


工控CTF之协议分析3——IEC60870

原创 Shadow\ S 于 2022-12-20 21:14:13 发布 801 收藏 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

IEC60870

- 子协议
 - IEC101 (任务相关)
 - IEC102 (电量相关)
 - IEC103 (保护相关)
 - IEC104 (101的网络版)
 - IECASDU (基于101/104的应用服务数据单元传输)
- 主要技巧
 - 筛选 `iec60870_asdu`
 - 关注IOA的值
 - 可尝试用type进行分类

例题1 HNGK-奇怪的工控协议

[外链图片转存失败,源站可能有防盗链, 请图灵识别](https://picture-ssh.  Shadow\ S 关注

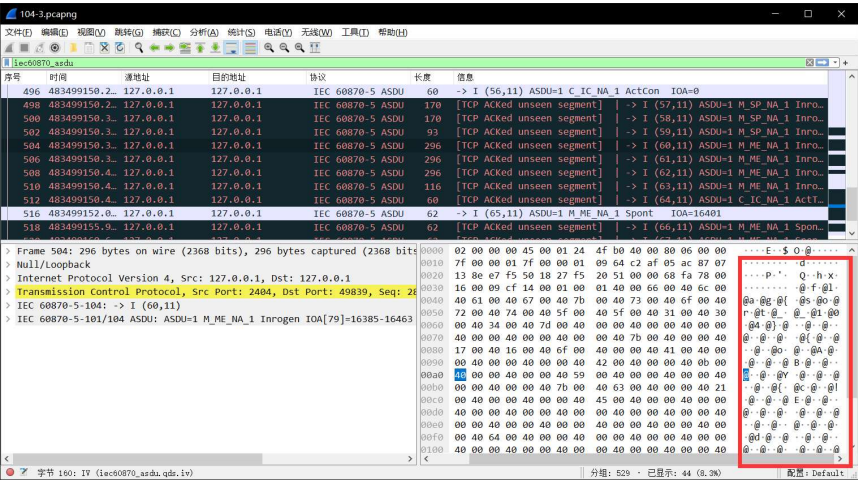
0 0 0

beijing.aliyuncs.com/img/WEB202212101509327.png)]

(图中应为一半以上涉及modbus)

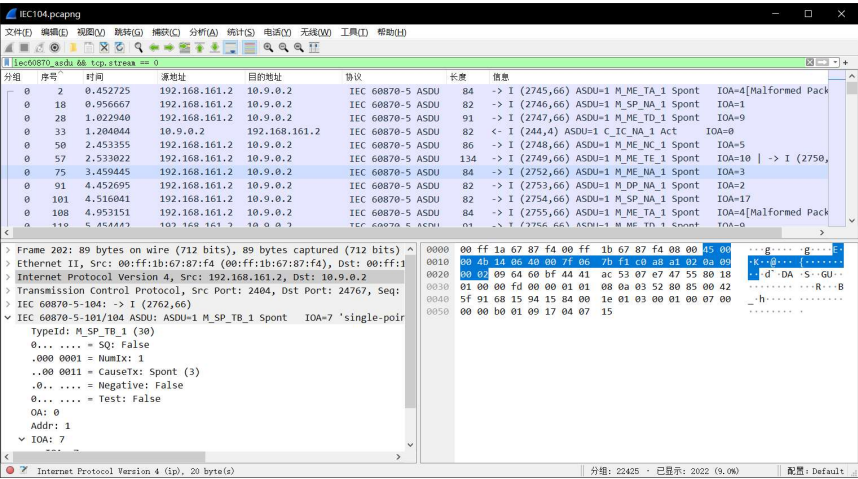
筛选条件iec60870_104, iec60870_asdu, 分别查看IOA的值并看数据书否有异常或奇怪的地方

发现flag



例题2 HNGK-协议分析

发现此题目存在多个连接, 按分组筛选 iec60870_asdu && tcp.stream == 0



发现有些数据包是报错的, 正确的包应该含有IOA的值 iec60870_asdu && tcp.stream == 0 && iec60870_asdu.normval

还有五百多条数据, 剩下的可以以TypeID为条件筛选, 一个一个筛过去

((((iec60870_asdu && tcp.stream == 0)) && (iec60870_asdu.normval)) && (iec60870_asdu.typeid == 34)) 发现IOA的值对应的基本都是乱码, 或者发现还有三百多条数据判断他是正常的

