隐写术总结

转载

浅墨微蓝 于 2018-05-12 14:43:06 发布 3635 收藏 11
分类专栏： 信息安全基础 文章标签： 隐写术 ctf


信息安全基础 专栏收录该内容
9 篇文章 1 订阅
订阅专栏

转自https://blog.csdn.net/captivate_guan/article/details/73692302

几种隐写术加密工具：

序号	工具	作者	主要方法	图像格式
1	BMP Secrets		空域替换法	JPEG、GIF、BMP等
2	DCT-Steg (DCT-Jpeg)	Stefan Katzenbeisser	DCT系数修改	JPEG
3	EzStego	Romana Machado	LSB方法	GIF
4	F5 v F0.9	Andreas Wachado	修改量化后的DCT系数	JPEG、GIF、BMP
5	Hide and Seek 95 v 1.1	Colin Moroney	空域LSB方法	BMP
6	JP Hide and Seek	Allan Latham	修改量化后的DCT系数	JPEG
7	JPHSWin	Allan Latham	修改量化后的DCT系数	JPEG
8	JSteg Shell	John Korejwa	修改量化后的DCT系数	输出JPEG
9	JSteg-Jpeg	Derek Upham	修改量化后的DCT系数	输出JPEG
10	OutGuess	Niels Provos	修改量化后的DCT系数	JPEG、PNM

人们在图像中隐藏秘密信息，用图像中的每个字节的最不重要的比特代替消息比特。但是图像并没有怎么改变（大多数图像标准规定的颜色的等级比人类眼睛能够察觉到的要多得多），秘密消息却能在接收端剥离出来。比如一张照片，在计算机中用24比特来描述每一个像素的颜色。如果把每个像素的24比特中最次要比特拿出来存放另外的文件，人的眼睛是分辨不出来隐藏了文件的照片与原来的照片有什么区别的。用这种方法可在大小为1024*1024字节的灰色刻度图片中储存64KB的消息。同样道理，我们也可以吧声音文件和视频文件中最次要比特拿出来存放要隐藏的文件。

解隐写题的思路:

首先看看图片是不是图种
然后使用binwalker分析图片,如果是有文件合成,分离
有时信息藏在备注中
工具stegsolve
编程分析
png图片像数保存是从左到右，从下往上排列的。
png图片经过了压缩，不好直接对比每个字节，而bmp图片是没有压缩的，直接保存各个像数点的数据。
mp3stego

转自https://www.cnblogs.com/ycll/p/6420509.html

工具：

（1）Stegsolve图片分析软件： 用于分析图片，图片是由各种不同颜色的像素点构成的（涉及LSB等图片图形学内容，感兴趣的可以自己去查），这个工具可以很容易的把不同颜色通道的图片信息显示出来。

（2） 二维码扫描： 在图片隐写中，扫描二维码得到答案的题目是比较常见的，但是有时候扫描之后出现的也不一定是最后答案，往往需要我们进一步的去破解，所以用手机扫描注定不方便，有个电脑上的软件会方便很多。

（3）十六进制分析工具：与这个相同的还有winhex，winhex更常用，且功能更强大，想使用哪个看个人喜好。计算机的世界，所有的东西都是由1和0组成的，二进制也可以转成十六进制，所以利用这个工具可以看到构成图片的最原始的数据，同时可以找到隐藏在图片里的秘密。

4）binwalk:这是在kali下自带的一个命令行工具，可以用来分析目标文件里是否有夹带其他东西，这在除了隐写以外的其他类型的题也是常用的工具。命令：binwalk –n 加文件 。比如说一张图片里面隐藏了一个压缩包，从表面上你是看不出什么的。但是使用binwalk命令，就可以分析出来。同样，把图片丢到十六进制查看器里面也可以看出来，但是新手对这些不熟悉很容易出错。毕竟压缩文件除了rar还有zip，又或许图片里面藏的是个txt。

另外，分析之后我们需要把这附带的其他文件提取出来，这就需要另外的一个命令，

binwalk –e 加文件。同样可以使用十六进制查看器，通过分离切割来得到，有兴趣的同样可以自己试试。

（5）PS:这个东西大家肯定不会陌生，有关图片隐写，ps有时候会用到，但几率不大。因为前面介绍的几种工具基本已经够用了，ps无非也就是有更进一步的能力而已。与ps相应的还有一个叫做FW的工具，也是Adobe系列的。要是一张图片真的什么都分析不出来，丢到PS里，说不定就会发现惊喜了，但是这样的题至今我也只遇过三题，其中两题都是跟FW有关的。

