实验吧CTF题库-隐写术(部分)



用kali下载图片

root@sch01ar:~# wget http://ctf5.shiyanbar.com/stega/spamcarver/spamcarver.jpg

用binwalk查看是否有隐藏的文件

root@sch01ar:~# binwalk /root/spamcarver.jpg

<pre>root@sch0lar:~# binwalk /root/spamcarver.jpg</pre>											
DECIMAL	HEXADECIMAL	DESCRIPTION									
0 64001	0x0 0xFA01	JPEG image data, JFIF standard 1.01 End of Zip archive									

隐藏着一个zip文件

用foremost分离出文件

root@sch01ar:~# foremost /root/spamcarver.jpg



在/root/output/的目录下,得到flag

< > ▲ 企主文件夹 output zip 00000101 →	۹ ::
③ 最近使用的	
	×۳
	大小 62
	类型 JP
	文件大小 11
	文件夹 <u>0(</u>
kov: 7adf6f07o0810003c585a7bc07868200	光圈
key. 7aulol07e0010003c305a7be97000a90	曝光
	焦距
	ISO
	测光

缝缝补补又三年:

NAVSAT 分值:10)				
来源: PicoCTF 2013	难度:易	参与人数:562人	Get Flag:233人	答题人数:247人	解题通过率:94%
缝缝补补又三年 格式:flag{xxx}					
解题链接: http://ctf5	.shiyanbar.com/	/stega/navsat/recove	ery.zip 通过		
					提交

下载zip文件, 打开

名称 大小 压缩后大小 美型 修改时间 CRC32 本地磁盘 Local 341,644 283,364 PDF 文件 2005/2/8 11:49 9CC8A6
■ 本地磁盘 ■ Chart-15.pdf 341,644 283,364 PDF 文件 2005/2/8 11:49 9CC8A6 □ La
Chart-15.pdf 341,644 283,364 PDF 文件 2005/2/8 11:49 9CC8A6
■ key.txt 27 27 文本文档 2013/4/15 3:09 EF2E7DH

key.txt文件打不开,flag应该就在里面

用c32打开文件,flag直接显示出来

l 🚰 🖌	1	a 🕻	1	0	⇒	F	1	3	3	2 (0	¥≡ ∳≡	× 🗖	B		F%\$	176	≡ ±
👫 Enjo	y C32	asm		(HE	X)re	cove	ery.z	ip										
00000	000:	3F	3F	03	04	ØA	00	00	00	00	00	22	79	8 E	42	F6	7D	│ ?? "y嶣鰙
00000	010:	2E	EF	1 B	00	00	00	1 B	00	00	00	ØF	00	10	00	4D	61	.?Ma
00000	020:	67	37	2D	42	57	2F	6B	65	79	2E	74	78	74	55	54	09	g7-BW/key.txtUT.
00000	030:	00	03	D Ø	FE	6A	51	ØB	FF	6A	51	75	78	ØB	00	01	04	
00000	040:	E8	03	00	00	04	E8	03	00	00	4B	65	79	3A	20	4E	65	??Key: Ne
00000	050:	78	74	20	73	74	6F	70	20	54	61	75	20	45	72	69	64	xt stop Tau Erid
00000	060:	61	6E	69	ØA	50	4B	03	04	14	00	00	00	08	00	27	B6	ani.PK'?
00000	070:	47	32	1 B	A6	C8	90	E4	52	04	00	80	36	05	00	14	00	G2. θ 滀R?
00000	080:	10	00	4D	61	67	37	2D	42	57	2F	43	68	61	72	74	2D	Mag7-BW/Chart-
00000	090:	31	35	2E	70	64	66	55	54	09	00	03	BA	36	08	42	AF	15.pdfUT?.B?
00000	0A 0 :	FE	6A	51	75	78	OB	00	01	04	E8	03	00	00	04	E8	03	
00000	0B 0 :	00	00	80	B7	63	94	25	51	D3	26	5A	B6	6D	DB	B6	BA	
00000	OC 0 :	6C	DB	B6	6D	74	97	AB	BA	6C	DB	B6	6D	DB	B6	ED	AA .	│ 1番『mt棲簂番『m番『愍
00000	OD 0 :	53	75	FB	FD	E6	9B	B9	73	D7	FC	B8	83	56	AE	CC	73	Su 貓萊 赋V s
00000	0E 0 :	22	77	44	EC	78	9E	88	80	D8	E4	8A	A2	E2	F4	CC	0C	"₩D靫滙屫鋳⑩籼.
00000	0F 0 :	20	30	6C	44	40	44	ØE	C6	D6	44	70	70	30	80	B2	66	,01DLD.浦D 0介f
00000	100:	Fő	16	AE	96	44	EC	FF	44	CA	30	80	E2	56	B6	AE	66	?畺D?D?ЩU懂f
00000	110:	CE	44	80	E2	B6	46	AE	66	A2	66	26	ØE	A6	66	30	02	朝町褙角 & 0.
00000	120:	02	30	2E	AE	CE	66	46	76	30	9E	1 B	C5	49	72	ØE	4B	.0. fFv0?驘r.K
00000	130:	40	48	A1	DC	A7	18	6F	67	78	20	9E	B6	B1	82	7B	AA	LH≪?ogx,灦醉{?
00000	140:	54	78	34	50	68	C7	10	78	EA	9D	32	1 E	E4	19	AE	AD	Tx4\h?x隄2.?
00000	150:	E5	48	3F	39	E3	12	B8	A5	31	34	45	34	CA	28	D3	5D	锕?9?弗14E4?酮
00000	160:	FE	27	CF	6F	A Ø	21	07	90	EØ	DC	75	24	20	DA	F5	DD	?嵴?

