神奇的Modbus的writeup

原创

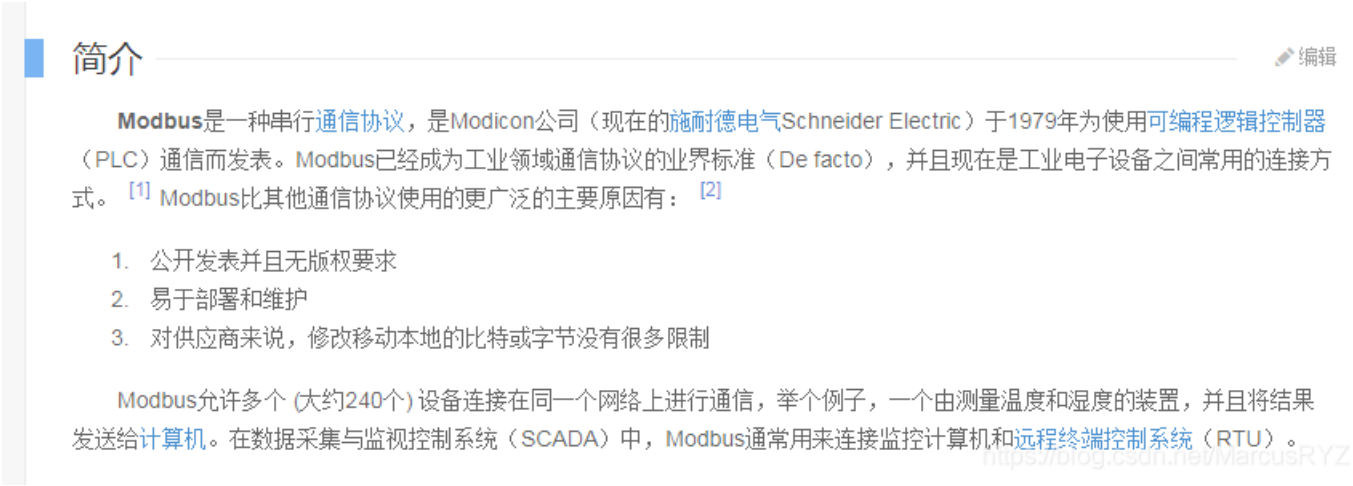
MarcusRYZ 于 2020-02-13 19:10:00 发布 2304 收藏 1

