# 工控CTF之协议分析1——Modbus

原创 Shadow丶S 已于 2022-12-20 21:13:50 修改 2277 收藏 8 版权
分类专栏： CTF刷题 工控 文章标签： 网络协议 tcp web安全



## 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
简单只能简单得干篇一律，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/1vWowLRkd0IdvL8GoMxG-tA?pwd=jkkg
提取码：jkkg

## Modbus

**Modbus**，市场占有率高、出题频率高,算是最常见的题目，因为这个协议也是工控领域最常见的协议之一，主要有三类

- Modbus/RTU

  从机地址1B+功能码1B+数据字段xB+CRC值2B

  最大长度256B，所以数据字段最大长度252B

- Modbus/ASCII

  由Modbus/RTU衍生，采用 `0123456789ABCDEF` 表示原本的从机地址、功能码、数据字段，并添加开始结束标记，所以长度翻倍

  开始标记：（0x3A）1B+从机地址2B+功能码2B+数据字段xB+LRC值2B+结束标记 `\r\n` 2B

  最大长度513B，因为数据字段在RTU中是最大252B，所以在ASCII中最大504B

- Modbus/TCP

不再需要从机地址，改用UnitID；不再需要CRC/LRC，因为TCP自带校验

传输标识符2B+协议标识符2B+长度2B+从机ID 1B+**功能码1B**+数据字段xB

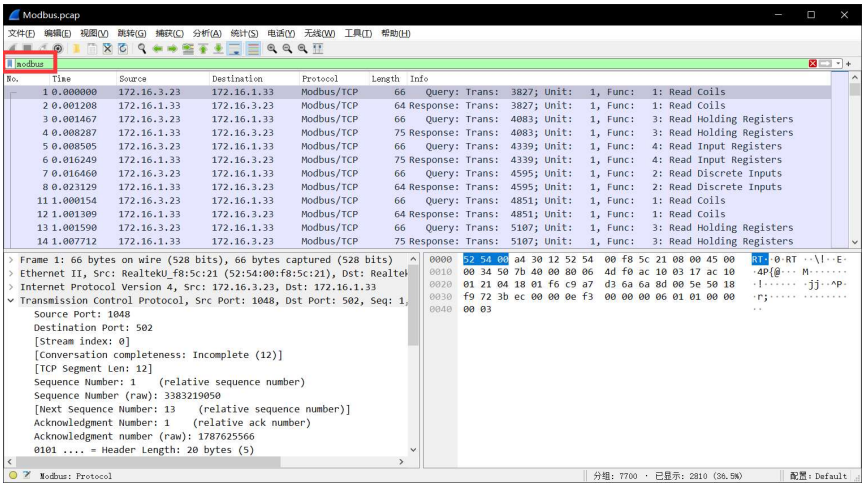
**题目中一般只考Modbus/TCP类型**

**功能码（常见）**

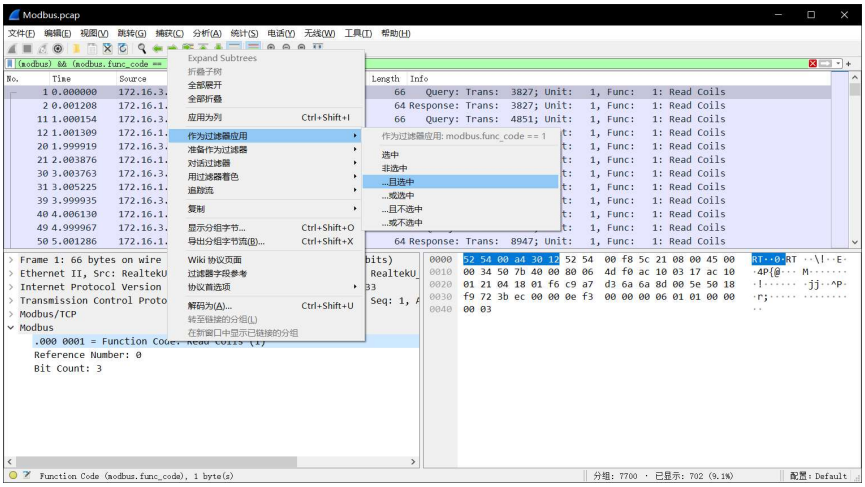
```
1：读线圈
2：读离散输入
3：读保持
4：读输入
5：写单个线圈
6：写单个保持
15：写多个线圈
16：写多个保持
```

