协议精准定位分析

发表于 2021-02-18 更新于 2021-08-31 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 | 协议精准定位分析

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

> *企业自动化运维管理员最近发现某工控设备频繁出现可疑地流量，请您帮助他分析确认一下问题。Flag格式为：flag{}。*

题目考点

解题思路

对流量包进行分析，发现有两个ip频繁的使用tcp协议在进行信息的传输。

追踪一下tcp流，查看一下详情。为了直观，在wireshark中转码

发现LSIS-XGT字样,发现是LSIS-XGT协议,

打开协议规范说明书XGB_FEnet(080611).pdf。

提取出发包内容来,发现发包有两种长度的包,收包也有两种长度的包,

```
1 发
2 4c5349532d58475400000000a0330000160003475800140000000100060025 4d4232303004007d000000
3 4c5349532d58475400000000a0330000120003435400140000000100060025 4d423230300100
4
5 收
6 4c5349532d58475400110100a01100000a000347590014000801000001 00
7 4c5349532d58475400110100a01100000d000343550014000801000001 00010000
```

首先根据协议类型分析发送包的第一个包

`4c5349532d58475400000000a0330000160003475800140000000100060025 4d4232303004007d000000`

首先LSIS Header 长度为20个字节,

`4c5349532d58475400000000a033000016000347`*为header*

再往后面两个字节`5800`表示写操作，往后两个字节`1400`表示数据类型,

再往后6个字节`000001000600`表示`Reseverd area, Number of blocks` 和 `length of variables`可以先不关注

取最后一部分进行关注分析`254d4232303004007d000000`

解码,继续分析文档

其中前面的`254d42323030`即 `%MB200`, 表示写入地址，`0400`表示写入数据长度，`7d000000` 四个字节正好是上面的写入长度

到这,这个协议其中一种发包情况就分析结束，其他的发包和回包都能通过协议手册进行分析。

此题的考点就在上述分析的这种类型的包内,而且写入的4个字节,后三个字节都是空的,

追踪流之后,可以将整个流的raw数据复制出来,然后,用脚本取出上面7d000000位置的数据来进行分析.

```
#coding:utf-8
import os
import base64

lines = open('./提取出的数据.txt').readlines()
flag = ''
for line in lines:
    line = line.strip()
    if len(line) == 84:
        t = line[76:78]
        x = int(t,16)
        y = chr(x)
        flag += y
    else:
        pass
    print(flag[::-1])
```

Flag

```
flag{c93650241853da240f9760531a79cbcf}
```


- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/济南站/gbjuP64PLn98WMkybo535L.html
- **版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

#Challenge #2020 #工业信息安全技能大赛 #济南站
病毒文件恢复
old_driver