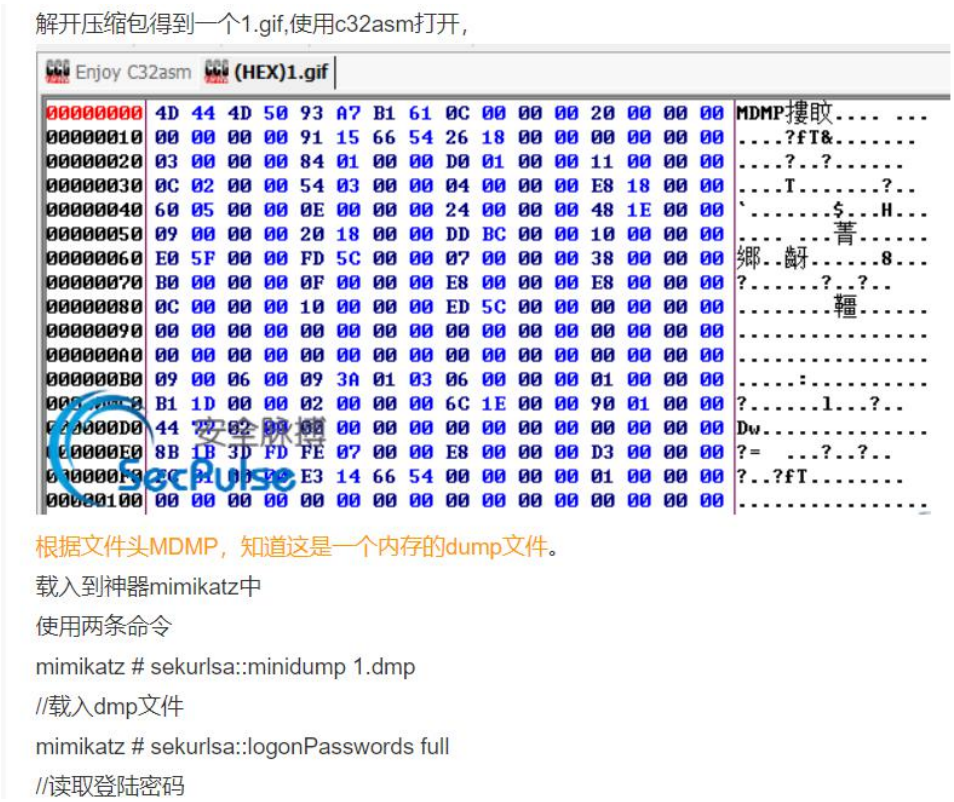
(MISC1)warmup

0x01

下载解压得到文件 1.gif 发现打不开 但是有 20 多 MB，这么大！
啥都没管先丢进 binwalk 看看，好多东西啊，无从下手。再用 foremost 分离提取一下，有两个文件夹 三张图片，捣鼓了一会发现没有什么东西……

0x02

用二进制文件形式打开，观察发现头是 mdmp，感觉有点东西，百度一下发现这是个什么 sql 产生的错误文件，昂不知道是什么，继续百度 CTF mdmp，发现有类似题目



再联系下题干说是要管理员的密码，那估计就是这样了……

0x03

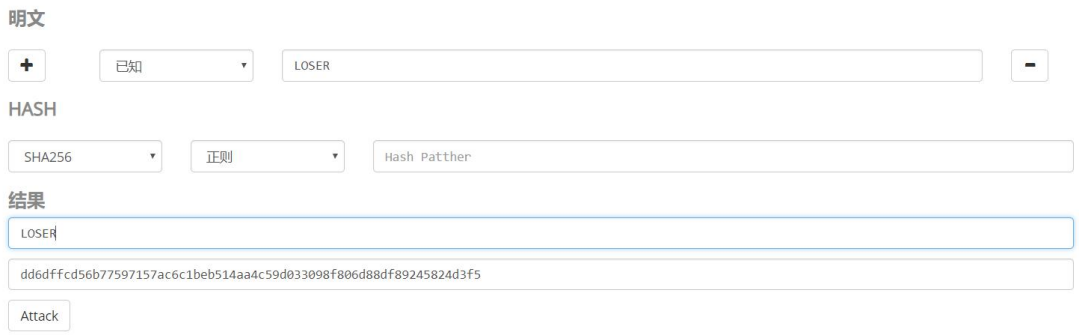
下载安装神器 mimikatz
接着按着样子输入命令
mimikatz # sekurlsa::minidump 1.dmp
mimikatz # sekurlsa::logonPasswords full

得到下面的画面，找到了 password：LOSER

```
Authentication Id : 0 ; 2353730 (00000000:0023ea42)
Session           : Interactive from 2
User Name         : Hgame
Domain            : xyf-PC
SID               : S-1-5-21-373264735-3061158248-1611926753-1003
        msv :
         [00000003] Primary
         * Username : Hgame
         * Domain   : xyf-PC
         * LM       : 758ff83c96bcac17aad3b435b51404ee
         * NTLM     : e527b386483119c5218d9bb836109739
         * SHA1     : ca17a8c02628f662f88499e48d1b3e9398bef1ff
        tspkg :
         * Username : Hgame
         * Domain   : xyf-PC
         * Password : LOSER
        wdigest :
         * Username : Hgame
         * Domain   : xyf-PC
         * Password : LOSER
```

