# CTF隐写总结！

原创

YICONGITSME 于 2018-08-06 19:38:43 发布 12598 收藏 55
分类专栏： CTF 文章标签： CTF 隐写



这个暑假在学安全，应对一个比赛。实验室朋友在一起学习，专攻自己的方向，相互帮助，讲解。主要是做CTF题，

我之前学过一些web的，sql注入挺让我头疼的，一次又一次的挫败。我这次先入手了隐写，学的也不是很深。下面是做的一些笔记，也是很全，也不是很好。

**0x00**

jpg文件头 十六进制FF D8 FF E0
cool edit 音频编辑
https://pc.qq.com/detail/0/detail_640.html Audacity
一段线代表- 一个点代表空格 大点代表. 空格分割字符
观察波形 解出摩斯码
http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx 摩斯解码
docx中文字可能会有隐藏文件，选择字体，去勾隐藏
http://www.atool.org/steganography.php 图片隐写术加密
ASCII在线转换器 二进制需用空格隔开
A-Z 65-90 a-z 97-122
图片可能是压缩包，打开压缩包，选择所有文件，选择图片
提示是弱口令 则可以用爆破 得到常用的密码
KRyLack Zip Password Recovery 压缩包密码破解工具
多次进行解密 Base64 rabbit 凯撒（需要列出所有组合，选择能成语句的）
http://tool.chinaz.com/Tools/Base64.aspx Base64 加密解密 用解码编码不行

**0x01**.

图片，按照套路应该就是先binwalk，再StegSolve，再Winhex，

将图层二进制的最低位获取出来，即LSB问题；
LSB算法基本步骤：
1 将原始载体图像的空域像素值由十进制转换成二进制；
2 用二进制秘密信息中的每一比特信息替换与之相对应的载体数据的最低有效位；
3 将得到的含秘密信息的二进制数据转换为十进制像素值，从而获得含秘密信息的图像。

**0x02.**

遇到二维码，用QR Research 解码，
unicode码 http://tool.chinaz.com/tools/unicode.aspx 解码
中文的话 有一种加密叫当铺密码， 根据字比划出头的数目转化为数字
binwalk是一个文件的分析工具，旨在协助研究人员对文件进行分析，提取及逆向工程。
http://www.cnblogs.com/pcat/p/5256288.html binwalk windows 安装

**0x03**.

图片用stegsolve 进行通道分析，red plane 0 可以观察到二维码很暗
用ps处理，调节亮度，对比度，色阶

**0x04**.

图片用hxd查看有没有压缩文件，txt文件，压缩密码爆破Zip Password Tool

http://www.cmd5.com/ MD5解密
压缩文件头 FF D9 50 4B 文本文件头 31 2E 74 78 74
或者用binwalk 分离图片发现压缩文件，foremost 分离文件 再 fcrackzip
F5隐写 https://github.com/matthewgao/F5-steganography
在cmd java Extract 图片路径 -p 123456 解出output.txt
http://tool.oschina.net/encrypt DES加密
遇到两张大致相同的图片。用stegsolve 进行combine
二维码图片如果是彩色，则需要进行red plane0 green，blue 通道分析

下面是一些实验的。基本上没用kali，因为win下的一些工具已经够我使用了。

1. wbStego（软件）
安装，选择encode 加密，选择decode解密
首先创建文件，选择文件目录，选择文件载体图片，进行加密，生成目标文件
解密，选择目标文件，无加密密码，生成解密文件。

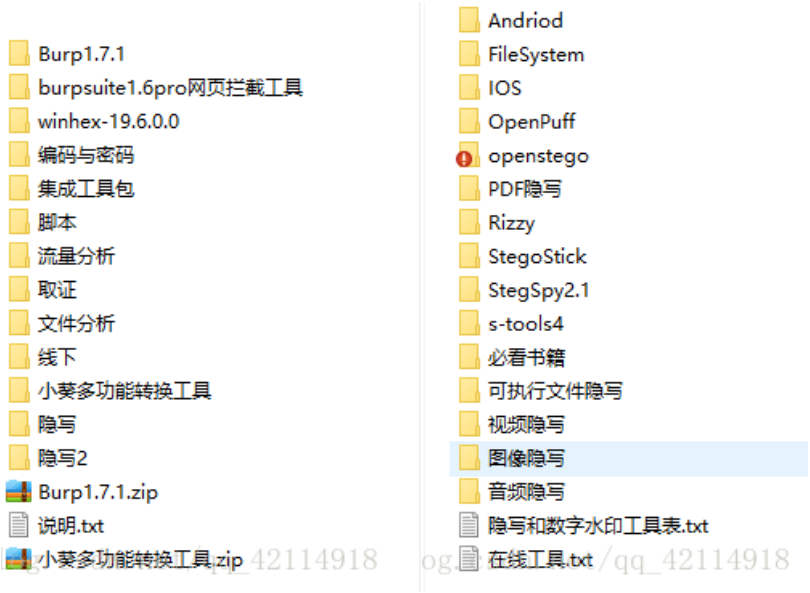
2. Hide and seek 利用像素LSB来隐藏 （命令行）
Hide hidden.txt ARDALA.GIF 执行命令生成OUTFILE.GIF 文件
seek OUTFILE.GIF out.txt 解密生成out.txt 和hidden.txt 内容相同

3. F5 针对 jpeg图像 （作为载体）（命令行）
运行ms_e.bat 把bmg图像 嵌入携密信息jpeg图像
运行ms_d.bat 提取秘密信息得到output.txt

4.S-Tools 音频文件（作为载体） 采用LSB占用比特位（软件）
拖拽wav音频文件到窗口中，再拖拽要待隐藏文件，需要输入加密密码
完成后，右击，reveal显示秘密信息，

5.mp3stego 将wav文件嵌入到mp3的比特流中（命令行）
mp3stegoon提取信息
把数据文件和wav文件压缩成mp3 文件
文件要存放在安装目录下
encode -E 数据文件名称 载体名称 携密文件名称 需输入密钥
decode -X 携密文件名称

工具真的非常多，都是学长留下来的宝贵财富，使我们受益




比赛完后成功的晋级了，我开始准备线下赛了。Good Luck To Me !