简单流量分析

发表于 2021-01-25 分类于 Challenge， 2019， 工业信息安全技能大赛， 山东站
Challenge | 2019 | 工业信息安全技能大赛 | 山东站 | 简单流量分析

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

> *不久前，运维人员在日常安全检查的时候发现现场某设备会不时向某不知名ip发出非正常的ICMP PING包。这引起了运维人员的注意，他在过滤出ICMP包分析并马上开始做应急处理很可能已被攻击的设备。运维人员到底发现了什么?flag形式为flag{}*

题目考点

解题思路

ICMP包长度转为ascii 码, 最后 base64 解码得 flag

```
#!/usr/bin/env python
# coding:utf-8
import base64
from scapy.all import rdpcap

packets=rdpcap("./2-8.pcap")
res = ""
for p in packets:
    if p.payload.payload.type == 8:
        l = len(str(p.payload.payload.payload))
        res += chr(l)

print base64.b64decode(res)
```

Flag

```
FLAG{xx2b8a_6mm64c_fsociety}
```

- ***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/山东站/wQwpcqxkStdjNFFLJMmpa3.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 # 山东站
另一个隐藏的黑客
奇怪的文件