

内存取证-volatility工具的使用 （史上更全教程，更全命令）

原创 已于 2023-07-15 15:40:47 修改 · 10w+ 阅读 · 320 点赞 · 1.3k 收藏 · 本内容遵循CC 4.0 BY-SA版权协议

收录于  内存取证  AtomGit开源社区

目录

- 内存取证-volatility工具的使用
 - 一，简介
 - 二，安装Volatility
 - 1.windows下
 - 2. Linux下（这里kali为例）
 - 三、安装插件
 - 四，工具介绍help
 - 五，命令格式
 - 编辑
 - 六，常用命令插件
 - ♥可以先查看当前内存镜像中的用户 **printkey -K "SAM\Domains\Account\Users\Names"**
 - ♥查看用户名密码信息(密码是哈希值，需要john爆破) **hashdump**
 - ♥如果john爆破不出来，就使用 **lsadmp** 查看强密码 **lsadmp**
 - ♥查看进程 **pslist**
 - ♥查看已知进程 **pslist**
 - ♥隐藏或解链的进程 **psscan**
 - ♥查看服务 查询服务名称 **svcsan**
 - ♥查看浏览器历史记录,获取当前系统浏览器搜索过的关键词 **iehistory**
 - ♥查看网络连接 获取当前系统 **ip netscan**
 - ♥查看网络连接 **connscan**
 - ♥查看网络连接 **connections**
 - ♥查看命令行操作，显示cmd历史命令 **cmdscan**
 - ♥查看进程命令行参数（具体一些可疑进程的参数指令） **cmdline**
 - ♥扫描所有的文件列表 **filescan**
 - ♥查看文件内容 **dmpfiles**
 - ♥查看当前展示的notepad内容 **notepad**
 - ♥显示有关编辑控件（曾经编辑过的内容）的信息 **editbox**
 - ♥提取进程 **memdump**
 - ♥屏幕截图 **screenshot**
 - ♥查看注册表配置单元 **hivelist**
 - ♥查看注册表键名 **hivedmp**
 - ♥查看注册表键值 **printkey**
 - ♥获取主机名 **printkey**
 - ♥列出用户名 **pringkey**
 - ♥查看运行程序相关的记录，比如最后一次更新时间，运行过的次数等。 **serassist**
 - ♥最大程序提取信息 **timeliner**
 - ♥查看剪贴板信息 **clipboard**
 - ♥显示关于计算机及其操作系统的详细配置信息（插件） **systeminfo**
 - ♥恢复被删除的文件 **mftparser**
 - ♥查看环境变量 **envvars**
 - ♥列出某一进程加载的所有dll文件 **dlllist**
 - ♥程序版本信息 **verinfo**
 - ♥产看进程树，可以轻松了解各进程之间的关系：父进程与子进程 **pstree**
 - ♥从内存文件中找到异常程序植入到系统的开机自启痕迹 **shimcache**

- 七，内存取证的大致思路
- 八，例题讲解
 - 题目一

- 解析
 - 1.从内存中获取到用户admin的密码并且破解密码，以Flag{admin,password}形式提交；
 - 2.获取当前系统 ip 地址及主机名，以 Flag{ip:主机名}形式提交；
 - 3.获取当前系统浏览器搜索过的关键词，
 - 4.当前系统中存在挖矿进程，请获取指



路baby

关注

登录后您可以享受以下权益：

 免费复制代码

 和博主大V互动

 下载海量资源

 发动态/写文章/加入社区

打赏

5.恶意进程在系统中注册了服务，请将服务名以 Flag{服务名}形式提交。

加油各位(◡‿◡)y 期待与君再相逢

内存取证-volatility工具的使用

一，简介

Volatility是一款开源内存取证框架，能够对导出的内存镜像进行分析，通过获取内核数据结构，使用插件获取内存的详细情况以及系统的运行状态。

Volatility是一款非常强大的内存取证工具,它是由来自全世界的数百位知名安全专家合作开发的一套工具,可以用于windows,linux,mac osx,android!取证。Volatility是一款开源内存取证框架，能够对导出的内存镜像进行分析，通过获取内核数据结构，使用插件获取内存的详细情况以及系统的运行

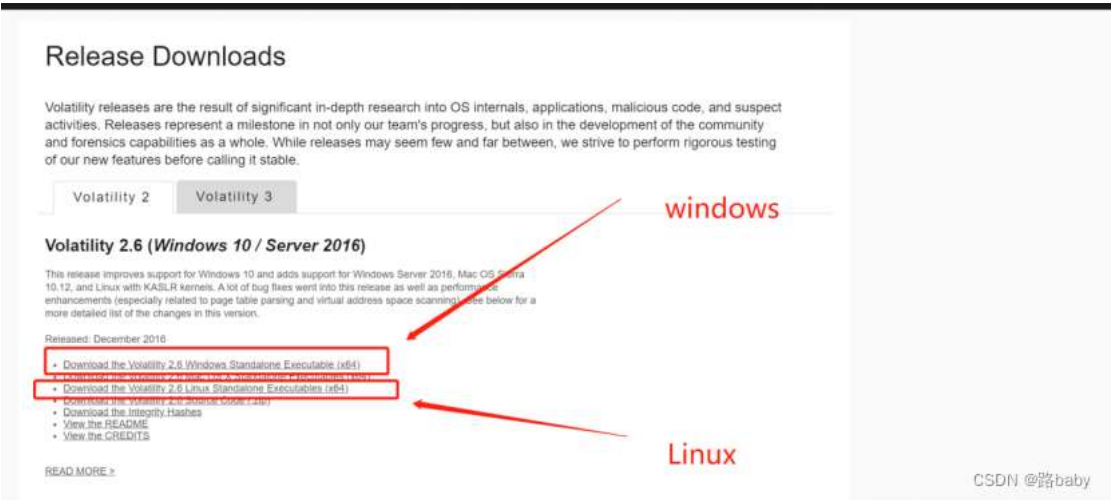
二，安装Volatility

在不同系统下都有不同的软件版本

官网地址：

官方地址

<https://www.volatilityfoundation.org/26>



根据自己需求下载

另外不同的版本下，也存在着一定命令上的差异，使用时一定需注意

支持的内存格式还是很多的，符合日常需求

What about hibernation, crash dumps, and page files?

