

bugku-writeup-MISC-你想要的种子嘛

原创

dark2019 于 2021-07-22 10:30:54 发布 51 收藏

分类专栏: [信息安全 wp](#) 文章标签: [杂项 bugku](#)

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_22597955/article/details/118991922

版权



[信息安全](#) 同时被 2 个专栏收录

53 篇文章 1 订阅

订阅专栏



[wp](#)

31 篇文章 0 订阅

订阅专栏

题目: 你想要种子嘛

考察点: 图片隐写

工具: steghide

binwalk

010 editor

想要种子吗

MISC

已解决

分数: 20

金币: 2

题目作者: [V3geD4g](#)

一血: [Tokeii](#)

一血奖励: 2金币

解决: 249

提示:

描述: flag{}

其他: [↓ torrent.jpg](#)

请输入flag

提交

https://blog.csdn.net/qq_22597955

01—steghide

安装命令:

```
apt-get install steghide
```

查看使用手册:

```
steghide --help
```

```
(kali㉿kali)-[~/Desktop/lx/123]
└─$ steghide --help
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
```

查看文件信息:

```
steghide info torrent.jpg
```

```
(kali㉿kali)-[~/Desktop/lx]
└─$ steghide info torrent.jpg
"torrent.jpg":
  format: jpeg
  capacity: 549.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "123.txt":
    size: 53.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

提取文件:

```
steghide extract -sf torrent.jpg
```

```
(kali@kali)-[~/Desktop/lx]
└─$ steghide extract -sf torrent.jpg
Enter passphrase:
wrote extracted data to "123.txt".
```

得到123.txt, https://pan.baidu.com/s/1oXOf-mKm5TOrbNWg0suWfg_m6qn

```
/home/kali/Desktop/lx/123.txt - Mousepad
File Edit Search View Document Help
https://pan.baidu.com/s/1oXOf-mKm5TOrbNWg0suWfg_m6qn
```

使用百度网盘下载, 得到123.zip, 其中包含加密的123.png, hin.txt文件

```
123.zip
Archive Edit View Help
+ ↑ Open Extract + +
← → ↑ Location: /
Name Size Type Date Modified
123.png 83.4 kB PNG image 17 January 2021, 01...
hin.txt 11 bytes plain text do 17 January 2021, 02...
```

打开hint.txt文件:

```
/home/kali/.cache/fr-k6nZy7/hint.txt - Mousepad
File Edit Search View Document Help
six six six|
```

尝试使用666, 打开123.png, 错误; 使用666666, 打开123.png, 正确。



傻了吧,
这里啥都没有

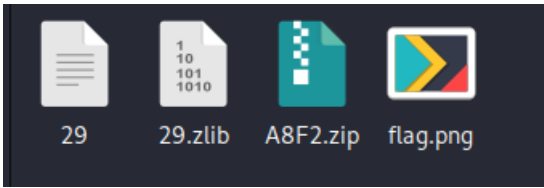
得到123.png。

02—binwalk分离

使用binwalk分离图片。