## 例题1 HNGK-Modbus流量分析

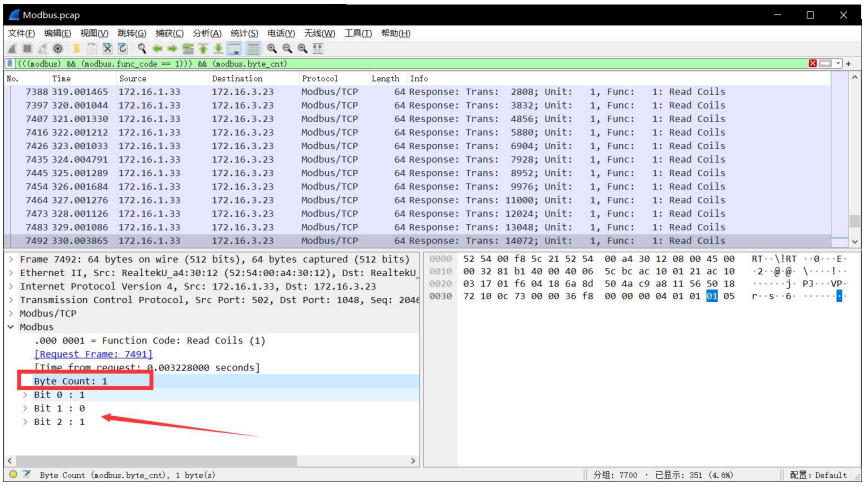
打开流量包发现基本都是Modbus/TCP协议，包含少量TCP协议，第一个筛选条件，找出所有Modbus协议



