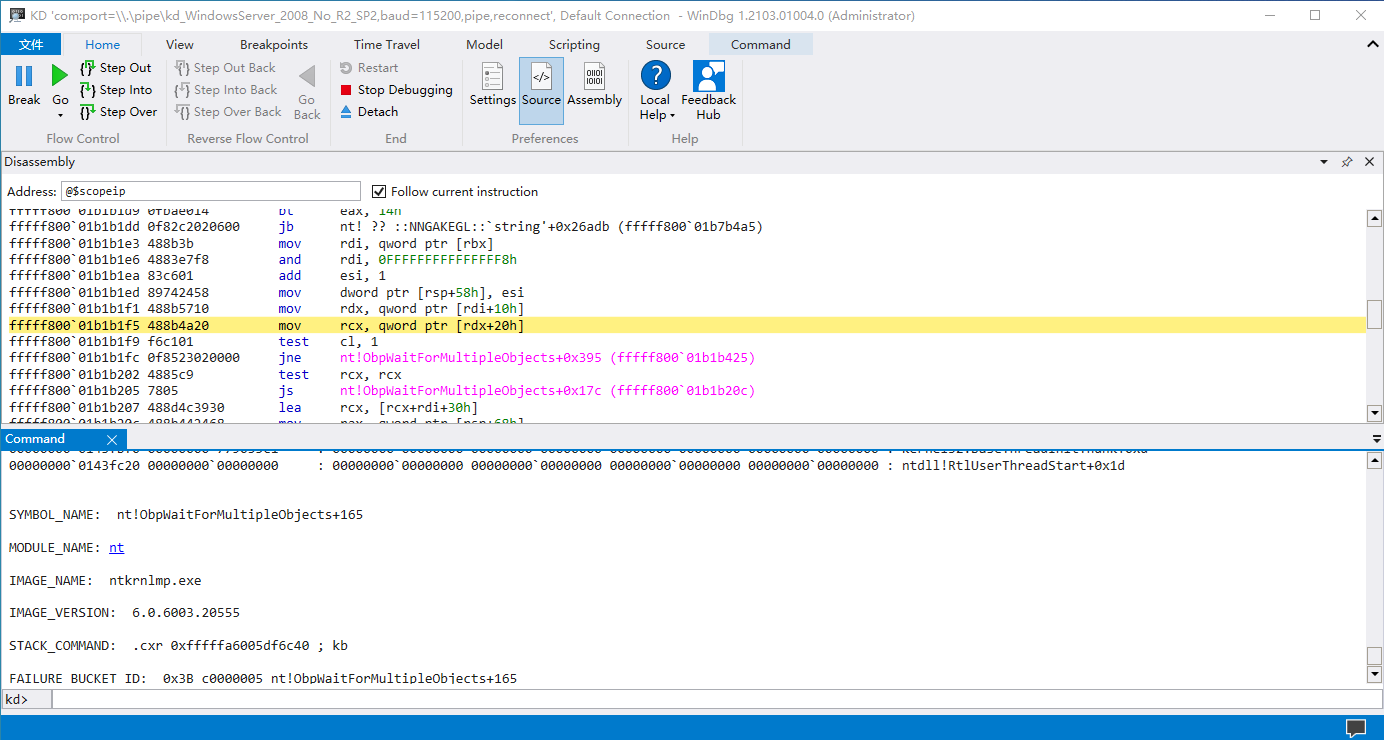
NtosKrnl\_Event\_Integer\_Overflow

调用堆栈

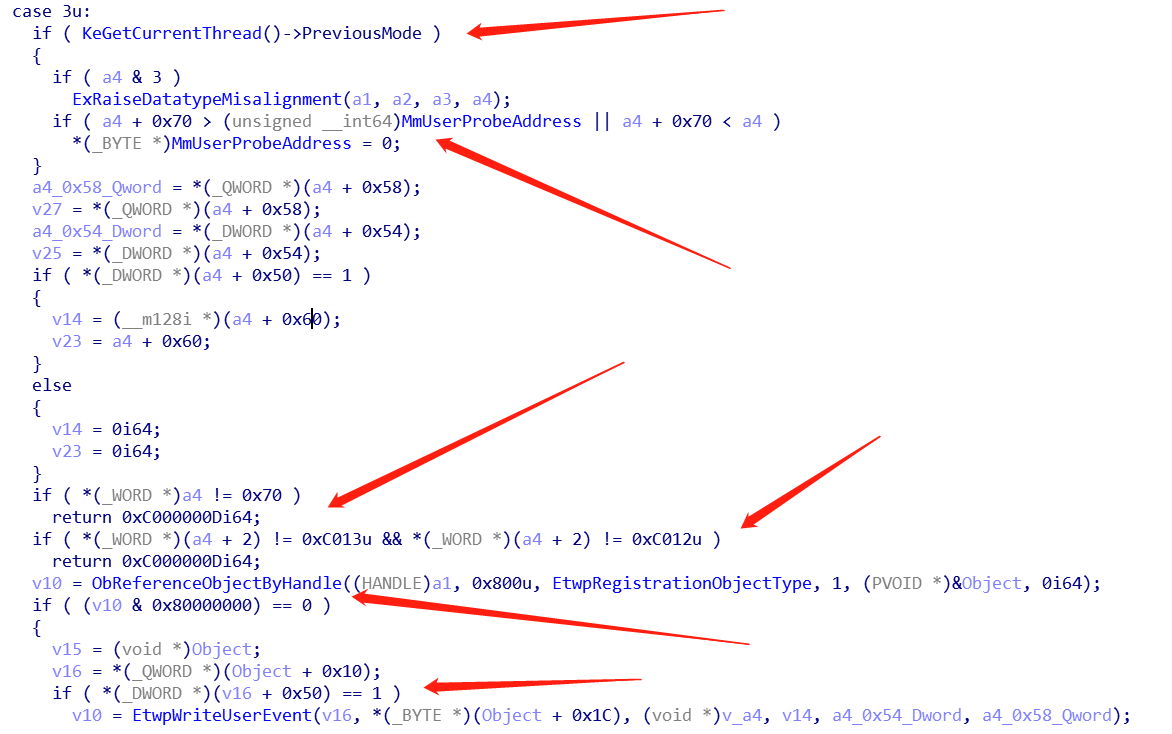
NtTraceEvent->EtwpWriteUserEvent -> Crash

EtwpWriteUserEvent 函数存在一个整数溢出漏洞 在最新版的Windows Server 2008 SP2 中可复现，可以导致Kernel Pool越界写，通过攻击者精心构造的内存布局可以达到权限提升的目的。

