CTF-内存取证

原创

刘姑娘的意中人 于 2021-12-13 17:01:05 发布 2254 收藏

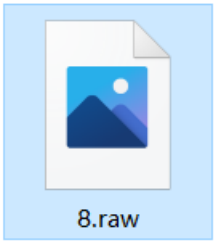
分类专栏： CTF 文章标签： 安全 web安全

本文链接：https://blog.csdn.net/curen110lj/article/details/121909228

一道简单得CTF题，主要是内存取证方法

8	2021/10/21 17:26	文件夹	
8.rar	2021/3/5 9:54	WinRAR 压缩文件	68,148 KB
flag.txt	2021/10/12 9:07	文本文档	1 KB
wP.docx	2021/12/13 16:35	DOCX 文档	90 KB
题干.txt	2021/3/5 9:54	文本文档	1 KB

这是题目及答案



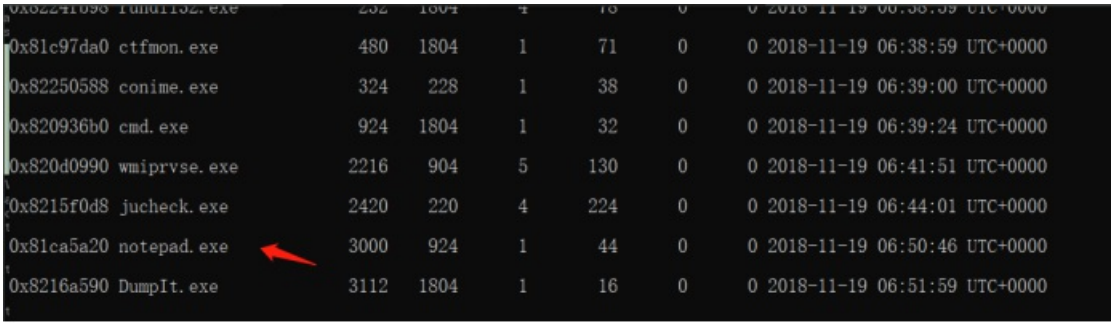
这是提取出来的内存文件

```
F:\VVVVVVV\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f 8.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 (F:\VVVVVVV\volatility_2.6_win64_standalone\8.raw)
                      PAE type : PAE
                           DTB : 0x372000L
                          KDBG : 0x80546ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-11-19 06:52:02 UTC+0000
     Image local date and time : 2018-11-19 14:52:02 +0800
```

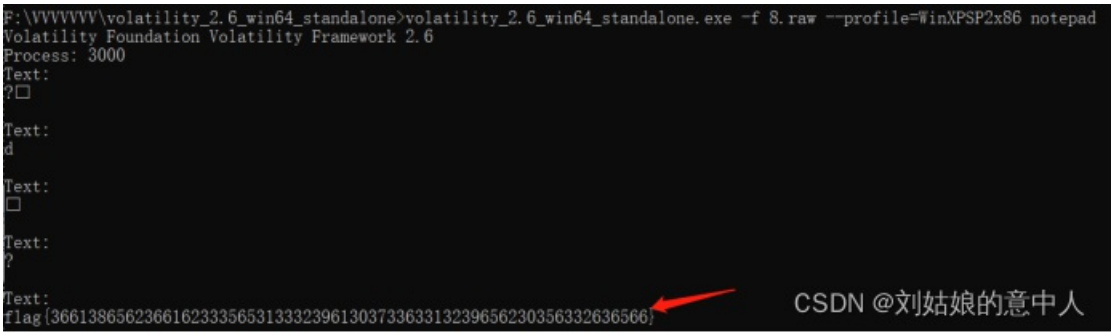

这里装好volatility后 打开8.raw后 显示为镜像系统等信息

```
F:\VVVVVVV\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f 8.raw --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
```

这里是查看截取时的在运进程



这边浏览众多进程后，一个个排查把算是，然后觉得这个文本文件可疑，进去查看下



Flag在这

此题更多是看会不会用工具，并无高深利用，算是掌握工具类的把。