CTF 内存取证

01

工具介绍

- volatility
- foremost
- binwalk
- dumpit

volatility

volatility 框架是一个完全开源的工具集合，在GNU通用公共许可证下以Python实现，用于从存储器（RAM）样本中提取数字信息。提取技术的执行完全独立于正在调查的系统，但提供了进入系统运行时状态的可见性。该框架旨在向人们介绍与提取数字信息相关的技术和复杂性，其支持的操作系统也非常广泛，同时支持windows，linux，Mac OSX，甚至也支持 Android 手机使用ARM处理器的取证，是目前最受欢迎的取证工具之一

常见的可以分析的后缀有： .raw、.vmem、.img、. dmg

foremost

foremost是一个控制台程序，用于根据页眉，页脚和内部数据结构恢复文件。这些内置类型查看给定文件格式的数据结构，从而实现更可靠，更快速的恢复。

在数字取证中和CTF中常用来恢复、分离文件。

它默认支持19种类型文件(jpg, gif, png, bmp, avi, exe, mpg, mp4, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, html, cpp 等文件)的扫描识别恢复，还可以通过(通过配置它的配置文件foremost.conf)增加新的支持类型。

binwalk

Binwalk是用于搜索给定二进制镜像文件以获取嵌入的文件和代码的工具。

具体来说,它被设计用于识别嵌入固件镜像内的文件和代码。

Binwalk使用libmagic库,因此它与Unix文件实用程序创建的魔数签名兼容。

Binwalk还包括一个自定义魔数签名文件,其中包含常见的诸如压缩/存档文件,固件头,Linux内核,引导加载程序,文件系统等的固件映像中常见文件的改进魔数签名。

dumpit

dumpit是一款绿色免安装的Windows内存镜像取证工具。利用它可以轻松地将一个系统的完整内存镜像dump下来，并用于后续的调查取证工作。

使用dumpit获取的内存文件可以使用volatility进行分析，ctf中遇到的部分题目便是使用dumpit制作的文件。

volatility安装

1、安装

在老版的kali linux中可以直接使用apt-get install volatility进行安装或已集成，此安装是快捷安装，如果想在其他linux版本、Windows或mac中安装可以直接下载源码，执行python setup.py install或执行python vol.py直接使用，下载方式如下：

git clone https://github.com/volatilityfoundation/volatility.git

volatility安装

2、依赖

如果只是使用volatility本体的话，就不需要安装依赖，如果还需要使用某些插件，就需要安装依赖，安装方式如下：

distorm3：一个很厉害的反编译库

安装方式：pip install distorm3

yara: 恶意软件分类工具

安装方式：pip install yara

pycrypto: 加密工具集

安装方式： pip install pycrypto

volatility安装

PIL：图片处理库

安装方式：pip install pillow

openpyxl: 读写excel文件

安装方式：pip install openpyxl

ujson: json解析

安装方式： pip install ujson

02

volatility的基本使用

--info

这个命令可以用来查看volatility已经添加的profile和插件信息

volatility --info

```
root@kali:~/Desktop/suspicion# volatility --info
Volatility Foundation Volatility Framework 2.6


Profiles
--------
VistaSP0x64            - A Profile for Windows Vista SP0 x64
VistaSP0x86            - A Profile for Windows Vista SP0 x86
VistaSP1x64            - A Profile for Windows Vista SP1 x64
VistaSP1x86            - A Profile for Windows Vista SP1 x86
VistaSP2x64            - A Profile for Windows Vista SP2 x64
VistaSP2x86            - A Profile for Windows Vista SP2 x86
Win10x64               - A Profile for Windows 10 x64
Win10x64_10586         - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393         - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x86               - A Profile for Windows 10 x86
Win10x86_10586         - A Profile for Windows 10 x86 (10.0.10586.420 / 2016-05-28)
Win10x86_14393         - A Profile for Windows 10 x86 (10.0.14393.0 / 2016-07-16)
Win2003SP0x86          - A Profile for Windows 2003 SP0 x86
Win2003SP1x64          - A Profile for Windows 2003 SP1 x64
Win2003SP1x86          - A Profile for Windows 2003 SP1 x86
Win2003SP2x64          - A Profile for Windows 2003 SP2 x64
Win2003SP2x86          - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64        - A Profile for Windows 2008 R2 SP0 x64
Win2008R2SP1x64        - A Profile for Windows 2008 R2 SP1 x64
Win2008R2SP1x64_23418  - A Profile for Windows 2008 R2 SP1 x64 (6.1.7601.23418 / 2016-04-09)
Win2008SP1x64          - A Profile for Windows 2008 SP1 x64
Win2008SP1x86          - A Profile for Windows 2008 SP1 x86
Win2008SP2x64          - A Profile for Windows 2008 SP2 x64
Win2008SP2x86          - A Profile for Windows 2008 SP2 x86
Win2012R2x64           - A Profile for Windows Server 2012 R2 x64
```

