攻防世界-杂项-simple_transfer

原创

土豆会发芽 于 2021-01-07 18:36:23 发布 560 收藏

分类专栏： 攻防世界之杂项 文章标签： 网络 linux

本文链接：https://blog.csdn.net/weixin_47717433/article/details/112328507

攻防世界之杂项 专栏收录该内容

12 篇文章 1 订阅

订阅专栏

攻防世界-杂项-simple_transfer

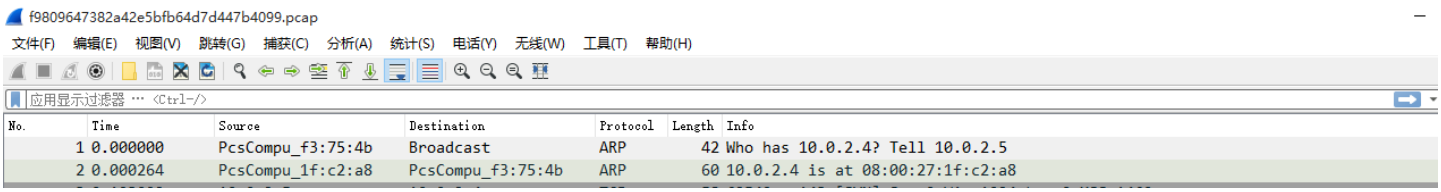
攻防世界杂项高手进阶区：simple_transfer。此题工具包括：wireshark,binwalk(linux操作系统)

题目

这道题是一个流量分析的

题

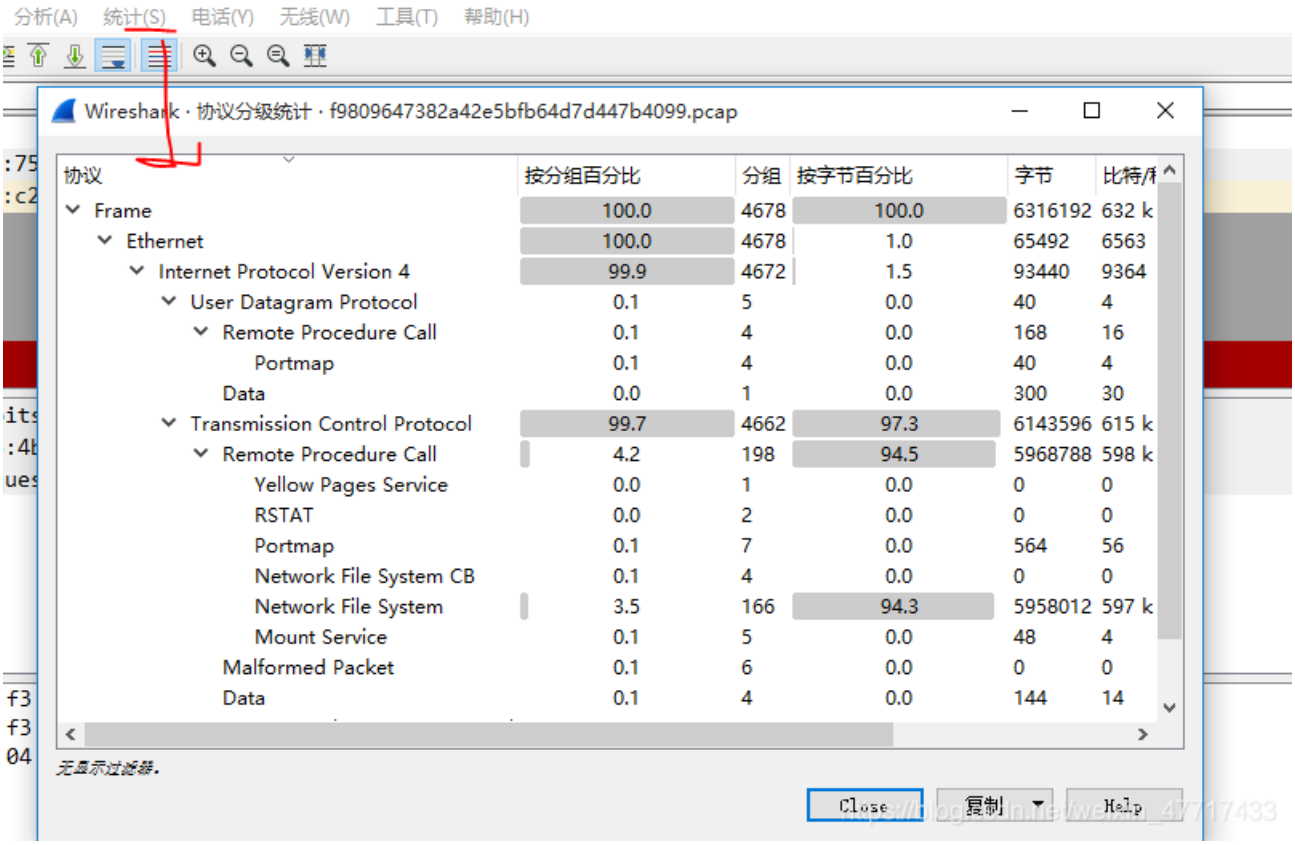
1.wiresahrk打开附件,此处附上wiresahrk流量分析使用方法wireshark过滤。打开文件如下图所示



