

week4-nse4u-wp

week4-nse4u-wp

misc

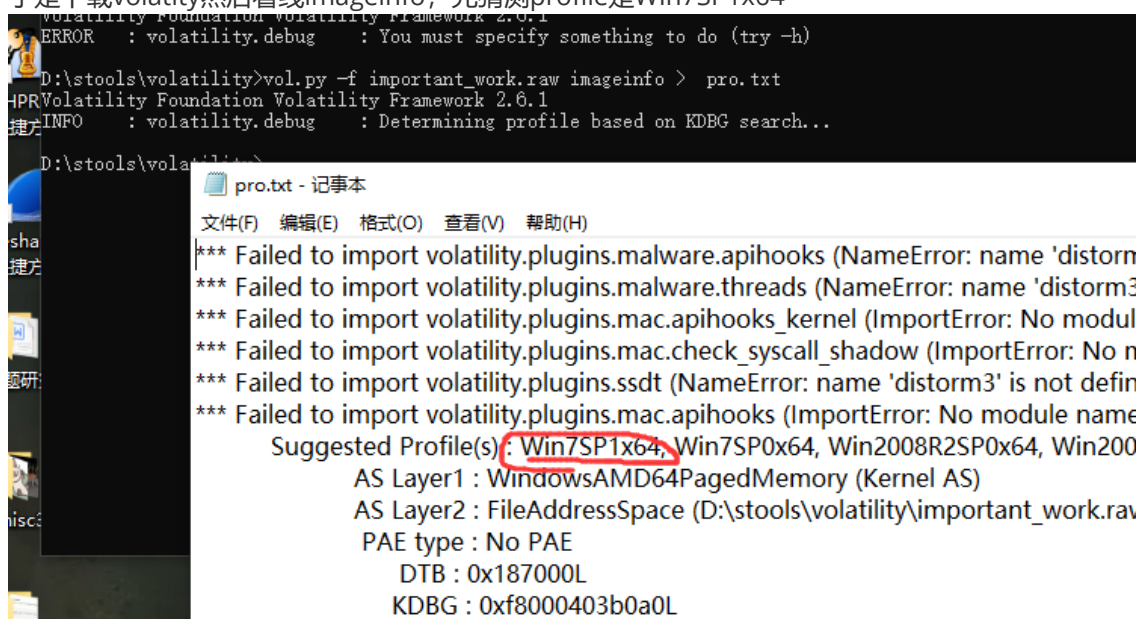
1. Akira之瞳

完结撒花

misc

1. Akira之瞳

1. 先下载下来，发现有一个raw文件，百度raw、dump、misc等关键字，得知这是要内存取证
2. 于是下载volatility然后看线imageinfo，先猜测profile是Win7SP1x64



