CTF-Misc之隐写术

原创

weixin_45982862 于 2020-11-30 20:02:08 发布 168 收藏 1

文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_45982862/article/details/110398544

CTF-Misc之隐写术

如题，介绍几种常见的隐写术，一般都是在题目给出的文件是图片或压缩包时可以考虑考虑。

直接附加

这里要先介绍一下常见文件类型的文件头和文件尾。

PNG：文件头，89 50 4E 47；文件尾，AE 42 60 82

JEPG：文件头，FF D8 FF；文件尾，FF D9

GIF：文件头，47 49 46 38；文件尾00 3B

ZIP：文件头，50 4B 03 04；文件尾50 4B

RAR：文件头，52 61 72 21；文件尾

我们可以通过二进制编辑器在文件尾后添加任意内容，比如说一个字符串甚至是其他文件。这样修改后的图片用图片查看器不会看出任何变化。

需要提取藏在里面的文件可以使用Binwalk等工具分离。

LSB

LSB，即Least Significant Bit（最低有效位）。

大多数PNG图片都由R G B三种颜色组成，每个颜色用8位数据表示，如果只是修改其中的最低位，我们通过肉眼是无法判别出来。

这时可以使用stegsolve等工具提取出隐藏信息。

EXIF

EXIF，即Exchangeable Image File Format（可交换图像文件格式）。

EXIF可以用来记录数吗照片的属性信息和拍摄数据等，如电脑上随便一张图片右击查看属性就能看到这张图片的拍摄时间等。

要查看EXIF信息可以通过exiftool等工具。

解题思路

1.如果给的是GIF的图片可以分帧看看出来的图片里面有没有藏二维码什么的。或者就是很多张图片代表着一个密码，例如攻防世界里的一道新手题，分出来的图片都是黑白的，又有很多张，可以考虑是不是摩斯密码。

2.拿到图片先右击查看下属性，有时候可能flag直接就藏在属性里面了。要是还花了很多时间去想些别的有的没的岂不是很亏。

3.再然后可以拿到010 Editor里面看看文件头文件尾什么的，看看是不是与其后缀匹配，不对的话先改过来。或者看看里面有没有藏些什么字符串或者图片等。

4.还是没有思路的话就放到stegsolve里面看看文件信息，里面可能藏了flag或者相关的信息，也可以切换不同的通道看看有没有隐藏些什么东西。如果是PNG图片的话还可以看看是不是LSB。

4.最后可以排除一下是不是EXIF啦。

这里只简述我做题这么久来常见的几种隐写方法，毕竟我做过的题也不多。总的来说还是要多结合题目的提示方向思考思考。

常用工具

010 Editor

一款常见的十六进制编辑器，可以在二进制下查看文件。

下载可以参考这篇知乎：https://zhuanlan.zhihu.com/p/31195150

Binwalk

Kali里面自带了。

使用方法可参考这篇文章：https://blog.csdn.net/wxh0000mm/article/details/85683661

exiftool

apt-get install exiftool

Kali终端输入此命令即可安装。如果失败了的话一般update一下就没问题了。

安装和使用方法可参考这篇文章：https://blog.csdn.net/weixin_34393428/article/details/88679127

stegsolve

这个用起来比较麻烦，需要配置JAVA环境，但配好后不需要安装了，这就是一个jar包可以直接用。

下载地址：http://www.caesum.com/handbook/Stegsolve.jar

这是使用方法：https://www.cnblogs.com/cat47/p/11483478.html

GIFsplitter

用来给给GIF文件分帧的。

这个我之前在博客上没有找到下载链接，好像是在百度知道还是哪里下到的，不是垃圾软件，应该是没问题的，用着也挺好。这里分享一下吧，实在找不到什么正规分享可以试试我下到的这个：

https://pan.baidu.com/s/1OGAmaeBP4osrhv4cylHOcA
提取码：1jz6

使用方法很简单这里就不赘述了。