3	0.193092	10.0.2.5	10.0.2.4	TCP	58 62549 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.193196	10.0.2.5	10.0.2.4	TCP	58 62549 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.193345	10.0.2.5	10.0.2.4	TCP	58 62549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.193446	10.0.2.5	10.0.2.4	TCP	58 62549 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.193558	10.0.2.4	10.0.2.5	TCP	60 143 → 62549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
> 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)
```


打开以后有点乱，于是进行协议分级。（*协议分级的作用是统计通信流量中不同协议占比的百分比，看谁占比更多*）



协议分级以后发现NFS协议占比94.3%，于是对NFS协议过滤。（*NFS是NetworkFileSystem的简写,即网络文件系统,网络文件系统是FreeBSD支持的文件系统中的一种，也被称为NFS.NFS允许一个系统在网络上与它人共享目录和文件。通过使用NFS，用户和程序可以像访问本地文件一样访问远端系统上的文件。*）

nfs

No.	Time	Source	Destination	Protocol	Length	Info
4147	17.146921	10.0.2.5	10.0.2.4	NFS	110	V106919319 proc-0 Call (Reply In 4158)
4151	17.147012	10.0.2.5	10.0.2.4	NFS	110	V6436758 proc-0 Call (Reply In 4162)
4234	51.418805	10.0.2.5	10.0.2.4	NFS	110	V4 NULL Call (Reply In 4236)
4236	51.419087	10.0.2.4	10.0.2.5	NFS	94	V4 NULL Reply (Call In 4234)
4238	51.419289	10.0.2.5	10.0.2.4	NFS	242	V4 Call (Reply In 4239) SETCLIENTID
4239	51.419480	10.0.2.4	10.0.2.5	NFS	130	V4 Reply (Call In 4238) SETCLIENTID
4240	51.419514	10.0.2.5	10.0.2.4	NFS	174	V4 Call (Reply In 4241) SETCLIENTID_CONFIRM

对协议包进行查看，发现一个PDF文件

nfs

No.	Time	Source	Destination	Protocol	Length	Info
4300	61.845705	10.0.2.5	10.0.2.4	NFS	210	V4 Call (Reply In 4301) GETATTR FH: 0x0163bd75
4301	61.845888	10.0.2.4	10.0.2.5	NFS	266	V4 Reply (Call In 4300) GETATTR
4303	62.583091	10.0.2.5	10.0.2.4	NFS	230	V4 Call (Reply In 4304) LOOKUP DH: 0x0163bd75/file.pdf
4304	62.583488	10.0.2.4	10.0.2.5	NFS	122	V4 Reply (Call In 4303) LOOKUP Status: NFS4ERR_NOENT
4306	62.583621	10.0.2.5	10.0.2.4	NFS	242	V4 Call (Reply In 4307) SETCLIENTID
4307	62.583814	10.0.2.4	10.0.2.5	NFS	130	V4 Reply (Call In 4306) SETCLIENTID

