

# 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](#)

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/liu914589417/article/details/120217742>

版权



[XCTF 专栏收录该内容](#)

24 篇文章 1 订阅

订阅专栏

## XCTF练习题—MISC—Hidden-Message

flag: Heisenberg

解题步骤:

1、观察题目, 下载附件

The screenshot shows the article's metadata on a dark background. It includes the title 'Hidden-Message', a 'Best Writeup' badge by '系统战队 • admin', a difficulty coefficient of 2.0 (two stars), the source 'su-ctf-quals-2014', a description '藏的什么信息?', and a 'None' scene. There is also a link to '附件1' (Attachment 1) and the CSDN @Hskb logo.

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
16	10.805847	192.168.56.1	192.168.56.101	UDP	65	3400 → 4400 Len=23

CSDN @Hskb

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

1011011100110101001011010001100100110101001000110011101100110101000110110011000

4、判断是二进制，进行转换，得出的结果如下，输入flag并不对

进制/类型	结果
ASCII码/十进制 (0 - 127)	117 110 100 101 102 105 110 101 100
十六进制 (0 - 7F)	75 6E 64 65 66 69 6E 65 64
八进制 (000 - 177)	165 156 144 145 146 151 156 145 144
二进制	01110101 01101110 01100100 01100101 01100110 01101001 01101110 01100101 01100100
字符串	undefined

这个在线转换计算器转换成十进制，十六进制，八进制，二进制和字符串的ASCII值。

CSDN @Hskb

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|tr01110|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