


# 工控CTF之协议分析5——COTP

原创 Shadow、S 于 2022-12-20 21:15:08 发布 1202 收藏 7 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

## COTP

可以理解为基于TCP的工控TCP，主要有五种类型：

- CR Connect Request (0x0e)——握手，发送方发送
- CC Connect Confirm (0x0d)——握手，接收方发送
- DT Data (0x0f)——传正常数据
- UD User Data (0x04)——少见，传自定义数据
- ED Expedited Data (0x01)——少见，传紧急数据

CR和CC只在建立连接时由双方发送，发起方发送CR，被动方发送CC，后续数据主要走DT。因为协议类似于TCP，较为底层，所以没有其他比较有用的协议字段可供解题；同样因为COTP较为底层，用来出题的概率较小，就像用纯TCP出题的概率一样

## 例题 2020ICSC济南站——COTP

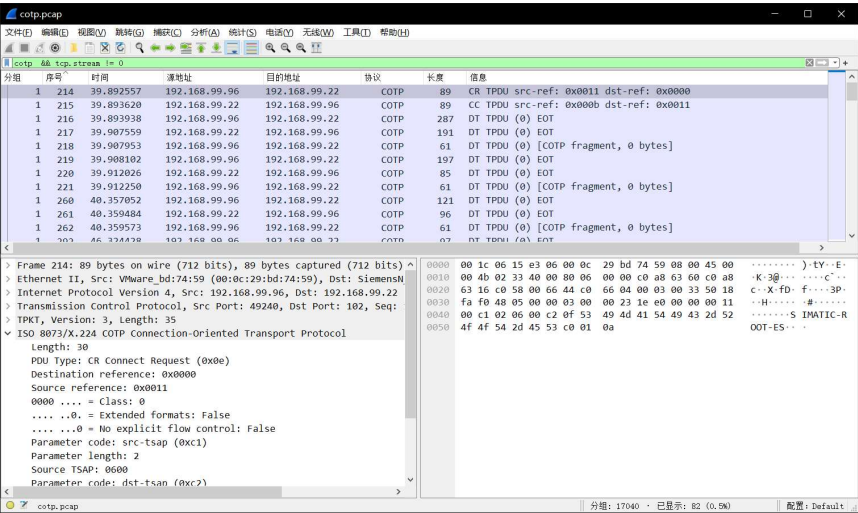
题目要求：找到黑客流量，flag为后90字节的16进制

 Shadow、S 关注

 1   7

打开题目，筛选COTP协议，发现没有经过握手，直接就是传数据，但是黑客要想传输必须要重新建立连接，也就是会有一个新的握手出现，将其筛选出来

```
cotp && tcp.stream != 0
```



题目明确是黑客流量，那么它应该存在大量可见字符，所以尝试提交握手后的几次数据，同时发现黑客建立了三次连接，数据几乎相同，符合黑客操作

找到后90个十六进制值即是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 35916 人正在系统学习中

- CTF之二维码扫描.7z

CTF入门之二维码扫描神器，支持二维码修复

12-02
- 从CTF到工控安全.pdf

从CTF到工控安全.pdf

02-26
- 61850通讯流程\_oragnelove的博客

COTP(Connection-Oriented Transport Protocol),即面向连接的传输协议,从这个名字就可以看出,它的...

7-24
- S7协议抓包分析(附pcap数据包)\_s7协议详解\_wespten的博客

COTP协议的全称是Connection-Oriented Transport Protocol,即面向连接的传输协议,从这个名字就可...

7-21
- 计算机网络小知识点

1.htonl将主机数转换成无符号长整型的网络字节顺序。本函数将一个32位数从主机字节顺序转换成网...

宇之日记 198
- 工控协议——S7通讯协议

工控协议——S7通讯协议S7协议简介2. TPKT协议3.COTP协议 S7协议简介 S7以太网协议本身也是T...

咸鱼!!! 2万+
- 西门子PLC协议-S7COMM-扩展\_幕峰者的博客

COTP功能包 举例 最后 之前详细写S7中PDU,但S7 Communication被封装在TPKT和SO-COTP协议中...

6-29
- python与西门子1200通讯\_西门子S7-1200的以太网通信\_weixin\_39845430的博...

第1~4层为底层驱动程序,由计算机本身完成;第5层TPKT,应用程数据传输协议,介于TCP和COTP协议之...

7-1
- COTP (Connection Oriented Transport Protocol)

2019独角兽企业重金招聘Python工程师标准>>> ...

weixin\_34062329的博客 709
- wireshark源代码分析 热门推荐

经过多次尝试，终于在windows上成功编译wireshark源代码，但用的不是下面的这个步骤，不过大同...

zx824 5万+
- 西门子S7通信协议以及JAVA版的实现\_java s7协议\_XS\_YOUIYOU的博客-CSDN...

S7协议TCP/IP实现依赖于面向块的ISO传输服务,S7协议包含在TPKT和ISO-COTP协议中,允许PDU(协...

7-22
- 传输协议数据单元TPDU的类型及英文全称

学习过程中总是有很多英文缩写，知道了其全称之后更容易理解记忆。 传输协议数据单元TPDU：Tra...

RealCoder的博客 1202
- 工业协议之 S7

S7 协议 1.S7协议模型 首先应当明确的是

Shadow` S 关注

- 2020ICPC济南区域赛 补题 & 总结

weixin\_44059127的博客 1949

前言 题目链接 <https://ac.nowcoder.com/acm/contest/10662> 参考题解 A - Matrix Equation 简要题意: ...
- 工控测试---协议---IEC\_MMS 61850--协议payload基本随机构造

我不是庸医 1055

目标: 构造随机的一个mms包, 进行异常包测试 构造工具: scrapy, 好处是只需要关心具体的tcp pa...
- 2021CTF工业信息安全技能大赛-控制器数据备份失败

qq\_43264813的博客 648

2021CTF工业信息安全技能大赛-控制器数据备份失败 企业工程师小杨定期对生产设备控制器工程进行...
- 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, 然后正好团队中有一个小伙伴电脑连不上局域网, 只能从我电脑中...
- 报文分析软件

04-20

本站配置一套网络通信记录分析系统, 实现过程层和站控层网络的实时监视、记录和实时分析...
- 工控CTF协议分析学习题目合集

12-20

主页工控CTF学习配套题目, 搭配学习
- 一道MMS工控协议CTF题的WriteUp-附件资源

03-02

一道MMS工控协议CTF题的WriteUp-附件资源
- 工控测试---协议---IEC\_MMS 61850--request类型协议报文解析

我不是庸医 2867

概述 MMS跑在应用层之上, MMS报文如下, MMS遵循OSI标准, 所以很多TCP/IP熟悉的人, 开始看...
- 工控协议-s7通讯协议

chenfeng857的博客 3762

工控协议——S7通讯协议 S7协议简介 2. TPKT协议 3.COTP协议 S7通信支持两种方式 S7comm协议 ...
- 西门子S7 模拟器使用教程

悦分享 5021

S7协议是西门子S7系列PLC通信的核心协议, 它是一种位于传输层之上的通信协议, 其物理层/数据链...
- 工控协议 S7comm-Plus 用 wireshark 打开

Reality 1215

近期用到S7comm-Plus协议, 用wireshark打开时显示为cotp:
- ctf中常用的PHP伪协议 最新发布

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?

- 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

私信

关注

搜博主文章

热门文章

【计算机网络】IP地址详解 27683



Shadow\ S 关注

1 7

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  
指尖上的圈春: 链接挂了

域——windows服务器域详解  
Shadow、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6——s7comm

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

COTP

例题 2020ICSC济南站—COTP