CTF-朴实无华的内存取证

原创

烟涛微茫信难求 于 2022-01-11 21:35:40 发布 2723 收藏 1

分类专栏： CTF 文章标签： unctf 网络安全

本文链接：https://blog.csdn.net/qq_43611848/article/details/122441337

版权

CTF 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

题目描述

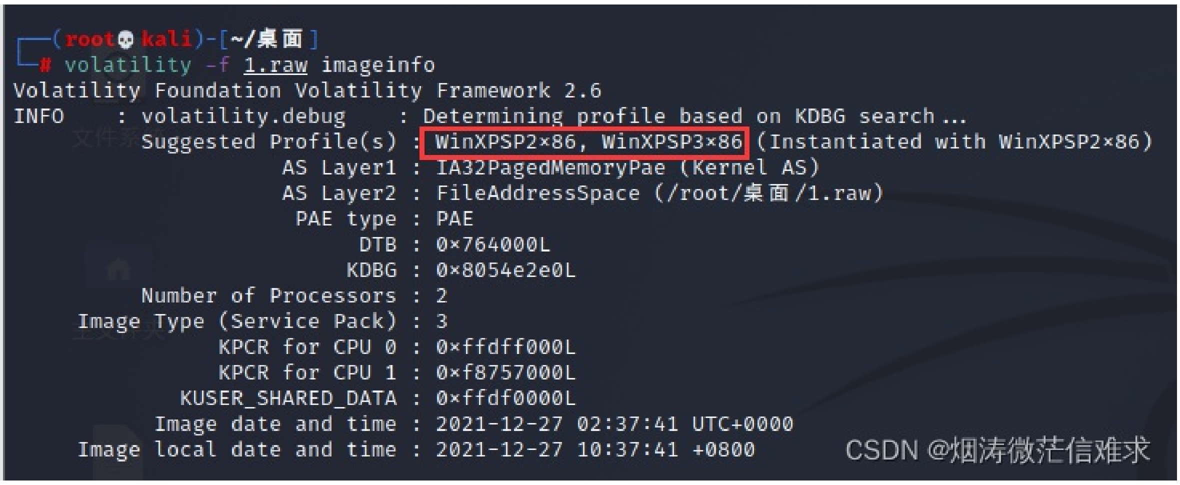
链接：https://pan.baidu.com/s/1dC4reO8opHQ3yZ8PdtD_AQ

提取码：lzsa

解题过程：

1.下载文件1.raw，放到kali里。

2.volatility -f 1.raw imageinfo

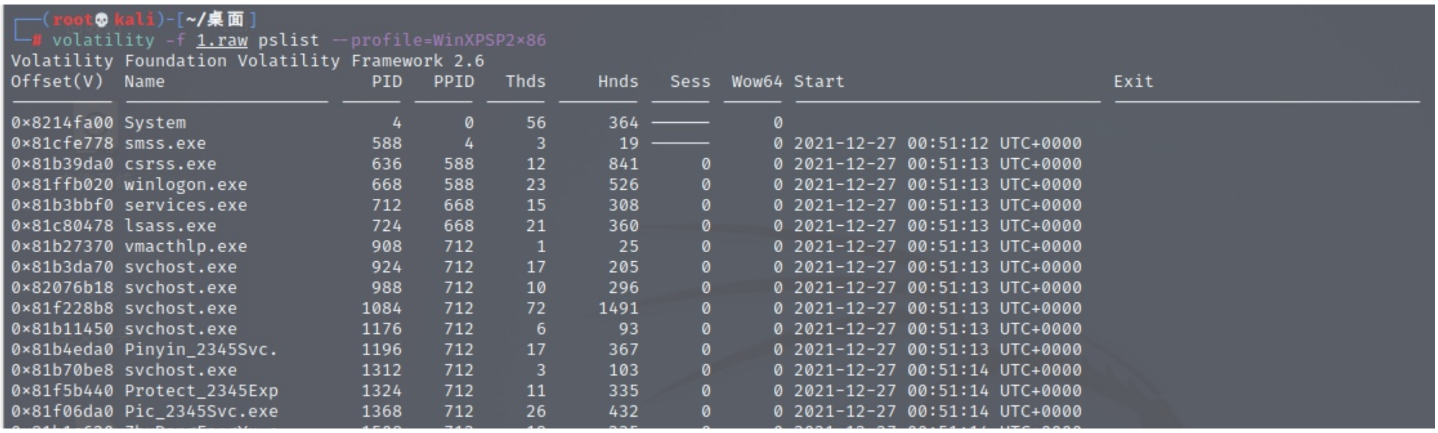


```
┌──(root💀kali)-[~/桌面]
└─# volatility -f 1.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/桌面/1.raw)
                      PAE type : PAE
                           DTB : 0x764000L
                          KDBG : 0x8054e2e0L
          Number of Processors : 2
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
                KPCR for CPU 1 : 0xf8757000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-12-27 02:37:41 UTC+0000
     Image local date and time : 2021-12-27 10:37:41 +0800
```

