CTF隐写题常规思路

原创

俩儿 于 2020-05-11 16:01:26 发布 531 收藏 4

图片隐写

1.查看图片不能正常打开
（1）windows/kali linux中都不能正常打开————格式不正确或者文件有缺损
（2）windows可以正常打开 kali linux不能正常打开————图片宽高有问题
2.图片可以正常打开
（1）排查属性中有无隐藏信息
（2）丢进kali binwalk看有没有隐藏文件 有就foremost分离
（3）没有异常丢进010 Editor查看尾部有没有隐藏信息

常见问题

1.压缩包伪加密
通常出现在压缩包有密码，但又没有任何密码的线索时
原理：在文件头的加密标志位做修改，使文件被识别为加密压缩包
方法：找50 4B 01 02后14 00 的后面改为 00 00
或者在kali中binwalk -e直接解压

2.文件头损坏
文件头缺损是常见的问题
常见文件头
JPEG (jpg) 文件头：FF D8 FF 文件尾：FF D9

PNG (png) 文件头：89 50 4E 47 文件尾：AE 42 60 82

GIF (gif)　文件头：47 49 46 38 或GI F8 9A 文件尾：00 3B

ZIP (zip) 文件头：50 4B 03 04 文件尾：50 4B

HTML (html) 文件头：68 74 6D 6C 3E

Wave (wav) 文件头：57 41 56 45

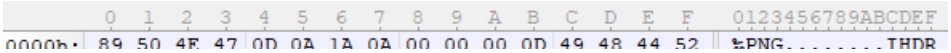
AVI (avi) 文件头：41 56 49 20

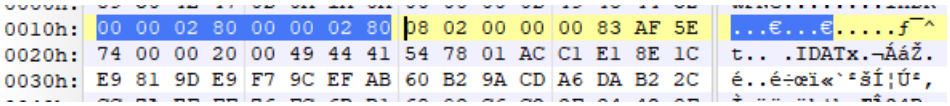
bmp　文件头：42 4D

RAR Archive (rar) 文件头：52 61 72 21

Photoshop (psd) 文件头：38 42 50 53

3.修改图片宽高
图片宽度高度被修改是常见的问题





4.Stegsolve的使用

Stegsolve是非常好用的隐写神器

举个例子：

根据题目给的线索