2022第二届网刃杯网络安全大赛-ICS

原创

夜白君 于 2022-04-25 10:08:27 发布 3621 收藏 4

分类专栏： 2022第二届网刃杯网络安全大赛 文章标签： 网络安全 第二届网刃杯 ICS CTF

本文链接：https://blog.csdn.net/qq_43264813/article/details/124398122

2022第二届网刃杯网络安全大赛 专栏收录该内容

4 篇文章 36 订阅

订阅专栏

2022第二届网刃杯网络安全大赛-ICS

前言

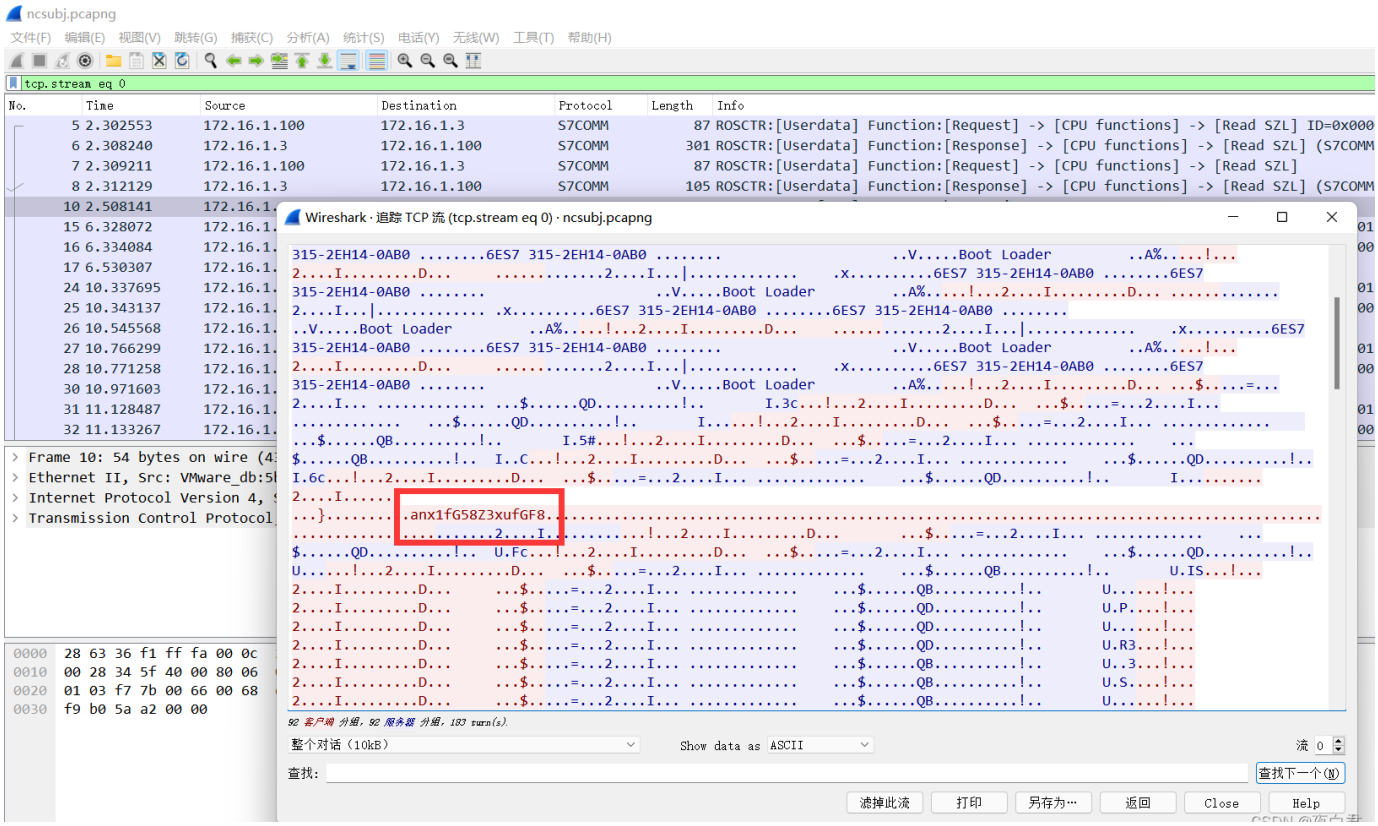
提示：该内容由夜刃TEOT战队-夜白君师傅原创，禁止抄袭！

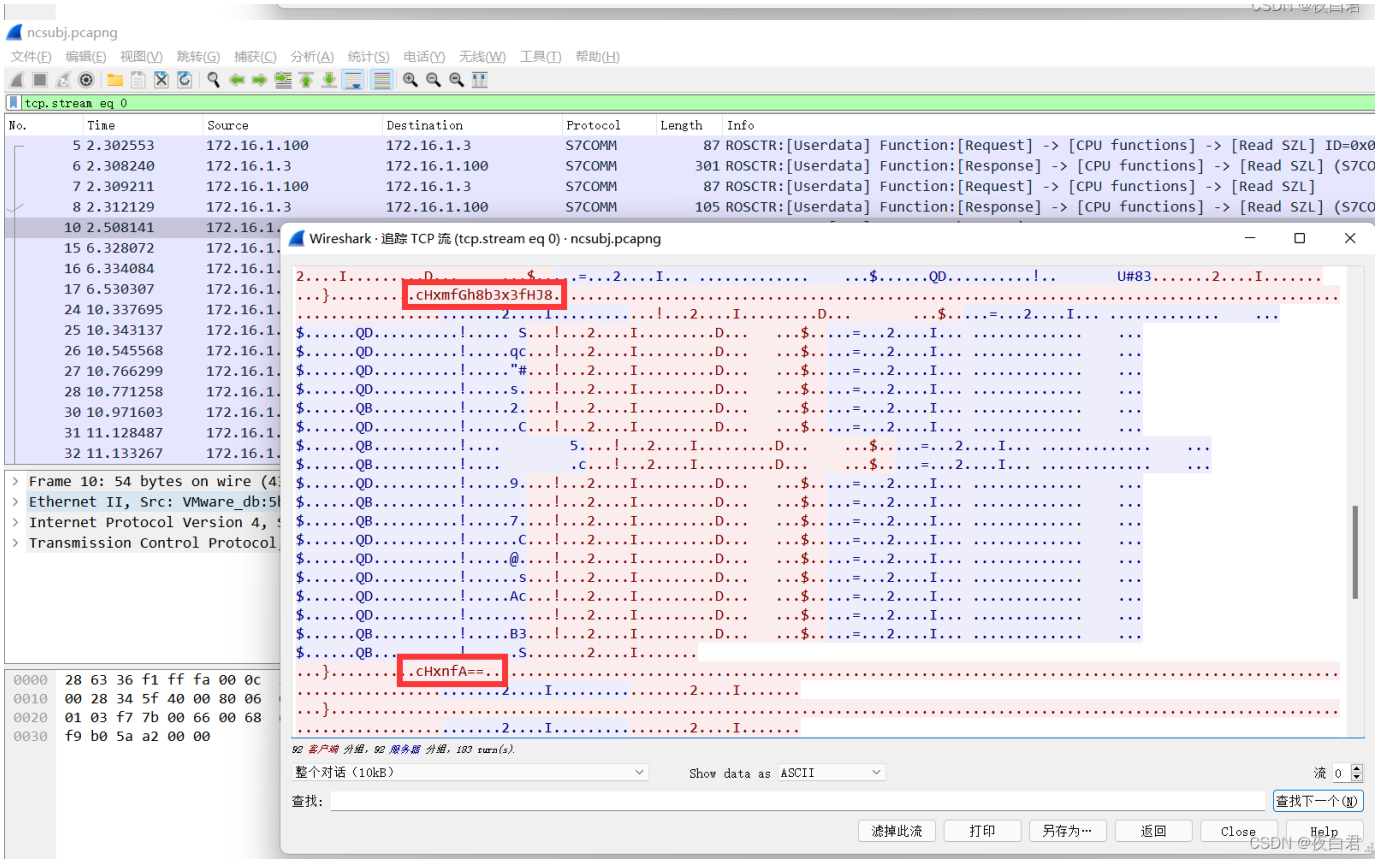
一、ICS1-ncsubj

难度系数：4.0

题目描述：wowowow，某厂商上位机TIA PORTIAL软件受到了hacker勒索软件的加密攻击，不过好在我们的监测系统捕获了攻击者非法操作的流量，具体的解密需要你自己去慢慢发现哟，flag格式为flag{}

