MemLabs - Lab4

3 minutos de leitura

> ## *Descrição do desafio*
>
> *Meu sistema foi comprometido recentemente. O Hacker roubou muitas informações, mas também apagou um arquivo meu muito importante. Não faço ideia de como recuperá-lo. A única evidência que temos, neste momento, é este despejo de memória. Por favor me ajude.*
>
> ***Nota** : Este desafio é composto por apenas 1 bandeira.*
>
> *O formato do sinalizador para este laboratório é:* ***inctf{s0me_l33t_Str1ng}***
>
> ***Arquivo de desafio** : MemLabs_Lab4 (https://github.com/joathamp/maratona_forense)*

Primeiro precisamos identificar o sistema operacional da imagem da memória.

```
$ volatility -f MemoryDump_Lab4.raw imageinfo
```

```
night-wolf@ubuntu:~/MemLabs/Lab4$ volatility -f MemoryDump_Lab4.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/night-wolf/MemLabs/Lab4/MemoryDump_Lab4.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027f60a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027f7d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-06-29 07:30:00 UTC+0000
     Image local date and time : 2019-06-29 13:00:00 +0530
```

A próxima coisa é verificar os processos em execução.

```
$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 pslist
```

```
night-wolf@ubuntu:~/MemLabs/Lab4$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     79      509 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa80014af950 smss.exe                256      4      3       32 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa8001c57b30 csrss.exe               328    320     11      385      0      0 2019-06-29 07:28:14 UTC+0000
0xfffffa8000ca8960 csrss.exe               376    368      7      200      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c6f760 wininit.exe             384    320      3       75      0      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c751f0 winlogon.exe            412    368      6      119      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001bc1b30 services.exe            472    384     13      193      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cb5940 lsass.exe               480    384      8      582      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cc1b30 lsm.exe                 488    384     12      187      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001d02b30 svchost.exe             580    472     11      358      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d30b30 VBoxService.ex          640    472     14      137      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d43a70 svchost.exe             708    472      7      260      0      0 2019-06-29 07:28:22 UTC+0000
0xfffffa8001dacb30 svchost.exe             804    472     19      393      0      0 2019-06-29 07:28:23 UTC+0000
0xfffffa8001db9b30 svchost.exe             840    472     21      431      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001dc6850 svchost.exe             864    472     37      917      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001df1060 audiodg.exe             952    804      7      131      0      0 2019-06-29 07:28:26 UTC+0000
0xfffffa8001e1b890 svchost.exe             220    472     16      323      0      0 2019-06-29 07:28:27 UTC+0000
0xfffffa8001e45630 svchost.exe             484    472     18      376      0      0 2019-06-29 07:28:29 UTC+0000
0xfffffa8001eaab30 spoolsv.exe            1132    472     15      286      0      0 2019-06-29 07:28:32 UTC+0000
0xfffffa8001ed7b30 svchost.exe            1176    472     21      307      0      0 2019-06-29 07:28:33 UTC+0000
0xfffffa8001f452e0 svchost.exe            1276    472     14      220      0      0 2019-06-29 07:28:34 UTC+0000
0xfffffa8001f81b30 taskhost.exe           1804    472     10      161      1      0 2019-06-29 07:28:42 UTC+0000
0xfffffa8001ff9630 taskeng.exe            1824    864      6       82      0      0 2019-06-29 07:28:42 UTC+0000
0xfffffa80020bbb30 dwm.exe                1908    840      5       77      1      0 2019-06-29 07:28:43 UTC+0000
0xfffffa80020f7b30 explorer.exe           1944   1872     37      854      1      0 2019-06-29 07:28:44 UTC+0000
0xfffffa80021abab0 VBoxTray.exe           1592   1944     13      141      1      0 2019-06-29 07:28:53 UTC+0000
0xfffffa8002201ab0 SearchIndexer.         1068    472     13      710      0      0 2019-06-29 07:28:58 UTC+0000
0xfffffa800226e910 SearchProtocol         1696   1068      7      225      1      0 2019-06-29 07:29:02 UTC+0000
0xfffffa8002279890 SearchFilterHo         1688   1068      5       78      0      0 2019-06-29 07:29:02 UTC+0000
0xfffffa8002292b30 dllhost.exe            2076    580     13      260      1      0 2019-06-29 07:29:02 UTC+0000
0xfffffa80022f0610 GoogleCrashHan         2272   2008      7       99      0      1 2019-06-29 07:29:08 UTC+0000
0xfffffa80022f6b30 GoogleCrashHan         2284   2008      7       93      0      0 2019-06-29 07:29:08 UTC+0000
0xfffffa80020a4420 DumpIt.exe             2624   1944      3       45      1      1 2019-06-29 07:29:25 UTC+0000
0xfffffa8002320350 conhost.exe            2636    376      3       50      1      0 2019-06-29 07:29:25 UTC+0000
0xfffffa8001cac460 csrss.exe              2700   2692      7      164      2      0 2019-06-29 07:29:30 UTC+0000
0xfffffa8002330060 winlogon.exe           2728   2692      6      121      2      0 2019-06-29 07:29:30 UTC+0000
0xfffffa8000e54b30 taskhost.exe           2976    472      9      160      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000e62b30 dwm.exe                3000    840      5       76      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000eaeb30 explorer.exe           3012   2992     28      677      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000eeeb30 VBoxTray.exe           2384   3012     14      144      2      0 2019-06-29 07:29:37 UTC+0000
0xfffffa8000f18b30 StikyNot.exe           2432   3012     10      137      2      0 2019-06-29 07:29:37 UTC+0000
```

