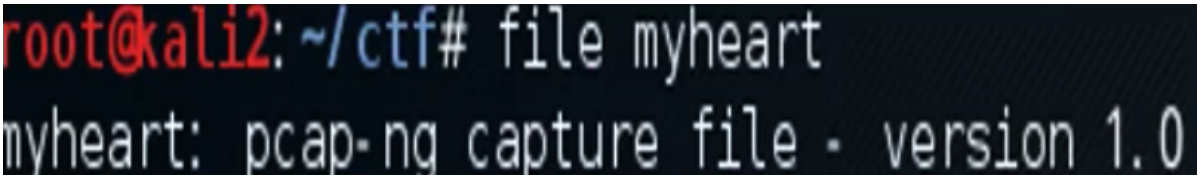
misc

文件操作与隐写

1.文件类型识别

1.1file命令

当文件没有后缀名或者有后缀名而无法正常打开时，根据识别出的文件类型来修改后缀名即可正常打开文件。
使用场景:不知道后缀名，无法打开文件。格式: `file myheart`



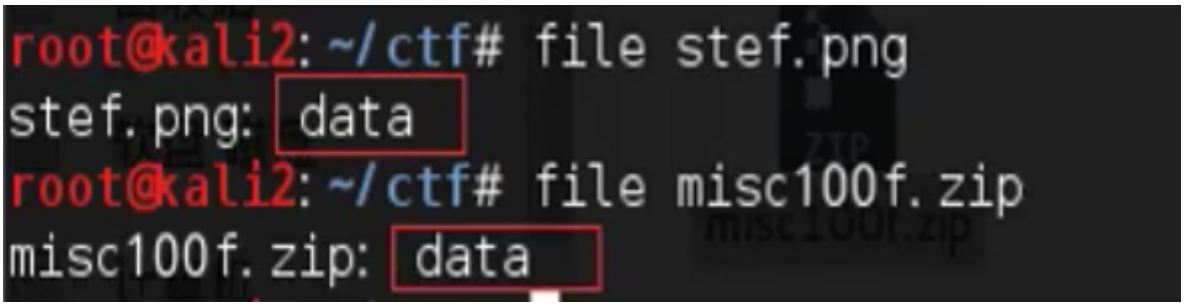
1.2winhex

通过`winhex`.程序中可以查看文件头类型，根据文件头类型判断出文件类型
使用场景: windows 下通过文件头信息判断文件类型

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

1.3文件头残缺或错误

通常文件无法正常打开有两种情况，一种是文件头部残缺， 另一种是文件头部字段错误。针对文件头部残缺的情况，使用`winhex`或者010 Editor程序添加相应的文件头，针对头部字段错误，可以找一个相同类型的文件进行替换。
使用场景:文件头部残缺或文件头部字段错误无法打开正常文件。
格式: file 文件名



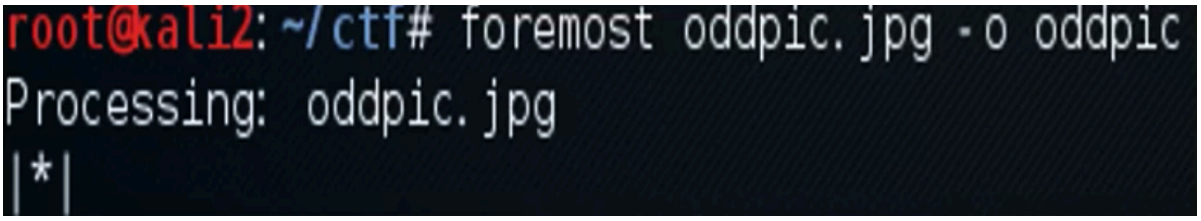
2.文件分离操作

2.1binwalk

Binwalk是Linux下用来分析和分离文件的工具，可以快速分辨文件是否由多个文件合并而成，并将文件进行分离。如果分离成功会在目标文件的目录。
同目录下生成一个形如_ 文件名_ extracted的文件目录，目录中有分离后的文件。
用法:
分析文件: `binwalk filename`
分离文件: `binwalk -e filename`

