攻防世界 - MISC - 06 - SimpleRAR

原创

古月浪子 于 2019-10-03 15:09:34 发布 8248 收藏 17

分类专栏： 攻防世界CTF新手练习区 文章标签： 攻防世界 XCTF CTF WP writeup

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/tqydyqt/article/details/101992518

版权

攻防世界CTF新手练习区 专栏收录该内容

11 篇文章 7 订阅

订阅专栏

攻防世界 - MISC - 06 - SimpleRAR

审题

思路

知识点

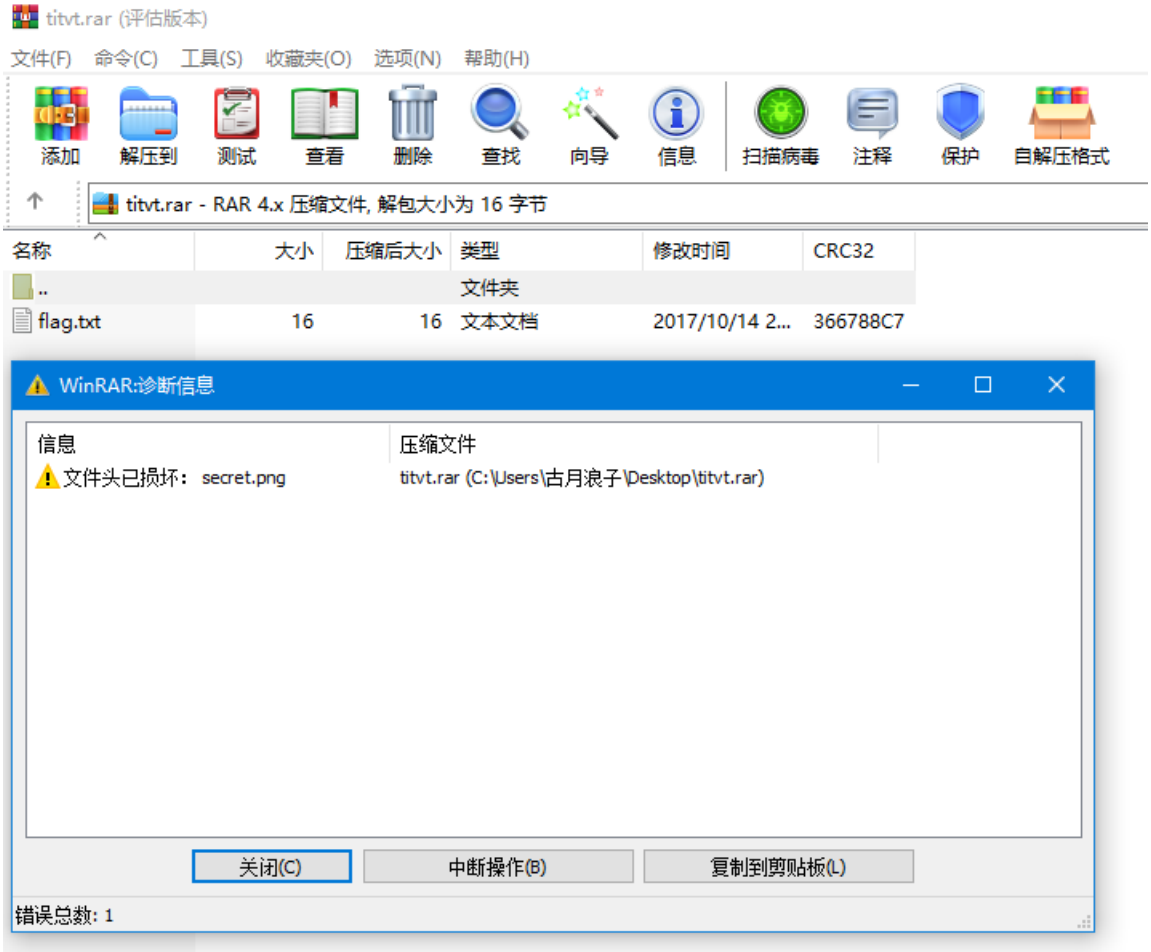
考查选手对rar文件头的理解、winhex更改文件的能力、PS提取图层的能力、CTF工具的使用、PS图像处理能力

