

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](#)

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/curen110lj/article/details/121909228>

版权



[CTF 专栏收录该内容](#)

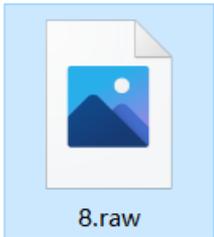
1 篇文章 0 订阅

订阅专栏

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:\VVVVVV\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:\VVVVVV\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
```

CSDN @刘姑娘的意中人

这里装好volatility后 打开8.raw后 显示为镜像系统等信息

```
F:\VVVVVV\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f 8.raw --profile=WinXPSP2x86 plist
Volatility Foundation Volatility Framework 2.6
Name: PID: PPID: Title: Image: Session: User64: Start: End:
-----
```

```
Process Name PID PPID PIDus PIDus Sess User04 Start Exit
```

这里是查看截取时的在运进程

Process Name	PID	PPID	PIDus	PIDus	Sess	User04	Start	Exit
0x82241098 rundll32.exe	202	1804	4	78	0	0	2018-11-19 06:38:59 UTC+0000	
0x81c97da0 ctfmon.exe	480	1804	1	71	0	0	2018-11-19 06:38:59 UTC+0000	
0x82250588 conime.exe	324	228	1	38	0	0	2018-11-19 06:39:00 UTC+0000	
0x820936b0 cmd.exe	924	1804	1	32	0	0	2018-11-19 06:39:24 UTC+0000	
0x820d0990 wmiprvse.exe	2216	904	5	130	0	0	2018-11-19 06:41:51 UTC+0000	
0x8215f0d8 jucheck.exe	2420	220	4	224	0	0	2018-11-19 06:44:01 UTC+0000	
0x81ca5a20 notepad.exe	3000	924	1	44	0	0	2018-11-19 06:50:46 UTC+0000	
0x8216a590 DumpIt.exe	3112	1804	1	16	0	0	2018-11-19 06:51:59 UTC+0000	

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

```
F:\VVVVVV\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f 8.raw --profile=WinXPSP2x86 notepad
Volatility Foundation Volatility Framework 2.6
Process: 3000
Text:
?[]
Text:
d
Text:
[]
Text:
?
Text:
flag{3661386562366162333565313332396130373363313239656230356332636566}
```

CSDN @刘姑娘的意中人

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。