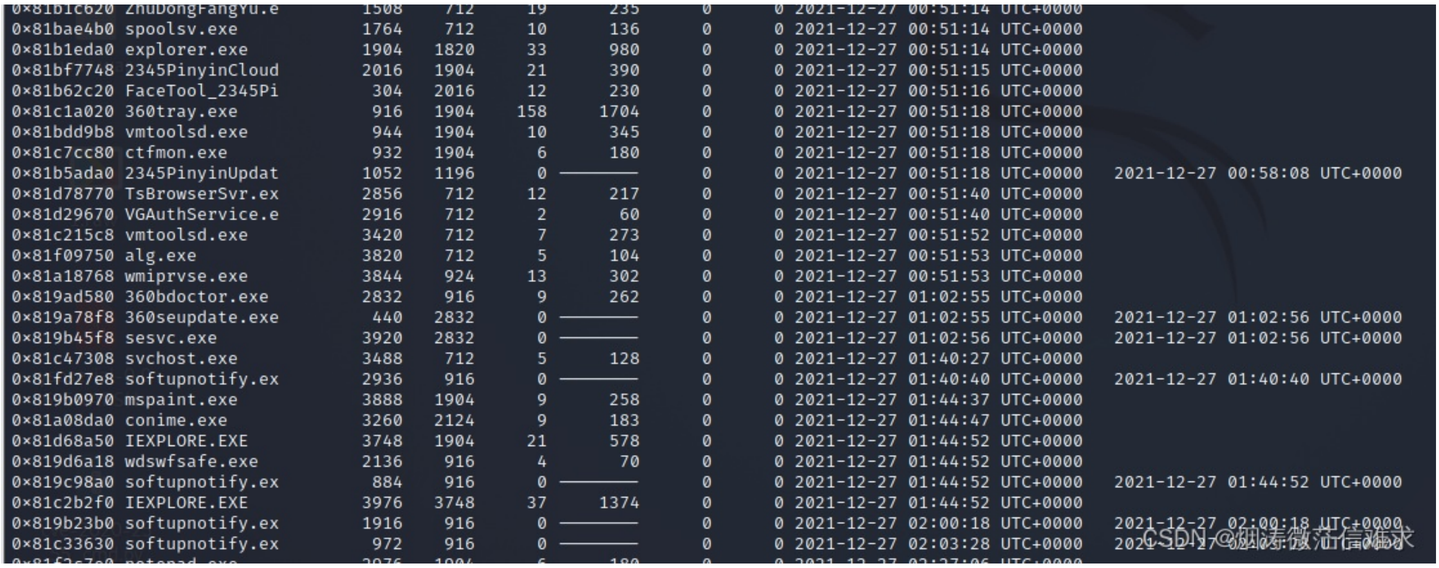
CSDN @烟涛微茫信难求

2.尝试第一个profile类型，查看进程

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



```
┌──(root💀kali)-[~/桌面]
└─# volatility -f 1.raw pslist --profile=WinXPSP2x86
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8214fa00 System                    4      0     56      364 ------      0
0x81cfe778 smss.exe                588      4      3       19 ------      0 2021-12-27 00:51:12 UTC+0000
0x81b39da0 csrss.exe               636    588     12      841      0      0 2021-12-27 00:51:13 UTC+0000
0x81ffb020 winlogon.exe            668    588     23      526      0      0 2021-12-27 00:51:13 UTC+0000
0x81b3bbf0 services.exe            712    668     15      308      0      0 2021-12-27 00:51:13 UTC+0000
0x81c80478 lsass.exe               724    668     21      360      0      0 2021-12-27 00:51:13 UTC+0000
0x81b27370 vmacthlp.exe            908    712      1       25      0      0 2021-12-27 00:51:13 UTC+0000
0x81b3da70 svchost.exe             924    712     17      205      0      0 2021-12-27 00:51:13 UTC+0000
0x82076b18 svchost.exe             988    712     10      296      0      0 2021-12-27 00:51:13 UTC+0000
0x81f228b8 svchost.exe            1084    712     72     1491      0      0 2021-12-27 00:51:13 UTC+0000
0x81b11450 svchost.exe            1176    712      6       93      0      0 2021-12-27 00:51:13 UTC+0000
0x81b4eda0 Pinyin_2345Svc.        1196    712     17      367      0      0 2021-12-27 00:51:13 UTC+0000
0x81b70be8 svchost.exe            1312    712      3      103      0      0 2021-12-27 00:51:14 UTC+0000
0x81f5b440 Protect_2345Exp        1324    712     11      335      0      0 2021-12-27 00:51:14 UTC+0000
0x81f06da0 Pic_2345Svc.exe        1368    712     26      432      0      0 2021-12-27 00:51:14 UTC+0000
```



