

隐写术总结篇幅之（一）

原创

Enoki 于 2019-02-23 00:35:29 发布 962 收藏

文章标签: [ctf 隐写](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43721621/article/details/87887818

版权

#ctf隐写术总结篇幅之（一）

关于隐写, 强烈推荐《数据隐藏技术揭秘》一书。多刷博客, 多看视频, 多看书, 多实践, 相信终能达成目标。

隐写常用工具

binwalk

固件分析工具, 常用于路由器逆向, 后门分析, 或识别二进制图像中的嵌入式文件和可执行代码;

命令: binwalk 文件名

常用参数:

-e (按预定义配置文件提取extract.conf, 通常提取rar)

-dd=xxx(提取某种类型的文件, xxx为文件类型, 如-dd=xxx=jpg)

-M 递归提取, 需要和-e和-D配合 (例, -Me)

stegsolve

●图片通道查看器

Analyse'下拉菜单:

FjJe Format :查看文件格式和参数信息,有时候flag会写在图片信息里Data Extract :数据提取,如LSB隐写等在这个选项中提取信息

Stereogram solver :立体视图,可以左右移动控制偏移量

Frame Broswer :逐帧浏览,如查看快速闪过的GIF图中的flag

Image Combiner :图片结合,可以对两张图片做xor、add、sub等运算

。

。

等等。

mp3隐写, 音频隐写等等的工具介绍后面会有说明, 这里就不在详细列举了。。

文本隐写种类总结

文本隐写术的方法主要可以分为以下四种:

●文档格式微调法:行移、字移、修改字符颜色等

●空格回车标点法:添加空格和回车, 添加标点符号

●字符特征法:字体替换、汉字结构

●自然语言法:同义词替换、句法变换

文档格式微调法

行移

行移是指调整文本文件中的垂直行距来隐藏信息的方法

嵌入信息的行的相邻_上下两行位置不动，作为参考，然后该嵌入信息的行上移，表示嵌入“1”，行下移,表示嵌入信息"0"。

-字移

字移是指通过将某行的字符进行水平移动来隐藏信息

如将一个单词左移或右移，而与其相邻的单词则不进行移动，可以作为提取隐藏信息时的参考，如规定左移代表“1”,右移代表“0”。

-修改字符颜色

改变文本字符颜色的十六进制颜色码微调，来嵌入信息。

空格标点符号法

添加空格和回车

基于空格和回车的隐写术是利用人类视觉系统对微小间隔不敏感的特点而设计的

与字移、行移等不同的地方在于，字移、行移等操作适用于利用格式化文档(如word)传递信息的过程，而对于纯文本文档(如txt)不能进行微调操作，这时可以考虑利用空格或是回车来隐藏信息。

与字移相比，字移引起的间隔往往是人类肉眼所捕捉不到的，但空格带来的间隔如果插入为止不当则会引起怀疑(如汉语中汉字与汉字间通常是没有间隔的，过多的间隔会引起注意，因此该方法通常适用于英文文本)，因此插入位置的选择往往是该类隐写术的关键。

逗号可为1，句号可为0以此隐藏

对标点改变字体隐藏信息

字体特征法

通过两种不同的字体来实现0和1转换。

汉字结构的间距来隐藏信息

自然语言法

同义词替换（绝对同义词，相对同义词）

语法变换（宾语前置，谓语后置，定语后置等实现0,1隐藏）

以上文本隐写的方法各有千秋，优点和缺点还有限制条件。这里就不说了。。打字有点累。

-- 图片隐写

双图隐写

这个在ctf有以下基础的三种

考察形式1：通过文件格式格式进行分析图片1—获得图片2

考察形式2：通过把图片1，对比和某种运算—对比的差异或来获得隐藏信息

考察3：把图片1，对文件格式等进行分析—图片1+图片2—通过某种运算—对比差异来获取信息

考察4：对文件格式进行分析—多个图片+图片2—某种运算-对比差异获取信息

图像拼接格式

可以查看一个图片里的十六进制，通过hex发现，图一数据里里还有另外一个图片的数据，拿出来，保存即可获得信息。

图层叠加

多个图层叠加在一起，然后形成了出题的图片

图像运算

加减乘除，逻辑运算，按比混合和位移

文件直接拼接

特征

- 1，给提示有另一文件隐藏
- 2，只有一张图片

修改文件格式

特征

- 1，分离图片，却无法打开
- 2，原图无法打开，多由压缩包分离得到

文件间接拼接

特征

图像结尾往往存在大量冗余。

双图层叠加

特征

- 1，图像缩略图和放大图不一样
- 2，用winhex打开，可以看到图片被ph0toshop编码过的标志。

双图像运算

特征

- 1，给的两张图片看起来完全相同
- 2，两张图片不同，但属于同一style

一图分多图

特征

- 1，每张图片各自能分析出信息，则考虑拼接信息
- 2，每张图片各自无法分析出有效信息，则考虑多图运算。

今天先介绍到这里，，由于0:27了，健康为重，祝大家一路顺风。