被篡改的数据

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge， 2020， 工业信息安全技能大赛， 济南站
Challenge | 2020 | 工业信息安全技能大赛 | 济南站 | 被篡改的数据

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *某黑客拿到上位机的权限后对工控设备存储的数据进行了大量的修改，请分析其攻击数据，并找到其中的flag信息。Flag格式为：flag{}。*

题目考点

- *流量分析*
- *S7Comm协议分析*

解题思路

1. S7Comm分析

S7Comm（S7 Communication）是西门子专有的协议，是西门子S7通讯协议簇里的一种。S7协议的TCP/IP实现依赖于面向块的ISO传输服务。S7协议被封装在TPKT和ISO-COTP协议中，这使得PDU（协议数据单元）能够通过TCP传送。它用于PLC编程，在PLC之间交换数据，从SCADA（监控和数据采集）系统访问PLC数据以及诊断目的。

2. 过滤S7Comm

在过滤器中输入S7Comm，过滤出S7Comm的数据，根据S7Comm的数据格式分析，S7Comm的PDU存在如下两个类型:

运行如下脚本：

```
import pyshark
def func_s7():
    try:
        captures = pyshark.FileCapture("")#这里为文件的路径
        func_codes = {}
        for c in captures:
            for pkt in c:
                if pkt.layer_name == "s7comm":
                    if hasattr(pkt, "param_func"):#param_func功能码字段
                        func_code = pkt.param_func
                        if func_code in func_codes:
                            func_codes[func_code] += 1
                        else:
                            func_codes[func_code] = 1
        print(func_codes)
    except Exception as e:
        print(e)
if __name__ == '__main__':
    func_s7()
```

执行后的如图所示，一共存在三种功能码：0x04(读取值 Read Var)出现3984次、0xf0(建立通信 Setup communication)出现2次、0x05(写入值 Write Var)出现4016次。

3. 功能码分析

因为异常数据很有可能被黑客写入设备，因此首先重点分析功能码为0x05的流量，在wireshark中过滤流量`s7comm.param.func ==0x05`，其中PDU为Job的数据包是有可能存在黑客写入的数据请求，于是人工审计PDU为Job的数据包。

4. 获取Flag

在19987包往后开始出现flag字样

依次提取出来即可

也可以使用脚本来提取

```
#!/usr/bin/python2.7.8
#encoding:utf-8

import pyshark

captures = pyshark.FileCapture("s702.pcapng")
list = []
for c in captures:
    for pkt in c:
        if pkt.layer_name == "s7comm" and hasattr(pkt, "param_func"):
            param_func = pkt.param_func
            try:
                if param_func=='0x00000005':
                    list.append(pkt.resp_data)
                else:
                    continue
            except Exception as e:
                print(e)
print (list)
```

Flag

```
flag{931377ad4a}
```


Challenge # 2020 # 工业信息安全技能大赛 # 济南站
IoT
工业物联网智能网关数据分析