CTF隐写术

原创

「已注销」 于 2020-01-06 17:50:41 发布 461 收藏 1

分类专栏： CTF 文章标签： 信息安全 安全

本文链接：https://blog.csdn.net/Deep___Learning/article/details/103859911

文章目录

常用工具

思路

LSB隐写

加密的ZIP压缩包

doc文件隐写

例题

常用工具

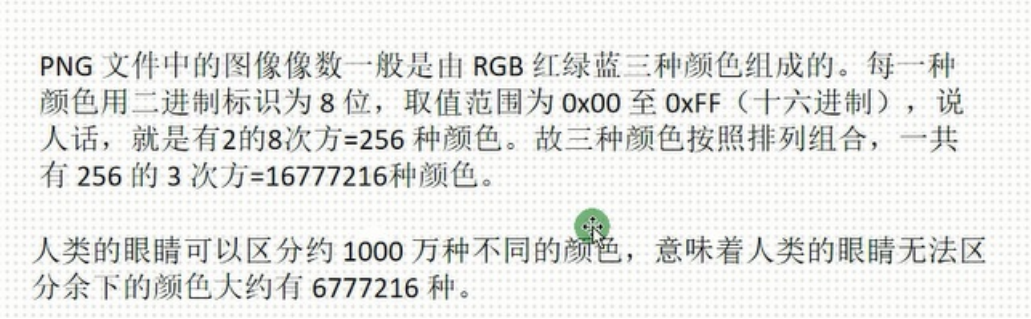
winhex：显示文件十六进制格式（也可以用hexdump）
foremost：文件提取工具（也可以用binwalk）
Stegsolve：LSB 查看图片最低有效位
Elcomsoft Password Recovery：压缩包解码

思路

1、查看文件属性，看能否发现隐藏信息
2、进行文件分离，看能否分离出有用文件
3、用WinHex打开文件，查找有用信息

LSB隐写

LSB隐写就是修改RGB颜色分量的最低二进制位（LSB），每个颜色会有8 bit，LSB隐写就是修改了像素中最低的1 bit，而人类的眼睛不会注意到这前后的变化，每个像素可以携带3 bit的信息。

