CTF---图片隐写相关

原创

xuqi7 于 2017-05-08 21:30:47 发布

分类专栏： ctf 文章标签： 图片 ctf

本文链接：https://blog.csdn.net/xuqi7/article/details/71436020

CTF—图片隐写相关

0 前言

CTF中，有一类题和图片相关，各种转换，这里记一些图片的玩法

1 jpg图片属性

正常的jpg图片，选中右键查看属性，在详细信息一栏会发现有很多属性可以修改，简单的题目可以在这里隐藏信息

2 图种

图种就是图片后面再放点信息进去，压缩包、txt文档、或者再来一张图片，要隐藏的信息完全没有限制，cmd举例如下：

```
:: /b表示二进制方式
copy a.jpg/b+b.zip/b c.jpg
copy a.jpg/b+b.txt/b c.jpg
copy a.jpg/b+b.jpg/b c.jpg
```

得到的c.jpg就是图种了

还原也比较简单，整理几种方法：

1. 使用工具分离，比较好用的工具有binwalk和foremost，binwalk建议使用这样的命令: `binwalk -eM <file_path>`，foremost直接跟文件路径就好了，一般foremost效果要好一些，可以都试一下
2. 在16进制编辑器打开然后手动分离，这种方式比较考验对文件格式的熟悉程度，需要对常见的文件类型开头结尾比较熟悉，16进制编辑器选择自己熟悉的就好，010Editor、WinHex、HxD都是比较成熟的软件，我会用rehex
3. 针对压缩文件的技巧，如果隐藏的信息是zip之类的压缩文件，可以直接把文件用压缩软件打开，就能提取压缩包里的文件了

注：有些图片后隐藏图片的情况，可能会把第二张图片头给去掉，然后把两张图片合在一起，由于特征没了，提取工具就没用了，使用手动分离的方法：16进制编辑器打开，找第一张图片的尾部，然后把第二张图片的头给加一下，这样就正常了

3 图层里的秘密 LSB

LSB, Least Significant Bit, 最低有效位，指图片像素的低位数据，因为低位对图片显示影响不大，所以可以用来隐藏数据
stegsolve是一个比较有名的查看图片LSB隐写的工具，一般有2种使用方法：

1. 把图片打开，点下面的箭头切换图层，可能会显示一些隐藏信息，如二维码图片
2. 提取低位数据：Analyse->Data Extract，可以先勾选 Red Green Blue的0位，点击 Preview试试看，一般都藏在0,1,2这些低位里面，只能试着观察了

有一个隐藏，检测，恢复的网站：http://incoherency.co.uk/image-steganography/

4 图片头损坏

有些图片会被故意修改前几个字节，导致无法显示
还原很简单，找一个类型相同的文件，在16进制编辑器里照着改回来就能正常打开了
pdf或其它有很明显固定文件头的文件也可以这么做

5 图片的高度

用16进制编辑器更改png图片的高度，会只显示图片的上面一部分，下面的部分就被隐藏了，是个藏东西的好办法
找表示宽度和高度的位置的话，010Editor比较方便，也可以先看看图片的属性，得到宽高值，转成16进制，搜索16进制值就找到了
注：

1. png图片的保存恢复效果比较好，jpg貌似有点问题
2. 试过改宽度，效果不好，高度很好掌握

6 图片隐写工具

图片隐写工具很多，慢慢补充，先写几个，以后再补

oursecret

这工具很强大，什么文件都能用来隐藏，完全没有限制
本来下载地址应该是: http://www.securekit.net/oursecret.htm, 但已经404了，随便搜一个在虚拟机里临时用一下吧

Outguess

支持3种用来隐藏信息的文件格式: PPM(Portable Pixel Map)、PNM(Portable Any Map)、jpg，需要密码
下载地址：https://github.com/resurrecting-open-source-projects/outguess
看着readme自己编译一下，使用方法如下：

```
# 隐藏
# hidden.txt是要隐藏的文件，demo.jpg是用来隐藏信息的图片，out.jpg是有隐藏信息的图片
outguess -k "my secret key" -d hidden.txt demo.jpg out.jpg
# 提取
outguess -k "my secret key" -r out.jpg hidden.txt
```

steghide

steghide可以在图片和音频文件中隐藏各种数据，windows和linux系统都支持
支持jpg、bmp，不支持png，密码可选

sourceforge和github地址：
http://steghide.sourceforge.net/
https://github.com/StefanoDeVuono/steghide

windows可以直接在sourceforge下载可执行文件
linux如果是debian系，可以使用apt安装: `sudo apt install steghide`

简单使用方法：

```
# 隐藏数据 To embed emb.txt in cvr.jpg
steghide embed -cf cvr.jpg -ef emb.txt
# 提取数据 To extract embedded data from stg.jpg
steghide extract -sf stg.jpg
```

F5

F5隐写是java编写的隐写工具，支持bmp、gif、jpg图像文件，需要密码
github地址: https://github.com/matthewgao/F5-steganography

简单使用方法：

```
# 隐藏数据 lopez.bmp是源图片，lopez.jpg是生成的图片，-c是注释，-e是要隐藏的文件，-p是密码
java Embed lopez.bmp lopez.jpg -c "comment hellowor.." -e hello.txt -p helloworld
# 提取数据
java Extract lopez.jpg -p helloworld
```

stegdetect

stegdetect 用于检测图片隐写方式

github的版本只能在linux下编译使用: https://github.com/abeluck/stegdetect

这里可以看到原始版本的介绍：
https://web.archive.org/web/20150415213536/http://www.outguess.org/detection.php

这里可以下载源码和windows版本：
https://web.archive.org/web/20150415220609/http://www.outguess.org/download.php
windows版本下载地址：https://web.archive.org/web/20150415220609/http://www.outguess.org/stegdetect-0.4.zip

2017/5/8