也可以把开头的两个??修改成PK,然后就能打开key.txt

	Enjoy	y C32	asm		(HE)	X)re	cove	ery.z	ip											1
	000000	300:	50	4 B	03	04	ØA	00	00	00	00	00	22	79	8 E	42	Fő	7D	PK	"y∎Bö}
	000000	910:	2E	EF	1 B	00	00	00	1 B	00	00	00	ØF	00	10	00	4D	61	.?	Ма
ľ		10 8 -		97	20	60	C7	95	XD.	XC.	70	95	76	70	76	CC	C 11	AU.	1 a7_DL	1/ban totllT
	key.	txt -	- i2	事本	-12 (m)) 7 1	sæ o	r) 7	#R 0 4	00										

文件(F) 编辑(E) 格式(D) 查看(V) 帮助(H) Key: Next stop Tau Eridani

In Hex, No One Can Hear You Complain:

In Hex, No One Ca	n Hear You C	Complain 分值:10)		
来源: PicoCTF 2013	难度:易	参与人数:488人	Get Flag:294人	答题人数:301人	解题通过率:98%
修改试试看? 格式:flag{xxx} 解题链接: http://ctf5.	shiyanbar.com	/stega/in-hex/kane.d	ocx 通过		
					提交

下载docx文件,直接打开,打不开

Microsoft Office Word	?	\times
无法打开 Office Open XML 文件	· kane. docx,因为内容有错误。 确定 详细信息(D)	>>>

用c32打开

I 🖾 🖂 P.	1	à	e	-				1	8 1	9	'n≡	-				ŧΣ	=:
Enjoy C32	asm	666	(HE)	X)ka	ne.c	locx	:										
The second secon	-	Page 1	•	·													
000000000:	50	4B	03	04	14	03	00	00	08	00	AA	91	71	42	7D	70	│ <mark>₽</mark> К <mark>.</mark>
00000010:	FF	33	1F	01	00	00	DB	03	00	00	13	00	00	00	5B	43_	<u>ü</u> 3?[C
00000020:	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
00000030:	60	BD	93	31	4F	C 3	30	10	85	F7	FE	8A	C8	2B	48	50	1綋10?.咓镨?J\
00000040:	18	10	42	49	3A	20	31	42	87	32	23	63	5F	12	8B	64	BI: 1B?#c .嬆
00000050:	B6	EE	40	69	FF	3D	E7	D 0	66	28	52	4B	51	C5	68	DF	颏Liÿ=缧f(RKQ答?
00000060:	BB	F7	3D	DB	E7	72	B1	19	FA	6C	ØD	48	D6	BB	4A	50	
00000070:	17	73	91	81	D3	DE	58	D7	56	E2	65	F5	98	DF	89	45	│
00000080:	3D	2B	57	DB	00	94	B1	D6	51	25	BA	18	C 3	BD	94	A4	=+W?影讀&?媒念
00000090:	3B	18	14	15	3E	80	E3	48	E3	71	50	91	97	D 8	CA	A Ø	↓:>■紡絞P畫廠?
000000A0:	F4	BB	6A	41	DE	CC	E7	B7	52	7B	17	C1	C5	30	26	ØF	艋iA九绶R{,倚<&.
000000B0:	51	97	CF	80	43	6B	20	5B	28	80	4F	68	80	48	C 8	4F	0柚媹k [*孫i∎J톸
000000000	8F	46	BE	22	F4	24	8D	D7	1F	03	EB	ØB	F6	20	D2	8E	· · · · · · · · · · · · · · · · · · ·
000000D0:	C 8	1E	BE	1D	38	64	6B	55	08	BD	D5	28	72	60	B9	76	??8.kU.秸*r`宽
000000E0:	E6	00	9F	EF	DØ	A9	73	D4	50	67	03	5D	B1	40	C 8	23	?////////////////////////////////////
000000F0:	68	8A	DB	1E	28	21	CF	A3	F9	A6	B1	18	A6	C 8	C9	2B	h卿.(•希 ?0?
00000100:	AØ	D7	40	64	17	C8	F9	47	DF	D3	F8	BD	C1	E5	03	40	₩ 场合? 思 G m G m G m G m G m G m G m G m G m G
66666116:	95	41	59	77	32	47	E3	19	AB	DE	78	88	70	90	C9	FA	ŊYw2G? Z范博悍?
00000120-	1.0	00	nn	0.	EC	07	AD.	79	n.e	96	EA	1.0	90	nn	E O	07	日本世界にした。

是个压缩文件, 改个zip后缀打开

找到flag



越光宝盒:



