CTF杂项思路总结

原创

AndSonder 于 2020-06-28 19:53:52 发布

分类专栏： 白 帽 子 文章标签： CTF

本文链接：https://blog.csdn.net/python_LC_nohtyp/article/details/107006168

CTF杂项知识点总结

文章目录

前言

最近参加了学校内部的CTF比赛，还是太菜了。现学现卖了好多东西。不过感觉还是学到不少东西。多参加参加比赛还是有好处的哈哈。第一次在学校通宵，为一件事情付出努力的感觉还是不错滴。

图片隐写方式总结

1. 属性隐藏信息

右击打开文件可能发现神奇的东西

2. Hex隐藏信息

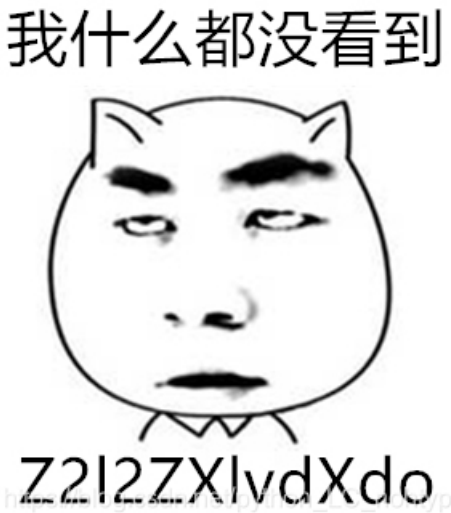
使用010editor或者winhex打开图片的hex格式，信息直接隐写在图片格式之中。比如我之前做的一道题，里面就隐写了JSFUCK编码，有的题目直接就把Flag隐写在里面。

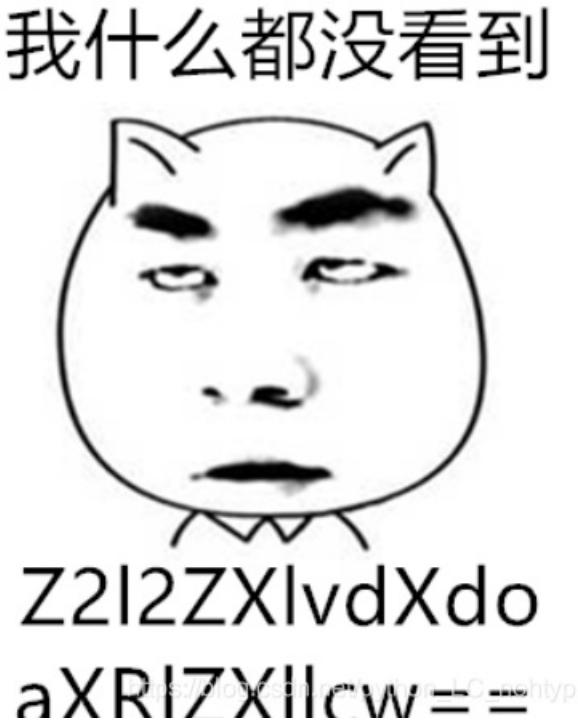
3. 颜色通道隐写

大体的形式就是根据图片的不同通道的颜色不同寻求flag，这种题目我展示还没遇到过，遇到了再回来补充
使用工具：Stegsolve.jar

4. 长度隐写

图片的长度被手动修改导致隐藏一部分的信息，我们可以通过修改会长度信息解答，比如这样的（这个是已经被我修改过的了）





这种题目一个很重要的技巧就是搜索图片的长度的hex码，因为图片的格式其实挺难看的，直接搜索长度或者宽度往往是最有效的方法。

这里总结一下常用的图片开头：

文件格式	文件头
JPEG (jpg)，	文件头：FFD8FF
PNG (png)，	文件头：89504E47

文件格式	文件头
GIF (gif)，	文件头：47494638
TIFF (tif)，	文件头：49492A00
Windows Bitmap (bmp)，	文件头：424D
CAD (dwg)，	文件头：41433130
Adobe Photoshop (psd)，	文件头：38425053
Rich Text Format (rtf)，	文件头：7B5C727466
XML (xml)，	文件头：3C3F786D6C
HTML (html)，	文件头：68746D6C3E
Email [thorough only] (eml)，	文件头：44656C69766572792D6
Outlook Express (dbx)，	文件头：CFAD12FEC5FD746F
Outlook (pst)，	文件头：2142444E
MS Word/Excel (xls.or.doc)，	文件头：D0CF11E0
MS Access (mdb)，	文件头：5374616E64617264
WordPerfect (wpd)，	文件头：FF575043
Adobe Acrobat (pdf)，	文件头：255044462D312E
Quicken (qdf)，	文件头：AC9EBD8F
Windows Password (pwl)，	文件头：E3828596
RAR Archive (rar)，	文件头：52617221
Wave (wav)，	文件头：57415645
AVI (avi)，	文件头：41564920
Real Audio (ram)，	文件头：2E7261FD
Real Media (rm)，	文件头：2E524D46
MPEG (mpg)，	文件头：000001BA
MPEG (mpg)，	文件头：000001B3
Quicktime (mov)，	文件头：6D6F6F76
Windows Media (asf)，	文件头：3026B2758E66CF11
MIDI (mid)，	文件头：4D546864

5. 文件隐藏

这个是比较常见的手法了，主要是使用bindwalk、foremost 或者 steghide去扫描隐藏的文件。这些工具在正常的kali系统中都有内置，steghide有的的可能没有，我用的Windows版的

流量包隐藏

使用wireshark解析即可。学会如何使用wireshark这个工具

音频文件隐藏

…待续