

CTF 内存取证 USB流量分析

原创

[MOLLMY](#) 于 2019-09-09 23:56:25 发布 4847 收藏 25

分类专栏: [CTF 笔记](#) [网络攻防](#) 文章标签: [CTF内存取证题](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/MOLLMY/article/details/100679762>

版权



[CTF 同时被 3 个专栏收录](#)

5 篇文章 0 订阅

订阅专栏



[笔记](#)

3 篇文章 0 订阅

订阅专栏



[网络攻防](#)

4 篇文章 0 订阅

订阅专栏

护网杯2019预选赛第二题

内存取证弟弟题?

题目名叫:

Baby_forensic

题目 [附件地址](#)

目录

[Baby_forensic](#)

知识点:

内存取证工具volatility 的使用:

取证方法建议

Keyboard scan code:

解题过程:

1. Kali中解压文件
2. pslist查看进程
3. 通过cmdscan[孙2] 提取命令历史记录, 结果如下
4. 通过filescan查看文件目录, 检查disk.zip:
5. 使用binwalk -e命令提取文件

知识点:

内存取证工具volatility 的使用:

volatility -f <文件名> --profile=<配置文件> <插件> [插件参数]

使用imageinfo插件来猜测dump文件的profile值: WinXPSP2x86

```
root@kali:~/quzhen# volatility -f mem.vmem imageinfo
```

grep是用来搜索特定的字符串, bgrep是用来搜索非文本数据模式和hexdump

volatility -info 用于查看volatility已经添加的profile和插件信息

Volatility -f file.raw imageinfo 判断当前镜像信息, 或kdbgscan, 仅适合windows内存镜像

常见插件:

Volatility -f file.raw --profile=WinXPSP2x86 notepad 查看当前展示的notepad文本

Volatility -f file.raw --profile=WinXPSP2x86 pslist 列出运行的进程, 如果Exit所在的一列显示了日期时间, 则表明该进程已经结束了

Hivelist 列出缓存在内存中的注册表

Filescan 扫描内存中的文件

Dumpfiles 将内存中的缓存文件导出

Volatility -f file.raw --profile=WinXPSP2x86 Memdump -p 进程号 -D ./ (导出目录) 将某个进程信息导出/根据pid dump出指定进程

Foremost 2888.dmp 分析dump出的内存文件

Svcscan 扫描windows的服务

Connscan 查看网络连接

Cmdscan 查看命令行上的操作

取证方法建议

RFC 3227提供了获取数字证据的许多做法, 比如, 收集数据的顺序可以决定调查的成败。

这个顺序称为波动顺序 (Volatility Order), 顾名思义, 调查人员必须首先收集易消失的数据。易失性数据是系统关闭时可能丢失的任何数据, 例如连接到仍然在RAM中注册的网站。调查人员必须将先从最不稳定的证据中开始收集数据:

- (1) 缓存
- (2) 路由表, 进程表, 内存
- (3) 临时系统文件
- (4) 硬盘

- (5) 远程日志，监控数据
- (6) 物理网络配置，网络拓扑
- (7) 媒体文件（CD，DVD）

Keyboard scan code:

USB_Interrupt in 表示该USB设备为键盘[孙1]，捕捉到的键盘数据位于Leftover Capture Data域;

键盘数据由8个字节组成:

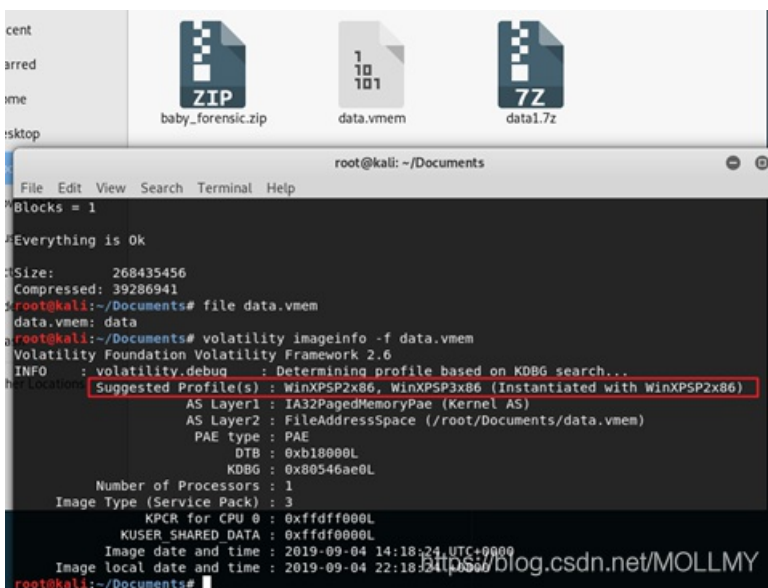
- Byte 0 键盘修饰符位，SHIFT, ALT, CTRL等
- Byte 1 保留位
- Byte 2-7 当前按下的键，最多6个，顺序不重要（一个键只有两种状态：pressed or not pressed）

