文件隐写

转载

weixin_30302609 于 2017-08-22 10:46:00 发布 761 收藏 2
文章标签： shell
原文链接：http://www.cnblogs.com/jiaxinguoguo/p/7410483.html

文件隐写
1、JPEG(jpg)，文件头：FF D8 FF E0 00 10 4A 46 49 46 文件尾：FF D9
2、PNG (png)，文件头: 89 50 4E 47 0D 0A 1A 0A 文件尾：49 45 4E 44 AE 42 60 82
3、GIF (gif)，文件头：47 49 46 38 39
4、bmp，文件头：42 4D E3 BF 22 00 00 00
5、rar文件头：52 61 72 21
6、zip文件头：50 4B 03 04 14 00 00 00 08 00
7、PDF文件头：25 50 44 46

tips:
1. 可以使用WinHex查看文件的十六进制编码，然后找到文件头尾，也可以用binwalk命令查看文件中是否有隐藏文件,bb分割文件。
使用binwalk分离所有jpg文件：

```
binwalk -D=jpeg a.jpg
```

2. Stegsolve可以查看png图片的各个颜色的通道，可左右滑动或者在analyse中查看隐藏字符。

3.使用braintools将图片中隐藏的bf代码解码出来：

```
bftools.exe decode braincopter doge.png --output dogeout.png

bftools.exe run dogeout.png
```

4.steghide可以在图片或音频中隐藏信息

```
steghide embed -cf a.jpg -ef key.txt    //加密
steghide extract -sf a.jpg -xf out.file -p password   //提取
```

但是steghide不支持读取字典文件，所以参考pcat写的py代码，用字典爆破

```
from subprocess import *

def foo():
    stegoFile='rose.jpg'
    extractFile='hide.txt'
    passFile='english.dic'

    errors=['could not extract','steghide --help','Syntax error']
    cmdFormat='steghide extract -sf "%s" -xf "%s" -p "%s"'
    f=open(passFile,'r')

    for line in f.readlines():
        cmd=cmdFormat %(stegoFile,extractFile,line.strip())
        p=Popen(cmd,shell=True,stdout=PIPE,stderr=STDOUT)
        content=unicode(p.stdout.read(),'gbk')
        for err in errors:
            if err in content:
                break
        else:
            print content,
            print 'the passphrase is %s' %(line.strip())
            f.close()
            return

if __name__ == '__main__':
    foo()
    print 'ok'
    pass
```

5.TweakPNG可以检查png文件

6. 当图片是bitmap(BMP)，用于处理由像素数据定义的图像的对象(LSB,与MSB相对，是最低有效位，即二进制数的最右端）wbStego可支持bmp隐写

7.gif分解，Gifsplitter

8.音频隐写 mp3Stego,可以在把wav压缩转换成mp3的过程中，对隐藏的txt文件加密压缩写入mp3;

9.zip伪加密，将压缩源文件目录区的全局方式位标记00 00改为09 00就会提示有密码，使用ZipCenOp解密即可（参考http://blog.csdn.NET/ETF6996/article/details/51946250）；

解密命令

```
Decode.exe -x -P password xx.mp3
```

posted on 2017-08-22 10:46 夹心果果 阅读(...) 评论(...) 编辑 收藏
转载于:https://www.cnblogs.com/jiaxinguoguo/p/7410483.html