imageinfo

这个命令可以用来获取内存镜像的摘要信息，比如系统版本，硬件架构等信息

volatility -f mem.vmem imageinfo

通过Suggested Profile(s) 可以知道这个镜像文件的版本最可能是WinXPSP2x86

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/suspicion/mem.vmem)
                      PAE type : PAE
                           DTB : 0x8b18000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-05-03 04:41:19 UTC+0000
     Image local date and time : 2016-05-03 12:41:19 +0800
```

pslist

这个命令可以直接列出运行的进程，如果进程已经结束，会在exit列显示日期和时间，表明进程已经结束了。

volatility -f mem.vmem --profile=WinXPSP2x86 pslist

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x821b9830 System                    4      0     62      253 ------      0
0x81fb9210 smss.exe                552      4      3       19 ------      0 2016-05-03 04:32:10 UTC+0000
0x81c14da0 csrss.exe               616    552     10      328      0      0 2016-05-03 04:32:12 UTC+0000
0x81f81880 winlogon.exe            640    552     18      449      0      0 2016-05-03 04:32:12 UTC+0000
0x8208fda0 services.exe            684    640     16      260      0      0 2016-05-03 04:32:12 UTC+0000
0x81c32b10 lsass.exe               696    640     18      333      0      0 2016-05-03 04:32:12 UTC+0000
0x820a19a0 vmacthlp.exe            852    684      1       25      0      0 2016-05-03 04:32:13 UTC+0000
0x81c30458 svchost.exe             864    684     18      201      0      0 2016-05-03 04:32:13 UTC+0000
0x81c67020 svchost.exe             948    684     11      238      0      0 2016-05-03 04:32:13 UTC+0000
0x81ce7da0 svchost.exe            1040    684     55     1103      0      0 2016-05-03 04:32:13 UTC+0000
0x81c25020 svchost.exe            1096    684      4       66      0      0 2016-05-03 04:32:13 UTC+0000
0x82002b28 svchost.exe            1256    684     13      194      0      0 2016-05-03 04:32:14 UTC+0000
0x81f6c988 explorer.exe           1464   1448     12      329      0      0 2016-05-03 04:32:14 UTC+0000
0x82085550 spoolsv.exe            1576    684     13      140      0      0 2016-05-03 04:32:14 UTC+0000
0x81f64560 vmtoolsd.exe           1712   1464      5      145      0      0 2016-05-03 04:32:15 UTC+0000
0x820a3528 ctfmon.exe             1736   1464      1       78      0      0 2016-05-03 04:32:15 UTC+0000
0x81f7d3c0 vmtoolsd.exe           2020    684      7      273      0      0 2016-05-03 04:32:23 UTC+0000
0x8207db28 TPAutoConnSvc.e         512    684      5       99      0      0 2016-05-03 04:32:25 UTC+0000
0x81c26da0 alg.exe                1212    684      6      105      0      0 2016-05-03 04:32:26 UTC+0000
0x81f715c0 wscntfy.exe            1392   1040      1       39      0      0 2016-05-03 04:32:26 UTC+0000
0x81e1f520 TPAutoConnect.e        1972    512      1       72      0      0 2016-05-03 04:32:26 UTC+0000
```

userassist

这个命令可以提取出内存中记录的当时正在运行的程序有哪些，运行过的次数，最后一次运行的时间等信息。

volatility -f mem.vmem --profile=WinXPSP2x86 userassist

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 userassist
Volatility Foundation Volatility Framework 2.6
------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
Last updated: 2016-05-03 04:31:34 UTC+0000

Subkeys:

Values:

REG_BINARY    UEME_CTLSESSION : Raw Data:
0x00000000  9c 27 8d 0e 01 00 00 00                         .'......

