攻防世界_MISC进阶区_simple_transfer

原创

RuoLi_s 于 2020-11-11 20:40:21 发布 1910 收藏 1

分类专栏： CTF 文章标签： 信息安全 wireshark linux unctf 安全

本文链接：https://blog.csdn.net/RuoLi_s/article/details/109630540

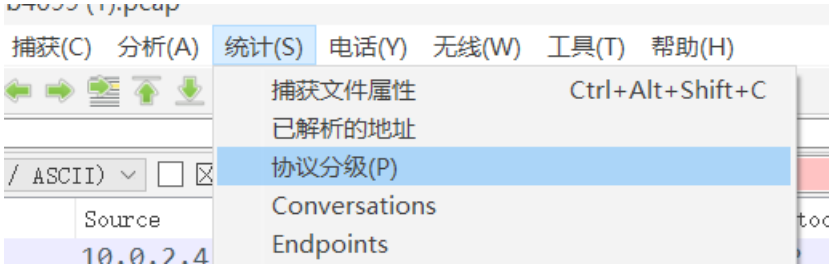
又做到了一个难缠的题（对于饶了很多弯的我来说、、、呜呜呜）

哎，话不多说了，直接看题吧

我们下载附件，看到是一个抓包分析的题。

第一步当然是直接打开，搜索flag，发现无果，

果断到统计–>协议分级查看：



可以看到，协议的字节百分比占用基本全在NFS协议上，直接过滤NFS

Wireshark · 协议分级统计 · f9809647382a42e5bfb64d7d447b4099 (1).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
Frame	100.0	4678	100.0	6316192	632 k	0
Ethernet	100.0	4678	1.0	65492	6563	0
Internet Protocol Version 4	99.9	4672	1.5	93440	9364	0
User Datagram Protocol	0.1	5	0.0	40	4	0
Transmission Control Protocol	99.7	4662	97.3	6143596	615 k	4458
Remote Procedure Call	4.2	198	94.5	5968788	598 k	13
Yellow Pages Service	0.0	1	0.0	0	0	1
RSTAT	0.0	2	0.0	0	0	2
Portmap	0.1	7	0.0	564	56	7
Network File System CB	0.1	4	0.0	0	0	4
Network File System	3.5	166	94.3	5958012	597 k	162
Mount Service	0.1	5	0.0	48	4	5
Malformed Packet	0.1	6	0.0	0	0	6
Data	0.1	4	0.0	144	14	4
Internet Control Message Protocol	0.1	5	0.0	908	90	5
Address Resolution Protocol	0.1	6	0.0	222	22	6

