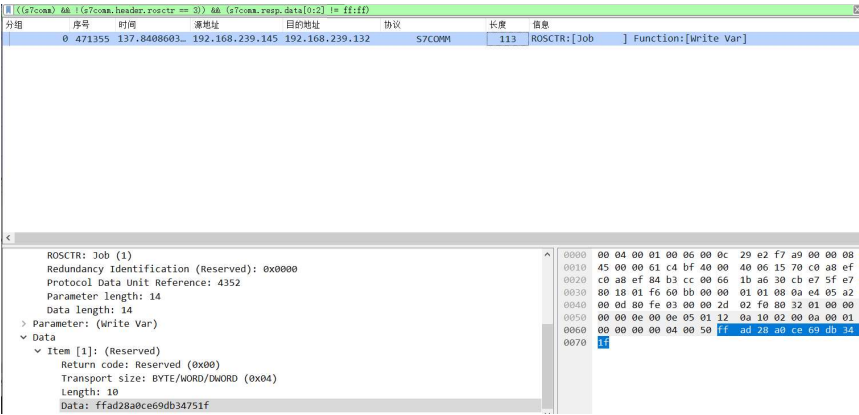
例题3 枢网智盾2021—异常流分析

发现流量都是s7协议写入数据

```
(s7comm) && !(s7comm.header.rosctr == 3)
```

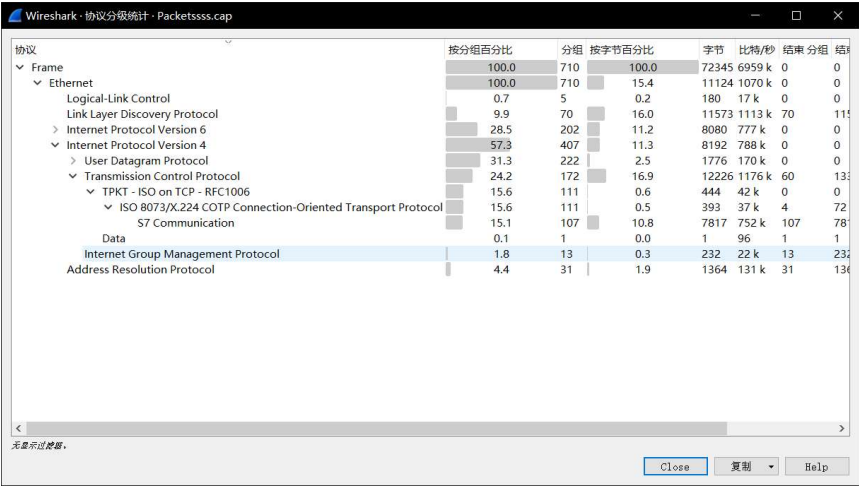
且发现写入数据内容都是ffff开头，先筛一下看看有没有不是ffff开头的

```
((s7comm) && !(s7comm.header.rosctr == 3)) && (s7comm.resp.data[0:2] != ff:ff)
```

