ctf--隐写术(持续更新)

原创

小健健健

 于 2020-10-19 20:09:40 发布 ○ 1161 ☆ 收藏 11

 分类专栏: ctf 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/superprintf/article/details/108994847



ctf 专栏收录该内容

7 篇文章 0 订阅 订阅专栏 有写的不全的看看大佬的文章 基础视频 链接: https://pan.baidu.com/s/13aiUAaBtRH76aZk_OYiM0Q 密码: 2094

工具

编辑16进制文件

1.winhex 2.010Editor

分离图片中隐藏的文件
1.binwalk:binwalk -e file (不加-e为仅查看)
2.foremost: foremost file -o outfile
3.7z
4.dd: dd if=file of=outfile bs=bs_size count=n skip=m
输入文件为file,输出文件为outfile,块大小为bs_size(往往设置成1),读写块的个数为n,跳过前m块使用dd时结合binwalk判断块的大小
5.010editor手动分离

打印文件中可显示的字符串(ascii转义后可显示) strings filename

查看gif图像每帧 stegsolve 网盘密码: iwhf

音频软件 adobe audition 密码: 6ppg



隐写术与加密的区别: 希腊单词隐写术(stegnos)加密(crypt) 英文单词隐写术(covered)加密(hidden) 加密(hidden)之后的内容是可见的,只不过顺序被打乱了,不经过分析就无法理解。隐写术中信息是不可见的,所以也叫隐蔽 (convered) **古时候的隐写术** 隐形墨水(酸性物质受热后颜色会变重)

缩影术(信息缩小成一个点,需放大查看) 水印(类似于人民币透光才能看到的信息)

\Box . ctf

word隐藏

1.word自带隐藏文字功能

隐藏文字:选中文字右键选择字体,勾选隐藏文字,即可隐藏。 显示文字:文件->选项->视图->隐藏文字

		选项		
视图	显示			
编辑	启动时展开任务窗格(R)	✓ 突出显示(H)	域底纹(E):	
堂坝与保存	✓ 屏幕提示(N)	□ 域代码(F)	选取时显示	٥
	✓ 状态栏(U)	□ 书签(K)		
	 ✓ 显示裁剪标记(R) ✓ 选择时显示浮动工具栏(D))) 🔽 右键时显示浮动工」	具栏(G)	
文件位置	字体替换(O)	○ 字体缺失提醒(M)		
修订				
中文版式	格式标记			
输出PDF	□ 利表付(1) □ 空格(S)	 □ 段洛标记(m) □ 隐藏文字(l) 	\mathbf{i}	
用户信息	□ 全部(L)			
	页面视图选项			
1121		✓ 垂直标尺(C)		
拼写检查	□ 正文边框(X)	□ 隐藏空白(B)		
安全性	✓ 単击万框时打勾	☑ 打开文件,展	示智能识别日录(W)	
□ 备份中心				
				取消 确定 Tilps://blog.csd/met/superprint
				联府 Titps://blog.csdn.net/superprint

2.白色字体隐藏,修改背景颜色



	选项
视图	用户信息
编辑	姓名(N): flag{hello_user}
常规与保存	缩写(l):
备份设置	
文件位置	通讯地址(M):
修订	
中文版式	
输出PDF	
用户信息	
打印	
拼写检查	
安全性	
3 备份中心	
	取消通常

图像隐藏

细微颜色差别 stegsolve工具 **gif多帧隐藏** 用stegsolve java -jar stegsolve.jar启动,查看git动图中每一张图的信息 **exif信息隐藏** windows上,图片右键,信息 1.windows下命令 copy /b pic.jpg+file.rar hidden.jpg 将file.rar藏在图片的末尾 用winhex查看二进制图片发现flag

