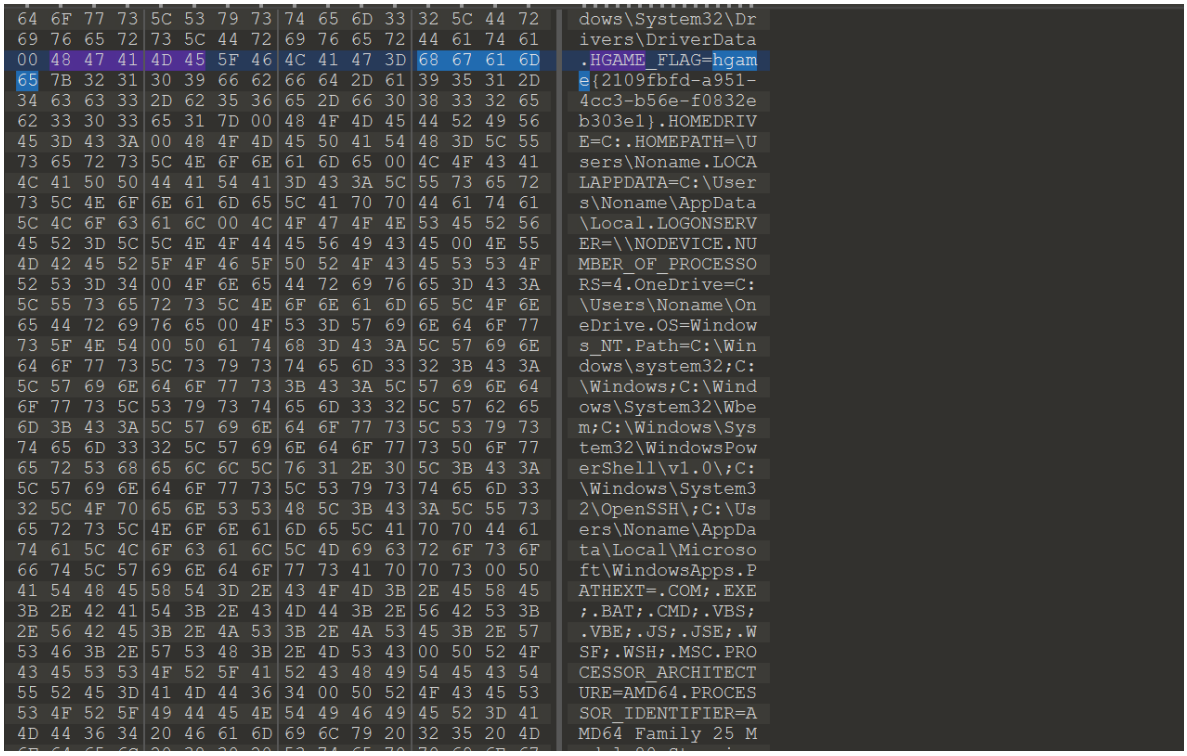
HGAME 2023 Week3 writeup by 1dn

Misc

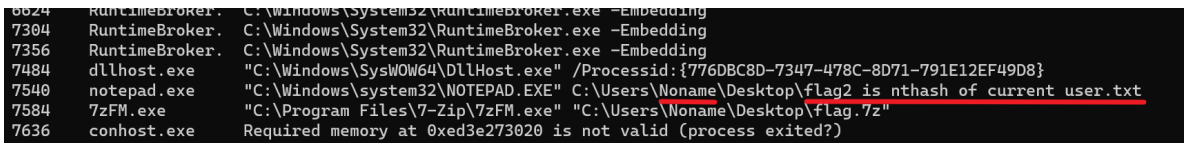
1.ezWin - variables

010里直接搜hgame



2.ezWin - auth

用volatility3的cmdline命令，发现flag相关信息



所以flag即为Noname的nt hash

再使用hashdump命令去查看账户信息，拿到nthash

```
User     rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount  503     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount      504     aad3b435b51404eeaad3b435b51404ee        c4b2cf9cac4752fc9b030b8ebc6faac3
Noname  1000    aad3b435b51404eeaad3b435b51404ee        84b0d9c9f830238933e7131d60ac6436
```

3.ezWin - 7zip

找一下跟flag相关的文件

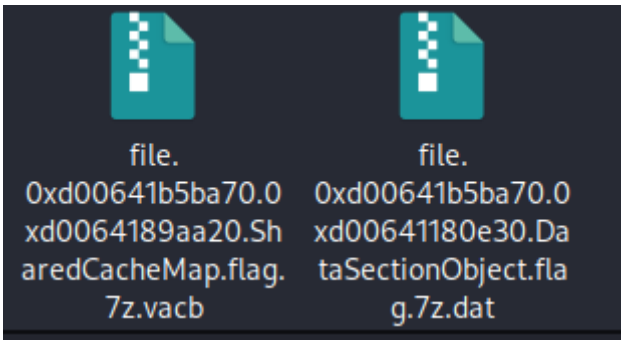
```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f /home/kali/Desktop/win10_22h2_19045.2486.vmem filescan | grep flag
0×d0064181c950.0\Users\Noname\Desktop\flag.7z    216
0×d00641b5ba70  \Users\Noname\Desktop\flag.7z    216
```

提取文件内容

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f /home/kali/Desktop/win10_22h2_19045.2486.vmem dumpfiles --virtaddr 0×d00641b5ba70
Volatility 3 Framework 2.4.1
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0×d00641b5ba70  flag.7z Error dumping file
SharedCacheMap  0×d00641b5ba70  flag.7z file.0×d00641b5ba70.0×d0064189aa20.SharedCacheMap.flag.7z.vacb
```

得到两个文件



将第一个文件后面的.vacb（或者第二个文件后面的.dat）删了，是个7z压缩包，压缩包密码是上一题nthash解密的结果，flag就在txt文件里

```
.. (上级目录)                                    文件夹
crack_nt_hash_for_7z_pwd.txt *          1 KB    1 KB  文本文档          2023-01-31 10:58
```

Crypto

1.LLLCG

output.txt的40个数里任意相邻两数中的较大数整除较小数的值即为a

```
10896510524738352828273081283110658285613966633649112409729597889095153066168639
80465990986336276384903707375227394223034256042622812751981085694555292380388664
57344842006422913342167824060644151888704413267011559130185793503076927127159936
75813772474243280626352888321213313718894912395388422448776832449873890579411993
73965//11376601256353152185503962572833792711262816547071400246285651162390432276547568621520807045539152955978339181948979612443582845433254521961199765280440194107715339964604936288497399764098445787826483305280141402883839578001618588242808179325708607533560698556547329365760234559423915099931743881780774751272558991275158030005
```

然后转回字符串

```
b'hgame{W0w_you_know_the_hidden_number_problem}'
```