

CTF常用隐写套路

转载

小毛毛2013 于 2018-08-24 13:34:23 发布 14130 收藏 42
分类专栏: [安全](#)



[安全 专栏收录该内容](#)

5 篇文章 0 订阅
订阅专栏

隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。隐写术的英文叫做Steganography，来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。

在CTF题目中，图片隐写题属于杂项的一部分，题目较为简单。本文大致梳理了下CTF比赛中图片隐写题的常用套路，如果未能看出题目破题点，可按照以下方法顺序逐一尝试：

1. 查看图片基本信息（对应题目难度：低）

该类题通过查看图片基本信息，可以直接获取FLAG，主要方法如下：

- A) 右键查看图片属性，检查图片简介、备注中是否有FLAG；
- B) 将图片用编辑器工具打开，如使用记事本、notepad+、winhex，检查是否包含FLAG；

```
00000F30 60 09 0B F0 01 53 70 1B 58 61 2B 51 A0 5F 4A D7 ` õ Sp Xa+Q _Jx
00000F40 01 EB C4 11 8D 59 03 54 F6 00 10 B0 68 7B 80 03 ëÄ Y Tö °h{€
00000F50 83 83 8F 4B C5 09 63 01 91 E6 B7 01 9E 07 0D 0E ff KÅ c `æ· ž
00000F60 00 05 11 90 92 23 80 10 11 F6 96 7C 8A 5F 03 52 ' #€ ö-|Š _R
00000F70 05 31 A0 9D 83 E0 03 38 A0 A2 4E D6 34 DE 23 AA 1 fà 8 çNÖ4P#ª
00000F80 E9 B3 00 0C C0 02 54 30 01 47 B5 92 25 30 05 A7 é³ À T0 Gµ' %0 $
00000F90 06 19 5E 91 05 6E 80 00 3E 00 12 58 F0 1A 47 20 ^ ` n€ > Xõ G
00000FA0 96 90 77 33 00 E0 D0 5A AF 5A 03 D5 35 08 62 90 - w3 àÐZ`Z Ö5 b
00000FB0 19 28 A0 4B 4D E1 00 82 F2 73 9A 20 05 FF 63 A7 ( KMá ,òsš ýcŠ
00000FC0 4F C0 01 8D 07 0B 5D 78 05 17 50 00 D5 90 01 0F CÀ ]x P Œ
00000FD0 F0 00 09 45 5F 49 68 02 57 20 77 5E 82 60 17 B0 õ E_Ih W w^, ` °
00000FE0 B0 CE F2 00 9A 27 46 32 20 90 89 F2 00 45 88 09 °îò š'F2 %ò E^
00000FF0 B8 D7 03 C7 94 01 28 F0 00 28 90 50 17 E0 05 5C ,x ç" (õ ( P à \
00001000 B4 07 E4 48 B1 82 70 01 6F C7 21 57 1A B0 84 71 ' àH±,p oç!W °,,q
00001010 05 45 38 79 9A 10 07 40 20 07 F6 29 44 24 80 06 E8yš @ ö)D$€
00001020 AE 40 83 38 9B B3 35 1A 04 8B D0 08 8F 10 09 93 @f8>³5 <Ð ``
00001030 A0 B3 42 CB 7D 81 00 00 3B 74 68 69 73 5F 69 73 °BË} ;this_is
00001040 5F 79 6F 75 72 5F 66 69 72 73 74 5F 73 74 65 67 _your_first_steg
00001050 6F 0A FLAG o
```

2. 多层文件（对应题目难度：中）

玩CTF的大概都听过一个神器 - stegsolve，用它把图片打开，该软件也有两种用途：

- A) 一直接右箭头（或者左箭头），说不定就会出来一个二维码；
- B) 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，在软件功能选项中查看Analyse→Data Extract，逐个调试。



3. 复合文件（对应题目难度：中）

CTF比赛中经常碰到png文件中复合其他文件的情况，如就是图片后面再放点压缩包、txt文档、或者再添加一张图片，具体操作方法如下：

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

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

```
copy /b a.jpg+b.jpg c.jpg
```

解题思路：通常这类图片比较大，可将图片后缀改为zip或者rar，解压即可。也可以用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；

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，用winhex找第一张图片的尾部，然后把第二张图片的头给加一下，再进行分离操作。

4. 改图片高度（对应题目难度：中）

CTF比赛中可利用16进制编辑工具更改图片的高度，使图片只显示一部分，下面的部分被隐藏，嗯，这是个藏东西的好办法！

当以上方法均不可以得到FLAG，且图片长宽比例诡异时，可以尝试改图片大小，下面介绍找图片宽度和高度的标志位的方法：

A) 对于png文件，其第二行第六列是高度位，改这一位即可；

B) 对于其他格式图片，可以先看看图片的属性，得到宽高值，转成16进制数，搜索该16进制值就能找到标志位了；

本文仅列举了几种博主目前遇到的CTF图片隐写套路，欢迎大家补充!