攻防世界MISC部分

原创

giunwr 于 2019-07-06 12:19:09 发布 6370 收藏 5

分类专栏： misc 文章标签： misc

本文链接：https://blog.csdn.net/qq_44105778/article/details/94842746

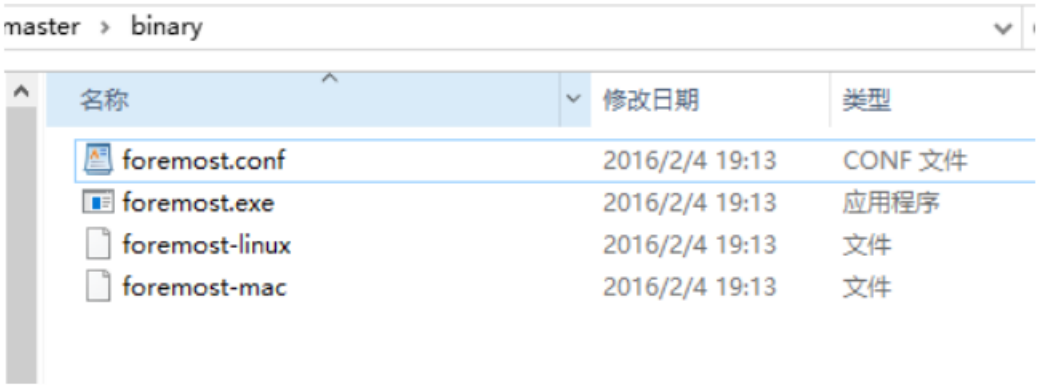
一、功夫再高也怕菜刀

下载附件，用foremost进行pcapng文件的分离，得到一个压缩包，打开压缩包，得到一份加密的flag文件。

foremost的下载地址https://github.com/raddyfiy/foremost （windows系统可用）

简单的使用介绍

用这个原代码你自己就可以编译出exe，如果懒得编译的话里面的binary里就有编译好的，直接用这个就好



可以把前两个文件复制到一个安全的文件夹，方便以后使用，不要误删就好。

分离文件的步骤:

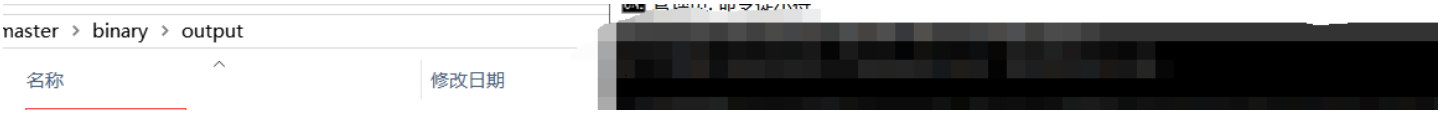
1.将所要解密的文件放入foremost所在的目录;

