

CTF实验吧安全杂项之抓到你了

原创

等月亮的人 于 2018-07-18 21:42:52 发布 1018 收藏

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/weixin_38635069/article/details/81105863

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

首先下载链接后, 在wireshark中打开文件

可以看到文件。

由题目可知入侵者通过ping进行入侵, 因此我们在过滤器中过滤icmp包。发现只有5条。

No.	Time	Source	Destination	Protocol	Length	Info
0.	528.18.923067	172.26.16.115	192.168.191.2	ICMP	42	Echo (ping) request id=0x0001, seq=37/9472, ttl=255 (no response found!)
	593.21.603159	172.26.16.115	192.168.191.2	ICMP	58	Echo (ping) request id=0x0001, seq=38/9728, ttl=255 (no response found!)
	672.26.616007	172.26.16.115	192.168.191.2	ICMP	58	Echo (ping) request id=0x0001, seq=39/9984, ttl=255 (no response found!)
	767.31.596796	172.26.16.115	192.168.191.2	ICMP	58	Echo (ping) request id=0x0001, seq=40/10240, ttl=255 (no response found!)
	821.36.604731	172.26.16.115	192.168.191.2	ICMP	58	Echo (ping) request id=0x0001, seq=41/10496, ttl=255 (no response found!)

题目还是有16字节, 我们可以看到只有第一个数据包的大小与其他四个数据包大小不一样, 刚好少了16个字节。

点击第一个数据包与其他数据包对比, 发现是缺少了data部分, 即flag

```
✓ [No response seen]
✓ Data (16 bytes)
  Data: 2122232425262728292a2b2c2d2e2f30
  [Length: 16]
```