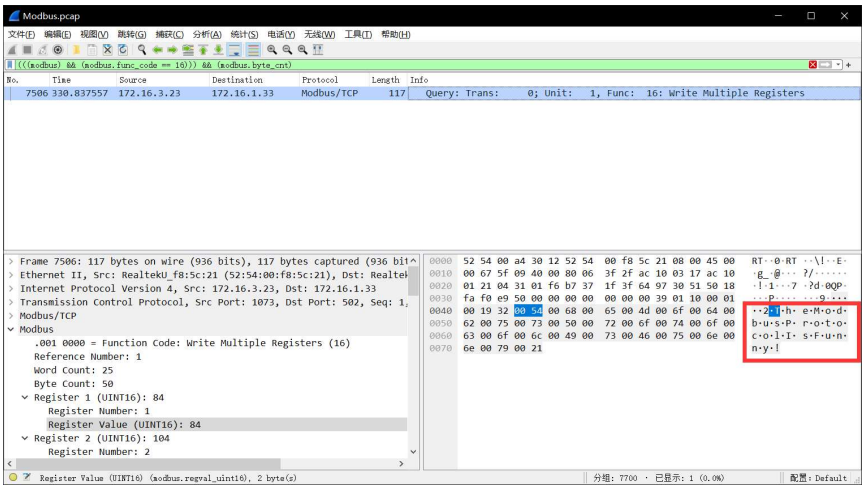

第二个筛选条件：分析功能码，以功能码为1举例




第三筛选条件，找回包（对比发现回包有一个代表长度的Byte Count），且发现看似是二进制的乱码




查找每一个功能码，最终在功能码16找到flag

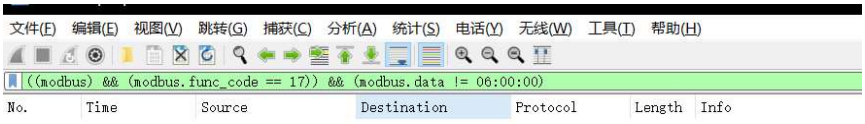



### 例题2 HNGK-modbus（异常流量）

flag为异常流量的序号

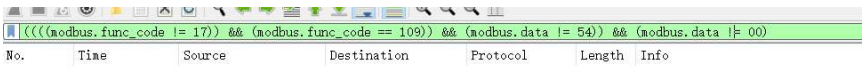
筛选出所有Modbus协议流量，发现有多种功能码，一个一个查询是否有异常流量

首先是17，发现请求包中无其他参数，查看前面几个回包均发现060000数据，猜测此为正常流量，于是将060000作为不查询条件




没有其余流量，判断功能码17无问题，将17作为不查询条件接着查看下一个功能码

功能码109：查询和返回都有数据，先将查询的数据54不选中，得到大量返回包，将其数据00不选中

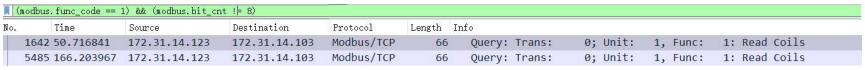



没有异常流量，查询下一功能码

功能码67：方式同上，这里将返回数据有多种情况

最终在功能码1中发现异常

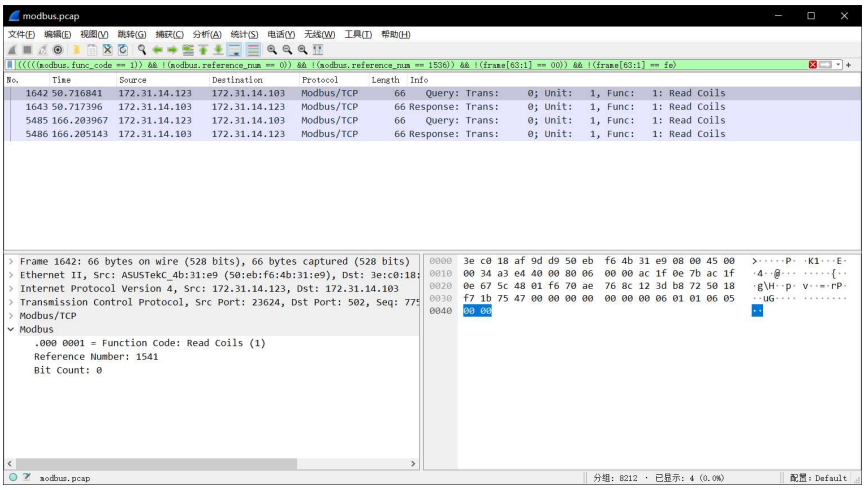
```
(modbus.func_code == 1) && (mo
```




有请求包就有返回包，四个包都是异常的，但是异常一定是有请求数据异常导致，所以实际上只需找到请求包即可

筛选条件有多种方式

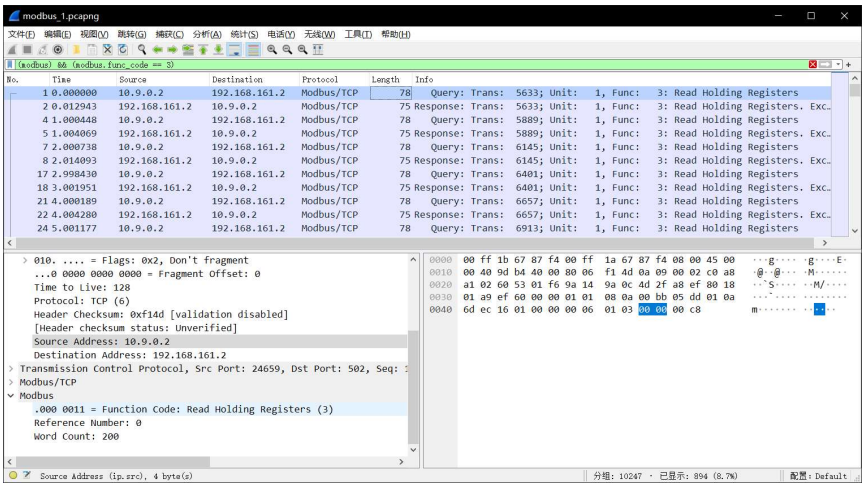
```
(((((modbus.func_code == 1)) && !(modbus.reference_num == 0)) && !
(modbus.reference_num == 1536)) && !(frame[63:1] == 00)) && !(frame[63:1] ==
fe)
```