The memory formats supported by Volatility 2.X include:

- Raw/Padded Physical Memory
- Firewire (IEEE 1394)
- Expert Witness (EWF)
- 32- and 64-bit Windows Crash Dump
- 32- and 64-bit Windows Hibernation
- 32- and 64-bit MachO files
- Virtualbox Core Dumps
- VMware Saved State (.vmss) and Snapshot (.vmsn)
- HPAK Format (FastDump)
- LIME (Linux Memory Extractor)
- QEMU VM memory dumps

1.windows下

直接下载解压就好了

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

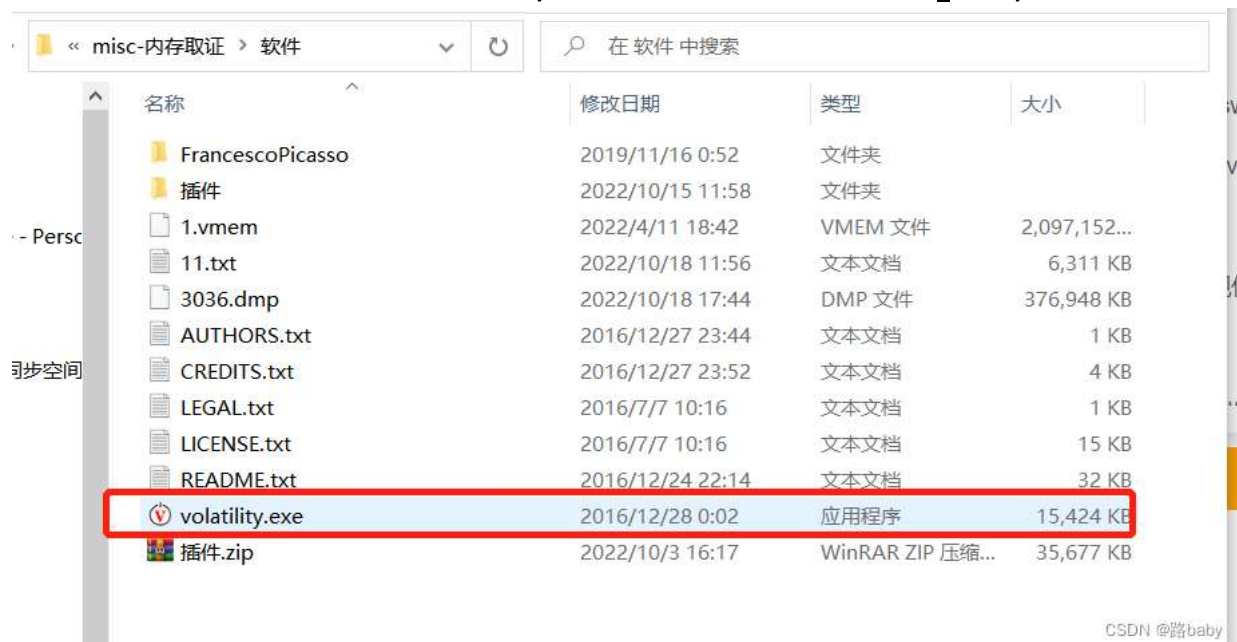
发动态/写文章/加入社区



路baby

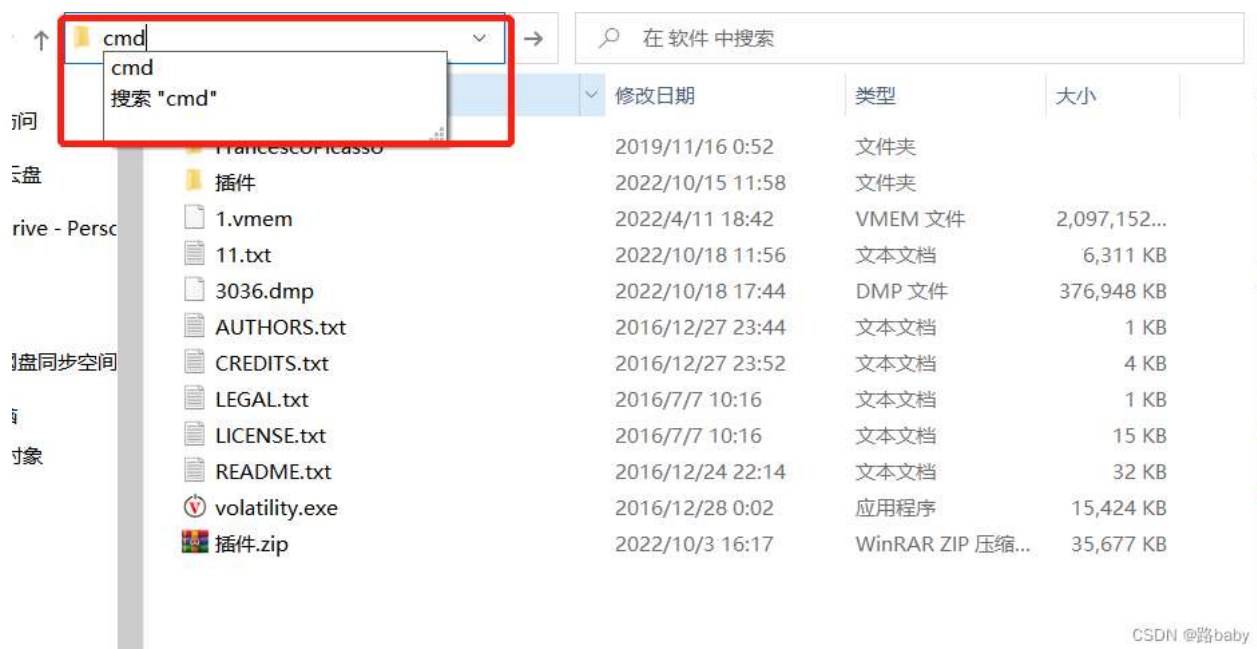
关注

点赞



CSDN @路baby

打开cmd 直接输入命令即可（cmd必须是当前目录，除非你设了环境变量）



CSDN @路baby

2. Linux下（这里kali为例）

Volatility2.6需要python2，pip安装模块也需要2版本，具体命令根据实际情况调整。

源码包（这是github,比较快，也可以下上面官网的，步骤是一样的）

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区



路baby

关注

打赏

源码包

<https://github.com/volatilityfoundation/volatility>

volatilityfoundation / volatility Public

<> Code Issues 146 Pull requests 41 Actions Projects Wiki Security Insights

master 11 branches 10 tags Go to file

iMHLv2 Merge pull request #765 from volatilityfoundation/win10_19041 ...

contrib	Move unstable plugins, plugins still
pyinstaller	Fix updated pyinstaller "empty DES
resources	Move the Volatility-1.4_rc1 branch
tools	Linux - Update check_fops for 4.20
volatility	add Win10 19041 support
.gitattributes	add .gitattributes
.gitignore	Add in initial version of unified output plugin.

