n0t3d password. Задача на форензику.

Официальное прохождение от автора задачи (И. А. Герасимов - laf3r.github.io).

Описание

Мы с моим знакомым поспорили, что я смогу достать его пароль из заметок. Я сделал снимок оперативной памяти его компьютера, но я не знаю, что мне делать дальше.

Прохождение

На входе у нас снимок оперативной памяти в .raw формате Для анализа снимка, я буду использовать программу Volatility v2. Для начала нам нужно определить профиль снимка. Определим его при помощи параметра **imageinfo**

```
remnux@remnux:~$ vol.py -f task1.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
INFO    : volatility.debug    : Determining profile based on KDBG
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel A
                     AS Layer2 : FileAddressSpace (/home/remnux/ta
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029fb130L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029fd000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-08-08 13:22:18 UTC+0000
     Image local date and time : 2022-08-08 15:22:18 +0200
remnux@remnux:~$
```

Я буду использовать профиль **Win7SP1x64**. Так как пароль хранится в заметках, то нужно искать программу для заметок. Мне

потребуется просмотреть список процессов и найти программу, куда пользователь может записывать заметки. Для того, чтобы просмотреть список процессов, я использую команду.

```
vol.py -f task1.raw --profile Win7SP1x64 pstree
```

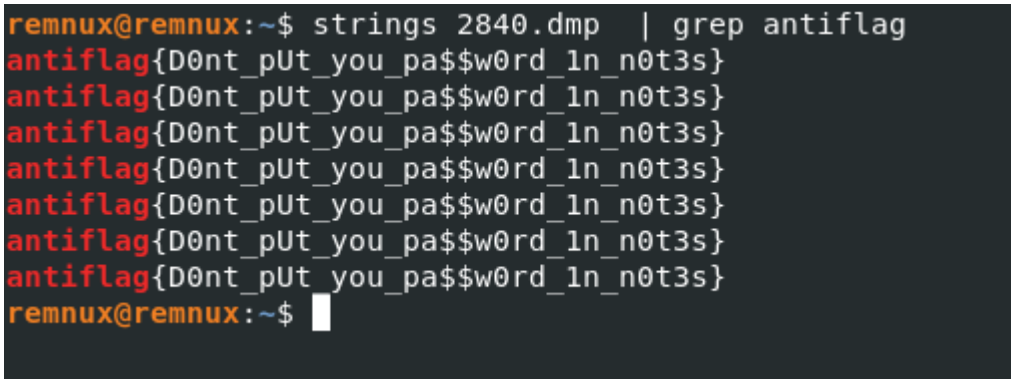
```
.... 0xfffffa80019079b0:dllhost.exe                  2620    628      6 13...2 2022-08-08 13:22:20 UTC+0000
.... 0xfffffa80018c7480:dllhost.exe                  2284    628      0 ------ 2022-08-08 13:22:12 UTC+0000
.... 0xfffffa8000e2e5b0:WmiPrvSE.exe                 2736    628      7    165 2022-08-08 13:21:14 UTC+0000
.... 0xfffffa8001d51060:dllhost.exe                  2500    628      0 ------ 2022-08-08 13:22:13 UTC+0000
... 0xfffffa8001f02060:taskhost.exe                  1784    508     10    170 2022-08-08 13:18:23 UTC+0000
 0xfffffa8002b19510:svchost.exe                       932    508     22    450 2022-08-08 13:18:20 UTC+0000
WARNING : volatility.debug    : PID 932 PPID 508 has already been seen
 0xfffffa8002773860:svchost.exe                      1000    508     43   1058 2022-08-08 13:18:20 UTC+0000
WARNING : volatility.debug    : PID 1000 PPID 508 has already been seen
 0xfffffa8001f4a750:svchost.exe                      1312    508     18    262 2022-08-08 13:18:21 UTC+0000
WARNING : volatility.debug    : PID 1312 PPID 508 has already been seen
 0xfffffa80027579b0:svchost.exe                       752    508      7    283 2022-08-08 13:18:19 UTC+0000
WARNING : volatility.debug    : PID 752 PPID 508 has already been seen
 0xfffffa8002a79770:svchost.exe                       628    508     13    367 2022-08-08 14:18:17 UTC+0000
WARNING : volatility.debug    : PID 628 PPID 508 has already been seen
 0xfffffa8001f02060:taskhost.exe                     1784    508     10    170 2022-08-08 13:18:23 UTC+0000
WARNING : volatility.debug    : PID 1784 PPID 508 has already been seen
 0xfffffa8000c445c0:System                               4      0     87    422 2022-08-08 14:18:16 UTC+0000
. 0xfffffa8001d4f2e0:smss.exe                          276      4      2     29 2022-08-08 14:18:16 UTC+0000
 0xfffffa8001e61060:csrss.exe                          416    396     10    206 2022-08-08 14:18:17 UTC+0000
. 0xfffffa8001c6ab00:conhost.exe                      2584    416      2     52 2022-08-08 13:22:14 UTC+0000
 0xfffffa8002a06060:winlogon.exe                       472    396      6    121 2022-08-08 14:18:17 UTC+0000
 0xfffffa8002e728c0:explorer.exe                      1328    908     27    744 2022-08-08 13:20:23 UTC+0000
. 0xfffffa80014f2850:notepad++.exe                    2840   1328     14    283 2022-08-08 13:21:58 UTC+0000
. 0xfffffa800181db00:DumpIt.exe                       2940   1328      2     46 2022-08-08 13:22:13 UTC+0000
. 0xfffffa8000e59b00:VBoxTray.exe                     1444   1328     16    147 2022-08-08 13:20:24 UTC+0000
remnux@remnux:~$
```

Почти в самом низу я замечаю notepad++. Я думаю, что там может хранится флаг. Флаг записан в программу, но похоже не сохранён в виде файла. Поэтому сдампить файл с флагом не получится, но он есть в программе. Поэтому можно сделать снимок памяти процесса. К параметру **memdump** нужно указать место, куда будет выгружаться снимок памяти процесса, и pid(номер процесса).

```
remnux@remnux:~$ vol.py -f task1.raw --profile Win7SP1x64 memdump --dump-dir ./ --pid 2840
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12:
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
************************************************************************
Writing notepad++.exe [  2840] to 2840.dmp
remnux@remnux:~$
```

```
vol.py -f task1.raw --profile Win7SP1x64 memdump --dump-dir ./ --pid 2840
```

Теперь поищим в снимке читаемые символы с форматом флага antiflag



`strings 2148.dmp | grep antiflag`

Флаг

`antiflag{D0nt_pUt_you_pa$$w0rd_1n_n0t3s}`