CTF 记一次音频隐写

原创

D-R0s1 于 2018-07-19 20:54:07 发布 4093 收藏 6
分类专栏： CTF WriteUp 文章标签： CTF Write Up 音频隐写 mp3stego的使用 misc

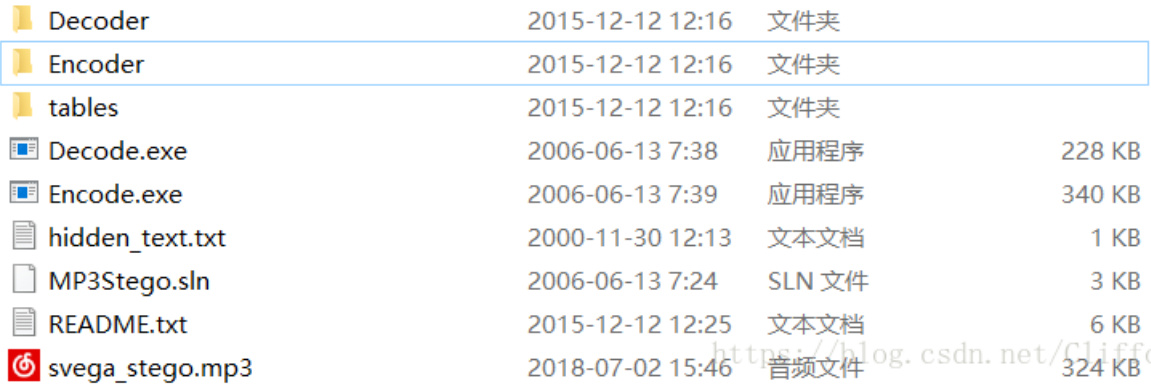
本文链接：https://blog.csdn.net/CliffordR/article/details/81122543

CTF WriteUp

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。闲话少说，直接开始吧。CliffordWR喜欢讲干货（真够自恋）。

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是什么用呢？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



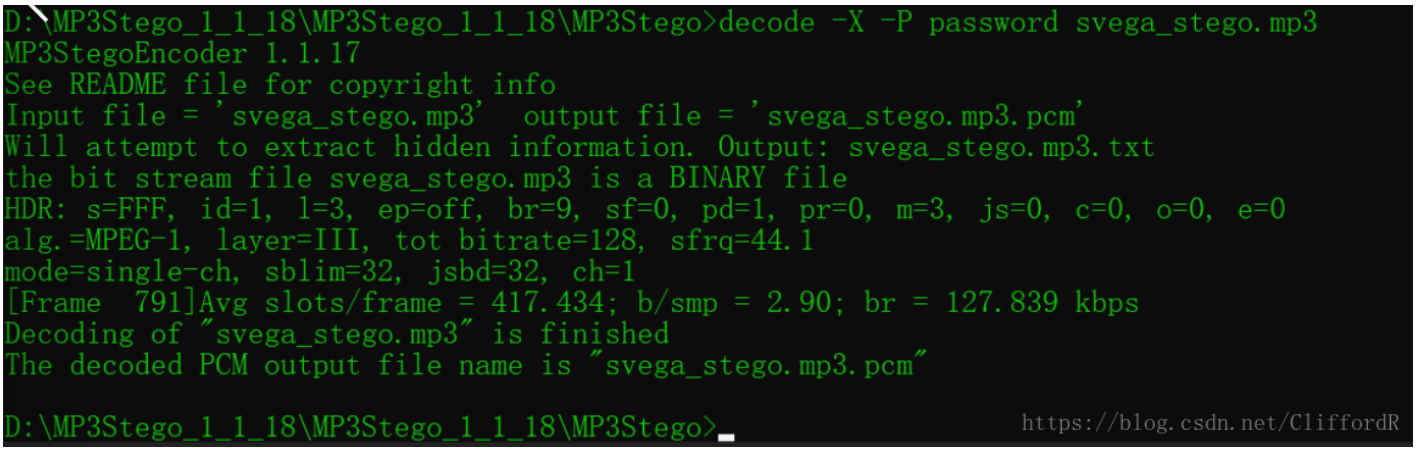
Mp3stego这个工具我安装在了我电脑的D盘，同时按住win键和r，打开dos命令框，

```
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



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。题目就这样简单加愉快的做完了，是不是很开心呢，快去找个音频隐写试试吧。