

2021/01/27_调试器_第3课_调试器的编写(断点功能)

笔记本： 调试器

创建时间： 2021/1/27 星期三 10:06

作者： ileemi

- ["U" 功能](#)
- [断点功能](#)
- [程序如何反调试](#)
- [反反调试](#)
- [思考](#)

"U" 功能

支持添加 "地址 (参数)", 这里就需要对输入的字符串进行分割 (`strtok`)

断点功能

在指定的地址下断点 (使其产生异常: `int3`)

在程序的入口地址设置断点, 程序执行断点后产生断点异常, EIP执行的是这条指令的下一条指令, 在还原目标进程中的代码时, 就需要将EIP的值修改为原来程序中产生断点异常的代码。

在调试状态下修改代码段的数据不需要更改访问权限 (此时权限较高)。在调试器中判断异常的来源, 软件内部产生的异常应将其交还给软件自己 (类似与调试器的 `Shift + F9`) 进行处理。

需要区分异常产生的由来是调试器还是程序本身。程序本身产生的异常就应该将异常交还给程序自己去处理。防止调试器被反调试。

通过调试器产生的异常和软件内部产生的异常一样时, 要防止程序进入递归。调试器产生的异常处理完毕后, 应将保存异常地址的成员置空。

一个地址被多次调用, 在此处下断点, 此地址上的断点应该根据被调次数产生对应次数的断点 (此段点不是一次性的)。**一次性断点适合在被调试进程的入口代码位置处设置。**

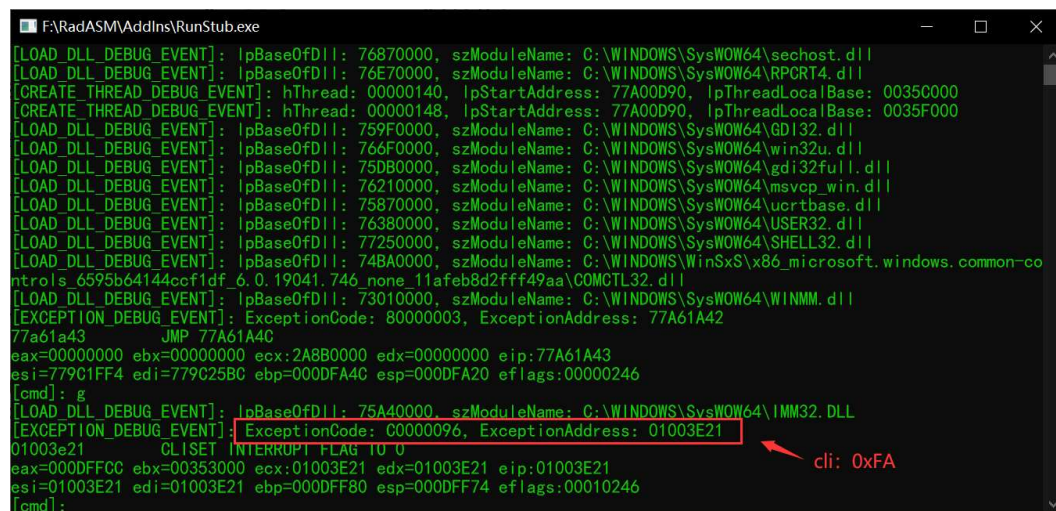
程序如何反调试

可检查函数头, 如果被设置为 "`int 3`", 就退出程序 (反调试)。检查的代码还可以进行加密处理。

```
.if byte ptr [offset START] == 0cch
    invoke ExitProcess, 0
.endif
```

反反调试

防止程序出现异常代码检测，不一定非要使用 "int 3" 异常代码在目标进程中下断点，也可以使用其它的汇编代码在目标进程中使其产生异常，比如使用**特权指令异常**：C0000096H (cli)，对应的宏为："STATUS_PRIVILEGED_INSTRUCTION"。



```
F:\RadASM\AddIns\RunStub.exe
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 76870000, szModuleName: C:\WINDOWS\SysWOW64\sechost.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 76E70000, szModuleName: C:\WINDOWS\SysWOW64\RPCRT4.dll
[CREATE_THREAD_DEBUG_EVENT]: hThread: 00000140, lpStartAddress: 77A00D90, lpThreadLocalBase: 0035C000
[CREATE_THREAD_DEBUG_EVENT]: hThread: 00000148, lpStartAddress: 77A00D90, lpThreadLocalBase: 0035F000
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 759F0000, szModuleName: C:\WINDOWS\SysWOW64\GDI32.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 766F0000, szModuleName: C:\WINDOWS\SysWOW64\win32u.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 75DB0000, szModuleName: C:\WINDOWS\SysWOW64\gdi32full.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 76210000, szModuleName: C:\WINDOWS\SysWOW64\msvcrt.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 75870000, szModuleName: C:\WINDOWS\SysWOW64\user32.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 76380000, szModuleName: C:\WINDOWS\SysWOW64\USER32.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 77250000, szModuleName: C:\WINDOWS\SysWOW64\SHELL32.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 74BA0000, szModuleName: C:\WINDOWS\WinSxS\x86_microsoft.windows.common-co
ntrols_6595b64144ccf1df_6.0.19041.746_none_11afeb8d2fff49aa\COMCTL32.dll
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 73010000, szModuleName: C:\WINDOWS\SysWOW64\WINMM.dll
[EXCEPTION_DEBUG_EVENT]: ExceptionCode: 80000003, ExceptionAddress: 77A61A42
77A61A43 JMP 77A61A4C
eax=00000000 ebx=00000000 ecx=2A8B0000 edx=00000000 eip:77A61A43
esi=779C1FF4 edi=779C25BC ebp=000DFA4C esp=000DFA20 eflags:00000246
[cmd]: g
[LOAD_DLL_DEBUG_EVENT]: lpBaseOfDll: 75A40000, szModuleName: C:\WINDOWS\SysWOW64\IMM32.DLL
[EXCEPTION_DEBUG_EVENT]: ExceptionCode: C0000096, ExceptionAddress: 01003E21
01003E21 CLIBSET INTERRUPT FLAG TO 0
eax=000DFFC0 ebx=00353000 ecx:01003E21 edx:01003E21 eip:01003E21
esi=01003E21 edi=01003E21 ebp=000DFF80 esp=000DFF74 eflags:00010246
[cmd]: cli: 0xFA
```

思考

被调试程序内部有 "单步异常"，用于反调试。注册一个SEH异常，在程序中故意产生