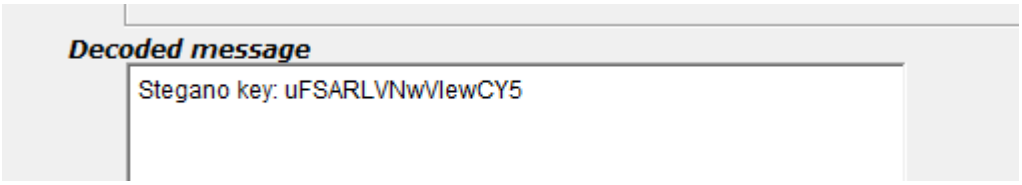
HGAME2020 WRITE UP

MISC

三重隐写

打开压缩包得到 3 个文件，Unlasting 封面图直接扫码得到“AES key: 1ZmmeaLL^Typbcg3”，You know LSB 使用 silenteye 得到



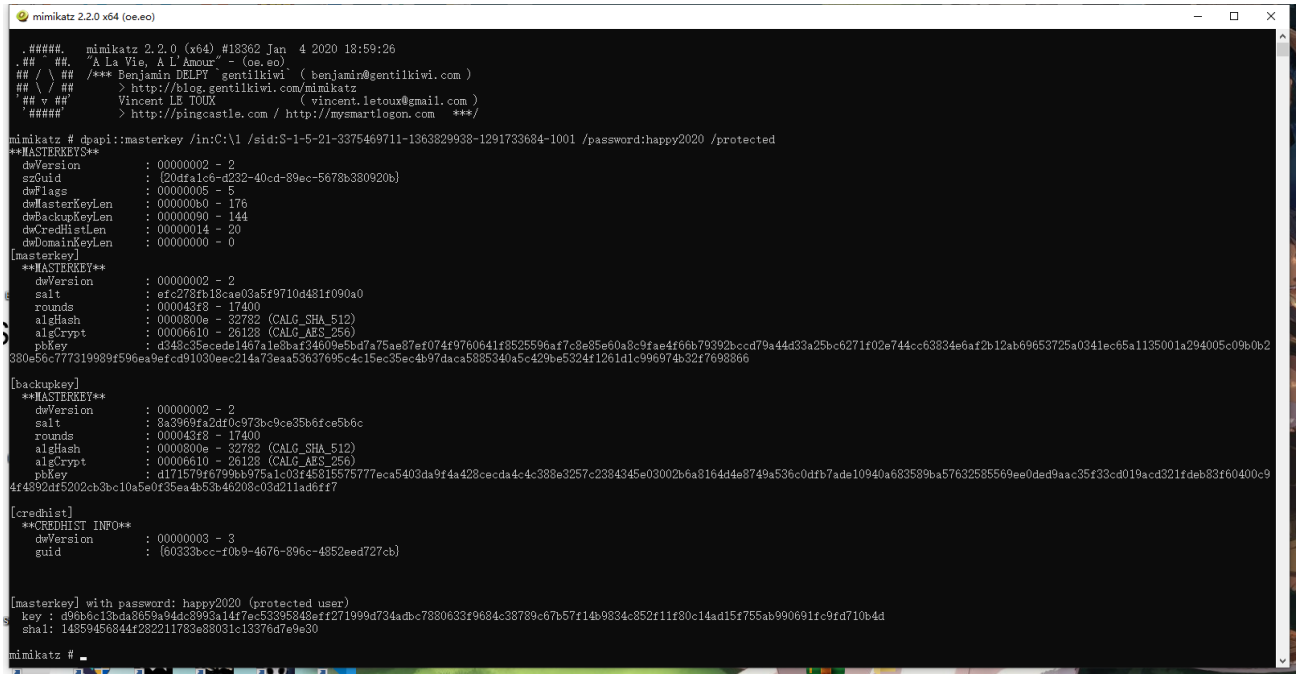
为最后一首歌的隐写密码，使用 MP3stego 得到压缩包密码 Zip Password: VvLvmGjpJ75GdJDP，解开压缩包得到文件用所给软件使用最初得到的 AES 密码解密得到 flag---hgame{i35k#zlewynLC0zfQur!*H9V$JiMVWmL}

日常

有两张看起来一样的图片，加上文字 blind 和 origin，应该是盲水印，用 blindwatermaster 脚本解得

，.ogg 文件用 binwalk 发现有压缩包，-e 指令取出，水印提示的 VeraCrypt 软件

打开得到三个文件，txt 是 mimikatz 的使用，查资料后感觉应该是使用 masterkey 解开 cookies，masterkey 在压缩包的 master key file 里，txt 的 NTLM 直接转换为明文密码 happy2020，逛了好久论坛终于看到关于离线用户 masterkey 但已知明文密码的 masterkey 获取方式，sid 通过 txt 已知，使用命令 mimikatz # dpapi::masterkey /in:C:\1 /sid:S-1-5-21-3375469711-1363829938-1291733684-1001 /password:happy2020 /protected 获得 masterkey，使用命令



dpapi::masterkey /in:C:\Cookies /masterkey:d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d /unprotect 得到 flag

CRYPTO

RSA?

Linux 直接打开 rsa 文件得到 c,e,q,n 值, e=2, 之前看到过 rabin 加密, 但 n=p*q+r 有点难，想了半天各种方法直到试下直接分解发现 n 分解不了。。。

$$m_p = c^{\frac{1}{4}(p+1)} \mod p$$

把 p 换成 n 写个脚本得到 flag

```
hgame{eaa5262c-4631-46ef-a97b-53277ab7e1d8}
```

ToyCipher_XorShift

感觉有点像 CBC 加密模式，BLOCKS 取块，pad 填充，f 为基本的异或位移加密，enc 调用了 f，encrypt 中最初 mid 为 iv，之后每次变为这次加密的块，（组织语言 ing。。。）解密只要写出反推的脚本就行了，对于 enc 加密只要反过来把 block 加密的顺序反过来就行了，对于 encrypt 先进行异或再 enc 加密，反过来先解密 enc 再异或就能得到

```
text += XOR(mid, dec(block))
mid = block
```

对于 f 的解密，因为位移后进行异或，解密再异或得到是位移位置的明文，也是用于下一块密文异或解密，所以要不断进行循环（好难组织语言），所以对于 f 解密函数为

```
def f(x, a, shr=True):
    x = x & MASK
    a = a % BITSLENGTH
    s = (1 << a) - 1
    if shr:
        s = s << (BITSLENGTH - a)
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & s) >> a
            s = s >> a
    else:
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & s) << a
            s = s << a
    return x & MASK
```

写脚本得 flag 为

```
'hgame{tHi$+4lgOr1thM_i5_3@sY-t0~b2EaK}
```