

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_43486981/article/details/108057934](https://blog.csdn.net/weixin_43486981/article/details/108057934)

版权



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](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 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）

WinHex - [ctfhub.png]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data  
File Edit

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00002F20	80	8E	5D	8E	C0	C9	4A	29	22	DA	42	13	E9	C0	B9	71	€Ž]ŽÀÉJ)"ÜB éÀ+q
00002F30	36	5E	6F	9A	DB	D3	7D	73	59	34	2D	2E	24	A3	09	FD	6^osŮÓ)sY4-.ŒŒ ý
00002F40	13	F8	1B	97	D3	E1	C7	A9	DA	41	C5	7E	81	73	C7	52	ø -ÓáÇEÚAÁ~ sçR
00002F50	CC	14	36	47	CA	F0	2D	4C	5D	28	E5	52	0C	76	8A	BA	ì 6GÈð-L] (âr vŠ°
00002F60	4B	A7	DC	D6	10	73	FD	45	F7	10	E0	6E	46	BB	90	B7	KŠÜÖ sýE+ ànF» ·
00002F70	9C	64	E4	D0	28	51	24	68	B2	49	D6	C9	DC	F3	3A	CD	œdãD(Q\$ñ°IÖÉÜó:í
00002F80	FA	E4	42	99	1C	74	AD	EC	80	28	D3	A7	73	BC	8E	E2	úáB™ t-ie(Ó\$š4Žã
00002F90	70	89	D2	DB	E1	0E	99	55	A4	4A	ED	2A	05	7C	51	21	phÔŮá ™UwJí*  Q!
00002FA0	4D	C0	C3	88	EB	17	39	F0	B7	5C	63	15	28	70	33	25	MÀÃ^e 9ð·\c (p3%
00002FB0	3D	68	1D	9C	1F	E0	C0	2A	3F	70	6E	EC	8E	15	72	36	=h œ àÀ*?pniŽ r6
00002FC0	11	44	4E	2C	B5	4D	3D	B9	6A	13	45	B2	F1	AD	12	0E	DN,µM=²j E²ñ-
00002FD0	24	C0	17	8A	4D	64	31	EB	FC	D5	E1	8C	11	75	E2	03	ŠÀ ŠMdlëuČáG uá
00002FE0	C0	E6	A6	32	7A	80	21	F0	1D	A4	2F	24	85	1C	1D	4D	Àæ!2z€!ð ¼/\$... M
00002FF0	01	B4	58	72	3B	CF	A5	0C	3F	B4	AD	18	48	64	F9	F8	‘Xr;İ¥ ?’- Hdùø
00003000	82	E7	18	18	3B	73	88	37	D4	5F	06	D6	40	CC	31	6F	,ç ;s^7Ĉ_ Ć@ilo
00003010	AC	94	3F	4D	D6	11	A6	34	15	33	89	7A	1C	2C	C6	E1	-“?MÖ ;4 3#z ,Eá
00003020	E2	50	D5	1D	82	DA	03	30	0C	FE	7F	C3	FF	0A	5B	C0	âPĈ ,Ú 0 p Äÿ [À
00003030	30	F8	CF	C1	B0	03	30	94	C3	B0	03	30	94	C3	B0	03	0øİÁ° 0"Á° 0"Á°
00003040	30	94	C3	B0	03	30	94	C3	B0	03	30	94	C3	B0	03	30	0"Á° 0"Á° 0"Á° 0
00003050	34	43	51	14	FF	05	2C	53	CC	6F	01	16	96	88	00	00	4C0 ÿ ,Sio -^
00003060	00	00	49	45	4E	44	AE	42	60	82	63	74	66	68	75	62	IEND\$B`,ctfhub
00003070	7B	34	30	66	61	36	30	65	36	65	38	62	65	31	34	66	{40fa60e6e8be14f
00003080	61	61	37	31	32	66	30	38	31	65	39	34	36	31	31	37	aa712f081e946117
00003090	32	62	39	34	35	34	31	37	64	7D							2b945417d}

[https://blog.csdn.net/weixin\\_40485551](https://blog.csdn.net/weixin_40485551)