分类专栏： 攻防世界MISC高手进阶区 文章标签： 安全

本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104300675

大家好，这次我为大家带来的是攻防世界misc部分神奇的Modbus的writeup。

先下载附件，发现是一个流量包，于是用wireshark打开。注意到题目中有Modbus这个词。上网查一下，发现是一个通信协议。



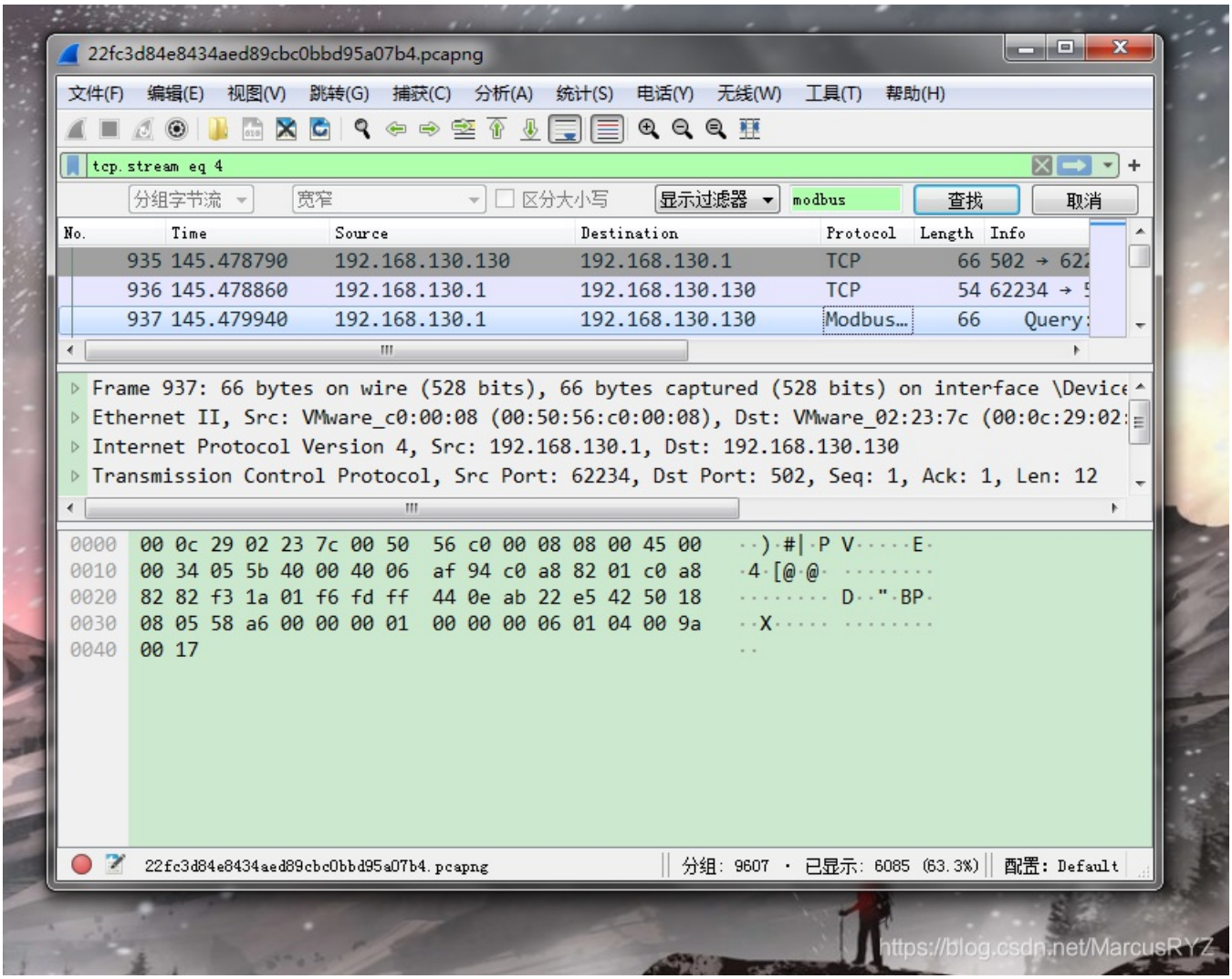
简介 编辑

Modbus是一种串行通信协议，是Modicon公司（现在的施耐德电气Schneider Electric）于1979年为使用可编程逻辑控制器（PLC）通信而发表。Modbus已经成为工业领域通信协议的业界标准（De facto），并且现在是工业电子设备之间常用的连接方式。[1] Modbus比其他通信协议使用的更广泛的主要原因有：[2]

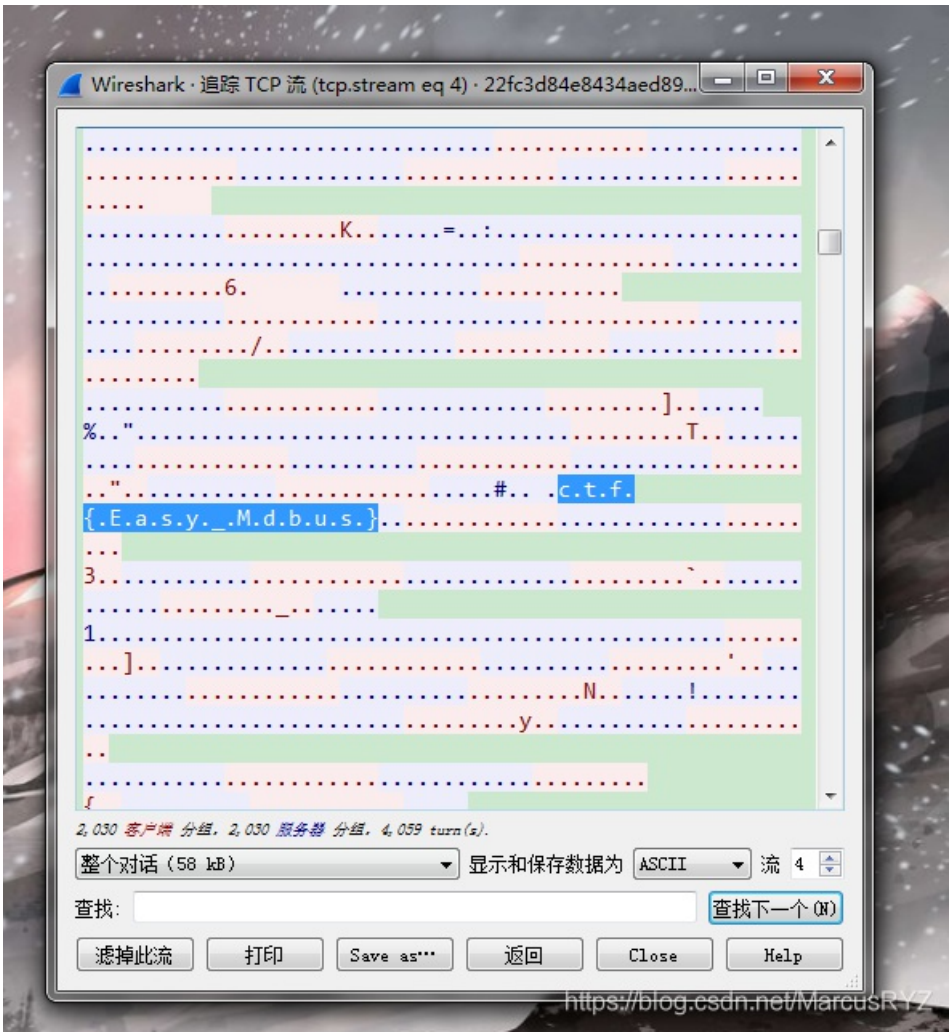
1. 公开发表并且无版权要求
2. 易于部署和维护
3. 对供应商来说，修改移动本地的比特或字节没有很多限制

Modbus允许多个(大约240个)设备连接在同一个网络上进行通信，举个例子，一个由测量温度和湿度的装置，并且将结果发送给计算机。在数据采集与监视控制系统（SCADA）中，Modbus通常用来连接监控计算机和远程终端控制系统（RTU）。

原来如此，那么就在wireshark的搜索栏中输入Modbus查找。



直接找flag貌似没有什么结果，那么我们就追踪TCP流，草草浏览一下，发现一些有价值的线索。



显然这个就是flag：Easy_Mdbus。直接提交发现一些错误，再仔细观察一下，flag应该是：Easy_Modbus。