[登录]

Misc 总结 ----隐写术之图片隐写(一)

[M1n3] / 2017-12-22 16:33:17 / 浏览数 23168 [安全技术] [CTF] [顶(0)] [踩(0)]

实验简介

隐写术是关于信息隐藏，即不让计划的接收者之外的任何人知道信息的传递事件（而不只是信息的内容）的一门技巧与科学。英文写作Steganography，而本套教程内容将

实验内容

本次图片隐写实验包括四大部分

- 一、附加式的图片隐写
- 二、基于文件结构的图片隐写
- 三、基于LSB原理的图片隐写
- 四、基于DCT域的JPG图片隐写
- 五、数字水印的隐写
- 六、图片容差的隐写

下面进行实验Part 1 附加式图片隐写

第一部分 附加式的图片隐写

在附加式的图片隐写术中，我们通常是用某种程序或者某种方法在载体文件中直接附加上需要被隐写的目标，然后将载体文件直接传输给接受者或者发布到网站上，然后接

而在CTF赛事中，关于这种图片隐写的大概有两种经典方式，一是直接附加字符串，二是图种的形式出现。

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Strings
    - binwalk
    - Winhex

附加字符串

- 实验：

```
- ██████████████████████████████████████████
- █████████ xscq.jpg█
- ████████████████████████████████
- ███████████████████████████████████████████Strings███████
- █Strings██████████████████base64█████████
- ████████flag█flag{welcome_to_xianzhi}
```

strings使用方法

strings命令在对象文件或二进制文件中查找可打印的字符串。字符串是4个或更多可打印字符的任意序列，以换行符或空字符结束。
strings命令对识别随机对象文件很有用。

选项：

- -a --all：扫描整个文件而不是只扫描目标文件初始化和装载段
- -f –print-file-name：在显示字符串前先显示文件名
- -t --radix={o,d,x} ：输出字符的位置，基于八进制，十进制或者十六进制
- -e --encoding={s,S,b,l,B,L} ：选择字符大小和排列顺序:s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit

Tips 我们使用strings + 文件名字的命令即可
具体步骤如下：

在cmd中打开strings工具，使用如下命令

```
strings ctf.jpg
```

□

得到如下字符串：ZmxhZ3t3ZWxjb21lX3RvX3hpYW56aGl9
我们尝试用base64解码，代码过程如下：

```
Python 2.7.12 (v2.7.12:d33e0cf91556, Jun 27 2016, 15:24:40) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b64decode('ZmxhZ3t3ZWxjb21lX3RvX3hpYW56aGl9')
'flag{welcome_to_xianzhi}'
>>>
```

有必要提到的是，为什么字符串要附加在文件的后面呢?那是因为，如果图片附加在中间，有可能破坏了图片的信息，如果字符串附加在图片的头部位置，又破坏了文件头，

思考

1. 我们是否可以使用16进制的编辑器找到这一串字符串？请用工具中的winhex尝试这种解法。
2. 隐写和密码学的区别是？

图种形式的隐写

图种：
一种采用特殊方式将图片文件（如jpg格式）与rar文件结合起来的文件。该文件一般保存为jpg格式，可以正常显示图片，当有人获取该图片后，可以修改文件的后缀名，将
图种这是一种以图片文件为载体，通常为jpg格式的图片，然后将zip等压缩包文件附加在图片文件后面。因为操作系统识别的过程中是，从文件头标志，到文件的结束标志位

实验

- ■■
- ■■■■■■■■cqzb.jpg■
- ■■■■■■■■■■■■■■■■■■■■■■■■■■■■
- ■■■■■■■■■■■■■■■■■
- ■■winhex■■■■■■■■■■■■■■■■■■■■
- ■■■■■■■■flag■flag■flag{This is easy}

