HGAME Week1 WriteUp

MISC

啥都写不出来，感觉自己要撑不住了（逃）

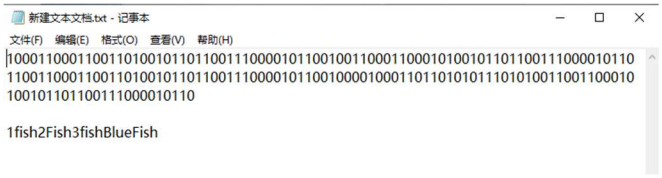
2. 三重隐写

下载文件发现有个 exe 应该是个工具先装了，可以想到应该是用来解 flag.crypto 这个文件的。这个 7z 文件是加密过的，突破口肯定在三个音频文件里。首先看到的就是这首 unlasting，这封面太奇怪了。。用 potplayer 把封面提取出来

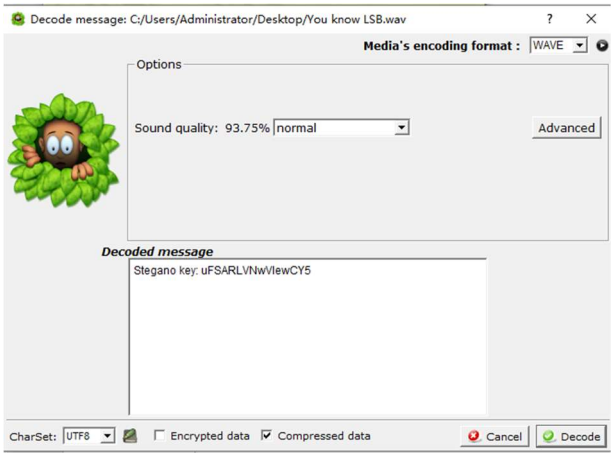
看着像个条码，用工具扫一下看看

Cover (front).pngAES key: 1ZmmeaLL^Typbcg3

得到一个 key，试一下是不是解压密码，发现并不是，那应该就是解 flag 的密码，反正肯定是有用的。接下来用记事本打开三个音乐文件看看，发现“上裹与手抄卷.mp3”这个文件里面有一句“Stegano key in LSB.”想到应该是用了 MP3Stego 工具且密码在 wav 文件里。查了一下如何解决 wav 文件的 LSB，一开始是用了一个脚本（https://ethackal.github.io/2015/10/05/derbycon-ctf-wav-steganography/）解出来



Woc，多么完美的句子，没错了这就是密钥，然后就拿去解密了，发现并不行？？肯定哪里出问题，一开始以为是工具的问题，换了一个版本，还是不行。又去查了一下，找到 silenteye 这个工具拖进去，得到



惊了，啥操作，肝好痛。那就是之前那个密钥错了，虽然不知道为什么那么有意义。。。用这个密钥从 MP3 文件中解出压缩包密码

解压出来，用最早扫出来的工具和密码解得 flag。