CTF随笔——隐写术

原创

逍遥成居士 于 2018-04-17 21:04:49 发布 3722 收藏 31
分类专栏： CTF 文章标签： CTF 信息安全 隐写术

本文链接：https://blog.csdn.net/lcx772092761/article/details/79898264

一、什么是隐写术

隐写术就是“”*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”。——维基百科*
翻译成人话就是，我把原来的信息或者东西放在另外的不相干的东西里，这样不知情者就不会知道我真正想表达的东西，举个栗子，我想给妹子送情书，但是我不想让其他人知道我给妹子送情书，于是我把这封情书放在一个西瓜里，这样不知情的人就会以为我给妹子送西瓜而不是送情书了2333333……
（现在JPEG 2000可执行任意代码漏洞已经加入Stego（杂项）豪华漏洞套餐）

二、隐写术常用的工具

这里只列举一下我用过或知道的一部分工具，不全和有错误的地方还请各位大佬留言指正。

1、压缩软件

这个就很常见了，比如winrar，360压缩，7-zip等等……

2、十六进制读写器

隐写术用到的工具比较小众，这里只列举我常用的一些工具，后面会不定时更新~

1、HxD（Windows）

用于查看修改文件的16进制代码

2、hexeditor（Linux）

也是用于查看和修改文件的16进制代码

3、binwalk（Linux）

用来分析文件信息，可以轻易的查看文件中是否包含其他隐藏文件，简单用法：
Linux下使用命令操作
`binwalk filename` 分析构成
`binwalk -e filename` 自动解压已知文件格式
`binwalk -D=[extension] filename` 根据后缀名解压，比如`-D=zip`等

4、StegSolve（Windows）

神器！能够对常见的图片格式进行偏移、LSB 提取、帧提取、像素偏移、数据提取，对两张图片进行结合等等，基本常见的分析需求都包含了。

5、Stegdetect（Windows）

用于检测 JPEG 文件中是否包含隐藏内容并尝试分析隐藏内容通过哪个隐写工具嵌入，使用方式：

- `stegdetect [-nqV] [-s <float>] [-d <num>] [-t <tests>] [file.jpg ...]`
- -q 仅显示可能包含隐藏内容的图像。
- -n 启用检查 JPEG 文件头功能，以降低误报率。如果启用，所有带有批注区域的文件将被视为没有被嵌入信息。如果 JPEG 文件的 JFIF 标识符中的版本号不是1.1，则禁用 OutGuess 检测。
- -s 修改检测算法的敏感度，该值的默认值为1。检测结果的匹配度与检测算法的敏感度成正比，算法敏感度的值越大，检测出的可疑文件包含敏感信息的可能性越大。
- -d 打印带行号的调试信息。
- -t 设置要检测哪些隐写工具（默认检测 jopi），可设置的选项如下： j 检测图像中的信息是否是用 jsteg 嵌入的。 o 检测图像中的信息是否是用 outguess 嵌入的。 p 检测图像中的信息是否是用 jphide 嵌入的。 i 检测图像中的信息是否是用 invisible secrets 嵌入的。
- -V 显示软件版本号。
  官网打不开，可以上GitHub或者直接使用一个编译好的Windows版本

6、Outguess（Windows）

这个是用来提取 JPEG 文件中使用 Outguess 算法的加入的隐藏信息，GitHub 或者编译好的Windows版本

7、JPHS（Windows）

用于对 JPEG 文件进行 Jhide 算法的隐写或提取，下载链接

8、MP3Stego（Windows）

对于MP3音频文件的隐写或提取，如：有一个名字叫“123.pm3”的文件，打开以后听是听不到任何信息的，我们可以用这个工具来进行信息的提取，使用命令`decode -X -P 123.mp3`就可以提取出一个信息文件（一般是txt），使用命令`encode -E 123.txt -P pass 123.mp3`是把123.txt文件写入123.mp3文件中下载连接

9、MSU StegoVideo

可以对视频文件进行隐写和提取的工具，具体我没有用过，大家可以去官网看一下

10、其他

在线二维码扫描
各种使用的工具

三、常见题目和注意事项

1、JPG文件

一个完整的JPG文件由`FF D8`开头，`FF D9`结尾，会忽略`FF D9`以后的内容，所以可以在JPG文件中加入其他文件，比如flag……
遇到这种题常用的解决方法有这么几种，用`Binwalk`分析出来里面隐藏的文件以后，把后缀名强制改为对应的文件后缀，但是这种办法不适用一个JPG隐藏多个文件或不知道后缀名的题，还可以使用`Binwalk`工具自动拆分功能，也可以使用`Winhex`等十六进制工具手动拆分。

