

攻防世界-simple_transfer

原创

[peng_xingang](#) 于 2021-11-29 16:12:26 发布 2474 收藏

分类专栏: [攻防世界 杂项](#) 文章标签: [安全 经验分享](#)

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/peng_xingang/article/details/121611425

版权



[攻防世界](#) 同时被 2 个专栏收录

12 篇文章 0 订阅

订阅专栏



[杂项](#)

9 篇文章 0 订阅

订阅专栏

打开题目, 下载附件, 发现是一个pcap文件。

simple_transfer

👍 25 最佳Writeup由 [B301](#) • [dals](#) 提供

难度系数: ★ 1.0

题目来源: [XCTF 3rd-HITB CTF-2017](#)

题目描述: 文件里有flag, 找到它。

题目场景: 暂无

题目附件: [附件1](#)

题目已答对

CSDN @peng_xingang

话不多说, 放到wireshark里面追踪流量。

搜索flag, 发现前面很多很多的TCP协议, 但是追踪进去没啥东西。

这里选择统计->协议分级, 看哪些协议的数据占比多。



应用显示

Wireshark · 协议分级统计 · f9809647382a42e5bfb64d7d447b4099.pcap

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	结束 分组	结束 字节	结束 位/秒
Frame	100.0	4678	100.0	6316192	632k	0	0	0
Ethernet	100.0	4678	1.0	65492	6,563	0	0	0
Internet Protocol Version 4	99.9	4672	1.5	93440	9,364	0	0	0
User Datagram Protocol	0.1	5	0.0	40	4	0	0	0
Remote Procedure Call	0.1	4	0.0	168	16	0	0	0
Portmap	0.1	4	0.0	40	4	4	40	4
Data	0.0	1	0.0	300	30	1	300	30
Transmission Control Protocol	99.7	4662	97.3	6143596	615k	4363	165096	16k
Remote Procedure Call	0.7	34	0.0	1996	200	13	404	40
Yellow Pages Service	0.0	1	0.0	0	0	1	0	0
RSTAT	0.0	2	0.0	0	0	2	0	0
Portmap	0.1	7	0.0	564	56	7	564	56
Network File System CB	0.1	4	0.0	0	0	4	0	0
Network File System	0.0	2	0.0	0	0	2	0	0
Mount Service	0.1	5	0.0	48	4	5	48	4
Dynamic Link Exchange Protocol	5.6	261	94.5	5966792	597k	261	5966792	597k
Data	0.1	4	0.0	144	14	4	144	14
Internet Control Message Protocol	0.1	5	0.0	908	90	4	572	57
Data	0.0	1	0.0	300	30	1	300	30
Address Resolution Protocol	0.1	6	0.0	222	22	6	222	22

无显示过滤器。

Help

复制 Close

CSDN@peng_xingang

找到一个占比94%的协议DLEP，那么就选中这个协议，右键作为过滤器应用直接开始搜索。

Mount Service	0.1	5
Dynamic Link Exchange Protocol	5.6	261
Data	0.1	4
Internet Control Message Protocol	0.1	5
Data	0.0	1
Address Resolution Protocol	0.1	6

作为过滤器应用

Prepare as Filter

查找

着色

复制为 CSV

复制为 YAML

CSDN@peng_xingang

搜索出来，但是提示unknown message!

分组详情 宽窄 区分大小写 字符串 flag

No.	Time	Source	Destination	Protocol	Length	Info
4333	62.598460	10.0.2.5	10.0.2.4	DLEP	21786	Message: Unknown (19010)
4335	62.598738	10.0.2.5	10.0.2.4	DLEP	1514	Message: Unknown (24244)
4336	62.598754	10.0.2.5	10.0.2.4	DLEP	5858	Message: Unknown (26943)
4337	62.598759	10.0.2.5	10.0.2.4	DLEP	20338	Message: Unknown (35529)
4338	62.598831	10.0.2.5	10.0.2.4	DLEP	37714	Message: Unknown (42723)
4340	62.599039	10.0.2.5	10.0.2.4	DLEP	21786	Message: Unknown (31465)
4342	62.599085	10.0.2.5	10.0.2.4	DLEP	20338	Message: Unknown (35368)