```
(kali@kali)~[~/Desktop/Lx/123]
$ binwalk -e 123.png
```

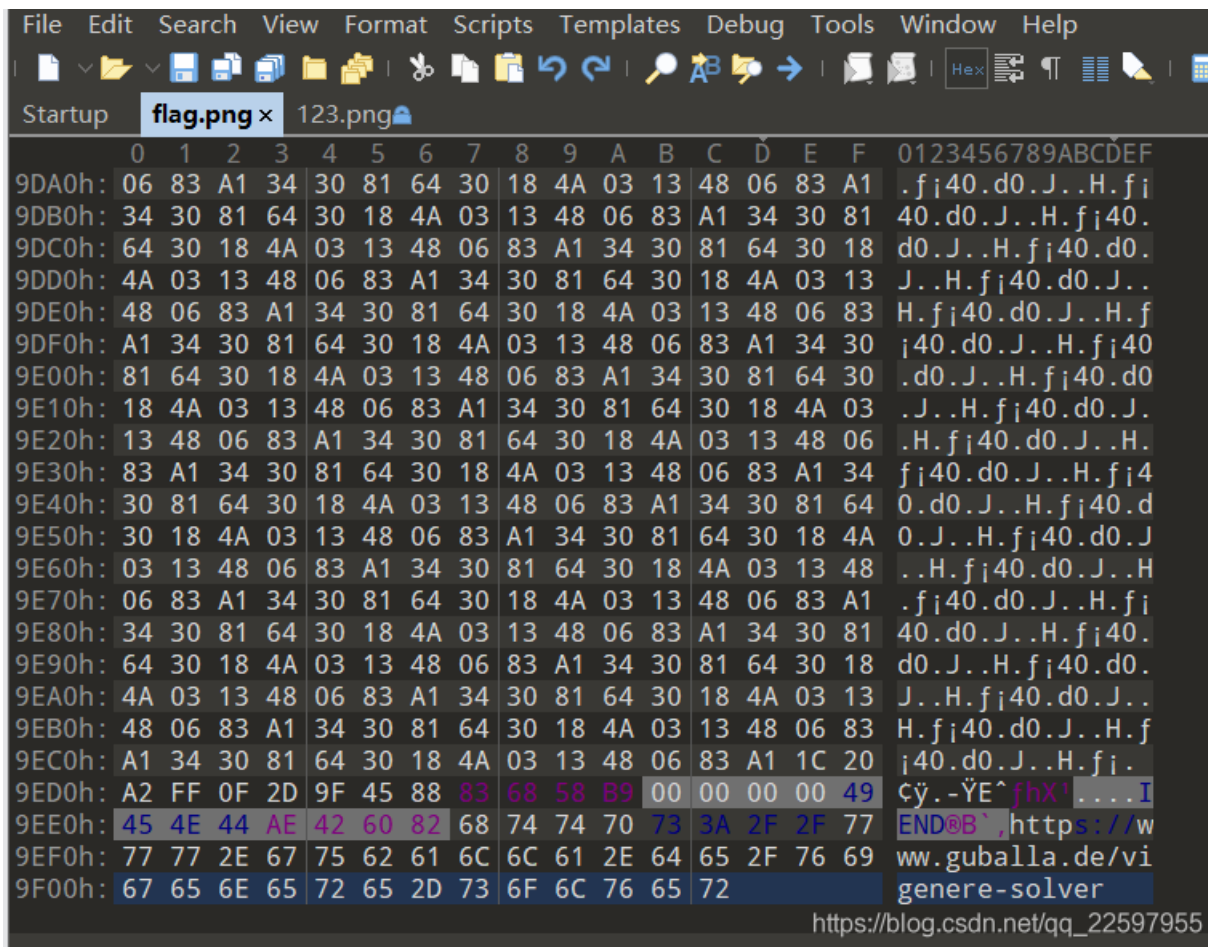
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 292 x 282, 8-bit/color RGBA, non-interlaced
41	0x29	Zlib compressed data, default compression
43250	0xA8F2	Zip archive data, at least v2.0 to extract, compressed size: 40009, uncompressed size: 40717, name: flag.png
83387	0x145BB	End of Zip archive, footer length: 22



得到flag.png。

03—010 editor 编辑图片

使用010 editor打开图片。



下拉框到最后，发现一个链接：

<https://www.guballa.de/vigenere-solver>

修改图片高度，与宽相同。

← → ↻ guballa.de/vigenere-solver

应用 翻译 百度一下, 你就知道 学习资料

support for Portuguese

This time both solvers have learnt to speak Portuguese.

[Weiterlesen ...](#)

2019-12-27 20:47

Solver: Support for Dutch added

The [Vigenere Solver](#) as well as the [Substitution Solver](#) now speak one additional language: Dutch. Some work was required, as my favorite site does not provide ngrams for Dutch.

[Weiterlesen ...](#)

Cipher Text:
fkyg(SfirsXmuqRoqpmr)

Cipher Variant: Classical Vigenere ▾
Language: English ▾
Key Length: 3-30
(e.g. 8 or a range e.g. 6-10)

Break Cipher Clear Cipher Text

Result

Clear text [\[hide\]](#)

Clear text using key "azy":
flag(Th1s1sY0urT0rrent)

https://blog.csdn.net/qq_22597955

解码，得到flag。

写在最后：解题思路为查找隐藏信息-解密-再次查找隐藏信息-解密，本题为多重信息隐藏，需要耐心不断查找，再加以解密，得到结果。