Clone
HTTPS GitHub CLI
<https://github.com/volatilityfoundation/volatility>
Use Git or checkout with SVN using the web URL.
Open with GitHub Desktop
Download ZIP

下载解压

```
unzip volatility-master.zip
```

安装依赖环境 (distorm3 crypto)

```
crypto
pip2 install pycryptodome
#如果安装失败，可使用以下命令切换国内源
pip2 install pycryptodome -i https://pypi.tuna.tsinghua.edu.cn/simple
```

distorm3下载地址

GitHub - vext01/distorm3: distorm3

下载解压

```
unzip distorm3-master.zip
```

登录后您可以享受以下权益：

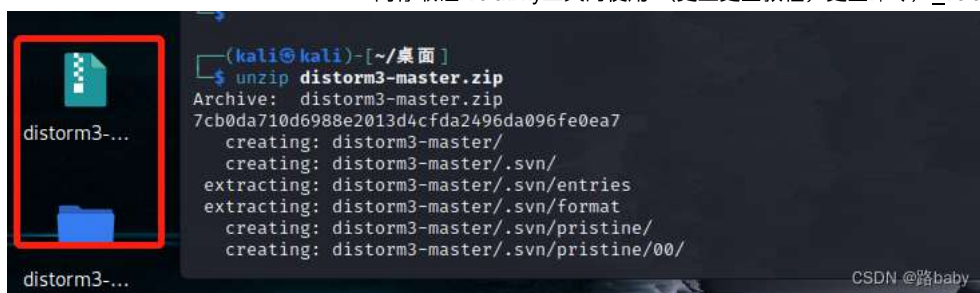
免费复制代码

和博主大V互动

下载海量资源

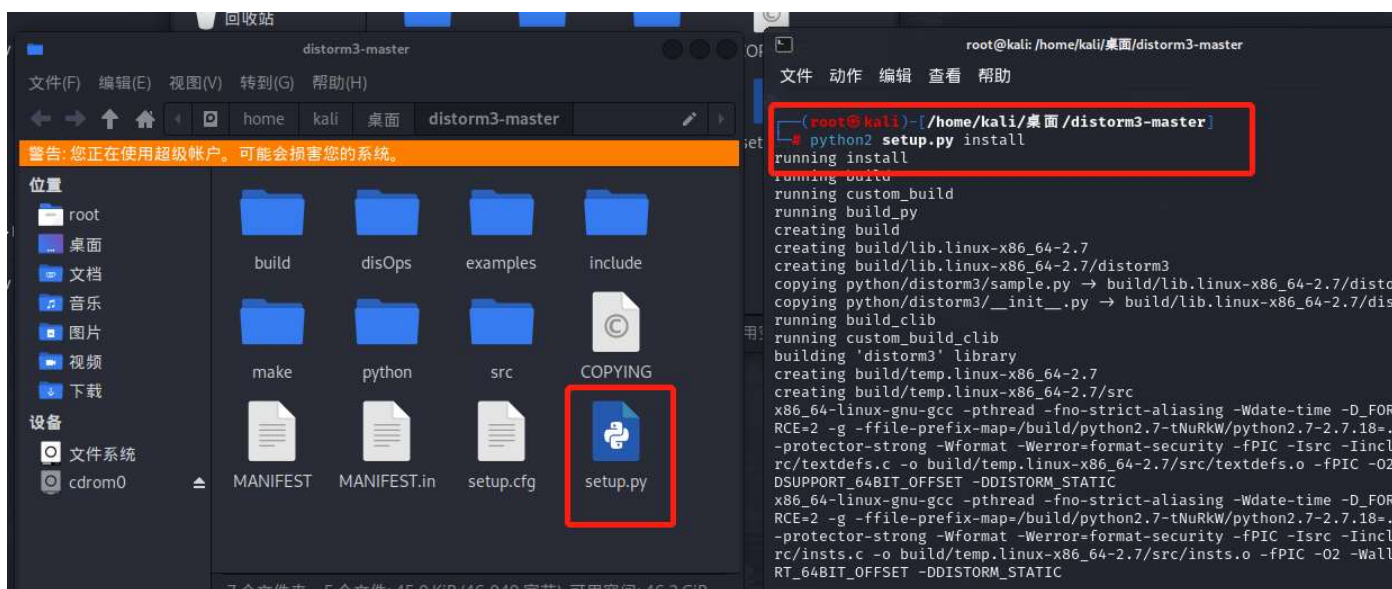
发动态/写文章/加入社区

路baby 关注



进行编译

```
python2 setup.py install
```



可选插件

Distorm3（反编译库）：pip install distorm3

Yara（恶意软件分类工具）：pip install yara

PyCrypto（加密工具集）：pip install pycrypto

PIL（图片处理库）：pip install pil

OpenPyxl（读写excel文件）：pip install openpyxl

ujson（JSON解析）：pip install ujson

安装Volatility

在解压后的Volatility目录下进行编译

```
python2 setup.py install
```

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

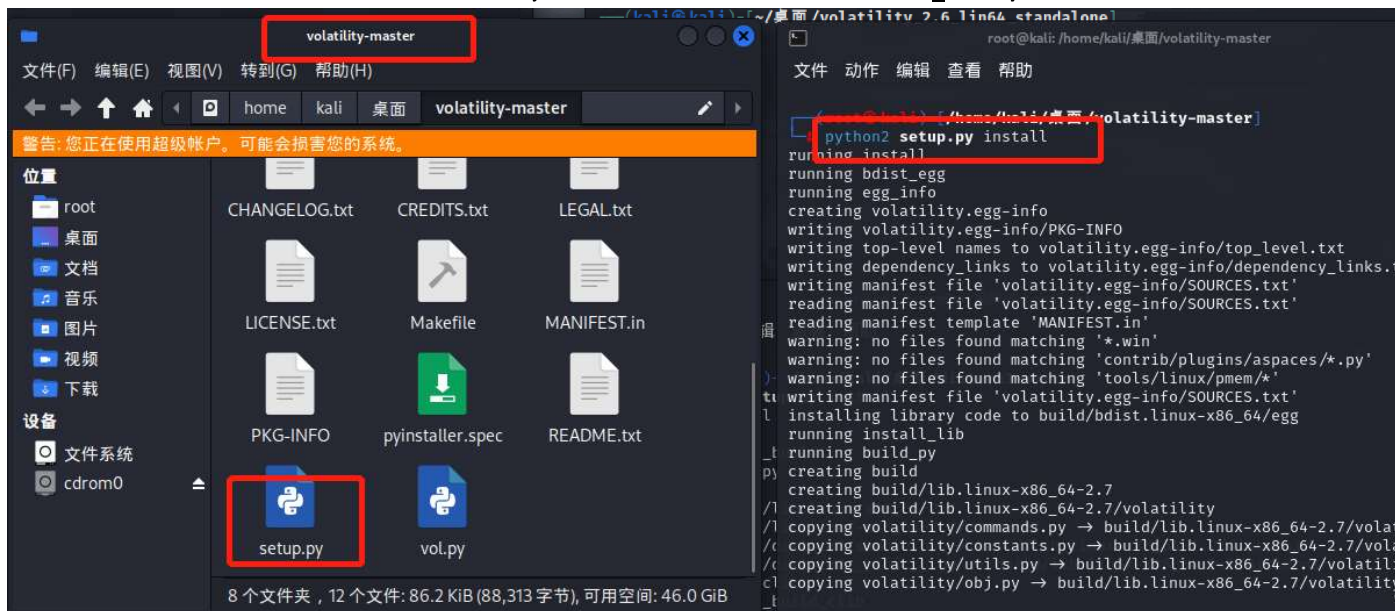
发动态/写文章/加入社区



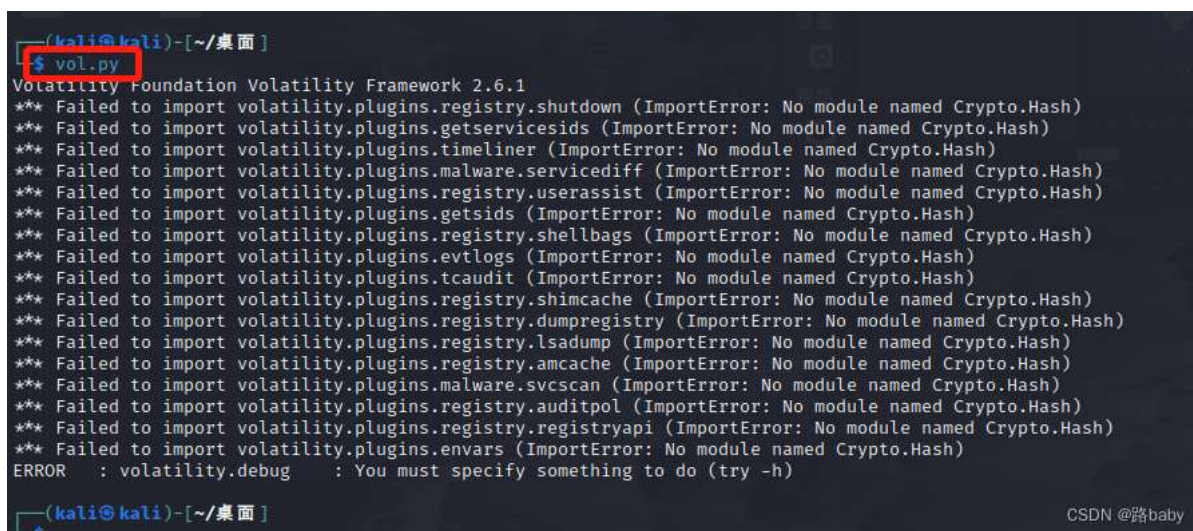
路baby

关注

点赞



检验



三、安装插件

安装mimikatz

将mimikatz.py复制到volatility-master/volatility/plugins/目录下，使用时需要添加参数--plugins=../volatility-master/volatility/plugins。运行时可能会出现如下错误，这是因为没有安装construct 模块：

```
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
ERROR : volatility.debug : You must specify something to do (try -h)
```

安装construct模块。

pip install construct

四、工具介绍help

输入vol.py -h 查看官方做出的帮助

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区



路baby

关注

点赞

```
(kali㉿kali)-[~/桌面]
$ vol.py --help
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtxlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help                list all available options and their default values.
                           Default values may be set in the configuration file
                           (/etc/volatilityrc)
  --conf-file=/home/kali/.volatilityrc
                           User based configuration file
  -d, --debug                Debug volatility
  --plugins=PLUGINS          Additional plugin directories to use (colon separated)
  --info                     Print information about all registered objects
  --cache-directory=/home/kali/.cache/volatility
                           Directory where cache files are stored
  --cache                    Use caching
  --tz=TZ                    Sets the (Olson) timezone for displaying timestamps