解题过程:

1. Kali中解压文件

由题目可知是内存取证，利用volatility工具分析解压的vmem文件

判断当前镜像信息，分析操作系统



2. pslist查看进程

```

root@kali:~/Documents# volatility -f data.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds MemSess Wow64 Start Exit
-----
0x817bd830 System 4 0 58 174 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81291da0 smss.exe 372 4 3 19 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81393020 csrss.exe 448 372 11 417 0 0 0 2019-09-04 14:17:12 UTC+0000
0x8134c7c0 winlogon.exe 476 372 24 461 0 0 0 2019-09-04 14:17:12 UTC+0000
0x813063d8 services.exe 668 476 16 271 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81445020 lsass.exe 680 476 27 374 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81479990 vmacthlp.exe 836 668 1 25 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81441208 svchost.exe 852 668 21 200 0 0 0 2019-09-04 14:17:12 UTC+0000
0x81054d50 svchost.exe 932 668 9 253 0 0 0 2019-09-04 14:17:13 UTC+0000
0x8133c348 svchost.exe 1024 668 79 1242 0 0 0 2019-09-04 14:17:13 UTC+0000
0x816c05b8 svchost.exe 1072 668 5 59 0 0 0 2019-09-04 14:17:13 UTC+0000
0x81571f10 svchost.exe 1104 668 16 199 0 0 0 2019-09-04 14:17:13 UTC+0000
0x816105b0 explorer.exe 1424 1392 15 380 0 0 0 2019-09-04 14:17:14 UTC+0000
0x81612380 spoolsv.exe 1568 668 16 132 0 0 0 2019-09-04 14:17:14 UTC+0000
0x8142a8b0 svchost.exe 1980 668 5 88 0 0 0 2019-09-04 14:17:31 UTC+0000
0x81520020 VGAuthService.e 224 668 2 60 0 0 0 2019-09-04 14:17:31 UTC+0000
0x80ee4020 vntoolsd.exe 300 668 9 265 0 0 0 2019-09-04 14:17:31 UTC+0000
0x80ea88b0 wmlprvse.exe 608 852 14 244 0 0 0 2019-09-04 14:17:39 UTC+0000
0x81506c88 alg.exe 1348 668 7 108 0 0 0 2019-09-04 14:17:40 UTC+0000
0x80ea05b0 rundll32.exe 1668 1424 4 78 0 0 0 2019-09-04 14:17:40 UTC+0000
0x80ecfb28 vntoolsd.exe 1680 1424 7 175 0 0 0 2019-09-04 14:17:40 UTC+0000
0x8147e7a0 ctfmon.exe 1692 1424 1 71 0 0 0 2019-09-04 14:17:40 UTC+0000
0x80e9cc68 wscntfy.exe 1824 1 39 0 0 0 2019-09-04 14:17:41 UTC+0000
0x80ef62d0 cmd.exe 1716 1424 1 34 0 0 0 2019-09-04 14:18:02 UTC+0000
0x80e94da0 conime.exe 1732 1716 1 38 0 0 0 2019-09-04 14:18:02 UTC+0000
0x816152d8 wordpad.exe 208 1424 4 113 0 0 0 2019-09-04 14:18:20 UTC+0000
0x816146a0 cmd.exe 548 300 0 0 0 0 0 2019-09-04 14:18:20 UTC+0000
0x8147b020 ipconfig.exe 440 548 0 0 0 0 0 2019-09-04 14:18:20 UTC+0000
root@kali:~/Documents#