O único processo interessante aqui é `StikyNot.exe` (isso é uma toca de coelho, nada importante ali).

Olhando para a descrição do desafio, ela diz algo sobre arquivos e um arquivo excluído. Assim, podemos usar `filescan` para procurar arquivos interessantes na memória, mas, para variar, usarei o `iehistory` plugin.

> *`iehistory` plugin recupera fragmentos de arquivos de cache index.dat de histórico do IE. Ele pode encontrar links básicos acessados (via FTP ou HTTP), links redirecionados (–REDR) e entradas excluídas (–LEAK). Aplica-se a qualquer processo que carregue e use a biblioteca wininet.dll, não apenas o Internet Explorer. Normalmente, isso inclui o Windows Explorer e até amostras de malware.*

para que possamos usá-lo para visualizar o histórico de arquivos e diretórios visitados pelo Windows Explorer.

```
$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 iehistory
..........
Process: 3012 explorer.exe
Cache type "URL " at 0x42f5000
Record length: 0x100
Location: :2019062920190630: SlimShady@file:///C:/Users/SlimShady/Desktop/Important.txt
Last modified: 2019-06-29 12:59:43 UTC+0000
Last accessed: 2019-06-29 07:29:43 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0
```

O que temos aqui, um arquivo de texto que parece importante!!!

Agora vamos procurar este arquivo na memória para descartá-lo.

```
$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 filescan | grep Important.txt
Volatility Foundation Volatility Framework 2.6.1
0x000000003fc398d0     16      0 R--rw-
\Device\HarddiskVolume2\Users\SlimShady\Desktop\Important.txt

$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 dumpfiles -Q 0x000000003fc398d0 -D
lab4_output/
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fc398d0   None   \Device\HarddiskVolume2\Users\SlimShady\Desktop\Important.txt
```

Infelizmente, `dumpfiles` não foi possível despejar o arquivo de texto (ele foi deletado pelo hacker).

Precisamos saber um pouco sobre a tabela MFT para resolver esse desafio.

- *O sistema de arquivos NTFS contém um arquivo chamado tabela de arquivos mestre ou MFT. Há pelo menos uma entrada na MFT para cada arquivo em um volume do sistema de arquivos NTFS. Todas as informações sobre um arquivo, incluindo seu nome, tamanho, carimbos de data e hora, permissões e conteúdo de dados, são armazenadas nas entradas da MFT ou no espaço fora da MFT descrito pelas entradas da MFT.*

- *À medida que os arquivos são adicionados a um volume do sistema de arquivos NTFS, mais entradas são adicionadas à MFT e ela aumenta de tamanho. Quando os arquivos são excluídos de um volume do sistema de arquivos NTFS, suas entradas MFT são marcadas como gratuitas e podem ser reutilizadas. No entanto, o espaço em disco que foi alocado para essas entradas não é realocado e o tamanho da MFT não diminui.*

