

xctf攻防世界 MISC高手进阶区 Cephalopod

原创

[18947943](#) 已于 2022-01-24 00:17:58 修改 10541 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

于 2022-01-24 00:17:29 首次发布

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/18947943/article/details/122659252>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

给的是一个pcap文件，果断塞入wireshark中，如图：

434c8c0ba659476caa9635b97f95600c.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(I) 帮助(H)

tcp.stream eq 1

分组字节流 宽窄 区分大小写 字符串 flag 查找 取消

No.	Time	Source	Destination	Protocol	Length	Info
75	17.252527	10.0.2.7	10.0.2.10	Ceph	315	Client Request
76	17.253073	10.0.2.10	10.0.2.7	TCP	66	6812 → 54924 [ACK] Seq=1704 Ack=1
77	17.261096	10.0.2.10	10.0.2.7	Ceph	769	ACK Client Reply
78	17.261114	10.0.2.7	10.0.2.10	TCP	66	54924 → 6812 [ACK] Seq=1625 Ack=2
99	17.277756	10.0.2.7	10.0.2.10	Ceph	354	ACK Client Capabilities
100	17.280977	10.0.2.10	10.0.2.7	Ceph	366	ACK Client Capabilities
102	17.319378	10.0.2.7	10.0.2.10	TCP	66	54924 → 6812 [ACK] Seq=1913 Ack=2
104	17.491383	10.0.2.7	10.0.2.10	Ceph	75	ACK

Caller User ID: 0
 Caller Group ID: 0
 Inode: 0
 Path, Inode: 0x0000000000000001, Rel: "flag.png"
 Encoding Version: 0x01
 Inode: 0x0000000000000001
 Relative component: flag.png
 Size: 8
 Data: flag.png

```

0060 00 00 00 00 00 00 00 08 29 10 00 00 00 00 00 00 ..... ).....
0070 00 00 00 00 24 08 a9 9e 03 00 00 00 00 00 00 00 ....$.
0080 05 00 00 00 02 00 00 00 00 00 01 00 01 13 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 c1 80 00 00 80 81 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 01 01 00 00 00 00 00 00 00 08 00 00 00 66 6c 61 .....fla
00e0 67 2e 70 6e 67 01 00 00 00 00 00 00 00 00 00 00 .....g.png
00f0 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 .....
0100 00 00 55 00 00 00 55 03 00 00 02 00 00 00 02 00 ..U...U.
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 54 2c .....T,
0120 9d 59 55 55 87 33 3c 77 9f 0c 00 00 00 00 00 00 ..YUU-3kw
0130 00 00 6d 23 b1 6b 9e a4 9e 7c 05 .....m#k-|-
  
```

字节 221-228: Data (ceph.string.data) 分组: 339 · 已显示: 80 (20.6%)

搜索到关键词

2. 问题分析

可以看到有一张png图片，那么判断流量包中可以提取该文件，尝试foremost并无法分离。

查看wp后，发现需要安装tcpxtract

```
sudo apt-get install tcpxtract
```

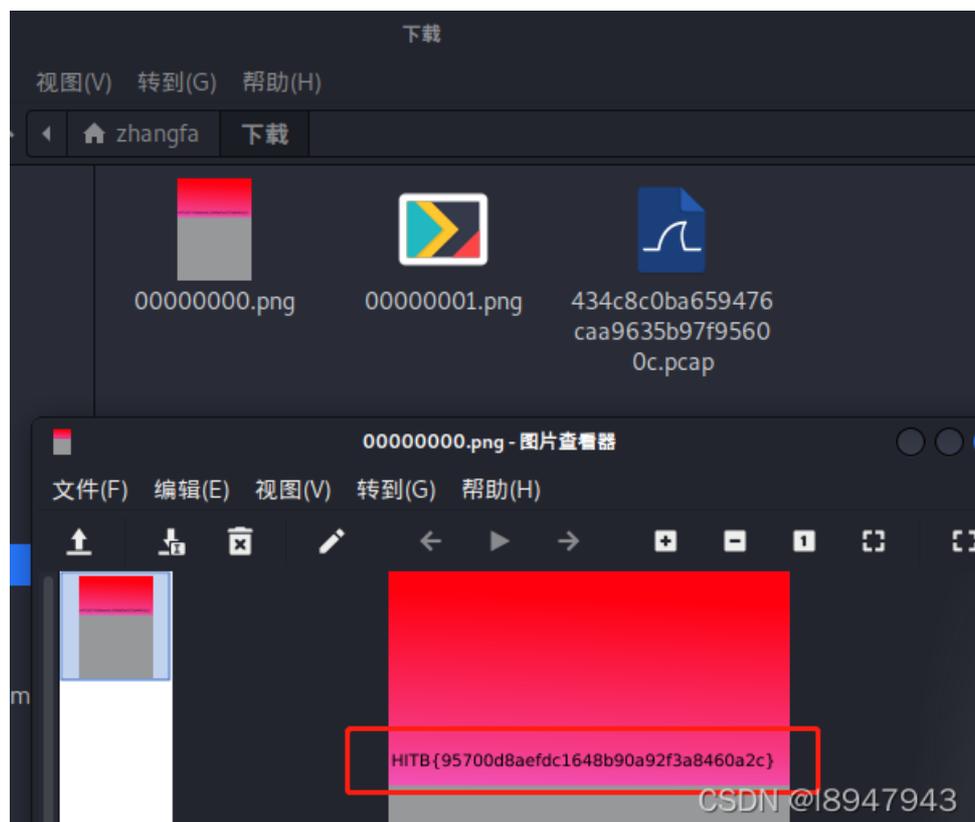
然后提取文件数据：

```
tcpxtract -f 434c8c0ba659476caa9635b97f95600c.pcap
```

```

(zhangfa@kali)-[~/下载]
└─$ tcpxtract -f 434c8c0ba659476caa9635b97f95600c.pcap
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], exporting
to 00000000.png
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], exporting
to 00000001.png
  
```

结果如图：



最终答案为： `HITB{95700d8aefdc1648b90a92f3a8460a2c}`