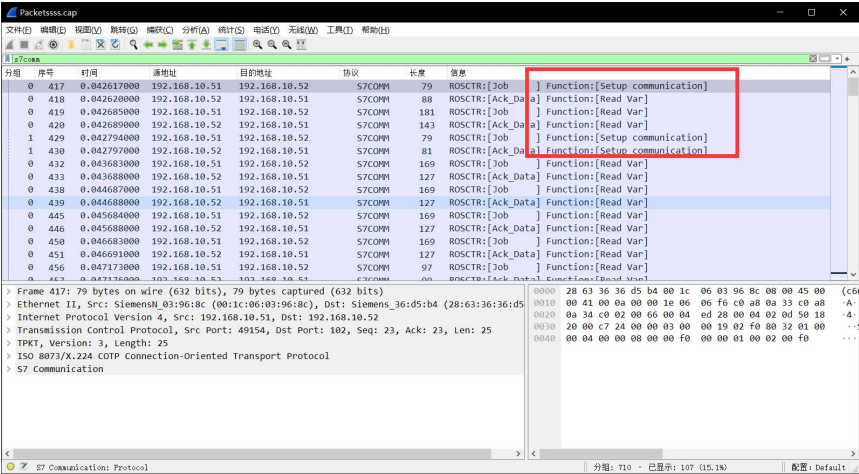


这个就是异常流量，得到flag

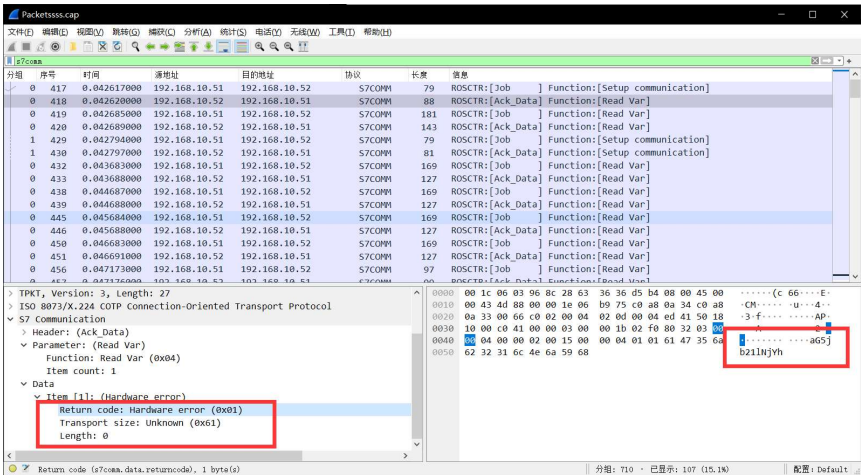
例题3 枢网智盾2021—工控协议分析



前面初始化setup出错误，没有ack的setup，往后看也没有什么明显的异常了



发现本该是应答初始化的地方变成了返回read结果，且是明文



尝试解码



得到flag

文章知识点与官方知识档案匹配，可进一步学习相关知识

网络技能树 支撑应用程序的协议 应用层的作用 35917 人正在系统学习中

- 工控CTF协议分析学习题目合集**
主页工控CTF学习配套题目，搭配学习

12-20
- 一道MMS工控协议CTF题的WriteUp-附件资源**
一道MMS工控协议CTF题的WriteUp-附件资源

03-02
- 工控安全-S7协议_Shray.io的博客**
S7Comm(S7 Communication)是西门子专有的协议,是西门子S7通讯协议簇里的一种。S7协议的TCP/...

7-22
- 西门子S7Comm以太网通讯协议解析_身在江湖的郭大侠的博客**
首先,这里所说的S7Comm 协议只是西门子S7通讯协议簇里的一种,以0x32开始的报文结构。1、S7Co...

7-21
- 工业协议数据模拟包S7Comm-Plus**
该工业协议数据包涵盖目前主流的数据包，可以用于开发自验或者测试进行工业协议的测试。...

08-05
- 从CTF到工控安全.pdf**
从CTF到工控安全.pdf

02-26

西门子PLC协议-S7COMM_s7connector 4096错误_幕峰者的博客
协议对接 附件 简述 前段事件对接西门子设备,是一台盾构机控制PLC(programmable logic controllers)...

西门子S7comm-plus通信过程及重放
2、西门子S7Comm协议分析 <https://laucy>

Shadow丶 S 关注

0 6

- 西门子以太网S7comm协议
西门子以太网S7comm协议，与西门子S7-300，西门子828D数控通信的协议

03-26
- S7COMM协议分析
S7COMM协议分析

东隅的博客 1276
- S7comm协议学习笔记

山兔的博客 1797

一、S7comm，西门子为了它生产的PLC、SCADA与PLC之间的通信而设计的专属私有协议。在应用...
- (二) S7Comm协议分析

weixin_43047908的博客 1868

目录前言S7Comm是什么？前言 上篇我们讲述了Modbus协议的基本原理和结构，这一篇我们把目光...
- S7协议抓包分析（附pcap数据包）
S7comm（S7 通信）是西门子专有协议，可在西门子 S7-300/400 系列的可编程逻辑控制器 (PLC) 之...