                           using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                           Filename to use when opening an image
  --profile=WinXPSP2x86      Name of the profile to load (use --info to see a list
                           of supported profiles)
  -l LOCATION, --location=LOCATION
                           A URN location from which to load an address space
  -w, --write                Enable write support
  --dtb=DTB                  DTB Address
  --shift=SHIFT              Mac KASLR shift address
  --output=text              Output in this format (support is module specific, see
                           the Module Output Options below)
  --output-file=OUTPUT_FILE
                           Write output in this file
  -v, --verbose              Verbose information
  --physical_shift=PHYSICAL_SHIFT
                           Linux kernel physical shift address
  --virtual_shift=VIRTUAL_SHIFT
                           Linux kernel virtual shift address
  -g KDBG, --kdbg=KDBG       Specify a KDBG virtual address (Note: for 64-bit
                           Windows 8 and above this is the address of
                           KdCopyDataBlock)
  --force                    Force utilization of suspect profile
  -k KPCR, --kpcr=KPCR       Specify a specific KPCR address
  --cookie=COOKIE            Specify the address of nt!ObHeaderCookie (valid for
                           Windows 10 only)

Supported Plugin Commands:
  apihooks                  Detect API hooks in process and kernel memory
  atoms                     Print session and window station atom tables
  atomscan                  Pool scanner for atom tables
  bigpools                  Dump the big page pools using BigPagePoolScanner
  bioskbd                   Reads the keyboard buffer from Real Mode memory
  callbacks                 Print system-wide notification routines
  clipboard                 Extract the contents of the windows clipboard
  cmdline                   Display process command-line arguments
  cmdscan                   Extract command history by scanning for _COMMAND_HISTORY
  connections               Print list of open connections [Windows XP and 2003 Only]
  connscan                  Pool scanner for tcp connections
  consoles                  Extract command history by scanning for _CONSOLE_INFORMATION
  crashinfo                 Dump crash-dump information
```

