关于CTF中的一些图片隐写

原创

CY_BRYANT 于 2020-01-26 19:39:39 发布 4192 收藏 23
分类专栏： CTF 文章标签： linux

本文链接：https://blog.csdn.net/qq_43721475/article/details/104088919


CTF 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

CTF中图片隐藏文件分离方法总结

前言

可以使用winhex之类的工具先行分析其是否为图片，可以看其头部信息，还有就是JPG图片有一个特性最后的应用数据块为FF E0 活着直接使用binwalk看看图片下有什么鬼玩意儿的。

binwalk分离

```
命令：binwalk -e 图片路径
```

foremost分离

foremost分离

```
命令：foremost 图片地址        #会在图片地址的目录下生成一个output的文件夹。输出到里面了。
```

dd分离

```
命令：dd if=要分离的图片名.jpg of=分离出来的图片名.jpg skip=偏移量 bs=1
```

图片隐藏flag怎么找

首先我们需要对图片进行分析，这里我们需要用到一个工具 binwalk ，想要了解这个工具可以参考这篇 Binwalk：后门（固件）分析利器 文章，以及 kali官方对binwalk的概述和使用介绍 。

这里我们就是最简单的利用，在binwalk后直接提供固件文件路径和文件名即可:
binwalk carter.jpg
在得到隐藏信息之后我们下一步就是把另一张jpg分离出，以下讨论几种方法：

（1）使用dd命令分离(linux/unix下)

我们可以使用dd命令分离出隐藏文件：
dd if=carter.jpg of=carter-1.jpg skip=140147 bs=1
可以参考 dd命令详解 ，这里if是指定输入文件，of是指定输出文件，skip是指定从输入文件开头跳过140147个块后再开始复制，bs设置每次读写块的大小为1字节 。
最后我们可以得到这样的一张carter-1.jpg图片：（图2）

（2）使用foremost工具分离

foremost是一个基于文件文件头和尾部信息以及文件的内建数据结构恢复文件的命令行工具，win可以下载地址，Linux可以通过下面命令安装使用：

```
apt-get install foremost
```

安装foremost后你可以使用foremost -help查看使用帮助，这里最简单分离文件的命令为：

```
foremost carter.jpg
```

当我们使用这行命令后，foremost会自动生成output目录存放分离出文件：

（3）hex编辑器分析文件

至于hex编辑器有很多，win下有用得较多的winhex,UltraEdit等，linux下有hexeditor等，这里我们以winhex为例手动分离，在分离之前我们需要知道一点关于jpg文件格式的知识，jpg格式文件开始的2字节是图像开始SOI(Start of Image,SOI)为FF D8，之后2个字节是JFIF应用数据块APPO(JFIF application segment)为FF E0，最后2个字节是图像文件结束标记EOI(end-of-file)为FF D9，如果你想详细了解更多关于这方面的知识可以参考jpg文件格式分析一文。
用winhex打开图片，通过Alt+G快捷键输入偏移地址22373跳转到另一张jpg的图像开始块，可以看到FF D8图像开始块。

• 而图像结束块FF D9

• 选取使用Alt+1快捷键选取FF为开始的块，Alt+2选取D9为结束块，然后右键->Edit->Copy Block->Into New File保存相应的文件后缀，例如new.jpg

• 其他
还有一种特例，它是事先制作一个hide.zip，里面放入隐藏的文件，再需要一张jpg图片example.jpg，然后再通过命令 copy /b example.jpg+hide.zip output.jpg生成output.jpg的新文件，原理是利用了copy命令，将两个文件以二进制方式连接起来，正常的jpg文件结束标志是FF D9，而图片查看器会忽视jpg结束符之后的内容，所以我们附加的hide.zip就不会影响到图像的正常显示。(参考AppLeU0的 隐形术总结)
针对这种特例我们可以直接将jpg文件改为zip文件后缀(其他文件如rar文件也类似)，就可以看到hide.zip压缩包里隐藏的文件。
比如当我们得到一张wh3r3_is_f14g.jpg文件：

• 当我们用winhex打开文件，发现wh3r3_is_f14g.jpg文件最后数据块不是FF D9 jpg文件的结束标志，而是zip文件的结束标志。

• 我们直接将文件改名为wh3r3_is_f14g.zip，打开得到flag.txt。

• 最后打开flag.txt得到flag。