隐写术总结

原创

lryong. 于 2016-06-12 01:13:20 发布 11595 收藏 10

分类专栏： 2016年6月

本文链接：https://blog.csdn.net/fengshenyue/article/details/51638986

2016年6月 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

隐写术总结

- 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**