error

2021-09-05 | Challenge， 2021， 第七届全国工控系统信息安全攻防竞赛， 四类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 四类 | error

点击此处获得更好的阅读体验

WriteUp来源

来自 `bad_cat` 战队

题目描述

> 查看附件以获取flag

提示信息

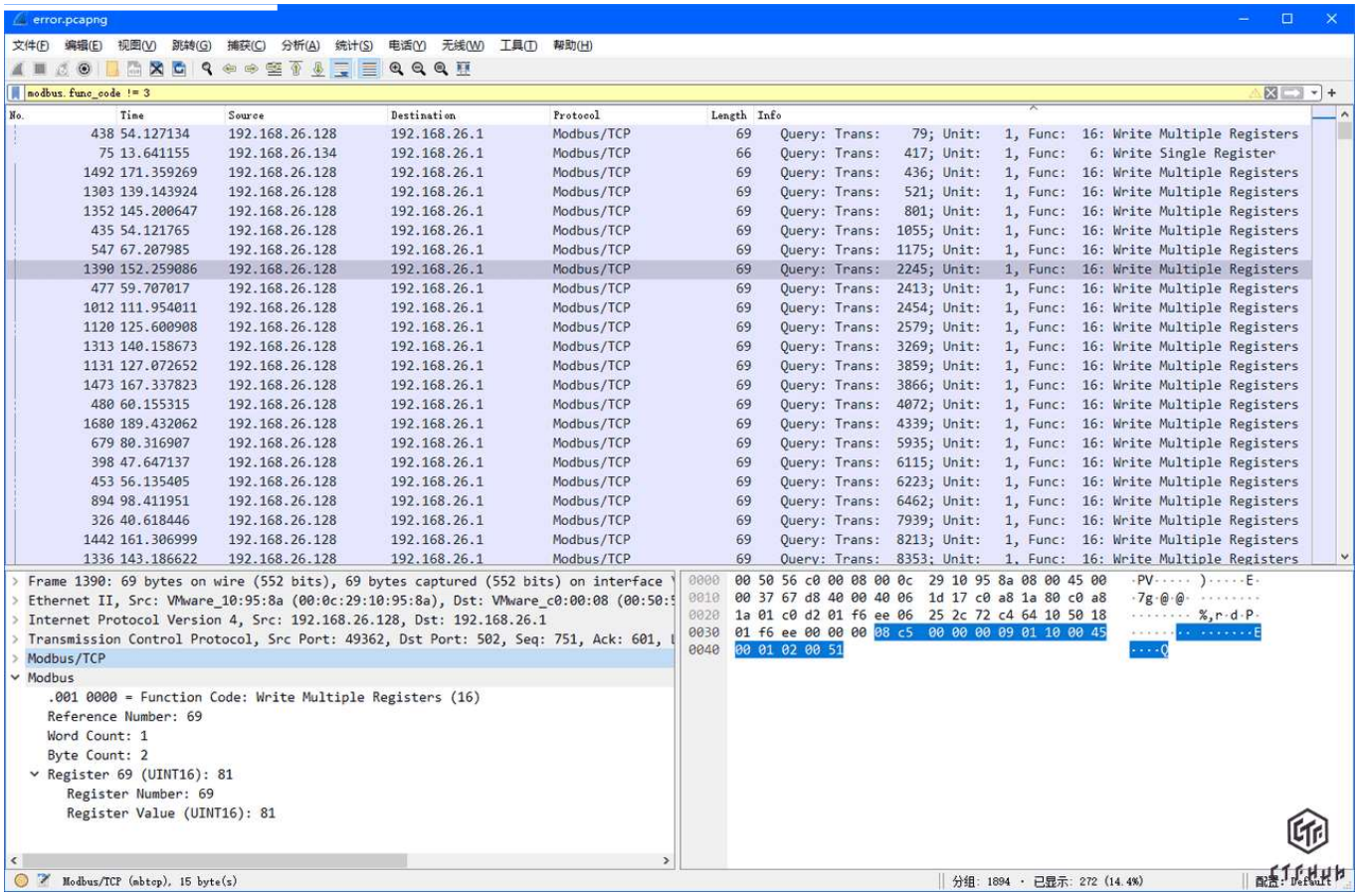
无

题目考点

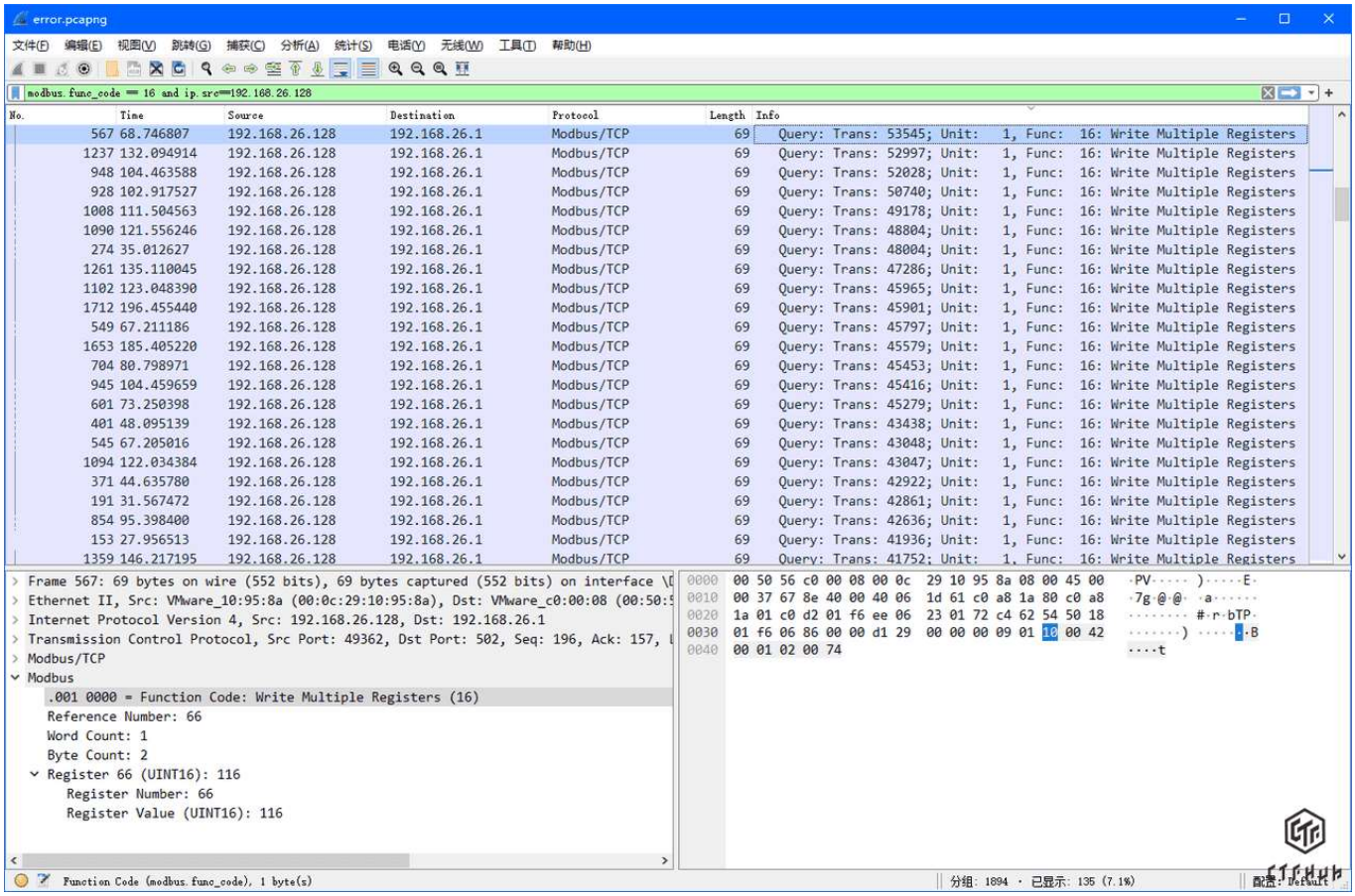
- 流量分析
- Modbus协议

解题思路

过滤出modbus协议的流量，发现其中除了读取Holding 寄存器之外，就是写多个寄存器，吧所有写入包过滤出来



