

CTF之Misc基础考法及知识点

原创

金帛  已于 2022-03-17 22:03:20 修改  235  收藏 8

分类专栏: [Misc总结](#) 文章标签: [安全 kali](#)

于 2022-02-12 17:41:52 首次发布

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/12872253606/article/details/122844570>

版权



[Misc总结](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

目录

一、简单的考法

二、zip

- 1、文件格式
- 2、伪加密
- 3、密码爆破

三、PNG

- 1、文件格式
- 2、高度显示不完整
- 3、宽度显示不完整
- 4、LSB隐写

四、JPG

- 1、文件格式
- 2、宽度高度的修改
- 3、base64源码转图片

五、GIF

- 1、文件格式

2、flag藏在某一帧中，用stegsolve查看

六、文件分离

1、自动分析文件和自动分离文件

2、手动文件分离

一、简单的考法

1、属性隐藏flag或者是某些重要的信息，如解压包密码

2、文件的十六进制数据（中间\结尾）隐藏字符段，那些隐藏的字符段一般都是有规律的，可能需要进行一下解码才能的到flag，例题：[Bugku之telnet_I2872253606的博客-CSDN博客](#)

3、增加文件后缀zip进行解压，解压后的文件里就有flag

4、补全文件头

5、常见的文件类型

常见的文件头类型如图所示

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

6、kali下file命令查看文件类型

命令：file 文件名

二、zip

1、文件格式

•头标识 50 4B 03 04

•版本号，头标识后面四位

•加密情况，版本号后面两位，00为未加密，其余通常为加密

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	50	4b	03	04	0a	00	00	00	00	70	84	49	54	dc	44	PK.....p	处T踰
00000010	01	99	03	00	00	00	03	00	00	00	0d	00	00	00	7a	69	.?.....zi
00000020	70	bd	e2	d1	b9	b0	fc	2e	74	78	74	36	36	36	50	4b	p解压包.txt666PK
00000030	01	02	3f	00	0a	00	00	00	00	00	70	84	49	54	dc	44	..?.....p
00000040	01	99	03	00	00	00	03	00	00	00	0d	00	24	00	00	00	.?.....\$...
00000050	00	00	00	00	20	00	00	00	00	00	00	00	7a	69	70	bdzip?
00000060	e2	d1	b9	b0	fc	2e	74	78	74	0a	00	20	00	00	00	00	度拱?txt.. .
00000070	00	01	00	18	00	75	77	22	ff	8f	1d	d8	01	75	77	22uw" ..?uw"
00000080	ff	8f	1d	d8	01	10	87	6f	fc	8f	1d	d8	01	50	4b	05	..?.噶?..?PK.□□
00000090	06	00	00	00	00	01	00	01	00	5f	00	00	00	2e	00	00_.....
000000a0	00	00	00														...

CSDN @金 帛

2、伪加密

原本没有加密的zip文件，在人为的修改16进制的情况（将版本号后面的00改掉），误让解压的时候以为加密了

3、密码爆破

使用工具ARCHPR进行爆破

三、PNG

1、文件格式

- 头识标，89 50 4E 47 0D 0A 1A 0A
- 宽度位0x10-0x13，不可随意更改，需根据CRC值修改
- 高度位0x14-0x17，可随便改
- CRC校验位0x1D-0x20，CRC是对文件数据块的校验，修改数据块会使校验失败，文件无法正常显示

