

# MISC入门之图片隐写

原创

laugholy 于 2020-08-11 16:19:00 发布 744 收藏 3

分类专栏: [笔记](#)

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/weixin\\_45986910/article/details/107934185](https://blog.csdn.net/weixin_45986910/article/details/107934185)

版权



[笔记 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

## ## CTF小白入门MISC之图片隐写##

图片隐写是MISC中的一部分。

小白从BUU中找到一些题目入门MISC之图片隐写 (大佬轻点打)

1.qr

直接下载得到附件



1abe854d-4770  
-4214-829b-bf6  
ff513fa14.png

扫码得到flag: (这里和下面就不把flag直接贴出来了, 自己实操比较有用, 想直接要flag直接就可以百度到)

这里通过这道题简单介绍下图片的文件格式

JPEG (jpg),	文件头: FFD8FF
文件尾: FF D9	
PNG (png),	文件头: 89504E47
文件尾: AE 42 60 82	
GIF (gif),	文件头: 47494638
文件尾: 00 3B	

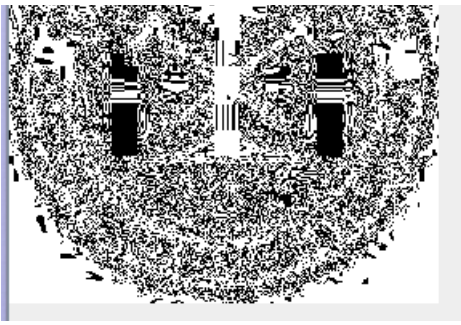
png和gif都是使用无损数据压缩的, jpg是有损压缩。jpg却更广泛

用于互联网中图片的传播使用。

2.LSB

下载得到附件, 根据提示LSB使用Stegsolve可以看到r,g,b的plane0上面都有东西





Extract Preview		
004e470d0a1a0a	0000000d49484452	.PNG.... .IHDR
0011800000118	080200000008ec7e	.....~
0000542494441	54789ceddd416e23	....BIDA Tx...An#
000416931ffff	b2f707c480932e57	9..Ail..
0157c3564b5682	8702c9f7d7d70b	..W.VKV.
07ffdf403c027	1012048404012141	.7.....' .....
08101012048404	012141e0cfe167ef	@H..... !A...g.
0bec39729383e6	c30775788cbbdfca	{.9r... ..ux....
0fe5bbb7bcdff9	9f62458280902020	..... .bE...

查看三原色的最低有效位发现隐写了图片

将其保存为png格式，得到二维码，扫描得到flag

简单补充一下LSB隐写的知识：

图片的颜色由三原色RGB（red,blue,green）混合而成，每种颜色从浅到深分为八个色阶。plane 0是最浅的，如果改变它我们用肉眼很难发现区别。LSB隐写就是改变RGB的plane 0，也就是最低有效位将一些信息存入其中。

### 3.大白

观察可以发现图片好像少了一部分

Name	Value	Start	Size	Color
> struct PNG_SIGNATURE ...		0h	8h	Fg: Bg:
> struct PNG_CHUNK chun...	IHDR (Criti...	8h	19h	Fg: Bg:
> struct PNG_CHUNK chun...	sRGB (Ancil...	21h	Dh	Fg: Bg:

打开010editor修改图片的大小

得到flag

### 4.flag

教练，我要打CTF

没发现有什么特殊的，binwalk一下也没发现什么，看一下LSB发现zip文件

Extract Preview		
504b030414000000	0800dd855d49fd91	PK..... ]I..
e24cd90800003d21	00000100000003led	.L....=! .....
5959cc0b5114be1d	b5336aafbdb10589	YY..Q... .3j.....
aa7d0b5afc4ca5f6	da6219d5e94fe942	.)Z.L.. .b...O.B
3bb56fb145637df0	8044e2c10389074f	;.o.Ec}. .D.....O
b648ac41c4c34f42	244844ec5bec1141	.H.A..OB \$HD.[..A
9d7be74c6f67e127	112fdce6ce37e7bb	{.Log.' ./...7..
e79c7beedab9336b	ca4223048783e849	..{...3k .B#....I
20830995fc4e3f93	fdc82faccf00b97e	....N?. ..../....~

需要对各种文件的格式稍微敏感一些，解压之后发现是ELF文件。在linux系统下运行得到flag

```
it. 未预期的符号 '1' 附近有语法错误
@kali:~/桌面$ ./flag
fidd0gfk67tok2yb0ard/g/1pwwjxub2ka1:~/桌面$
```

#### 5.乌丰镇会种图

使用010editor打开，最后可以找到flag。或者直接搜索得到flag

#### 6.你竟然赶我走

同样在010editor找到flag。