MOCTF misc 杂项 writeup （持续更新）

原创

Um0 于 2019-03-15 21:01:57 发布 503 收藏

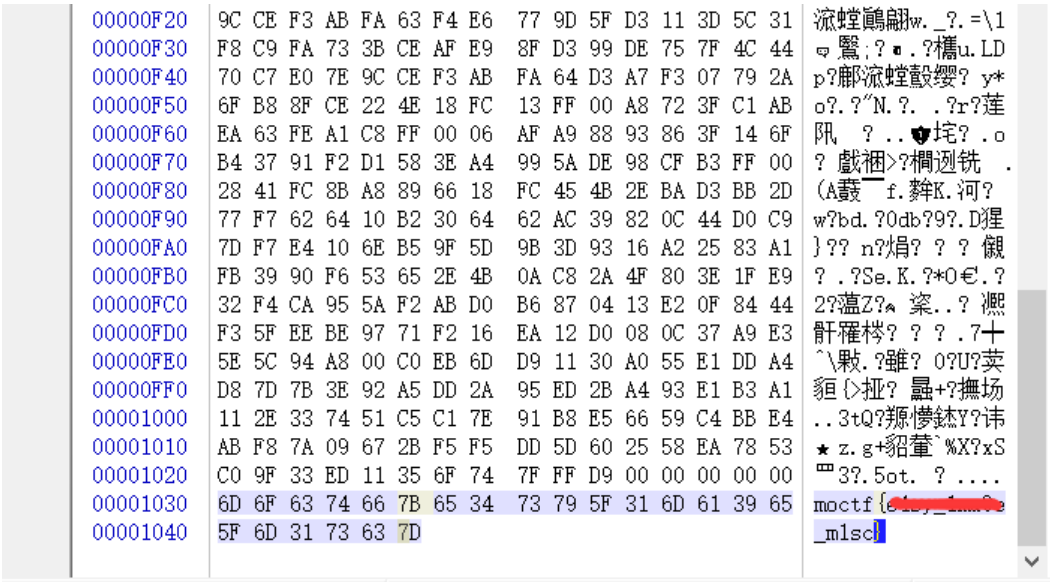
分类专栏： MOCTF 文章标签： ctf moctf 杂项 misc

本文链接：https://blog.csdn.net/qq_41358038/article/details/88583930

MOCTF misc 杂项 writeup （持续更新）

1.我可是黑客

打开之后是张图片，查看属性等操作后无果，扔到winhex里，在最低端发现了flag



2.假装安全

又是一张图片，直接foremost一下
（大家可以在找找在Windows上使用foremost的放发，非常方便，遇到图片隐写的题可以直接foremost一下，有时候会有奇效）
分离出了一个压缩包，发现有加密。
猜测为伪加密，用winhex打开压缩包

zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	14	00	00	08	08	00	14	69	0F	4B	05	42	PK.....i.K.B
00000010	E8	C6	18	00	00	00	16	00	00	00	08	00	00	00	66	6C	杵.....fl
00000020	61	67	2E	74	78	74	CB	4D	4E	73	2E	4A	CB	A9	0C	36	ag.txt蔓Ns.J拴.6
00000030	4C	CD	2F	A9	76	48	2D	CD	89	CF	49	A9	05	00	50	4B	L?/?vH-?墦I?..PK
00000040	01	02	3F	00	14	00	09	08	08	00	14	69	0F	4B	05	42	..?.....i.K.B
00000050	E8	C6	18	00	00	00	16	00	00	00	08	00	24	00	00	00	杵.....$...
00000060	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	67	....flag
00000070	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	.txt.. .....
00000080	9F	4A	58	8E	84	15	D3	01	DC	E1	95	32	8E	0F	D3	01	焊X?? ? 茆? ?.?.
00000090	DC	E1	95	32	8E	0F	D3	01	50	4B	05	06	00	00	00	00	茆? ? ? PK.....
000000A0	01	00	01	00	5A	00	00	00	3E	00	00	00	00	00			....Z...>.....

将这个9改为0，发现加密去掉了，打开里面的flag.txt，得到flag（还需要栅栏解密一下）

3.扫扫出奇迹

打开之后是个经过反色处理的二维码，这里介绍两个方法

- 打开QQ，发送图片，选中，就会发现图片被反色处理了

- 利用Windows系统自带的画图工具打开，
  快捷键ctrl+shift+i
  进行反色处理

两种方法都能得到正确的二维码，扫出flag

4.光阴似箭

打开后是一张图片，flag不断闪过
把图片下载下来，用StegSolve打开，Analyse，Frame Browser，就能翻到flag了

5.杰斯的魔法

```
document.write(unescape('%3Cscript%20language%20%3D%20%22javascript%22%3Ealert%28%22moctf%7Bscrlpt_1s_magica1%7D%22%29%3B%3C/script%3E'));
```

解题关键在这一部分
%7B 是 { 的url编码
%7D 是 } 的url编码
flag就显而易见了