2.2foremost

如果binwalk无法正确分离出文件，可以使用foremost，将目标文件复制到kali中，成功执行后，会在目标文件的文件目录下生成我们设置的目录，目录中会按文件类型分离出文件。
用法:
foremost 文件名 -o 输出目录名



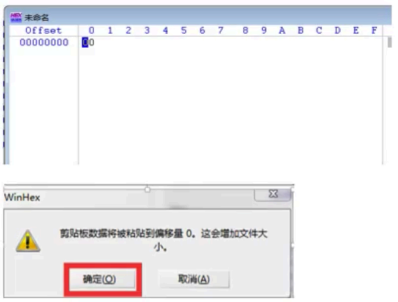
2.3dd

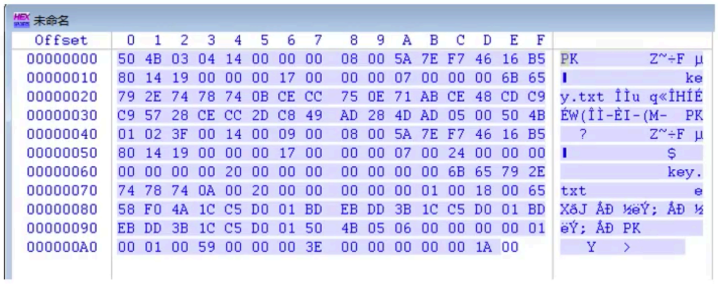
当文件自动分离出错或者因为其他原因无法自动分离时，可以使用dd实现文件手动分离。

格式:
dd if=源文件 of=目标文件名名bs=1 skip=开始分离的字节数
参数说明:
if=file #输入文件名，缺省为标准输入。
of=file #输出文件名，缺省为标准输出。
bs=bytes #同时设置读写块的大小为bytes，可代替ibs和obs。
skip=blocks #从输入文件开头跳过blocks个块后再开始复制。

2.4winhex

可以使用winhex实现文件手动分离，将目标文件拖入winhex中，找到要分离的部分，点击复制即可。
使用场景: windows 下利用winhex程序对文件进行手动分离
例:新建一个文件，文件大小1byte， 在文件开头位置点击粘贴，弹出提示框选否、确定，将文件保存为想要的后缀即可。





2.5010Editor

3.文件合并操作

3.1linux下的文件合并

使用场景: linux 下，通常对文件名相似的文件要进行批量合并
格式: cat 合并的文件>输出的文件

完整性检测: linux下计算文件md5:
md5sum 文件名

3.2Windows下的文件合并

使用场景:windows下，通常要对文件名相似的文件进行批量合并
格式: copy/B合并的文件输出的文件命令

完整性检测: windows 下计算文件md5:
certutil -hashfile 文件名 md5

4.文件内容隐写

文件内容隐写，就是直接将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。如果在文件中间部分，通常搜索关键字KEY或者flag来查找隐藏内容。
使用场景: windows下， 搜索隐写的文件内容

4.1winhex/010editor

通常将要识别的文件拖入winhex中，查找具有关键字或明显与文件内容不和谐的部分，通常优先观察文件首部和尾部，搜索flag或key等关键字，最后拖动滚轮寻找。

4.2Notepad++

使用notepad++打开文件，查看文件头尾是否有含有关键字的字符串，搜索flag或key等关键字，最后拖动滚轮寻找。
另外通过安装插件HEX-Editor可以实现winhex的功能。

5.图片隐写术

图片隐写的常见隐写方法
1.细微的颜色差别
2.GIF图多帧隐藏
3.颜色通道隐藏
4.不同帧图信息隐藏
5.不同帧对比隐写
6.Exif信息隐藏

7.图片修复
8.图片头修
9.图片尾修复
10.CRC校验修复
11.长、宽、高度修复
12.最低有效位LSB隐写
13.图片加密
14.Stegdetect
15.outguess
16.Jphide
17.F5

