HGAME 2020 WRITE UP

MISC

1. 欢迎参加 HGAME

base64 转码得摩斯代码解密得到 flag　　W3LCOME_TO_2020_HGAM3

2. 壁纸

binwalk 分离图片得压缩包，密码是 p 站 id

pixiv.net/artworks/76953815

hgame{Do_y0u_KnOW_uNiC0d3?}

得到 unicode 转码得

3. 克苏鲁神话

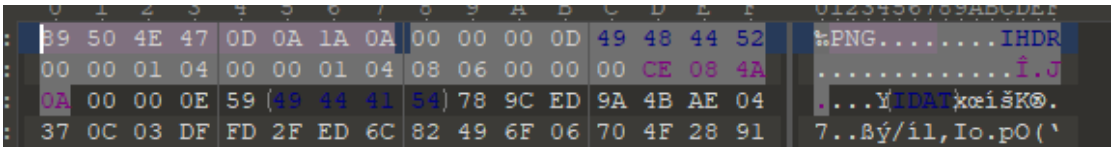
很明显的明文爆破，用 ARCHPR 明文攻击得到 doc 文件，句子是培根密码加密得到的，解密后得到 FLAGHIDDENANDOC，但不对，可能规则的不同，猜了一下改为 FLAGHIDDENINDOC 打开 doc，doc 基本就是隐藏文字了，ctrl+a 全选字体取消隐藏得到 flag

后留下了这份手稿，希望遗嘱执行人会用谨慎作

hgame{YOu_h@Ve_FOUnd_mY_S3cReT}↵

4. 签到题 ProPlus

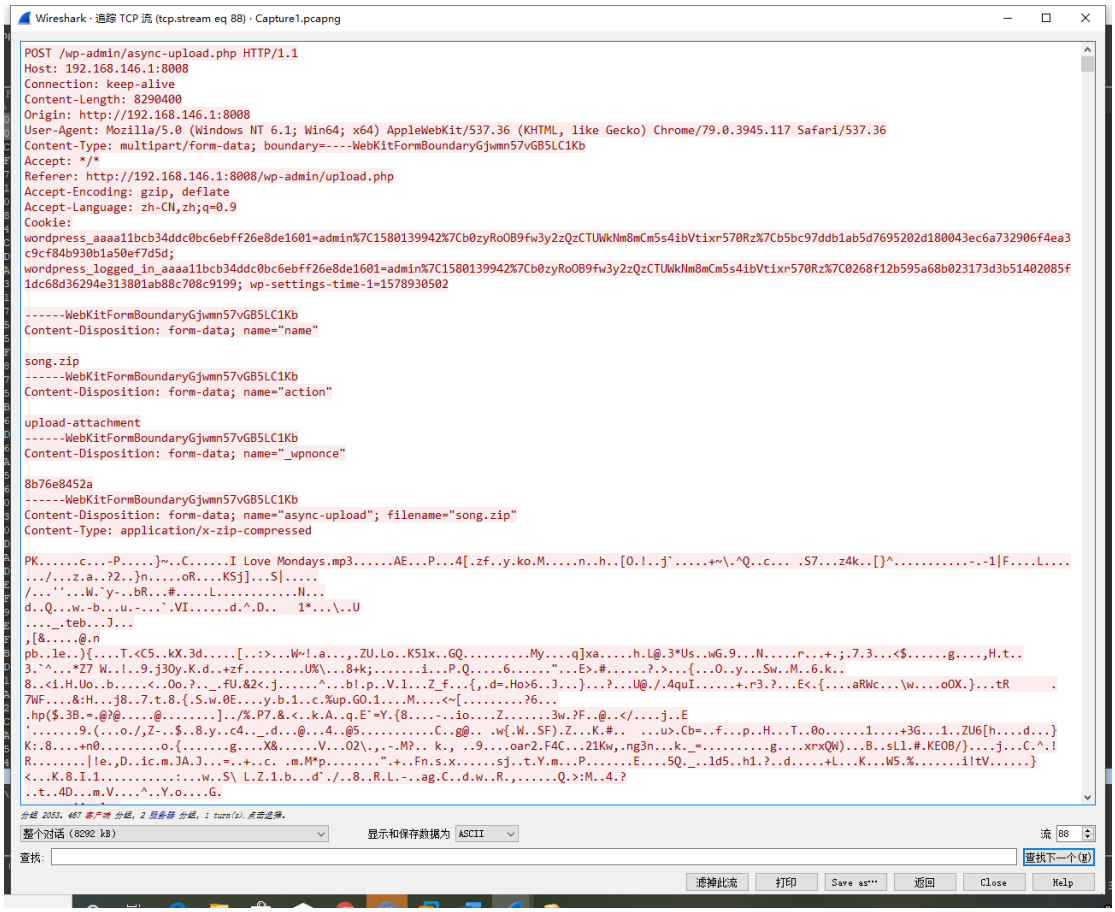
根据提示将大写密文进行三栏栅栏密码解密，再经过间隔为五的凯撒密码解密得到压缩包密码，得到 ook 密码，转换后得到 base32，转换后得到 base64，用 linux base64 -d 指令直接将 base64 解码后内容保存至 txt，使用 010editor 查看发现文件头是 png 格式文件头，