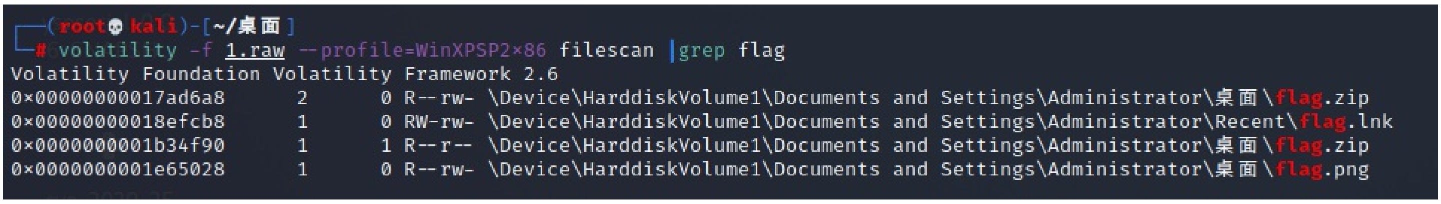
```
0×81b1c620 ZhuDongFangYu.e       1508    712     19      235       0       0 2021-12-27 00:51:14 UTC+0000
0×81bae4b0 spoolsv.exe           1764    712     10      136       0       0 2021-12-27 00:51:14 UTC+0000
0×81b1eda0 explorer.exe          1904   1820     33      980       0       0 2021-12-27 00:51:14 UTC+0000
0×81bf7748 2345PinyinCloud       2016   1904     21      390       0       0 2021-12-27 00:51:15 UTC+0000
0×81b62c20 FaceTool_2345Pi        304   2016     12      230       0       0 2021-12-27 00:51:16 UTC+0000
0×81c1a020 360tray.exe            916   1904    158     1704       0       0 2021-12-27 00:51:18 UTC+0000
0×81bdd9b8 vmtoolsd.exe           944   1904     10      345       0       0 2021-12-27 00:51:18 UTC+0000
0×81c7cc80 ctfmon.exe             932   1904      6      180       0       0 2021-12-27 00:51:18 UTC+0000
0×81b5ada0 2345PinyinUpdat       1052   1196      0 ————————       0       0 2021-12-27 00:51:18 UTC+0000   2021-12-27 00:58:08 UTC+0000
0×81d78770 TsBrowserSvr.ex       2856    712     12      217       0       0 2021-12-27 00:51:40 UTC+0000
0×81d29670 VGAuthService.e       2916    712      2       60       0       0 2021-12-27 00:51:40 UTC+0000
0×81c215c8 vmtoolsd.exe          3420    712      7      273       0       0 2021-12-27 00:51:52 UTC+0000
0×81f09750 alg.exe               3820    712      5      104       0       0 2021-12-27 00:51:53 UTC+0000
0×81a18768 wmiprvse.exe          3844    924     13      302       0       0 2021-12-27 00:51:53 UTC+0000
0×819ad580 360bdoctor.exe        2832    916      9      262       0       0 2021-12-27 01:02:55 UTC+0000
0×819a78f8 360seupdate.exe        440   2832      0 ————————       0       0 2021-12-27 01:02:55 UTC+0000   2021-12-27 01:02:56 UTC+0000
0×819b45f8 sesvc.exe             3920   2832      0 ————————       0       0 2021-12-27 01:02:56 UTC+0000   2021-12-27 01:02:56 UTC+0000