翻译如下

AI写代码

```
1 Volatility Foundation Volatility Framework 2.6
2 用法: Volatility - 内存取证分析平台
3
4 Options:
5   -h, --help                列出所有可用选项及其默认值
6                             默认值可以在配置文件中设置
7                             (/etc/volatilityrc)
8   --conf-file=/home/kali/.volatilityrc
```

登录后您可以享受以下权益:

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区



路baby

关注

打赏

输入 `vol.py --info` 可查看插件。

```
(kali㉿kali)-[~/桌面]
└─$ vol.py --info
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getuids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)

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_10240_17770 - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586    - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
```

CSDN @路baby

翻译如下

bash		AI写代码
1	Volatility Foundation Volatility Framework 2.6	
2		
3	Profiles	
4	-----	
5	VistaSP0x64 - Windows Vista SP0 x64 的配置文件	
6	VistaSP0x86 - Windows Vista SP0 x86 的配置文件	
7	VistaSP1x64 - Windows Vista SP1 x64 的配置文件	
8	VistaSP1x86 - Windows Vista SP1 x86 的配置文件	
9	VistaSP2x64 - Windows Vista SP2 x64 的配置文件	
10	VistaSP2x86 - Windows Vista SP2 x86 的配置文件	
11	Win10x64 - A Profile for Windows 10 x64	
12	Win10x64_10240_17770 - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)	
13	Win10x64_10586 - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)	

展开

五，命令格式

`volatility -f [image] --profile=[profile] [plugin]`

`volatility -f [对象] --profile=[操作系统] [插件参数]`

在分析之前，需要先判断当前的镜像信息，分析出是哪个操作系统 命令 `imageinfo` 即可获取镜像信息。

`Volatility -f xxx.vmem imageinfo`

在查到操作系统后如果不确定可以使用以下命令查看

`volatility -f xxx.vmem --profile= [操作系统] volshell`

举个例子 像这种什么都找不到 什么都

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区

路baby

关注

打赏

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x86 volshell
Volatility Foundation Volatility Framework 2.6
No suitable address space mapping found
Tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64FitMap: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VMWareMetaAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
Win10AMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64FitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VMWareMetaAddressSpace: VMware metadata file is not available
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf000ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
Win10AMD64PagedMemory: Incompatible profile Win7SP1x86 selected
WindowsAMD64PagedMemory: Incompatible profile Win7SP1x86 selected
LinuxAMD64PagedMemory: Incompatible profile Win7SP1x86 selected
AMD64PagedMemory: Incompatible profile Win7SP1x86 selected
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found
```

CSDN @路baby

像这种就是合格的

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP0x64 volshell
Volatility Foundation Volatility Framework 2.6
Current context: System @ 0xfffffa8018d45740, pid=4, ppid=0 DTB=0x187000
Welcome to volshell! Current memory image is:
file:///F:/%C4%DA%B4%E6%C8%A1%D6%A4/%D0%C2%BD%A8%CE%C4%BC%FE%BC%D0/misc-%C4%DA%B4%E6%C8%A1%D6%A4/%C8%ED%
BC%FE/1.vmem
To get help, type 'hh()'
>>> -
```

CSDN @路baby

当我们确定操作系统就可以利用插件去做题了

六、常用命令插件

♥可以先查看当前内存镜像中的用户 **printkey -K "SAM\Domains\Account\Users\Names"**

```
volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
```

♥查看用户名密码信息(密码是哈希值，需要john爆破) **hashdump**

```
volatility -f 1.vmem --profile=Win7SP1x64 hashdump
```

查看当前操作系统中的 password hash，例如 Windows 的 SAM 文件内容(mimikatz插件可

♥如果john爆破不出来，就使用 **lsadmp** 查看强密码 **lsadump**

```
volatility -f 1.vmem --profile=Win7SP1x64 lsadump
```

♥查看进程 **pslist**



路baby

关注

登录后您可以享受以下权益：

📄 免费复制代码

👍 和博主大V互动

📁 下载海量资源

✍ 发动态/写文章/加入社区

打赏

```
volatility -f 1.vmem --profile=Win7SP1x64 pslist
```

pslist: 该插件列举出系统进程，但它不能检测到隐藏或者解链的进程，psscan可以

♥查看已知进程pslist

```
volatility -f 1.vmem --profile=Win7SP1x64 pslist -p 2588
```

♥隐藏或解链的进程psscan

```
volatility -f 1.vmem --profile=Win7SP1x64 psscan
```

psscan: 可以找到先前已终止(不活动)的进程以及被rootkit隐藏或解链的进程

♥查看服务 查询服务名称svcsan

```
volatility -f 1.vmem --profile=Win7SP1x64 svcsan
```

svcsan: 扫描 Windows 的服务

♥查看浏览器历史记录,获取当前系统浏览器搜索过的关键词 iehistory

```
volatility -f 1.vmem --profile=Win7SP1x64 iehistory
```

♥查看网络连接 获取当前系统 ip netscan

```
volatility -f 1.vmem --profile=Win7SP1x64 netscan
```

有一些版本 这个命令是使用不了 这里我们就要使用 (connscan,connections)

