CTFHUB技能树-Misc-数据隐写

原创

老大的豆豆酱 于 2020-08-17 16:27:07 发布 458 收藏 4

分类专栏： CTF 数据隐写 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43486981/article/details/108057934


CTF 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏


数据隐写

1 篇文章 0 订阅

订阅专栏

隐写术

知识点来源参考：https://blog.csdn.net/u011028345/article/details/75311346?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-2.channel_param&depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-2.channel_param

和https://www.cnblogs.com/-chenxs/p/11493898.html

- 隐写术可以利用图片、音频、视频为载体将数据隐藏在其中，将数据隐写到图像中较为常见。
- **图像隐写术**进行数据隐写分为以下几类：
  1.在图片右击查看属性，在详细信息中隐藏数据
  2.将数据类型进行改写（rar或者zip数据改为jpg等格式）
  3.根据各种类型图像的固定格式，隐藏数据
  在编译器中修改图像开始的标志，改变其原来图像格式
  在图像结束标志后加入数据
  在图像数据中加入数据，不影响视觉效果情况下修改像素数据，加入信息
  4.利用隐写算法将数据隐写到图片中而不影响图像（仅限于jpg图像） 隐写常用的算法有F5，guess jsteg jphide。
- **破解隐写术方法及步骤**
  1.查看图像属性详细信息是否有隐藏内容
  2.利用**winhex或nodepad++打开搜索ctf,CTF，flag,key等关键字是否存在相关信息**
  3.检查图像的开头标志和结束标志是否正确，若不正确修改图像标志恢复图像，打开查看是否有flag或ctf信息，（往往gif属于动图，需要分帧查看各帧图像组合所得数据 若不是直接的ctf或flag信息 需要考虑将其解码）

```
jpg图像开始标志：FF D8 结束标志 ：FF D9
gif图像开始标志：47 49 46 38 39 61 (GIF89)结束标志：01 01 00 3B
bmp图片开始标志：42 4D //92 5B 54 00 00 00 00 00 结束标志：00
png图片开始标志：89 50 结束标志：60 82
```

4.将图片放置在kail系统中，执行binwalk xxx.jpg 查看图片中是否是多个图像组合或者包含其他文件（若存在多幅图像组合，再执行foremost xxx.jpg会自动分离；若检测出其他文件修改其后缀名即可，如zip）
5.使用StegSolve对图像进行分通道扫描，查看是否为LSB隐写
6.在kail下切换到F5-steganography，在java Extract运行
命令：java Extract 123456.jpg图片的绝对地址 -p 123456
判断是否为F5算法隐写
7.在kali系统中使用outguess-master工具（需要安装），检测是否为guess算法隐写

- **算法隐写的具体操作**
  1.F5算法隐写
  具体操作：在kail下切换到F5-steganography，在java Extract运行
  命令：java Extract 123456.jpg图片的绝对地址 -p 123456
  2.LSB算法隐写
  具体操作：在Stegsolve.jar分析data Extract的red blue green
  3.guess算法隐写
  具体操作：在kail下切换到outguess目录下，直接用命令即可
  命令:outguess -r /root/angrybird.jpg(绝对路径) 123.txt(信息存放的文本)

图片简单隐写

题目附件下载下来是个二维码，

微信扫一扫发现是CTFHUB的公众号。

使用winhex工具打开图片，在文件最后发现了flag（这里使用的是上述破解隐写术方法中的第二种）