```
4308 62.583851    10.0.2.5        10.0.2.4        NFS     174 V4 Call (Reply In 4314) SETCLIENTID_CONFIRM
```

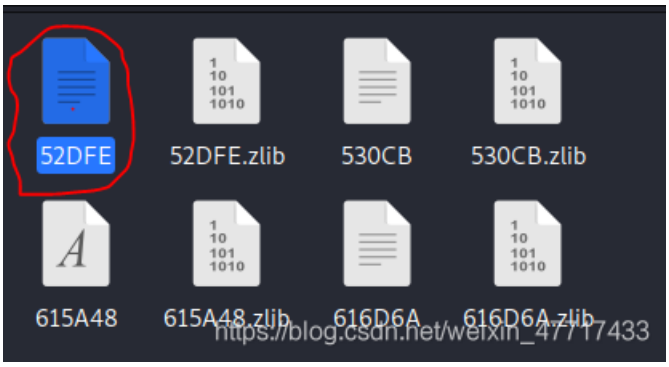
因为文件被包含在协议中，所以利用binwalk工具进行分离

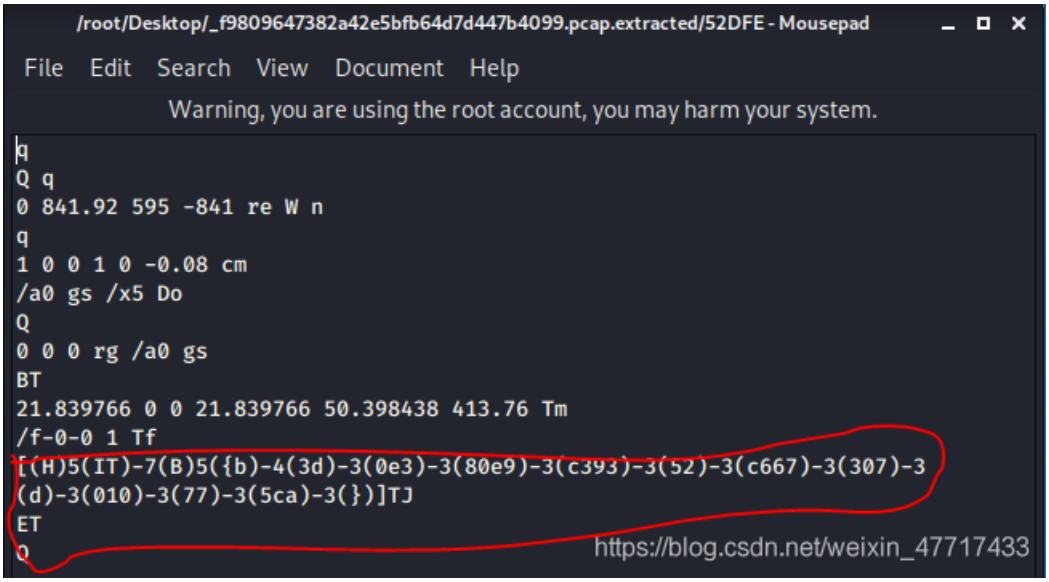
2.binwalk分离文件(linux操作系统下操作)

```
root@kali:~/Desktop# 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
```

由上图可知，分离出一个PDF文件，版本为1.5。接下来在分离出的文件查看PDF





尝试输入此处的flag:HITB{b3d0e380e9c39352c667307d010775ca}

最后答题成功。