## xctf攻防世界 MISC高手进阶区 misc\_pic\_again

# 原创

18947943 ● 于 2022-01-14 18:11:08 发布 ● 5652 ☆ 收藏
 分类专栏: <u>攻防世界misc之路</u> 文章标签: <u>misc</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/l8947943/article/details/122499487</u>
 版权



<u> 攻防世界misc之路 专栏收录该内容</u>

68 篇文章 2 订阅 订阅专栏

1. 进入环境,下载附件

一张png图片,如图:



没有其他提示

### 2. 问题分析

- winhex大法

   一通操作无果
- binwalk大法
   一通操作无果

### 3. StegSolve大法 这点我属实没思路,参考大佬wp:





在BitPlanes界面,提取RGB为0通道的,点击Preview,发现提取的内容,开头以PK开始,如图:

<u>ه</u>	– 🗆 X										
Extract Preview											
5041030414000000       080073118c4933e2       PKs13.         776a2c0900003c21       00001001c003155       wj, 10</td 54090003a94d4e58       bf4d4e5875780b00       TMNX .MNXux         010400000000400       000000ed596f6c5b      Yol[         5715bfcfcedf2675       9cd26eeelf1a6b6b       W&u .nkk         513a296ed2a6594a       356ae75f5f2aa70d       Q:)nYJ       5j*         9488ac131674ec03       1fca24a47de0c390      t\$.}											
f6814f1010525352 adl3e2438a04aa04ORSRC											
Bit Planes	Order settings										
Alpha 7 6 5 4 3 2 1 0	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 🗾 0	Bit Plane Order										
Blue 7 6 5 4 3 2 1 2 0	● RGB ○ GRB										
	◯ RBG ◯ BRG										
Preview Settings Include Hex Dump In Preview	⊖ GBR ⊖ BGR										
Preview Save Text Save Bin Cancel CSDN @18947943											

也就是说,提取的这个文件是.zip隐写的内容(如何判断,参考之前的文件标识推断: https://blog.csdn.net/holandstone/article/details/7624343),我们将其保存为.zip文件

-	<u>چ</u>	– 🗆 ×
	Extract Preview	
	rennseredare arearenneanean	
	63b138edb196afb6 a9549ca962df4701 c.8Tb.G.	
	8c04e276014934fc 44bffb731b8e4774v.I4. DsGt	
7	cl242d189389c712 70fb8e0e8dbe008c .\$ p	
į,	0e2353e3ff0d971d 54cfc904970fe150 .#S TP	
7	2983c200c7394del 47243a38ea292449 )9M. G\$:8.)\$I	
2	3ad57d76db648flc 4e3blc648d249176 :.}v.d N;.d.\$.v	
	ab63c7124a895b7f c71db1ff62461ca5 .cJ.[[bF	
1	f547627192a494a7 6276db1db745c524 .Gbq bvE.\$	
0	4e264d7260 N&Mr`	=
1		<b>•</b>
	Dit Dianos	Ordor softings



#### 打开,如图:

<ul> <li>3 1.zip - Bandizip (Standard) –</li> <li>文性(日) 編撮(日) 奇邦(日) 洗面(〇) 抑悶(〇) 工目(円) 帮助(日)</li> </ul>												
		<u></u> 远坝( <u>C</u>	「「「」」」	上其(1) 報助 上 法 添加		97 Mil	) 扫描	。 。 章	(代码页			
₽ 1.zip			名称				压	缩后大小 2,348	原始大小 8,508	类型		
			<								>	
							① 文件:	1,文件夹:05	的物质	月475	43	

将压缩文件里的内容丢入winhex,在文本中搜flag或者ctf,如图:

Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	$\odot$	ANSI	ASC	II	~
00000590	4C	89	EA	4C	89	F6	44	89	FF	41	FF	14	DC	48	83	C3	L‰êI	l‰öD‰ÿA	ÿ ÜH	fÃ	
000005A0	01	48	39	EB	75	EA	48	83	С4	08	5B	5D	41	5C	41	5D	H9ē	éuêH∱Ä	[]A\	A]	
000005B0	41	5E	41	5F	С3	66	66	2E	0F	1F	84	00	00	00	00	00	A^A	Ãff.	,,		
000005c0	F3	С3	00	00	48	83	EC	08	48	83	C4	08	С3	00	00	00	ćÃ	Hfì Hf	ÄÃ		
000005D0	01	00	02	00	00	00	00	00	68	63	74	66	7в	73	63	78		hc	tf{s	cx	
000005E0	64	63	33	74	6F	6B	33	79	62	30	61	72	64	34	67	34	dc3t	ok3yb0	ard4	g4	
000005F0	31	6E	7E	7E	7E	7D	00	00	00	00	01	1B	03	3в	30	00	ln~~	~~ }	;	0	
00000600	00	00	05	00	00	00	04	FE	FF	FF	7C	00	00	00	44	FE		þÿÿ	1 1	Dþ	
00000610	FF	FF	4C	00	00	00	31	FF	FF	FF	Α4	00	00	00	54	FF	ÿÿL	1ÿÿÿ	a i	Гÿ	
00000620	FF	FF	C4	00	00	00	C4	FF	FF	FF	0C	01	00	00	14	00	ÿÿÄ	Äÿÿÿ			
00000630	00	00	00	00	00	00	01	7A	52	00	01	78	10	01	1B	0C		zR	х		
00000640	07	08	90	01	07	10	14	00	00	00	1C	00	00	00	F0	FD				ðý	
00000650	FF	FF	2A	00	00	00	00	00	00	00	00	00	00	00	14	00(	37	089	9479	943	2
																					~

最终的答案为: hctf{scxdc3tok3yb0ard4g41n~~~}