[网络安全自学篇]MISC-图片隐写

原创

D.T.69 于 2021-05-12 11:32:55 发布 737 收藏 6
分类专栏： 安全学习规划 文章标签： 安全

什么是隐写术？

隐写术（Steg）就是一种保密通信技术，将秘密信息隐藏于可公开的普通载体中进行传送，实现隐蔽通信，可以让计划者之外的人即使得到传递的信息，也不知道隐秘的数据，从而达到安全传递秘密消息的目的，保证通信安全。

CTF隐写术常用的信息载体类型：

1.图片文件（jpeg/png/gif…）
2.文档文档（txt/pdf/doc..）
3.音频文件（mp3/wav…）

认识常见文件头标识
FFD8FF ----- JPEG (jpg)
89504E47 ----- PNG (png)
47494638 ----- GIF (gif)
424D ----- Windows Bitmap (bmp)
504B0304 ----- ZIP Archive (zip)
52617221 ----- RAR Archive (rar)
57415645 ----- Wave (wav)
41564920 ----- AVI (avi)
D0CF11E0 ----- MS Word/Excel (xls.or.doc)
255044462D312E ---Adobe Acrobat (pdf)

工具
Binwalk ：帮助我们识别文件结构
Foremost ： 将多个合并文件分离
Exiftool：读取jpeg 图片的 exif 信息。
Pngcheck：查看 png 图片模块信息。
MP3Stego ： 可以将 wav 文件和需要隐藏的文件合并成一个新的MP3 文件
Stegosolve：神器，通常使用 frame browser 功能来查看图片不同通道，不同色块来分析图片隐藏信息。
注意：运行需要 Java 环境

常见隐写类型

01图片隐写常见的两种

1）图片尾部插入特殊字符串

这种类型的隐写一般最简单也最容易发现，所以一般会配合编码来增加难度。

方法：winhex打开图片，在末尾添加特殊字符串

其他类型可以自行百度一下

06PNG图片IDAT隐写

- 认识PNG图片结构

PNG图像格式文件由一个8字节的PNG文件头标志和按照特定结构组织的3个以上的数据块组成。

文件头：89 50 4E 47 0D 0A 1A 0A

- 四个关键数据块如下：

PNG文件格式中的数据块

数据块符号	数据块名称	多数据块	可选否	位置限制
IHDR	文件头数据块	否	否	第一块
PLTE	调色板数据块	否	是	在IDAT之前
IDAT	图像数据块	是	否	与其他IDAT连续
IEND	图像结束数据	否	否	最后一个数据块

IHDR隐写-IHDR结构

文件头数据块IHDR(header chunk)：它包含有PNG文件中存储的图像数据的基本信息，并要作为第一个数据块出现在PNG数据流中，而且一个PNG数据流中只能有一个文件头数据块。

文件头数据块由13字节组成，它的格式如下表所示。

域的名称	字节数	说明
Width	4 bytes	图像宽度，以像素为单位
Height	4 bytes	图像高度，以像素为单位
Bit depth	1 byte	图像深度： 索引彩色图像：1，2，4或8 灰度图像：1，2，4，8或16 真彩色图像：8或16
ColorType	1 byte	颜色类型： 0：灰度图像，1，2，4，8或16 2：真彩色图像，8或16 3：索引彩色图像，1，2，4或8 4：带α通道数据的灰度图像，8或16 6：带α通道数据的真彩色图像，8或16
Compression method	1 byte	压缩方法(LZ77派生算法)
Filter method	1 byte	滤波器方法
Interlace method	1 byte	隔行扫描方法： 0：非隔行扫描 1： Adam7(由Adam M. Costello开发的7遍隔行扫描方法)

实验：14-IHDR隐写

- 1，看似普通的1.png图片如下：

- 3，我们知道IHDR能够控制图片显示的大小，改变长度

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	02	9C	00	00	02	DD	08	06	00	00	00	FE	1A	5A	œ ÝÞ Z
00000032	B6	00	00	00	04	73	42	49	54	08	08	08	08	7C	08	64	¶ sBIT | d
00000048	88	00	00	00	09	70	48	59	73	00	00	0B	12	00	00	0B	^ pHYs
00000064	12	01	D2	DD	7E	FC	00	00	00	16	74	45	58	74	43	72	ÒÝ~ü tEXtCr
00000080	65	61	74	69	6F	6E	20	54	69	6D	65	00	31	32	2F	31	eation Time 12/1
00000096	39	2F	31	35	6C	F1	55	23	00	00	00	1C	74	45	58	74	9/15lñU# tEXt

- 2，Winhex查看16进制代码：

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	02	9C	00	00	02	DD	08	06	00	00	00	FE	1A	5A	œ ÝÞ Z
00000032	B6	00	00	00	04	73	42	49	54	08	08	08	08	7C	08	64	¶ sBIT | d
00000048	88	00	00	00	09	70	48	59	73	00	00	0B	12	00	00	0B	^ pHYs
00000064	12	01	D2	DD	7E	FC	00	00	00	16	74	45	58	74	43	72	ÒÝ~ü tEXtCr
00000080	65	61	74	69	6F	6E	20	54	69	6D	65	00	31	32	2F	31	eation Time 12/1
00000096	39	2F	31	35	6C	F1	55	23	00	00	00	1C	74	45	58	74	9/15lñU# tEXt

42

其他类型隐写

01 Bftools隐写

02 F5隐写

03 Fireworks隐写

04 outguess隐写

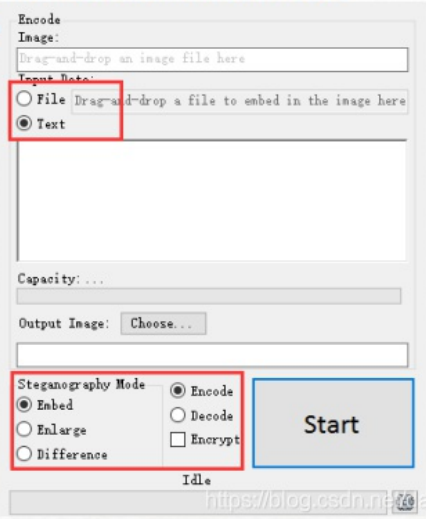
05 Imagestegography隐写

06 Stegdetect隐写/steghide隐写

05Imagestegography举例

简单的图形界面，输入密码字符串，或者也可以拖动一个密码文件，然后加密。将程序调为decode模式，拖动加密后的文件，点击START之后，密码字符串或者隐写文件就输出出来了。

在线链接：http://www.atool.org/steganography.php



60

Reference：

图片隐写.pdf