下载图片

图片打不开



用c32打开,发现png头不对

1			~			1							•					
	Enjoy C32	asm	666	(HE)	X)tir	ngK	.png	1										
h		_							_		_	_	_	_	_	_	_	
	000000000:	90	47	4E	47	ØE	18	ØA	18	00	00	00	ØD	49	48	44	52	GNGIHDR
	00000010:	មម	មម	61	DD	មម	មម	61	20	08	02	00	00	00	09	91	FE	?痰
	00000020:	85	00	00	00	09	70	48	59	73	00	00	ØB	13	00	00	0B	?pHYs
	00000030:	13	01	00	9A	9C	18	00	00	00	20	63	48	52	4D	00	00	殰 cHRM
	00000040:	78	25	00	00	80	83	00	00	F9	FF	00	00	80	E9	00	00	z%∎?.?∎?.
	00000050:	75	30	00	00	EA	60	00	00	3A	98	00	00	17	6F	92	5F	│u0阘?o扣
	00000060:	C5	46	00	01	20	3F	49	44	41	54	78	DA	EC	FD	69	8C	臚 ?IDATx陟齣?
	00000070:	50	59	76	26	08	9E	BB	BC	D5	76	33	DF	DD	E9	4E	D2	│\∀∪&.灮颊∪3咻镹?
	00000080:	C9	ΕØ	12	64	EC	91	91	A9	54	6E	92	52	29	69	32	55	舌.d鞈懇Tn扲)i2U
	00000090:	92	5A	B5	09	55	25	34	66	A9	5F	8D	41	ØF	30	03	9C	│ 抁?U%4f _ 岮.0
	000000A0:	06	98	6E	60	A6	67	06	E8	59	78	06	EA	FA	31	5D	98	│
	- • ם• • • • •	nn	1.9	77	CC	69	9 N	nD	00	6.6	04	E9	1.0	60	AE.	ne	99	禅明 シ中豆DI 下り

把90 47 4E 47 0E 1A 0A 1A修改成89 50 4E 0D 0A 1A 0A

Ē				k	_	⇒_				8 20	8 9		í =	2		11111		f S	
1	Enjo	y C32	asm	<u>666</u>	(HE)	X)tir	ngK	.png			1								
ſ	00000	300	89	50	4E	47	ØD	ØA	18	ØA	00	00	00	ØD	49	48	44	52	%PNGIHD
I	000000	910:	00	88	01	DD	00	88	01	20	08	02	00	00	00	09	91	FE	
I	000000	320:	85	00	00	00	09	70	48	59	73	00	00	ØB	13	00	00	ØB	?pHYs
I	000000	330:	13	01	00	9A	90	18	00	00	00	20	63	48	52	4D	00	00	│殰 CHRM
I	000000	340:	7A	25	00	00	80	83	00	00	F9	FF	00	00	80	E9	00	00	z%∎?.?∎?.
I	000000	050:	75	30	00	00	EA	60	00	00	3A	98	00	00	17	6F	92	5F	│u0阘?o扣
	00000	360:	C5	46	00	01	20	3F	49	44	41	54	78	DA	EC	FD	69	8C	│臚?IDAT×陟齣?

保存,打开图片,得到flag



Dark Star:

 Dark Star 分值:20

 来源: PicoCTF 2013
 难度:中
 参与人数:983人
 Get Flag:334人
 答题人数:361人
 解题通过率:93%

 Sure are a lot of stars out there... but there's a lot of empty space for things to hide in, too.

解题链接: http://ctf5.shiyanbar.com/stega/dark-star/darkstar.img 通过

提交

下载文件

用binwalk查看,里面有很多的image文件

root@sch01ar:~# binwalk /root/darkstar.img

root()cch()lar, t	binub lk	/root/darkctar	- m.c
	DINMALK	/ TUUL/ UATKSLAT	• TIIIO

DECIMAL	HEXADECIMAL	DESCRIPTION
3146752	0x300400	PNG image, 192 x 56, 8-bit/color RGBA, non-interlaced
3146809	0x300439	Zlib compressed data, default compression
4719616	0x480400	JPEG image data, JFIF standard 1.01
4721664	0x480C00	JPEG image data, JFIF standard 1.01
4729856	0x482C00	JPEG image data, JFIF standard 1.01
4730238	0x482D7E	Copyright string: "Copyright (c) 1998 Hewlett-Packard
4738048	0x484C00	JPEG image data, JFIF standard 1.01
4738346	0x484D2A	Copyright string: "Copyright 1999 Adobe Systems Incor
4740040	0x4853C8	JPEG image data, JFIF standard 1.02
4743332	0x4860A4	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <r< td=""></r<>
obe.com/ti	ff/1.0/" xmlns:ex:	if="htt
4754432	0x488C00	JPEG image data, JFIF standard 1.01
4754814	0x488D7E	Copyright string: "Copyright (c) 1998 Hewlett-Packard
4762624	0x48AC00	JPEG image data, JFIF standard 1.01
4764672	0x48B400	JPEG image data, JFIF standard 1.01
4768768	0x48C400	JPEG image data, JFIF standard 1.01
4771840	0x48D000	JPEG image data, JFIF standard 1.01
4772138	0x48D12A	Copyright string: "Copyright 1999 Adobe Systems Incor
4773924	0x48D824	JPEG image data, JFIF standard 1.02
4793236	0x492394	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#' xml
4794731	0x49296B	<pre>Unix path: /ns.adobe.com/xap/1.0/sType/ResourceRef#'</pre>
4794794	0x4929AA	Unix path: /ns.adobe.com/xap/1.0/mm/'>
4795282	0x492B92	Unix path: /purl.org/dc/elements/1.1/'>
4803584	0x494C00	JPEG image data, JFIF standard 1.01
4809728	0x496400	1PEG image data 1ETE standard 1 01

用foremost分离文件

root@sch01ar:~# foremost /root/darkstar.img

分离出一个png图片,打开,得到flag



Chromatophoria:



然后选择



勾起这三个勾,然后点击Preview

	_	×
Extract Preview		

Bit Planes	Order settings												
Alpha 7 6 5 4 3 2 1	Extract By Row Column												
Red 7 6 5 4 3 2 1 0	Bit Order (MSB First LSB First												
Green 7 6 5 4 3 2 1 2 0	Bit Plane Order												
Blue 7 6 5 4 3 2 1	● RGB ○ GRB												
	⊖ RBG ⊖ BRG												
Preview Settings	⊖ GBR ⊖ BGR												
Preview Save Text Save Bin Cancel													

发现flag

	_		Х
Extract Preview			
4865792049207468 696e6b2077652063 Hey I th ink we c 616e207772697465 2073616665667920 an write safely 696e207468697320 66696c6520776974 in this file wit 6866757420616e79 6fee652073656569 hout any one seei 6e672069742e2041 6e797761792c2074 ng it. A nyway, t 6865207365637265 74206b6579206973 he secre t key is 3a2073743367305f 7361757275735f77 : st3g0_ saurus_w 7233636b7300000 000000000000000000000000000000000000			
Bit Planes Order settings			
Alpha 7 6 5 4 3 2 1 0 Extract By Row Col	lumn		
Red 7 6 5 4 3 2 1 ≥ 0 Bit Order © MSB First ○	LSB Fir	st	
Green 7 6 5 4 3 2 1 ✓ Ø Blue 7 6 5 4 3 2 1 ✓ Ø Bit Plane Order			
RBG BRG			
Include Hex Dump In Preview 🗹 🕓 GBR 🕓 BGR			
Preview Save Text Save Bin Cancel			

九连环:

先看一下是否有隐藏的文件

froot@sch #binwa	01ar]-[~] alk 123456cry.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 19560 asd/	0x0 0x4C68	JPEG image data, JFIF standard 1.01 Zip archive data, at least v1.0 to extract, name:
48454 ssed size: 48657 48962	0xBD46 184, uncompressed 0xBE11 0xBF42	Zip archive data, at least v1.0 to extract, compre d size: 184, name: asd/qwe.zip End of Zip archive End of Zip archive

图片里隐藏有zip文件

分离出来



分离出的zip文件里有一个图片和一个压缩包,都需要密码



使用binwalk直接分离图片和压缩文件

└──[root@sch01ar]-[~] └──- #binwalk -e 123456cry.jpg

iroot@scl #binw	h 01ar]-[~] alk -e 123456cry.j	pg	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 19560 asd/	0x0 0x4C68	JPEG image data, JFIF standard 1.01 Zip archive data, at least v1.0 to extract, name:	
48454 ssed size: 48657 48962	0xBD46 184, uncompressed 0xBE11 0xBF42	Zip archive data, at least v1.0 to extract, compr size: 184, name: asd/qwe.zip End of Zip archive End of Zip archive	-e

图片被直接分离出来



• FIVE1

题目提示



图片内有五位数密码

图片:



下载图片

下载完图片后查看图片是否有隐藏的文件

```
[root@sch01ar]-[~]
_____ #binwalk 1111110000000000.jpg
```



有一个zip的隐藏文件, zip里有一个hacker.jpeg的图片

foremost分离jpg图片和zip压缩包

```
[root@sch01ar]-[~]
└──- #foremost 111111000000000.jpg
```

但是zip文件有密码



fcrackzip爆破一下密码

得到密码,FC00



打开hacker.jpeg又是一张图片



用c32打开,拉到最后,看到一句话

echo

"LSOuLi4gIC4tICAuLi4uLiAgLSOuLi4gIC4tICAuLi4uLiAgLi0gIC0tLi4uICAuLi4uLSAgLi4uLS0gIC0tLS4uICAtLS0tLiAgLi4uLi0 gIC4tICAtLS0tLSAgLiAg" >1.txt

对echo后的语句进行base64解码

解出了一串摩斯密码

解密

英文字母:	
7A57A5A743894A0E	
乾妍为摩斯电的 清陈 生成摩斯代码的分摊方式: ● 全格分摊 ○ 甲科杜/分摊	
。 度斯由码,(格式要求,可用态格或单约杆/本公隔庭斯由码,但且可用一种,不可浸用)	
	转换为英文字母成功!
转换为英文字母	

结果为: 7A57A5A743894A0E

拿去进制转换得不出什么有用的东西

拿去md5解密,得到admin,admin就是flag

	密文: 7A57A5A743 类型: 自动	894A0E	~ [帮助]
		查询	加密	
查询结果:				
admin				
1添加省注1				

• 欢迎来到地狱

欢迎来到地狱.zip里有三个文件

🧱 欢迎来到地狱.zip (评估版本)														
文件(E) 命令(C) I	[具(<u>S</u>) 收藏共	ŧ(<u>O)</u> 选项(<u>N</u>)	帮助(<u>H</u>)											
添加 解压到		話 删除	武 前号 前号 前号 市会 市会		山 市 注释	▲ ●解压格式								
🚹 🗋 欢迎来到	🗈 🖹 欢迎来到地狱.zip\欢迎来到地狱\欢迎来到地狱 - ZIP 压缩文件, 解包大小为 1,110,405 字节													
名称 ^	大小	压缩后大小	类型	修改时间	CRC32									
<mark>.</mark>			本地磁盘											
🧮快到终点了.zip	62,756	62,714	WinRAR ZIP 压缩	2017/10/13 1	E5761A89									
🖻 地狱伊始.jpg	54,881	52,874	JPG 文件	2017/10/16 1	92B367F1									
🗐 第二层地狱.docx	992,768	980,427	Microsoft Office	2017/10/15 8	B08FB4									