按照题干要求，提交管理员密码的 sha256

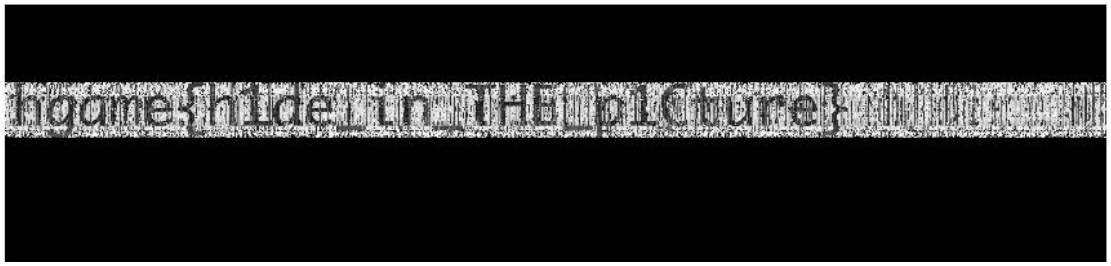
使用工具：https://www.wishingstarmoye.com/ctf/hashattack



提交：hgame{dd6dffcd56b77597157ac6c1beb514aa4c59d033098f806d88df89245824d3f5}

(MISC3)暗藏玄机

题目给了两张图片，正好这两天看了些 MISC 的东西，听说了一个叫盲水印的东西，用 stegsolve 打开发现其中一张有横线，符合盲水印的特点，下载工具 BlindWaterMark-master，win 下配置好所需的工具输入代码 python bwm.py decode 0.png 1.png result.png , result.png 为 输出的文件



(CYRPTO1)easy_rsa

刚刚接触 rsa,简单了解了一下 rsa

主要参数有 p,q,n,e,d,c,m

p,q 为两个较大的、互质的数

n=p*q

phi(n)是欧拉函数，phi（n）=（p-1）（q-1）

e 是随机一个 1<e<phi(n)的一个数，且与 phi(n)互素

(e,n)称为公钥

e*d=1 mod phi(n),

(d,n)称为私钥

c=pow(m,e,n)=m^e%n

m=pow(c,d,n)=c^d%n

0x01

题目给了 e1,e2,n,c1,c2,得知已知 n，e 的情况下，可以通过分解 n 得到 p，q

故而求得 d,无奈分解了半天无果，应该是思路错了……

0x02

百度了下 RSA 的主要攻击方法

https://blog.csdn.net/qq_38204481/article/details/83189041

https://blog.csdn.net/huanghelouzi/article/details/82943615

https://www.sohu.com/a/243246344_472906

第三个挺牛的

发现在已知两对公钥的情况下应当使用共模攻击

https://www.cnblogs.com/gwind/p/8013154.html

这是共模攻击的前提条件，这也是为啥最后我得到了个 51 位的数字，而题目则要求是 17 位数字！！！

gcd(e1,e2)=1 !!!

而题目中的 gcd(e1,e2)=3 !!!

当n不变的情况下，知道n,e1,e2,c1,c2 可以在不知道d1,d2的情况下，解出m。

首先假设，e1，e2互质

即

$$gcd(e1,e2)=1$$

此时则有

$$e1*s1+e2*s2 = 1$$

贴一下最初用的代码

```
import gmpy2
n=187115775425611431525771949607687004102790873190791598691365943
c1=982266932179633503937264933456488823103596770140636969749202660
c2=192244435800663432138663938566273988418431244693997622517410875
e1=209472
e2=15951
s=gmpy2.gcdext(e1,e2)
s1=s[1]
s2=s[2]
m=(pow(c1,s1,n)*pow(c2,s2,n))%n
print(m)
```

这里最后得到的是：

211655262573966881062823795220179644607412162371069

也就是那个 51 位数……

0x03

想到的是 51 和 17 正好差了三倍，而且正好 gcd(e1,e2)=3!!!

这三者之间是否有些联系？

c=pow(m,e,n)=m^e%n

三次方！！！

17 位数^3=51 位数

直接将得到的 m 开三次方根，得到的是 59594981651654664.0 数数正好 17 位数

于是直接提交 flag~ ,傻不拉几的,肯定报错啊,然后想到应该会有精度丢失吧。

再将得到的59594981651654664.0^3 回去,发现确实是这样，两个数据差距不大

```
211655262573966881062823795220179644607412162371069
59594981651654664.0
211655262573965549227134522321362153629073490706944
```

之后想到 9^3=..9,末尾改 669

```
211655262573966881062823795220179644607412162371069
59594981651654669
211655262573965602500562093237207582301234059100309
```

改 679

```
211655262573966881062823795220179644607412162371069
59594981651654679
211655262573965709047417235068925257387298440488839
```

改 689,发现末尾两个已经相等了

```
211655262573966881062823795220179644607412162371069
59594981651654689
211655262573965815594272376900678689462353814684769
```

最后改 789，出来了

```
m = pow(c1,s1,n)*pow(c2,s2
print(m)
z=pow(m,float(1)/float(3))
print(z)
n=pow(59594981651654789,3)
print(n)
```

```
wff1136424713@ubuntu:~$ python '/home/wff1136424713/
p/new 1.py'
3
-1195
15693
211655262573966881062823795220179644607412162371069
59594981651654664.0
211655262573966881062823795220179644607412162371069
```

提交 flag： hgame{59594981651654789}