


工控CTF之协议分析2——MMS

原创 Shadow、S 已于 2022-12-20 21:13:43 修改 1035 收藏 1 版权

分类专栏: 工控 CTF刷题 文章标签: tcp web安全

 工控 同时被 2 个专栏收录

5 订阅 9 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

MMS

工控领域的TCP协议，有时 **wireshark** 会将response包解析为tcp协议，影响做题，如果筛选mms时出现连续request包，考虑wireshark解析错误，将筛选条件删除手动看一下

- initiate（可以理解为握手）
 - initiate-RequestPDU
 - initiate-ResponsePDU
- confirmed（可以理解为交互，即传数据）
 - confirmed-RequestPDU
 - confirmed-ResponsePDU

通常为

1轮initiate：即发送1个initiate-R

 Shadow、S

关注

 0



 1

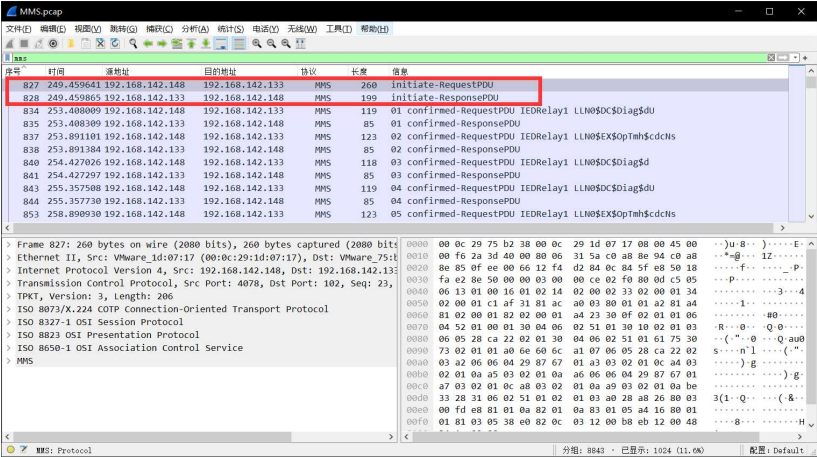
n轮confirmed：直到会话主动关闭或被动断开即confirmed-RequestPDU和confirmed-ResponsePDU交替发送和接收

交互时的指令称为confirmedService

常见的confirmedService有

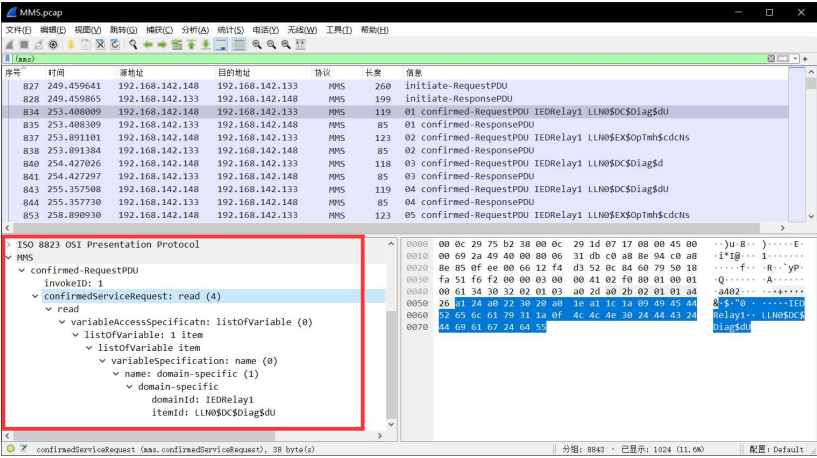
- 对象操作
 - getNameList (1)
 - read (4)
 - write (5)
 - getVariableAccessAttributes (6)
 - getNamedVariableListAttributes (12)
- 文件操作
 - fileOpen (72)
 - fileRead (73)
 - fileClose (74)
 - fileDirectory (77)

例题1 HNGK-MMS



经过“握手”“分手”后开始传输数据，发现confirmedService的值均为4，查看是否有不是4的数据包 (mms) && (mms.confirmedServiceRequest != 4)

