CTF隐写总结

原创

普通Gopher 于 2019-09-30 19:53:49 发布 1324 收藏 19

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/qq_43442524/article/details/101789131

打了有小半年ctf比赛了，一直没有时间来写几篇关于ctf的博客，今天抽出时间写了点杂项中隐写的总结，希望能够帮到大家

简述

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”。

CTF隐写常见方式：

1.增加数据的方式 隐藏信息
另存为.zip后解压，正常的.JPG图片在文本编辑器（winhex）中，16进制是以FF D9结尾
原理：a.先制作一个1.zip 把含有隐藏的内容放进去‘
b.另找一张.jpg图片(2.jpg)，执行命令：copy /b 2.jpg+1.zip output.jpg,得到一张output.jpg图片
c.图片查看器会忽视jpg结束符之后的内容，所以附加的1.zip不会影响图像的正常显示

2.修改数据的方式 隐藏信息
利用LSB（最低有效位）来进行隐写
原理：图片的像素由三种颜色组成，即三原色，由这三种颜色可以组成其他各种颜色
例如：在.png图片的存储中，每个颜色会有8bit，LSB隐写就是修改了像数中最低的1bit，在人烟看来是看不出区别的，也就隐藏了信息
例如：把‘A’隐藏进图片，可以把‘A’转成16进制0x61再转成二进制01100001，再修改为红色通道的最低位为这些二进制字符串
工具：stegsolve
注意：隐写的载体不能使.jpg格式，jpg图片对像素数进行了有损的压缩，修改的信息可能会被破坏

3.隐写与加密
例如：打开一个.gif文件报错，这时，需要我们手动修复图片，首先需要对于这种图片的文件结构有所了解
查看.gif图片文档格式链接：http://dev.gameres.com/Program/Visual/Other%20/GIFDoc.htm
浏览图片后发现，有个PASSWORD一闪而过，gif与其他图片的最大区别是gif是动态图，可以由多帧组成，顺序播放，我们可以使用工具一帧一帧的观察图片，得到密文，进行解密
工具：Stegsolve或Namo_GIF_gr

4.载体
拿到一张含有信息的图片时：
a.分析数据隐藏在哪里，也就是说利用什么作为载体
b.进一步分析是加密的或是编码的
总结：我们要对一个图片的格式有所了解，知道哪些地方是可疑的，那些可以隐藏信息，那些有冗余的成分
例如：jpg图片可以吧信息隐藏在头部exif部分（插入了数码照片的信息），可以用查看属性的方式修改，也可以用exif编辑器编辑工具：power_exif

5.编程辅助
有一些情况下，没有现成的工具来完成，可以写一些的程序来辅助我们进行分析，或者是加解密
例如：一个png图片找flag，首先要对png图片格式了解：http://www.cnblogs.com/fengyv/archive/2006/04/30/2423964.html
先用stegsolve查看一下，没有发现问题，然后看一下结构，发现有一些异常的IDAT块（png图片中存储图像像数数据的块），可以用pngcheck来辅助我们观察，命令：pngcheck.exe -v 1.png,找到异常的IDAT部分，利用winhex扣出来研究

6.双图
给出两张图片，或是需要去寻到原来图片进行对比找出隐藏的信息

隐写解决方案

一、隐写术可以利用图片、音频、视频为载体将数据隐藏在其中，将数据隐写到图像中较为常见。

二、图像隐写术进行数据隐写分为以下几类：

1.在图片右击-属性-详细信息中隐藏数据信息

2.将数据类型进行改写（rar类型数据 将其改写成jpg格式）

3.根据各种类型图像的固定格式，隐藏数据

修改图像开始标志，改变其原有图像格式；

在图像结束标志后加入数据；

在图像数据中假如数据，不影响视觉效果情况下修改像素数据，加入信息。

4.利用隐写算法将数据隐写到图像中而不影响图像（仅限于jpg图像），隐写算法常见有F5、Guess、JSteg和JPHide等

三、破解隐写术方法及步骤：

1.查看图像-属性-详细信息是否包括隐藏内容

2.利用WinHex打开图像，搜索CTF、ctf或flag看是否在打开数据中存在相关信息

3.检查图像开始标志和结束标志是否正确，若不正确修改图像标志恢复图像，打开查看是否ctf或flag等信息（往往gif属于动图，需要分帧查看各帧图像组合所得数据 若不是直接的ctf或flag信息 需要考虑将其解码）

jpg图像开始标志：FF D8 结束标志：FF D9

gif图像开始标志：47 49 46 38 39 61 结束标志：01 01 00 3B

4.将图像放置kali系统中，执行binwalk xxx.jpg 查看图像中是否是多个图像组合或者其中包含其他文件（若存在多幅图像组合，再执行foremost xxx.jpg会自动分离；若检测出其他文件修改其后缀即可，如.zip）

5.使用StegSolve对图像进行分通道扫描，查看是否为LSB隐写

6.在windows系统命令行下使用F5-steganography-master进行jpg图像是否为F5算法隐写

7.在kali系统中使用outguess-master工具（需要安装），检测是否为guess算法隐写

8.改图片高度（对应题目难度：中）

CTF比赛中可利用16进制编辑工具更改图片的高度，使图片只显示一部分，下面的部分被隐藏，嗯，这是个藏东西的好办法！

当以上方法均不可以得到FLAG，且图片长宽比例诡异时，可以尝试改图片大小，下面介绍找图片宽度和高度的标志位的方法：

A）对于png文件，其第二行第六列是高度位，改这一位即可；

B）对于其他格式图片，可以先看看图片的属性，得到宽高值，转成16进制数，搜索该16进制值就能找到标志位了；

常用脚本

异或和

```
#!/usr/bin/env python
# -*- coding: gbk -*-
# -*- coding: utf_8 -*-

from PIL import Image

png1=Image.open('1.png')
png2=Image.open('2.png')
#png2不是RGB类型，转换
png2=png2.convert('RGB')
#获取图片大小信息
width,height=png2.size
pic=Image.new('RGB',(width,height))
for y in range(height):
    for x in range(width):
        b1,g1,r1=png1.getpixel((x,y))
        b2,g2,r2=png2.getpixel((x,y))
        #两张图片逐像素异或
        b,g,r=b1^b2,g1^g2,r1^r2
        #异或后图片黑色置成白色，其他置成黑色
        if((b,g,r)==(0,0,0)):
            pic.putpixel([x,y], (255,255,255))
        else:
            pic.putpixel([x,y],(0,0,0))
            pic.show()
            pic.save('3.png')
```

三原色

```python
#-*- coding:utf-8 -*-
from  PIL import Image
import re

x = 503 #x坐标  通过对txt里的行数进行整数分解
y = 122 #y坐标  x*y = 行数

im = Image.new("RGB",(x,y))#创建图片
file = open('misc100.txt') #打开rbg值文件

#通过一个个rgb点生成图片
for i in range(0,x):
    for j in range(0,y):
        line = file.readline()#获取一行
        rgb = line.split(",")#分离rgb
        im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))#rgb转化为像素
im.show()
```