- *Um arquivo cujo tamanho seja menor ou igual a 1024 bytes será armazenado diretamente na tabela MFT (denominado arquivo "residente"), caso ultrapasse 1024 bytes a tabela conterá apenas a informação de sua localização (denominado "não residente" Arquivo).*

Então, vamos procurar `Important.txt` na tabela MFT.

```
$ volatility -f MemoryDump_Lab4.raw --profile Win7SP1x64 mftparser > mft.txt
```

```
164435 **************************************************
164436 **************************************************
164437 MFT entry found at offset 0x3bd8ac00
164438 Attribute: In Use & File
164439 Record Number: 60583
164440 Link count: 2
164441
164442
164443 $STANDARD_INFORMATION
164444 Creation                    Modified                    MFT Altered                 Access Date                 Type
164445 ------------------------- ------------------------- ------------------------- ------------------------- ----
164446 2019-06-27 13:14:13 UTC+0000 2019-06-27 13:26:12 UTC+0000   2019-06-27 13:26:12 UTC+0000   2019-06-27 13:14:13 UTC+0000   Archive
164447
164448 $FILE_NAME
164449 Creation                    Modified                    MFT Altered                 Access Date                 Name/Path
164450 ------------------------- ------------------------- ------------------------- ------------------------- ---------
164451 2019-06-27 13:14:13 UTC+0000 2019-06-27 13:14:13 UTC+0000   2019-06-27 13:14:13 UTC+0000   2019-06-27 13:14:13 UTC+0000   Users\SlimShady\Desktop\IMPORT~1.TXT
164452
164453 $FILE_NAME
164454 Creation                    Modified                    MFT Altered                 Access Date                 Name/Path
164455 ------------------------- ------------------------- ------------------------- ------------------------- ---------
164456 2019-06-27 13:14:13 UTC+0000 2019-06-27 13:14:13 UTC+0000   2019-06-27 13:14:13 UTC+0000   2019-06-27 13:14:13 UTC+0000   Users\SlimShady\Desktop\Important.txt
164457
164458 $OBJECT_ID
164459 Object ID: 7726a550-d498-e911-9cc1-0800275e72bc
164460 Birth Volume ID: 80000000-b800-0000-0000-180000000100
164461 Birth Object ID: 99000000-1800-0000-690d-0a0d0a0d0a6e
164462 Birth Domain ID: 0d0a0d0a-0d0a-6374-0d0a-0d0a0d0a0d0a
164463
164464 $DATA
164465 0000000000: 69 0d 0a 0d 0a 0d 0a 6e 0d 0a 0d 0a 0d 0a 63 74  i......n......ct
164466 0000000010: 0d 0a 0d 0a 0d 0a 0d 0a 66 7b 31 0d 0a 0d 0a 0d  ........f{1.....
164467 0000000020: 0a 5f 69 73 0d 0a 0d 0a 0d 0a 5f 6e 30 74 0d 0a  ._is......_n0t..
164468 0000000030: 0d 0a 0d 0a 0d 0a 5f 45 51 75 34 6c 0d 0a 0d 0a  ......_EQu4l....
164469 0000000040: 0d 0a 0d 0a 5f 37 6f 5f 32 5f 62 55 74 0d 0a 0d  ...._7o_2_bUt...
164470 0000000050: 0a 0d 0a 0d 0a 0d 0a 0d 0a 5f 74 68 31 73  ..........._th1s
164471 0000000060: 5f 64 30 73 33 6e 74 0d 0a 0d 0a 0d 0a 0d 0a 5f  _d0s3nt........_
164472 0000000070: 6d 34 6b 65 0d 0a 0d 0a 0d 0a 5f 73 33 6e 0d 0a  m4ke......_s3n..
164473 0000000080: 0d 0a 0d 0a 0d 0a 73 33 7d 0d 0a 0d 0a 47 6f 6f  ......s3}....Goo
164474 0000000090: 64 20 77 6f 72 6b 20 3a 50                      d.work.:P
164475
```

E aqui está, os caracteres da bandeira estão espalhados pelo arquivo, técnica anti-strings :)

> ***Bandeira: inctf{1_is_n0t_EQu4l_7o_2_bUt_th1s_d0s3nt_m4ke_s3ns3}***