简单图片隐写术破解

原创

皮一下怎么了 于 2017-03-03 20:45:30 发布 22245 收藏 12
分类专栏： CTF解题记录 文章标签： CTF 隐写术 破解

本文链接：https://blog.csdn.net/qq_37226316/article/details/60148155


CTF解题记录 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

这是百度杯上的一个小测试题,首先点击访问看到图片

一看名字就猜到应该是包含了压缩包,但是我们还是用工具看看,保存图片放到kali中,在终端切换到图片所在目录用binwalk查看,执行命令:binwalk zip.jpg

```
root@kali:~/桌面# binwalk zip.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
8204          0x200C          TIFF image data, little-endian offset of first image directory: 8
15164         0x3B3C          Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
18187         0x470B          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description
 rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://
80985         0x13C59         Zip archive data, at least v2.0 to extract, compressed size: 34, un
compressed size: 32, name: key.txt
81071         0x13CAF         End of Zip archive
```

发现确实存在压缩包文件,继续将其提取出来,执行命令:binwalk -e zip.jpg

多出了一个压缩包文件,我们将其拿出来放在windows下解压发现文件破损,于是继续尝试用winhex查看,找到压缩包用winhex打开

13C59.zip

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	50	4B	03	04	14	00	00	00	08	00	A5	91	BB	46	BC	BD	PK ¥'»F¼½
00000016	30	5C	22	00	00	00	20	00	00	00	07	00	00	00	6B	65	0\" ke
00000032	79	2E	74	78	74	36	62	65	35	33	30	65	37	38	61	64	y.txt6be530e78ad
00000048	65	36	30	35	33	34	37	30	35	39	37	30	31	61	35	34	e605347059701a54
00000064	66	39	39	36	65	6B	65	79	2E	74	78	74	D0	01	44	96	f996ekey.txtÐ D-
00000080	22	B5	65	98	D0	01	50	4B	05	06	00	00	00	00	01	00	"µe˜Ð PK
00000096	01	00	59	00	00	00	47	00	00	00	00	00					Y G

发现flag,即为flag{6be530e78ade605347059701a54f996e}