攻防世界 Crypto高手进阶区 5分题 简单流量分析

原创

思源湖的鱼 于 2021-01-07 14:45:19 发布 588 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112236517

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是简单流量分析的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

题目描述

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{}

binwalk无果

查找关键词无果

每个包都有一串字符

```
4c ed fb cc 1f 50 78 4f  43 72 fe b3 08 00 45 00   L····PxO Cr····E·
00 65 00 01 00 00 40 01  cf fb c0 a8 03 49 36 c7   ·e····@· ·····I6·
af e3 08 00 a3 16 00 00  00 00 50 5a 63 37 39 41   ········ ··PZc79A
41 47 45 30 50 32 46 57  4f 30 59 6d 55 6e 58 75   AGE0P2FW O0YmUnXu
39 68 67 74 49 74 45 4f  33 36 76 54 4f 63 39 66   9hgtItEO 36vTOc9f
69 54 79 39 76 53 49 34  69 51 65 70 55 31 65 4f   iTy9vSI4 iQepU1eO
79 58 42 61 72 77 43 6d  50 35 61 57 67 72 36 53   yXBarwCm P5aWgr6S
32 56 74                                           2Vt
```

但是常规解密失败

那猜测是某几个长度不对劲的包有问题
或者在长度或ttl之类的数值上做了隐写或加密

然后发现包长度从90到164
而data段的长度从48到122
对应ascii码是`0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_abcdefghijklmnopqrstuvwxyz`

那就提取data长度
转为ascii码
再base64

```python
from pyshark.capture.file_capture import FileCapture
from base64 import b64decode
from sys import argv

def solve(file_name):
    packets=FileCapture(input_file=file_name)
    res=''
    for packet in packets:
        for pkt in packet:
            if pkt.layer_name=='icmp' and int(pkt.type,16):
                res+=chr(int(pkt.data_len))
    return b64decode(res)

if __name__=='__main__':
    print solve(argv[1])
```

得到flag：`flag{xx2b8a_6mm64c_fsociety}`

结语

数据包某个数值的长度常被用来传递信息