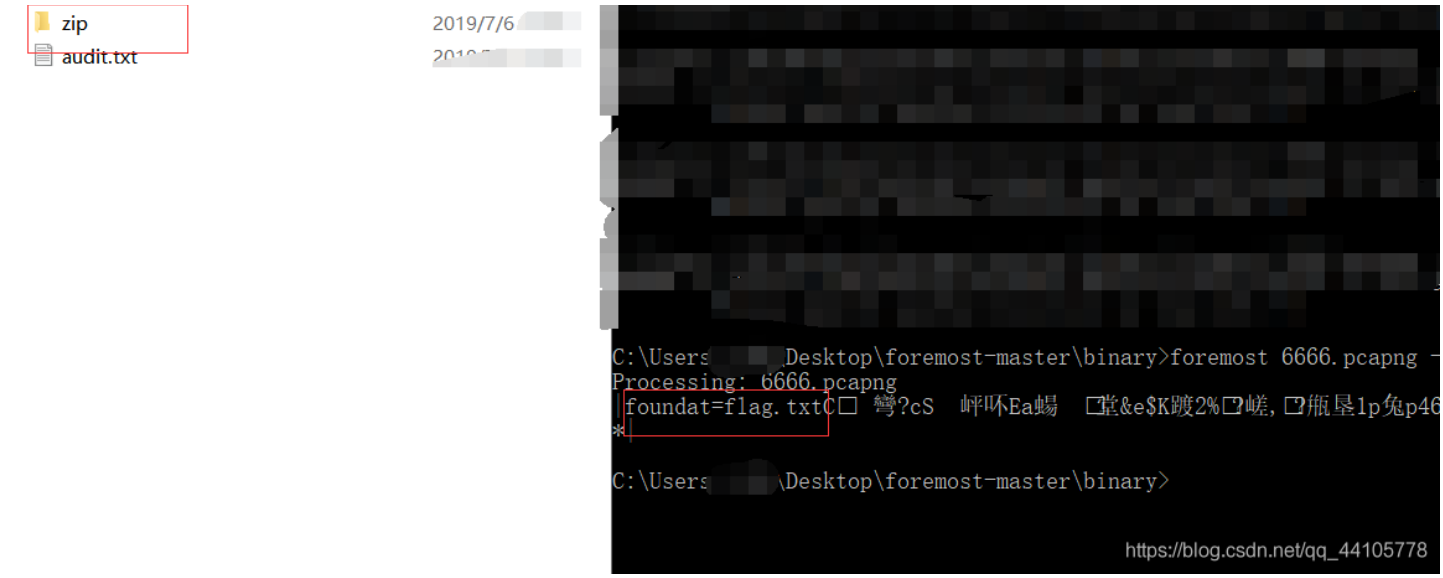
2.cmd进入foremost所在目录，cd 文件夹路径

3.