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	垺NG.....IHDR
00000010	00	00	11	10	00	00	0c	12	08	02	00	00	00	75	81	b8u.?
00000020	42	00	00	00	03	73	42	49	54	08	08	08	db	e1	4f	e0	B....sBIT...垺O?
00000030	00	00	20	00	49	44	41	54	78	9c	ec	bd	cb	8e	24	3b	..IDATx滌剿?;□□
00000040	b2	2d	b6	cc	e8	1e	91	55	b5	1f	a7	1b	12	f4	b8	12	?短?慤???.舫.□□□□
00000050	20	8a	07	34	13	a0	91	d1	5f	e9	9f	34	d0	4c	f3		柏.4..燒_闊4壤?□
00000060	3b	69	a8	85	d3	a7	4f	9f	de	55	95	19	e1	4e	5b	1a	;i縵O繆U?酸[.□□□
00000070	18	49	a7	bf	22	c3	33	23	5f	55	be	50	60	45	7a	30	.Iᵱ"?#_U綰`Ez□□□
00000080	e8	7c	18	8d	46	a3	19	4d	fe	cb	ff	f9	7f	00	20	e9	鏽..F?M ??.?□□
00000090	a9	7f	00	60	66	fe	d9	3f	24	08	8c	7d	fd	77	7a	0a	?.`f ?\$.病齶z.□□
000000a0	74	e7	08	20	e7	15	ff	55	a4	f4	9d	44	43	df	f7	7d	t? ? U .DC喙}□□
000000b0	df	77	5d	8c	31	7a	8e	18	09	80	06	92	66	e9	d5	06	遷]?z?.€.拈擒.□□□
000000c0	3d	47	33	91	ba	4a	9e	c6	18	01	88	88	a7	fe	01	80	=G3懔J焮..盜 .e□
000000d0	31	f8	87	f2	d0	d3	10	82	88	a8	aa	a7	fe	81	22	14	1鴉蚰?供i .".□□□
000000e0	83	0a	55	0a	a0	02	c0	80	10	40	68	9b	a6	69	42	db	?U...紘.Bh湫iB?□□
000000f0	84	10	54	55	10	a0	07	11	ad	51	5d	de	35	79	02	40	?TU....璉]?y.@□□□
00000100	41	95	c8	d8	c7	18	fb	be	37	b3	3a	73	5d	13	11	21	A警庠. 7?s]..!□□
00000110	09	31	b3	28	42	cf	a6	30	11	11	18	00	6f	af	92	00	.1?B夕0....o痕.□□
00000120	fc	89	37	37	a0	c3	f0	e7	63	10	8b	31	2e	e6	ef	fb	鼓77.灭鏹.?.鸞?□□
00000130	de	3f	d4	fd	1c	29	08	8d	89	ce	f3	7b	7d	26	20	60	?札.)..壩高}& `□□
00000140	a2	94	85	37	7b	db	17	7e	c2	54	ce	a4	f7	4a	5f	61	?{?~耆韦鯨_a□□□
00000150	34	be	16	d4	20	4c	63	ea	df	70	a8	b6	3f	09	b9	4b	4??Lc贗pú?.笙□□□□
00000160	01	93	26	c2	bb	51	24	a8	f7	2a	01	e4	be	a5	88	28	.?禄Q\$ *.渚 (□□
00000170	2d	bd	08	08	92	8b	1d	43	55	81	d9	17	ca	d4	e8	4c	-?.根.CU.?试鏹□□□
00000180	5a	35	29	ce	e9	41	94	a1	81	e7	07	40	15	cf	07	c0	Z5)伍A敗.?.?□□□

2、高度显示不完整

例题: [Bugku之隐写_I2872253606的博客-CSDN博客](#)