由于是 Kernel Pool OverFlow 所以引发的错误多种多样



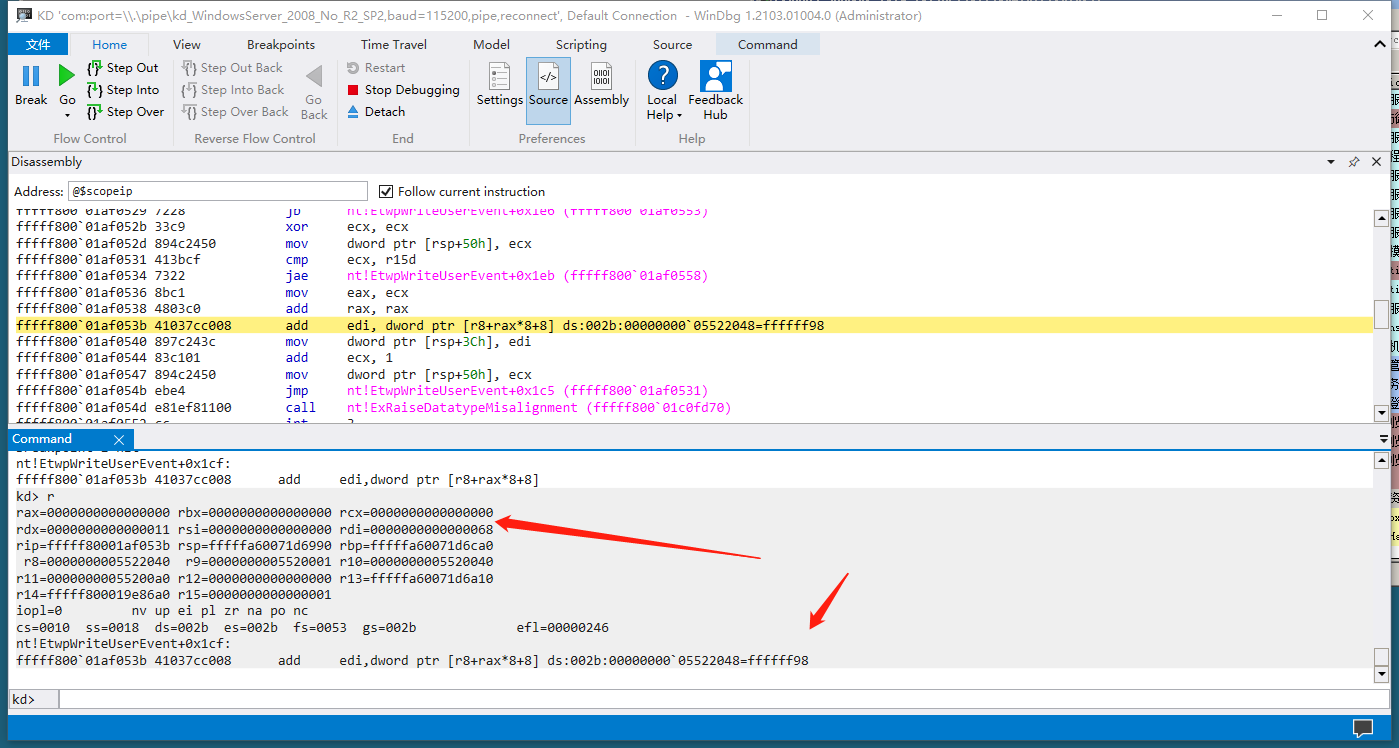
调用 NtTraceEvent 函数 Flag 设置为0x03，经过一些判断条件后会调用到EtwpWriteUserEvent函数。

