Kali linux下图片隐写,图片隐写信息快速检测工具——zsteg

转载

老魏一凡 于 2021-05-14 21:11:44 发布
文章标签： Kali linux下图片隐写

CTF的图片隐写题中有一种常见的题型——基于LSB原理的图片隐写，而最常用工具就是Stegsolve，但是过程还是有些缓慢和复杂，终于在一次比赛中发现了一个强大的工具——zsteg，这是一个用于检测PNG和BMP中的隐藏数据隐藏数据的工具，可以快速提取隐藏信息，下面就以曾遇到的两个例子说明。

安装

Ubuntu中可以使用apt-get命令行工具来安装Ruby和RubyGems，如下所示：

1sudo apt-get install ruby-full rubygems

Kali Linux 中则自带了RubyGems。

然后用以下命令安装zsteg后即可使用：

1$gem install zsteg

对于目标图片，可以分别输入以下命令尝试：

1

2

3$zsteg 你瞅啥.bmp --bits 1 --channel r --lsb --order xy --limit 2048

$zsteg 你瞅啥.bmp --bits 1 --channel g --lsb --order xy --limit 2048

$zsteg 你瞅啥.bmp --bits 1 --channel b --lsb --order xy --limit 2048

各选项含义如下，还有更多选项可以通过-h选项查看

--bits 1：每次只摘取颜色通道中的第 1 个比特。

--channel r：只摘取红色通道的比特位。

--lsb：按最低有效位优先的顺序进行摘取。

--order xy：按照从左至右、从上至下的顺序对图像素点进行摘取。

--limit 2048：最多摘取输出 2048 字节。

QWB-2019 强□先锋-打野

当然，上面给出的选项都太过复杂了，而且在这道题中也发现没有有效信息。所以本文重点想介绍的事--all选项，这是一个懒人专属的选项 ，可将所有可能的摘取方法都尝试一遍：

发现没有有效信息，于是使用一个懒人专属的选项 --all，可将所有可能的摘取方法都尝试一遍：

最终在结果中挑选出可能的隐写信息：qwxf{you_say_chick_beautiful?}

```
# root @ kali in ~ [11:07:20]
$ zsteg 01.bmp --all
[?] 2 bytes of extra data after image end (IEND), offset = 0x269b0e
extradata:0         .. ["\x00" repeated 2 times]
imagedata           .. text: ["\r" repeated 18 times]
b1,lsb,bY           .. <wbStego size=120, ext="\x00\x8E\xEE", data="\x1Ef\xDE\x9E\xF6\xAE\xFA\
 even=false>
b1,msb,bY           .. text: "qwxf{you_say_chick_beautiful?}"
b2,msb,bY           .. text: "i2,C8&k0."
b1,lsb,bY,prime     .. text: "riI?/1>^J"
b3,lsb,bY,prime     .. text: "QE 9)\"IE\""
b4,lsb,bY,prime     .. text: "RBRC44T#4$4D52C2"
b5,msb,bY,prime     .. text: "ram9u!J1"
b6,lsb,bY,prime     .. file: GeoSwath RDF
b2,r,lsb,xY         .. text: "UUUUUU9VUUUUUUUUUUUUUUUUUUUUUU"
```

网鼎杯-2018 第二场 套娃

同样的，2018网鼎杯的一道题也可以用同样的方法做出来：

```
# root @ ubuntu in ~/套娃/2/3/4/5/6 [22:10:21]
$ zsteg 6.png --all | grep flag
b1,bgr,lsb,xy       .. text: "+flag{03a253f5-8e93-4533-bcfc-af908830095d}\nq"
```