观察报文，发现有个pdf文件

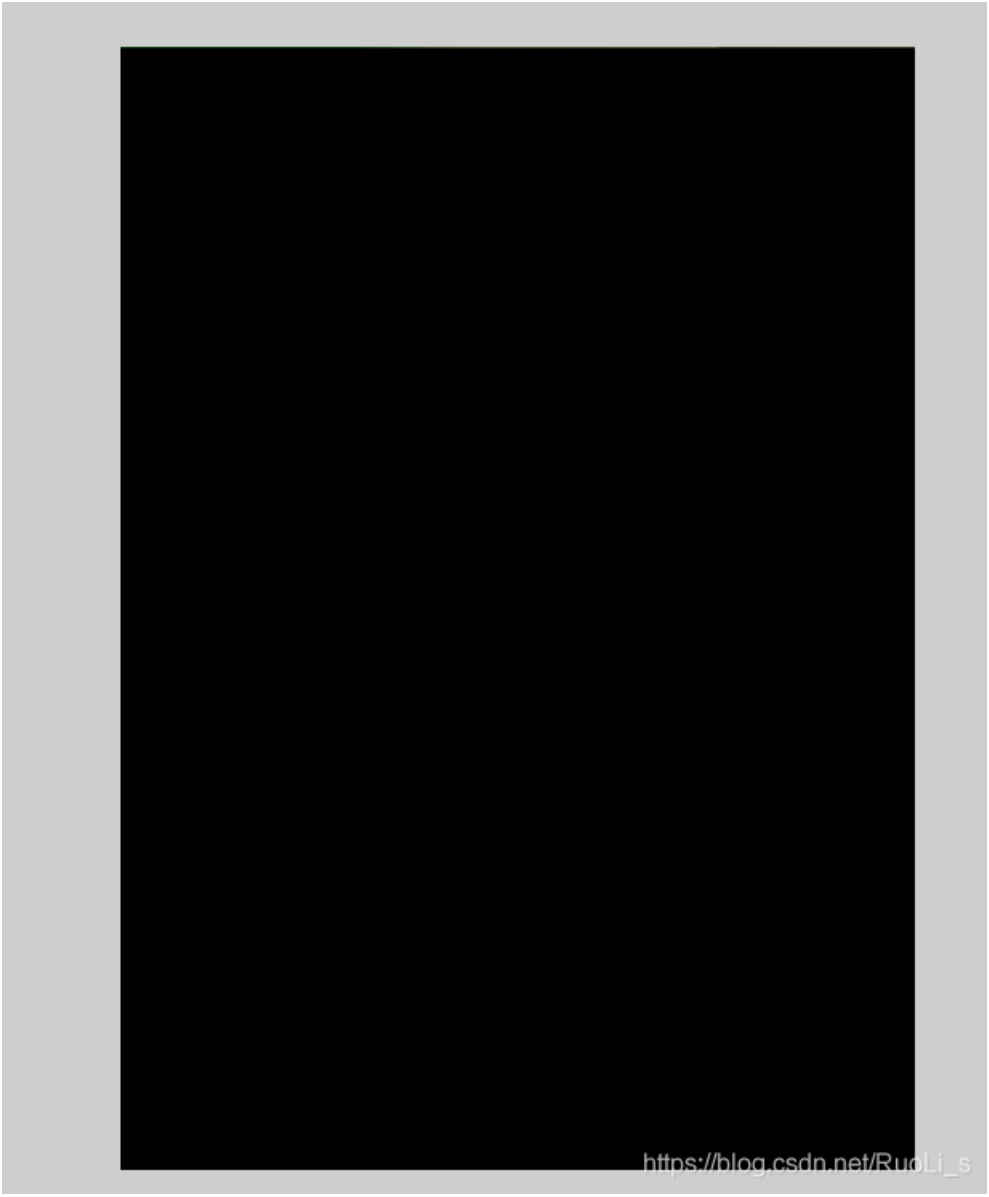
```
266 V4 Reply (Call In 4294) GETATTR
210 V4 Call (Reply In 4298) GETATTR FH: 0x0163bd75
266 V4 Reply (Call In 4297) GETATTR
210 V4 Call (Reply In 4301) GETATTR FH: 0x0163bd75
266 V4 Reply (Call In 4300) GETATTR
230 V4 Call (Reply In 4304) LOOKUP DH: 0x0163bd75/file.pdf
122 V4 Reply (Call In 4303) LOOKUP Status: NFS4ERR_NOENT
242 V4 Call (Reply In 4307) SETCLIENTID
130 V4 Reply (Call In 4306) SETCLIENTID
```

直接foremost分解；

```
root@kali:~/桌面# ls
a.pcap
root@kali:~/桌面# foremost a.pcap -o a
Processing: a.pcap
|*|
root@kali:~/桌面# ls
a  a.pcap
root@kali:~/桌面#
```

这里是因为文件名太长，我提前给重命名了

打开pdf文件，里面什么都没有，



右键单击，发现又复制图片，所以知道应该是有图片给遮挡住了。
直接CTRL + A 全选，新建一个txt文件，CTRL + V 粘贴，
得到flag。

HITB{b3d0e380e9c39352c667307d010775ca}