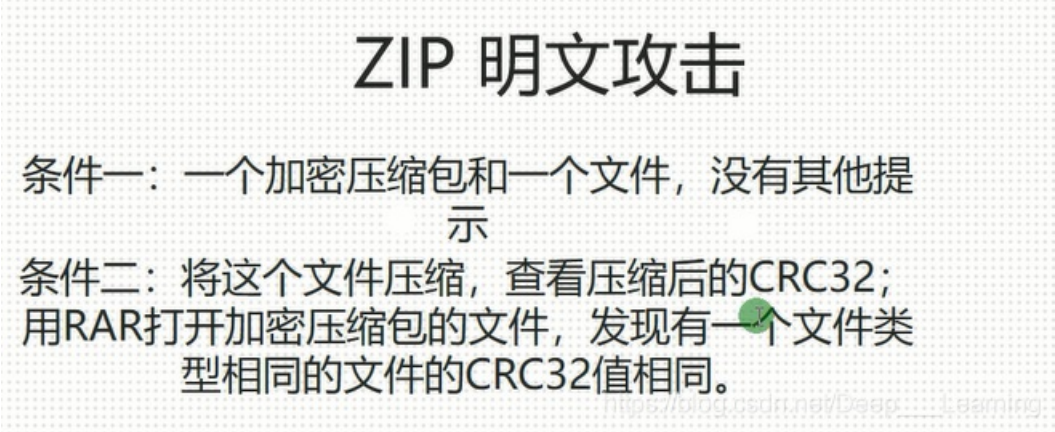


加密的ZIP压缩包

1、考虑是否为伪加密

2、用明文攻击

明文攻击：明文攻击是一种攻击模式，指攻击者已知明文、密文以及算法，求解密钥的过程。



3、暴力

doc文件隐写

1、字体颜色改变，尝试修改字体的颜色

2、word隐藏文字设置

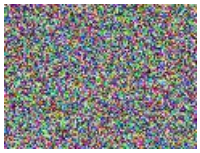
例题

图片隐写：

例1

用StegSolve打开，可以看到图片中有一个二维码，扫描二维码即可。

例2



用WinHex打开图片，搜索字符串FLAG即可

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00041856	9F	99	60	BF	02	58	BE	02	66	37	F8	32	17	19	55	34	Ÿ™`¿ X¾ f7ø2 U4
00041872	36	DC	EC	23	BE	57	EF	E2	C3	DC	8E	71	52	9F	03	F6	6Üì#¾WïâÃÜŽqRŸ ö
00041888	A3	7E	73	46	C8	17	AA	2C	51	60	2D	81	12	C3	DC	4E	£~sFÈ ª,Q`- ÃÜN
00041904	2D	FE	16	6B	E9	F9	6F	ED	D7	E1	B6	71	60	68	53	D4	-þ kéùoí×á¶q`hSÔ
00041920	21	27	E2	8B	BC	85	6D	D5	3E	71	6A	1F	24	AB	96	1E	!'â‹¼…mÕ>qj $«–
00041936	ED	68	45	CA	70	77	0D	85	DC	82	22	BA	A6	E1	93	E5	íhEÊpw …Ü,"º¦á"å
00041952	6D	2A	4C	45	69	8C	17	B9	5C	FB	FC	30	BC	30	21	AE	m*LEiŒ ¹\ûü0¼0!®
00041968	F3	FD	E8	FE	39	8E	7F	BE	1F	E6	FA	87	DB	D3	DF	9C	óýèþ9Ž ¾ æú‡ÛÓßœ
00041984	AF	53	07	BF	A7	6A	1B	96	FD	FF	67	F7	C6	1A	89	0E	¯S ¿§j –ýÿg÷Æ ‰
00042000	ED	82	D0	64	72	67	74	FB	C2	20	CA	9E	EE	DF	4A	B9	í‚ÐdrgtûÂ ÊžîßJ¹
00042016	F9	46	72	4B	F9	E3	B1	68	51	E0	D5	B0	0C	73	8D	C1	ùFrKùã±hQàÕ° s Á
00042032	BC	AC	0E	5F	67	6E	58	89	8B	34	4A	32	38	5C	1B	F7	¼¬ _gnX‰‹4J28\ ÷
00042048	97	B4	4E	87	73	94	64	F0	3B	63	91	E2	58	3C	C7	41	—´N‡s”dð;c‘âX<ÇA
00042064	B3	8C	ED	84	DC	61	B1	4D	3E	00	7E	0A	5C	90	D2	80	³Œí„Üa±M> ~ \ Ò€
00042080	72	03	42	C3	B8	3A	C8	18	35	12	53	BB	9D	DC	A2	DC	r BÃ¸:È 5 S» Ü¢Ü
00042096	9A	1F	2A	81	33	BC	46	4C	41	47	7B	50	75	52	65	5F	š * 3¼FLAG{PuRe_
00042112	52	40	4E	44	30	4D	5F	44	61	54	61	5F	46	72	30	4D	R@ND0M_DaTa_Fr0M
00042128	2F	44	33	56	2F	55	52	40	4E	44	30	4D	7D	10	52	08	/D3V/UR@ND0M} R
00042144	DA	9A	24	98	34	9E	0E	50	F2	8E	77	A1	10	7E	21	6A	Úš$˜4ž Pòžw¡ ~!j
00042160	34	2F	69	C0	0F	62	4B	47	75	F3	C2	22	40	6A	F1	C8	4/iÀ bKGuóÂ"@jñÈ
00042176	74	7A	EB	A0	2E	13	A2	00	D0	46	AA	EC	E5	F1	B7	2A	tzë . ¢ ÐFªìåñ·*
