

图像隐写工具---steghide

原创

Hydra 于 2018-11-10 20:36:12 发布 12787 收藏 15

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_40657585/article/details/83931078

版权



[工具问题](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

背景

先简单描述一下该隐写工具，该工具是在一个隐写rose的题中做到的，也是试了很多种方法，什么stegslope, wbstego，只要是我有的工具基本都试过了，还有其他一些隐写套路，改后缀爆破等等，反正没有得出答案。看了一下题解，需要用到steghide这个工具。

steghide介绍

Steghide是一款开源的隐写术软件，它可以让你在一张图片或者音频文件中隐藏你的秘密信息，而且你不会注意到图片或音频文件发生了任何的改变。而且，你的秘密文件已经隐藏在了原始图片或音频文件之中了。这是一个命令行软件。因此，你需要学习使用这个工具的命令。你需要通过命令来实现将秘密文件嵌入至图片或音频文件之中。除此之外，你还需要使用其他的命令来提取你隐藏在图片或音频中的秘密文件。

用法介绍

--help 自带的介绍

steghide version 0.5.1

the first argument must be one of the following:

embed, --embed	embed data
extract, --extract	extract data
info, --info	display information about a cover- or stego-file
info <filename>	display information about <filename>
encinfo, --encinfo	display a list of supported encryption algorithms
version, --version	display version information
license, --license	display steghide's license
help, --help	display this usage information

embedding options:

- ef, --embedfile select file to be embedded
- ef <filename> embed the file <filename>
- cf, --coverfile select cover-file
- cf <filename> embed into the file <filename>
- p, --passphrase specify passphrase
- p <passphrase> use <passphrase> to embed data
- sf, --stegofile select stego file
- sf <filename> write result to <filename> instead of cover-file
- e, --encryption select encryption parameters
- e <a>[<m>]|<m>[<a>] specify an encryption algorithm and/or mode
- e none do not encrypt data before embedding
- z, --compress compress data before embedding (default)
- z <l> using level <l> (1 best speed...9 best compression)
- Z, --dontcompress do not compress data before embedding
- K, --nochecksum do not embed crc32 checksum of embedded data
- N, --dontembedname do not embed the name of the original file
- f, --force overwrite existing files
- q, --quiet suppress information messages
- v, --verbose display detailed information

extracting options:

- sf, --stegofile select stego file
- sf <filename> extract data from <filename>
- p, --passphrase specify passphrase
- p <passphrase> use <passphrase> to extract data
- xf, --extractfile select file name for extracted data
- xf <filename> write the extracted data to <filename>
- f, --force overwrite existing files
- q, --quiet suppress information messages
- v, --verbose display detailed information

options for the info command:

- p, --passphrase specify passphrase
- p <passphrase> use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt

To extract embedded data from stg.jpg: steghide extract -sf stg.jpg

用法示例:

将secret.txt文件隐藏到text.jpg中:

```
# steghide embed -cf test.jpg -ef secret.txt -p 123456
```

从text.jpg解出secret.txt:

```
#steghide extract -sf test.jpg -p 123456
```

爆破密码

```

#!/usr/bin/python
# -*- coding:utf8 -
from subprocess import *

def foo():
    stegoFile='C:\Users\ppp\Desktop\rose.jpg'
    extractFile='C:\Users\ppp\Desktop\hide.txt'
    passFile='C:\Users\ppp\Desktop\linshi.txt'

    errors = ['could not extract', 'steghide --help', 'Syntax error']
    cmdFormat = "D:\CTF\CTF工具合集\隐写\图像隐写\steghide>steghide.exe 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

```

```

C:\python27-x64\python2.exe D:/untitled2/test_1.py
系统找不到指定的路径。
the passphrase is 123456
ok

```



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)