## CTF——杂项WriteUp(题目1:代号)





CTF 专栏收录该内容

2 篇文章 0 订阅 订阅专栏



下载附件,解压得一张照片,看下图(叫"代号.jpg"):

看看照片上的妹妹,是不是很可爱呢?拿到图片,我第一反应就是拖到记事本里面,然后CTRL+f查看关键字"flag, key等",不 过本题没有如何发现.

好吧,那我们就copy到kali里面,用binwalk命令查看图片都隐藏什么信息吧(原图被我重命名为1.jpg),请看下图(图片里面内嵌有加密的zip文件):

	:	ŧ!		#!		TGZ									/0
	int-	-shared-	rest	art-vm-	VMw	areTools-	- <u>1</u> v	mware-te	ools-	UseFull					
s_	fol						root(	@kali: ~				•	•	8	
=		文件(F)	编辑(E)	查看(V)	搜索(S)	终端(T)	帮助(	H)							
		root@ka	li:~# k	binwalk	/root/D	esktop/	/1.jpg	I		THE				Â	"f
2		DECIMAL		HEXADEC	IMAL	DESCR	RIPTIC	N							
4		0 23949		0x0 0x5D8D		JPEG Zip a	image archiv	e data, ve data,	JETE sta encrypt	ndard 1. ed at le	01 ast v2.0	) to	ext	ra	
•		ct, com 218683	pressed	1 size: 0x3563B	194574,	uncomp End c	oresse of Zip	d size: archiv	e, foote	name: 1 r length	.png : 22				
M		root@ka	<b>li:~</b> #												
4															
•															~

在命令行用foremost命令分离图片, (备注:执行命令前, 先将主目录下的output文件夹下的内容清空) 看下图:





解压zip文件,确实是加密的,所以,接下来就是想法设法爆破密码了。

copy压缩包,回到物理主机,打开ARCHPR破解软件,然而我们首先想到的是明文攻击(因为同时分离出来一张照片 0000000.png)将图片压缩,按下图操作,那就开始明文攻击吧!请看下图:





点击"开始",我Cao,好像不行哦:无法进行明文攻击.请看下图:



那特么怎么搞呢????就只能暴力攻击了,那就暴力攻击吧,请看下图(得解压密码:9527):





解压得1.png图片。打开图片看看吧,这张图片肯定是我们主攻的目标了, 按我的习惯,还是托到记事本里面看看吧,发现没有什么异样的 那就打开看看图片属性啥的,特么也是没有发现什么特殊的地方 那!!!!!!我们再打开图片看看,请看下图:

照片 - 1.png								—		×
🔨 查看所有照片	十 添加到	Ð	Ŵ	$\heartsuit$	ୢ	¥	$\odot$	‰ ⊻	Ŕ	





我们会发现图片不全呀!!!!图片的"下体"去哪里啦????第一感觉技术flag藏在MM的下面了——>那就是图片的宽高问题了...

好吧,把图片放到FlexHEX中,看看吧:

