

2021-内存取证wp

原创

Maya_Soy 于 2021-06-15 15:22:32 发布 688 收藏 9

分类专栏: [内存取证 Kali volatility](#) 文章标签: [python kali](#)

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/Maya_Soy/article/details/117924561

版权



[内存取证](#) 同时被 3 个专栏收录

1 篇文章 0 订阅

订阅专栏



[Kali](#)

1 篇文章 0 订阅

订阅专栏



[volatility](#)

1 篇文章 0 订阅

订阅专栏

使用工具

volatility WinHex

1. 从内存中获取到用户admin的密码并且破解密码,作为flag提交;

使用imageinfo得到操作系统

volatility.exe -f E:\网络安全\volatility\1.vmem imageinfo

```
PS E:\2021网络安全\volatility_2.6_win04_standalone> .\volatility_2.6_win04_standalone.exe -f E:\2021网络安全\volatility_2.6_win04_standalone\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 (E:\2021网络安全\volatility_2.6_win04_standalone\1.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800040580x0L
Number of Processors : 1
Image Type (Service Pack) : 1
EPCR for CPU 0 : 0xfffff80004059400L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2020-10-15 06:34:03 UTC+0000
Image local date and time : 2020-10-15 14:34:03 +0800
PS E:\2021网络安全\volatility_2.6_win04_standalone>
```

使用hashdump得到密码hash

volatility.exe -f E:\网络安全\volatility\1.vmem --profile=Win7SP1x64 hashdump

```
image date and time : 2020-10-15 00:34:03 UTC+0800
image local date and time : 2020-10-15 14:34:03 +0800
PS E:\2021网络安全\volatility_2.0_win64_standalone> .\volatility_2.0_win64_standalone.exe -f E:\2021网络安全\volatility_2.0_win64_standalone\1.vmem --profile=Win7SP1x64 hzhdump
Volatility Foundation Volatility Framework 2.0
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5947e0c089e0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5947e0c089e0:::
test:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5947e0c089e0:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:aef4a59b219c8e8c8aa2ca7b3ba9b7dc:::
PS E:\2021网络安全\volatility_2.0_win64_standalone>
```

使用hashcat破解密码hash，得到明文密码

```
(rootkali) ~
└─$ hashcat -s 3 -m 1000 acf4a59b219c8e8c8aa2ca7b3ba9b7dc 7a7a7a7a7a --force
hashcat (v6.1.1) starting ...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i7-7700K CPU B 4.20GHz, 1423/1487 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found in potfile! Use --show to display them.

Started: Tue Jun 15 01:33:28 2021
Stopped: Tue Jun 15 01:33:29 2021

(rootkali) ~
└─$ hashcat -s 3 -m 1000 acf4a59b219c8e8c8aa2ca7b3ba9b7dc 7a7a7a7a7a --force --show
acf4a59b219c8e8c8aa2ca7b3ba9b7dc:Hbcker

https://blog.csdn.net/Maya_Soy
```

2. 获得当前系统的主机名，将主机名作为flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 hivelist
```

```
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Virtual Physical Name
0xfffff8a0000f010 0x00000000234ed010 [no name]
0xfffff8a000024010 0x0000000023538010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000061010 0x00000000234f7010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000d3b010 0x000000001c966010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000d51010 0x000000001be7a010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000fa6010 0x000000001e5010 \SystemRoot\System32\Config\SECURITY
0xfffff8a001032410 0x00000000081c9110 \SystemRoot\System32\Config\SAM
0xfffff8a00109b410 0x0000000008000410 ??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a0010be010 0x0000000011cec010 ??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001727010 0x00000000351dd010 ??\C:\Users\test\ntuser.dat
0xfffff8a00178e010 0x00000000379f3010 ??\C:\Users\test\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a001878410 0x0000000070e34010 ??\C:\System Volume Information\Syscache.hve
0xfffff8a003276010 0x0000000014a03010 \SystemRoot\System32\Config\DEFAULT

(rootkali) ~\Desktop\volatility
└─$ python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 hivelist

https://blog.csdn.net/Maya_Soy
```

```
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2020-08-03 02:49:17 UTC+0800

Subkeys:

