工业协议分析2

发表于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 工业协议分析2

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/5960

题目描述

> *在进行工业企业检查评估工作中，发现了疑似感染恶意软件的上位机。现已提取出上位机通信流量，尝试分析出异常点，获取FLAG。*

题目考点

- *UDP数据包分析*

解题思路

打开流量包，发现存在关于ARP、UDP、SNA协议的流量包，其中存在大量的UDP流量，如图所示：

首先对UDP流量包进行分析，分析发现UDP流量包的长度存在大量相同，一共出现的长度分别为16 17 12 14 10 18 19 20 22 25 32 89 95 104 105 116 131 137 524 528，在这些长度中仅12 89 104 105 131 137出现一次，其余长度多次出现，于是猜测这仅出现一次的流量包存在异常，于是分别分析12 89 104 105 131 137对应的流量包，发现131，137对应的流量包存在异常的字符串，如图所示：

提取出字符串666c61677b37466f4d3253746b6865507a7d，并转换成对应ACII码，得到Flag,

Flag

```
1 flag{7FoM2StkhePz}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/cNmpHkuUpUdjfJVbKAsF6T.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 # 2019 # 工业信息安全技能大赛 # 深圳站
组态软件安全分析
工业协议分析1