悦分享 2828
- 上位机工业协议-S7COMM

xdpcxq的专栏 521

协议主要针对西门子相关设备通信。先了解基本通信对象、通信环境、通信报文，再处理。协议 访问...
- CTF6靶机实战.zip
CTF6靶机实战包括三部分: 1) 靶机实战过程 2) 文件上传的反弹shell文件(shell.php) 3) 系统...

05-25
- S7comm协议模拟器与协议解析文档以及示例pcap包
S7协议西门子私有协议但网上分析人数较多基本算半公开。压缩包内附带协议解析文档与博客...

09-25
- 西门子S7通讯协议API
S7通讯协议 包含API函数说明和接口 整个编程的方式均有说明

01-27
- 西门子S7-communication协议说明文档

09-14

由于国内没有西门子S7协议的过多资料，以上文档是本人参阅外文资料，总结得来，十分详细
- 2022工业互联网大赛-杭州-CTF题目

09-14

第一次参加工控类的CTF，然后正好团队中有小伙伴电脑连不上局域网，只能从我电脑中...
- CTFHub S7协议恶意攻击分析 WP
S7协议恶意攻击分析 WP

qq_61993117的博客 1473
- CTF:S7comm协议受攻击报文分析 最新发布

npu_nazi的博客 205

某组织通过特殊手段获取到了城市供水企业的某些流量数据。作为安全研究人员需要分析出其中特殊...
- 2021CTF工业信息安全技能大赛-异常的s7comm

qq_43264813的博客 2589

2021CTF工业信息安全技能大赛-异常的s7comm 工程师小夏在针对西门子300PLC设备不定期的停止...
- ctf工控 流量题

qq_61768489的博客 1128

某工程师在运维中发现了设备的某些异常，怀疑可能遭受到了黑客的攻击，请您通过数据包帮助运维...
- ctf中常用的PHP伪协议

02-15

在CTF比赛中，常常会使用PHP伪协议来绕过服务器的安全限制或者执行本不应该执行的操作。PHP...

“相关推荐”对你有帮助么？

- 非常没帮助
- 没帮助
- 一般
- 有帮助
- 非常有帮助

关于我们

招贤纳士

商务合作

寻求报道

400-660-0108

kefu@csdn.net

在线客服

工作时间 8:30-22:00

公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号 经营性网站备案信息
北京互联网违法和不良信息举报中心 家长监护 网络110报警服务 中国互联网举报中心 Chrome商店下载 账号管理规范
版权与免责声明 版权申诉 出版物许可证 营业执照 ©1999-2023北京创新乐知网络技术有限公司

Shadow\ S
码龄4年 高校学生

126

4万+

2万+

25万+

原创

周排名

总排名

访问

等级

1830

202

306

48

1675

积分

粉丝

获赞

评论

收藏

Shadow\ S

关注

0

6

私信

关注

搜博主文章



热门文章

【计算机网络】IP地址详解 27683

DOS攻击 21648

ACL原理及配置 14442

eNSP下载安装超详细，华为模拟器下载安装 11328

域——windows服务器域详解 8888

分类专栏

	CTF刷题	27篇
	工控	9篇
	渗透测试	55篇
	逆向分析	1篇
	网络安全	46篇
	计算机网络	16篇



最新评论

- 【计算机网络】IP地址详解
大口喝咖啡: 应该是本地地址吧
- 华为模拟器eNSP免费下载
指尖上的圆春: 链接挂了
- 域——windows服务器域详解
Shadow丶 S: 什么参数，具体点
- 域——windows服务器域详解
sweet-琉璃: 参数不正确怎么办呢？
- 华为模拟器eNSP免费下载
打码不打你: 文件没了

最新文章

- LitCTF2023 WP
- 工控CTF之协议分析7——OMRON
- 工控CTF之协议分析8——特殊隧道
- 2023年 1篇 2022年 91篇
- 2021年 34篇

目录

- 协议分析
- CTF之协议分析文章合集
- S7comm
- 例题1 2020ICSC湖州站—工控协...
- 例题2 2020ICSC济南站—被篡改...



Shadow丶 S

关注

0



6