文件操作与隐写

原创

xici_ 于 2020-07-13 23:15:53 发布 339 收藏 4
分类专栏： 小饼干

本文链接：https://blog.csdn.net/xici_/article/details/107326173

一、文件操作

1.分析下载的文件:文件类型的识别

（原理：每个文件都会有相应的结构，根据文件头识别不同的文件）

1.1手工分析：windows :WinHex
010 Editor
notepad++（下载插件 hex editora安装在notepad++的安装路径)；
1.2 工具分析 Linux

当文件出现无法打开的情况，需要查看文件头，如果损坏或者缺失需要进行相应补充。

2.文件分离：

（原理：依照文件头类型，去查找十六进制）
a.自动化 （kail）
binwalk:分析+分离
foremost 分离（按照类型分类）
b.半自动化

c.手工：通过十六进制数，选中导出

二、隐写

1.文件内容隐写

将key以十六进制的形式写在文件中，通常在文件的开头部分或结尾部分，分析时通常重点观察文件开头和结尾部分。如果在文件中间部分，通常搜索关键词KEY或者flag来查找隐藏内容。
使用场景：windows下，搜索隐写的文件内容

1.1.Winhex/010Editor
通常将要识别的文件拖入winhex中，查找具有关键字或明显与文件内容不和谐的部分，通常优先观察文件头部和尾部，搜索flag或key等关键字，最后拖动滚轮寻找。

1.2.Notepad++
使用notepad++打开文件，查看文件头尾是否含有关键字的字符串，搜索flag或者key等关键字，最后拖动滚轮寻找。
另外通过安装插件HEX-Editor可以实现winhex的功能。

2.图片文件隐写
图片隐写的常见隐写方法：
1.细微的颜色差别
2.GIF图片多帧隐藏
  1.颜色通道隐藏
  2.不同帧图信息隐藏
  3.不同帧对比隐写
3.Exif信息 (图片属性信息）隐藏
4.图片修复
  1.图片头修复
  2.图片尾修复
  3.CRC校检修复
  4.长、宽、高度修复
5.最低有效位LSB隐写
6.图片加密
  1.Stegdetect
  2.outguess
  3.Jphide
  4.FS

1.Firework（图层分解和帧分解）
使用winhex打开文件时会看到文件头部中包含firework的标识，通过firework可以找到隐藏图片（使用场景：查看隐写的图片文件）

2.Exif
Exif按照JPEG的规格在JPEG中插入一些图像/数字相机的信息数据以及缩略图像。可以通过与JPEG兼容的互联网浏览器/图片浏览器/图像处理等一些软件来查看Exif格式的图像文件，就跟浏览通常的JPRG图像文件一样。
图片右键属性，查看exif或查看详细信息，在相关选项卡中查找flag信息。

3.Stegsolve（最常用）
当两张JIP图片外观、大小、像素都基本相同时，可以考虑进行结合分析，即将两个文件的像素RGB值进行XOR.ADD.SUN等操作，看能否得到有用的信息，StegSolve可以方便的进行这些操作。
使用场景：两张图片信息基本相同
1 .通道分离 2.LSB分离 3.图像对比

4.LSB（最低有效位Least Significant Bit）
LSB替换隐写基本思想是用嵌入的秘密信息取代载体图像的最低比特位，原来的7个高位平面与替代秘密信息的最低平面组合合成含隐藏信息的新图形。
  1.像素三原色（RGB）
  2.通过修改像素中最低位的1bit来达到隐藏的效果
  3.工具：stegsolve（图像分析工具） zsteg（需要先下载安装） wbstego4 python脚本

5.针对PNG图像

工具：TweakPNG（TweakPNG是一款简单易用的PNG图像浏览工具，它允许查看和修改一些PNG图像文件的元信息储存。）
使用场景：文件头正常使用却无法打开文件，利用TweakPNG修改CRC
原理：图像头部不止是文件类型的标识，还包含了长度、高度以及校验值
　　通常情况下，一个图像的产生，就会被赋予各种文件头部的信息；一般情况下图像刚产生的时候，长宽高等信息会被校验，产生一个x1值；如果这个图像被修改了，有可能产生图像无法打开或者显示不全：
1.校验值被修改为x2：使用Tweak去检验的时候，通过长、宽、高算出来的值是x1，跟现在的x2不一致，产生报错。
2.高度被修改，比如减半
总结：如果计算出来的数值报错，那一定是被修改过

6.加密图片的解密

可以将文字或者文件隐藏到图片中
命令：bftools　图像化：slienteye

a.Bftools
bftools用于解密图片信息
使用场景：在Windows的cmd下，对加密过得图片文件进行解密
格式：
Bftools.exe decode braincopter 要解密的图片名称-output 输出文件名
Bftools.exe run 上一步输出的文件

b.SilentEye
silentEye 是一款可以将文字或者文件隐藏到图片的解密工具
使用场景：Windows下打开silentEye工具，对加密的图片进行解密

7.jpeg解密：

分析工具：Stegdetect

8.JPG图像加密方式：

1.Stegdetect工具探测加密方式
stegdetect程序主要用于分析JPEG文件。因此用Stegdetect可以检测到通过JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和Camouflage等这些隐写工具隐藏的信息。
2.Jphide
　Jphide是基于最低有效位LSB的JPEG格式图像隐写算法.
例: Stegdetect提示jphide加密时，可以用Jphs工具进行解密，打开jphswin.exe，使用open jpeg打开图片，点击seek,输入密码和确认密码，在弹出文件框中选择要保存的解密文件位置即可，结果保存成txt文件。

3.Outguess(一般用于解密文件信息)
使 用 场 景:　　Stegdetect识别 出来或者题目提示是outguess加密的图片
该工具需编译使用: /configure && make && make install
格　　式: outguess-r 要解密的文件名输出结果文件名

4.F5
F5一 般用于解密文件信息。
使用场景: Stegdetect识别 出来是F5加密的图片或题目提示是F5加密的图片

进入F5-steganography_ F5目录，将图片文件拷贝至该目录下，从CMD进入该目录
格式: Java Exrtact要解密的文件名-p密码