（6）密码学：这就涉及到一个很大的方面了。有时候我们找到了图片里面藏的密码，但是出题人不会很直白的告诉我们答案，就会进行加密。常见的密码有md5,base64，当然还有各种各样奇怪的密码。不过野不用着急，这都是一个积累的过程，先去了解md5和base64的特征，然后拿解到的密码去网上搜索。大部分常见的密码类型网上都有在线解码网站

三.一些经验技巧：我一直认为看再多的东西都不如实际做几题来的印象深刻，不然很多东西都是看了就忘的。但是一些经验技巧也可以让后面学习的人少走些弯路（PS:这些都是我以前做题的时候总结的，也许不一定都是对的，毕竟接触这块还不是很久，还有很多地方要学习的，但是也可以参考一下，找到自己的一个做题思路才是最重要的）

（1）一般拿到一张图片，先看图片格式。常见的有JPG，PNG和BMP。JPG比起PNG，是有过压缩的图片，所以JPG格式的图片通常是没必要放到图片分析器里去看的。由于进过压缩，所以里面是不能放下二维码的。而我们使用图片分析器来分析图片，60%是为了找到里面隐藏的二维码。

（2）JPG格式的图片通常里面都有藏着另外的东西，大体上是压缩文件之类的，当然，也有往里面放音频的……所以先丢去binwalk分析才是正确的。

（3）PNG格式的图片首先就可以考虑藏二维码的问题了，不过也不是说他里面不会藏有其他文件哟。

（4）BMP是位图文件,能放的东西就更多了，可以拿去PS里看一下，说不定在就出现了两个图层了。

（5）无格式的东西，图片隐写的题，出题人很喜欢绕一个弯。有时候下载下来的东西是没有后缀格式的，这时候需要手动去添加。丢到十六进制查看器里去看它的头部十六进制，取前四个到百度搜一下就知道是什么格式了。同理，也有人会把头部文件给删除，这时候要靠他的后缀手动添加头部。这些都是在十六进制查看器里完成的。

（6）遇到音频的时候，音频也是可以藏东西的。我一般是喜欢用AU，当然也有其他比较专门的工具，可以自己去找找。查看音频的波形，有时候里面会藏有一段莫尔斯电码。

转自https://www.cnblogs.com/linwx/p/7831022.html

一.图像隐写术进行数据隐写分为以下几类：

1.在图片右击查看属性，在详细信息中隐藏数据
2.讲数据类型进行改写（rar或者zip数据改为jpg等格式）
3.根据各种类型图像的固定格式，隐藏数据
修改图像开始的标志，改变其原来图像格式
在图像结束标志后加入数据
在图像数据中加入数据，不影响视觉效果情况下修改像素数据，加入信息
4.利用隐写算法将数据隐写到图片中而不影响图像（仅限于jpg图像） 隐写常用的算法有F5，guess jsteg jphide。
二.破解隐写术方法及步骤
1.查看图像属性详细信息是否有隐藏内容
2.利用winhex或nodepad++打开搜索ctf,CTF，flag,key等关键字是否存在相关信息
3.检查图像的开头标志和结束标志是否正确，若不正确修改图像标志恢复图像，打开查看是否有flag或ctf信息，（往往gif属于动图，需要分帧查看各帧图像组合所得数据 若不是直接的ctf或flag信息 需要考虑将其解码）
jpg图像开始标志：FF D8 结束标志 ：FF D9
gif图像开始标志：47 49 46 38 39 61 (GIF89)结束标志：01 01 00 3B
bmp图片开始标志：42 4D //92 5B 54 00 00 00 00 00 结束标志：00
png图片开始标志：89 50 结束标志：
4.将图片放置在kail系统中，执行binwalk xxx.jpg 查看图片中是否是多个图像组合或者包含其他文件（若存在多幅图像组合，再执行foremost xxxjpg会自动分离；若检测出其他文件修改其后缀名即可，如zip）
5.使用StegSolve对图像进行分通道扫描，查看是否为LSB隐写
6.在kail下切换到F5-steganography，在java Extract运行
命令：java Extract 123456.jpg图片的绝对地址 -p 123456
判断是否为F5算法隐写
7.在kali系统中使用outguess-master工具（需要安装），检测是否为guess算法隐写