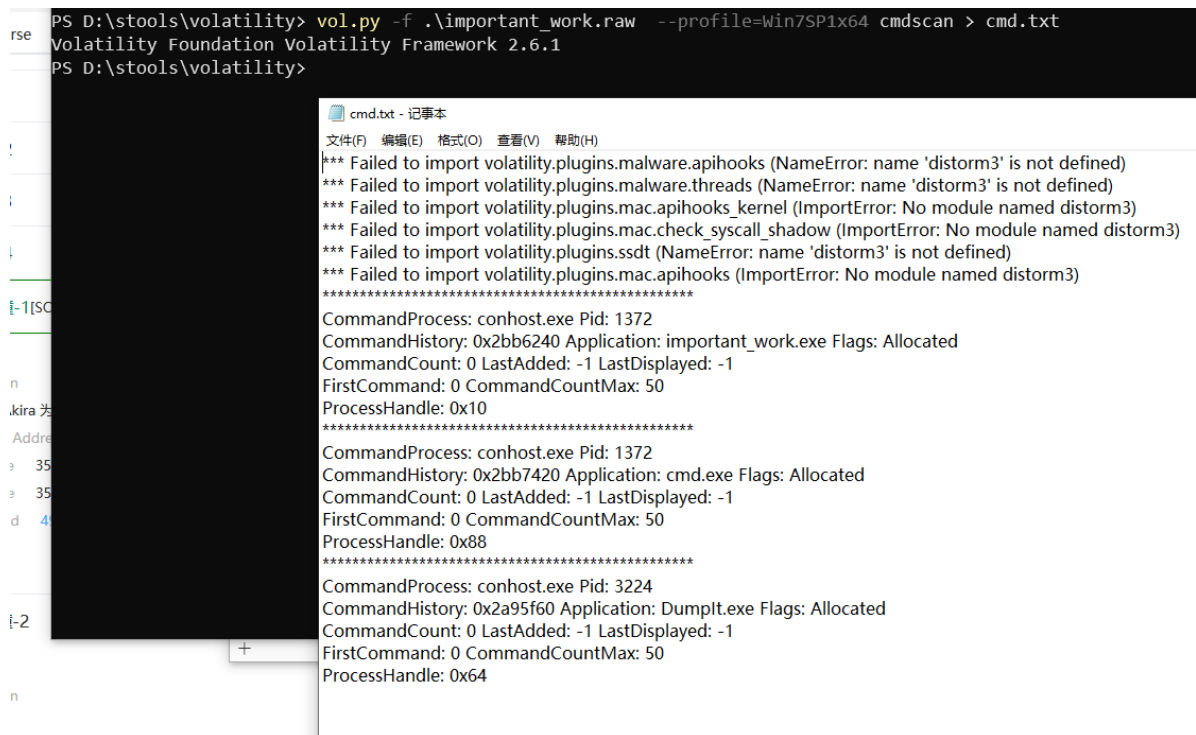
The screenshot shows a Windows command prompt window with the following text:

```
Volatility Foundation Volatility Framework 2.6.1
ERROR : volatility.debug : You must specify something to do (try -h)
D:\stools\volatility>vol.py -f important_work.raw imageinfo > pro.txt
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
```

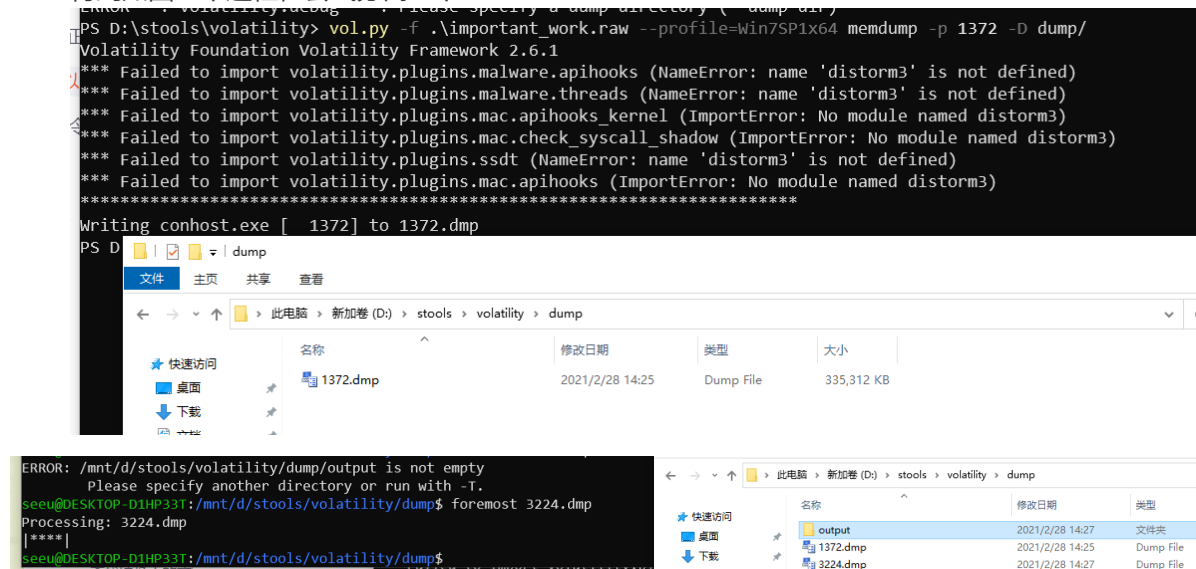
Below the command prompt, a Notepad window titled "pro.txt - 记事本" is open, displaying the output of the command. The text in the Notepad window is as follows:

```
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** 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.mac.check_syscall_shadow (ImportError: No module named 'distorm3')
*** Failed to import volatility.plugins.ssdtd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named 'distorm3')
Suggested Profile(s): Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (D:\stools\volatility\important_work.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf8000403b0a0L
```

