CTF图片隐写入门

原创

huster0828 于 2020-11-10 20:08:47 发布 1054 收藏 5

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/huster0828/article/details/109604969

版权

判断图片类型

根据图片的后缀名不能准确的判断图片的类型，但通过图片文件头部分析能获得图片的类型。（查看的时候打开命令行终端，cd到图片目录下,binwalk一下就ok啦）

在windows下安装ubuntu子系统，c盘路径在/mnt/c中

```
1.jpg
huster@LAPTOP-4J27RSD4:/mnt/c/study/01$ binwalk 1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

常见图片文件的文件头标志

1.JPEG

- 文件头标识(2 bytes):0xff.0xd8(SOI)(JPEG文件标识)
- 文件结束标识(2 bytes):0xff,0xd9(EOI)

2.TGA

- 未压缩的前5字节 00 00 02 00
- RLE压缩的前五字节 00 00 10 00 00

3.PNG

- 文件头标识(8 bytes) 89 50 4E 47 0D 0A 1A 0A

4.GIF

- 文件头标识(6 bytes) 47 49 46 38 39(37) 61

5.BMP

- 文件头标识(2 bytes) 42(B) 4D(M)

常规图片隐写

图片隐写常见的两种：

- 插入：插入往往利用文件格式的无关数据或者空白区域，放置需要的数据，不会改变原始数据，只是增加了隐写的内容
- 替换：替换的经典例子就是LSB替换方法，把每个字节最低有效位变换，不会改变文件大小，但是源文件发生了变化

不同文件合并

这种类型首先需要binwalk一下，会出现不同类型文件，再foremost分离一下就可以得到flag啦

图片合并

这种类型的隐写也是比较容易发现的，如果发现图片是jpg的话，观察文件结束符之后的内容，查看是否有附加内容，正常图片都会是FF D9结尾的。

文件中插入字符

这种类型一般会出现在文件的头部或者尾部，发现之后解码就行啦

JPEG图片隐写

JPEG图片格式分为两部分：标记码和压缩数据，标记码有字节，高字节固定为0xFF。

- JPEG文件以0xFF 0xD9结束
- 如果后面还有信息，可以用winhex复制出来，保存为新的文件
- 从文件有可以看出文件格式

PNG(便携式网络图形)

该图片的特点是存储图片的方式。该类型的图片会通过无损压缩的方式存储图片。图片将会把图片源码使用zlib的压缩编码后分为IDAT块进行存储。每个IDAT能够存储65524大小的数据

BMP图片隐写

BMP是windows操作系统中的标准图像，文件格式可分为两类：设备相关位图和设备无关位图使用非常广泛，它采用位映射存储格式，除了图像深度可选以外，不采用其他任何压缩，因此BMP文件所占用的空间很大，由于BMP文件格式是windows环境中交换与图有关的数据的一种标准，因此在windows环境中运行的图形图像软件都支持BMP图像格式。

BMP图像与其他图像的主要区别是能够直接从源代码中获取与图像相关的信息，而不是压缩数据

BMP图像隐写——LSB隐写

- 因为BMP图片特征是对图像进行映射存储，所以最常见隐写方式为LSB隐写
- LSB也就是最低有效位
- LSB隐写原理就是图片中的像数一般是由三种颜色组成及三原色，由这三种颜色可以组成其他各种颜色。
- 常见的LSB隐写也分为两类：
  - 将最低位次层次的二进制代码直接替换位flag的ascii码
  - 在最低位层次中加入一张带有flag的图片

GIF图片隐写

这一类需要注意的是，有的题目可能会把gif的后缀改成jpg,这种情况用binwalk查看一下，如果是gif，就将后缀名改为gif,然后再一帧一帧的观察。