发现均为4，无异常，那么flag基本就藏在数据流中了，一层一层查看数据



发现domainID和itemID，分别对其过滤查看

((mms)) && (mms.domainId != "IEDRelay1") 发现domainID都是一样的值

再对itemID过滤，这里发现虽然



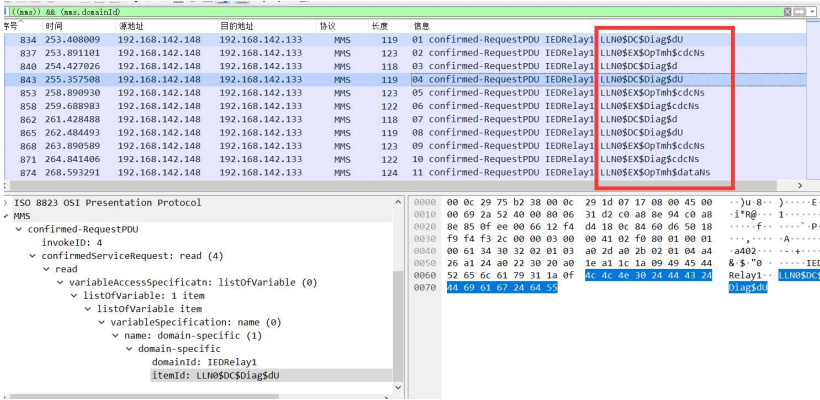
Shadow S

关注

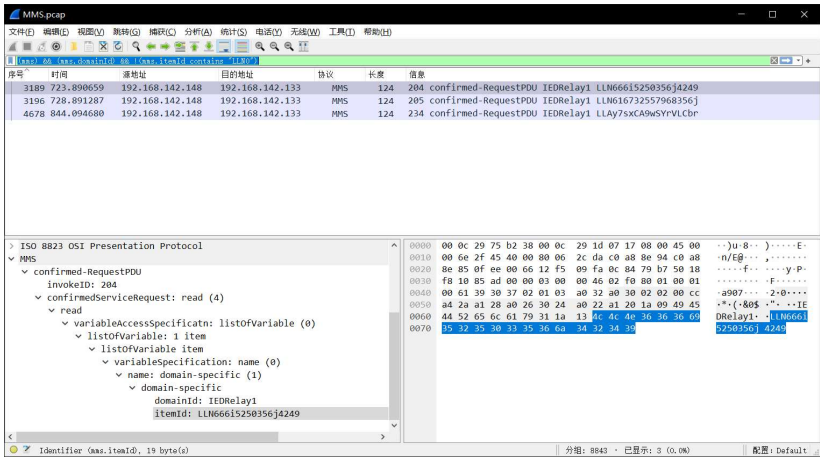
0

0

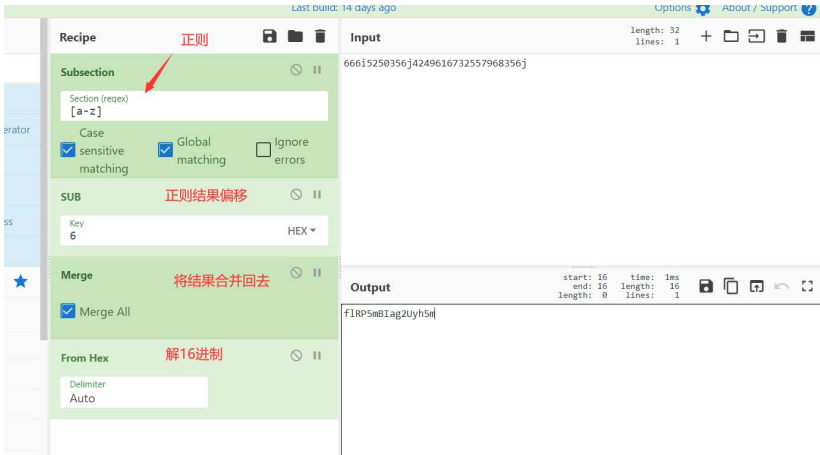
1



(mms) && (mms.domainId) && !(mms.itemId contains "LLN0")

