图片隐写

原创

Nebula1805 于 2021-02-09 16:09:48 发布 150 收藏 2

分类专栏： 涅普冬令营学习笔记 文章标签： 其他

本文链接：https://blog.csdn.net/Nebula1805/article/details/113757980

涅普冬令营学习笔记 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

涅普冬令营第一课-------图片隐写 入口

1.图片属性信息

右击图片属性，查看详细信息是否隐藏数据

2.文件十六进制藏有字符串

- strings查找可打印的字符（kali预装）
  格式：strings Tile
- grep使用正则表达式搜索,并输出匹配的行
  格式：grep flag
- file识别文件类型
  格式： file 文件

3.文件包含

- binwalk分离文件 (kali预装)（详细使用）.
  binwalk file
  binwalk -e file
  window下：binwalk windows安装和使用方法.
- foremost提取文件
  foremost file
  formost -t需要恢复文件类型后缀(如jpg)-扫描的分区-o指定存放文件的目录
  指定存放文件的目录必须为空,不然会报错
  也可以用dd
  dd if=1. pcapng of=1.7z bs=1 skip=24437
  dd命令使用详解.
  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

4.修改文件头

在编译器中修改图像开始的标志，改变其原来图像格式

详见: 常见到的文件头和文件尾.

文件类型	文件头	文件尾
JPEG (jpg)	FF D8 FF	FF D9
PNG (png)	89 50 4E 47	AE 42 60 82
GIF (gif)	47 49 46 38	00 3B
TIFF (tif)	49 49 2A 00	
Windows Bitmap (bmp)	42 4D	
ZIP Archive (zip)	50 4B 03 04	50 4B
RAR Archive (rar)	52 61 72 21	07 00
CAD (dwg)	41 43 31 30	
Adobe Photoshop (psd)	38 42 50 53	
Rich Text Format (rtf)	7B 5C 72 74 66	
XML (xml)	3C 3F 78 6D 6C	
HTML (html)	3C 68 74 6D 6C	3C 2F 68 74 6D 6C 3E
Email thorough only (eml)	44 65 6C 69 76 65 72 79 2D 64 61 74 65 3A	
Outlook Express (dbx)	CF AD 12 FE C5 FD 74 6F	
Outlook (pst)	21 42 44 4E	
MS Word/Excel (xls or doc)	D0 CF 11 E0	
MS Access (mdb)	53 74 61 6E 64 61 72 64 20 4A	
WordPerfect (wpd)	FF 57 50 43	
Postscript (eps or ps)	25 21 50 53 2D 41 64 6F 62 65	
Adobe Acrobat (pdf)	25 50 44 46 2D 31 2E	
Quicken (qdf)	AC 9E BD 8F	
Windows Password (pwl)	AC 9E BD 8F	
Wave (wav)	57 41 56 45	
AVI (avi)	41 56 49 20	
AVI (avi)	41 56 49 20	
Real Audio (ram)	2E 72 61 FD	
Real Media (rm)	2E 52 4D 46	
MPEG (mpg)	00 00 01 BA	
MPEG (mpg)	00 00 01 B3	
Quicktime (mov)	6D 6F 6F 76	
Windows Media (asf)	30 26 B2 75 8E 66 CF 11	

文件类型	文件头	文件尾
MIDI (mid)	4D 54 68 64	

5.gif

- 特殊帧隐藏着flag信息（ps/ stegsolve）
- 帧的时间间隔与密码相关联（摩斯密码等）

6.png

- 基于文件结构的图片隐写.
- lsb：

> 1. 基于LSB原理的图片隐写.
> 2.zsteg：https://blog.csdn.net/Amherstieae/article/details/107512398

7.jpg

jphide(jphs）

outguess
outguess -k “key” -r 文件名 -t 保存的文件名
jphs和outguess.

steghide
steghide extract -sf good-已合并.jpg -p 123456

stegdetect（鸡肋
stegdetect.exe -tjopi -s1000.0 *.jpg （查看图片隐写方式）
stegbreak -r rules.ini -f password.txt -t p *.jpg（爆破密码）

F5-steganography
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
java Extract F5.jpg -e misc -p 11111

水印(单图)(工具+Java盲水印) 水印

参考：隐写术之图片隐写
CTF中的隐写术
隐写术 方法总结