CTF-Misc基础知识之图片及各种工具

原创

Ke1R 于 2022-04-17 16:39:35 发布 1279 收藏

文章标签： 网络安全

本文链接：https://blog.csdn.net/m0_62770485/article/details/124231894

MISC作为CTF中比较重要的一类题型，分值占比较大，为了帮助大家更好的学习MISC的做题方法，我总结了常见的图片类型中的几种题型及工具：

图片，音频，视频

> 首先就是大家常见的图片分析，图片修复，图片修改长宽高，图片拼接，二维码扫描，LSB隐写等等。

遇到图片类型的题，首先最基础的图片分析，将图片丢到winhex或者010editor中分析。分析此图片有无隐写信息或分析是否包含压缩包等。以下是总结的各类型文件的文件头：

```
PNG (png)，文件头：89504E47
GIF (gif)，文件头：47494638
TIFF (tif)，文件头：49492A00
Windows Bitmap (bmp)，文件头：424DC001
CAD (dwg)，文件头：41433130
Adobe Photoshop (psd)，文件头：38425053
Rich Text Format (rtf)，文件头：7B5C727466
XML (xml)，文件头：3C3F786D6C
HTML (html)，文件头：68746D6C3E
Email [thorough only] (eml)，文件头：44656C69766572792D646174653A
Outlook Express (dbx)，文件头：CFAD12FEC5FD746F
Outlook (pst)，文件头：2142444E
旧版office MS Word/Excel (xls.or.doc or.ppt)，文件头：D0CF11E0
MS Access (mdb)，文件头：5374616E64617264204A
WordPerfect (wpd)，文件头：FF575043
Adobe Acrobat (pdf)，文件头：255044462D312E
Quicken (qdf)，文件头：AC9EBD8F
ZIP Archive (zip)，文件头：504B0304
RAR Archive (rar)，文件头：52617221
Wave (wav)，文件头：57415645
JPEG (jpg)，文件头：FFD8FFE1
<.img
src=“data:image…”
alt=“Base64 encoded image” /> 生成图片（常用于base64隐写图片）
```

查看图片基本信息，kali下输入:

```
exiftool 1.jpg
```

当需要文件分离时，需要在Kali下文件分离

binwalk 文件分离

binwalk文件分离

```
binwalk -e +文件名 ||binwalk +文件名
```

foremost文件分离

```
foremost -i +文件名
```

dd 文件分离

dd命令作用是用指定大小的块拷贝一个文件，并在拷贝的同时进行指定的转换。

```
dd if=原文件名 of=(要分解的文件名) skip=5016064(十进制值) bs=1
```

当遇到图片隐写题时，可以使用**Stegsolve**工具（可用于逐帧分析GIF图片，lsb隐写等）

使用方法如下：

```
File Format:文件格式
Data Extract:数据提取
Steregram Solve:立体试图 可以左右控制偏移
Frame Browser:帧浏览器
Image Combiner:拼图，图片拼接
```

stegdetect 查询jpg图片经过哪种隐写 将图片复制到 stegdetect.exe所在目录下右键PowerShell命令

```
.\stegdetect.exe -tjopi -s 10.0 .\hide.jpg
```

检测该图片用的是哪种加密方式.

F5图片隐写 Kali工具 点开F5-steganography文件夹 在控制端导入 输入java Extract 图片

图片高宽的修改

tweakpng.exe打开图片提示IDHRcyc错误，表示文件尺寸被修改，且未修改crc值

outguess(关键词 猜)

```
无加密:outguess -r /root/angrybird.jpg -t 11.txt
解密 outguess -k “my secret key” -r out.jpg hidden.txt
```

steghide隐写 (图片或音频) Kali命令

```
steghide extract -sf 文件(密码一般为空或者文件名)
```

题目提示NTFS 是在txt中隐藏了txt文件 cmd 输入

```
notepad .txt:.txt
```

IDAT模块很多时 用**tweakpng**修改 Kali中用

```
pngcheck -vv 查看
```

JPHS隐写:(txt藏在JPG里) 打开需要提取隐藏信息的图片h.jpg 点seek输入对应密码（大多为123456）

zsteg可以检测PNG和BMP图片里的隐写数据。

zsteg支持检测：
1：LSB steganography in PNG & BMP
2：zlib-compressed data
3：OpenStego
4：Camouflage 1.2.1
5：LSB with The Eratosthenes set

```
zsteg -E “extradata:0” xxxx.png > flag
```

MP3stego(音频隐写)详细看

https://blog.csdn.net/myloveprogrmming/article/details/52641916

Audacity 音频查看工具

针对音频题目的常用工具，具体使用教程见

http://www.360doc.com/content/13/0620/17/1437142_294320939.shtml

时间有限，有空的时候还会继续补充。有不对的地方望大家指正。