REG_BINARY    UEME_CTLCUACount:ctor :
ID:             1
Count:          2
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00   ................

REG_BINARY    UEME_UITOOLBAR  :
ID:             1
Count:          5
Last updated:   2016-05-03 04:31:34 UTC+0000
Raw Data:
0x00000000  01 00 00 00 0a 00 00 00 50 d4 8a ac f4 a4 d1 01   ........P.......

REG_BINARY    UEME_UITOOLBAR:0x4,7031 :
ID:             1
Count:          3
```

hivelist

这个命令可以列举缓存在内存中的注册表。

volatility -f mem.vmem --profile=WinXPSP2x86 hivelist

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1e9f9d8 0x0bf169d8 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1cee5d0 0x0be075d0 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe1b99b60 0x0ae0ab60 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b95008 0x0adc6008 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a7c2a8 0x0a76b2a8 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a72b60 0x0a6e1b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe146c398 0x084a3398 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1699758 0x08246758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe166faa8 0x05e7eaa8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe16aab60 0x082a6b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe12e9008 0x02d7f008 [no name]
0xe1035b60 0x02b08b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02b02008 [no name]
```

hivedump

这个命令可以打印出注册表中的数据。

volatility -f mem.vmem --profile=WinXPSP2x86 hivedump -o 0xe16aab60

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 hivedump -o 0xe16aab60
Volatility Foundation Volatility Framework 2.6
Last Written         Key
2016-05-03 03:41:48 UTC+0000 \SAM
2016-05-03 03:41:48 UTC+0000 \SAM\SAM
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\000003E9
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members\S-1-5-21-1844237615-1677128483-1801674531
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Members\S-1-5-21-1844237615-1677128483-1801674531\000003EA
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Names
2016-05-03 03:50:51 UTC+0000 \SAM\SAM\Domains\Account\Aliases\Names\HelpServicesGroup
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Groups
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Groups\00000201
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Groups\Names
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Groups\Names\None
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Users
2016-05-03 04:32:14 UTC+0000 \SAM\SAM\Domains\Account\Users\000001F4
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Users\000001F5
2016-05-03 03:50:15 UTC+0000 \SAM\SAM\Domains\Account\Users\000003E8
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Users\000003EA
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Users\Names
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Users\Names\Administrator
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Account\Users\Names\Guest
2016-05-03 03:50:15 UTC+0000 \SAM\SAM\Domains\Account\Users\Names\HelpAssistant
2016-05-03 03:51:02 UTC+0000 \SAM\SAM\Domains\Account\Users\Names\SUPPORT_388945a0
2016-05-03 03:42:51 UTC+0000 \SAM\SAM\Domains\Builtin
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases
2016-05-03 03:41:48 UTC+0000 \SAM\SAM\Domains\Builtin\Aliases\00000220
```

printkey

这个命令可以获取sam表中的信息。

volatility -f mem.vmem --profile=WinXPSP2x86 printkey -K "SAM\Domains\Account\Users\Names"

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem  --profile=WinXPSP2x86 printkey -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: Names (S)
Last updated: 2016-05-03 03:51:02 UTC+0000

Subkeys:
  (S) Administrator
  (S) Guest
  (S) HelpAssistant
  (S) SUPPORT_388945a0

Values:
REG_DWORD                     : (S) 0
```