从地狱伊始.jpg开始

图片无法正常显示



用c32打开,看看文件头是否是正常的

(HEX)	也狱住	尹始 ,	ipg]														
🙀 文件(E)	编	辑 <mark>(</mark> E) #	叟索 <mark>(</mark>	<u>S</u>)	查看	i(⊻)	I	具 <mark>(</mark> 工) 7	高级 <mark>(</mark>	<u>A</u>)	窗口	ם <mark>(ש</mark>)ב) ∄	帮助 <mark>(</mark> 上	<u>1</u>)
	a 🛍	1	6	⇒	F	E, ,	1 12	8		a t)	:= -	× III	EB		F%\$	176	- H
202 - 1	_																
Enjoy C32	asm	975.2	(HE)	X)地	斌伊	始」	pg										
000000000:	00	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00	
00000010:	FF	E1	00	22	45	78	69	66	00	00	4D	4D	00	2A	00	00	ÿ?"ExifMM.*
00000020:	00	08	00	01	01	12	00	03	00	00	00	01	00	01	00	<u>0a</u>	
00000030:	00	00	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	ÿ?C
00000040:	02	02	02	02	02	02	02	03	05	03	03	03	03	03	06	04	
00000050:	04	03	05	07	00	07	07 00	87	00	07 00	07 00	80	89	UB	07	80	
000000000000000000000000000000000000000	00 OF	0H OF	90 0D	97 00	07 0E	0H OR	0D 0C	0H BC	0H OC	UD EE	DR.	00	10	01	82	82	ii2C I
00000070.	82	83	83	03	86	03	03	86	80	88	87	88	80	80	802	802	
000000090:	00	90	00	00	00	00	00	00	00	80	00	00	00	00	00	00	
000000A0:	0C	9C	00	0C	00	0C	0C	0C	0C	0C	0C	0C	0C	9C	0C	9C	
000000B0:	0C	0C	0C	0C	00	0C	0C	0C	0C	0C	0C	0C	0C	OC	$\mathbf{F}\mathbf{F}$	C 0	ij?
000000C0:	00	11	08	00	7D	03	45	03	01	22	00	02	11	01	03	11	
000000D0:	01	FF	64	00	1F	00	00	01	05	61	01	01	01	01	01	00	.ÿ?
000000E0:	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	
000000F0:	UA	OB	FF	C4	00	85	10	00	02	01	03	03	02	04	03	05	y??
00000100:	94	04	04	10	00	01 44	70	97	02	03	99	04	11	05	12	21	10 05 110 2 Å 2 #
00000110:	51	41 R1	00	15	51	01 D1	07 E 0	22	33	14	32	82	90	H 1 80	16	20	18
00000120.	18	19	18	25	26	27	28	29	28	34	35	36	37	38	39	30	28'()*456789:

文件头前少了FF D8 FF E1,添加上去,编辑->插入数据



在此处依次添加E1,FF,D8,FF

添加完后保存,图片就可以正常显示

很久很久以前,有一位。。。。。。小姐姐。。。。。。 扑通一下子。。。。。 掉进了地狱。(别问 我为啥,因为<u>她沉行不行</u>)。。。。。总之。。。有一位河神有一天对你说:"年轻的樵夫呀,你 掉的是这个小姐姐呢,还是。。。。。总之你快去救她吧!"对了,我这里有盘盘的资源<u>呦!</u> *http://pan.baidu.com/s/1i49Thlj*

有一个百度云的链接,https://pan.baidu.com/s/1i49Jhlj,打开,是一个音频文件

▶ 地狱之声.wav		▶ 保存到网盘	▲ 下载(19.1M)	举报
② 2017-10-16 11:47	失效时间:永久有效			

下载,用Audacity打开

•••								地狱之	ŧ.						
文件(F)	编辑(E)	视图(V)	播录(R) 轨道	荁(T) 生成(G) 效果(C)	分析(A) 帮助	H)								
					I <u>≯</u> ∅ ₽ ↔ ¥	● 2 - 57 ×	-48 -42		-18 -12-	9-6-30	10 左 -57 ∽ ~	-48 -42	23630 R R I	-24 -18 -1	2-9-6-30
ALSA	• 🔊 d	efault: Cl	D:0	v 11	[▼]	🐠 Ensoniq A	udioPCI: Es 🔻								
-5		N .	5		10	15	20	25	5	30	35		40	45	50
×地狱之 立体声,4 32位浮点 静音 <u></u> <u>-</u>	■ ▼ 1 8000Hz 独奏 + C 五 -C -1	.0 .5 .0- .5 .5						• • • •		> >					
	t)) 	.0 .5 .0 .5 .5	-	••				• • •	- • · 	• •• P - P		•••			-

目测为摩斯密码



按照上图的方式,得到一串摩斯密码

-.- . -.-- .-.. . - ..- ... --. ---

解密

英文字母:	
KEYLETUSGO	
转换为摩斯电码 清除 生成摩斯代码的分隔方式: ◎ 空格分隔 ○ 单斜杠/分隔	
摩斯电码 : (格式要求:可用空格或单斜杠/来分隔摩斯电码,但只可用一种,不可混用)	转换为蓝文字母成功!
	+02232223
转换为英文字母	