🖆 FlexHEX - [1.png] —	×													
文件(E) 流(E) 编辑 搜索(S) 定位(E) 查看(Y) 工具(I) 窗口(W) 帮助(H)														
File1 1. png	→ X													
	<u>^</u>													
00000020 6C 00 00 09 70 48 59 73 00 00 0B 13 00 00 0B pHYs 1 ∎∎														
00000040 6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66 otoshop ICC prof 理题和非常														
88888888F 56 14 15 11 9C 48 55 C4 82 D5 8A 48 9D 88 E2 A8 U 注U時? H漆紅 III ·································														
00000090 28 B8 67 41 8A 88 5A 8B 55 5C 38 EE 1F DC A7 B5 (音A妓Z婾\8? 堙柴 ■稀露■■														
0000000B0 0F 80 11 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8 ■ & 表 9R? :? 耐無j 涕損														
000000C0 1F 8F 4F 48 C4 C9 BD 80 02 15 48 E0 04 20 10 E6 雇H纳組 H? 嫠 轢腹。														
00000000 CB C2 67 05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC 粉? yx <sup>∞</sup> t?? ■A 企業														
000000E0 01 HF 0F 00 02 00 70 D5 2E 24 12 C7 E1 FF 83 BH														
88888188 88 22 94 88 14 88 88 18 88 98 88 98 88 94 81 88 94 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.														
00000150 80 BD 05 00 76 8E 58 90 0F 40 60 00 80 99 42 2C ■? v頚? @`■橞, ■ 跳動)()														
00000170 D2 BF E0 H9 5F 70 85 B8 48 01 00 C0 CB 95 CD 97 1 秋噪_PHH 很吨字 ■週間■選加 BBBBB198 LED D2 22 1L D9 05 D8 10 77 52 58 58 52 21 52 52 2 第2 110130000														
88888198 6C B1 42 61 17 29 18 66 89 F4 22 9C 97 9B 23 13 1 还a ) f ? 注?														
88888148 48 E7 83 4C CE 8C 88 88 1A F9 D1 C1 FE 38 3F 98 H? L? [2] [3] [3] [3] [3] [3] [3] [3] [3] [3] [3														
000001B0 E7 E6 E4 E1 E6 66 E7 6C EF F4 C5 A2 FE 6B F0 6F 驿徭+鏻推注牛餺 编载 ■影推														
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●														
┃	~													
就绪 大小: 200, 839 字节 11 稀疏 无变化	皆ち <sup>Tong</sup>													

怎么改呢?????也不能瞎几把改呀????那就是爆破了!!!!好吧,自己动手写个脚本开始爆破吧(也可以去网上下载),请看下图:

	3	crc32key = <b>0x656</b>	5 <b>9C6C #���</b> @x�	<b>}�</b> winhex <b>��</b> cop	py hex value <b>(</b>	<b>}</b> €}								
مړ		data = bytearray	b'\x49\x48\x44\x	52\x00\x00\x03\	\xE5\x00\x00\	x01\xB4\x08\x06	\x00\x00\x00')							
0		5 n = 4095 # <b>@@@@@@@@@ffffffff,@@@@@@@@</b> @@@@@@@@@@@@												
~		for w in range(n)	):# <b>\$_</b> J <b>\$</b> h <b>\$\$\$\$</b>											
±		width = byted	array(struct.pack	:('>i', w))#qÏ8∢	ا <b>ئ</b> ي¢iÏ4¢ي	12 <b>00</b>								
		for h in rang	ge(n):											
00		height =	bytearray(struct	.pack('>i', h))										
Б	10		<pre>range(4):</pre>											
	11	data	[x+4] = width[x]											
A	问题	输出调试控制台终时					2: Python		+ 🛛	Ŵ	^			
	PS C:\ bytear PS C:\	Users\test8> & "C: ray(b'\ <mark>x00\x03</mark> Users\test8> []	/Program Files (x \\xe5') bytearray(	86)/Python37-32/ b \x00\x00\x02\>	/python.exe" xb4'	'c:/Users/test8/[	Desktop/CTF 脚本	/高和宽爆	破 . py"					
	🖄 FlexHE	X - [1.png]					- 🗆	$\times$						
	文件(17)	(a) 编辑 - <del>如</del> 去(c)	⇒倍(𝔄) 杏毛(𝔄)	⊤⊟/∿ ☎⊓(⋓)	≢88h(¥)									

×11	- \ <u>r</u> /	20167771	洲科	12;	¥ /5	/ >	ЕΙΣ	<u>1</u>	브1	3 V./	<u>т</u>	77	<b>(</b> )	堕ー	ι \ <u>π</u> γ	<del>(1</del> 5	149) \ <u>11</u>	/											
	P		0	a	1	Ж	Ē	ß	>	<b>&lt;</b>	1	ŕ	r In	1	4	X	¢	⇒											
Fil	le1	🖬 1. png																								4	Þ	×	
	00	000000	89	50	41	47	ØD	ØA	10	ØA	00	00	00	ØD	49	48	44	52	塒NG			IHDR	儞	∎ ∎朝	劉			~	
	00	000010	00	00	03	E5	<b>G</b> (	00	01	B4	08	06	00	00	00	65	66	9C	?	?		ef渓		∎∎ 4∰	齫				
	00	000020	60	00	00	00	69	70	48	59	73	00	00	ØB	13	00	00	ØB		pHYs	5		1 潁	蓋∎					
	00	000030	13	01	00	9A	90	18	00	00	ØA	4D	69	43	43	50	50	68	殖	Ī	MiC	CPPh	ē購	議論	駧				
	00	000040	6F	74	бF	73	68	óΕ	70	20	49	43	43	20	76	72	бF	66	otosi	iop 1	1 C C	prof	瓑	融調相	影				
	00	000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile	x跳s	SwX	散 >喵	酒和	剛輔					//blog.oodp.pot/Cro
	0	000060	F7	65	ØF	56	42	D8	FØ	B1	97	6C	81	00	22	23	AC	08	e Vi	M服	1?	#?	日古日	⊸					/blog.csun.net/Grea

