图片隐写题思路

原创

stars77 于 2019-05-31 17:00:32 发布

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42040292/article/details/90719439

图片隐写题思路

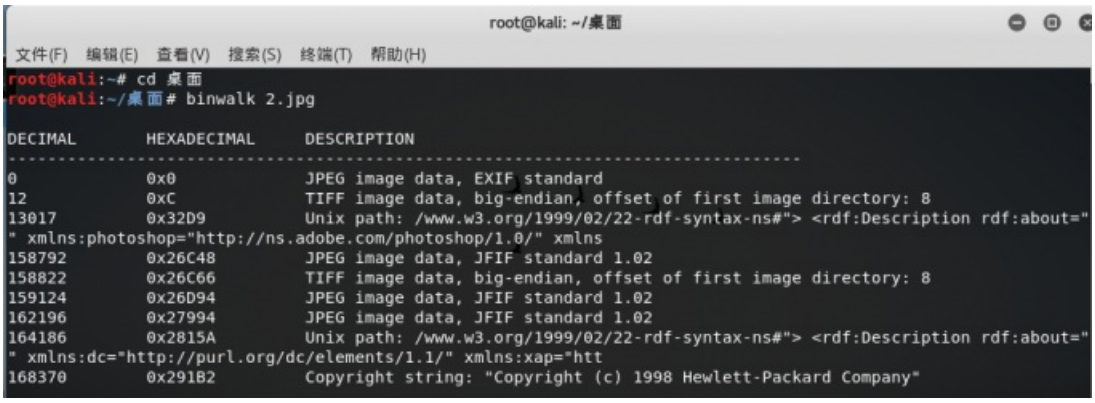
做CTF杂项的时候会碰到让下载图片，从图片里面找flag，这里介绍两个软件binwalk和foremost,它可以查看下载的文件中是否包含其它文件。

0X01 binwalk相关命令

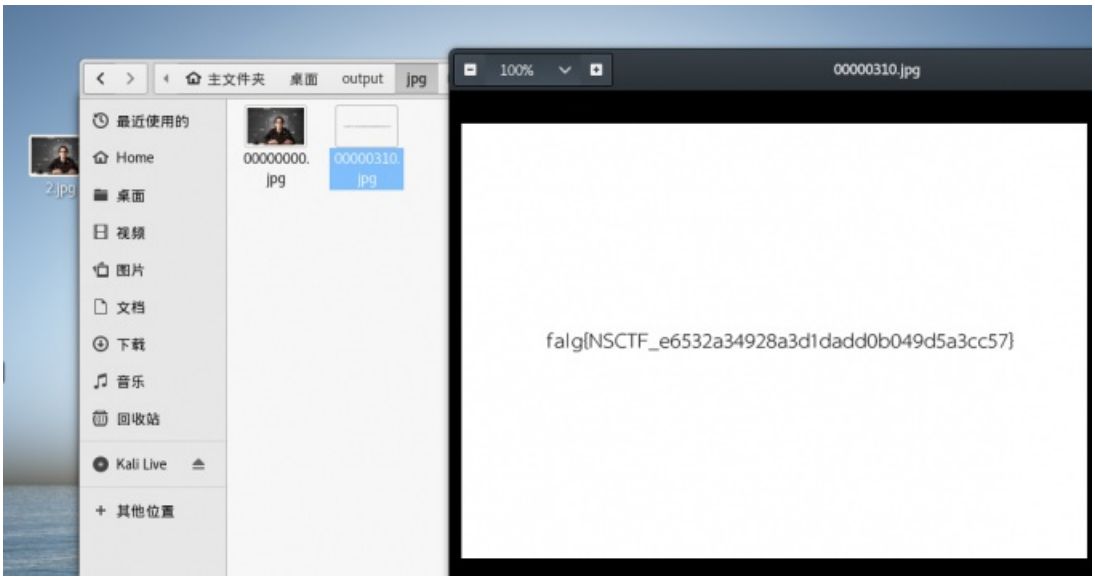
打开kail，直接在终端输入binwalk（前提是kali安装了这个软件，如果没有需要自己搜一下具体安装方法）。打开软件后，使用命令“binwalk -e 文件路径”就可以分离所需要分离的文件了。

这里以bugku一道题为例，下载后来得到如下图片：

将这张图片放到桌面并用binwalk打开它



这里可以看到这张图片里包含了两个图片文件，159124和162196，用命令“binwalk -e 文件路径”将其分离随后得到另一张含有flag的图片



0X02foremost相关命令

foremost的命令是"foremost -T 文件名"，然后会在桌面有一个输出文件夹，里面就会有分离出来的含有flag的图片。

0X03 "dd"相关命令

使用方法如下

```
root@kali:~/桌面# dd if=2.jpg of=2-1.jpg skip=158792 bs=1
记录了27689+0 的读入
记录了27689+0 的写出
27689 bytes (28 kB, 27 KiB) copied, 0.0785581 s, 352 kB/s
```

相关的其它命令如下

dd命令使用详解

1.命令简介
dd 的主要选项:

指定数字的地方若以下列字符结尾乘以相应的数字:

b=512, c=1, k=1024, w=2, xm=number m

if=file #输入文件名，缺省为标准输入。
of=file #输出文件名，缺省为标准输出。
ibs=bytes #一次读入 bytes 个字节(即一个块大小为 bytes 个字节)。
obs=bytes #一次写 bytes 个字节(即一个块大小为 bytes 个字节)。
bs=bytes #同时设置读写块的大小为 bytes ，可代替 ibs 和 obs 。
cbs=bytes #一次转换 bytes 个字节，即转换缓冲区大小。
skip=blocks #从输入文件开头跳过 blocks 个块后再开始复制。
seek=blocks #从输出文件开头跳过 blocks 个块后再开始复制。(通常只有当输出文件是磁盘或磁带时才有效)。
count=blocks #仅拷贝 blocks 个块，块大小等于 ibs 指定的字节数。
conv=conversion[,conversion...] #用指定的参数转换文件。