# 【CTF-MISC基础】干货总结--文件隐写--图片隐写

原创

ATFWUS 于 2020-07-14 17:26:31 发布 2508 收藏 34

分类专栏： CTF-MISC 文章标签： ctf misc 干货 文件隐写 图片隐写



本文链接：https://blog.csdn.net/ATFWUS/article/details/107336145






## 0x01.文件操作与隐写

### 1.文件类型识别

对于没有后缀名的文件类型识别。

**方法一**：Linux下`file`命令。

- 格式：`file 文件名`。

**方法二**：windows下通过winhex查看文件头字段识别文件类型。

- 最好使用Notepad++，安装插件HEX-Editor进行查看。

常见的文件头类型如图所示

| 文件类型 | 文件头 |
| --- | --- |
| JPEG (jpg) | FFD8FFE1 |
| PNG (png) | 89504E47 |
| GIF (gif) | 47494638 |
| TIFF (tif) | 49492A00 |
| Windows Bitmap (bmp) | 424DC001 |
| ZIP Archive (zip) | 504B0304 |
| RAR Archive (rar) | 52617221 |
| Adobe Photoshop (psd) | 38425053 |
| Rich Text Format (rtf) | 7B5C727466 |
| XML (xml) | 3C3F786D6C |
| HTML (html) | 68746D6C3E |
| Adobe Acrobat (pdf) | 255044462D312E |
| Wave (wav) | 57415645 |
| pcap (pcap) | 4D3C2B1A |

**文件头残缺情况：** 使用十六进制编辑器010editor编辑器进行编辑。

## 2.文件分离操作

**方法一：** Linux下使用Binwalk工具进行文件的分析和分离。

- 分析文件：`binwalk filename`
- 分离文件：`binwalk -e filename`

**方法二：** 如果binwalk无法正确分离出文件，可以使用formost工具。

- `foremost 文件名 -o 输出目录名`

**方法三：** 当文件自动分离出错或因为其他原因无法自动分离时，用dd工具进行手动分离。

- `dd if=源文件 of=目标文件名 bs=1 skip=开始分离的字节数`
- 参数：`if=file`输入文件名，省略为标准输入。
- 参数：`of=file`输出文件名，省略为标准输出。
- 参数：`bs=bytes`同时设置读写块的大小为bytes。
- 参数：`skip=blocks`从输入文件开头跳过blocks个块后再开始复制。
- 参数：`count`一共取的块。

**方法四：** 使用010Editor直接选择对应的十六进制，然后右键单独保存，实现分离。

### 3.文件合并操作

**Linux下：** `cat 要合并的文件 输出的文件`

- 完整性检测：`md5sum 文件名`

**Windows下：** `copy /B 合并的文件 输出的文件`

- 完整性检测：`certutil -hashfile 文件名 md5`

### 4.文件内容隐写

- 概述：文件内容隐写，是直接将KEY以十六进制的形式写在文件中，通常在文件的开头或结尾部分，**分析时通常重点观察文件开头和结尾部分**。如果在文件内容中间部分，通常搜索关键字KEY或者flag来查找隐藏内容。

## 0x02.图片文件隐写

### 1.Firework

- 使用010Editor打开文件后，如果看到文件头部包含firework的标识，可以通过firework来找到隐藏的图片。

### 2.Exif

- Exif按照JPEG的规格在JPEG中插入一些图像、数字相机的信息数据以及缩略图像，可以通过与JPEG兼容的图片浏览器，图片处理软件等查看Exif格式的图像文件。
- 右键属性，查看exif或者详细信息，在相关的选项卡中查找flag。

### 3.Stegsolve

- 当两张jpg图片的样式，大小，像素基本相同时，可以考虑进行结合分析，将两个文件的像素进行ADD,SUB,XOR等操作，看是否可以得到有用的信息。Stegsolve工具可以方便的进行这些操作。

## 4.LSB（最低有效位）

LSB替换隐写的基本思想：用嵌入的秘密信息取代载体图像的最低比特位，原来的7个高低平面与替代 秘密信息的最低位平面组合成含隐藏信息对=的新图形。

通过修改像素中最低位的一位来达到隐藏的效果。

也可以使用Stegsolve来进行。

Linux下的工具：zteg工具

下载：`gem install zsteg`

检测LSB隐写：`zsteg xxx.png`

Windows下的工具：wbstego4工具。能够解密通过LSB加密的图片。

其它方式：Python脚本。

## 5.TweakPNG

- TweeakPNG是一款PNG图像浏览工具，它允许查看和修改一些PNG图像文件的原信息存储。
- 如果文件头是正常的，但却无法打开，可以使用TweakPNG修改CRC。出现校验信息错误时，可以根据错误的CRC去十六进制中搜索，然后改成正确的CRC。（CRC上一行之后的 8个字节，前四个为宽度，后四个为高度（十六进制下的第二行前八位））
- 有时不是CRC的错误，而是图片的宽高错误，需要通过CRC计算出正确的高度或宽度。可以通过脚本进行计算。

## 6.Bftools

Bftools常用于解密图片信息。

Windows下：

- `Bftools.exe decode braincopter 要解密的图片名称 -output 输出文件名`
- `Bftools.exe run` 上一步输出的文件。

## 7.SilentEye

- Windows下可视化解密工具。

## 8.JPG图像加密

Stegdetect 工具用于探测JPEG文件的加密方式。（Linux下）

- 可以检测到JSteg，F5，Camouflage，OutGuess，JPHide，appendX，Invisible Secrets等加密方式所隐藏的信息。

```
stegdetect xxx.jpg
```

```
stegdetect -s 敏感度 xxx.jpg
```

## 9.Jphide

- 基于LSB的JPEG格式图像隐写算法。
- 如果使用Stegdetect检测到使用jphide，可以使用Jphs进行解密。

## 10.Outguess

outguess用于解密文件信息。

如果确认使用OUtguess加密的图片，可以使用outguess进行解密。

```
outguess -r 要解密的文件名 输出结果文件名
```

## 11.F5

- 识别是F5加密后，进入F5-stegangraphy_F5目录，将图片文件拷贝下来，cmd进入该目录。
- `Java Exrtact 待解密文件名 -p 密码`
- 运行成功后，在output.txt可以看到解密结果。

## 12.二维码处理

- 使用工具CQR打开图片，查看内容字段。
- 如果二维码的定位角覆盖，该工具有一定几率识别，如果不能识别，需要使用其他工具将另外几个角的定位符移动搭配相应的位置，补全二维码。
- 如果二维码定位点中间是白色，可能是被反色了，可以使用其它工具进行反色再回来扫描。