```

进程分析:

wscntfy.exe, Windows系统关键进程, 负责检查计算机的安全状态, 包括防火墙、病毒防护软件、自动更新三个安全要素, 如果这些服务状态不正常, 系统就会在状态栏进行告警提示。这个进程也可能被病毒软件和黑客程序伪装

ctfmon.exe, Microsoft Office产品套装的一部分, 是有关输入法的一个可执行程序。它可以选择用户文字输入程序, 和微软Office XP语言条。这不是纯粹的系统程序, 但是如果终止它, 可能会导致不可知的问题。另外, ctfmon.exe可能被感染上木马而成为病毒程序

wordpad.exe, 是微软Microsoft Windows自带的免费字处理工具。

Conime.exe, 输入法编辑器

Cmd.exe, windows系统的命令程序

根据进程列表可以推断出当前用户可能正在使用写字板和命令程序, 可以从这两个方面入手

查看进程wordpad, 保存为dmp文件

```

root@kali:~/Documents# volatility -f data.vmem --profile=WinXPSP2x86 memdump -p 1716 -D ./psdump
Volatility Foundation Volatility Framework 2.6
*****
Writing cmd.exe [ 1716] to 1716.dmp
root@kali:~/Documents# volatility -f data.vmem --profile=WinXPSP2x86 memdump -p 548 -D ./psdump
Volatility Foundation Volatility Framework 2.6
*****
Writing cmd.exe [ 548] to 548.dmp

```

用hexeditor查看导出的dmp文件, 检索flag, 这几个进程文件里都有提示:

invalid flags (%08x) specified to RtlCreateHeap,

```

Z.....[.u.9=<..].....;E.....).}.E.....E.P.E.P.E
vZ]: Invalid flags (%08x) specified to RtlCreateHeap
.....u.).....V.o..E......j.E.P.F..YY.L
for its manifest ntstatus 0x001x

```

无其他发现

3. 通过cmdscan[孙2] 提取命令历史记录, 结果如下

```
root@kali:~/Documents# volatility -f data.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: csrss.exe Pid: 448
CommandHistory: 0x36e3850 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2d0
Cmd #0 @ 0x55d868: hill matrix 3,2,2,9,7,7,6,4,9
```

有用的信息: hill_matrix, 应该是用到了hill cipher

通过cmdline查看命令行用到的参数:

```
root@kali:~/Documents# volatility -f data.vmem --profile=WinXPSP2x86 cmdline
Volatility Foundation Volatility Framework 2.6
*****
System pid: 4
*****
smss.exe pid: 372
Command line : \SystemRoot\System32\smss.exe
*****
csrss.exe pid: 448
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3
erverDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,
*****
winlogon.exe pid: 476
Command line : winlogon.exe
*****
services.exe pid: 668
Command line : C:\WINDOWS\system32\services.exe
*****
lsass.exe pid: 680
Command line : C:\WINDOWS\system32\lsass.exe
*****
vmacthlp.exe pid: 836
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
*****
svchost.exe pid: 852
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
*****
svchost.exe pid: 932
Command line : C:\WINDOWS\system32\svchost -k rpcss
*****
svchost.exe pid: 1024
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
*****
svchost.exe pid: 1072
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
```

```
Command line : C:\WINDOWS\system32\wscntfy.exe
*****
cmd.exe pid: 1716
Command line : "C:\WINDOWS\system32\cmd.exe"
*****
conime.exe pid: 1732
Command line : C:\WINDOWS\system32\conime.exe
*****
wordpad.exe pid: 200
Command line : "C:\Program Files\Windows NT\Accessories\WORDPAD.EXE" "C:\Documents and Settings\Administrator\桌面\disk.zip"
*****
cmd.exe pid: 548
*****
ipconfig.exe pid: 440
root@kali:~/Documents#
```

发现可能通过写字板程序产生了一个文件: disk.zip

4. 通过filescan查看文件目录, 检查disk.zip:

Filescan没有发现直接的flag文件, 媒体文件气球.wav也没有有什么有用的信息

最后在disk.zip中寻找

```
0x0000000012c5f8 1 0 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\mvdocs.dll
0x0000000012c9828 1 0 R--rw- \Device\HarddiskVolume1\WINDOWS\Media\Windows XP 气球.wav
0x0000000012cc320 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\开
*****
0x0000000012f1f90 1 0 R--r-- \Device\HarddiskVolume1\WINDOWS\Fonts\microsf.ttf
0x0000000012f2230 1 0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\mfcc42loc.dll
0x0000000012f22c8 1 1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\My Documents
0x0000000012f24a8 1 0 R--r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\disk.zip
0x0000000012f25d8 1 1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595
```