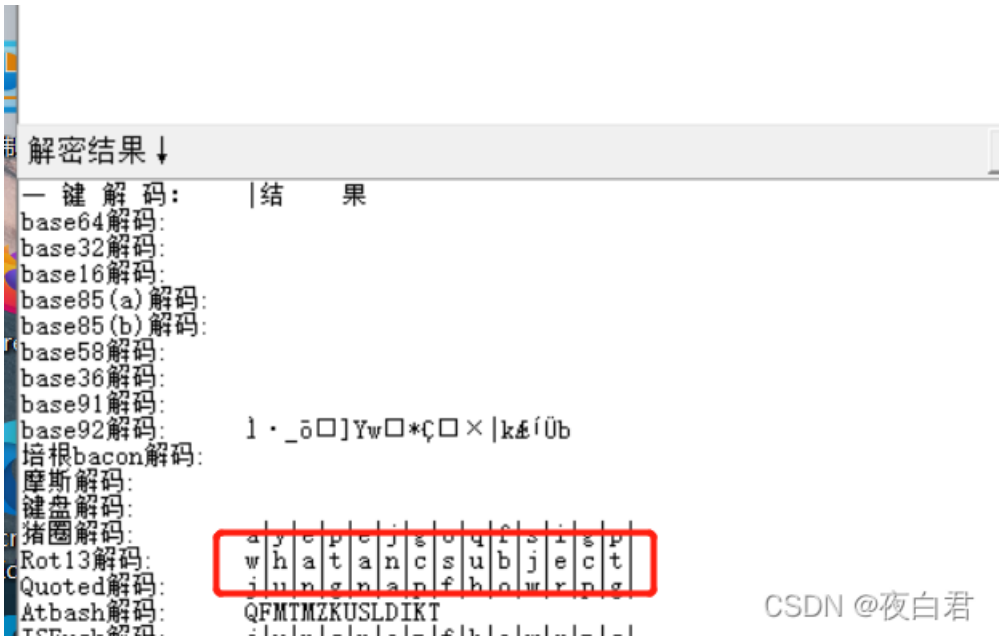
打开数据包进行分析查看，追踪TCP流发现了三段疑似Base64字符串





拼接整理在一起使用Base64进行解码

观察分析疑似依旧有编码加密存在，使用随波逐流继续解码分析拿到flag



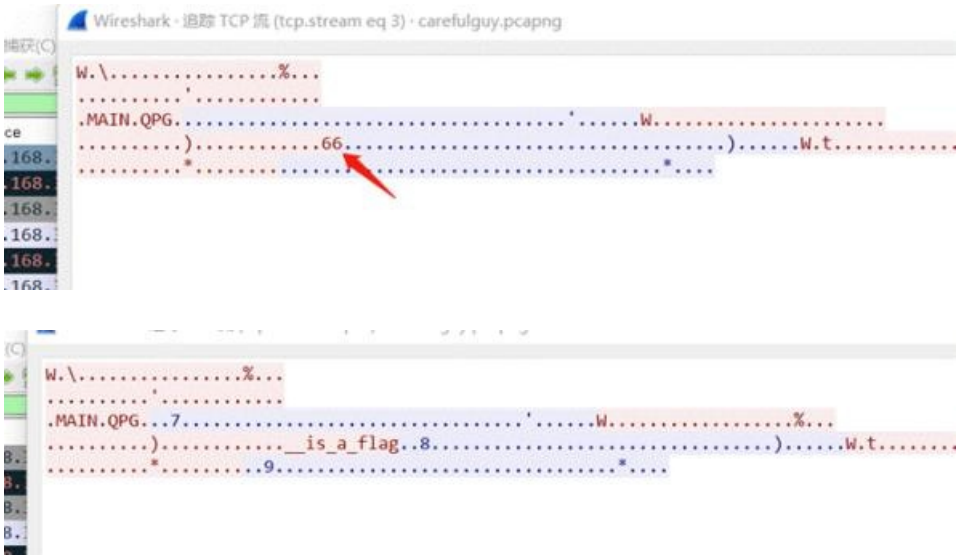
flag{whatancsubject}

二、ICS4-carefulguy

难度系数：4.0

题目描述：电厂工程师Bob正在对将电磁阀的工程写入PLC，传输时受到黑客攻击被迫停止，重启后才恢复运作，黑客的攻击导致工程师的数据丢失了一些，实时监测设备抓到一些流量包，你能从流量包中找出遗失的数据吗？