3. 先试试看能不能找出当时在运行的程序啥的
4. 先看看cmd中运行了什么



5. 得到如图三个进程，尝试分离一下



6. 发现分出来都没啥用

7. 看看内存中的文件吧

```

0010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0030 00 00 80 bf 00 00 80 bf ff ff ff ff 50 4a 2a 49 .....PJ*I
0040 a5 05 d7 01 00 00 00 00 .....

```

ps>volatility>vol.py -f important_work.raw --profile=Win7SP1x64 userassist > inner.txt
 Volatility Foundation Volatility Framework 2.6.1

inner.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not d
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module n
*** Failed to import volatility.plugins.ssdtd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm

```

8. Registry: \??\C:\Users\Genga03\ntuser.dat
 Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4...

Subkeys:

Values:

```

REG_BINARY Microsoft.Windows.GettingStarted :
Count: 14
Focus Count: 21
Time Focused: 0:07:00.500000
Last updated: 2021-02-18 02:59:05 UTC+0000
Raw Data:
0x00000000 00 00 00 00 0e 00 00 00 15 00 00 00 a0 68 06 00 .....h..
0x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....

```

9. 发现似乎没啥用
10. 于是查看下进程

lists.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

0x00000000 520 508 11 235 1 0 2021-02-18 09:45:41 UTC+0000
0x00000001 568 500 14 283 0 0 2021-02-18 09:45:41 UTC+0000
0x00000002 576 500 10 618 0 0 2021-02-18 09:45:41 UTC+0000
0x00000003 584 500 11 167 0 0 2021-02-18 09:45:42 UTC+0000
0x00000004 680 508 7 139 1 0 2021-02-18 09:45:42 UTC+0000
0x00000005 720 568 13 411 0 0 2021-02-18 09:45:42 UTC+0000
0x00000006 780 568 3 59 0 0 2021-02-18 09:45:42 UTC+0000
0x00000007 820 568 7 315 0 0 2021-02-18 09:45:42 UTC+0000
0x00000008 896 568 21 455 0 0 2021-02-18 09:45:42 UTC+0000
0x00000009 940 568 23 487 0 0 2021-02-18 09:45:42 UTC+0000
0x0000000a 968 568 44 900 0 0 2021-02-18 09:45:42 UTC+0000

```

C:\Windows\System32\cmd.exe

```

Count: 16
Focused: 0
Updated: 2021-02-18 09:41:04 UTC+0000
Data:
000000 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 .....
000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
000030 00 00 80 bf 00 00 80 bf ff ff ff ff 10 69 00 2d .....l.-
000040 da 05 d7 01 00 00 00 00 .....

```

REG_BINARY \ALLUSERSPROFILE\Microsoft\Windows\Start Menu\Programs\7-Zip\7-Zip File Manager.lnk :

```

Count: 2
Focused: 0
Updated: 2021-02-18 03:22:28 UTC+0000
Data:
000000 00 00 00 00 02 00 00 00 00 00 00 00 02 00 00 00 .....
000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
000030 00 00 80 bf 00 00 80 bf ff ff ff ff 50 4a 2a 49 .....PJ*I
000040 a5 05 d7 01 00 00 00 00 .....