Dump出媒体文件气球.wav和之前发现的disk.zip

将dump出的文件重命名为气球.wav 和disk.zip

```
root@kali:~/Documents# unzip disk.zip
Archive: disk.zip
  inflating: disk.img
root@kali:~/Documents#
```

```
root@kali:~/Documents/filedump# ls
balloon.wav  disk.img  disk.zip
root@kali:~/Documents/filedump# ls -l
total 2052
-rw-r--r-- 1 root root 8192 Sep 9 03:27 balloon.wav
-rw-r--r-- 1 root root 2048000 Sep 4 10:11 disk.img
-rwxr-xr-x 1 root root 45056 Sep 9 03:28 disk.zip
root@kali:~/Documents/filedump# strings balloon.wav
RIFF
WAVEfmt
data
f
l
```

经查看，wav文件中没有有用的信息

disk.zip解压后得到一个镜像文件disk.img，查看它的imageinfo，无果

File命令发现是linux下的ext2文件系统：

```
root@kali:~/Documents/filedump# volatility -f disk.img imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : No suggestion (Instantiated with no profile)
      AS Layer1 : FileAddressSpace (/root/Documents/filedump/disk.img)
      PAE type : No PAE
root@kali:~/Documents/filedump# volatility -f disk.img kdbgscan
Volatility Foundation Volatility Framework 2.6
root@kali:~/Documents/filedump# file disk.img
disk.img: Linux rev 1.0 ext2 filesystem data, UUID=63f426ba-3c01-4149-8b3e-639ff00156b9 (large files)
root@kali:~/Documents/filedump#
```

5. 使用binwalk -e命令提取文件

```
root@kali:~/Documents/filedump# ls
balloon.wav  disk.img  disk.zip
root@kali:~/Documents/filedump# binwalk -e disk.zip
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          Zip archive data, at least v2.0 to extract, compr
sk.img
42835        0xA753      End of Zip archive, footer length: 22
root@kali:~/Documents/filedump# ls
balloon.wav  disk.img  disk.zip  _disk.zip.extracted
root@kali:~/Documents/filedump# cd _disk.zip.extracted/
root@kali:~/Documents/filedump/_disk.zip.extracted# ls
0.zip  disk.img  提取出的文件
root@kali:~/Documents/filedump/_disk.zip.extracted# file 0.zip
0.zip: Zip archive data, at least v2.0 to extract
root@kali:~/Documents/filedump/_disk.zip.extracted# file disk.img
disk.img: Linux rev 1.0 ext2 filesystem data, UUID=63f426ba-3c01-4149-8b3e-639f
root@kali:~/Documents/filedump/_disk.zip.extracted# unzip 0.zip
Archive: 0.zip
  replace disk.img? [y]es, [n]o, [A]ll:
  new name: from 0.zip disk.img
  inflating: from 0.zip disk.img
root@kali:~/Documents/filedump/_disk.zip.extracted# ls
0.zip  disk.img  from 0.zip disk.img
root@kali:~/Documents/filedump/_disk.zip.extracted# file from 0.zip disk.img
from 0.zip_disk.img: Linux rev 1.0 ext2 filesystem data, UUID=63f426ba-3c01-414
root@kali:~/Documents/filedump/_disk.zip.extracted# binwalk -e disk.img
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          Linux EXT filesystem, rev 1.0, ext2 filesystem da
```

```
root@kali:~/Documents/filedump/_disk.zip.extracted# cd disk.img.extracted/
root@kali:~/Documents/filedump/_disk.zip.extracted/_disk.img.extracted# ls
0.ext  ext-root
root@kali:~/Documents/filedump/_disk.zip.extracted/_disk.img.extracted# cd ext-root
root@kali:~/Documents/filedump/_disk.zip.extracted/_disk.img.extracted/ext-root# ls
usb.pcapng
```

经过两次binwalk 提取到以上文件，发现一个usb.pcapng文件（usb流量分析）



得到LHBDSLUDRIDT

转为小写 即为flag

别问我为什么转小写，我也不知道

提交大写的不对，小写显示正确

[孙1]<https://bitvijays.github.io/LFC-Forensics.html#usb-keyboard>

[孙2]The cmdscan plugin searches the memory of csrss.exe on XP/2003/Vista/2008 and conhost.exe on Windows 7 for commands that attackers entered through a console shell (cmd.exe). This is one of the most powerful commands you can use to gain visibility into an attackers actions on a victim system, whether they opened cmd.exe through an RDP session or proxied input/output to a command shell from a networked backdoor.

[孙3]<https://bitvijays.github.io/LFC-Forensics.html#usb-keyboard>