解密结果为KEYLETUSGO

第二层的word文档的密码就是letusgo,不是LETUSGO

用密码letusgo打开文档



你现在在第二层地狱中,凶猛 的。。。。额。。。。哈士 奇。。。。。把守着通向第三层地

只有一个狗的图片还有一段话,检查一下文档是否有隐藏的文字



检测到存在隐藏文字



既然有隐藏文字,那就显示这些隐藏的文字

Word 选项



得到了隐藏的文字

2	G	段落	G		样式
	么。。	0 0 0 0	0000	。你要用]你
	手中的	〕剑(握革	<u>草,</u> 老子	·剑呢, in	nage
	stegan	ography	, , , 톳	是不是掉	车第
	二层地	₩的哪₽	里 了)↓		

image steganography,图片隐写

把word文档里的狗的图片保存下来,用工具看一下图片里隐写了些什么

二、、解密带隐藏信息的图片
1. 从电脑中选择一张带有隐藏信息的图片: 刘览… dog.png
2. 输入需要解开信息的密码(如果没有密码可以不填):信息查看密码,可以为空即为图片解密不需要密码
解密出隐藏的信息
图片中隐藏的信息为:key{you are in finally hell now}

得到一个key,这个key就是下一关的密码

🔚 快到终点了.zip (i	平估版本)	地狱大门.jpg - 照片						
文件(F) 命令(C) I	[具(S) 收藏夹(🔨 查看所有照片	1		â	D	Ø	୍
添加解压到	测试查试		in the second	and the second				
🚹 🗎 快到终点	了.zip - ZIP 压		and the second	A 1	Sa.		T.d.	
名称	大小			10- Mar	311		46	
<mark>.</mark>					and the		Safe P	
National States *	62,606			C SID		AN CONTRACTOR	they a	
■ 最后一层地狱.tx	124		X		A CARLER ST			

一个地狱大门.jpg和最后一层地狱.txt

🥘 最后	一层地狱.	txt - 记事z	4		-		\times
文件(E)	编辑(E)	格式(<u>O</u>)	查看(V)	帮助(<u>H</u>)			
这里有- (tips:	一个大门 : 01110	门,勇士)0100111	把它轰; [010101]	开吧。 10111101	.101011011011110111010101101100011010010	1)	

一串二进制

八个为一组进行转换

二进制转换到 二进制(例: 01100001 01100010 01100011)

ASCII转换到	ASCII (例: a b c)	1	
ruokou	ling		
添加空格	删除空格	□ 将空白字符转换	
	AUGI-OKLE TH		

ruokouling,即弱口令

查看一下地狱之门.jpg是否有隐藏的文件

```
┌─[root@sch01ar]─[~]
└──- #binwalk 地狱大门.jpg
```

froot@sch01a #binwalk	a r ─ ~ 地狱大门 . jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 62584	0x0 0xF478	JPEG image data, JFIF standard 1.01 End of Zip archive

有一个隐藏的zip压缩包

分离文件



但是需要密码打开压缩包里面的内容

🔲 🗋 打开	▼ □↑ 解压缩	C+ 64	- O		
〈 后退 〉	〇 位置	i(L) :	/		
名称		▼ 大小	۱.	类型	修改日期
📄 小姐姐诶.txt		A 313	字节	纯文本文档	2017年10月13日 18:40
		: 需要密码 输入归档文 密码(P):	文件打包器 3 4 (件"000001: (○ 取消(C)	21.zip"的密码。	

根据二进制解出的提示,密码可能是弱口令,Password成功

里面的txt里有一段话,还有一段密文



首先对

VTJGc2RHVmtYMTlwRG9yWjJoVFArNXcwelNBOWJYaFZlekp5MnVtRlRTcDZQZE42elBLQ01BPT0=

进行base64解密,得到

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

再进行Rabbit解密,得到

fxbqrwrvnwmngrjxsrnsrnhx

最后进行凯撒密码的解密,得到所有可出现的结果

kcgvwbwasbrslwocxwsxwsmc ldhwxcxbtcstmxpdyxtyxtnd meixydycudtunyqezyuzyuoe nfjyzezdveuvozrfazvazvpf ogkzafaewfvwpasgbawbawqg phlabgbfxgwxqbthcbxcbxrh qimbchcgyhxyrcuidcydcysi rjncdidhziyzsdvjedzedztj skodejeiajzatewkfeafeauk tlpefkfjbkabufxlgfbgfbvl umqfglgkclbcvgymhgchgcwm vnrghmhldmcdwhznihdihdxn woshinimendexiaojiejieyo xptijojnfoefyjbpkjfkjfzp yqujkpkogpfgzkcqlkglkgaq zrvklqlphqghaldrmlhmlhbr aswlmrmqirhibmesnminmics btxmnsnrjsijcnftonjonjdt cuynotosktjkdogupokpokeu dvzopuptluklephvqplqplfv ewapqvqumvlmfqiwrqmrqmgw fxbqrwrvnwmngrjxsrnsrnhx gycrsxswoxnohskytsotsoiy hzdstytxpyopitlzutputpjz iaetuzuyqzpqjumavuqvuqka jbfuvavzraqrkvnbwvrwvrlb