🔛 WinHex - [g	irl.pr	ig]																
🌇 文件(F) 编	辑(E) #	叟索(S)	导航	(N)	查	₫(V)	Ţ	Ι (T)	ŧ	ΨT	具(I)	选	项(C) 1	窗口(W) 帮助(H)	2
🗅 🍺 🗔 🎝) 📚	B			5		Ē	ß	BB 10	1-2 0 ⁻	P) //		<u>ا</u> ر ا	не»		$\rightarrow + \oplus + \rightarrow + $	పి తే శ
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASC	• II
00099184	05	0D	BA	62	D4	6B	C4	19	AB	E7	3E	80	AD	2B	CD	6A	°bÔkÄ «ç> −+i	Ĺj
00099200	23	DF	$\mathbf{F0}$	11	3B	B1	E0	4A	8A	В0	2A	38	6B	29	75	7C	#βð ;±àJа*8k)ι	1
00099216	47	81	4F	BE	2E	29	56	91	55	57	10	41	77	Α2	56	11	G O¾.)V'UW Aw¢™	7
00099232	12	81	СВ	53	88	50	B5	AD	16	64	EA	4C	F6	5B	F3	12	ËS^Pµ- dêLö[d	5
00099248	08	DF	96	33	9C	B7	7A	80	21	42	E8	6F	50	1B	D1	5D	β-3α·z€!BèoP Í	Ň]
00099264	9B	35	C1	54	E7	32	AE	8D	8F	70	10	EA	F9	AF	13	17	⇒5ÁTç2© pêù	
00099280	71	9C	73	2B	03	5D	F1	28	B5	BF	Α4	D9	D2	2E	ЗA	1E	gœs+]ñ(µ¿¤ÙÒ.∶	
00099296	7F	69	40	68	17	5E	59	A3	54	DF	30	B2	98	EE	23	D4	i@h ^Y£TBO°~î	ŧÔ
00099312	E9	15	78	В9	6E	1C	76	5F	32	E5	97	Α6	A 7	65	68	6A	é x'n v_2å-¦§eł	nj
00099328	44	16	EF	D3	1B	D1	61	EA	51	65	03	93	1F	20	23	2B	D ïÓ ÑaêQe "	‡+
00099344	58	96	73	48	5C	AE	F3	1A	A1	B 3	84	BA	43	DC	4A	E2	X−sH\©ó ;³"°CÜ	Jâ
00099360	17	Α5	53	E7	C4	EA	4E	3C	79	85	A0	28	EB	7C	43	5B	¥SçÄêN≺y… (ë∣(2[
00099376	AC	32	16	00	12	BB	05	53	CF	B 9	6B	E9	C 5	9D	B1	BD	−2 » SÏ'kéÅ :	£¥≨
00099392	CD	27	57	28	AB	2F	58	ЗD	69	4E	21	83	07	AO	0C	DE	Í'W(«/X=iN!f	Þ
00099408	E3	00	38	F1	51	59	B2	8F	50	BD	Α4	55	D4	AO	6D	AB	ã 8ñQY° P≒≭UÔ r	ï≪
00099424	AE	7C	44	23	D1	EE	50	04	CB	E6	11	05	B1	5F	13	FF	⊗ D#ÑîP Ëæ ±_	Ÿ
00099440	D9	66	6C	61	67	7B	68	65	6C	6C	6F	5F	6D	61	6E	5F	Ùflag{hello_mar	<u> </u>
00099456	68	65	72	65	5F	69	73	5F	66	6C	61	67	7D				here_is_flag}	
																		-
页 270 / 271					偏利	多地均	lt:	9	9.200)			=	35	洗块	4		无 大小:

图片修复

1.修复图片的宽和高
 2.修复IDAT数据长度
 3.修复CRC
 4.构造RGB图片

不同格式的文件头 jpg头: FFD8FF png头: 89504E47 gif头: 47494638 pdf头: 255044462D312E zip头: 504B0304 rar头: 52617221

