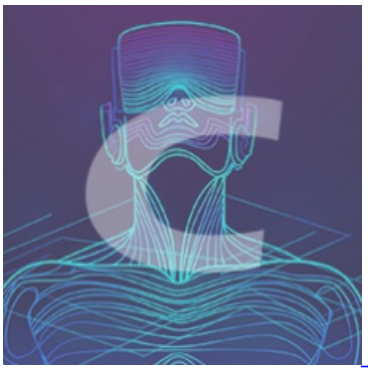
Kali Steghide开源隐写工具

原创

@小张小张 于 2020-09-15 19:23:56 发布 1326 收藏 7

分类专栏： 渗透工具 文章标签： linux 安全漏洞

本文链接：https://blog.csdn.net/weixin_46700042/article/details/108565769



Kali linux Steghide开源隐写工具

1.介绍(图像隐写工具—steghide)

Kali Linux操作系统通常被用来做渗透和审计工作，但是除此之外，这里介绍另外一个特别的功能：将目标文件隐藏到图片或者音频中。Steghide是一款开源的隐写术软件，它可以让你在一张图片或者一个音频文件中隐藏你的秘密信息，而且不会让别人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，也可以提取你隐藏在图片或音频中的秘密文件；

2.安装steghide工具到Kali linux中

如果你的Kali Linux还没有更新过的话，那么执行以下命令进行更新。

```
# apt-get update
```

当系统更新完毕后，采取在线安装的方式把steghide工具装入到你的kali系统中。

```
# apt-get install steghide
```

如果不是root权限的话，记得前面加上sudo。

安装完成以后，可以用steghide --help命令查看一下帮助说明。

3.使用steghide隐藏文件

为隐藏文件，我们首先得准备待隐藏的文件和待隐藏文件的载体（图片或者音频文件），我们可以把两个文件放到同一个目录下。

启动终端，进入测试目录。创建测试带隐藏文件：

vim test.txt

在文件中写入测试内容：IT hidden in the picture!!

3.1 隐藏文件

接下来我们按一下方式执行命令：

1.steghide embed -cf [图片文件载体] -ef [待隐藏文件] 2. [回车] 3. 输入密码，提取文件时用到，如果不想设密码，直接按回车 4. [ENTER]

hide

打开一下图片，并没有发现什么异常。

bk

3.2 查看已嵌入目标文件的图片的文件信息

使用以下命令显示隐藏在文件中的信息。

steghide info background.jpg

hiinfo

3.3 提取隐藏的文件

把含有隐藏文件的图片换一个目录，这里把它拷到了桌面上，进行以下提取实验。

steghide extract -sf background.jpg

extract

---

4. 常用用法介绍：

steghide embed -cf picture.jpg -ef secret.txt
然后设置密码。
该命令将文件secret.txt嵌入到封面文件picture.jpg中；

同时在您嵌入您的秘密数据之后，您可以将文件picture.jpg发送给应该收到密码的人员。接收方必须以下列方式使用steghide：
steghide extract -sf picture.jpg
运用如上命令，然后输入设置方设置的密码就可以得到隐藏文件;

如果您收到包含嵌入式数据的文件，并且要在提取该文件之前获取相关信息，请使用info命令：
steghide info picture.jpg
输入密码后就可以得到该文件的相关信息;

用法示例：
将post.txt文件隐藏到xxx.jpg中：
steghide embed -cf xxx.jpg -ef post.txt -p 123456（不加-p参数 不设置密码 ）

从xxx.jpg解出post.txt:
steghide extract -sf xxx.jpg -p 123456（-p 密码）

stegsolve：
可以发现图片下隐藏的东西，
可以查看动图的帧数;

或者通过箭头能发现意外的东西

还有通过修改图片宽和高获得图片下隐藏的信息，工具用winhex来修改宽和高的数据在第二行，前四位为宽，后四位为高。

5.常用参数：

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 display information about
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 embed into the file 'filename'
-p, --passphrase specify passphrase
-p use 'passphrase' to embed data
-sf, --stegofile select stego file
-sf write result to 'filename' instead of cover-file
-e, --encryption select encryption parameters
-e none do not encrypt data before embedding
-z, --compress compress data before embedding (default)
-z using level (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 extract data from
-p, --passphrase specify passphrase
-p use to extract data
-xf, --extractfile select file name for extracted data
-xf write the extracted data to
-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 use 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