

# xctf攻防世界 MISC高手进阶区 simple\_transfer

原创

18947943 于 2022-01-12 19:16:57 发布 150 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc foremost](#)

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/122460189>

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

内容是个pcap文件, 果断用wireshark打开

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_f3:75:4b	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.5
2	0.000264	PcsCompu_1f:c2:a8	PcsCompu_f3:75:4b	ARP	60	10.0.2.4 is at 08:00:27:1f:c2:a8
3	0.193092	10.0.2.5	10.0.2.4	TCP	58	62549 → 143 [SYN] Seq=0 Win=1024
4	0.193196	10.0.2.5	10.0.2.4	TCP	58	62549 → 53 [SYN] Seq=0 Win=1024
5	0.193345	10.0.2.5	10.0.2.4	TCP	58	62549 → 25 [SYN] Seq=0 Win=1024
6	0.193446	10.0.2.5	10.0.2.4	TCP	58	62549 → 1025 [SYN] Seq=0 Win=1024
7	0.193558	10.0.2.4	10.0.2.5	TCP	60	143 → 62549 [RST, ACK] Seq=1 Ack=
8	0.193569	10.0.2.4	10.0.2.5	TCP	60	53 → 62549 [RST, ACK] Seq=1 Ack=

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
> Ethernet II, Src: PcsCompu\_f3:75:4b (08:00:27:f3:75:4b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 08 00 27 f3 75 4b 08 06 00 01 ..... :uK...
0010 08 00 06 04 00 01 08 00 27 f3 75 4b 0a 00 02 05 ..... :uK...
0020 00 00 00 00 00 00 0a 00 02 04
```

## 2. 问题分析

使用wireshark找到flag

题目提示, [文件里有flag, 找到它](#)。那么说明数据流中包含flag, 我们使用wireshark中的分组字节流查找flag关键字, 如图:

f9809647382a42e5bfb64d7d447b4099.pcap

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

应用显示过滤器: <Ctrl-/>

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
4644	62.620464	10.0.2.4	10.0.2.5	TCP	66	2049 → 854 [ACK] Seq=9585 Ack=56
4645	62.620484	10.0.2.5	10.0.2.4	DLEP	65226	Message: Unknown (38506)
4646	62.620506	10.0.2.4	10.0.2.5	TCP	66	2049 → 854 [ACK] Seq=9585 Ack=56
4647	62.620612	10.0.2.4	10.0.2.5	TCP	66	2049 → 854 [ACK] Seq=9585 Ack=57
4648	62.620626	10.0.2.5	10.0.2.4	DLEP	62070	Message: Unknown (30838)
4649	62.620645	10.0.2.4	10.0.2.5	TCP	66	2049 → 854 [ACK] Seq=9585 Ack=57
4650	62.620654	10.0.2.5	10.0.2.4	DLEP	31514	Message: Unknown (21731)

> [SEQ/ACK analysis]  
TCP payload (31448 bytes)

Dynamic Link Exchange Protocol, Message: Unknown (21731)  
Message Type: Unknown (21731)  
Message Length (bytes): 1779  
Unknown Data Item  
Type: Unknown (57962)  
Length (bytes): 56458  
Value

```

75d0 73 29 0a 20 20 20 2f 46 6c 61 67 73 20 33 32 0a s) /F lags 32
75e0 20 20 20 2f 46 6f 6e 74 42 42 6f 78 20 5b 20 2d /Font BBox [ -
75f0 31 30 32 30 20 2d 34 36 32 20 31 37 39 33 20 31 1020 -46 2 1793 1
7600 32 33 32 20 5d 0a 20 20 20 2f 49 74 61 6c 69 63 232 ] /Italic
7610 41 6e 67 6c 65 20 30 0a 20 20 20 2f 41 73 63 65 Angle 0 /Asce
7620 6e 74 20 39 32 38 0a 20 20 20 2f 44 65 73 63 65 nt 928 /Desce
7630 6e 74 20 2d 32 33 35 0a 20 20 20 2f 43 61 70 48 nt -235 /CapH
7640 65 69 67 68 74 20 31 32 33 32 0a 20 20 20 2f 53 eight 12 32 /S
7650 74 65 6d 56 20 38 30 0a 20 20 20 2f 53 74 65 6d temV 80 /Stem
7660 48 20 38 30 0a 20 20 20 2f 46 6f 6e 74 46 69 6c H 80 /FontFil
  
```

Value (dlep.dataitem.value), 31,440 byte(s) | 分组: 4678 · 已显示: 4678 (100.0%) 配置: Default

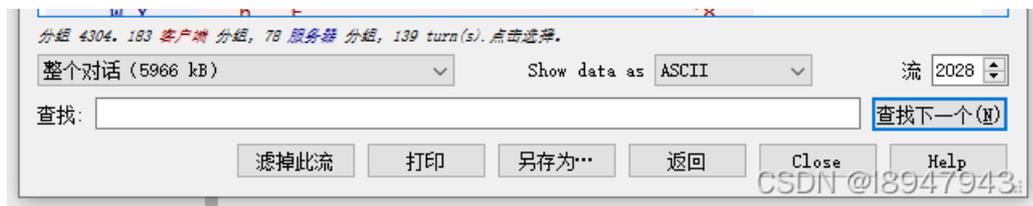
### 追踪流

上下滑动，翻一翻发现了端倪，如图：

Wireshark · 追踪 TCP 流 (tcp.stream eq 2028) · f9809647382a42e5bfb64d7d4...

