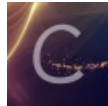


隐写术 - 有用工具和资源的列表

转载

[浅汐、沐雪](#) 于 2019-06-12 21:21:59 发布 2376 收藏 7

分类专栏: [CTF](#) 文章标签: [隐写术](#)



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

隐写术

工具

[Steghide](#)

[Foremost](#)

[Stegsolve](#)

[strings](#)

[Exiftool](#)

[Exiv2](#)

[Binwalk](#)

[Zsteg](#)

[Wavsteg](#)

[Sonic visualizer](#)

[Bruteforc3rs](#)

[StegCracker](#)

[Fcrackzip](#)

网络工具

[Unicode文本隐写术](#)

[np1et在线](#)

[dcode.fr](#)

挑战

隐写术将文件或消息隐藏在另一个文件中，有许多有趣的隐写CTF挑战，其中标志隐藏在图像，音频文件甚至其他类型的文件中。这是我使用的大多数工具和一些其他有用资源的列表。

注意：此列表将定期更新，如果您有任何建议，请随时到下午

最后更新：29.1.2019

工具

Steghide

Steghide是一个隐藏数据的程序，可以隐藏各种图像和音频文件中的数据，只支持这些文件格式：JPEG, BMP, WAV and AU。但它对从其他文件中提取嵌入和加密数据也很有用。它可以安装 `apt` 并且源可以在github上找到。

有用的命令：

```
steghide info file :显示有关文件是否包含嵌入数据的信息。  
steghide extract -sf file :从文件中提取嵌入数据
```

Foremost

Foremost是一个程序，它根据页眉，页脚和内部数据结构恢复文件，我发现它在处理png图像时很有用。它可以安装 `apt` 并且源可以在github上找到。

有用的命令：

```
foremost -i file : 从给定文件中提取数据。
```

Stegsolve

有时在图像本身中隐藏着一条消息或文本，为了查看它，您需要应用一些颜色过滤器或使用颜色级别。您可以使用GIMP或Photoshop或任何其他图像编辑软件，但stegsolve使它更容易。它是一个小型的java工具，可以在图像上应用许多颜色过滤器。我个人认为它非常有用。你可以从github得到它

strings

Strings是一个linux工具，可以在文件中显示可打印的字符串。在解决隐秘挑战时，这个简单的工具非常有用。通常，嵌入数据受密码保护或加密，有时密码是文件本身的密码，可以通过使用字符串轻松查看。这是一个默认的linux工具，所以你不需要安装任何东西。

有用的命令：

```
strings file : 在给定文件中显示可打印的字符串。
```

Exiftool

有时重要的东西隐藏在图像或文件的元数据中，exiftool可以非常有助于查看文件的元数据。你可以从[这里](#)得到它

有用的命令：

```
exiftool file : 显示给定文件的元数据
```

Exiv2

一种类似于exiftool的工具。

它可以安装， `apt` 并且

可以在github上找到。

[官方网站](#)

有用的命令：

```
exiv2 file : 显示给定文件的元数据
```

Binwalk

Binwalk是一种用于搜索嵌入式文件和数据的图像和音频文件等二进制文件的工具。

它可以安装，`apt` 并且源可以在github上找到。

有用的命令：

```
binwalk file : 显示给定文件中的嵌入数据  
binwalk -e file : 显示和提取给定文件中的数据
```

Zsteg

zsteg是一个可以检测png和bmp文件中隐藏数据的工具。

安装它： `gem install zsteg`，源可以在github上找到

有用的命令：

```
zsteg -a file : 运行给定文件上的所有方法  
zsteg -E file : 从给定的有效负载中提取数据（例如： zsteg -E b4, bgr, msb, xy name.png）
```

Wavsteg

WavSteg是一个python3工具，可以隐藏wav文件中的数据和文件，也可以从wav文件中提取数据。

你可以从github得到它

有用的命令：

```
python3 WavSteg.py -r -s soundfile -o outputfile : 从wav声音文件中提取数据并将数据输出到新文件中
```

Sonic visualizer

Sonic visualizer声波可视化工具是一种用于查看和分析音频文件内容的工具，但在处理音频隐写时它会很有用。您可以在音频文件中显示隐藏的形状。

官方网站

Bruteforcers

StegCracker

使用steghide强制密码的工具

Fcrackzip

有时提取的数据是受密码保护的zip，此工具强制执行zip存档。

它可以安装，`apt` 并且源可以在github上找到。

有用的命令：

```
fcrackzip -u -D -p wordlist.txt file.zip : 使用给定wordlist中的密码强制给定zip文件
```

网络工具

Unicode文本隐写术

一个用于unicode隐写术的网络工具，它可以编码和解码文本

npiet在线

piet的在线翻译。piet是一种深奥的语言，piet中的程序是图像。阅读更多关于piet的[信息](#)

dcode.fr

有时在解决隐写术挑战时，您需要解码一些文本。dcode.fr有很多解码器，可以提供很多密码，非常有用。

挑战

一些隐写挑战平台

[Hack The Box](#)

[root me](#)

[RingerZeroCTF](#)

转载自：<https://0xrick.github.io/lists/stego/>