MISC中图片隐藏文件分离

原创

Alst0n 于 2019-09-28 11:45:36 发布 2039 收藏 30

分类专栏： MISC 文章标签： CTF MISC 图片隐藏文件分离 binwalk foremost

本文链接：https://blog.csdn.net/Sc0fie1d/article/details/101602492

0x00介绍

在CTF的MISC中，经常会将flag隐藏在图片中。我们可以用Linux下的 `binwalk` 或者 `foremost` 进行图片文件的分离，这里我们选用分别介绍两种方法。

在Kali Linux上安装binwalk和foremost：

```
# apt-get install binwalk
# apt-get install foremost
```

题目中给出的图片如下图所示，图片名称为2.jpg，从图片中我们得不到任何信息：

0x01 Binwalk

分析

我们用binwalk分析图片的组成：

```
# binwalk 2.jpg
```

```
root@kali:~/Downloads# binwalk 2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
40078         0x9C8E          Zip archive data, at least v2.0 to extract, compressed size: 19, uncompressed size: 17, name: flag.txt
40225         0x9D21          End of Zip archive, footer length: 22
```

从分析结果中我们可以看到，图片文件中隐藏了一个名为flag.txt的文件，而且是被压缩过的，其起始块是40078。

分离

我们使用`dd`命令分理出隐藏在图片中的.zip文件：

```
# dd if=2.jpg of=1.zip skip=40078 bs=1
```

其中`if=2.jpg`是输入文件，`of=1.zip`是输出文件，`skip`是指定从输入文件开头跳过40078个块后再开始复制，`bs`设置每次读写块的大小为1字节 。

```
root@kali:~/Downloads# dd if=2.jpg of=1.zip skip=40078 bs=1
169+0 records in
169+0 records out
169 bytes copied, 0.000865345 s, 195 kB/s
root@kali:~/Downloads# ls
1.zip  2.jpg
root@kali:~/Downloads#
```

然后我们将分离出来的1.zip解压，就可以看到flag：

```
root@kali:~/Downloads# unzip 1.zip
Archive:  1.zip
  inflating: flag.txt
root@kali:~/Downloads# cat flag.txt
Asuri{never_m1nd}root@kali:~/Downloads#
root@kali:~/Downloads#
```

0x02 Foremost

利用以下命令：

```
foremost 2.jpg
```

可以直接将图片文件中包含的所有文件分离，输出到一个output文件夹中。打开这个文件夹，我们可以看到audit.txt为记录分离过程的文件，jpg为该图片文件中包含的所有.jpg文件，zip为该图片文件中包含的所有.zip文件。打开zip文件，并解压其中的00000078.zip，就可以得到flag。