所需工具

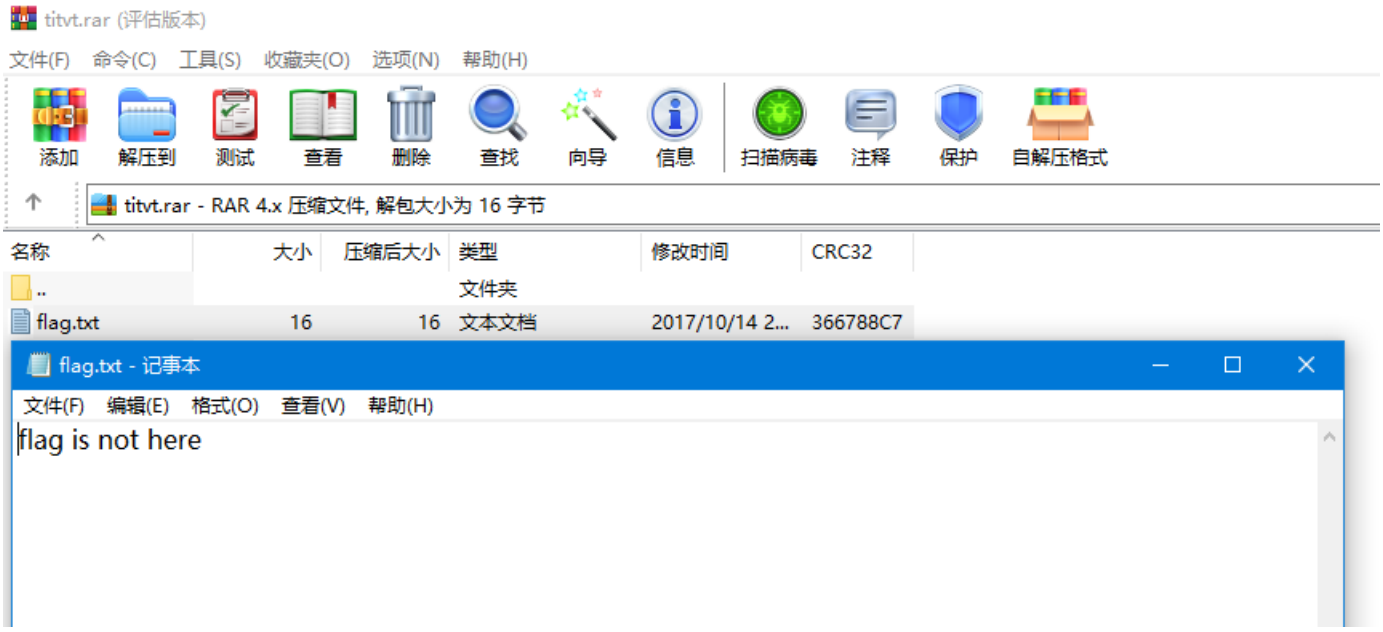
WinRAR、winhex、PhotoShop、StegSolve

解题

使用WinRAR打开附件，发现secret.png的文件头损坏了，并且还有一个flag.txt



抱着侥幸的心理打开flag.txt



既然没有flag，那么我们用winhex打开附件

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç^g6m»NK 0
00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	flag.txt °W
00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000050	65	A8	3C	7A	20	90	2F	00	3A	15	00	00	42	16	00	00	e¨<z / : B
00000060	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	¼éŒ/n„OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png ð@«
00000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑU€ ™Ä ‡“"
00000090	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ ±¤X 3ƒ ô: B
000000A0	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	…–!« C fìa !
000000B0	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«= €° Å ¡ „B°C)
000000C0	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú #™Ìó Ä…†gs9Þ
000000D0	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc'ÞÄwí¨ÜFôÅTÍUj
000000E0	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	A9	8F	D5	3F	ª£_Ínw; ïz™©© Õ?
000000F0	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	ªùU žc¢œ†ˆÌYÌÿ
00000100	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{‹ ùÀ÷æ0ã%`UX
00000110	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šÌæÍËý $Cƒ0FÖ–0

