

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](#)

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/qq_44105778/article/details/94842746

版权



[misc](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

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

名称	修改日期	类型
foremost.conf	2016/2/4 19:13	CONF 文件
foremost.exe	2016/2/4 19:13	应用程序
foremost-linux	2016/2/4 19:13	文件
foremost-mac	2016/2/4 19:13	文件

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
```

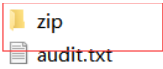
这样就会生成一个输出文件夹。

https://blog.csdn.net/qq_44105778

master > binary > output

名称

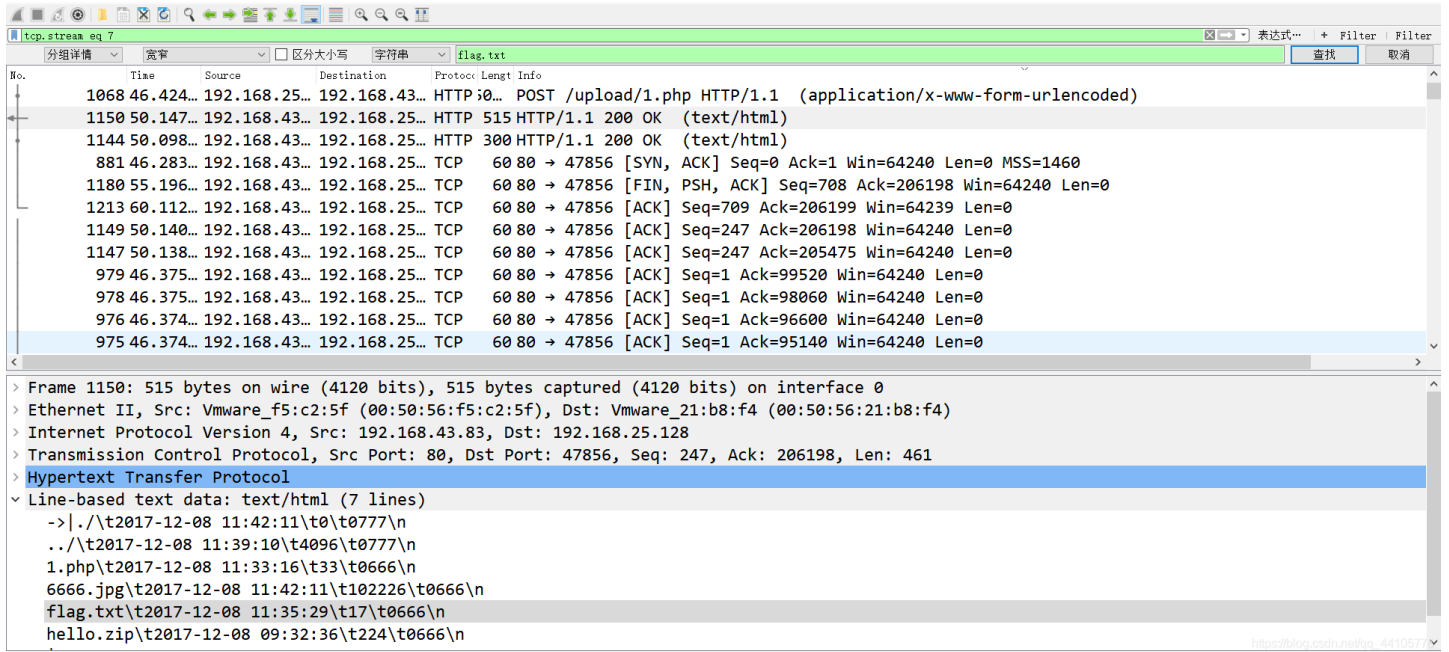
修改日期



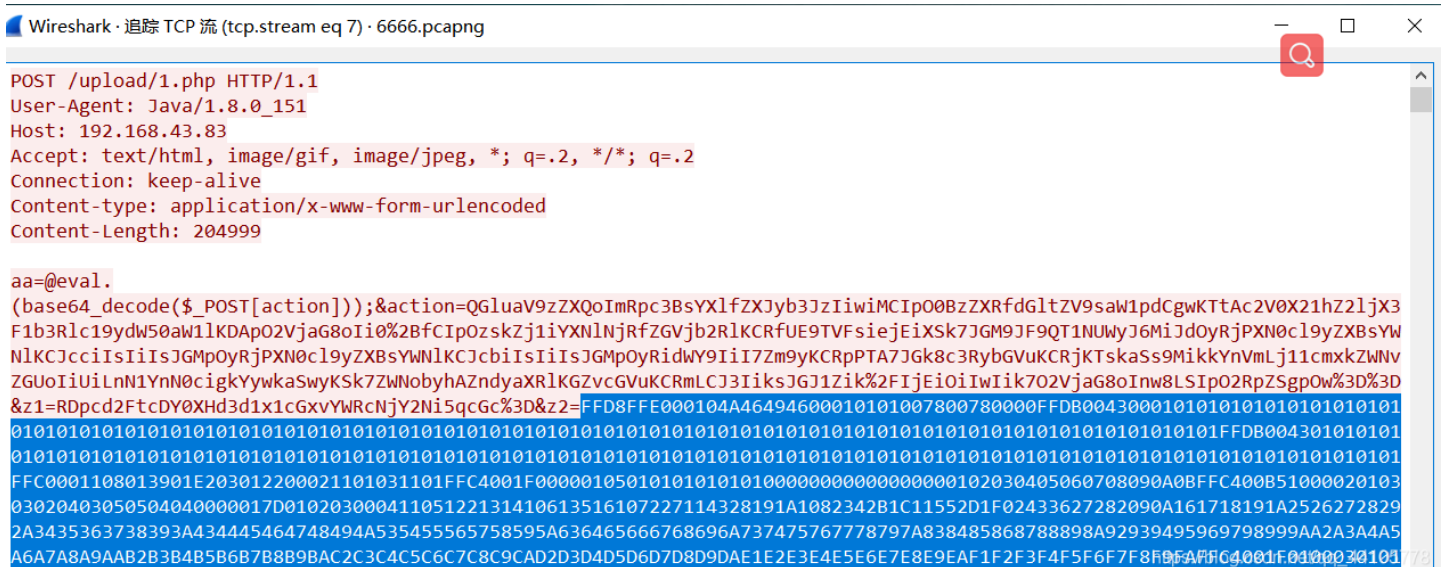
2019/7/6
2019/7/6



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。