### 例题3 HNGK-modbus协议分析（偏脑洞）

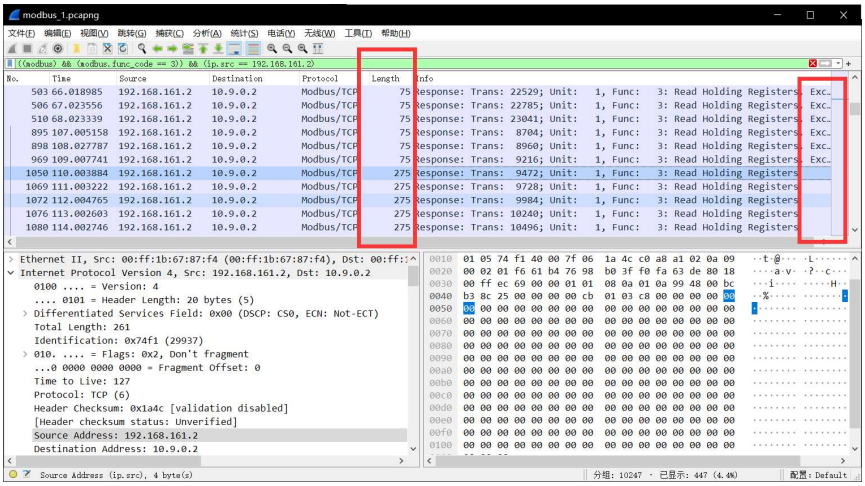
以Modbus协议为条件筛选，发现功能码大部分为3，少数为2和6，老规矩，一个一个分析