之后进行查看，只有写多个寄存器时是写入了数据的，进一步把 `Write Multiple Register` 过滤



发现每个数据包写入了两个字节，但其实写入的内容大部分都是在0-127，而且是写入了不同位置的寄存器

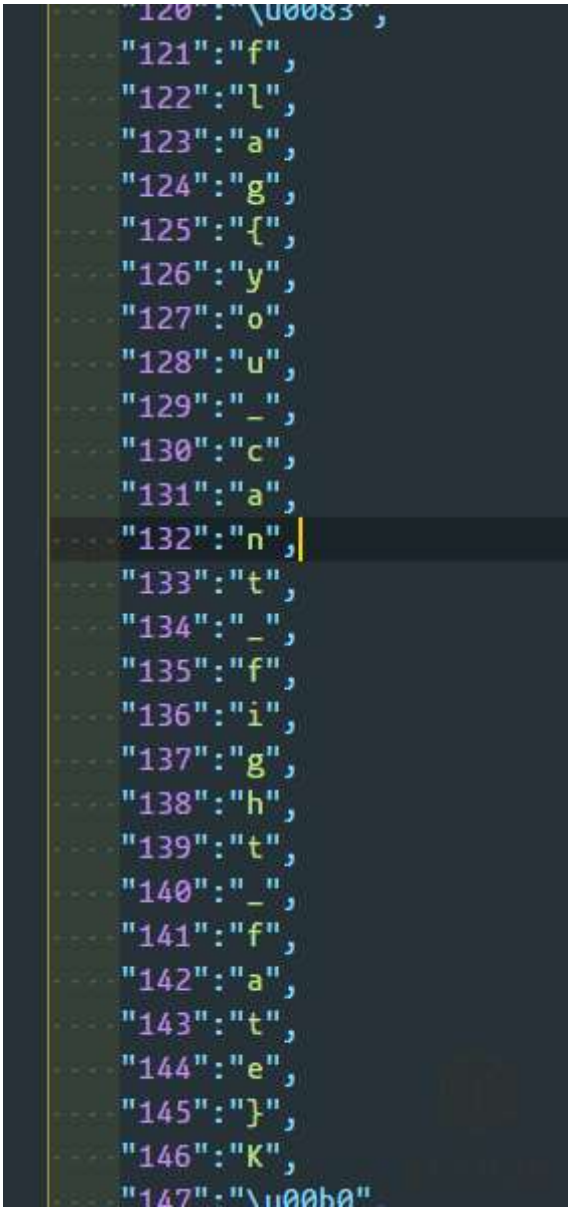
首先将上述条件过滤后的数据包分组另存为modbus.pcap，之后写脚本把这部分提取出来

```
import pyshark
import json
cap = pyshark.FileCapture('modbus.pcap')
ret = {}
for pkt in cap:
    k = int(pkt.modbus.regnum16)
    v = int(pkt.modbus.regval_uint16)
    ret[k] = chr(v)
    print(k,v)
print(json.dumps(ret))
```

之后得到结果

```
{"101": "\u009f", "102": "+", "56": "r", "103": "\u00c1", "104": "K", "51": "\u00b3
```

之后进行排序，很容易就可以发现flag



Flag

```
1  flag{you_cant_fight_fate}
```


Challenge # 2021 # 第七届全国工控系统信息安全攻防竞赛 # 四类

‹ Web1 梯形图 ›