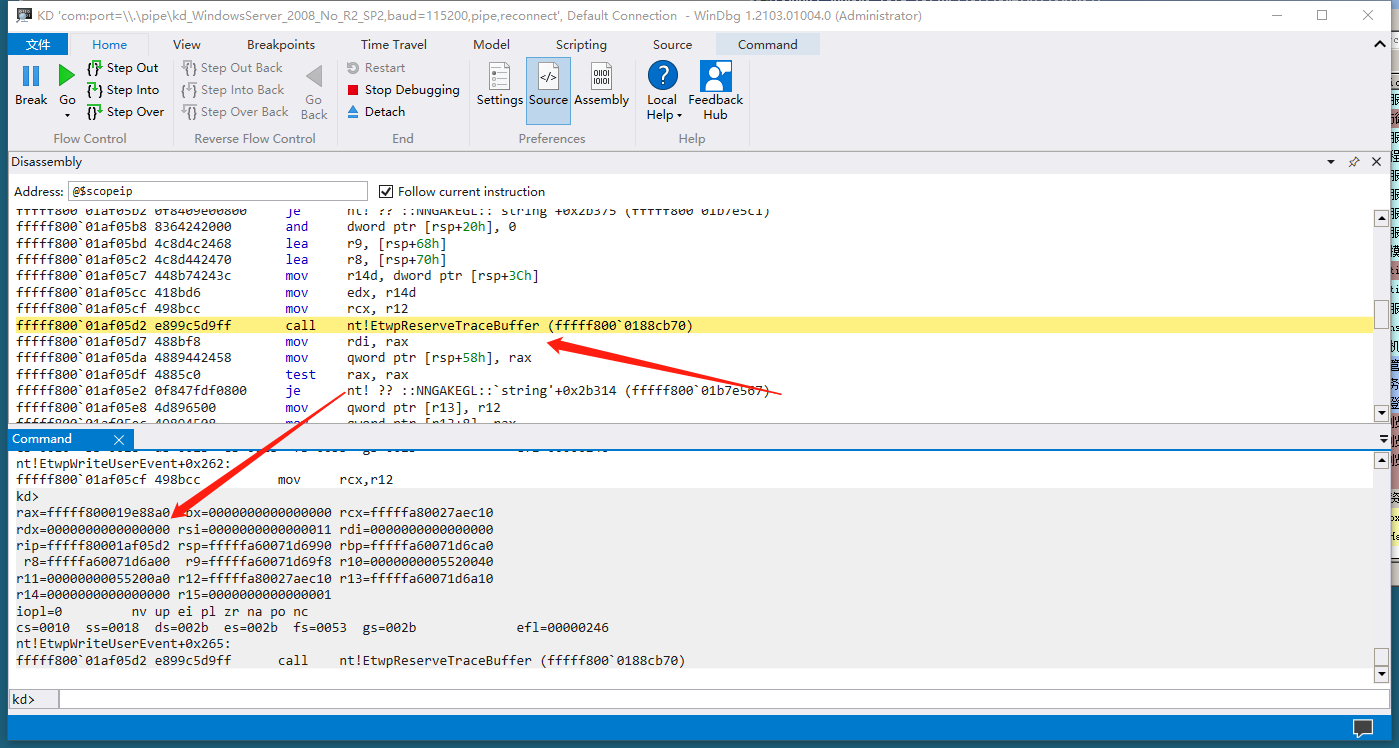


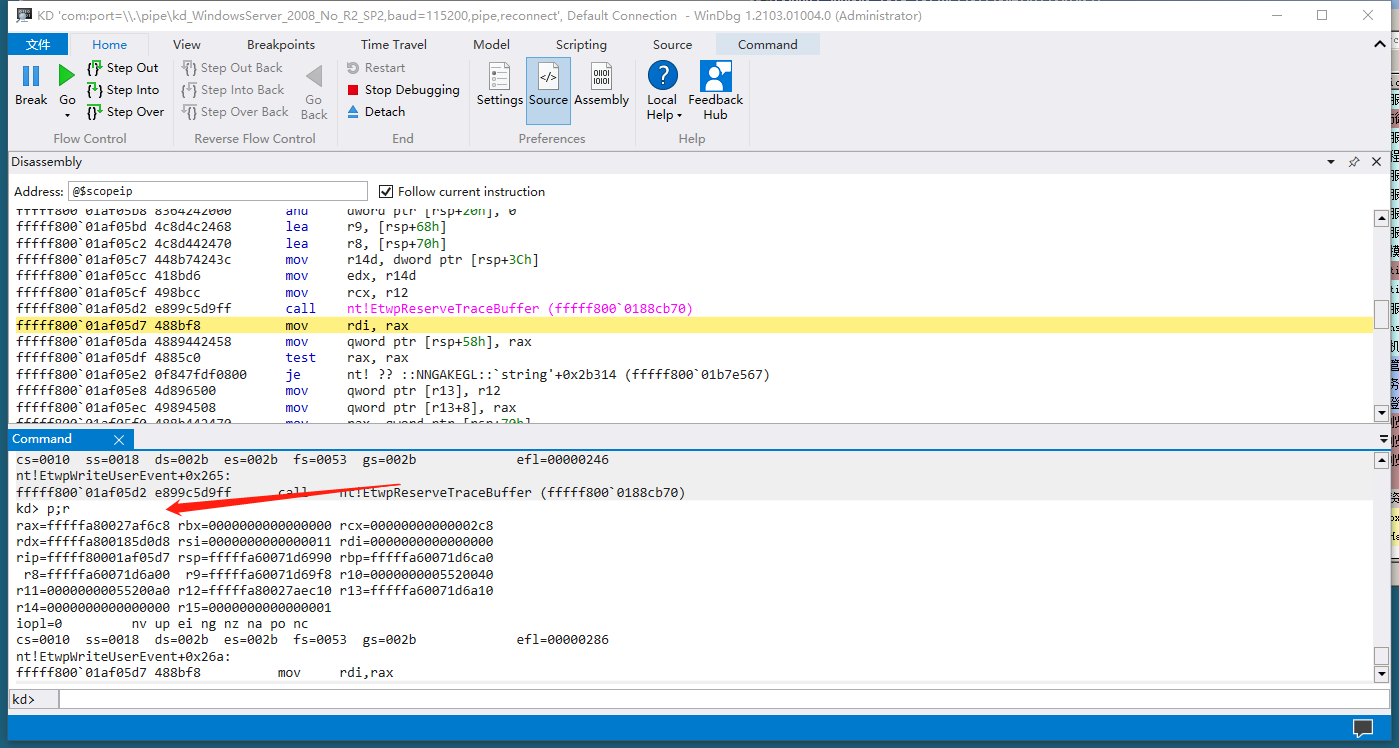
主要注意的是ObReferenceObjectByHandle 函数，我们要传入一个 EtwpRegistrationObjectType 句柄，并且该句柄要启动跟踪功能。