filescan

这个命令可以扫描内存中的文件。

volatility -f mem.vmem --profile=WinXPSP2x86 filescan

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 filescan | more
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x0000000001ebbaa0      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce8
3
0x0000000001ebbca8      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-ww_b8438ace\9.0.
30729.4148.policy
0x0000000001ebbd40      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
0x0000000001ebc140      5      1 RWDr-- \Device\HarddiskVolume1\System Volume Information\tracking.log
0x0000000001ee4f30      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce8
3
0x0000000001ee6420      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53
0x0000000001ee8c78      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32
0x0000000001eebbe0      2      1 ------ \Device\NamedPipe\Winsock2\CatalogChangeListener-410-0
0x0000000001f6b9e0      1      1 ------ \Device\NamedPipe\net\NtControlPipe1
0x0000000001fa75c8      3      1 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\wbem\mof
0x0000000001ff0028      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001ff00d0      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\桌面
0x0000000001ff05b0      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\system32\oembios.bin
0x0000000001ff06a8      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce8
3
0x0000000002002420      2      1 R--rw- \Device\HarddiskVolume1\Program Files\Common Files\Microsoft Shared\web server extensions\40\isapi\_vti_aut
0x00000000020026e0      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\WINABC.IME
0x0000000002008028      2      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\spool\drivers\color
0x0000000002008d58      1      1 ------ \Device\NamedPipe\wkssvc
0x0000000002008e88      2      1 ------ \Device\NamedPipe\wkssvc
0x0000000002008f90      1      1 ------ \Device\NamedPipe\srvsvc
0x0000000002009318      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce8
3
```

cmdscan

这个命令可以扫描内存中的系统执行命令的历史记录。

volatility -f mem.vmem --profile=WinXPSP2x86 cmdscan

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 616
CommandHistory: 0x55cc00 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x628
Cmd #19 @ 0xe300f7: ??????????????????????????????????????????????????
????'+7;GKW|????????????????????????????????????????????????????????
?????????????
```

netscan || connscan

这个命令可以扫描内存中的系统的网络连接记录。

volatility -f mem.vmem --profile=WinXPSP2x86 netscan

```
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 netscan
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : This command does not support the profile WinXPSP2x86
root@kali:~/Desktop/suspicion# volatility -f mem.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x020575f0 192.168.1.185:1031        192.168.1.1:139           0
root@kali:~/Desktop/suspicion#
```

netscan命令只能扫描Vista（或以后）系统网络连接情况和socks情况

connscan命令可以获取网络连接池中的tcp连接情况

hashdump

这个命令可以获取内存中的系统密码。

volatility -f mem.raw --profile=WinXPSP2x86 hashdump

```
root@kali:~/Desktop# volatility -f mem.raw --profile=WinXPSP2x86 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:1e27e87bd14ec8af43714428b303e3e4:1e581aafa474dfadfdf83fc31e4fd4ea:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:687255e91a0f559b6d75553dbd51f785:b6125736bdd2d5f154fdce59f52e39f1:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:fb41f8d1334fba131974c39bfab09512:::
root@kali:~/Desktop#
```

hashdump

这个命令可以获取内存中的系统密码。

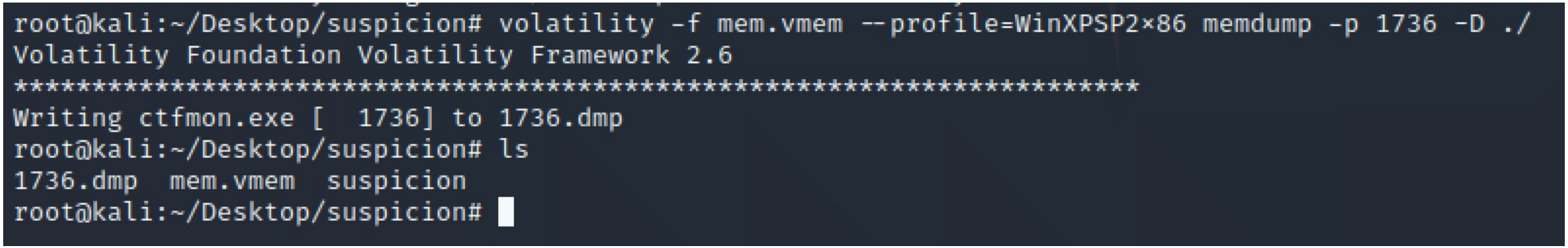
volatility -f mem.raw --profile=WinXPSP2x86 hashdump -y 0xe10182f8 -s 0xe1492b60

```
root@kali:~/Desktop# volatility -f mem.raw --profile=WinXPSP2x86 hashdump -y 0xe10182f8 -s 0xe1492b60
Volatility Foundation Volatility Framework 2.6
Administrator:500:1e27e87bd14ec8af43714428b303e3e4:1e581aafa474dfadfdf83fc31e4fd4ea:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:687255e91a0f559b6d75553dbd51f785:b6125736bdd2d5f154fdce59f52e39f1:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:fb41f8d1334fba131974c39bfab09512:::
root@kali:~/Desktop#
```