可以看到从here后面开始就应该是secret.png的部分了，百度了一下rar每个块的开头

每一个块都是由以下域开始的：【译者注：即每一个块的头部都是由以下域（可称之为头域）组成的】

HEAD_CRC 2 bytes CRC of total block or block part

整个块或者块某个部分的CRC（根据块类型而有不同）

HEAD_TYPE 1 byte Block type

块类型【译者注：也可以理解为块头部类型，因为不同的块对应不同的块头部。后文也经常混淆这两种概念。】

已经声明过的块类型包括：

HEAD_TYPE=0x72 marker block【译者注：有些文献里也称之为MARK_HEAD】

标志块【译者注：一个固定为0x52 61 72 21 1A 07 00的7字节序列】

HEAD_TYPE=0x73 archive header【译者注：有些文献里也称之为MAIN_HEAD】

归档头部块

HEAD_TYPE=0x74 file header【译者注：有些文献里也称之为FILE_HEAD】

文件块【译者注：直译为文件头部，但是此处的类型应该指的是整个块的类型，而非块头部结构的类型，因此感觉称之为文件块更合适。】

HEAD_TYPE=0x75 old style comment header

老风格的 注释块【译者注：直译为注释头部，基于和文件块一样的原因，感觉称之为注释块更合适】

HEAD_TYPE=0x76 old style authenticity information

老风格的 授权信息块/用户身份信息块

HEAD_TYPE=0x77 old style subblock

老风格的 子块

HEAD_TYPE=0x78 old style recovery record

老风格的 恢复记录块

HEAD_TYPE=0x79 old style authenticity information

老风格的 授权信息块/用户身份信息块

HEAD_TYPE=0x7a subblock

子块

HEAD_TYPE=0x7b end block

结束块【译者注：一个固定为0xC4 3D 7B 00 40 07 00的7字节序列】

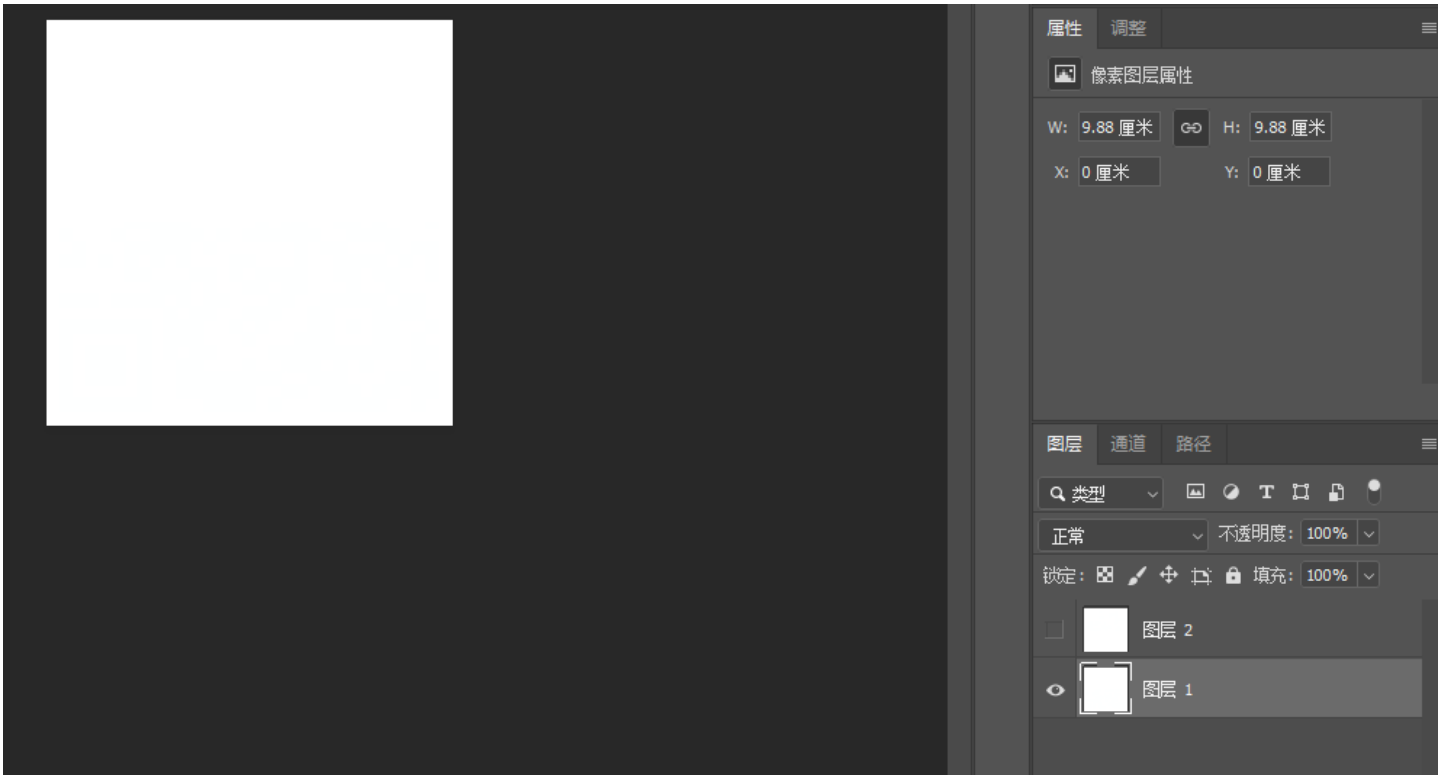
我们要的是文件块而不是子块，于是更改7A为74，成功解压，发现是一张空白的图片，继续用winhex打开