发现有一条密文像拼音

	密文框:
	kcgvwbwasbrslwocxwsxwsmc
	ldhwxcxbtcstmxpdyxtyxtnd
	meixydycudtunyqezyuzyuoe
	nfjyzezdveuvozrfazvazvpf
	ogkzafaewfvwpasgbawbawqg
	phlabgbfxgwxqbthcbxcbxrh
	qimbchcgyhxyrcuidcydcysi
	rjncdidhziyzsdvjedzedztj
	skodejeiajzatewkfeafeauk
	tlpefkfjbkabufxlgfbgfbvl
	umqfglgkclbcvgymhgchgcwm
-	vnrghmhldmcdwhznihdihdxn
	woshinimendexiaojiejieyo
L	xptijojnfoefyjbpkjfkjfzp
	yqujkpkogpfgzkcqlkglkgaq
	zruklalphaahaldrmlhmlhhr

这个就是flag

• 女神又和大家见面了

下载图片,用binwalk看一下是否有隐藏文件

```
[─[root@sch01ar]-[~]
```

```
L____ #wget http://ctf5.shiyanbar.com/stega/3.jpg
```

root@sch01 #binwalk	a r - [~] 3.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 8204 ge directory: 15164 ard Company" 18187 <rdf:descript ="http://</rdf:descript 	0x0 0x200C 8 0x3B3C 0x470B tion rdf:about="	<pre>JPEG image data, JFIF standard 1.01 TIFF image data, little-endian offset of first ima Copyright string: "Copyright (c) 1998 Hewlett-Pack Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> " xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc</pre>
80985 ssed size: 140 1488494	0x13C59 97224, uncompress 0x16B66E	Zip archive data, at least v2.0 to extract, compre sed size: 1428163, name: music.mp3 End of Zip archive

分离文件



分离出的zip压缩包里面有一个mp3文件和txt文件

) (注	"佰版本)							
文件(F) 命令(C) I	[具(S) 收藏夹(O) 选项(N)	帮助(H)					
添加 解压到					<mark>に</mark> 信息	2日 描病:	■ 注释	▲ 自解压格式
🗈 👔 00000158.zip - ZIP 压缩文件, 解包大小为 1,428,185 字节								
名称 ^	大小	压缩后大小	类型		修改时间	J	CRC32	
			本地磁盘					
🖲 music.mp3	1,428,163	1,407,224	MP3 文件		2015/10	/26 1	B024A8AF	
☐ 描述.txt	22	27	文本文档		2015/10	/26 1	5BB149	

查看txt文件里的内容

可能是音频隐写

用MP3Stego来查看

Decode.exe -X -P simctf music.mp3

C:\Users\hp\Desktop\MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P simctf music.mp3 MP3StegoEncoder 1.1.17 See README file for copyright info Input file = 'music.mp3' output file = 'music.mp3.pcm' Will attempt to extract hidden information. Output: music.mp3.txt the bit stream file music.mp3 is a BINARY file HDR: s=FFF, id=1, 1=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0 alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1 mode=stereo, sblim=32, jsbd=32, ch=2 [Frame 3416]Avg slots/frame = 417.837; b/smp = 2.90; br = 127.963 kbps Decoding of "music.mp3" is finished The decoded PCM output file name is "music.mp3.pcm"

输出了一个music.mp3.txt的文件,打开

[] music.mp3.txt - 记事本
 文件(F) 編輯(E) 格式(O) 查看(V) 帮助(H)
 U21tQ1RGe01QM19NUDNfc2RmZHNmfQ==

是一串密文,base64解密一下

SimCTF{MP3_MP3_sdfdsf}

得到flag

• so beautiful so white

so beautiful so white 分值:10

来源:北邮天枢战队	难度:易	参与人数:2026人	Get Flag:1004人	答题人数:1072人	解题通过率:94%
压缩包的密码就藏在这 格式:CTF{}	幅白色图片中,	仔细找找看吧			
解题链接: http://ctf5	.shiyanbar.con	n/stega/white.zip			

U2ItQ1RGe01QM19NUDNfc2RmZHNmfQ==

提交

题目提示:压缩包的密码在白色图片中

white.zip文件中有两个文件

🧱 white.zip (评估版本)													
文件(E) 命令(C) I	[具(<u>S</u>) 收藏夹(<u>O)</u> 选项(<u>N</u>)	帮助(<u>H</u>)										
添加 解压到					病毒 注释	▲ 自解压格式							
white.zip - ZIP 压缩文件, 解包大小为 33,121 字节													
名称 ^	大小	压缩后大小	类型	修改时间	CRC32								
.			本地磁盘										
🔚 zip.zip	30,808	30,808	WinRAR ZIP 压缩	3 2016/3/2 10:4	8 5897A557								
🖻 password.png	2,313	2,196	PNG 文件	2016/3/1 13:5	8 5D0FBB								

一个有解压密码的zip.zip,里面应该有发flag,还有一个password.png的白色图片,解压密码应该在里面

Stegsolve打开password.png,为一张空白图片

🕌 StegSolve 1.3 by Caesum	_	×
File Analyse Help		
Normal Image		
< >		

点击这个按钮几次,就会得到一个key

🛃 StegSolve 1.3 by Caesum	_		\times
File Analyse Help			
Random colour map 3			
key{forensics_is	_ f	ur	1}