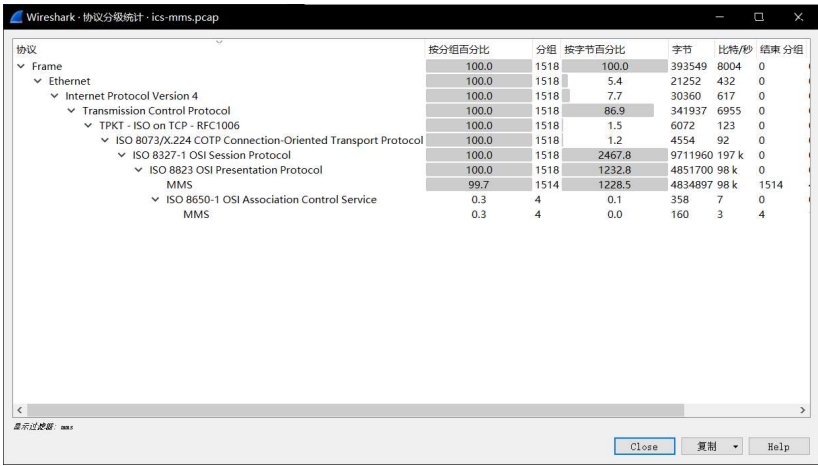


66是flag中的ascii码，猜测可能是十六进制，但是i、j明显不在此范围内，猜测可能存在偏移，这里猜测偏移6，因为字母的十六进制为6c

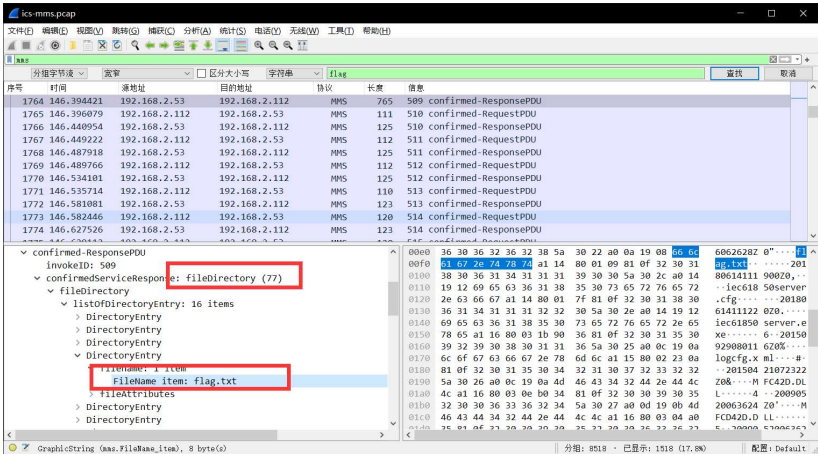


发现i和ag，猜测前后每两字节取值，因为两数据取自不同的itemId，拼接flag并加上{}即可

例题2 HNGK-流量分析

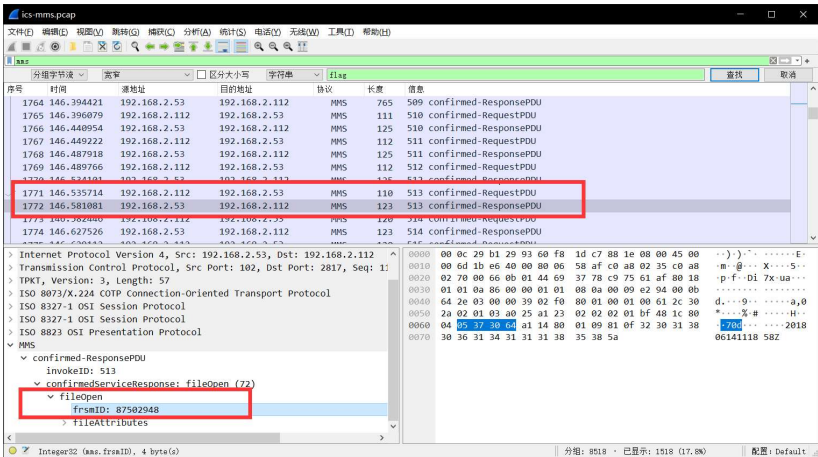


发现大部分均为getNameList获取对象名，回复包也是get到的数据，先查询有无包含flag字符串

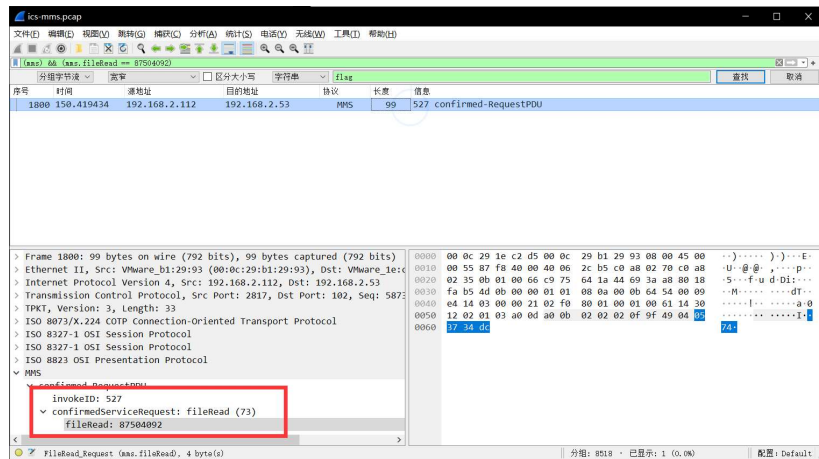


既然有列出目录再往后找，找到fileopen flag.txt

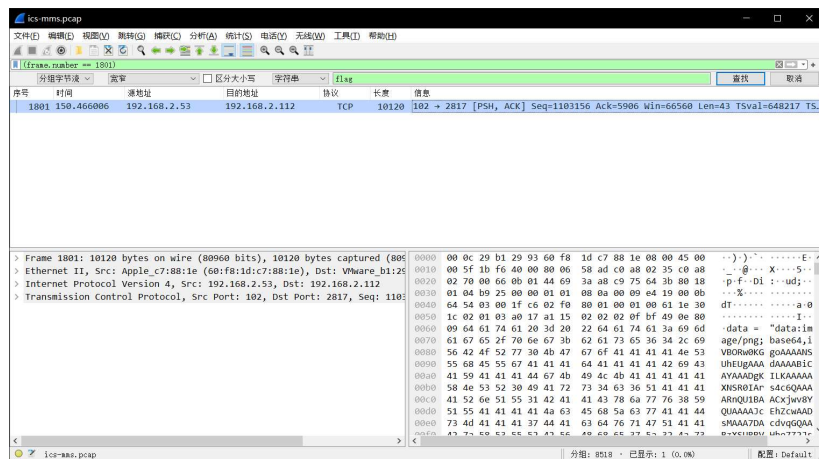
查看返回值，得到一个打开该文件的句柄或者ID



往后发现再次列出目录打开flag.txt，尝试找是否有读文件操作即fileOpen，mms.fileOpen == frsmID，依次尝试得到的几个id，在第二次打开中即frsmID=87504092找到读文件操作



找到这串请求的返回包即序号1801，得到一串图片base64



将base64转图片得到flag



判断题目类型

可以在wireshark—统计—协议分级中查看各协议占比



MMS协议报文实例分析

12-06

对报文进行解析及分析，对每一包发送内容进行详细分析，server to client 告知流属性等。



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...

工控CTF之协议分析9——其他协议_ctf 工控_Shadow丶S的博客

7-15

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...

工控安全:CTF赛前小知识[转]_KEYONE的博客

7-16

ZoomEye 是知道创宇打造的面向网络空间的搜索引擎,ZoomEye 于 2015 年 3 月上线了工控专题 ...



32如何让Wireshark支持61850 MMS报文解析

01-28

32如何让Wireshark支持61850 MMS报文解析



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W



Shadow丶S

关注

2021CTF工业信息安全技能大赛

2021CTF工业信息安全技能大赛-工控梯形图分析1 小张在进行设备调试时,编写了一段模拟量转...

CTF实践_ctf工控 修复数据库漏洞_Suzy_Rose的博客 7-12
实验目的:通过对目标靶机的渗透过程,了解CTF竞赛模式,理解CTF涵盖的知识范围,如MISC、PPC...

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

工控CTF (wp) aarong的博客 7089
这里写自定义目录标题欢迎使用Markdown编辑器新的改变功能快捷键合理的创建标题,有助于...