```

ps>volatility>vol.py -f important_work.raw --profile=Win7SP1x64 userassist > inner.txt
 Volatility Foundation Volatility Framework 2.6.1

ps>volatility>vol.py -f important_work.raw --profile=Win7SP1x64 pelist > lists.txt
 Volatility Foundation Volatility Framework 2.6.1

```

0x00000000 2572 568 13 251 0 0 2021-02-18 09:47:00 UTC+0000
0x00000001 2596 568 13 182 0 0 2021-02-18 09:47:00 UTC+0000
0x00000002 736 1252 7 245 1 0 2021-02-18 09:47:11 UTC+0000
0x00000003 2552 1252 5 101 0 0 2021-02-18 09:47:11 UTC+0000
0x00000004 1092 2232 1 16 1 1 2021-02-18 09:47:15 UTC+0000
0x00000005 1372 520 2 63 1 0 2021-02-18 09:47:16 UTC+0000
0x00000006 1340 1092 1 29 1 1 2021-02-18 09:47:16 UTC+0000
0x00000007 3128 720 6 102 1 0 2021-02-18 09:47:21 UTC+0000
0x00000008 3184 720 6 99 0 0 2021-02-18 09:47:22 UTC+0000
0x00000009 3216 2232 2 75 1 1 2021-02-18 09:47:22 UTC+0000
0x0000000a 3224 520 2 61 1 0 2021-02-18 09:47:22 UTC+0000

```

第 50 行, 第 29 列 100% Windows (CRLF) UTF-8

12. 在1092号进程中发现一个important_work,分离出来foremost一下,里面有很多文件夹,其中一个

zip文件有密码

```
00 4C 69 7A 20 74 ... ..Liz t
2F 73 72 63 2E 70 o Aoi Bird/src.p
01 00 18 00 F9 1F ng.. ....û.
D0 05 D7 01 F4 35 @9I.x.y-ts@.x.65
00 00 00 00 03 00 @9I.x.PK.....
25 00 EF BB BF 50 ..6...à¿e.%.i»¿P
20 73 68 61 32 35 assword is sha25
73 73 77 6F 72 64 6(login_password
)
```

13. 发现密码是登录密码的sha256, 这个important_work是画师在做的, 画师是最后一个登录的人, 那么最后一个登录的人的密码就是这里要密码

14. 于是hashdump一下密码

```
D:\stools\volatility>vol.py -f important_work.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** 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.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

15. 想了很久也不知道怎么解哈希, 找到一个在线解密网站, 解开了

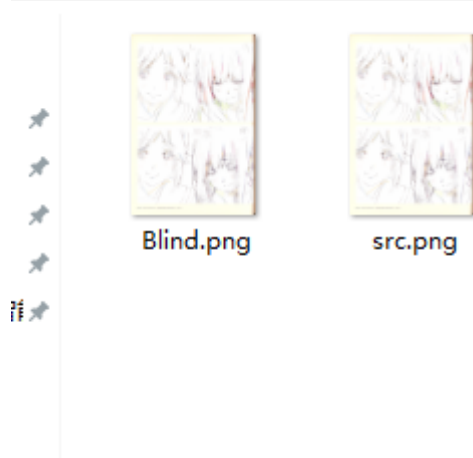
密文: 84b0d9c9f830238933e7131d60ac6436

类型: NTLM ▼ [\[帮助\]](#)

查询 加密

查询结果:
asdqwe123

16. 然后sha256一下, 打开压缩包, 发现是两张一样的图片, 看到blind和src想到盲水印



17. 于是盲水印走一波，得到图片，带到ps里放大看看得到flag

```
ImportError: No module named cv2  
D:\stools\BlindWater>python bwmforpy3.py decode src.png Blind.png 22.png  
18. image<src.png> + image(encoded)<Blind.png> -> watermark<22.png>  
S  
X
```



完结撒花