6.图片文件隐写

6.1 Firework

使用winhex打开文件时会看到文件头部中包含firework的标识，通过firework可以找到隐藏图片。
使用场景:查看隐写的图片文件

6.2 Exif

Exijf按照PEG的规格在PEG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PEG兼容的互联网浏览器/图片浏览器/图像处理等一些软件来查看Exift格式的图像文件就跟浏览通常的PEG图像文件一样，图片右键属性，查看exif或 查看详细信息，在相关选项卡中查找flag信息。

6.3 Stegsolve

当两张jpg图片外观、大小、像素都基本相同时，可以考虑进行结合分析，即将两个文件的像素RGB值进行XOR、ADD、SUB等操作，看能否得到有用的信息，StegSolve可以方便的进行这些操作。
使用场景:两张图片信息基本相同

6.4LSB(最低有效位Least Significant Bit)

LSB替换隐写基本思想是用嵌入的秘密信息取代载体图像的最低比特位，原来的的7个高位平面与替代秘密信息的最低位平面组合成含隐藏信息的新图形。
1.像素三原色(RGB)
2.通过修改像素中最低位的1bit来达到隐藏的效果
3.工具: stegsolve、 zsteg、 wbstego4、 python脚本

6.5Tweak PNG

TweakPNG是一款简单易用的PNG图像浏览工具，它允许查看和修改一些PNG图像文件的元信息存储。
使用场景:文件头正常却无法打开文件，利用TweakPNG修改CRC
例:
1.当PNG文件头正常但无法打开文件，可能是CRC校验出错，可以尝试通过TweakPNG打开PNG，会弹出校验错误的提示，这里显示CRC是fe1a5ab6，正确的是b0a7a9f1。打开winhex搜索fe1a5ab6将其改为b0a7a9f1。

1. 文件头正常却无法打开文件，利用TweakPNG 修改CRC....
2. 有时CRC没有错误，但是图片的高度或者宽度发生了错误，需要通过CRC计算出正确的高度或者宽度。可以用下面的py脚本，需要改文件位置和TweakPNG得到的CRC实际值，用计算出高度，利用01Editor修改宽高

6.6Bftools

bftools用于解密图片信息。
使用场景:在windows的cmd下，对加密过的图片文件进行解密格式:
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

6.7SilentEye

silenteye是一款可以将 文字或者文件隐藏到图片的解密工具。
使用场景: windows' 下打开silentEye工具，对加密的图片进行解密
例:
1.使用silentEye程序打开目标图片，点击image一>decode，点击decode，可以查看隐藏文件，点击保存即可

2.如果需要密码，勾选encrypteddata，输入密码和确认密码，点击decode再解密

6.8JPG图像加密

1)Stegdetect工具探测加密方式

Stegdetect.程序主要用于分析PEG文件。因此用stegdetect 可以检测到通过Steg、JPHide. OutGuess、Invisible Secrets、F5、appendX和Camouflage等这些隐写工具隐藏的信息。
stegdetect xxx.jpg
`stegdetect -s`敏感度`xx.jpgexi`

2)Jphide

Jphide是基于最低有效位LSB的JPEG格式图像隐写算法.例:
Stegdetect提示jphide加密时，可以用Jphs.工具进行解密，打开jphswin.exe， 使用open jpeg打开图片，点击seek，输入密码和确认密码，在弹出文件框中选择要保存的解密文件位置即可，结果保存成txt文件。

3.Outguess

outguess 一般用于解密文件信息。
使用场景:`Stegdetect`识别出来或者题目提示是outguess加密的图片该工具需编译使用: ./configure && make && make install
格式: outguess -r 要解密的文件名输出结果文件名

4.F5

F5一般用于解密文件信息。
使用场景: `Stegdetect`识 别出来是F5加密的图片或题目提示是F5加密的图片
进入`F5-steganography_F5`目录，将图片文件拷贝至该目录下，从CMD进入该目录

格式: `Java Exrtact`要解密的文件名 -p 密码