```
AD297FD5A7FD7F37F4AC8B8E92FF00D7E8FE46BC5AD276BFCFEFF7B57F87CE4FAAB7BD865771E9ADBD2D251FD36DBE156693E6C9BA90E580C21D9866FF
009F780F1B467A4926E00FF176E0B3118731C7CD8D876128A738B780F2646FFA6B2678C1E49E30480356EFEEDCF00D7D27F37ACAD47A5FF00FBF07F23
5E3577A7AB7F85FF001F7775B37756B452F680DAB827BC9C75F5F651DB6D39FEE56FB526F0EE1CB30D9F28018C00E3F751F57B8931FF002D1B191E99E3
2319C999F681B7A90C6156C60609DD73276E31F2E7B8183F2F37EE7EFD9FD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4ADE4F5F4EDBD97BBA2E
9A7F2A3E830EB45E89F7DD41EBD5FC7AF7F78AC9B59E658327293B9CF2E1BEF7FB5FF02EBF8D15763FF571FF00B8BFFA08A2B86DFE1FFC05797F93FBFE
FE9E65DA5FF81BFF002F5FE96BFFD9HTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:07 GMT
Server: Apache/2.4.23 (win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 7
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

https://blog.csdn.net/qq_44105778

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)

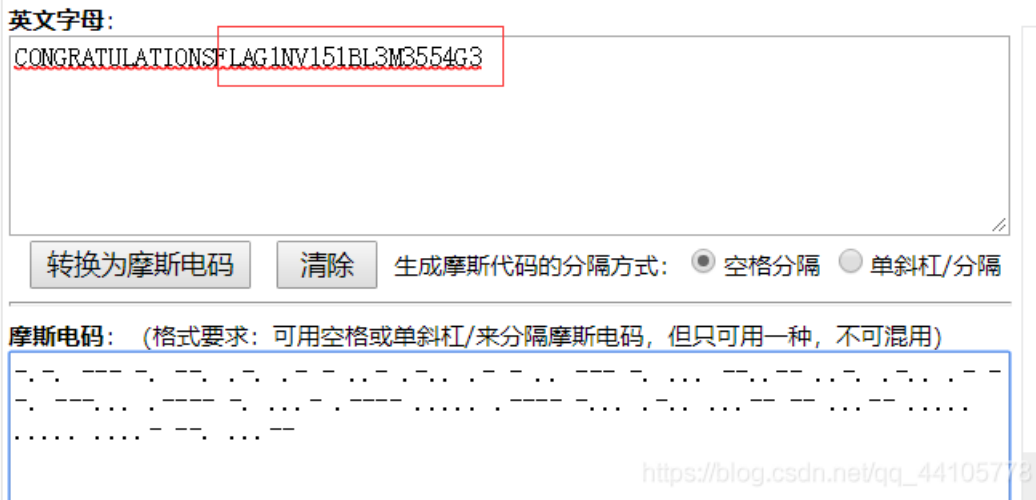
下载附件后，发现是pdf,那么

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：THER EISA CIPHER

先取出第一个字母：TEESCPE

再取出第二个字母：HRAIHR

连在一起就是：TEESCPEHRAIHR

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 EIRP 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

解密

```
ggq@gqlfch0ohtjpt_sw{gfhs#}
```

解密 使用英文字典智能分析

```
第1次解密:ggq@gqlfch0ohtjpt_sw{gfhs#}  
第2次解密:ffp@fp1epg0ngsios_rv{fegfr#}  
第3次解密:eeo@eoldof0mfrhnr_qu{edfec#}  
第4次解密:ddn@dn1cne0legmq_pt{dcedp#}  
第5次解密:ccm@cmlbmd0kdbflp_os{cbdcc#}  
第6次解密:bb1@b11alc0icoeko_nr{bacbn#}  
第7次解密:aak@aklzk0ibndin_mq{azbam#}  
第8次解密:zzi@zilvia0hamcim_lp{zyazl#}  
第9次解密:yvi@vilxiz0gzlhh1_ko{vxzyk#}  
第10次解密:xzh@xhlwhv0fykagk_in{xwvxi#}  
第11次解密:wwg@wglvgx0exjzfi_im{wvwi#}  
第12次解密:vvf@vflufw0dwiyei_hl{vuwh#}  
第13次解密:uae@ueltev0cvhxdh_gk{utvug#}  
第14次解密:ttd@tdlsdu0bugwcf_j{tsutf#}  
第15次解密:ssc@sc1rct0atfvbf_ei{srtse#}  
第16次解密:rrb@rblqbs0zseuae_dh{rqsrd#}
```

https://blog.csdn.net/qq_44105778

然后再进行栅栏解密得到flag

```
ssC@sClrct0atfvbf_ei{srtse#}
```

每组字数

加密

解密

```
ssctf{ssCtf_seC10ver#@rabit}
```

https://blog.csdn.net/qq_44105778

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/cronvick/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
```