简单的检测方式：
打开工具中的binwalk。使用如下命令：

```
binwalk cqzb.jpg
```

□

我们可以发现，binwalk自动识别出来了zip文件，而且偏移也告诉我们了,当然我们这里如果使用

```
binwalk cqzb.jpg -e
```

这样的命令，是很快就能把ZIP文件给提取出来的，但是这里我想讲的是如何用winhex等16进制编辑器，将压缩包提取出来。

使用winhex16进制编辑器提取ZIP文件

- 首先需要了解一下什么是文件头
  文件头就是是位于文件开头的一段承担一定任务的数据。一般都在开头的部分。以jpg图片和zip压缩包文件为例。图6和图7分别是jpg图片的文件头以及jpg图片的结尾。
  我们如何，找到JPG图片和ZIP图片呢？
  JPG图片的文件头和结束标志

□
上图，FF D8 FF E1就是JPG图片的文件头，一般当我们看到文件开头是如此的格式，我们就能认为这是一个JPG图片了。
□
上图以 03 FF D9为结束标志，这是JPG图片的结束标志位。

ZIP文件的文件头和结束标志

□
上图 50 4B 03 04就是ZIP文件的文件头，一般以PK表示。

- 找到cqzb.jpg 中隐藏的ZIP文件

上文我们讲述了，JPG图片的结束标识是03 FF D9,ZIP文件的文件头是50 4B 03
04，我们只需要在winhex中找到ZIP文件的文件头即可，滑动滚条到最底下。上文讲了一般附加的位置是在原本文件的后面，所以我们果断滑动滚动条到最后。
□

从图中我们可以明显看到cqzb.jpg明显不是以FF D9结尾，而且我们在上面不远的地方发现了zip的文件头50 4B 03 04，所以我们可以断定这是个图种文件了

- 分离ZIP文件
  下一步我们该如何用winhex截取我们所需要的文件呢？
  我们选取以50开头以及到末尾的的数据，右键单击，选择编辑，复制选块到新文件，保存新文件为zip格式命名规则即可。

  保存为ZIP文件，解压缩后就能得到flag，所以最后的flag是flag{This is easy}

思考

1. 自己动手使用binwalk分离图片
2. 除了上述讲的方法我们是否可以使用其他手段分离文件？如dd这样的工具？

上一篇：Pentest WiKi Part... 下一篇：Misc 总结 ----隐写术之图...

1. 1 条追加内容

追加 于 2017年12月22日 16:35

追加附件

两题.zip(0.042 MB) 下载附件

---

1. 12 条回复


ssss 2017-12-23 22:59:34

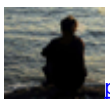
动动手指，沙发就是我的了！

0 回复Ta


176****6583 2017-12-24 12:13:10

动动手指，沙发就是我的了！

0 回复Ta


p0 2017-12-25 10:53:59

动动手指，沙发也不是我的了！

0 回复Ta


152****5136 2017-12-25 20:21:25

动动手指，沙发也不是我的了！+1

0 回复Ta


wahaha_a 2017-12-26 14:59:23

学习1

0 回复Ta


VS0X 2018-01-10 15:17:17

动动脚趾也是我的

0 回复Ta


threst 2018-01-18 13:11:20

学习了，感谢大佬分享

0 回复Ta


ghd仰望 2018-01-22 18:33:22

学习学习

0 回复Ta


老锥 2018-01-23 15:04:34

支持

0 回复Ta


189****5586 2018-09-14 09:37:37

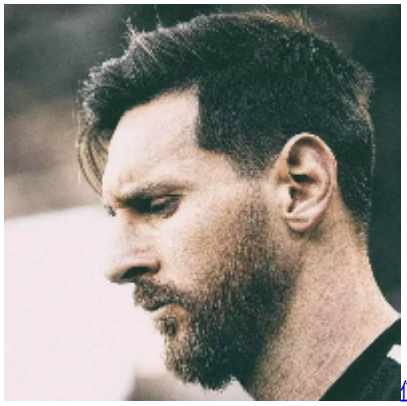
FF D9是JPG文件结束的标志，和0x03没有关系。

0 回复Ta

Catcher 2018-11-26 14:42:15

学习一波~

0 回复Ta



信安路人 2019-04-17 20:30:35

请问实验的文件有吗

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板