攻防世界 MISC

原创

dalssss 于 2019-10-04 01:51:15 发布 459 收藏

分类专栏： MISC 文章标签： MISC 攻防世界

本文链接：https://blog.csdn.net/qq_42201260/article/details/102034300

功夫再高也怕菜刀

下载完附件，发现是简单的流量分析。。

```
->|./    2017-12-08 11:42:11      0        0777
../      2017-12-08 11:39:10      4096     0777
1.php    2017-12-08 11:33:16      33       0666
6666.jpg         2017-12-08 11:42:11      102226   0666
flag.txt         2017-12-08 11:35:29      17       0666
hello.zip        2017-12-08 09:32:36      224      0666
|<-
```

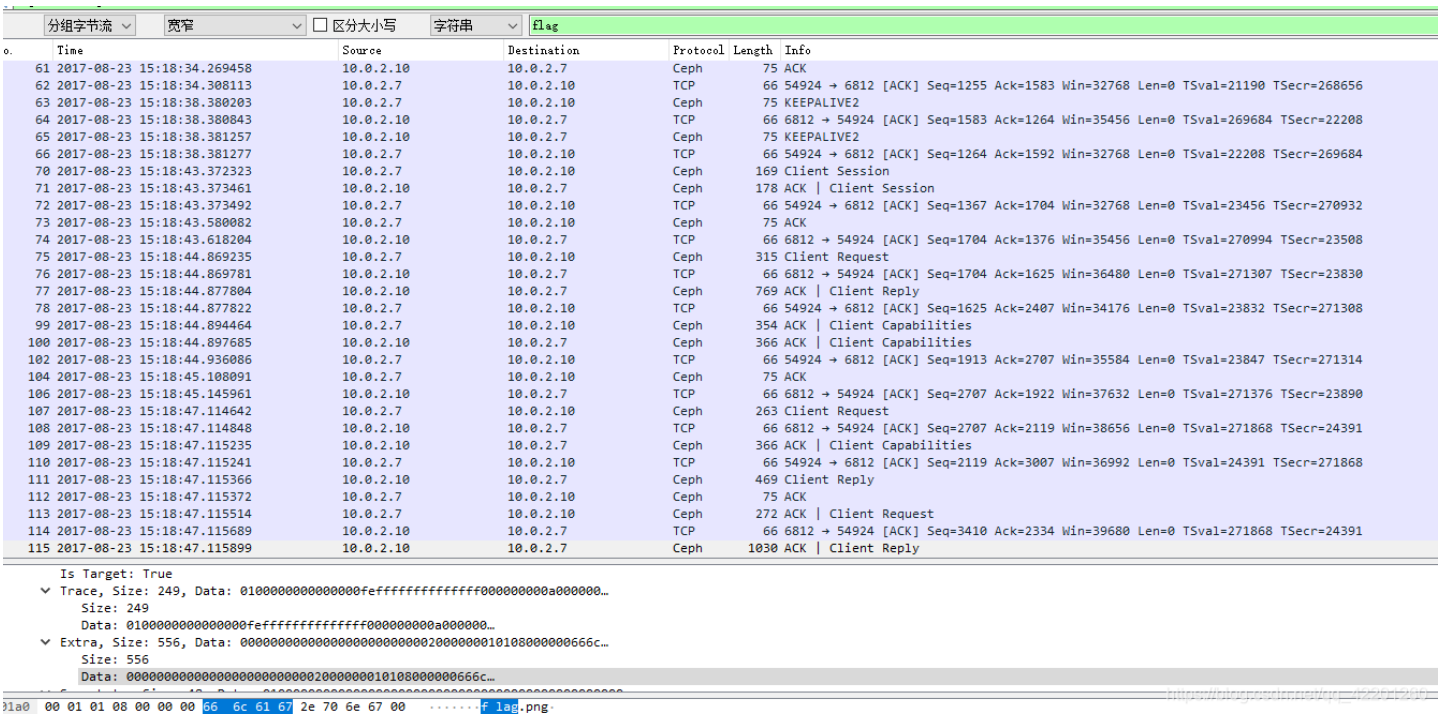

发现里面有个几个文件，去kali下用foremost把它分离下。。

```
root@kali:/file# foremost 19ae303d520c4790b0401569b354e6a2.pcapng
Processing: 19ae303d520c4790b0401569b354e6a2.pcapng
|foundat=flag.txtC????cS???J??Ea?v?
                                  ??&e$K??2%?$??,?=?J??1p??p46PK?
*|
root@kali:/file# ls
12.png  19ae303d520c4790b0401569b354e6a2.pcapng  output
```

里面的压缩把进去是要密码的，找到上传的数据包，把jpg文件格式开头（FFD8）和结尾（FFD9）的图片数据copy出来，导入到010ed中，另存为jpg格式就出现压缩包的密码了。

Cephalopod

是到流量题。。放到wireshark里看看，发现了图片名为flag.png的图片



丢到kali里用binwalk看看能不能分离，发现不行，在接着用foremost试试，还是不行，最后去看看下wp，发现是用这款“tcpxtract”。。

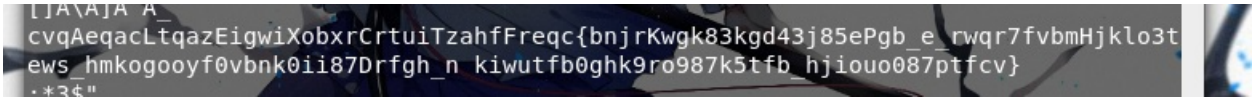
```
tcpxtract -f 40150e85ac1b4952f1c35c2d9103d8a40c7bee55.pcap Found file of type "png" in session
```

分离出两张图片，还是不能查看，但是放入winhex发现，它的头部少了89
加上后保存，其中一张可以打开，出现了flag

hit-the-core

下载附件完发现是个.core文件(这他喵的是什么…)
百度了一下，发现是一个linux系统下程序崩溃生成的文件，里面有内存映射和存储调试信息的文件，主要是用来调试的。。

我丢到kali strings 看了下，有点小收获，找到了一个疑似flag，但应该不是的字符串。。仔细一看发现“A”后面的大写字母都有规律的样子，我用脚本跑了一下，就出flag了



```
string = "cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii8
7Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}"
flag = ""
for i in range(3, len(string),5):
 flag += string[i]
print(flag)
```