

攻防世界 Misc Hidden-Message

原创

==Microsoft== 于 2022-03-26 15:59:10 发布 159 收藏

分类专栏: [Misc](#) 文章标签: [ctf](#) [pwn](#) [php](#)

世上没有白读的书, 每一页都算数。

本文链接: <https://blog.csdn.net/MrTreebook/article/details/123757560>

版权



[Misc](#) 专栏收录该内容

50 篇文章 0 订阅

订阅专栏

攻防世界 Misc Hidden-Message

1.wireshark打开

1.wireshark打开

Hidden-Message.pcap

应用显示过滤器: <Ctrl-/>

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	10.895847	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
17	10.955907	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23
18	11.999860	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
19	12.067990	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
20	12.151881	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23
21	13.207824	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
22	13.279951	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23

> Frame 1: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)

> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: CadmusCo_9c:c3:4c (08:00:27:9c:c3:4c)

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101

> User Datagram Protocol, Src Port: 3401, Dst Port: 4400

> Data (23 bytes)

```
0000 08 00 27 9c c3 4c 0a 00 27 00 00 08 00 45 00  ..'.L.. '.....E.
0010 00 33 41 0d 00 00 40 11 47 f6 c0 a8 38 01 c0 a8  .3A...@. G...8...
0020 38 65 0d 49 11 30 00 1f 8d 2e 49 6e 20 63 6f 6e  8e.I.0.. ..In con
0030 74 72 61 73 74 20 74 6f 20 63 6c 61 73 73 69 63  trast to classic
0040 61  a
```

- 发现只有红框位置0101不断变换
- 感觉是隐写

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 10.895847	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
17 10.955907	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23
18 11.999860	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
19 12.067990	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
20 12.151881	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23
21 13.207824	192.168.56.1	192.168.56.101	UDP	65	3400->4400 Len=23
22 13.279951	192.168.56.1	192.168.56.101	UDP	65	3401->4400 Len=23

Name: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface eth0
 Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: CadmusCo 9c:c3:4c (08:00:27:9c:c3:4c)

CSDN @==Microsoft==

10110111100110101001011010001100100110101001000110011101100110101000110110011000

但是1打头

不像ascii码

1,0互换

然后转ascii

得到flag: Heisenberg