♥查看网络连接connscan

```
volatility -f 1.vmem --profile=Win7SP1x64 connscan
```

connscan: 查看网络连接

♥查看网络连接connections

```
volatility -f 1.vmem --profile=Win7SP1x64 connections
```

connections: 查看网络连接

♥查看命令行操作，显示cmd历史命令 cmdscan

```
volatility -f 1.vmem --profile=Win7SP1x64 cmdscan
```

cmdscan: 可用于查看终端记录

♥查看进程命令行参数（具体一些可疑进程的参数指令） cmdline

```
volatility -f 1.vmem --profile=Win7SP1x64 cmdline
```

♥扫描所有的文件列表 filesan

```
volatility -f 1.vmem --profile=Win7SP1x64 filesan
```

(linux配合 grep 命令进行相关字符定向扫描，如：grep



路baby

关注

登录后您可以享受以下权益：



免费复制代码



和博主大V互动



下载海量资源



发动态/写文章/加入社区

打赏

例

```
volatility -f 1.vmem --profile=Win7SP1x64 filescan grep "flag.txt"
```

```
cat system.txt|grep -i computername
```

♥查看文件内容dmpfiles

```
volatility -f 1.vmem --profile=Win7SP1x64 dmpfiles -Q 0xxxxxxx -D ./
```

需要指定偏移量 -Q 和输出目录 -D

dmpfiles：导出某一文件(指定虚拟地址)

♥查看当前展示的notepad内容 notepad

```
volatility -f 1.vmem --profile=Win7SP1x64 notepad
```

查看当前展示的 notepad 文本（--profile=winxp啥的低版本可以，win7的不行，可以尝试使用editbox）

♥显示有关编辑控件（曾经编辑过的内容）的信息 editbox

```
volatility -f 1.vmem --profile=Win7SP1x64 editbox
```

editbox：显示有关编辑控件（曾经编辑过的内容）的信息 查看内存中记事本的内容

♥提取进程memdump

```
volatility -f 1.vmem --profile=Win7SP1x64 memdump -p xxx --dump-dir=./
```

memdump：提取出指定进程，常用foremost 来分离里面的文件

需要指定进程-p [pid] 和输出目录 -D

```
memdump -p 332 -D XX/
```

提取进程 -p 进程号 -D 当前输出路径（导出为332.dmp）

dump出来的进程文件，可以使用 foremost 来分离里面的文件，用 binwak -e 不推荐

```
strings -e l 2040.dmp | grep flag 查找flag
```

♥屏幕截图screenshot

```
volatility -f 1.vmem --profile=Win7SP1x64 screenshot --dump-dir=./
```

screenshot：保存基于GDI窗口的伪截屏

♥查看注册表配置单元hivelist

```
volatility -f 1.vmem --profile=Win7SP1x64 hivelist
```

hivelist：列出所有的注册表项及其虚拟地址和物理地址

♥查看注册表键名hivedmp

```
volatility -f 1.vmem --profile=Win7SP1x64 hivedump -o 0xfffff8a001032410
```

♥查看注册表键值printkey

```
volatility -f 1.vmem --profile=Win7SP1x64 printkey
```

登录后您可以享受以下权益：

📄 免费复制代码

👍 和博主大V互动

📁 下载海量资源

✍ 发动态/写文章/加入社区



路baby

关注

打赏

♥ 获取主机名 **printkey**

```
volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "ControlSet001\Control\ComputerName\ComputerName"
```

♥ 列出用户名 **pringkey**

```
volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
```

♥ 查看运行程序相关的记录，比如最后一次更新时间，运行过的次数等。 **serassist**

```
volatility -f 1.vmem --profile=Win7SP1x64 userassist
```

♥ 最大程序提取信息 **timeliner**

```
volatility -f 1.vmem --profile=Win7SP1x64 timeliner
```

timeliner: 将所有操作系统事件以时间线的方式展开

♥ 查看剪贴板信息 **clipboard**

```
volatility -f 1.vmem --profile=Win7SP1x64 clipboard
```

clipboard: 查看剪贴板信息

♥ 显示关于计算机及其操作系统的详细配置信息（插件） **systeminfo**

```
volatility -f 1.vmem --profile=Win7SP1x64 systeminfo
```

systeminfo: 显示关于计算机及其操作系统的详细配置信息（插件）

♥ 恢复被删除的文件 **mftparser**

```
volatility -f 1.vmem --profile=Win7SP1x64 mftparser
```

mftparser: 恢复被删除的文件

♥ 查看环境变量 **envvars**

```
volatility -f 1.vmem --profile=Win7SP1x64 envvars
```

envvars: 查看环境变量

♥ 列出某一进程加载的所有dll文件 **dlllist**

```
volatility -f 1.vmem --profile=Win7SP1x64 dlllist -p 2588
```

dlllist: 列出某一进程加载的所有dll文件

需要指定进程-p [pid]

♥ 程序版本信息 **verinfo**

```
volatility -f 1.vmem --profile=Win7SP1x64 verinfo
```

列出PE | 程序版本信息

♥ 查看进程树，可以轻松了解各进程之间的关系：



路baby

关注

登录后您可以享受以下权益：

📄 免费复制代码

👍 和博主大V互动

📁 下载海量资源

✍ 发动态/写文章/加入社区

打赏

```
volatility -f 2008.raw --profile=Win2008R2SP1x64 pstree
```

在进程中PPID比PID还大, 那就可能这个进程有异常程序

♥从内存文件中找到异常程序植入到系统的开机自启痕迹 shimcache

```
volatility -f 2008.raw --profile=Win2008R2SP1x64 shimcache
```

七, 内存取证的大致思路

首先确定镜像是何种操作系统的, 命令imageinfo即可获取镜像信息。

需要获取的是计算机在这一时刻运行了哪些进程。

Volatility提供了众多的分析进程的命令, 如pstree、pesscan、pslist.....