EtwpWriteUserEvent 函数中此处存在一个整数溢出， EtwpReserveTraceBuffer 函数的第二个参数为分配内存的大小，该函数返回值是一个Large Pool中的一部分，其自己实现了内存管理机制，在此不过多赘述。



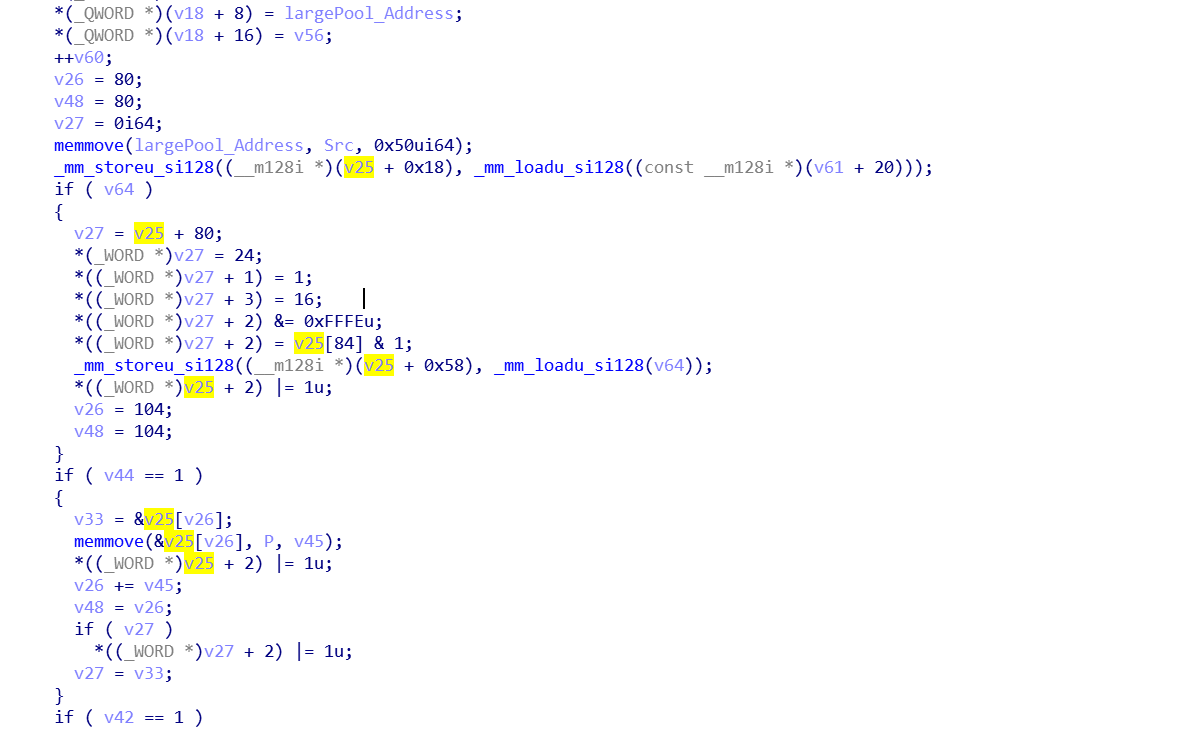






分配完内存后，该函数会初始化内存，此处就存在一个越界写，后续还有大量字符拷贝，设置结构体等操作。只要执行次数过多，覆盖了其他块的结构或触发访问异常，则会导致BSOD。





因为是整数溢出导致的池溢出，所以触发的异常是多种多样的。

