

20210201Misc第一课 图片隐写

原创

4XWi11 于 2021-02-02 13:02:56 发布 626 收藏

分类专栏: #M1sc

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/m0_49109277/article/details/113550149

版权



[M1sc 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

图片隐写

一、图片隐写类型

- 右击属性
- 文件末尾藏有字符串
- 文件包含
- 修改文件头
- GIF
- png(bmp)
- JPG
- 双图隐写
- stegpy
- slienteye

二、每种类型的综述

通用情况

- 对于图片文件，在没给出文件后缀名的情况下，用010edit查看内码判断，或者在kali下可以显示图片的缩略图，或者可以用

```
file + 该文件名
```

- kali下的一些命令

```
binwalk file # 检查图片是否隐写别的文件
binwalk -e file # 效果稍用不同，在一些情况下特别有用
foremost file # 分离图片和图片中隐写的文件
dd if=file of=out.jpg bs=1 skip=271007 # 可以针对性分离某个文件，在隐写文件较多的情况下使用
```

- kali下查看JPG图片内码的命令：

```
strings file
```

- 破坏文件头，一定不能显示，破坏文件尾，文件不一定显示不正常

JPG

文件起始标志：FFD8~FFD9

kali下查找JPG图片内码中的字符

```
grep -a "你要查找的字符" file
```

png

1. 文件起始标志：89 50 4E 47 ~ IHDR ~ 49 48 44 52

2. 修改IHDR 修改高度隐写：

1. 选中49~00，CRC-32校验是否正确

2. 用脚本爆破

3. IDAT 隐写

1. pngcheck工具

2. zlib脚本

```
#!/usr/bin/env python
import zlib
import binascii
IDAT = "0025BB07654A7B7AFAD6AF7EFFD75E69EE2F5BE77F79DDAFF7FDE63F37C537F6EDF2FF5CEEEEEB1FE8FDEF6005F000
000025BB2B6D4E7A7A2AF6EFFE7FC74E4B8E2F5BE77B79D5AFF7FFEE3F76C537F4FDFAFB7CFEF6FB3AE8F5EB0000600000025
BB2B79EE7A796BE6FFF7BC7CE4B8EA95B263BD9DFB756FFFF3F76C777F6DCEE77F054FC733EF8F7E000000000000213A6F79
EE7A59DBA3DFFFFB87CD4BCEA95B363BD9DFB756FFFF3F76C777F6DCEE77F054FC733EF8F7E00000000000029B26F7DE67A53
DBE3FFFFFAA78D4BCEADDB163BD1DABFD6EFD3F7ACF57F6DCEE5F0D4FE723CAFF8000000000000029B76F5DEF7A7BF3C9FB2FFBA7
9FF3DBADDC9643B99E1FF76F9FBFDACF4FB6DCEAFECFCFFD42CF AFC000000000000000BB74777CF5A7BF2C8F745BDB7BFF3D9
ADFE9643FB9E3EF7AE5FBFBECF1FB6D4E2FFECADFFF42CFAE8000000000000000EB75367CF5AFBE2D8E444BDB7BFF3D1ADFE96
5AFB9CBFF78E5FBFEFCF1FB4D4EAFECB7F4FE74FBE000000000000002EAF5A23EF7AFBE2D9FC4675B7FAFBD1CFBEA67AFB9C
B9A78ADFBAFECF9FB49CFEFC7774FE74FFE000000000000002F0F5F23AF72FBE2D9FC47F537FAFBDBC73EA67CFB9CB7878D
DFBBF6CE9BF69CFEFC577CFEFCFD800000000000002F9A5F27E772FB82D1FDD7F4377AFBDB472EEA7FFB9CB787ADDFBFF6
CA99F6D9DCFF2857FCFAFEFD800000000000002F9A5F65E73AFB82F9F9D3F6F77E7A9B4FAFEAFFD9C9F87EFDE3F76C38DF6
-----"
```


3. binwalk -e file

GIF

工具

1. ps
2. stegsolve
3. Ulead GIF 帧持续时间转换成二进制0 1或者摩斯 ·-

LSB隐写

LSB最低有效位颜色