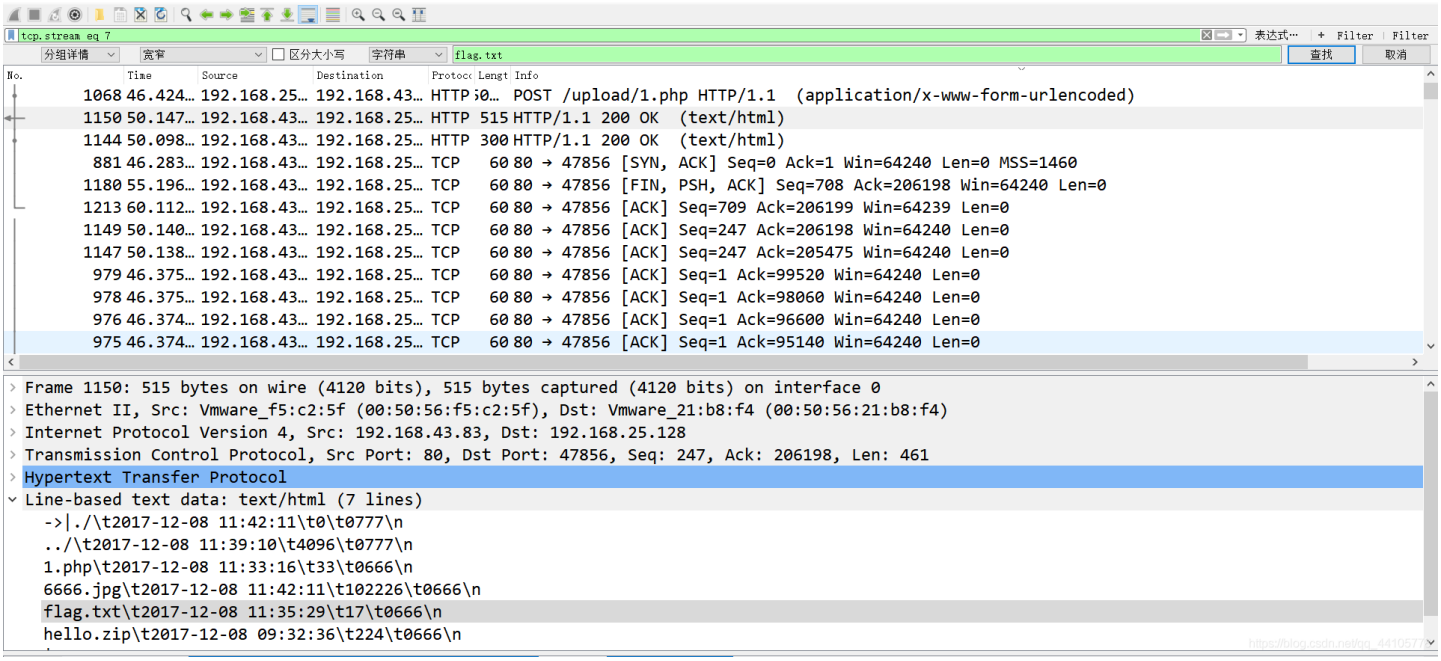
```
foremost 待分离的文件名
```

这样就会生成一个输出文件夹。

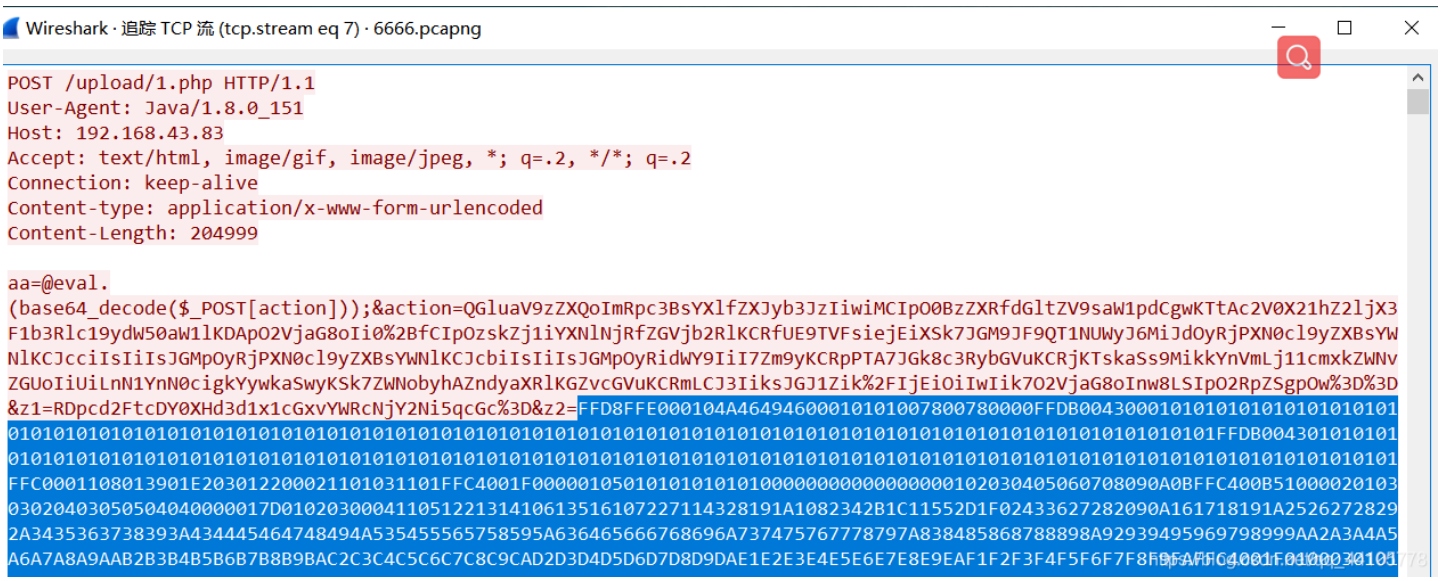


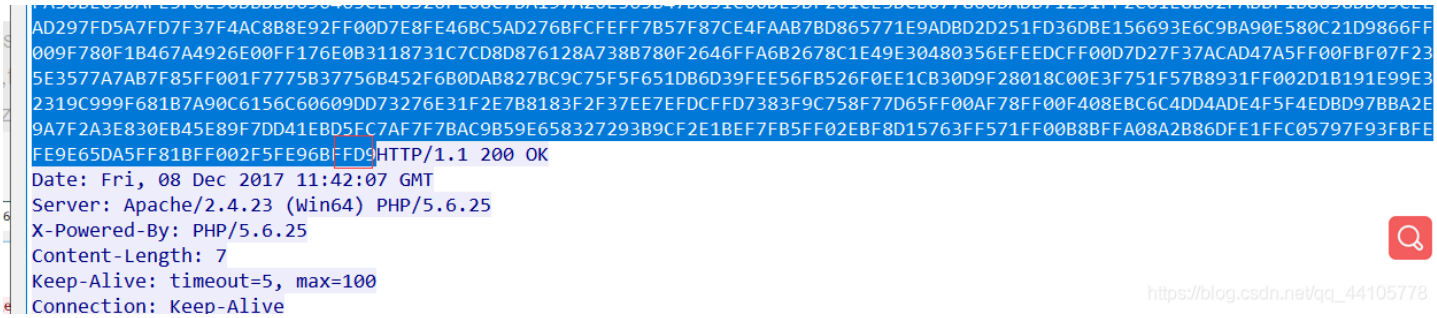


在zip里可以发现一个加密的flag.txt文件。用wireshark打开6666.pcapng文件，查找flag.txt关键字