00042192	B6	8C	08	92	10	58	23	BF	75	12	1B	1D	F7	4F	FC	30	¶Œ ’ X#¿u ÷Oü0
00042208	E5	D8	C2	D8	B7	CB	42	15	9B	BA	BF	8E	C0	25	E9	1E	åØÂØ·ËB ›º¿ŽÀ%é
00042224	AC	0D	65	1B	B3	9D	54	38	73	7E	04	D6	42	0A	38	6D	¬ e ³ T8s~ ÖB 8m
00042240	C7	EB	4D	86	0E	B6	A0	B8	72	D9	B4	39	33	E4	DF	9B	ÇëM† ¶ ¸rÙ´93äß›
00042256	31	B2	13	C4	0C	87	C6	8D	76	53	34	10	D2	81	22	66	1² Ä ‡Æ vS4 Ò "f
00042272	C3	45	E8	18	1F	4E	1B	60	BF	6E	8C	C4	96	29	E3	D0	ÃEè N `¿nŒÄ–)ãÐ
00042288	B5	7E	0F	4D	DA	6F	C7	FC	F6	6D	35	D2	4A	93	A3	5D	µ~ MÚoÇüöm5ÒJ“£]
00042304	51	4D	AF	AA	FE	48	66	14	25	0D	5E	2F	8A	DE	23	64	QM¯ªþHf ¶ % ^/ŠÞ#d
00042320	B6	A9	0D	1C	3E	68	E1	2D	3B	C0	0A	67	F8	85	C5	63	¶© >há-;À gø…Åc
00042336	93	4D	4F	61	52	38	E2	13	48	D1	09	10	58	F5	54	9A	“MOaR8â HÑ XõTš
00042352	F3	E2	36	DC	80	D1	E3	3A	1F	AF	0A	0E	A2	C8	E8	F9	óâ6Ü€Ñã: ¯ ¢Èèù
00042368	98	1E	C7	87	20	3A	A3	78	06	EF	2D	5D	EB	BD	18	19	˜ Ç‡ :£x ï-]ë½
00042384	E1	7E	9D	66	7B	C0	4A	27	BF	EB	DE	35	83	B1	C3	81	á~ f{ÀJ'¿ëÞ5ƒ±Ã
00042400	C9	A1	BF	EB	CC	4F	5E	69	49	3A	36	04	74	2E	57	B6	É¡¿ëÌO^iI:6 t.W¶
00042416	05	22	34	74	E2	F3	55	B1	B8	54	8C	08	BC	08	C2	5A	"4tâóU±¸TŒ ¼ ÂZ
00042432	42	74	F5	8D	32	A3	9F	C6	81	04	CD	D7	5A	BB	02	89	Btõ 2£ŸÆ Í×Z» ‰
00042448	E3	EE	1E	32	D7	E0	95	54	0A	5D	FC	27	0D	C0	C9	E3	ãî 2×à•T]ü' ÀÉã
00042464	20	E6	C9	09	7B	2D	56	0A	61	B5	D6	98	AE	D6	95	F1	æÉ {-V aµÖ˜®Ö•ñ
00042480	65	9D	A5	F1	93	BB	2C	DF	5D	7D	AD	3B	83	1D	EE	9A	e ¥ñ“»,ß]}-;ƒ îš
00042496	5D	07	6C	F8	E3	DF	89	99	A7	7A	CF	34	EF	8C	D3	77	] løãß‰™§zÏ4ïŒÓw
00042512	1C	C1	9C	57	8E	FE	E8	C8	A0	12	25	5B	67	90	AE	54	ÁœWŽþèÈ %[g ®T
00042528	2E	03	41	C9	C9	AB	59	FB	F8	06	2E	AF	46	E2	E0	32	. AÉÉ«Yûø .¯Fâà2
00042544	62	70	43	D2	DC	6D	4D	43	92	2A	DF	E4	6F	DC	21	67	bpCÒÜmMC’*ßäoÜ!g
00042560	19	B4	45	47	01	29	8B	71	9B	BC	81	04	2A	D2	D9	C1	´EG)‹q›¼ *ÒÙÁ
00042576	B1	AE	FA	94	9D	F4	DC	FE	55	CC	3E	7D	10	E5	B6	22	±®ú”ôÜþUÌ>} å¶"

创作打卡挑战赛