打开数据包进行分析查看，追踪TCP流发现了该位置一直存在数字，疑似16进制，将其每个流的摘取出 来排除其中is a flag和@那一部分



666c61677b703475733331357633727931 6e7433726573746963397d

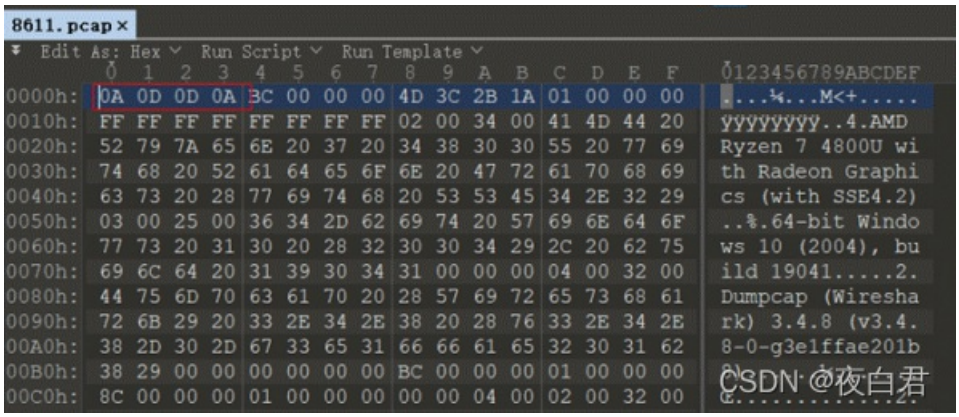
flag{p4us315v3rylnt3restic9}

三、ICS5-喜欢移动的黑客

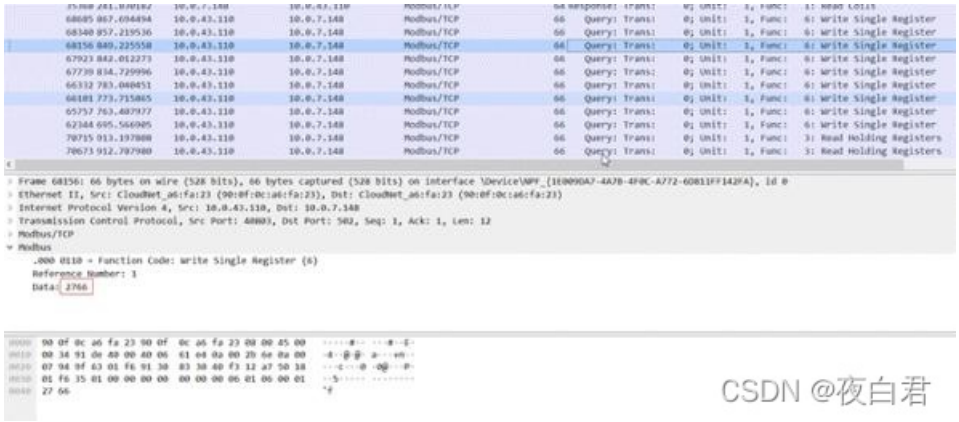
难度系数：3.0

题目描述：Monkey是一家汽修厂的老板，日常喜欢改装车，但由于发动机的转速有上限，发动机最多能接受10000转/分钟的转速，Monkey在最新一次对发动机转速进行测试时发生了故障，机械师阿张排查时测试期间，有一些异常的流量，请根据阿张捕获的流量包分析发动机的转速达到了多少转才出现的故障,flag为flag{data+包号}

