图片隐写方法

原创

君陌上 于 2021-07-16 15:18:57 发布 486 收藏 2

图片隐写概念

顾名思义，就是将想要表达的信息隐藏在图片中。

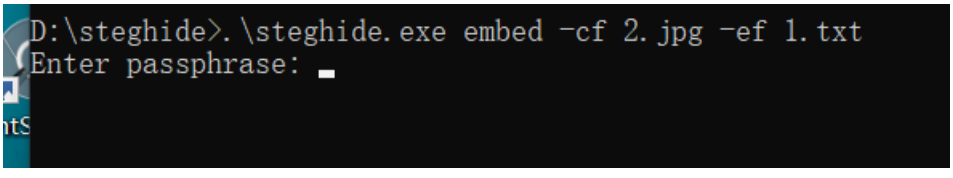
使用工具

1、cmd命令
2、steghide

下载网址;http://steghide.sourceforge.net/download.php

步骤

1、打开命令提示符，进入到steghide文件夹
2、输入\steghide>.\steghide.exe embed -cf 2.jpg -ef 1.txt
然后给出一个密码即可。
3、提取文字：wrote extracted data to"1.txt"



notepad 1.txt即可

binwalk

在ctf中我们没有密码，就需要binwalk这个工具。

注意：这个工具需要python3环境，对于安装可以参考博客：binwalk

用法：

1、-e 分解出压缩包

binwalk -e pcat.bin

2、-D或者–dd 分解某种类型的文件（在windows里要用双引号括起来）

binwalk -D=jpeg pcat.bin

3、-M 递归分解扫描出来的文件（得跟-e或者-D配合使用）

binwalk -eM pcat.bin

4、-h寻求其他用法

```
Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence
of bytes
    -A, --opcodes               Scan target file(s) for common executable opcod
e signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type[:ext[:cmd]]>  Extract <type> signatures (regular expression),
 give the files an extension of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 le
vels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (de
fault: current working directory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extrac
tion utilities
    -V, --subdirs               Extract into sub-directories named by the offse
t

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analysis

    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold (
default: 0.95)
    -L, --low=<float>           Set the falling edge entropy trigger threshold
(default: 0.85)

Binary Diffing Options:
    -W, --hexdump               Perform a hexdump / diff of a file or files
    -G, --green                 Only show lines containing bytes that are the s
ame among all files
    -i, --red                   Only show lines containing bytes that are diffe
rent among all files
    -U, --blue                  Only show lines containing bytes that are diffe
```