0×81c47308 svchost.exe           3488    712      5      128       0       0 2021-12-27 01:40:27 UTC+0000
0×81fd27e8 softupnotify.ex       2936    916      0 ————————       0       0 2021-12-27 01:40:40 UTC+0000   2021-12-27 01:40:40 UTC+0000
0×819b0970 mspaint.exe           3888   1904      9      258       0       0 2021-12-27 01:44:37 UTC+0000
0×81a08da0 conime.exe            3260   2124      9      183       0       0 2021-12-27 01:44:47 UTC+0000
0×81d68a50 IEXPLORE.EXE          3748   1904     21      578       0       0 2021-12-27 01:44:52 UTC+0000
0×819d6a18 wdswfsafe.exe         2136    916      4       70       0       0 2021-12-27 01:44:52 UTC+0000
0×819c98a0 softupnotify.ex        884    916      0 ————————       0       0 2021-12-27 01:44:52 UTC+0000   2021-12-27 01:44:52 UTC+0000
0×81c2b2f0 IEXPLORE.EXE          3976   3748     37     1374       0       0 2021-12-27 01:44:52 UTC+0000
0×819b23b0 softupnotify.ex       1916    916      0 ————————       0       0 2021-12-27 02:00:18 UTC+0000   2021-12-27 02:00:18 UTC+0000
0×81c33630 softupnotify.ex        972    916      0 ————————       0       0 2021-12-27 02:03:28 UTC+0000   2021-12-27 02:03:28 UTC+0000
0×81f2c7e0 notepad.exe           2076   1904      6      180       0       0 2021-12-27 02:27:06 UTC+0000
```

CSDN @烟涛微茫信难求

3.grep过滤flag关键字试试

volatility -f 1.raw --profile=WinXPSP2x86 filescan |grep flag

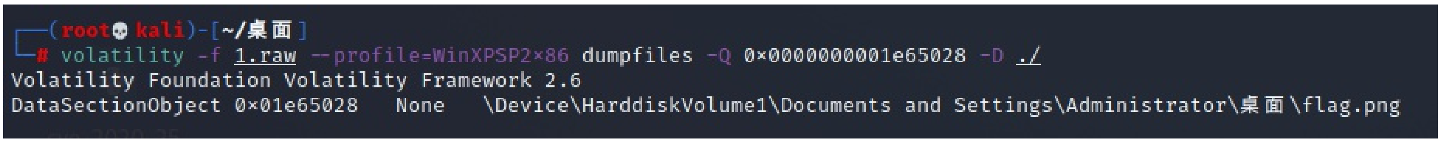
发现了线索



```
┌──(root💀kali)-[~/桌面]
└─# volatility -f 1.raw --profile=WinXPSP2×86 filescan |grep flag
Volatility Foundation Volatility Framework 2.6
0×00000000017ad6a8      2      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.zip
0×00000000018efcb8      1      0 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Recent\flag.lnk
0×0000000001b34f90      1      1 R--r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.zip
0×0000000001e65028      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.png
```