Values:
REG_SZ ComputerName : (S) TEST-PC
REG_SZ ComputerName : (S) mmsrvc

(rootkali) ~\Desktop\volatility
└─$ python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 printkey -o 0xfffff8a000024010 -x "ControlSet001\Control\ComputerName\Compu
terName"

https://blog.csdn.net/Maya_Soy
```

3. 获取当前系统浏览器搜索过的关键词，作为Flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 iehistory
```

```
root@kali: ~/Desktop/volatility
python vol.py -f /root/Desktop/1.vmem --profile=win7SP1x64 iehistory
```

```
File Offset: 0x200, Data Offset: 0x0, Data Length: 0x400
*****
Process: 1092 ieexplor.exe
Cache type "URL" at 0x26a5580
Record length: 0x180
Location: Visited: admin@http://cn.bing.com/search?q=sdfdasfulip123&form=PRCNZ&ocid=iehp&httpsmsn=1&msnews=1&refig=30371a07b20949789dbe8fab6ef7e873
Last modified: 2021-06-15 05:43:09 UTC+0000
Last accessed: 2021-06-15 05:43:09 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0xf4
*****
```

4. 当前系统中存在挖矿进程，请获取指向的矿池地址，作为Flag提交；

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 netscan
```

```
0x3d9199f0 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 412 svchost.exe
0x3d913d00 TCPv4 0.0.0.0:49153 0.0.0.0:0 LISTENING 820 svchost.exe
0x3d913d00 TCPv6 :::49153 :::0 LISTENING 820 svchost.exe
0x3d913d00 TCPv4 0.0.0.0:49153 0.0.0.0:0 LISTENING 820 svchost.exe
0x3d9199f0 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 412 wininit.exe
0x3d9199f0 TCPv6 :::49152 :::0 LISTENING 412 wininit.exe
0x3d91ba90 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 412 wininit.exe
0x3ec526f0 TCPv4 192.168.127.128:49292 94.230.165.85:5555 ESTABLISHED 2368 l.exe

root@kali: ~/Desktop/volatility
python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 netscan
```

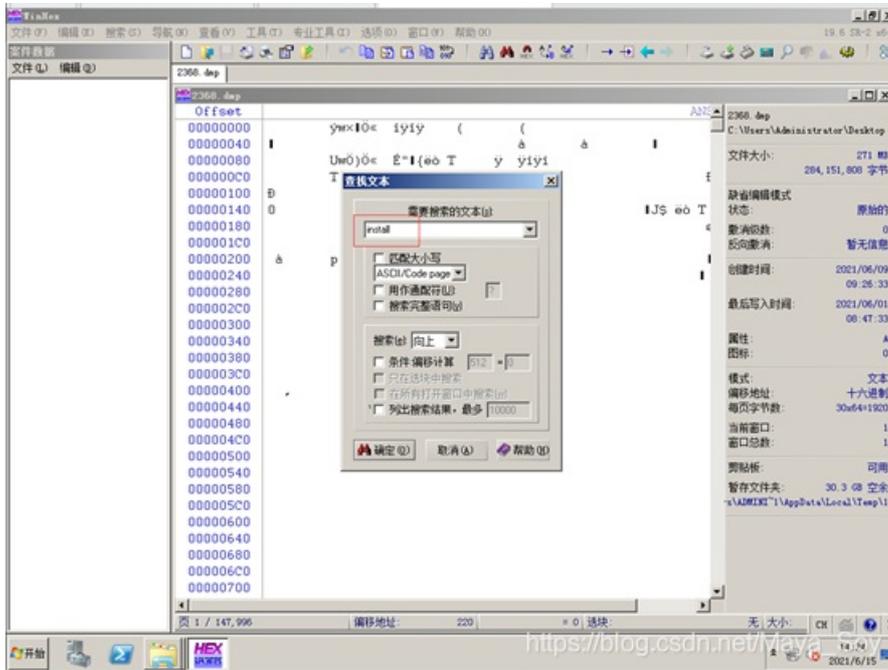
5. 恶意进程在系统中注册了服务，请将服务名以Flag{服务名}形式提交。

将进程导出来，然后使用Winhex分析

```
File Actions Edit View Help
0x3d9199f0 TCPv6 :::0 LISTENING 412 wininit.exe
0x3d91ba90 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 412 wininit.exe
0x3ec526f0 TCPv4 192.168.127.128:49292 94.130.165.85:5555 ESTABLISHED 2368 1.exe

