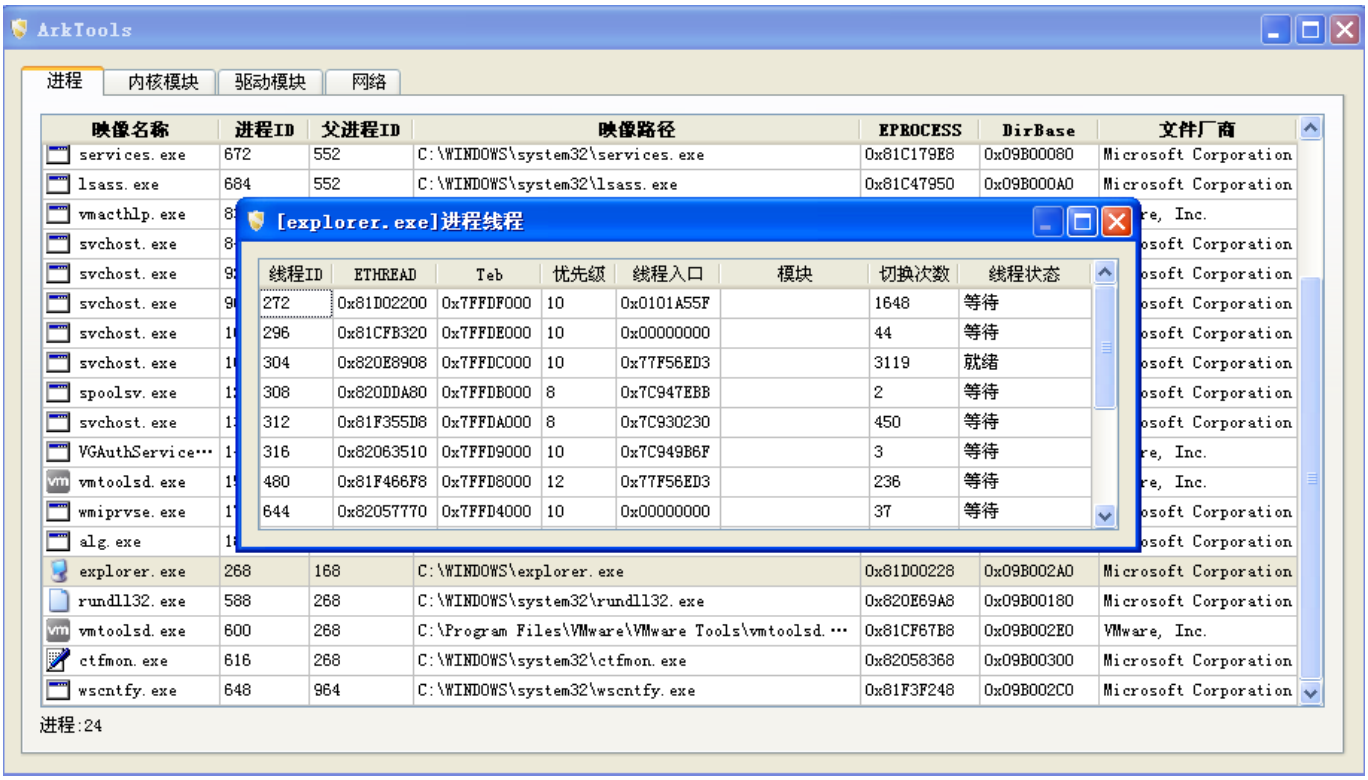
ArkTools

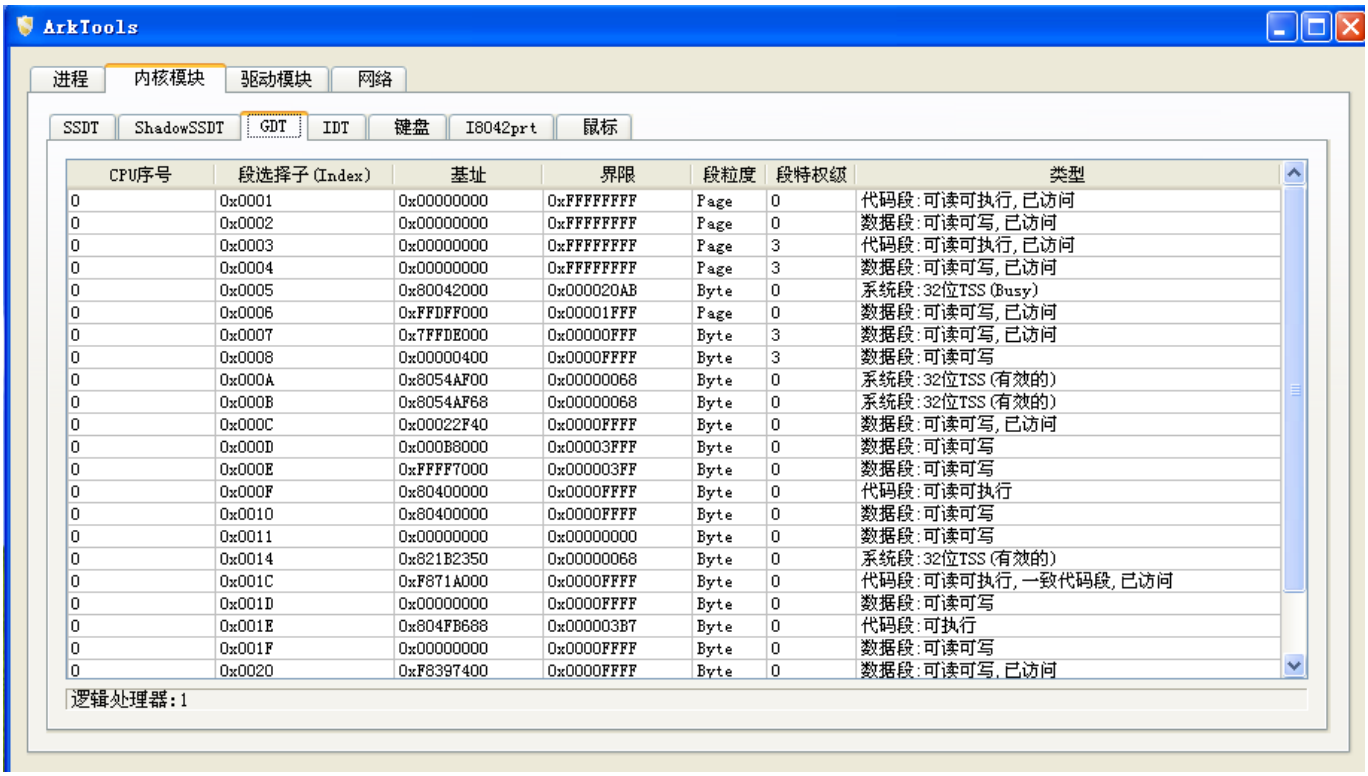
科锐3阶段内核课程课后小项目

32位的内核工具.
仅可在XP sp3下可运行,有时间会尝试改成64位的

实现的功能:

- 进程遍历
- 进程线程遍历
- 读写进程内存(Ring0封装好了,Ring3通信未写完)
- 显示IDT/GDT
- 显示SSDT/ShadowSSDT
- 显示键盘/鼠标/i8042port/TCPIP的分发函数