3、宽度显示不完整

需根据爆破文件的CRC值修改宽度, 否则会打开文件失败

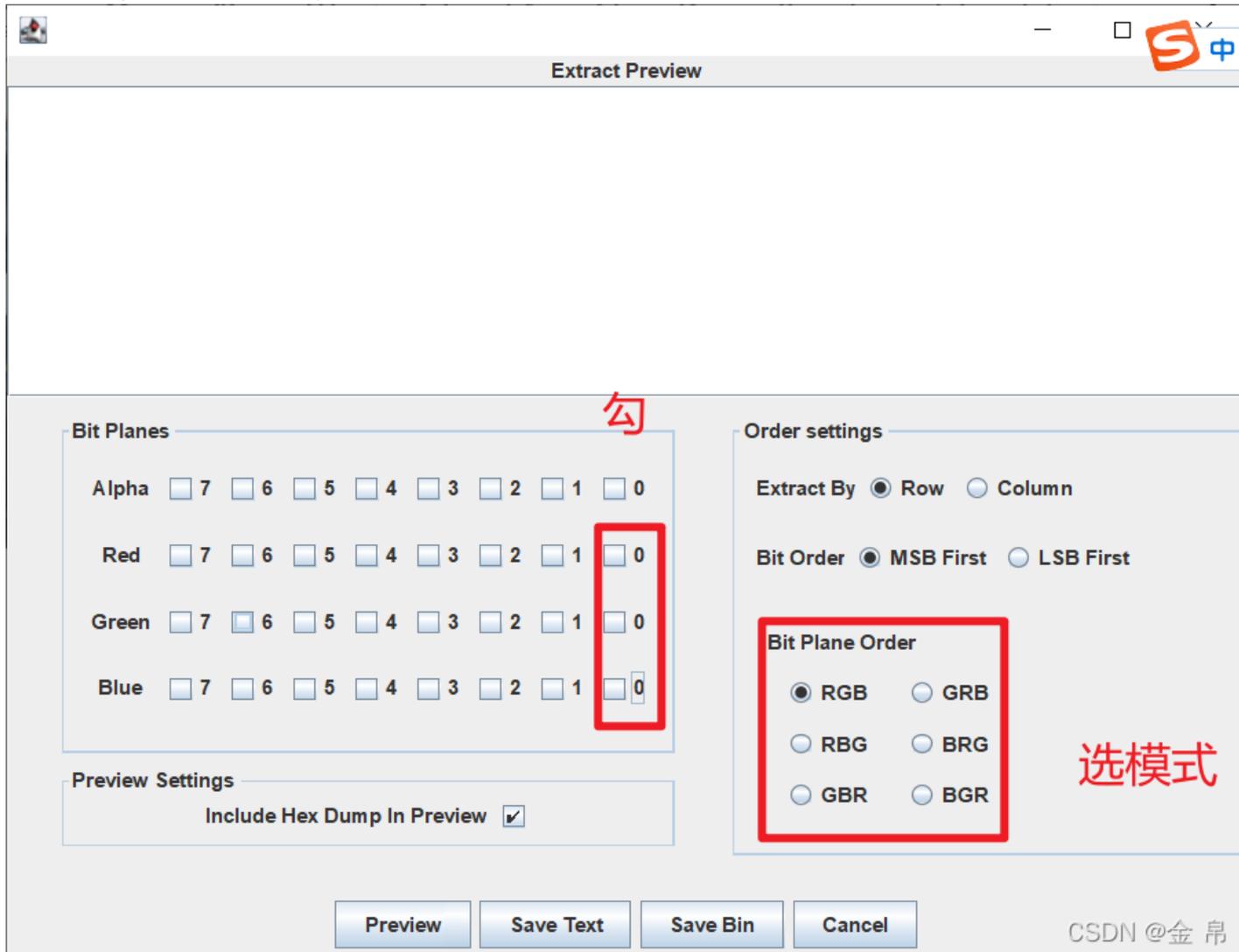
4、LSB隐写

使用工具stegsolve或者是kali看, kali看得全一点,

例题: [Bugku之赛博朋克_I2872253606的博客-CSDN博客](#)

