攻防世界 MISC Reverse-it

原创

YUK_103 于 2020-01-05 14:27:51 发布 1791 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/YUK_103/article/details/103842782

首先给了一个不知道是什么东西的文件。将它放进winhex以及用binwalk都不知道他到底是什么文件。

但是。。。。

reverse-it，考虑从这个文件的16进制信息下手

```
84 00 84 00 10 10 10 00  64 94 64 A4 01 00 0E FF
8D FF
```

这是文件结尾的东西，这上图和下图是不是有点相似之处?

JPEG (jpg)，文件头：FFD8FF

不错，整个文件被倒过来了。

这里我是使用python脚本给逆转过来的。

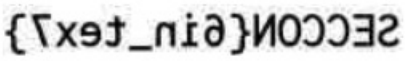
```python
import os
f = open('1',"rb")#二进制形式打开
f = f.read()[::-1]
for i in f:
    ans = str(hex(i))[2:][::-1]
    if len(ans) == 1:
        ans = ans + '0'
    print(ans,end='')
```

这样可以得到这个文件的正着的hex字符，我们新建一个文件，将其复制进去并保存。得：

1 | test.jpg | t.jpg

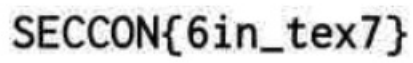
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48	ÿØÿà JFIF H
00000010	00	48	00	00	FF	E1	00	D2	45	78	69	66	00	00	4D	4D	H ÿá ÒExif MM
00000020	00	2A	00	00	00	08	00	07	01	12	00	03	00	00	00	01	*
00000030	00	01	00	00	01	1A	00	05	00	00	00	01	00	00	00	62	b
00000040	01	1B	00	05	00	00	00	01	00	00	00	6A	01	28	00	03	j (
00000050	00	00	00	01	00	02	00	00	01	31	00	02	00	00	00	19	1
00000060	00	00	00	72	01	32	00	02	00	00	00	14	00	00	00	8C	r 2 Œ
00000070	87	69	00	04	00	00	00	01	00	00	00	A0	00	00	00	00	‡i
00000080	00	00	00	48	00	00	00	01	00	00	00	48	00	00	00	01	H H
00000090	73	74	6E	65	6D	65	6C	45	20	70	6F	68	73	6F	74	6F	stnemelE pohsoto
000000A0	68	50	20	65	62	6F	64	41	00	46	32	30	30	31	3A	30	hP ebodA F2001:0
000000B0	30	3A	32	32	20	31	30	3A	34	31	3A	30	32	00	00	03	0:22 10:41:02
000000C0	A0	01	00	03	00	00	00	01	00	01	00	00	A0	02	00	04	
000000D0	00	00	00	01	00	00	00	C8	A0	03	00	04	00	00	00	01	È
000000E0	00	00	00	1A	00	00	00	00	FF	E1	09	90	68	74	74	70	ÿá http
000000F0	3A	2F	2F	6E	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	://ns.adobe.com/
00000100	78	61	70	2F	31	2E	30	2F	00	3C	3F	78	70	61	63	6B	xap/1.0/ <?xpack
00000110	65	74	20	62	65	67	69	6E	3D	22	EF	BB	BF	22	20	69	et begin="ï»¿" i
00000120	64	3D	22	57	35	4D	30	4D	70	43	65	68	69	48	7A	72	d="W5M0MpCehiHzr
00000130	65	53	7A	4E	54	63	7A	6B	63	39	64	22	3F	3E	20	3C	eSzNTczkc9d"?> <
00000140	78	3A	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	3A	x:xmpmeta xmlns:
00000150	78	3D	22	61	64	6F	62	65	3A	6E	73	3A	6D	65	74	61	x="adobe:ns:meta
00000160	2F	22	20	78	3A	78	6D	70	74	6B	3D	22	58	4D	50	20	/" x:xmptk="XMP
00000170	43	6F	72	65	20	35	2E	34	2E	30	22	3E	20	3C	72	64	Core 5.4.0"> <rd
00000180	66	3A	52	44	46	20	78	6D	6C	6E	73	3A	72	64	66	3D	f:RDF xmlns:rdf=
00000190	22	68	74	74	70	3A	2F	2F	77	77	77	2E	77	33	2E	6F	"http://www.w3.o
000001A0	72	67	2F	31	39	39	39	2F	30	32	2F	32	32	2D	72	64	rg/1999/02/22-rd
000001B0	66	2D	73	79	6E	74	61	78	2D	6E	73	23	22	3E	20	3C	f-syntax-ns#"> <
000001C0	72	64	66	3A	44	65	73	63	72	69	70	74	69	6F	6E	20	rdf:Description
000001D0	72	64	66	3A	61	62	6F	75	74	3D	22	22	20	78	6D	6C	rdf:about="" xml
000001E0	6E	73	3A	78	6D	70	3D	22	68	74	74	70	3A	2F	2F	6E	ns:xmp="http://n
000001F0	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	s.adobe.com/xap/
00000200	31	2E	30	2F	22	20	78	6D	70	3A	43	72	65	61	74	6F	1.0/" xmp:Creato
00000210	72	54	6F	6F	6C	3D	22	50	69	78	65	6C	6D	61	74	6F	rTool="Pixelmato

打开图片



你可以拿个镜子一靠，直接看。我这里没有镜子，于是又写了一个脚本

```
from PIL import Image
im = Image.open("t.jpg")
pim = im.load()
an = Image.open("t.jpg")
ans = an.load()
for i in range(im.size[0]):
    for j in range(im.size[1]):
        ans[i, j] = pim[im.size[0]-i-1, j]
an.show()
```



get flag

PIL操作： 传送门

以上。