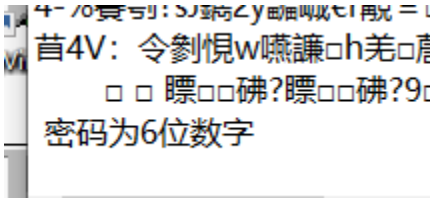
将后缀改为 png 得到二维码，扫码得到 flag

5. 每日推荐

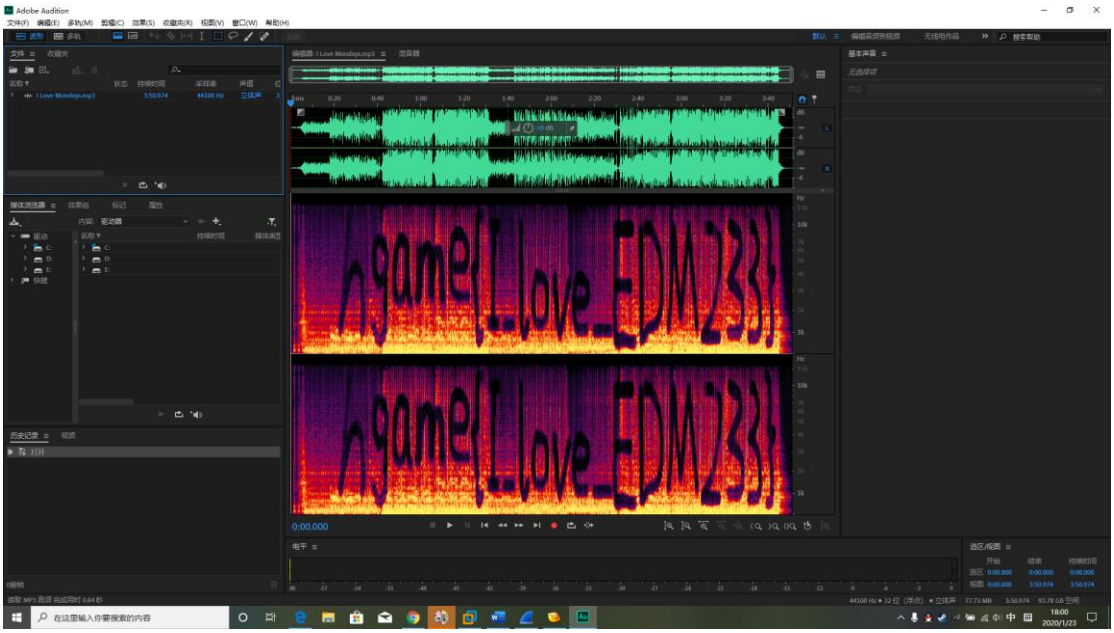
网易云？压缩包的味道，搜索 16 进制 50 4B 03 04，发现确实存在，追踪 tcp 流，



将原始数据保存为 zip 并出去压缩包外信息后打开发现需要密码，txt 查看发现提示



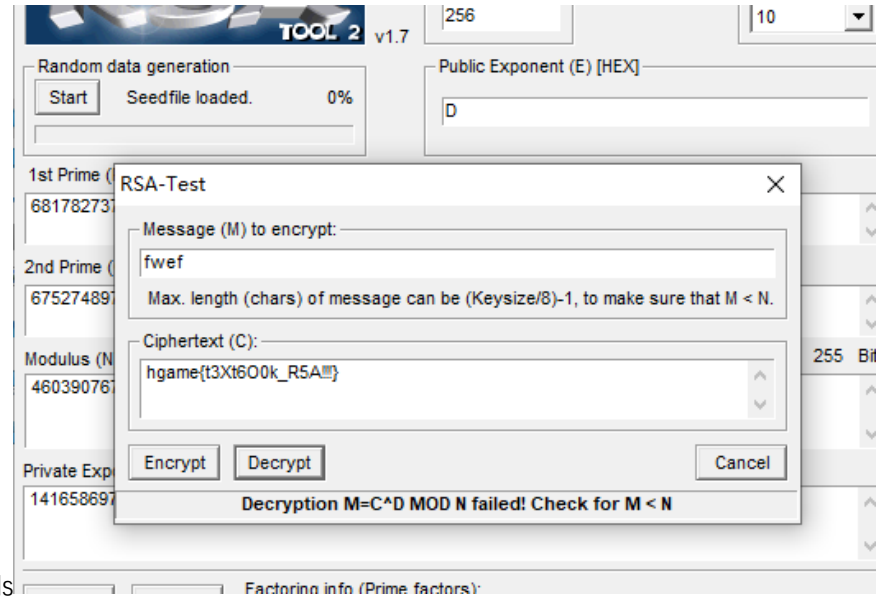
6 位数字密码直接爆破得到 mp3 文件，MP3stego 坏了先用 au 打开看看，



显示频谱得到 flag。

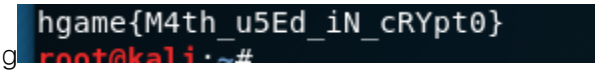
CRYPTO

1. InfantRSA



Rsatools

2. Affine

模运算加密，把'{'前的 hgame 代入算出 A=13,B=14，凑出一个逆元为 105，写个逆脚本得到 flag 

3. Reorder

每次重新连接端口的加密方式都不一样，最后得到的是 32 位的密文，可以选择输入 31 个 1 和 1 个 2，第一次 2 在最左侧，每次输入都把 2 向右移动一次，观察 2 在得到输出的位置，最后得到密文是按照 2 的规律排列得到 flag。