ctf隐写术的一些个人总结

原创

tansty_zh 于 2020-08-28 23:16:15 发布 856 收藏 4
分类专栏： ctf 文章标签： 安全

一、文件分离

1.binwalk
binwalk -e sim.jpg
分离文件

2.foremost
foremost 文件名 -o 输出目录名

3.dd
dd if=源文件 of=目标文件名 bs=1 count=几块 skip=开始分离的字节数
参数说明：
if=file 输出文件名
of=file 输出文件名
bs=bytes 同时设置读写块大小为bytes，可代替ibs和obs
skip-blocks 从输入文件开头跳过blocks个块后开始复制

4.文件合并：
cat gif01 gif02 gif03 > 1.gif
md5sum 1.gif 查看1.gif的MD5 校验值

二、图片隐写

1.zsteg xxx.png 检测lsb隐写

2.wbstego 加解密bmp

3.TwwakPNG 检测crc校验值

4.bftools
在Windows的cmd下，对加密过的图片文件进行解密

```
格式:
bftools.exe  decode  braincopter  要解密的图片名称 -output 输出文件名
```

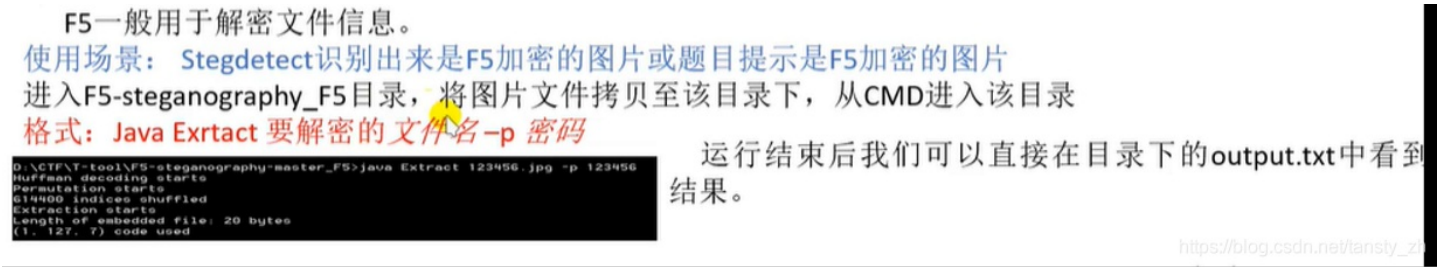
5.stegdetect工具探测加密方式
主要用于分析peg文件

```
stegdetect  xxx.jpg
```

stegdetect -s 敏感度 xxx.jpgex

6.

7.



三、压缩文件伪加密

原理我就不说了，直接用最简单的方法
使用ZipCenOp.jar直接破解伪加密

```
1. java -jar ZipCenOp.jar e xxx.zip 加密
2. java -jar ZipCenOp.jar r xxx.zip 解密
3. java -jar ZipCenOp.jar r LOL.zip
```

rar文件伪加密：
第24个16进制数尾数改为0

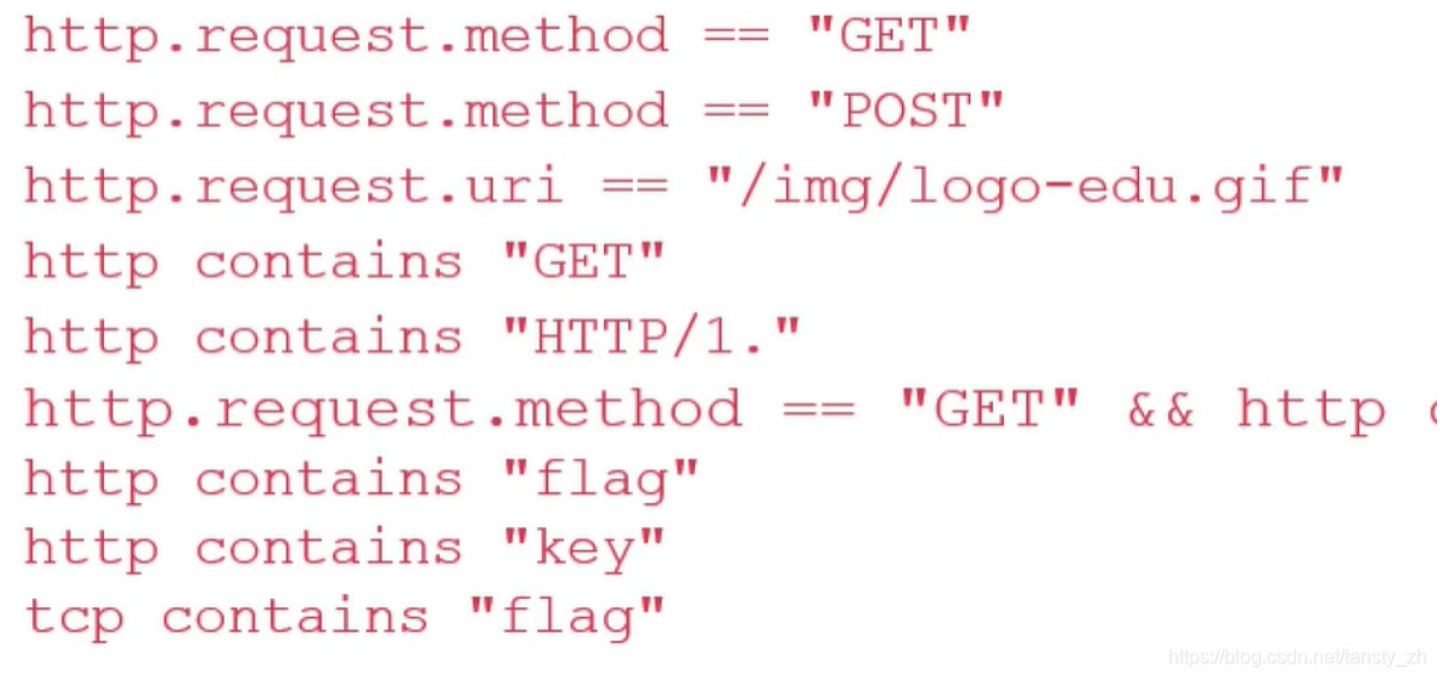
四、流量取证

wireshark过滤命令：

```
1.过滤IP，如源IP或者目标x.x.x.x
ip.src  eq  x.x.x.x  or  ip.dst eq x.x.x.x

2.过滤端口
tcp.port eq 80 or udp.port eq 80
tcp.dstport ==80  只显示tcp协议的目标端口为80‘
tcp.srcport ==80 只显示tcp协议的源端口为80
tcp.port  >=1  and  tvp.port <=80


3.http模式过滤
```



追踪流

常见的HTTP流关键内容：
1、HTML中直接包含重要信息
2、上传或下载文件内容，通常包含文件名、hash值等关键信息，常用POST请求上传
3、一句话木马，POST请求，内容包含eval，内容使用base64加密

wireshark 数据提取
文件–导出对象

无线流量包：

```
1.aircrack-ng检查cap包：
aircrack-ng  xxx.cap

2.用aircrack-ng跑字典进行握手包破解
aircrack-ng  xxx.cap  -w  pass.txt
```