CTF 图片相关

原创

这是游戏吗 于 2018-11-13 18:31:07 发布 2475 收藏 9

CTF—图片相关

0x00 前言

CTF中，有一类题就是图片，各种玩弄图片，反正你就是想不到，下面我就说下我知道的一些图片的玩法

0x01 jpg图片的属性

这算最简单的一种，正常的jpg图片，选中右键查看属性，在详细信息一栏会发现有很多属性就是自己可以修改的，有的人可以凭借相片里的这些信息进行社工，查找地点，放在ctf里就可以藏信息了

0x02 图种

图种呢，就是图片后面再放点信息进去，压缩包、txt文档、或者再来一张图片 看我是怎么放的(cmd下)：

- `copy a.jpg/b+b.zip/b c.jpg`
- `copy a.jpg/b+b.txt/b c.jpg`
- `copy a.jpg/b+b.jpg/b c.jpg`

得到的c.jpg就是图种了，想藏什么随便你，图种可不是随便叫的
至于还原也很简单

- 改后缀为zip，解压即可
- 记事本或者winhex打开，就可以看到了（记事本可能会卡死）
- 可以用winhex找图片的开头结尾标志，手动分离出来，也可以使用kali下的工具binwalk或者foremost分出来，像这种手动分离还是挺快的

注：比较高级点的图片隐藏图片的话，有的会把第二张图片头给去掉，然后把两张图片合在一起，这样那些提取工具就没用了，这个时候需要稍微细心点，我一般是拿winhex找第一张图片的尾部，然后把第二张图片的头给加一下，这样就正常了

0x03 图层里的秘密 LSB

玩ctf的大概都听过一个神器，`stegsolve`，用它把图片打开，一直按右箭头，说不定就会出来一个二维码
或者是它的第二个用途，提取低位信息，这涉及到图片隐写的一个大类，lsb隐写，一般都藏在0,1,2这些低位里面：
Analyse→Data Extract，剩下就是自己试了
有一个隐藏，检测，恢复的网站：http://incoherency.co.uk/image-steganography/ 感兴趣可以自己试试

0x04 图片头损坏

这类的话，别的像word文件，pdf文件也有，它们都有比较明显的头信息，感兴趣可以拿winhex看看，做法也很简单，找一个类型相同的文件，在winhex里照着改回来就能正常打开了

0x05 图片的高度

新get到一个姿势，用16进制编辑工具更改图片的高度，会只显示图片的一部分，下面的部分就被隐藏了，是个藏东西的好办法
找表示宽度和高度的位置的话，可以先看看图片的属性，得到宽高值，转成16进制，搜索16进制值就找到了
注：png图片的保存恢复效果比较好，jpg貌似有点问题，QQ空间居然不接受改过高度的png图片……
（试过改宽度，效果不好，高度很好掌握）

0x06 图片隐写的工具

怎么说呢，工具很多，这类要慢慢补充，先写几个，剩下的以后补

oursecret

下载地址：http://steganography.findmysoft.com/download/ （小心捆绑软件）
这工具很强大，什么文件都能用来隐藏

Image Steganography

下载地址：http://imagesteganography.codeplex.com/
比较精巧

Outguess

下载地址：https://github.com/crorvick/outguess
下载之后看着readme自己编译一下，使用方法如下：

```
outguess -k “my secret key” -d hidden.txt demo.jpg out.jpg   # 隐藏
outguess -k “my secret key” -r out.jpg hidden.txt            #提取
```

官网应该挂了，就别找了

给我老师的人工智能教程打call！http://blog.csdn.net/jiangjunshow