secret.png

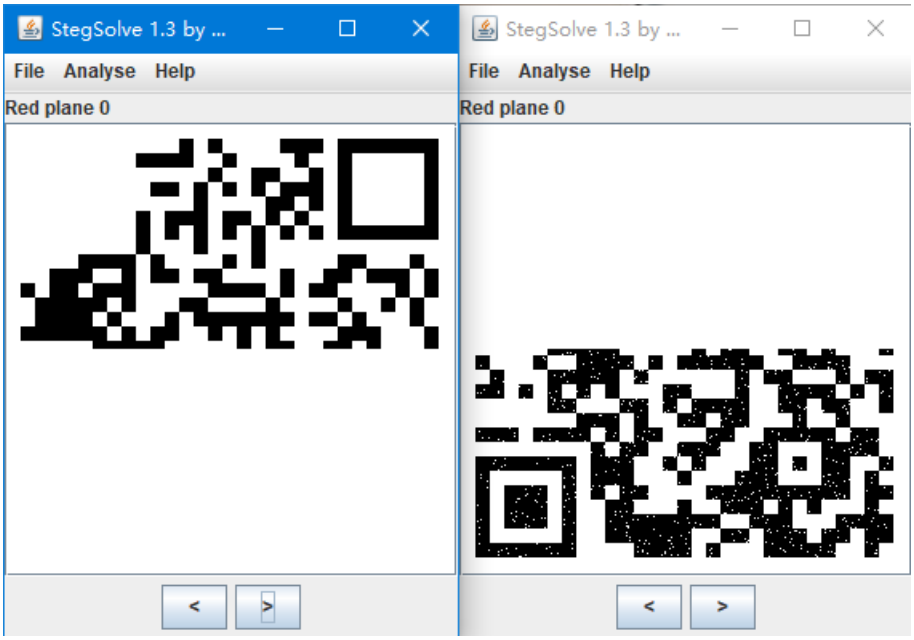
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GIF89a ' þÿÿ
00000010	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	ÿÿÿÿÿÿ !ÿ XMP

```
00000020  44 61 74 61 58 4D 50 3C  3F 78 70 61 63 6B 65 74  DataXMP<?xpacket
00000030  20 62 65 67 69 6E 3D 22  EF BB BF 22 20 69 64 3D   begin="ï»¿" id=
00000040  22 57 35 4D 30 4D 70 43  65 68 69 48 7A 72 65 53  "W5M0MpCehiHzreS
00000050  7A 4E 54 63 7A 6B 63 39  64 22 3F 3E 20 3C 78 3A  zNTczkc9d"?> <x:
00000060  78 6D 70 6D 65 74 61 20  78 6D 6C 6E 73 3A 78 3D  xmpmeta xmlns:x=
00000070  22 61 64 6F 62 65 3A 6E  73 3A 6D 65 74 61 2F 22  "adobe:ns:meta/"
00000080  20 78 3A 78 6D 70 74 6B  3D 22 41 64 6F 62 65 20   x:xmptk="Adobe
00000090  58 4D 50 20 43 6F 72 65  20 35 2E 33 2D 63 30 31  XMP Core 5.3-c01
000000A0  31 20 36 36 2E 31 34 35  36 36 31 2C 20 32 30 31  1 66.145661, 201
```

发现是gif格式，将其重命名并用PhotoShop打开，发现有两个空白的图层



将两个图层分别提取出来，用StegSolve打开，不断点击箭头直到显示出图像



将两幅二维码拼接到一起并补全定位点，扫描二维码得到flag

flag

flag{yanji4n_bu_we1shi}

反思与心得

这道题考查了非常多的知识点，根本不像一道1★的题。。。
网上很多WP说A8 3C 74是rar对png的文件头编码，这种说法是错误的，做学问切忌一知半解！
很多专门针对CTF而编写的工具是我们日常生活中用不到的，要多收集整理此类工具并灵活运用
（吐槽：360压缩压根不提示你文件头损坏=_=...）