```

.....|.E.....$. '6...
ctf-client.....#.....
\u6...B...Q.<.uY...
.....|.E.....
.....:.....Y.T.3.....
\u6...B...Q.<.uY...#.....
0.....0.....Y.T.....Y.T.3.....Y.T.
3.....#.....}..E.....$. '7...
ctf-client.....#.....
\u6...B...Q.<.uY...
.....:.....}..E.....
.....:.....Y.T.3.....
\u6...B...Q.<.uY...#.....
0.....0.....Y.T.....Y.T.3.....Y.T.
3.....#.....~..E.....$. '7...
ctf-client.....#.....
\u6...B...Q.<.uY...
.....:.....~..E.....
.....:.....Y.T.3.....
\u6...B...Q.<.uY...#.....
0.....0.....Y.T.....Y.T.3.....Y.T.
3.....#.....E.....$. '8...
ctf-client.....#.....
\u6...B...Q.<.uY... file.pdf...
.....:.....}..E.....
4...E.....E.....
.....:.....'8...
ctf-client.....#Y.T.5.....#Linux
NFSv4.0 10.0.2.5/10.0.2.4 tcp.@.....tcp.....
10.0.2.5.141.147.....<..E.....#...wT.Y
  
```



说明文件中有隐藏pdf, 因此自然想到了文件分离

### foremost文件分离

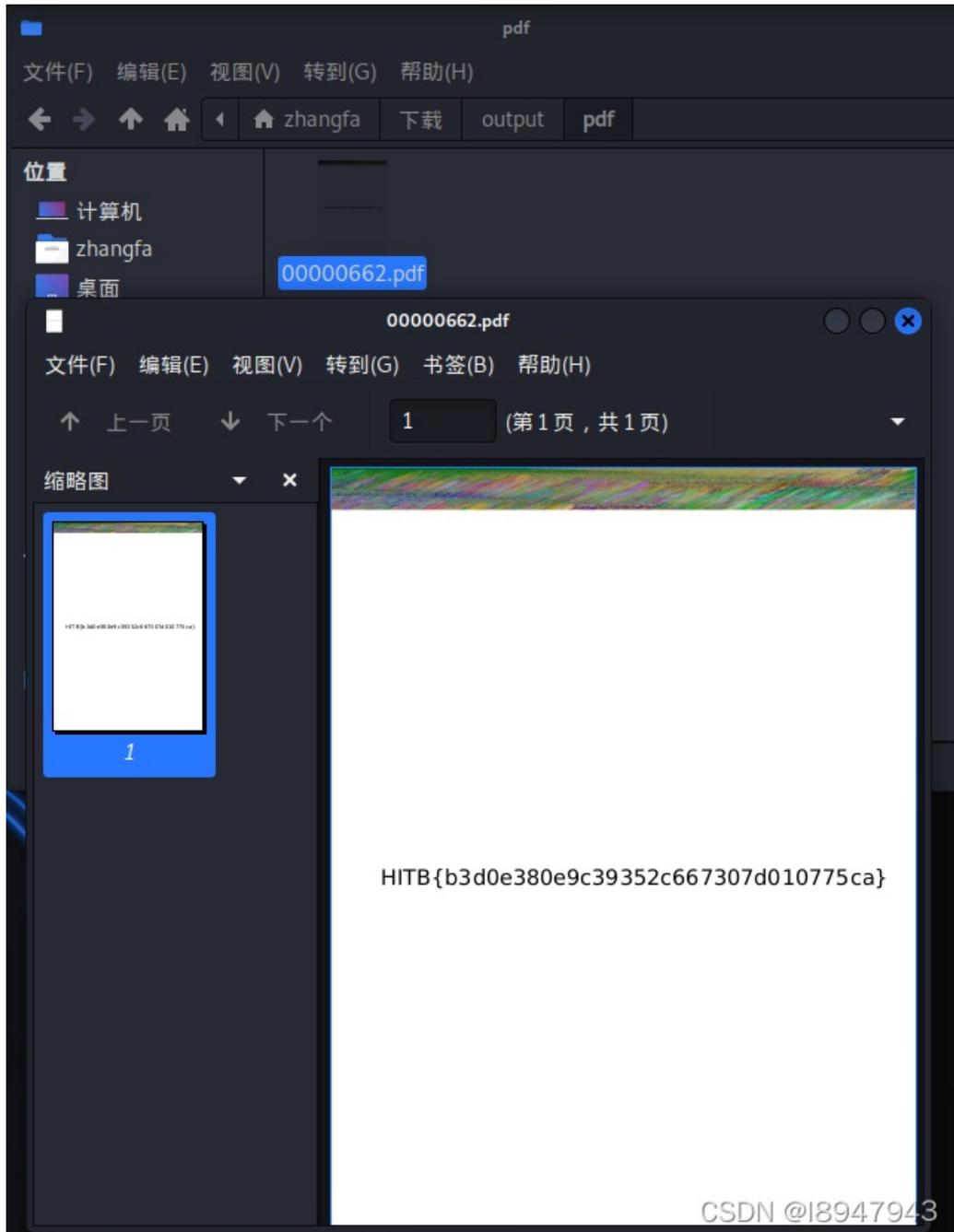
先安装foremost