以功能码3为例：请求包几乎都一样，无明显异常



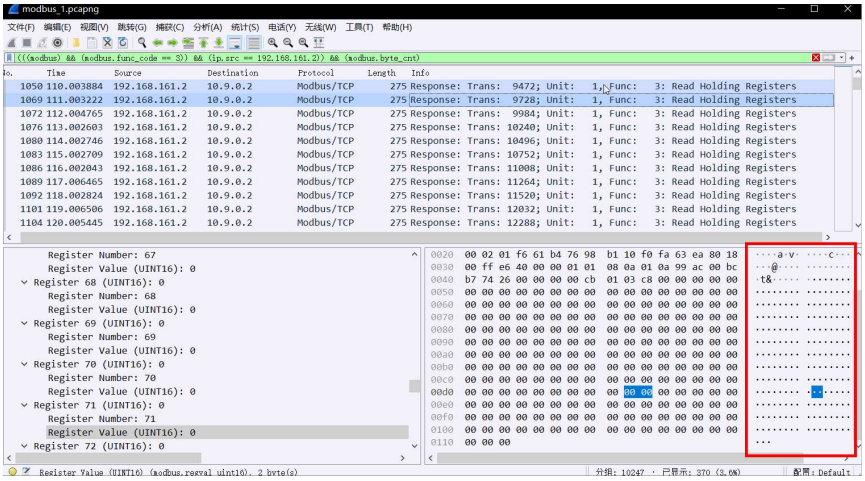

筛回复包，题中源ip为192.1688.161.2的是回复，所以ip.src == 192.168.161.2

可以看到有很多无效数据

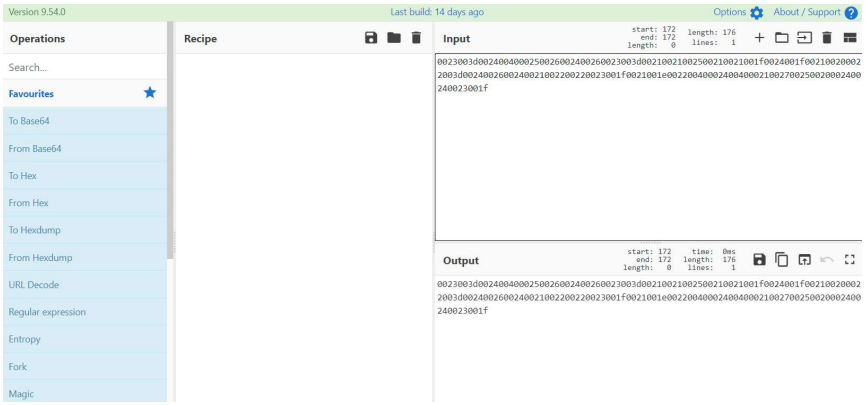



将无效数据筛除，条件有很多，这里筛选包含byte count的数据即为回复数据

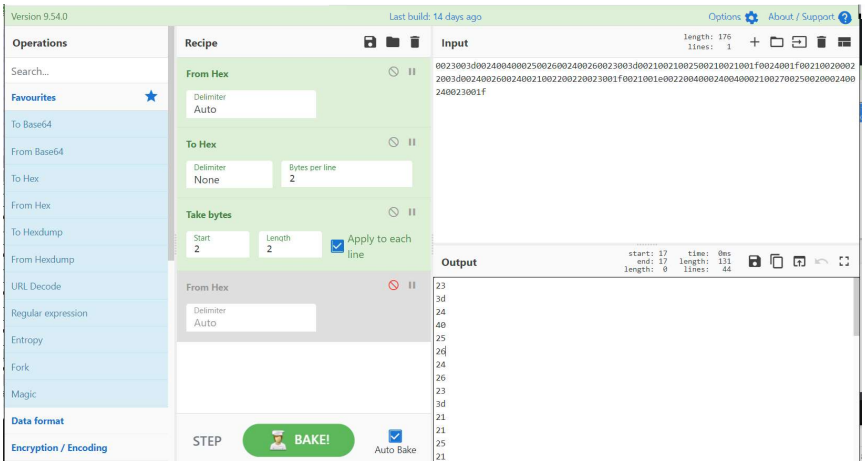
从头到尾看一遍会发现响应值逐渐出现数据，看似很有规律且都是键盘上那一行字符



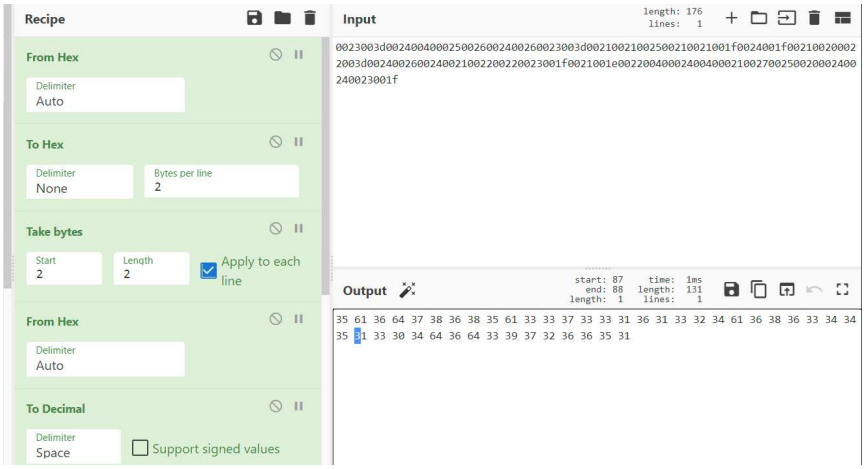

复制16进制流并剔除不需要的杂数据



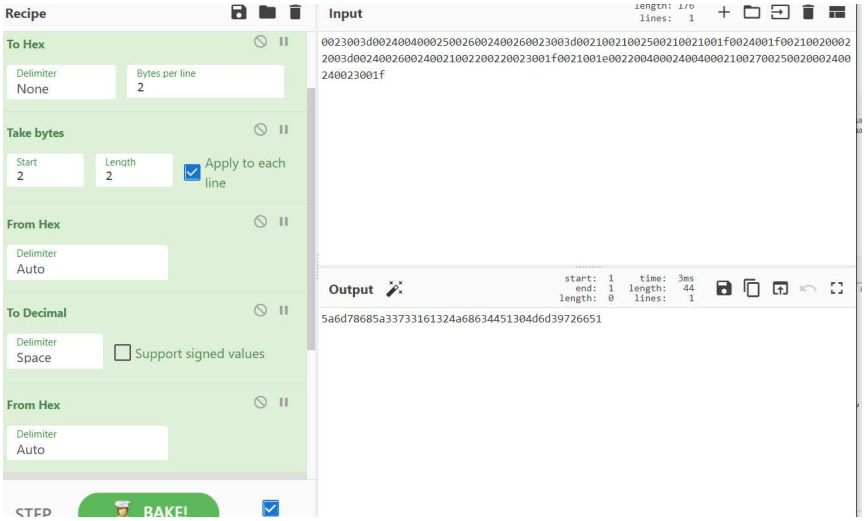

将无用字符00删除，得到有用十六进制



将其转为十进制



这一题的脑洞也就是这里，将十进制当做十六进制处理，发现居然没有乱码，得到的结果很合理



再解十六进制得到明显base64，解得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

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…

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

Shadow丶S　关注　3　8

杂项_流量包类_ctf杂项modbus_天问_Herbert555的博客 7-10
工控modbus题目:I2S-协议分析题目提示公开协议,在协议过滤规则中过滤 modbus 协议:题目提示正常…

