

内存取证_CTF

原创

此笙 于 2021-09-15 10:45:05 发布 429 收藏 2

分类专栏: [CTF](#) 文章标签: [linux](#)

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/a1912993110/article/details/120301948>

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

内存取证

1. 获取内存镜像信息, 获取系统版本

```
volatility -f 1.raw imageinfo
```

```
(root@kali) - [~/桌面]
# volatility -f 1.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86 WinXPSP3x86 (Instantiated with
inXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/root/桌面/1.raw)
PAE type : PAE
DTB : 0xb00000L
KDBG : 0x8054d2e0L
Number of Processors : 1
Image Type (Service Pack) : 2
KPCR for CPU 0 : 0xffdff000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2021-09-08 05:30:23 UTC+0000
Image local date and time : 2021-09-08 13:30:23 +0800
CSDN @此笙
```

2. 查看进程信息

```
volatility -f 1.raw --profile=WinXPSP2x86 pslist
```

```
(root@kali)-[~/桌面]
└─# volatility -f 1.raw --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64
Start Exit
-----
0x821b7830 System 4 0 53 248 0 0
0x81fe6cc0 smss.exe 512 4 3 21 0 0
2021-09-08 05:15:53 UTC+0000
0x81d32558 csrss.exe 580 512 11 370 0 0
2021-09-08 05:15:53 UTC+0000
0x81fdc998 winlogon.exe 604 512 15 421 0 0
2021-09-08 05:15:54 UTC+0000
0x81f93400 services.exe 704 604 16 279 0 0
2021-09-08 05:15:54 UTC+0000
0x820aca60 lsass.exe 716 604 20 348 0 0
2021-09-08 05:15:54 UTC+0000
0x820b5b60 vmacthlp.exe 868 704 1 24 0 0
2021-09-08 05:15:54 UTC+0000
0x81e311a0 svchost.exe 884 704 16 190 0 0
2021-09-08 05:15:54 UTC+0000
0x820c6b88 svchost.exe 940 704 11 255 0 0
2021-09-08 05:15:55 UTC+0000
0x82086b28 svchost.exe 1084 704 58 1129 0 0
2021-09-08 05:15:55 UTC+0000
```

留意可疑进程例如: cmd.exe (控制台) notepad.exe (记事本) StickyNot.exe(便笺) wab.exe (Windows联系人)

3.查看cmd.exe的使用情况

```
volatility -f 1.raw --profile=WinXPSP2x86 cmdscan
```

```
(root@kali)-[~/桌面]
└─# volatility -f 1.raw --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: csrss.exe Pid: 580
CommandHistory: 0x565c60 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x524
*****
CommandProcess: csrss.exe Pid: 580
CommandHistory: 0x566bb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x4cc
Cmd #0 @ 0x3689ed8: git push -u origin master
Cmd #1 @ 0x566148: ok...
Cmd #2 @ 0x56aa08: then delete .git and flagfile
Cmd #3 @ 0x368a798: You can never find my account
Cmd #4 @ 0x56a580: hahaha!
```

4.查看notepad.exe中的内容

```
volatility notepad -f 1.raw pslist --profile=WinXPSP2x86
```

5.提取可疑进程

```
volatility -f 1.raw --profile=Win7SP0x86 memdump -p 252 -D ./
```

1. --profile 的参数为系统版本
2. -p 的参数为进程ID
3. -D 的参数为保存文件路径

进程里面可能会隐藏flag等关键信息，可以使用以下命令检索.dmp文件

```
strings -e l 252.dmp | grep flag
```

6.扫描内存中的关键文件

```
volatility -f 1.raw --profile=WinXPSP2x86 filescan | grep 'P@ssw0rd_is_y0ur_bir7hd4y.zip'
```

7.导出文件

```
volatility -f 1.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000002c61318 -D ./
```

1. -Q的参数为内存地址
3. -D的参数为保存文件路径

8.列举用户及密码

```
volatility -f 1.raw --profile=WinXPSP2x86 hashdump
```

```
(root@kali)-[~/桌面]
└─# volatility -f 1.vmem --profile=Win7SP1x64 hashdump 1
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CTF:1000:aad3b435b51404eeaad3b435b51404ee:be5593366cb1019400210101581e5d0d:::
```

或者使用password kit forensic工具，一把梭

The screenshot shows the 'Recover File Password' application window. The main area displays details for 'Target.vmem', including its folder path (D:\Desktop\内存分析), file type (Windows users from a memory image), and complexity (Instant Unprotection). The MD5 hash is D0C314B9110482CFD96A649AD4820E77. Under the 'Accounts' section, a password is listed as 'WIN-QUN5RVOOF27\CTF' with a green highlight indicating a successful recovery: 'flag(W31C0M3 TO THiS 34SY F0R3NSiCX)'.

At the bottom of the window, a summary bar shows 'PASSWORDS FOUND: 1' and 'TIME ELAPSED: 42 seconds'. Action buttons include 'Print', 'Save Job', 'RESUME ATTACKS', 'SAVE REPORT', and 'DONE'. A watermark 'CSDN @此笙' is visible in the bottom right corner.

总结

近期通过CTF比赛对内存取证的一些认识