2、GIF文件

GIF文件开头是`GIF8`四位，具体可查阅GIF文档。

3、Zip文件

zip文件加密一般三种情况
第一种是真的使用密码加密，这种情况只能在其他地方寻找到密码
第二种是伪加密，讲原理之前，先了解一下`zip`文件里面的构成以及含义

压缩源文件数据区：

`50 4B 03 04`：这是头文件标记
`14 00`：解压文件所需 pkware 版本
`00 00`：全局方式位标记（有无加密）
`08 00`：压缩方式
`5A 7E`：最后修改文件时间
`F7 46`：最后修改文件日期
`16 B5 80 14`：CRC-32校验
`19 00 00 00`：压缩后尺寸
`17 00 00 00`：未压缩尺寸
`07 00`：文件名长度
`00 00`：扩展记录长度

压缩源文件目录区：

`50 4B 01 02`：目录中文件文件头标记
`3F 00`：压缩使用的 pkware 版本
`14 00`：解压文件所需 pkware 版本
`00 00`：全局方式位标记（有无加密）
`08 00`：压缩方式
`5A 7E`：最后修改文件时间
`F7 46`：最后修改文件日期
`16 B5 80 14`：CRC-32校验
`19 00 00 00`：压缩后尺寸
`17 00 00 00`：未压缩尺寸
`07 00`：文件名长度
`24 00`：扩展字段长度
`00 00`：文件注释长度
`00 00`：磁盘开始号
`00 00`：内部文件属性
`20 00 00 00`：外部文件属性
`00 00 00 00`：局部头部偏移量

压缩源文件目录结束标志：

`50 4B 05 06`：目录结束标记
`00 00`：当前磁盘编号
`00 00`：目录区开始磁盘编号
`01 00`：本磁盘上纪录总数
`01 00`：目录区中纪录总数
`59 00 00 00`：目录区尺寸大小
`3E 00 00 00`：目录区对第一张磁盘的偏移量
`00 00`：ZIP 文件注释长度
对于伪加密来说，把压缩源文件目录区的全局方式位标记改为`90 00`就可以直接打开了，但是如果提示文件损坏，那么就说明这个文件不是伪加密
第三种情况是真加密，但是我们不需要暴力破解，而是通过一种叫做`CRC32碰撞`的攻击方式。
这种攻击方式不同于暴力破解，暴力破解的枚举的是密码，而`CRC32碰撞`枚举的是内容，假如一个加密的压缩包内部只有一个很小的文件，而它的CRC32值与zip文件的CRC32的值一样的，那么我们就可以去使用`CRC32碰撞`去破解，这里从网上找到了一个大佬写的破解脚本GitHub代码链接

4、双图问题

对于两张图片的问题，可以用`StegSolve`工具对双图进行各种操作，看属否获取有用的信息，这类题可能与密码、二维码等有关。

5、F5 隐写

这一个隐写算法原理比较难，有兴趣的同学可以看看这一篇博客，这种题做法是，首先下载`F5 隐写`解密工具，然后使用命令`java Extract ../fileName.jpg -p fileName`就会生成解密以后的文件。

6、jphide隐写

这个隐写原理如下：
Jphide是基于最低有效位LSB的JPEG格式图像隐写算法，使用JPEG图像作为载体是因为相比其他图像格式更不容易发现隐藏信息，因为JPEG图像在DCT变换域上进行隐藏比空间域隐藏更难检测，并且鲁棒性更强，同时Blowfish算法有较强的抗统计检测能力。
由于JPEG图像格式使用离散余弦变换(Discrete Cosine Transform，DCT)函数来压缩图像，而这个图像压缩方法的核心是：通过识别每个8×8像素块中相邻像素中的重复像素来减少显示图像所需的位数，并使用近似估算法降低其冗余度。因此，我们可以把DCT看作一个用于执行压缩的近似计算方法。因为丢失了部分数据，所以DCT是一种有损压缩(Loss Compression)技术，但一般不会影响图像的视觉效果。
以上内容以及该算法的解法引用自这里若侵删

四、总结

隐写术是个非常好玩的脑洞题，设计各个方面的知识，虽然有套路，但是套路可以嵌套套路，题目解法千变万化，目前我也仅仅是入门阶段，上述内容也比较适合新手入门使用，若有欠缺的地方，还请各位大佬批评指正。

> 维基百科
> https://zh.wikipedia.org/wiki/%E9%9A%90%E5%86%99%E6%9C%AF
> 百度百科
> https://baike.baidu.com/item/%E9%9A%90%E5%86%99%E6%9C%AF