

BUUCTF: 百里挑一

原创

末初 于 2020-04-07 20:23:26 发布 2065 收藏 2

分类专栏: [CTF_MISC_Writeup](#)

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/mochu777777/article/details/105372624>

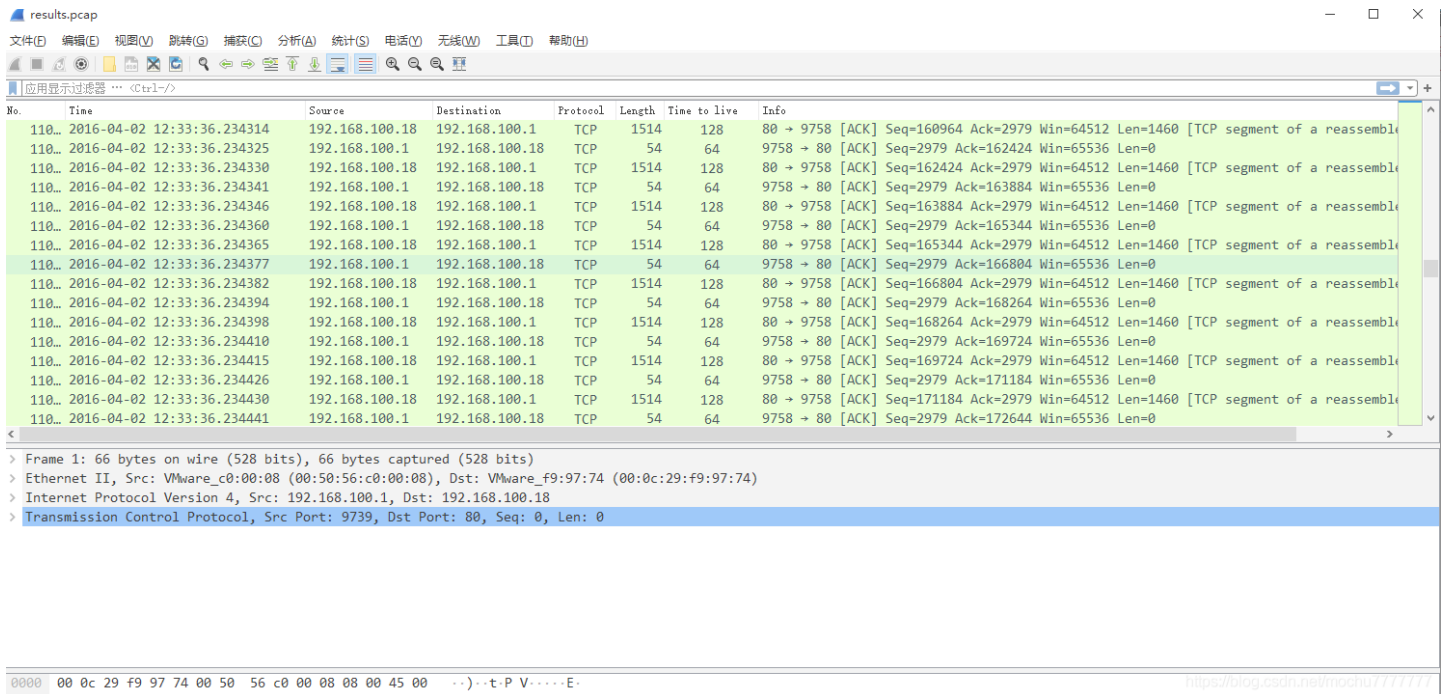
版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

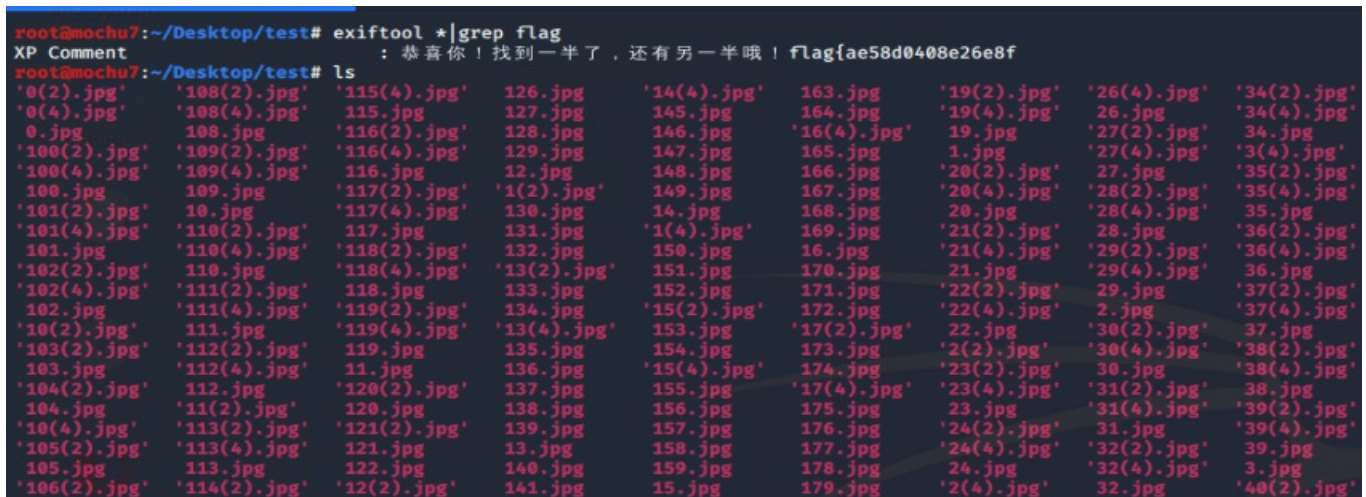
订阅专栏



全是在传图片时候的流量, 先把图片保存出来

文件 -> 导出对象 -> HTTP -> 保存到一个文件夹

然后使用kali下的 `exiftool` 找到了一半flag



```
100.jpg '114(4).jpg' 123.jpg 142.jpg 160.jpg 17.jpg 25(2).jpg 3(2).jpg '40(4).jpg'
'107(2).jpg' 114.jpg 124.jpg '14(2).jpg' 161.jpg '18(2).jpg' '25(4).jpg' '33(2).jpg' 40.jpg
'107(4).jpg' '11(4).jpg' '12(4).jpg' 143.jpg 162.jpg '18(4).jpg' 25.jpg '33(4).jpg' '41(2).jpg'
107.jpg '115(2).jpg' 125.jpg 144.jpg '16(2).jpg' 18.jpg '26(2).jpg' 33.jpg '41(4).jpg'
root@mochu7:~/Desktop/test# exiftool *|grep flag
XP Comment : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
root@mochu7:~/Desktop/test#
```

<https://blog.csdn.net/mochu7777777>

另外一半在tcp114追踪流当中

过滤器输入: `tcp.stream eq 114`

```
.....
.....
.....
.....
.....
.....
.....m`.U`O..~b0R.NJS
.N.... g.S.NJS.T..2.6.a.3.c.0.5.8.9.d.2.3.e.d.e.e.c.}.....http://
ns.adobe.com/xap/1.0/.<?xpacket begin='...'
id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://
www.w3.org/1999/02/22-rdf-syntax-ns#" /></x:xmpmeta>
```

<https://blog.csdn.net/mochu7777777>

`flag{ae58d0408e26e8f26a3c0589d23edeec}`