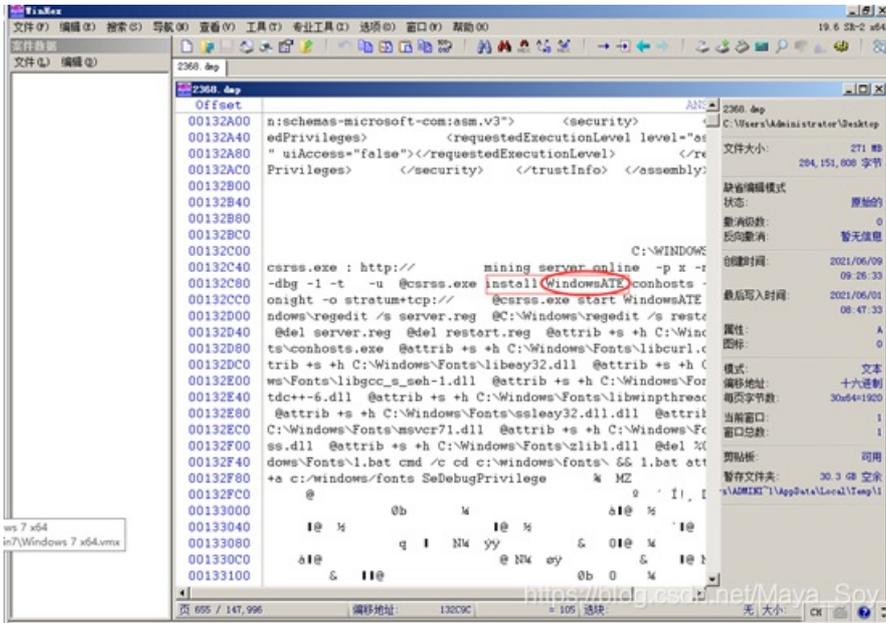
root@kali:~/Desktop/volatility# python vol.py --root/Desktop/1.mem --profile=win7SP1x64 memdump -p 2368 -o 2368
Volatility Foundation Volatility Framework 2.6.1
** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
** 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.getsysids (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.evtflogs (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.tcaudit (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.malware.threads (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
** 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.ssdts (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Writing 1.exe [ 2368 ] to 2368.dmp
```

https://blog.csdn.net/Maya_Soy



https://blog.csdn.net/Maya_Soy

flag{WindowsATE}



6. 黑客在登录系统后下载了文件，请将文件内容作为flag提交：

```
python -f vol.py /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
```

```
(root@kali)~/Desktop/volatility
# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
Volatility Foundation Volatility Framework 2.6.1
0x000000003b33fb70 16 0 R-rwd \Device\HarddiskVolume2\Users\test\Desktop\flag.txt
0x0000000039cc588 2 0 R-rw- \Device\HarddiskVolume2\Users\test\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk

(root@kali)~/Desktop/volatility
# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 filescan | grep flag
```

```
(root@kali)~/Desktop/volatility
# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000003b33fb70 -D ./
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.apihooks (NameError: name 'distorm3' is not defined)
*** 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.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.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.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcsan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdtd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
DataSectionObject 0x3b33fb70 None \Device\HarddiskVolume2\Users\test\Desktop\flag.txt

(root@kali)~/Desktop/volatility
# python vol.py -f /root/Desktop/1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000003b33fb70 -D ./
```

https://blog.csdn.net/Maya_Soy

```
(root@kali)~/Desktop/volatility
# ls
2368.dmp CHANGELOG.txt file.None.0xfffffa800f6b6200.dat LICENSE.txt PKG-INFO README.txt tools
AUTHORS.txt CONTRIB file.None.0xfffffa800f6b6200.dat Makefile pyinstaller resources volatility
BUILD CREDITS.txt LEGAL.txt MANIFEST.in pyinstaller.spec setup.py volatility.egg-info

(root@kali)~/Desktop/volatility
# cat file.None.0xfffffa800f6b6200.dat
flag{dasdqwdxczaqwcascas}

(root@kali)~/Desktop/volatility
#
```

https://blog.csdn.net/Maya_Soy