filesca命令可以对打开的文件进行扫描。

命令dumpfile和memdump命令将相关数据导出, 然后对导出的数据进行二进制分析。

简单说只要熟悉Volatility工具的常用命令, 并能够对结合其他类型的知识 (图片隐写、压缩包分析等) 对提取出的文件进行分析, 便可轻松解决。

但当然具体问题具体分析吗 但插件就上面的

八, 例题讲解

这里我们就找两个典型例题 讲解一下哦

题目一

是46届世界技能大赛湖北省选拔赛 也是今年金砖比赛的样题

链接: <https://pan.baidu.com/s/1tYglicQjExmaMLYa3YeSA>

提取码: lulu

你作为 A 公司的应急响应人员, 请分析提供的内存文件按照下面的要求找到 相关关键信息, 完成应急响应事件。

- 1、从内存中获取到用户admin的密码并且破解密码, 以Flag{admin,password} 形式提交(密码为 6 位);
- 2、获取当前系统 ip 地址及主机名, 以 Flag(ip:主机名)形式提交;
- 3、获取当前系统浏览器搜索过的关键词, 作为 Flag 提交;
- 4、当前系统中存在挖矿进程, 请获取指向的矿池地址, 以 Flag(ip:端口)形式 提交;
- 5、恶意进程在系统中注册了服务, 请将服务名以 Flag(服务名)形式提交。

上题已经看到进程

解析

1.从内存中获取到用户admin的密码并且破解密码, 以Flag{admin,password} 形式提交(密码为 6 位);

不管什么题内存取证的第一步肯定是要去判断当前的镜像信息, 分析出是哪个操作系统 使用参数 imageinfo 查看系统信息

```
volatility -f 1.vmem imageinfo
```

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility debug : Determining profile based on KDBG search
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (F:\内存取证\新建文件夹\misc-内存取证\软件\1.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80004044070L
Number of Processors : 1
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffff80004045d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-06-10 10:34:38 UTC+0000
Image local date and time : 2019-06-10 18:34:38 +0800
```

操作系统我们一般取第一个就可以了

接下来就可以输入参数

可以先查看当前内存镜像中的用户

```
volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
```

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2019-06-07 04:37:21 UTC+0000

Subkeys:
(S) admin
(S) Administrator
(S) Guest

Values:
REG_DWORD : (S) 0
```

CSDN @路baby

使用hashdump获取sam

```
volatility -f 1.vmem --profile=Win7SP1x64 hashdump
```

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:29fb61bd2963b1975cf435a2565af910:::
```

CSDN @路baby

可以通过john工具来进行

好像跑不出来结果。应该是设定了强密码。于是只能使用了lsadump命令来查看

```
volatility -f 1.vmem --profile=Win7SP1x64 lsadump
```

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 L.....
0x00000010 66 00 6c 00 61 00 67 00 7b 00 34 00 30 00 36 00 f.l.a.g.{.4.0.6.
0x00000020 39 00 39 00 30 00 66 00 66 00 38 00 38 00 66 00 9.9.0.f.f.8.8.f.
0x00000030 31 00 33 00 64 00 61 00 63 00 33 00 63 00 39 00 1.3.d.a.c.3.c.9.
0x00000040 64 00 65 00 62 00 62 00 63 00 30 00 37 00 36 00 d.e.b.b.c.0.7.6.
0x00000050 39 00 35 00 38 00 38 00 63 00 7d 00 00 00 00 00 9.5.8.8.c.}.....

OPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 01 00 00 00 22 0c 11 ce 0e f5 6b c9 f3 4e 83 b0 ....".k.N.
0x00000020 8c 0f 9e 75 79 4e 6f 6a 2e 78 8c 18 2e 81 74 3b ...uyNoj.x...t;
0x00000030 bb 2c 09 a5 bb b2 5d a3 3f 1e 79 09 00 00 00 00 .....].?.y.....
```

CSDN @路baby

输入让你无语的MD5

解密

md5

dfsddew

```
flag{admin.dfsddew}
```

2.获取当前系统 ip 地址及主机名，以 Flag{ip:主机名}形式提交；

Netscan 可以查ip

```
volatility -f 1.vmem --profile=Win7SP1x64 netscan
```



路baby

关注

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区

```

F:\内存取证\新建文件夹\misc-内存取证\软件>Volatility -f 1.vmem --profile=Win7SP1x64 netstat
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xfffff8a000c78010 0x000000005ce3d010 \SystemRoot\System32\Config\SECURITY
0xfffff8a000ce3010 0x000000005745d010 \SystemRoot\System32\Config\SAM
0xfffff8a000e1b010 0x000000004ec81010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000eab210 0x00000000609a3210 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001508010 0x000000004018a010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a001569010 0x000000003a00d010 \??\C:\Users\admin\ntuser.dat
0xfffff8a0016f9010 0x00000000443a4010 \??\C:\Users\admin\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002f58420 0x0000000063533420 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010 0x0000000007082010 [no name]
0xfffff8a000024010 0x00000000070cd010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000052330 0x000000000707b330 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00010c010 0x000000000558d010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000b5e010 0x000000005b340010 \SystemRoot\System32\Config\SOFTWARE

```

CSDN @路baby

Ip:192.168.85.129

主机名需要通过查询注册表, 先用hivelist

Volatility -f 1.vmem --profile=Win7SP1x64 hivelist

```

F:\内存取证\新建文件夹\misc-内存取证\软件>Volatility -f 1.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xfffff8a000c78010 0x000000005ce3d010 \SystemRoot\System32\Config\SECURITY
0xfffff8a000ce3010 0x000000005745d010 \SystemRoot\System32\Config\SAM
0xfffff8a000e1b010 0x000000004ec81010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000eab210 0x00000000609a3210 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001508010 0x000000004018a010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a001569010 0x000000003a00d010 \??\C:\Users\admin\ntuser.dat
0xfffff8a0016f9010 0x00000000443a4010 \??\C:\Users\admin\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002f58420 0x0000000063533420 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010 0x0000000007082010 [no name]
0xfffff8a000024010 0x00000000070cd010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000052330 0x000000000707b330 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00010c010 0x000000000558d010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000b5e010 0x000000005b340010 \SystemRoot\System32\Config\SOFTWARE

```

CSDN @路baby

然后我们需要一步一步去找键名

volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey

```

F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5} (S)
Last updated: 2019-06-07 04:39:22 UTC+0000

Subkeys:
(S) ControlSet001
(S) ControlSet002
(S) MountedDevices
(S) RNG
(S) Select
(S) Setup
(S) WPA
(V) CurrentControlSet

Values:
F:\内存取证\新建文件夹\misc-内存取证\软件>

```

profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001"



路baby

关注

登录后您可以享受以下权益:

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ControlSet001 (S)
Last updated: 2019-06-07 04:34:15 UTC+0000

Subkeys:
(S) Control
(S) Enum
(S) Hardware Profiles
(S) Policies
(S) services

Values:
```

CSDN @路baby

继续

volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control"

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: Control (S)
Last updated: 2019-06-07 04:39:30 UTC+0000

Subkeys:
(S) ACPI
(S) AGP
(S) AppID
(S) Arbiters
(S) BackupRestore
(S) Class
(S) CMF
(S) CoDeviceInstallers
(S) COW_Name_Arbitr
(S) ComputerName
(S) ContentIndex
(S) CrashControl
(S) CriticalDeviceDatabase
(S) Cryptography
(S) DeviceClasses
(S) DeviceOverrides
(S) Diagnostics
(S) ELS
(S) Errata
(S) FileSystem
(S) FileSystemUtilities
```

CSDN @路baby

继续

volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control\ComputerName"

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control\ComputerName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2019-06-07 04:39:31 UTC+0000

Subkeys:
(S) ComputerName
(V) ActiveComputerName

Values:
```

CSDN @路baby

再来

volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control\ComputerName\ComputerName"

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 -o 0xfffff8a000024010 printkey -K "ControlSet001\Control\ComputerName\ComputerName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2019-06-07 04:34:14 UTC+0000

Subkeys:

Values:
REG_SZ : (S) _name_
REG_SZ : (S) WIN-9FBAEH4UV8C
```

CSDN @路baby

得到主机名WIN-9FBAEH4UV8C

也可以直接通过 hivedump查询相应的键名 但比较慢

volatility -f 1.vmem --profile=Win7SP1x64 hivedump -o 0xfffff8a000024010 > system.tx

3. 获取当前系统浏览器搜索过的关键词，作为 Flag 提交；

这里使用iehistory

登录后您可以享受以下权益：

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区



路baby

关注

打赏

volatility -f 1.vmem --profile=Win7SP1x64 iehistory

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 iehistory
Volatility Foundation Volatility Framework 2.6
*****
Process: 2208 explorer.exe
Cache type "DEST" at 0x4773e89
Last modified: 2019-06-07 13:44:58 UTC+0000
Last accessed: 2019-06-07 05:45:00 UTC+0000
URL: admin@file:///C:/Users/admin/Desktop/flag.txt
CSDN @路baby
```

flag{admin@file:///C:/Users/admin/Desktop/flag.txt}

4.当前系统中存在挖矿进程, 请获取指向的矿池地址, 以 Flag{ip :端口}形式提交;

volatility -f 1.vmem --profile=Win7SP1x64 netscan

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(IP) Proto Local Address Foreign Address State Pid Owner Created
0x7d41ced0 UDPv4 0.0.0.0:3355 ** 1088 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv6 ::::3355 ** 1088 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv4 0.0.0.0:123 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv6 ::::123 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv4 0.0.0.0:504 ** 504 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv6 ::::504 ** 504 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv4 192.168.85.129:1900 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv6 fe80::956c:2834:441:73be:1900 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:445 ** 520 lsass.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::445 ** 520 lsass.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:445 ** 4 System 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::445 ** 4 System 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49155 ** 512 services.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::49155 ** 512 services.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49155 ** 512 services.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::49155 ** 512 services.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49154 ** 944 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::49154 ** 944 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 192.168.85.129:49163 ** 2588 svchost.exe 2019-06-07 04:41:33 UTC+0000
0x7d41ced0 TCPv6 fe80::956c:2834:441:73be:49163 ** 2588 svchost.exe 2019-06-07 04:41:33 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:135 ** 740 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv6 ::::135 ** 740 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49152 ** 412 wininit.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv6 ::::49152 ** 412 wininit.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49153 ** 792 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv6 ::::49153 ** 792 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv4 192.168.85.129:138 ** 4 System 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv6 ::::138 ** 4 System 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv4 0.0.0.0:0 ** 1088 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv6 ::::0 ** 1088 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv4 127.0.0.1:60214 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv4 192.168.85.129:1900 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv4 192.168.85.129:139 ** 4 System 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 TCPv6 ::::139 ** 4 System 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv4 192.168.85.129:137 ** 4 System 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv6 fe80::956c:2834:441:73be:137 ** 4 System 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv4 127.0.0.1:1900 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv6 ::::1900 ** 2104 svchost.exe 2019-06-10 10:31:19 UTC+0000
0x7d41ced0 UDPv4 0.0.0.0:123 ** 504 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv6 ::::123 ** 504 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 UDPv4 0.0.0.0:3355 ** 1088 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv4 0.0.0.0:49156 ** 520 lsass.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv6 ::::49156 ** 520 lsass.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv4 116.207.167.180 ** 944 svchost.exe 2019-06-10 10:31:23 UTC+0000
0x7d41ced0 TCPv6 ::::116.207.167.180 ** 944 svchost.exe 2019-06-10 10:31:23 UTC+0000
```

唯一已建立的

flag{54.36.109.161:2222}

5.恶意进程在系统中注册了服务, 请将服务名以 Flag{服务名}形式提交。

上一题中已经知道了进程号为2588

volatility -f 1.vmem --profile=Win7SP1x64 pslist -p 2588

```
F:\内存取证\新建文件夹\misc-内存取证\软件>volatility -f 1.vmem --profile=Win7SP1x64 pslist -p 2588
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Tids Hnds Sess Wow64 Start Exit
0xfffffa80193f37e0 svchost.exe 2588 3036 8 81 0 0 2019-06-10 10:32:19 UTC+0000
CSDN @路baby
```

查到父进程是3036

然后通过svcsn可以查询服务名称, 找到对应服务名

volatility -f 1.vmem --profile=Win7SP1x64 svcsn

```
Offset: 0xdae120
Order: 398
Start: SERVICE_AUTO_START
Process ID: 3036
Service Name: VMnetDHCP
Display Name: VMware DHCP Service
Service Type: SERVICE_INTERACTIVE_PROCESS, SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\ProgramData\VMnetDHCP\loader.exe
```

flag{VMnetDHCP}

加油各位(・ω・)y 期待与君再相逢



路baby

关注

登录后您可以享受以下权益:

免费复制代码

和博主大V互动

下载海量资源

发动态/写文章/加入社区