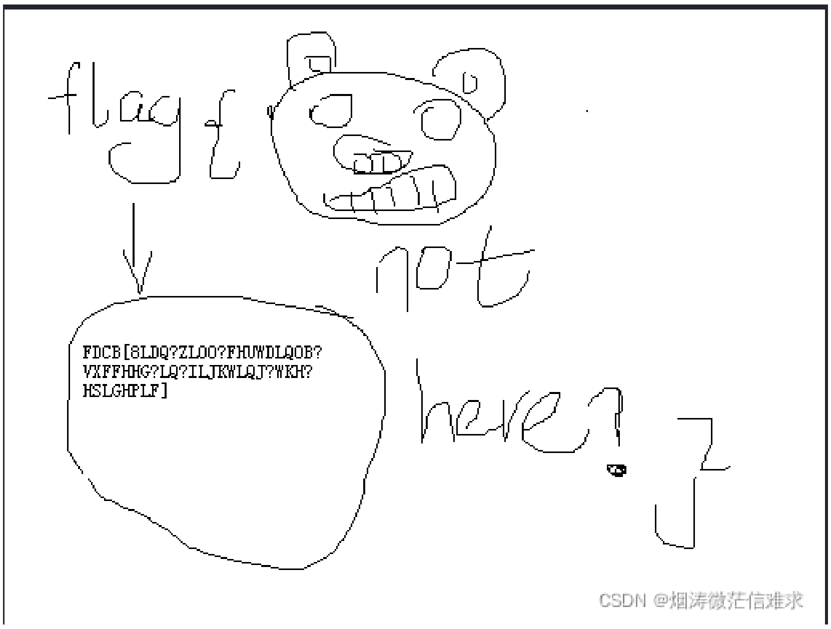
4.先把png图片提出来看看

volatility -f 1.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000001e65028 -D ./



```
┌──(root💀kali)-[~/桌面]
└─# volatility -f 1.raw --profile=WinXPSP2×86 dumpfiles -Q 0×0000000001e65028 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0×01e65028   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.png
```

5.查看图片



6.把那一圈字符串提取出来看看：

6.把那一串字符串提取出来看看：
FDCB[8LDQ?ZLOO?FHUWDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]
这一串，开头是四个字符，还有中括号包着，明显是flag的格式，而且中间的多个问号盲猜是下划线，根据经验应该是ASCII码移位了。尝试“[”的ASCII码为91，“{”的ascii码为123，所以猜测所有字符ASCII码要加32，再次尝试问号的ASCII码为63，加32等于95，正好对应下划线，验证了猜想，所以把所有ASCII码加32。

手算太麻烦了，python三行代码解决

```
string = 'FDCB[8LDQ?ZLOO?FHUWDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]'
for i in string:
    print(chr(ord(i) + 32), end='')
```

结果为：fdcb{Xldq_zloo_fhuwdlqob_vxffhhg_lq_iljkwlqj_wkh_hslghplf}

7.看上去不大对，根据经验凯撒解密一下试试
结果为：cazy{Uian_will_certainly_succeed_in_fighting_the_epidemic}
这就对了嘛（PS：第一个U应为X，行该是出题的时候误把B写成8了）
所以flag是cazy{Xian_will_certainly_succeed_in_fighting_the_epidemic}
西安一定会战胜疫情！加油！！！