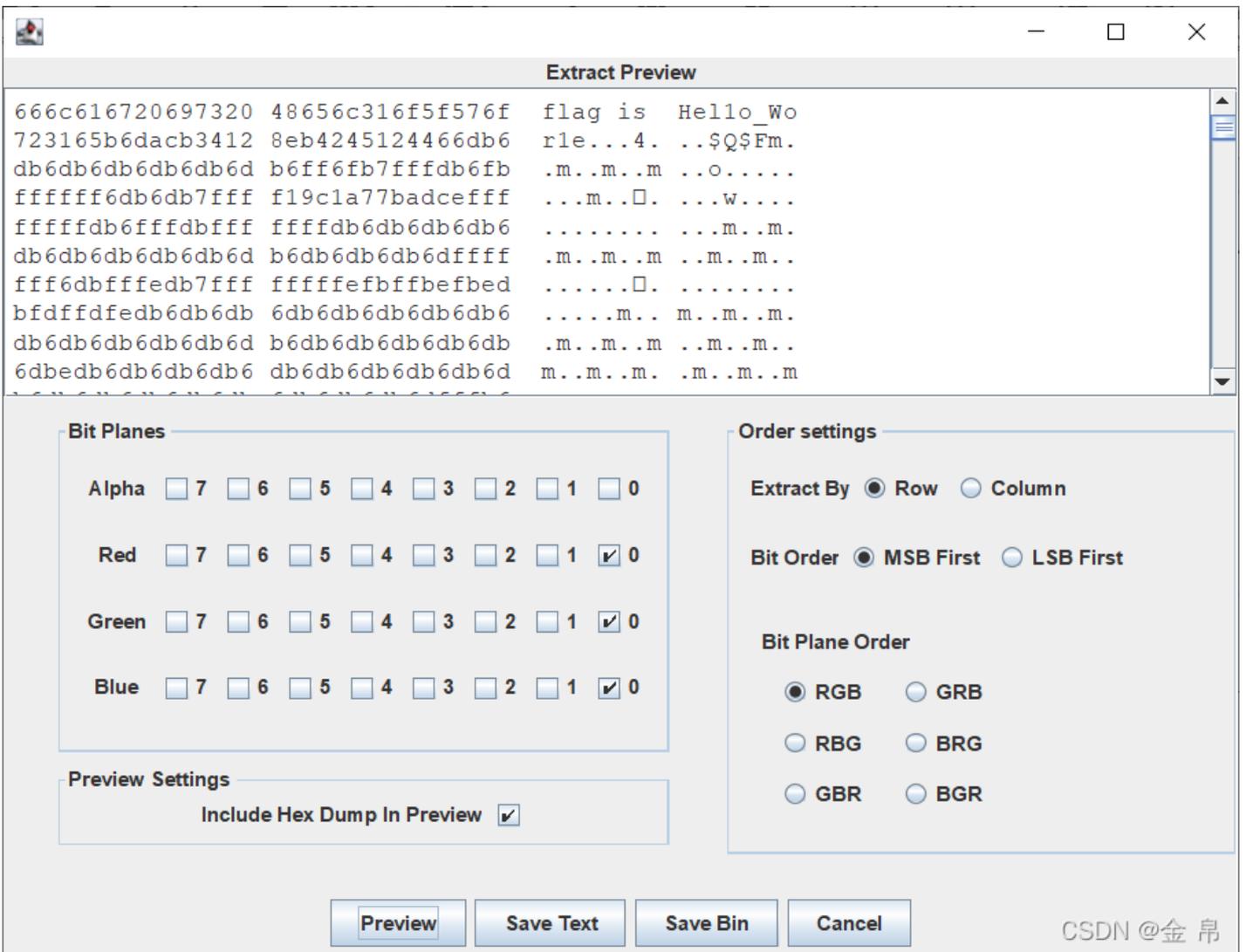
- 用stegsolve查看

文件用stegsolve打开，Analyse，Date Extract



勾选后面三个0，模式一般都是RGB，发现没有的话，可以尝试换一个模式

再点Preview，数据拖到最上方



发现flag

•用kali查看

得先下载zsteg工具，具体方法自行百度，将文件拖入kali

输入命令zsteg 文件名

即可查看被隐藏的内容

自动分离不管用的时候使用，具体操作自己百度

例题: [Bugku之easy_nbt_l2872253606的博客-CSDN博客](#)