图中圈黄的部分,有何不同???所以把图片的高度中的01改为02,看下图:

## 😫 FlexHEX - [1.png]

文件(	( <u>F</u> ) 流( <u>R</u> ) 纟	扁辑	搜索(	<u>5</u> )	定位()	<u>N</u> )	查看(	<u>v</u> ) _	L首(I	) 窗	ï□(₩)	帮助	<u> </u>					
	) 🔒 🗧	L)	<b>a</b>	Ж	È	Ē	X	<b>)</b>	🏲	14	N I		¢ →	•				
File	1 💽 1. png																	
	00000000	89	50 4	E 47	ØD	0A ·	1 0	A 01	0 0 0	តត ត	D 49	48	44 52	h <del>th</del> NG	I	HDR	儼∎■輛	
	00000017	00	00 03	3 E5	00	00	02 B	4 08	3 06	关于提	交修改	t			$\times$	ef渓		
	00000020	60	00 00	3 00	69	70	48 5	9 73	3 00							Ĩ,	1 漓書 ■	
	00000030	13	01 0	9 9 A	90	18	00 0	0 01	4D		撤消	刨表	将被复位	핥: 在它保存/	后你将	Ph	ē黷 巍癫	
	00000040	6F	74 6F	73	68	6F (	702	0 4	43	<u> </u>	》 不可	ど撤消	任何改变	ź°		of	瑯髏調播	
	00000050	69	6C 69	5 00	00	<b>78</b>	DA 9	D 53	3 77		-					>喵	洍碅鼬■	
	00000060	F7	65 ØF	56	42	D8	FO B	1 97	7 6C							<b>‡?</b>	崩∎沗∎∎│	
	00000070	C 8	10 59	) A2	10	92	00 6	1 8/	+ 10			- - - -	二、六人(	<b>は</b> ケノー		?		
	00000080	56	14 19	5 11	90	48	55 C	4 82	2 D 5			小円亚	示这个资	警告。		<b>絕</b>	■■通■躍轉	
	00000090	28	B8 67	7 41	8A	88	5A 8	B 59	5 5C		(I)	保友		🖌 町N省		重柴	■稽靏■■	
	000000A0	7D	7A EF	F ED	ED	FB	D7 F	B B(	C E7			1417		A 4X/H		y?	穽∎∎ ∎∎	
	000000B0	ØF	80 11	1 12	26	91 I	E6 A	2 66	00	39 5	2 85	30 3	3A D8	長 1 1	9R?	:?	而無j鷋	
	000000000	1F	8F 4F	- 48	C4	C9	BD 8	0 02	2 15	48 E	0 04	20	10 E6	廜H纳科	₹ H?	嫠	穀朖	
	000000D0	CB	C2 67	7 05	C5	00	00 F	0 03	3 79	78 7	E 74	B0 3	3F FC	耢?	_yx~t	7 7	■■▲ 石憲道■	
	000000000	04	AF 21		60	00	70 h	r 01	- <b>0</b> 1-	40.0	7 64		<b>NO NA</b>		o & #X	1163		

## 保存,打开看看效果:

照片	⁺ - 1.png								-		$\times$
	查看所有照片	十 添加到	Ð	Ŵ	$\heartsuit$	ୢ	Ŕ	$\odot$	‰ ✓	Ŕ	
	H <	ello			flag	this is	the key}			>	•



鸡动吗??????终于看到MM的下体的那个红色的flag了,接下来就识别图中的flag,复制提交既可。

本文属于原创,转载请说明出处。有问题的请留言!



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