[纵横网络靶场社区]Modbus协议_ctf modbus流量分析_末 初的博客-CSDN... 7-1
下载附件进行流量分析,查看Modbus协议,点击长度排序,发现一个长度比较突出的包包末尾写的就是fla…

NSSCTF之Misc篇刷题记录⑨ 最新发布 Aluxian_的博客 674
[GKCTF 2021]签到 [NISACTF 2022]bmpnumber [领航杯江苏省赛 2021]签到题 [鹤城杯 2021]Misc2 […

CTFHub 简单Modbus协议分析 WP qq_61993117的博客 1175
简单Modbus协议分析wp

记一道国外ctf杂项题_ctf杂项modbus_沐一 · 林的博客 6-25
CTF密码学总结(一) 沐一· 林: 太久了,忘记了 CTF密码学总结(一) jyw358: Known High Bits Factor Atta…

经典的modbus 从站模拟设备 03-14
问题是好像不能模拟除1之外的从站地址 其他功能OK

从CTF到工控安全.pdf 02-26
从CTF到工控安全.pdf

CTF:Modbus协议报文_恶意节点查找及错误报文分析 npu_nazi的博客 515
所提供的压缩包是某工控业务网络中的实际捕获的通信数据包。请你发现并找出其中所有的Modbus/T…

之江杯-modbus、异常的流量分析 Fisher 791
1

【CTF】- 练习日志8.25-27 pyhsaihz的博客 1112
ctf练习记录

某赛两杂项-CTF-brainfuck编码、modusbus协议分析 CTF小杂鱼的专栏 6180
一、某赛的brainfuck题目。 Brainfuck是一种极小化的计算机语言，它是由Urban Müller在1993年创建…

CTF-Misc(base64÷4、神奇的Modbus) m0_46335150的博客 2297
CTF-Misc(base64÷4、神奇的Modbus) 一、base64÷4 1.下载附件得到一个文本文件，一串数字加字母…

Brainfuck编译器源代码 09-29
Brainfuck是一种极小化的计算机语言，它是由Urban Müller在1993年创建的。由于fuck在英语…

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

含物联网协议modbus流量包pcap 05-30
含物联网协议modbus流量包pcap，可通过wireshark打开后，直接用modbus进行过滤。（注意…

2021 N1CTF CTF 真题.zip 12-07
2021 N1CTF CTF 真题

计算机网络实验四——TCP/UDP协议分析 buguo西瓜 1万+
一. 实验目的 1、 加深理解TCP报文结构 2、 通过跟踪TCP应用通信，能结合报文对整个通信过程进…

MODBUS通讯之数据帧格式解读（附资料下载） 热门推荐 weixin_39917818的博客 2万+
1.Modbus数据帧构成：地址域 + 功能码 + 数据 + 差错校验 下面逐一解释各部分的具体含义：（1）…

攻防世界-misc-神奇的Modbus mlws1900的博客 210
结果是错误的，看了其他人的wp，看到要补全modbus，有点小坑。下载附件，得到一个流量包，wire…

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…

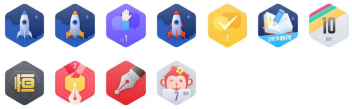
ctf中常用的PHP伪协议 02-15
在CTF比赛中，常常会使用PHP伪协议来绕过服务器的安全限制或者执行本不应该执行的操作。 PHP…




Shadow丶S 关注 3 8

Shadow丶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
指尖上の圊春: 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6——s7comm

2023年 1篇 2022年 91篇

目录

协议分析

CTF之协议分析文章合集

Modbus

例题1 HNGK-Modbus流量分析

例题2 HNGK-modbus（异常流…

例题3 HNGK-modbus协议分析…

Shadow丶S 关注