图片隐写

转载

DING8838203 于 2016-10-10 14:41:00 发布 257 收藏
文章标签： java 密码学
原文链接：http://www.cnblogs.com/Sm411Veg/articles/5945752.html

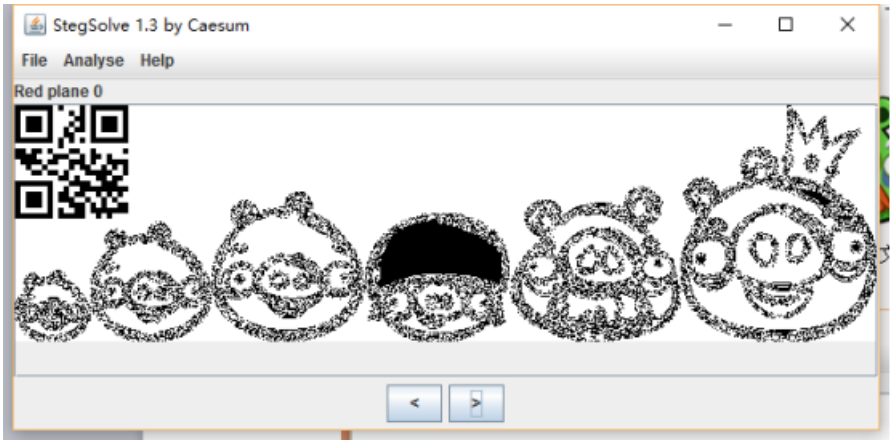
信息安全的一个分支是信息隐藏与传递，当年很火的图种就是其中之一，而作为最易于使用的是图片隐写，在各种CTF中，也有出现

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”。

0x0001

一个24位的位图中的每个像素的三个颜色分量（红，绿和蓝）各使用8个比特来表示。如果我们只考虑蓝色的话，就是说有2^8种不同的数值来表示深浅不同的蓝色。而像11111111和11111110这两个值所表示的蓝色，人眼几乎无法区分。因此，这个最低有效位就可以用来存储颜色之外的信息，而且在某种程度上几乎是检测不到的。如果对红色和绿色进行同样的操作，就可以在差不多三个像素中存储一个字节的信息。

这个图片是很经典的最低有效位的隐写，来自于实验吧隐写题目（侵删），拿到图片先考虑最低有效位的隐写，因为比较常见且容易解决，新手下载一个StegSolve，这需要搭建一个JAVA环境，然后需要简便操作即可发现端倪



这里会发现在红色 plane0 模式下显示了一个二维码。扫码即可得flag

0x0002

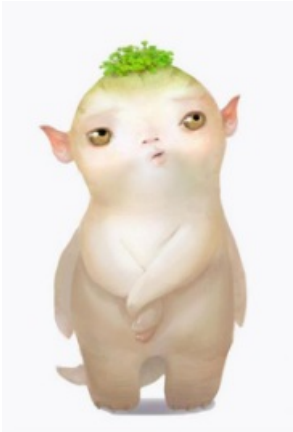
还有一种最常见的是图种形式，其中之一就是文档格式变换，在jpg或者png格式下是一个图片，在别的格式下就不一样了，或者txt里乱码藏着key，或者rar、zip解压后隐藏文件

0x0003

还有最常见的叠图，俩图相叠，下层图片内容就被隐藏，具体细节处不赘述，需新手自己摸索，只提供思路

0x0004

再有就是看到一个图片先观察大小，发现大小和他的清晰度不太成正比，这时候就需要考虑包含文件



这个就是一个典型，修改为zip后缀后发现key.txt文件，但是有解压密码，无法解压，kali Linux集成了binwalk，提取，提取txt文件，然后发现加密，winhex 16进制文件查看后发现加密数字，改后拿到flag

0x0005

接下来是一些各种格式图片的一些规律与格式

jpg
头: FF D8 FF E0 00 10 4A 46
后缀FFD9

gif 图片的速度也可用Stegsolve调节

隐藏在详细信息中

gif 文件头 GIF89a 47 49 46 38 39 61

png 文件头 、IHDR块、PLTE块、tRNS块、IDAT块、文件尾
89 50 4E 47 0D 0A 1A 0A
IHDR(00000008~00000020):
块长度，ihdr标识，宽，高
（可选数据块）00000021~0000002F
文件尾：45 4E 44 AE 42 60 82

zip文件头：
zip伪加密，在文件名后 50 4B 01 02 3F 00 14 00 0*（改成 00）
504B0304

摩斯密码通常三个元素

bmp（http://www.cnblogs.com/tiandsp/archive/2012/10/22/2734552.html

）

十进制1078，实际数据开始的偏移是。
第一排a-d
文件头42 4D
大小为0006395E

steghide
在文件中隐藏数据
steghide --embed -cf /root/Desktop/1111.jpg -ef /root/Desktop/embeddate
检查图片中隐藏的信息
steghide info /root/Desktop/1111.jpg
steghide extract -sf background.jpg

wav：
52 49 46 46 文见头 紧接大小（倒序）
Foremost （ foremost -v -i /root/Desktop/oddpic.jpg -o /root/aaa） 目录必须为空
支持恢复如下格式：avi, bmp, dll, doc, exe, gif, htm, jar, jpg, mbd, mov, mpg, pdf, png, ppt, rar, rif, sdw, sx, sxc, sxi, sxw, vis, wav, wmv, xls, zip。

mp3：mp3stego
decode -X -P simctf music.mp3

转载于:https://www.cnblogs.com/Sm411Veg/articles/5945752.html