base64stego的writeup

原创

MarcusRYZ 于 2020-02-10 23:32:58 发布 716 收藏 2

分类专栏： 攻防世界MISC新手练习区 文章标签： 安全

本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104256644

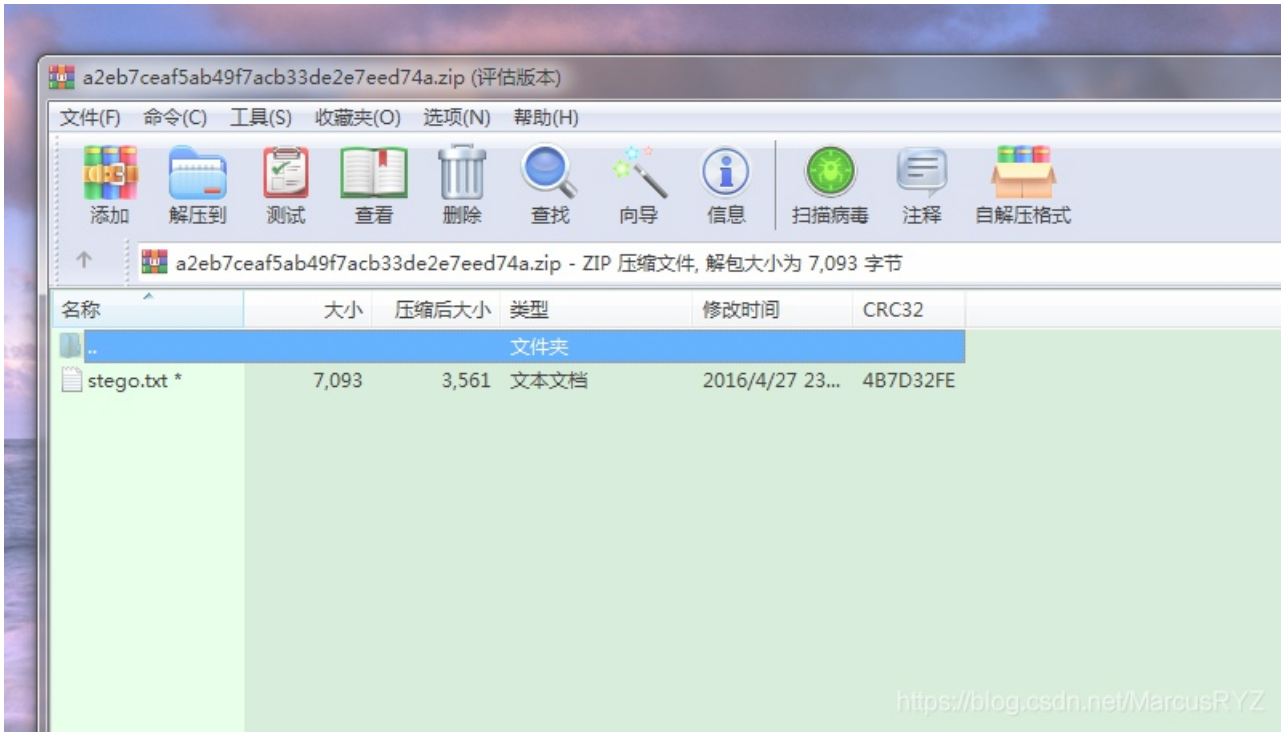
攻防世界MISC新手练习区 专栏收录该内容

12 篇文章 0 订阅

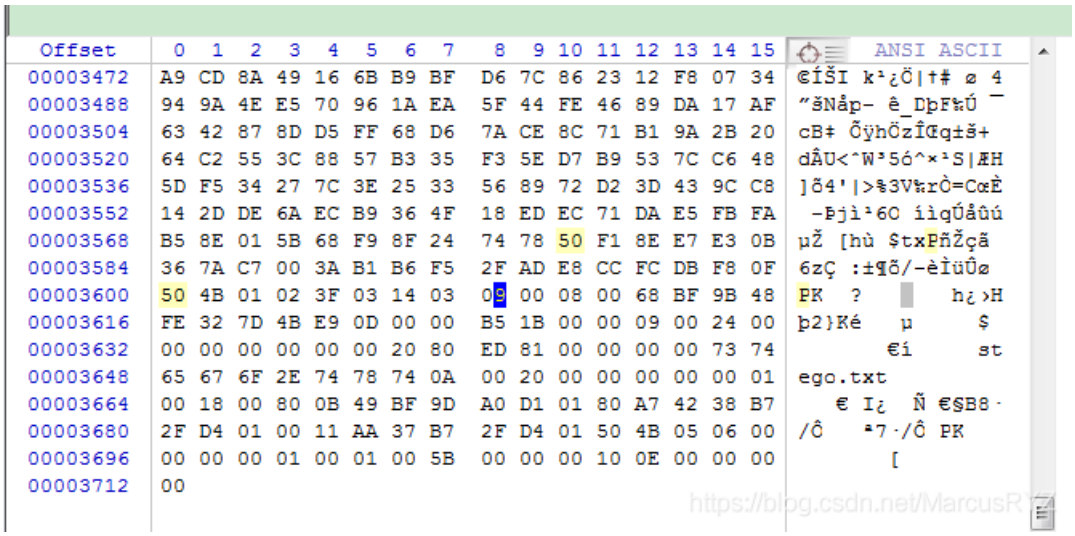
订阅专栏

大家好，这次我为大家带来攻防世界misc部分base64stego的writeup。

先下载附件，是一个压缩包，用WinRAR查看一下，发现压缩包被加密了。



由于这道题没有任何关于压缩包解压密码的提示，暴力破码也肯定不现实，因此我们想到这会不会是一个伪加密。用winhex打开一看，果然如此。



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00003472	A9	CD	8A	49	16	6B	B9	BF	D6	7C	86	23	12	F8	07	34	©ÍŠI k¹¿Ö|†# ø 4
00003488	94	9A	4E	E5	70	96	1A	EA	5F	44	FE	46	89	DA	17	AF	”šNåp- ê_DþF‰Ú ¯
00003504	63	42	87	8D	D5	FF	68	D6	7A	CE	8C	71	B1	9A	2B	20	cB‡ ÕÿhÖzÎŒq±š+
00003520	64	C2	55	3C	88	57	B3	35	F3	5E	D7	B9	53	7C	C6	48	dÂU<ˆW³5ó^×¹S|ÆH
00003536	5D	F5	34	27	7C	3E	25	33	56	89	72	D2	3D	43	9C	C8	]õ4'|>%3V‰rÒ=CœÈ
00003552	14	2D	DE	6A	EC	B9	36	4F	18	ED	EC	71	DA	E5	FB	FA	-Þjì¹6O íìqÚåûú
00003568	B5	8E	01	5B	68	F9	8F	24	74	78	50	F1	8E	E7	E3	0B	µŽ [hù $txPñŽçã
00003584	36	7A	C7	00	3A	B1	B6	F5	2F	AD	E8	CC	FC	DB	F8	0F	6zÇ :±¶õ/-èÌüÛø
00003600	50	4B	01	02	3F	03	14	03	09	00	08	00	68	BF	9B	48	PK ? h¿›H
00003616	FE	32	7D	4B	E9	0D	00	00	B5	1B	00	00	09	00	24	00	þ2}Ké µ $
00003632	00	00	00	00	00	00	20	80	ED	81	00	00	00	00	73	74	€í st
