攻防世界 Misc高手进阶区 4分题 Hidden-Message

原创

思源湖的鱼 于 2020-12-04 10:55:26 发布 1939 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 misc 端口隐写 wireshark

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110630239

前言

继续ctf的旅程

攻防世界Misc高手进阶区的4分题

本篇是Hidden-Message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

下下来一个流量包

扔进wireshark

72	40.092118	192.168.56.1	192.168.56.101	UDP	65 3401 → 4400 Len=23
73	41.143891	192.168.56.1	192.168.56.101	UDP	65 3401 → 4400 Len=23
74	42.195775	192.168.56.1	192.168.56.101	UDP	65 3400 → 4400 Len=23
75	42.263750	192.168.56.1	192.168.56.101	UDP	65 3400 → 4400 Len=23
76	42.327784	192.168.56.1	192.168.56.101	UDP	65 3401 → 4400 Len=23
77	43.375790	192.168.56.1	192.168.56.101	UDP	65 3401 → 4400 Len=23
78	44.423964	192.168.56.1	192.168.56.101	UDP	65 3400 → 4400 Len=23
79	44.495936	192.168.56.1	192.168.56.101	UDP	65 3400 → 4400 Len=23
80	44.563916	192.168.56.1	192.168.56.101	UDP	65 3400 → 4400 Len=23

发现只有红框位置0101不断变换

感觉是隐写

提取出来

```
10110111100110101001011010001100100110101001000110011101100110101000110110011000
```

但是1打头
不像ascii码

转换进制
无果

猜测10互换

然后转ascii

得到flag：`Heisenberg`

结语

端口隐写有点意思