- [Timestamps]
 - [Time since first frame in this TCP stream: 11.180565000 seconds]
 - [Time since previous frame in this TCP stream: 0.000016000 seconds]
 - TCP payload (21720 bytes)
- Dynamic Link Exchange Protocol, Message: Unknown (31465)
 - Message Type: Unknown (31465)
 - Message Length (bytes): 9551
 - [Expert Info (Warning/Protocol): Signal length does not match reported length remaining]
 - [Signal length does not match reported length remaining]
 - [Severity level: Warning]
 - [Group: Protocol]
 - Unknown Data Item
 - Type: Unknown (23714)
 - Length (bytes): 9121
 - Value
 - Unknown Data Item
 - Type: Unknown (25539)
 - Length (bytes): 14022
 - Value

```

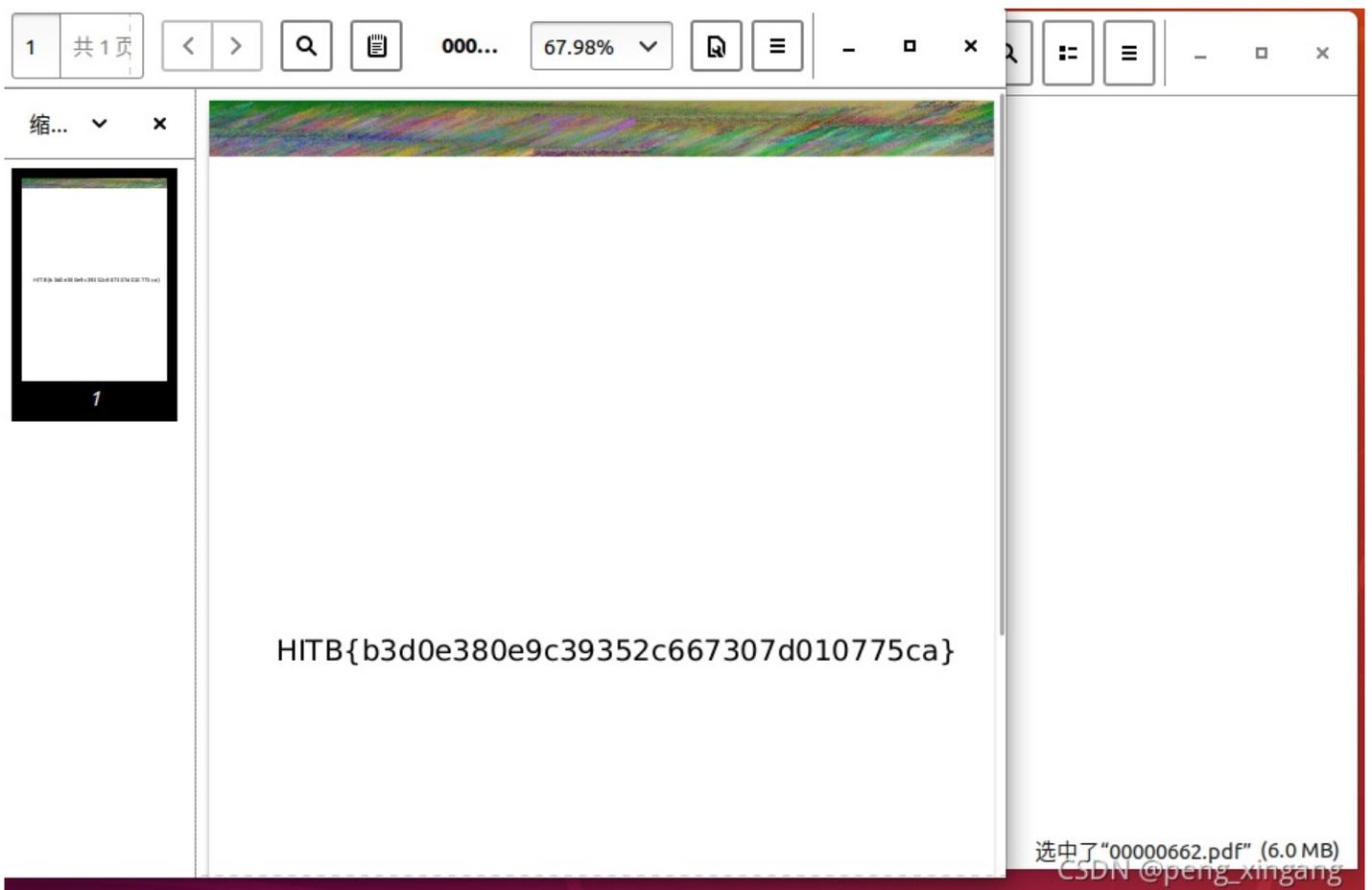
0040  4a 88 7a e9 25 4f 5c a2 23 a1 54 c7 25 06 4a c7  J·z·%0\· #·T·%·J·
0050  a5 3c 12 0a 42 e8 65 48 42 09 86 fe e8 aa c2 4e  <··B·eH B······N
  
```

CSDN @peng_xingang

没有啥信息没关系，这么大的unknown message摆在面前，尝试一下分解。

```
foremost -t all -i f9809647382a42e5bfb64d7d447b4099.pcap
```

发现输出一个pdf，打开就是flag。



1 共1页 67.98%

HITB{b3d0e380e9c39352c667307d010775ca}

选中了“00000662.pdf” (6.0 MB)
CSDN @peng_xingang

HITB{b3d0e380e9c39352c667307d010775ca}

尝试提交，成功！