先学习一下png格式

crc校验49484452...08040000并得到四位数字

00000000:	8950	4e47	0d0a	1a0a	0000	900d	4948	4452		PNG.	1题	IHDRP
00000010:	0000	10 01a	0000	1 001a	0804	0000	00 03	R:8 4	•			C.
00000020:	4500	0000	0467	414d	4100	00b1	8f0b	fc61	E		gAMA.	a
00000030:	0500	0000 '	2063	4852	4d00	007a	2600	0080		(cHRM.	.z&
00000040:	8400	00fa	0000	0080	e800	0075	3000	00ea				.u0
										~0		
3:0000h: ()E上 E2 个II	DET 8D	00_00	<u>00,0</u> 0	49 44	<u>4</u> 1 54	BA 4	3 5E	BE	.âv		IDAT°C^¾
3:0010h: E	SF B4 2	25 54	DD CB	44A* 84	13 74	A2 4A		410年9	в0	ï′%	TÝËJ′	.t¢Jn.)°
3:0020h: H	30 8F B	EF CF	19 36	C6 40	6A EF	EE F2	2 39 7	9 3E	B1	°.ï	Ï.6Æ@	jïîò9y>±

1题修改图片高度

修改图片宽度和高度来暴露隐藏的部分(winhex工具) 链接: https://pan.baidu.com/s/1y22OzQ6Z381LWkibTXoYZA 密码: nsdi



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	^
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNG IHDR
00000016	00	00	01	F3	00	00	02	80	08	06	00	00	00	99	DA	A9	ó € ™Ú©
00000032	F6	00	00	00	01	73	52	47	42	00	AE	CE	10	E9	00	00	ö sRGB ®Î é
00000048	00	wid	ltŋ)	41	4D	He	igh	t00	B1	8F	0B	FC	61	05	00	00	gAMA ± üa
00000064	00	09	70	48	59	73	00	00	0B	13	00	00	0B	13	01	00	pHYs
00000080	9A	9C	18	00	00	FF	A5	49	44	41	54	78	5E	94	FD	85	šœ 资料HAT 20 家.万
00000096	97	25	5B	76	DD	8D	B6	2D	5B	92	2D	68	B5	24	4B	AD	-%[vÝ ¶-[′-hµ\$K-



2题修复IDAT长度 网盘下载图片 密码: uvhf



IDAT数据长度部分为0,我们需要修复,这一段的IDAT是从30004h-36273h

除去内容部分有4h的CRC,4h的长度,4h的IDAT标示,3627h-30004h+1h-4h-4h=6264h,填写在数据长度部分,显示原图片

00030000:	0ee2	768d	0000	0000	4944	4154	ba43	5ebe	v <mark>IDAT</mark> .C^.
00030010:	efb4	2554	ddcb	4ab4	1374	a24a	6e14	29b0	%TJ. <u>.</u> t.Jn.).
00030020:	b08f	efcf	1936	c640	6aef	eef2	3979	3eb1	6.@j9y>.
	<u> </u>			~ - · -	1000	~ ~ ·			
00036250:	a029	f3fb	0142	1cbf	22a1	5f1e	2dfd	e8d5	.)B"
00036260:	2381	a379	3d15	213f	3fdf	fe3f	3003	6bc1	#y=.!???0.k.
00036270:	cd56	d230	0000	00a0	4944	4154	5532	4673	.V.0IDATU2Fs
	- · · -	· ·						- • • •	



3题修复CRC校验

crc在线工具网站

windows下图片可以打开(不用修复CRC校验)其他系统下图片不能打开则有一定概率存在CRC校验码错误的问题 爆破图片修改前的宽和高来匹配CRC校验码,并用正确的宽和高来修复图片

import binascii
def str2num(s):
return int(s, 16)
dic = '''abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!"#\$%&'()*+,/:;<=>?@[\]^_`{ }~'''
crc1 = str2num("BBB16F8C")#crc值
for x in dic:
for a in dic:
for b in dic:
for c in dic:
for d in dic:
str = x+a+b+c+d
<pre>str_crc = binascii.crc32(str.encode()) & 0xffffffff</pre>
<pre>if (str_crc == crc1):</pre>
<pre>print("crc1:", str)</pre>

4题构造RGB图片 我的另一篇博客

pdf隐写

音频隐写

视频隐写

adobe audition 密码: 6ppg

数据包隐写

wireshark