ArkTools
进程
内核模块
驱动模块
网络
映像名称 进程ID 父进程ID 映像路径 EPROCESS DirBase 文件厂商
services.exe 672 552 C:\WINDOWS\system32\services.exe 0x81C179E8 0x09B00080 Microsoft Corporation
lsass.exe 684 552 C:\WINDOWS\system32\lsass.exe 0x81C47950 0x09B000A0 Microsoft Corporation
vmacthlp.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
VGAuthService…
vmtoolsd.exe
wmiprvse.exe
alg.exe
explorer.exe 268 168 C:\WINDOWS\explorer.exe 0x81D00228 0x09B002A0 Microsoft Corporation
rundll32.exe 588 268 C:\WINDOWS\system32\rundll32.exe 0x820E69A8 0x09B00180 Microsoft Corporation
vmtoolsd.exe 600 268 C:\Program Files\VMware\VMware Tools\vmtoolsd.… 0x81CF67B8 0x09B002E0 VMware, Inc.
ctfmon.exe 616 268 C:\WINDOWS\system32\ctfmon.exe 0x82058368 0x09B00300 Microsoft Corporation
wscntfy.exe 648 964 C:\WINDOWS\system32\wscntfy.exe 0x81F3F248 0x09B002C0 Microsoft Corporation
[explorer.exe]进程线程
线程ID ETHREAD Teb 优先级 线程入口 模块 切换次数 线程状态
272 0x81D02200 0x7FFDF000 10 0x0101A55F 1648 等待
296 0x81CFB320 0x7FFDE000 10 0x00000000 44 等待
304 0x820E8908 0x7FFDC000 10 0x77F56ED3 3119 就绪
308 0x820DDA80 0x7FFDB000 8 0x7C947EBB 2 等待
312 0x81F355D8 0x7FFDA000 8 0x7C930230 450 等待
316 0x82063510 0x7FFD9000 10 0x7C949B6F 3 等待
480 0x81F466F8 0x7FFD8000 12 0x77F56ED3 236 等待
644 0x82057770 0x7FFD4000 10 0x00000000 37 等待
进程:24


ArkTools
进程
内核模块
驱动模块
网络
SSDT
ShadowSSDT
GDT
IDT
键盘
I8042prt
鼠标
CPU序号 段选择子(Index) 基址 界限 段粒度 段特权级 类型
0 0x0001 0x00000000 0xFFFFFFFF Page 0 代码段:可读可执行,已访问
0 0x0002 0x00000000 0xFFFFFFFF Page 0 数据段:可读可写,已访问
0 0x0003 0x00000000 0xFFFFFFFF Page 3 代码段:可读可执行,已访问
0 0x0004 0x00000000 0xFFFFFFFF Page 3 数据段:可读可写,已访问
0 0x0005 0x80042000 0x000020AB Byte 0 系统段:32位TSS(Busy)
0 0x0006 0xFFDFF000 0x00001FFF Page 0 数据段:可读可写,已访问
0 0x0007 0x7FFDE000 0x00000FFF Byte 3 数据段:可读可写,已访问
0 0x0008 0x00000400 0x0000FFFF Byte 3 数据段:可读可写
0 0x000A 0x8054AF00 0x00000068 Byte 0 系统段:32位TSS(有效的)
0 0x000B 0x8054AF68 0x00000068 Byte 0 系统段:32位TSS(有效的)
0 0x000C 0x00022F40 0x0000FFFF Byte 0 数据段:可读可写,已访问
0 0x000D 0x000B8000 0x00003FFF Byte 0 数据段:可读可写
0 0x000E 0xFFFF7000 0x000003FF Byte 0 数据段:可读可写
0 0x000F 0x80400000 0x0000FFFF Byte 0 代码段:可读可执行
0 0x0010 0x80400000 0x0000FFFF Byte 0 数据段:可读可写
0 0x0011 0x00000000 0x00000000 Byte 0 数据段:可读可写
0 0x0014 0x821B2350 0x00000068 Byte 0 系统段:32位TSS(有效的)
0 0x001C 0xF871A000 0x0000FFFF Byte 0 代码段:可读可执行,一致代码段,已访问
0 0x001D 0x00000000 0x0000FFFF Byte 0 数据段:可读可写
0 0x001E 0x804FB688 0x000003B7 Byte 0 代码段:可执行
0 0x001F 0x00000000 0x0000FFFF Byte 0 数据段:可读可写
0 0x0020 0xF8397400 0x0000FFFF Byte 0 数据段:可读可写,已访问
逻辑处理器:1