最后在typeid=9处发现两个等号收尾的以两字节为一组的数据

(((((iec60870_asdu && tcp.stream == 0)) && (iec60870_asdu.normval)) && (iec60870_asdu.typeid != 34)) && (iec60870_asdu.typeid != 9))

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-Ur2BOPfZ-1671529464979)(https://picture-ssh.oss-cn-beijing.aliyuncs.com/img/WEB202212101614117.gif)]

将其提取出来解base64错误, 发现开头mZhx, 而flag的base64对应值为Zmxh, 猜测是前后颠倒两两一组

得到flag

Shadow S

关注

题目难点在于连接过多，筛选复杂，出题人还算良心第一条连接就有flag，否则还要多次筛选tcp.stream；对于数据敏感性也是难点，再翻数据的时候能发现数据异常或特征；筛选小技巧typeid

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

	IEC104工控协议生成工具 04规约调试工具，模拟104主控站，方便104规约的理解	11-15
	CTF真题-Dest0g3CTF2022招新赛 CTF真题-Dest0g3CTF2022招新赛，来自BUUCTF。	06-01
	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
	lib60870 IEC101，IEC101 NET开源代码 lib60870.NET是.net开源代码，包含IEC101，104的源代码，支持客户端和服务端的代码。	06-25
	IEC60870-5-104通讯协议文本 国际标准-IEC60870-5-104通讯协议文本，完整的通讯协议介绍，部分指令实例介绍。	11-26
	lib60870.NET:lib60870.NET的官方存储库，是C#中IEC 60870-5-101104协... 自述文件lib60870.NET v2 lib60870.NET库，用于C#中基于IEC 60870-5的协议 当前实现仅包...	05-06
<hr/>		
IEC60870-5-103继电保护设备信息接口通信协议测试方法		测控道 3480
1 前言 IEC60870-5-103继电保护设备信息接口标准提供了继电保护设备（或测控设备）的信息接口规...		
<hr/>		
工业协议解析——IEC60870-104		weixin_38843284的博客 3163
104报文较为繁琐。共有S帧、I帧、U帧。简单的说I帧是用来传输数据、S帧是用来信息确认、U帧用...		
<hr/>		
IEC60870-5-104通信协议测试方法		测控道 3800
1 前言 IEC60870-5-104规定了采用标准传输协议子集的IEC60870-5-101网络访问。IEC60870-5-101...		
<hr/>		
2020年江西工业互联网安全技术技能大赛WP		y920312的专栏 1888
目录 ## 黑客留下的文件 ## 黑客留下的文件 1、前置知识 已知新型的php一句话木马如果接收到pass...		
	2022工业互联网大赛-杭州-CTF题目 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...	09-14
	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
	从CTF到工控安全.pdf 从CTF到工控安全.pdf	02-26
<hr/>		
工控计算机电力行业标准.标准协议工控协议_IEC104.pdf		weixin_33007357的博客 393
工控协议简介IEC 104匡恩网络版权所有© 2014工控网络安全培训体系工业系统网络安全概述针对工...		
<hr/>		
IEC-60870-5-104 scada		波波诸葛伟 2274
<hr/>		
IEC60870-5-101协议解析		Lanceli 8279
IEC 60870-5-101 (IEC101) 是电力系统监测、控制和相关通信的标准，用于电力系统的远程控制、...		
<hr/>		
工控测试---协议---IEC104报文基础理解		我不是庸医 1207
字段基本内容 帧格式 I:0 S:01 U:11 操作对象 Typeld 公共地址 Addr 信息题地址 IO...		
<hr/>		
工业控制协议IEC-104学习记录		我不是庸医 1974
目录 协议（规约） 帧结构 I帧详解 S帧详解 U帧详解 以APDU来传输 I帧 计数的，用来信息传输发送 ...		
<hr/>		
IEC60870-5-102电力系统电能累计量传输通信协议测试方法		测控道 1248
1 前言 IEC60870-5-102电力系统电能累计量传输通信协议规定了电能计量终端与电网各级电能计...		
<hr/>		
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”对你有帮助么？

非常没帮助

没帮助



Shadow\ S

关注

0

0



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
- 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
指尖上的圍春: 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



Shadow\ S

关注

0

0

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

IEC60870

例题1 HNGK-奇怪的工控协议

例题2 HNGK-协议分析



Shadow、S

关注

👍 0

💬

🌟 0