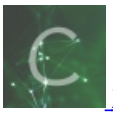
XCTF练习题---MISC---Hidden-Message

原创

Hskb 于 2021-09-10 11:48:42 发布 1071 收藏 1

分类专栏： XCTF 文章标签： unctf 网络安全

本文链接：https://blog.csdn.net/liu914589417/article/details/120217742



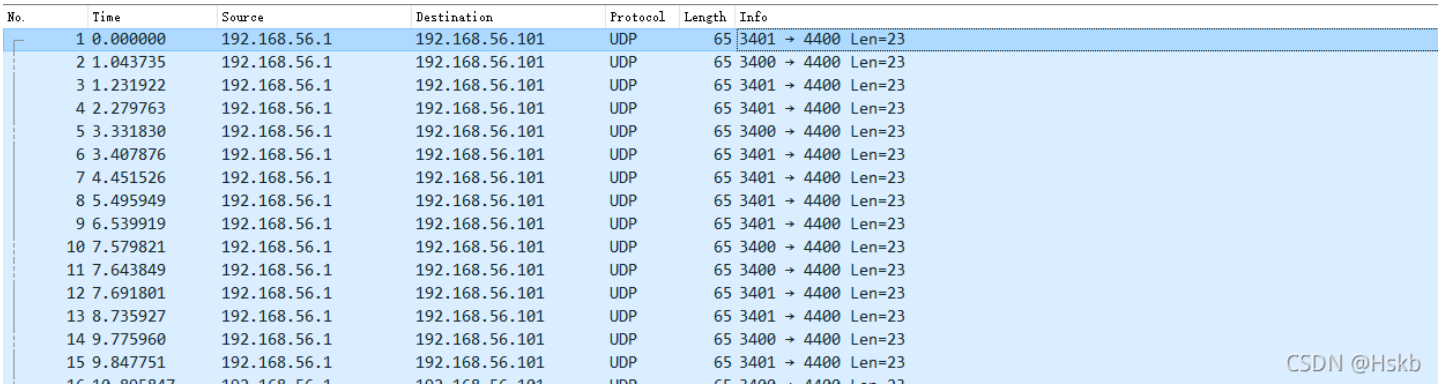
XCTF练习题—MISC—Hidden-Message

flag：Heisenberg

解题步骤：

1、观察题目，下载附件

2、拿到手以后发现是一个数据包格式，打开看一下



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
2	1.043735	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23
3	1.231922	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
4	2.279763	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
5	3.331830	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23
6	3.407876	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
7	4.451526	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
8	5.495949	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
9	6.539919	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
10	7.579821	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23
11	7.643849	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23
12	7.691801	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
13	8.735927	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23
14	9.775960	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23
15	9.847751	192.168.56.1	192.168.56.101	UDP	65	3401 → 4400 Len=23

3、查看UDP流，并没有什么有价值的信息，经过仔细观察，发现3401和3400两个数字有点问题，感觉有点像二进制，先拿出来再说

```
1011011110011010100101101000110010011010100100011001110110011010100011011001100
```

4、判断是二进制，进行转换，得出的结果如下，输入flag并不对

5、突然迷茫，想很长时间也没想到什么办法，后来突然想到是不是10转换，上Kali，输入下面两个命令引用tshark和perl。

命令1：tshark -r flag.pcap -Tfields -e udp.srcport #打印数据包UDP协议源端口

命令2：tshark -r flag.pcap -Tfields -e udp.srcport | while read port; do echo -n

$$done|tr0110|perl-lpe=pack"B*",$$

博客园地址：https://www.cnblogs.com/redHskb/
知乎地址：https://www.zhihu.com/people/yi-kuai-xiao-bing-gan-43-64/posts
欢迎关注评论，耶斯莫拉