发现有个6666.jpg文件，使用TCP追踪流，复习下面蓝色部分。FFD8开头，FFD9结尾，并在winhex中新建文件复制并粘贴。注意粘贴格式选择为ASCII Hex。





报存为jpg格式，可以得到图片，图片里的文字就是密码，输入密码，得到flag.

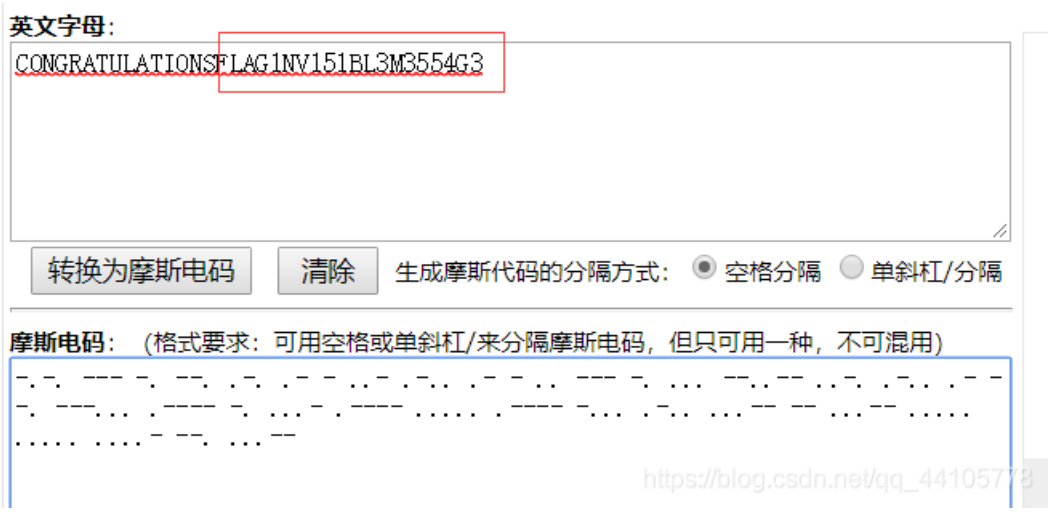
二、菜狗收到了图后很开心，玩起了pdf(flag格式为大写)