这个key应该就是zip.zip的解压密码

里面有个a.gif,但是不能正常显示



可能文件头有问题,用c32打开



前面的GIF8没有了,把文件头补上去,47 49 46 38

打开gif动图可以看到一个小熊,然后一串字符串一闪而过

用Stegsolve打开



选择Frame Browser



点击这个按钮, 依次看每一帧图片

最终得到flag, CTF{AS3X}

• 打不开的文件

看题目名,估计就是和文件头有关

gif文件打不开



用c32打开

905 · ^	ut 🕛	ाम्स	ᄲ	, ,	Z¥(2)	모엽	1121	Т.	÷(_	., ,	=13X	<u>(11)</u>	BUH	- (**	/ +	h PAU	<u></u> ,
💕 🖟		à 🕯	1	¢	⇒	E,	45	1 13	1		0	*= *=	•	H:B HH		F%\$	$\underline{1}^{\rm cu}_{ ^{\rm sl}}$	
📆 Enjo	oy C 3	2asm	ans.	(HE	X)xx	.git											Γ	
00000	000:	39	61	C2	01	52	01	F7	FF	00	ED	ED	EC	F7	F7	F7	9C	<mark>9</mark> a?R.?. <mark>晒祺鼢?⊄</mark>
00000	01 O :	90	90	80	80	80	03	03	03	A3	A3	A3	3F	3F	3F	5C	5 B	┼指寣?#???\[
00000	02 0 :	5B	60	6C	60	E9	E9	E9	93	93	93	F9	F9	Fő	DE	DE	DD	[111 殚閾摀 鲛掭
00000	030	12	01	02	F4	F4	F4	74	74	74	FA	F5	F4	83	83	83	FE	趑魌tt 魞傻?
00000	040:	F9	F9	EÓ	EÓ	E5	BE	BE	BE	63	62	62	40	40	40	E2	E2	治寰揪cbbLLL 付
00000	05 0 :	E1	CE	CE	CE	53	53	53	ØA	ØA	ØA	FC	FC	FA	7F	7F	7F	嵛挝\$\$\$?■■
00000	060:	DA	D9	D9	FA	FD	FC	D6	D5	D5	20	20	20	43	43	43	AE	谫蠃 终?,,CCC?
00000	070:	AE	AE	F2	F2	F2	0C	01	01	33	33	33	C9	C9	C9	D1	D1	蝌?333缮裳?
00000	~~~			-				4.00						-				大学, 《中学》, "中学

文件头少了47 49 46 38, 补上去

补完之后打开动图, key在动图的帧中

用Stegsolve打开,得到一串字符串:dGhpcyBpcyBhlGdpZg==

base64解密一下得到key, this is a gif

• IHDR



下载后能显示

用c32打开

🛄 Enjoy C	32asr	n 📠	į (H	IEX)IH	DR.	png											
0000000	9: 8	9 51	34	E -	47	ØD	ØA	18	ØA	00	00	00	ØD	49	48	44	52	塒NGIHDR
0000001	9: 0	0 0	0	2	9C	00	00	01	DD	08	06	00	00	00	FE	18	5A	??Z
0000002	9: B	6 <mark>0</mark> 1	0	0	00	04	73	42	49	54	08	08	08	08	70	08	64	?sBIT .d
0000003	9: 8	B <mark>0</mark> 1	3 0	0	00	09	70	48	59	73	00	00	0B	12	00	00	ØB	?pHYs
0000004	9: 1	2 01	D	2	DD	7E	FC	00	00	00	16	74	45	58	74	43	72	<u>逸</u> ~?tEXtCr
0000005	9: 6	5 <mark>6</mark> 1	7	4	69	6F	6E	20	54	69	6D	65	00	31	32	2F	31	eation Time.12/1
0000006	9: 3	9 21	3	1	35	6C	F1	55	23	00	00	00	10	74	45	58	74	9/151馯#tEXt
0000007	9: 5	3 61	6	6	74	77	61	72	65	00	41	64	6F	62	65	20	46	Software.Adobe F
0000008	9: 6	9 72	2 6	5	77	6F	72	6B	73	20	43	53	35	71	B5	E3	36	ireworks CS5q点6
0000009	9: 0	0 0	3 0	6	07	70	72	56	57	78	9C	ED	5A	49	AC	DB	44	prUWx滍ZI D
000000A	9: 1	8 91	F	0	F2	5E	5F	FA	5A	77	C6	93	D6	B5	E3	F4	20	<mark>│ - 僉騘_鵯₩荬值泗-</mark>
000000B	9: 4	3 D9	0	B	14	C 3	91	22	ØE	10	41	20	ΕØ	08	88	4A	F8	C?.脩"A ?鱷?
0000000	9: 0	4 A8	3 1	C	7A	AB	2A	38	70	60	C8	20	71	02	5F	2A	40	.?z?8p`?q*@
000000D	9: 0	8 5	5 0	8	50	41	08	21	84	AA	02	8F	AD	84	B5	65	DF	_U.PA.!劒.彮劦e?
000000E	9: 8	4 11	3 4	2	08	50	81	B2	2F	FD	99	71	96	F1	4B	93	17	?B-P伈/龣q栺K?

图片提示, Adobe Firework CS5

用Adobe Firework CS5打开图片,移走下方的图片,得到flag



• Fonts

Fonts 分值:10

 来源: hanyuhang
 难度:易
 参与人数:1396人
 Get Flag: 896人
 答题人数:903人
 解题通过率:99%

 Flag格式: CTF{xxxx}

 解题链接: http://ctf5.shiyanbar.com/stega/Fonts.doc
 通过

下载文档,打开,得到flag



 \times

• 想看正面? 那就要看仔细了!

下载图片



右键查看属性

📓 meinv.jpg 属性



•无处不在的广告

下载图片,用Stegsolve打开



在此处找到一个二维码,用qr research扫一下,得到flag