```
$ apt-get install foremost
```

我们使用foremost去分离文件, 命令:

```
$ foremost f9809647382a42e5bfb64d7d447b4099.pcap
```

得到的结果如图:



最终flag为: HITB{b3d0e380e9c39352c667307d010775ca}

#### 4. kali工具之binwalk

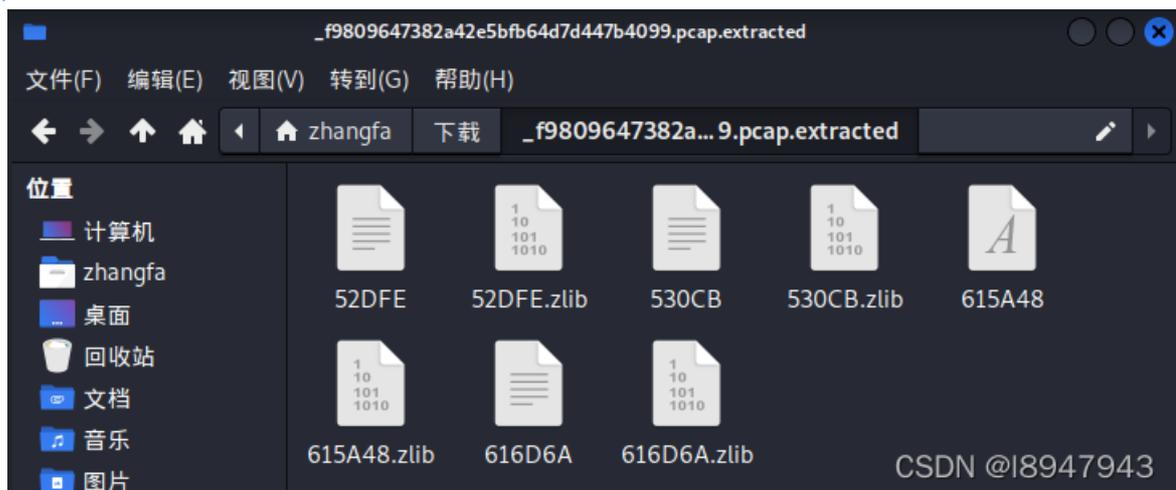
使用binwalk，但是不知道为什么只能检测出有pdf文件包含，分离不出来文件就很迷，如图：

```
(zhangfa@kali) - [~/下载]
$ binwalk -e f9809647382a42e5bfb64d7d447b4099.pcap
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Libpcap capture file, little-endian, version 2.4, Ethernet, snaplen: 262144
339380	0x52DB4	PDF document, version: "1.5"
339454	0x52DFE	Zlib compressed data, default compression
340171	0x530CB	Zlib compressed data, default compression
6380104	0x615A48	Zlib compressed data, default compression
6385002	0x616D6A	Zlib compressed data, default compression

CSDN @I8947943

结果如图：



一堆莫名其妙的zlib文件和无后缀的文件，估计binwalk使用不对，蹲个好心人拯救一下我~~~

### 3. 总结

今天题不难，感觉有点累，刷不动了，附个美图欣赏欣赏吧！