memdump

这个命令可以获取内存中指定进程的数据。

volatility -f mem.vmem --profile=WinXPSP2x86 memdump -p 进程id号 -D 目录名



命令总结

- imageinfo：显示目标镜像的摘要信息
- pslist：列举出系统进程，但不能检测隐藏或解链的进程
- psscan：可以找到已经终止的进程以及被rootkit隐藏或解链的进程
- pstree：以树的形式查看进程列表，也不能检测隐藏或解链的进程
- memdump：提取指定进程，然后用foremost分离提取的文件
- filescan：扫描所有的文件列表
- hashdump：查看当前操作系统中的password hash
- svcscan：扫描windows的服务
- connscan：查看网络连接
- netscan：查看当时的网络连接

命令总结

- hivelist：查看缓存在内存的注册表
- hivedump：打印出注册表中的数据
- printkey：获取注册表中的值
- userassist：提取内存中记录当时正在运行的程序有哪些，运行过次数，最后一次运行的时间等信息
- cmdscan：提取内存中保留的cmd命令使用情况
- iehistory：获取ie浏览器的使用情况
- hashdump：获取内存中的系统密码
- timeliner：最大程度的将内存中的信息提取出来，自动从多个位置来收集系统的活动信息

命令总结

- linux_pslist：列举系统进程
- linux_psaux：列举系统所有进程的详细信息
- linux_pstree：以树的形势查看进程列表
- linux_lsof：查看进程相关文件
- linux_memmap：查看进程内存信息
- linux_dump_map：dump出内存信息
- linux_lsmod：查看已载入系统的模块
- linux_proc_maps：查看进程细节包括共享库、开始和结束位置等信息
- linux_netstat：查看网络连接情况
- linux_find_file：查看可疑文件的位置

03

例题讲解

内存取证

- **题目下载**
- 链接: https://pan.baidu.com/s/14MziOdJBMpD7CtQc03Ixjw
  提取码: ms4w
- **题目说明**
- 一天中午小明出去吃饭，临走前还忘记了锁电脑，这时同寝室的小黑想搞点事情，懂点黑客和社工知识的小黑经过多次尝试获得了密码成功进入电脑，于是便悄悄在电脑桌面上写了什么，想给小明一个惊喜，同时还传送走了小明的机密文件，正巧这时小明刚好回来，两人都吓了一跳，小黑也不管自己在电脑上留下的操作急忙离开电脑，故作淡定的说：“我就是随便看看”。

内存取证-1

- **解题过程**
- 1、首先确认raw文件
- 2、使用volatility进行分析
- 3、题目提示：小黑写的是啥，据说是flag？那么需要找到小黑写的东西

内存取证-2

- **解题过程**
- 1、分析题目，需要获取到小黑传送走的机密文件
- 2、使用volatility进行分析，分析进程，找一下怎么传送的机密文件
- 3、提取文件，分析文件内容

内存取证-3

- **解题过程**
- 1、分析题目，小明的密码是啥？
- 2、使用volatility进行分析，分析进程，找一下怎么传送的机密文件
- 3、提取文件，分析文件内容

04

真题练习

内存取证-password

题目描述：听说flag就是系统密码？
flag格式为flag{系统密码}

解题过程

1、先使用imageinfo获取镜像系统版本信息

2、获取密码可以使用hashdump获取hash

3、在线解hash（在线网站：www.cmd5.com、www.somd5.com）

内存取证-隐藏的秘密

题目描述：明明在计算机管理中没有这个用户，为什么还会被这个用户登录呢？

flag为flag{md5(用户名:密码)}

解题过程

1、先使用imageinfo获取镜像系统版本信息

2、获取密码可以使用hashdump获取hash

3、导出注册表，分析注册表

4、找到异常的用户

THANKS