HGAME WRITEUP WEEK4——FzWjScJ

MISC

0x01 Warmup

解压zip是一张gif图，然而并打不开……在多次烦出题人加上自己瞎倒腾之后(binwalk)知道了这是一个改了后缀的内存文件~~（出题人真任性）~~,然后得到了一个内存取证神器`mimikatz`，在短暂的学习文档后用了几个指令`log(登陆windows）`、`privilege::debug(获得权限）`、`sekurlsa::minidump 1.gif(模拟使用内存)`、`sekurlsa::logonPasswords(抓取密码)`,然后得到密码：

```
tspkg :
  * Username : xyf
  * Domain   : xyf-PC
  * Password : LOSER
```

再找一个加密网站加密成sha256就行，得到flag：`hgame{dd6dffcd56b77597157ac6c1beb514aa4c59d033098f806d88df89245824d3f5}`(随便吐槽一句，win10真厉害）

0x02 Clodown

解压后是2个G的mp4（大写的震惊，还以为老司机开车了），但是依旧打不开，吸取教训的我去binwalk了一波……结果跑了不知道多长时间易得又是一道内存取证题（日语草），在kali里好像有一个取证工具叫volatility,然后用`volatility -f memory.mp4 imageinfo`找到适用机型……但是并没找到，后面py出题人得到正确架构——Win7SP1x64（扫出来都是win8win10=。=）

然后开始第二步，查看SAM和System的注册表地址，输入指令`volatility -f memory.mp4 --profile=Win7SP1x64 hivelist`，找到两个地址`0xfffff8a003652010`和`0xfffff8a000024010`

```
root@kali:~/CTF/neicunquzheng# volatility -f memory.mp4 --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a003652010 0x00000000260a9010 \SystemRoot\System32\Config\SAM
0xfffff8a0062bd010 0x000000002143e010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00000f010 0x000000002bfa9010 [no name]
0xfffff8a000024010 0x000000002bf34010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000652d0 0x000000002c3772d0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0007e1010 0x0000000027e59010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0007f8280 0x000000002779dd280 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001041350 0x000000001de7c350 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001087010 0x000000001071a010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a0017dd010 0x000000000bd36010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a002054010 0x000000006509d010 \??\C:\Users\xyf\ntuser.dat
0xfffff8a0020be010 0x00000000078b6010 \??\C:\Users\xyf\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a00364f010 0x0000000025e26010 \SystemRoot\System32\Config\DEFAULT
```

进行查找用户密码的指令`volatility -f memory.mp4 --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a003652010`得到用户密码的哈希值：0bb8d932bbfee69fbc874214f39b1b67

```
root@kali:~/CTF/neicunquzheng# volatility -f memory.mp4 --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a003652010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
xyf:1001:aad3b435b51404eeaad3b435b51404ee:0bb8d932bbfee69fbc874214f39b1b67:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:291e1d2ec16a080d9132d9b71af271cc:::
Hgame:1003:aad3b435b51404eeaad3b435b51404ee:e527b386483119c5218d9bb836109739:::
```

去网上找了个hash解密网站（并不会用hashcat=。=）解的密码：admin123456，再去用sha256加密一波得到flag：`hgame{ac0e7d037817094e9e0b4441f9bae3209d67b02fa484917065f71b16109a1a78}`

0x03暗藏玄机

ZIP解压后两个图片，百度了一下得知应该是盲水印然后去下了个工具试了试，得到flag：`hgame{h1de_in_THE_p1Cture}`