下载附件后，发现是pdf,那么

在google上安装插件PDF Viewer，控制台输入document.documentElement.textContent（获取整个文档的文本以及CDATA数据），得到一串AB编码而成的字符串，猜测是摩斯密码，利用记事本的功能快速，将A变为 . ，B变为 - ，

然后将替换后的字符进行摩斯解密在线解密即可得出flag

j



三、SSCTF线上选举美男大赛开始了，泰迪拿着他的密码去解密了，提交花括号内内容（Z2dRQGdRMWZxaDBvaHRqcHRfc3d7Z2ZoZ3MjfQ==）

前置知识

所谓**栅栏密码**，就是把要加密的明文分成N个一组，然后把每组的第i个字连起来，形成一段无规律的话。

一般比较常见的是2栏的栅栏密码。

比如明文：THERE IS A CIPHER

去掉空格后变为：THEREISACIPHER

两个一组，得到：TH ER EI SA CI PH ER

先取出第一个字母：TEESCPE

再取出第二个字母：HRIAIHR

连在一起就是：TEESCPEHRIAIHR

这样就得到我们需要的密码了！

而解密的时候，我们先吧密文从中间分开，变为两行：

T E E S C P E

H R I A I H R

再按上下上下的顺序组合起来：

THEREISACIPHER

分出空格，就可以得到原文了：

THERE IS A CIPHER

但是有些人就偏不把密码作出2栏，比如：

明文：THERE IS A CIPHER

七个一组：THEREIS ACIPHER

抽取字母：TA HC EI RP EH IE SR

组合得到密码：TAHCEIRPEHIESR

那么这时候就无法再按照2栏的方法来解了…

不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话）

这样，我们可以通过分析密码的字母数来解出密码…

比如：TAHCEIRPEHIESR

一共有14个字母，可能是2栏或者7栏…

尝试2栏…失败

尝试7栏…成功

然而当栅栏和拼音相结合后，诞生出一种令人痛恨的新思路（如韵母和声母）

凯撒移位密码

也就是一种最简单的错位法，将字母表前移或者后错几位，例如：

明码表：ABCDEFGHIJKLMNOPQRSTUVWXYZ

密码表：DEFGHIJKLMNOPQRSTUVWXYZABC

这就形成了一个简单的密码表，如果我想写frzy（即明文），那么对照上面密码表编成密码也就是iucb（即密文）了。密码表可以自己选择移几位，移动的位数也就是密钥。

进制转换密码。 比如给你一堆数字，乍一看头晕晕的，你可以观察数字的规律，将其转换为10进制数字，然后按照每个数字在字母表中的排列顺序，拼出正确字母。

举例：110 10010 11010 11001

解：

很明显，这些数字都是由1和0组成，那么你很快联想到什么？二进制数，是不是？嗯，那么就试着把这些数字转换成十进制试试，得到数字6 18 26 25，对应字母表，破解出明文为frzy

然后再进行栅栏解密得到flag

四、一个恐怖份子上传了这张照片到社交网络。里面藏了什么信息？

本题为jpg图片信息隐写outguess 工具（在kali里，可对jpg图形隐藏信息查询）

安装方法
终端命令输入git clone https://github.com/crorvick/outguess进行下载，下载完成后进入outguess文件夹，

执行命令./configure && make && make install 进行编译及安装。
使用方法

加密：
outguess -k “my secret key” -d hidden.txt demo.jpg out.jpg
加密之后，demo.jpg会覆盖out.jpg,
hidden.txt中的内容是要隐藏的东西

解密：
outguess -k “my secret key” -r out.jpg hidden.txt或者outguess -r lamb.jpg hidden.txt

解密之后，解密内容放在hidden.txt中
然后使用cat hidden.txt查看

-r解密，-d加密

使用,下面2行代码得到flag

```
outguess -r lamb.jpg  hidden.txt
cat hidden.txt
```