[工控CTF]2021工业信息安全技能大赛(江西站)-WP_工控比赛wp_3tefanie、... 7-21
工控流量分析 hint:某企业车间PLC运行异常,造成生产线无法正常运行。请您帮助改企业车间分析...

工控CTF之协议分析7——OMRON song123sh的博客 864
工控CTF之协议分析7——OMRON

MMS (Manufacturing Message Specification) 协议分析 学习记录 5725
1、简介 MMS(Manufacturing Message Specification)中文翻译为制造报文规范,在介绍MMS之...

工控ctf qq_45951598的博客 6352
文章目录黑客的大意 黑客的大意 下载后得到mail,在文件后面jpg 打开图片是一个这样的图片,...

工控CTF之协议分析1——Modbus song123sh的博客 2278
工控CTF之协议分析1——Modbus

从CTF到工控安全.pdf 02-26
从CTF到工控安全.pdf

一道MMS工控协议CTF题的Wri... Panda - 专注于网络空间安全研究 - www.cnpanda.net 4382
0x01 赛题说明 赛题说明: 只能变电站通过 61850 规约进行监控层到间隔层的数据采集,请分析...

2021CTF工业信息安全技能大赛(常州站)-工控图片分析 qq_43264813的博客 629
2021CTF工业信息安全技能大赛(杭州站)-工控图片分析 题目内容: 小李捕获到一份文件,请分析...

国产61850(CMS)协议与国际61850(MMS)协议... 最新发布 m0_58637974的博客 1544
MMS(Manufacture Message Specification)是制造报文规范,本身是很优秀的规范,这一点是不...

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...

CTFHub 工控现场的恶意扫描 WP qq_61993117的博客 150
工控现场的恶意扫描wp

纵横网络靶场社区 MMS协议分析 qq_61993117的博客 480
排一下包的长度,发现有一个包的长度不正常,点进去看一下内容是一张base64解码的图片。然...

MMS协议 zhanggong2046的专栏 2942
MMS介绍 MMS是Multimedia Messaging Service (多媒体消息服务)的缩写,即所说的彩信,...

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。...

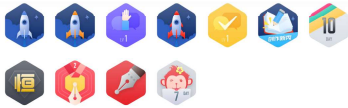
“相关推荐”对你有帮助么?

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

Shadow、S 关注 0 1



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



Shadow、S

关注

0



1

例题2 HNGK-流量分析



Shadow S

关注

👍 0



🌟 1