

攻防世界crypto高手题的工业协议分析2

原创

沐一·林 于 2021-09-08 21:58:07 发布 75 收藏 1

分类专栏: [CTF 密码学](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/xiao__1bai/article/details/120189759

版权



CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏



密码学

51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之工业协议分析2

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的工业协议分析2

工业协议分析2

最佳Writeup由 [系统战队](#) · admin 提供

WP 建议

难度系数: ★★2.0

题目来源: 2019工业信息安全技能大赛个人线上赛第一场

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。flag形式为 flag{}

题目场景: 暂无

题目附件: 附件1

CSDN @沐一一沐, 一沐沐一

下载附件, 是一个pcapng流量文件:



64da5a...

(这里积累第一个经验)

题目描述说已提取出上位机通信流量, 尝试分析出异常点, 获取FLAG。flag形式为 flag{}, 这其实就是一个暗示, flag就在通信流量中, 至于哪里异常, 查了资料, 有的说UDP的长度有部分异常, 要一个个点击查看。可是为什么我感觉UDP大的一堆, 小

的也一堆，也不知道哪里异常：

Destination	Protocol	Length	Info
192.168.1.123	UDP	62	11000 → 64406 Len=20
192.168.1.181	UDP	58	64406 → 11000 Len=16
192.168.1.123	UDP	566	11000 → 64406 Len=524
192.168.1.181	UDP	58	64406 → 11000 Len=16
192.168.1.123	UDP	62	11000 → 64406 Len=20
192.168.1.181	UDP	58	64406 → 11000 Len=16
192.168.1.123	UDP	566	11000 → 64406 Len=524
192.168.1.181	UDP	58	64406 → 11000 Len=16
192.168.1.123	UDP	62	11000 → 64406 Len=20
192.168.1.181	UDP	58	64406 → 11000 Len=16
192.168.1.123	UDP	566	11000 → 64406 Len=524
192.168.1.181	UDP	58	64406 → 11000 Len=16

bled]

CSDN @沐一一沐，一沐沐一

然后就是题目暗示说flag在异常流量中，那直接明文匹配查找不就行了？先搜索flag，无果，换十六进制666c6167试试，查到了，用as printable text 选项dump下来即可：

The image shows the Wireshark interface with a packet capture filtered by '666c61'. The packet list pane shows several UDP packets between 192.168.1.123 and 192.168.1.181. The packet details pane shows the selected packet's header and data. A context menu is open over the data field, with 'as Printable Text' highlighted. The data field shows a hex dump of the packet payload, with the flag '666c6167' visible in the hex dump.

CSDN @沐一一沐，一沐沐一

结果：

16进制到文本字符串

加密或解密字符串长度不可以超过10M

1 666c61677b37466f4d3253746b6865507a7d



16进制转字符

字符转16进制

测试用例

清空结果

复制结果



西部数码
www.west.cn

企业网站专用云服务器 仅需78元

更安全、更稳定、更快速的云服务器，仅需78元！

西部数码

1 flag{7FoM2StkhePz}

CSDN @沐一一沐，一沐沐一

总结：

1:
(这里积累第一个经验) 题目描述说已提取出上位机通信流量，尝试分析出异常点，获取FLAG。flag形式为 flag{}，这其实就是一个暗示，flag就在通信流量中，至于哪里异常，查了资料，有的说UDP的长度有部分异常，要一个个点击查看。可是为什么我感觉UDP大的一堆，小的也一堆，也不知道哪里异常。
然后就是题目暗示说flag在异常流量中，那直接明文匹配查找不就行了？先搜索flag，无果，换十六进制666c6167试试，查到了，用as printable text 选项dump下来即可。

解毕！敬礼！