修复pcap包头



2766,为16进制，转换为10进制得到10086+包号68156组成flag{1008668156}



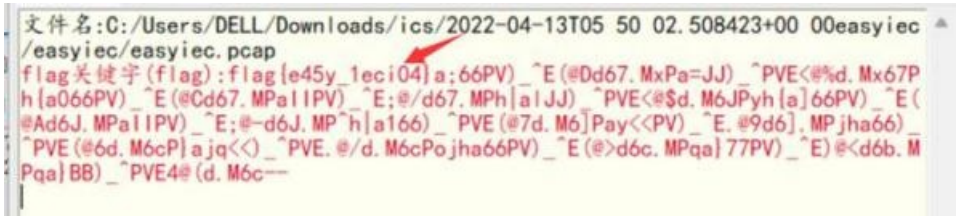
flag{1008668156}

四、ICS6-easyiec

难度系数：3.0

题目描述：小Q刚刚入职了电力部门，刁钻的主管让他学习第一堂课工控ctf，但是小Q从来没有接触过ctf，你能帮助他吗？

使用工具梭哈一下即可拿到flag



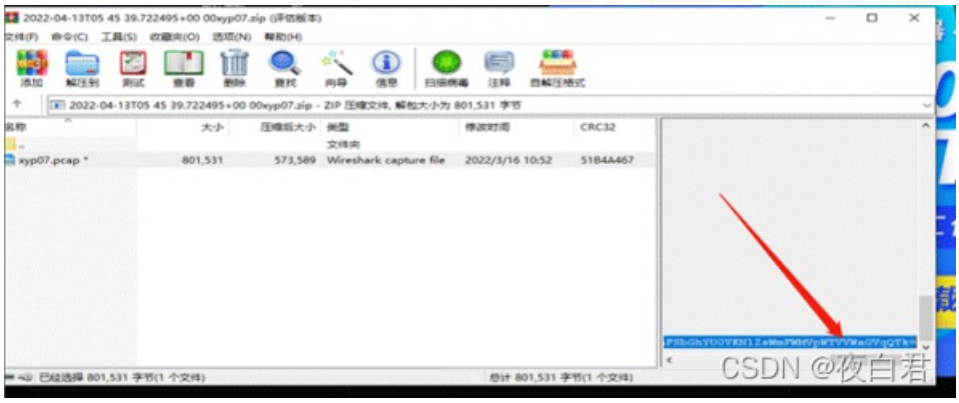
flag{e45y_1eci04}

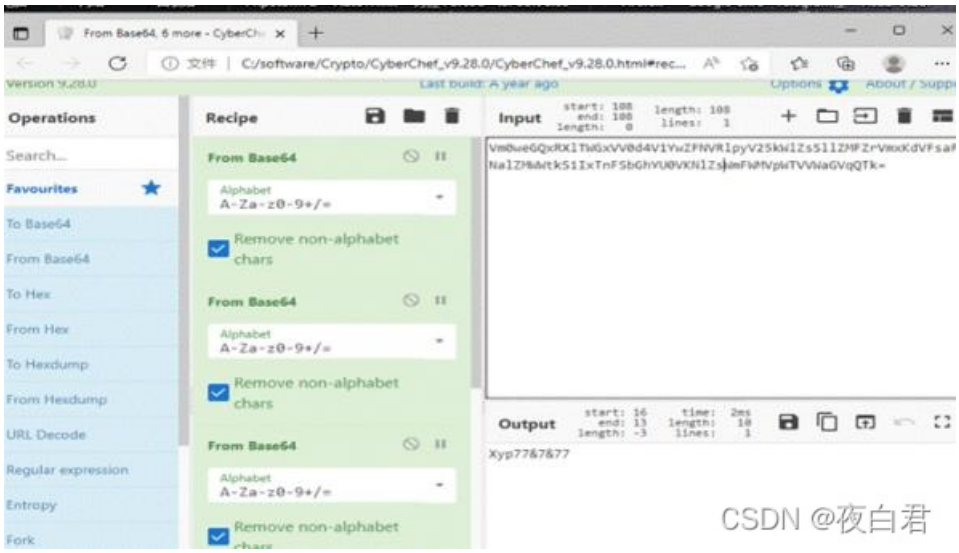
五、ICS8-xyp07

难度系数：3.0

题目描述：电气公司的师傅九爷今日收了他的第七个徒弟，取名做小七，九爷生来喜欢7这个数字，于是决定重点培养小七，于是便给小七出了一道测试题，初入行业的小七显得不知所措，你能帮助他解决这个问题么？

解压发现需要密码，在压缩包注释中发现加密字符串，解码拿到密码





打开pcap查看分析发现在TCP流1中有一串疑似加密字符串，解一下发现为flag

flag{welcome_S7_world_xyp07}