




# 记一次MP3隐写

原创

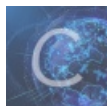
D-R0s1  于 2018-10-08 22:27:27 发布  1142  收藏 1

分类专栏: [CTF WriteUp 杂项](#) 文章标签: [mp3stego 杂项 音频隐写](#)

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/CliffordR/article/details/82974875>

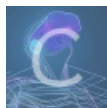
版权



[CTF WriteUp](#) 同时被 2 个专栏收录

28 篇文章 3 订阅

订阅专栏



[杂项](#)

7 篇文章 0 订阅

订阅专栏

[记一次misc中的mp3隐写](#)

在解决ctf中mp3隐写时，常常会用到一款工具——mp3stego。这款工具的安装还请自行百度。由于这篇文章专门为mp3setego这款工具量身打造的，解题过程中遇到的其他知识点就一带而过了，题目是内部平台上的也就不分享给大家了，毕竟各大CTF平台上都有此类题目。

这个题目的名字叫做pick\_me\_up，是一个压缩包的形式，解压缩后发现一个mp3文件，还有一个jpg，解压出来心里就差不多有数了，音频隐写类的，但是那个jpg有什么用呢？那是给mp3文件解密的密码。这个jpg还死活打不开，图片隐写？？刚开始以为文件头有问题，查了文件头，跑了binwalk，发现都没用，扔进winhex查找password，找到一句话password is password，顿时心里那个mmp啊，其实写到这里也就说明了一个问题，解决问题的方法和思路很重要，方法不对，努力白费啊！好了，密码已经找到了现在解密mp3，用mp3stego解密mp3时一定注意，要把需要解密的mp3文件放在MP3Stego的MP3Stego文件夹里

Decoder	2015-12-12 12:16	文件夹	
Encoder	2015-12-12 12:16	文件夹	
tables	2015-12-12 12:16	文件夹	
Decode.exe	2006-06-13 7:38	应用程序	228 KB
Encode.exe	2006-06-13 7:39	应用程序	340 KB
hidden_text.txt	2000-11-30 12:13	文本文档	1 KB
MP3Stego.sln	2006-06-13 7:24	SLN 文件	3 KB
README.txt	2015-12-12 12:25	文本文档	6 KB
svega_stego.mp3	2018-07-02 15:46	音频文件	324 KB

Mp3stego这个工具我安装在了我电脑的D盘，同时按住win键和r，打开dos命令框，

```
C:\Users\lenovo>D:
D:\>cd \MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego
D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego>
```

到mp3stego的目录下，然后使用命令：decode -X -P password svega\_stego.mp3

```
D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego>decode -X -P password svega_stego.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'svega_stego.mp3' output file = 'svega_stego.mp3.pcm'
Will attempt to extract hidden information. Output: svega_stego.mp3.txt
the bit stream file svega_stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of 'svega_stego.mp3' is finished
The decoded PCM output file name is 'svega_stego.mp3.pcm'
```

命令解释：-X -P 后面紧跟的先是密码，后是要解密的文件名。现在再回到MP3Stego的目录下就会发现多出了一个.txt文件，里面就是解密出来的东西了。