Misc常见图片隐写

原创

PEN202012138 于 2021-01-17 18:19:45 发布 1012 收藏 15

分类专栏： web misc 文章标签： web

本文链接：https://blog.csdn.net/m0_51450047/article/details/112755190


web 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏


misc

1 篇文章 0 订阅

订阅专栏

Misc常见图片隐写

1. 查看属性

一般真相和图片的内容没有关系

> 这种是最简单的隐藏flag的方式，直接右键查看图片属性，在其中找到flag即可
>
> 有时图片信息中并不会直接给你flag，而是给你一段经过加密的字符或文字，这时观察密文的特征，找出密文对应的加密方式，选择相应的解密工具即可得到flag

2. 伪装成图片的压缩包

一般这种图片看起来和普通图片没什么区别，但其实这个图片是由压缩包伪装成的，一般flag的文本文件就藏在这个压缩包中

解密

要是想知道这张图片到底是不是由图片伪装的，用WinRAR的方式打开图片试一下就知道了

如果，是你就会发现一片新大陆，反之，就是什么都没有，即这张图片不是压缩包

加密

看过了解密，我对这个加密方式也就产生了浓厚的兴趣，于是就上网搜了搜此加密方式，具体如下：

方法一

1. 先准备好一张图片`a.jpg`和要隐藏的压缩包`b.zip`；
2. 打开命令行提示符，将活动目录改到图片和压缩包所在的目录；
3. 输入命令`copy/b a.jpg+b.zip c.jpg`，回车，就能在文件夹中看到一个图片文件`c.jpg`，这个图片就是已经伪装好的压缩包

方法二

1. 在图片和压缩包所在的文件夹新建一个文本文件，文本内容就是刚才的命令`copy/b a.jpg+b.zip c.jpg`；
2. 然后将文件保存为`压缩包伪装成图片.bat`，主要是将文件保存为***bat***格式；
3. 双击***bat***文件就可以看到文件夹中多了一个图片文件`c.jpg`,这个图片c即伪装的压缩包

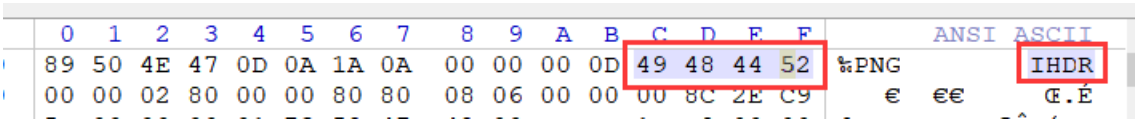
3. WinHex工具de使用

0x1 修改图片宽高

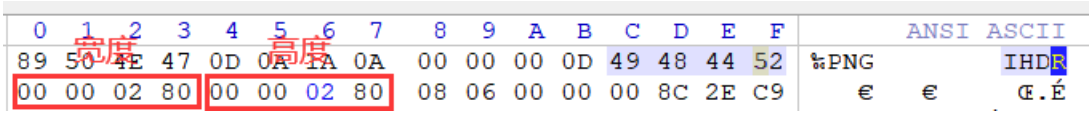
多见于png图片，这种一般是将图片有flag的那一部分通过改变图片高或者宽进行隐藏，一般看到图片题中显示不完整的图片多为这种隐藏方式；

但这并不意味着看起来完整的图片就没有隐藏部分，实际上flag可能隐藏在其另一部分

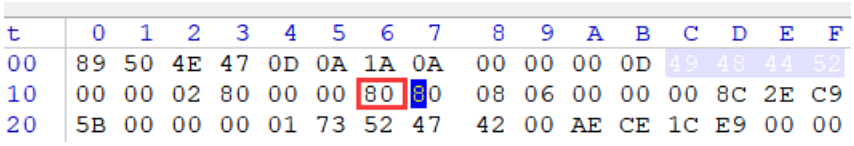
1. 用winhex打开图片，找到png图片前缀IHDR



图片前缀后面各8位的16进制数字就是就是图片宽度和高度



修改图片高度（02 --> 80）



放大图片向下滑动即可看见flag

flag{H@v3_Y0u_
1e@rned_H0w_T0_H!
de_He1ght}

0x2将flag隐藏在字节中

将flag藏在侧边栏的字符串中，这一类的

用WinHex打开图片后，用搜索文本flag开头；

如果有，仔细看一下后面的字符串，

如果没有，那就是真的没有，尽早试试其他方法吧！

0x3文件开头和结尾的补写

有的图片文件在用WinHex打开后会发现文件开头或者结尾不全，

1. 将文件开头或结尾补全
2. 将图片保存，再打开图片就可以了

附：常见图片文件的开头和结尾

文件格式	文件头	文件尾
JPEG (jpg)	FFD8FF	FF D9
PNG (png)	89504E47	AE 42 60 82
GIF (gif)	47494638	00 3B

4. LSB隐写(最低有效位)

需要**先配置好Java环境**，以及工具***Stegsolve.jar***

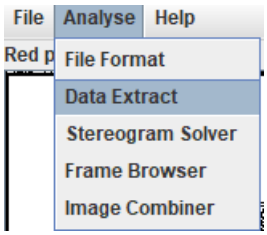
File Format:文件格式，这个主要是查看图片的具体信息
Data Extract:数据抽取，图片中隐藏数据的抽取
Steregram Solve:立体试图 可以左右控制偏移
Frame Browser:帧浏览器，主要是对GIF之类的动图进行分解，动图变成一张张图片，便于查看
Image Combiner:拼图，图片拼接

具体操作：

用Stegsolve.jar打开图片；

先点击下面的切换按钮，观察图片有无异常；

再进行如下操作；



勾选R，G，B的最低位即第0位，以及右侧选择框中的`LSB First`；

接着点击下方的`Preview`按钮，在文本框中查看有无flag；

如果没有，选择`Save Bin`选项，将图片导出，再次查看图片；

可能会得到一个flag或藏有flag的二维码。

5. F5-steganography工具的使用

打开命令行，切到F5文件所在所在的位置

在命令行中输入

```
java Extract 图片的绝对路径/123.jpg -p 密码
```

然后打开F5文件夹中的output.txt文件查看flag

6. Silenteye的使用

1. 使用***silenteye***打开图片；
2. 点击两次**decode**即可