黑客的Fuzz

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 ， 石家庄站
Challenge | 2020 | 工业信息安全技能大赛 | 石家庄站 | 黑客的Fuzz

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进行扫描fuzz攻击，请分析其攻击数据，并找到其中的flag信息。flag格式为：flag{}。 ----本题由恒安嘉新贡献*

题目考点

解题思路

使用s7comm协议对读数据包的地址进行提取分析

可以看到读取值16进制为0x04

功能码附录：

- *0x00 - CPU services CPU服务*
- *0xf0 - Setup communication 建立通信*
- *0x04 - Read Var 读取值*
- *0x05 - Write Var 写入值*
- *0x1a - Request download 请求下载*
- *0x1b - Download block 下载块*
- *0x1c - Download ended 下载结束*
- *0x1d - Start upload 开始上传*
- *0x1e - Upload 上传*
- *0x1f - End upload 上传结束*
- *0x28 - PI-Service 程序调用服务*
- *0x29 - PLC Stop 关闭PLC*

可以在wireshark中看到读取码0x04和地址码

需要将全部s7协议读取的地址码利用脚本读取出来得到以下文件

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

#此程序是s703流量的exp，对所有读数据包的地址进行提取分析其规律并查找flag，发现其地址是16进制的图片，将所有的地址取出后还原为图片，找到exif信息中的flag。
import pyshark
captures = pyshark.FileCapture("s703.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=='0x00000004':
                    list.append(pkt.param_item_address)
                    print list
                else:
                    continue
            except Exception as e:
                print(e)
```

使用winhex查看图片中存在的字符串，是隐藏的flag。

Flag

```
flag{50f84daf3a6dfd6a9f20c9f8ef428942}
```


 # Challenge # 2020 # 工业信息安全技能大赛 # 石家庄站
简单的固件逆向分析
工具提交说明