00003648	65	67	6F	2E	74	78	74	0A	00	20	00	00	00	00	00	01	ego.txt
00003664	00	18	00	80	0B	49	BF	9D	A0	D1	01	80	A7	42	38	B7	€ I¿ Ñ €§B8·
00003680	2F	D4	01	00	11	AA	37	B7	2F	D4	01	50	4B	05	06	00	/Ô ª7·/Ô PK
00003696	00	00	00	01	00	01	00	5B	00	00	00	10	0E	00	00	00	[
00003712	00																

将蓝色标记处的9改为0并保存即可。解压文件后找到一个TXT文档，打开发现密密麻麻的字符。结合题目猜测这是base64编码，直接解码无疑是不行的。这是想到这可能是base64隐写。所谓base64隐写，就是依据每一串base64编码末尾可能存在的等号进行隐写，具体请大家自己查阅百度。

然后我写了一个python脚本将隐藏的二进制编码提取出来并且转为字符。

```
def base64_decode(strings):
    aaa = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    if strings[-2] == "=":
        strings1 = bin(aaa.find(strings[-3]))[2:].zfill(10)
        strings1 = strings1[-4:]
    else:
        strings1 = bin(aaa.find(strings[-2]))[2:].zfill(10)
        strings1 = strings1[-2:]
    return strings1
path = input("输入TXT文档所在的文件夹")
filename = input("输入TXT文档名")
f = open(path + "\\" + filename + ".txt", "r")
bb = ""
for line in f.readlines():
    base64 = line.strip()
    if base64[-1] == "=":
        bb += base64_decode(base64)
i = 0
b = ""
flag = ""
while i <= len(bb) - 1:
    b += bb[i]
    if i % 8 == 7:
        flag += chr(int(b, 2))
        b = ""
    i += 1
f = open(path + "\\" + "result.txt", "w")
f.write(flag)
```

运行之后flag就出来了，flag：Base_sixty_four_point_five 。