三.算法隐写的具体操作

1.F5算法隐写

具体操作：在kail下切换到F5-steganography，在java Extract运行
命令：java Extract 123456.jpg图片的绝对地址 -p 123456

2.LSB算法隐写

具体操作：在Stegsolve.jar分析data Extract的red blue green

3.guess算法隐写

具体操作：在kail下切换到outguess目录下，直接用命令即可
命令:outguess -r /root/angrybird.jpg(绝对路径) 123.txt(信息存放的文本)
四.工具使用
1.MP3stego
encode -E hidden_text.txt -P pass svega.wavsvega_stego.mp3

Decode.exe -X -P pass(密码) svega_stego.mp3(要拷贝到目录下) //解码

2.stedgetect

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

s – 修改检测算法的敏感度，该值的默认值为1。检测结果的匹配度与检测算法的敏感度成正比，算法敏感度的值越大，检测出的可疑文件包含敏感信息的可能性越大。

d – 打印带行号的调试信息。

t – 设置要检测哪些隐写工具（默认检测jopi），可设置的选项如下：

j – 检测图像中的信息是否是用jsteg嵌入的。

o – 检测图像中的信息是否是用outguess嵌入的。

p – 检测图像中的信息是否是用jphide嵌入的。

i – 检测图像中的信息是否是用invisible secrets嵌入的。

命令：stegdetect.exe -tjopi -s10.0 xxx.jpg

转自https://blog.csdn.net/fengshenyue/article/details/51638986

- 图种,只要将图片保存为zip压缩包格式,然后解压出来就可以了
- jpg的结束符:`FF D9`
- 观察文件结束符之后的内容，查看是否附加的内容，正常图片都会是FF D9结尾的。还有一种方式来发现就是利用binwalk这个工具，在kali下自带的一个命令行工具。利用binwalk可以自动化的分析图片中附加的其他的文件，其原理就是检索匹配文件头，常用的一些文件头都可以被发现，然后利用偏移可以配合winhex或者是dd分割出隐藏的部分。
- 还有另一类隐藏的方法就是利用修改数据的方式来隐藏自己传递的信息.**利用LSB来进行隐写**.如果是要寻找这种LSB隐藏痕迹的话，有一个工具是个神器，可以来辅助我们进行分析。Stegsolve这个软件….打开之后，使用Stegsolve——Analyse——Frame Browser这个可以浏览三个颜色通道中的每一位，可以在红色通道的最低位，发现一个二维码，然后可以扫描得到结果。
- 隐写的载体是PNG的格式，如果是像之前的jpg图片的话就是不行的，原因是jpg图片对像数进行了有损的压缩，你修改的信息可能会被压缩的过程破坏。而PNG图片虽然也有压缩，但却是无损的压缩，这样子可以保持你修改的信息得到正确的表达，不至于丢失。BMP的图片也是一样的，是没有经过压缩的，可以发现BMP图片是特别的大的，因为BMP把所有的像数都按原样储存，没有压缩的过程。
- qrcode，用在线的就可以解开http://tool.chinaz.com/qrcode/
- **Stegsolve**
- **Stegdetect**
- 一个jpg的图片。除了我们之前说到的隐藏在结束符之后的信息，jpg图片还可以把信息隐藏的exif的部分。exif的信息是jpg的头部插入了数码照片的信息，比如是用什么相机拍摄的。这些信息我们也是可以控制的，用查看属性的方式可以修改一部分的信息，还可以用exif编辑器来进行编辑。
- 隐写术有的时候难，就是难在了一张图片有太多的地方可以隐藏信息了，有的时候根本连隐藏的载体都找不到，在你的眼里他就是一张正常的图片。
- 这个题需要我们对于png图片的格式有一些了解，先用stegsolve查看一下，其他的LSB之类的并没有发现什么问题，然后看了一下结构发现，有一些异常的IDAT块。IDAT是png图片中储存图像像数数据的块。

  解隐写题的思路:

  - 首先看看图片是不是**图种**
  - 然后使用binwalker分析图片,如果是有文件合成,分离
  - 有时信息藏在备注中
  - 工具stegsolve
  - 编程分析

  png图片像数保存是从左到右，从下往上排列的。

- png图片经过了压缩，不好直接对比每个字节，而bmp图片是没有压缩的，直接保存各个像数点的数据。
- **mp3stego**