

看雪学院-OllyDBG入门系列（四）内存写入 笔记

原创

Cytosine 于 2017-02-05 12:57:50 发布 1092 收藏

分类专栏: [笔记_看雪学院OD入门系列](#) [解密 OllyDBG 逆向](#) 文章标签: [Note OllyDBG 内存断点](#)

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/Cytosine/article/details/54880664>

版权



[笔记_看雪学院OD入门系列](#) 同时被 3 个专栏收录

3 篇文章 0 订阅

订阅专栏



[解密](#)

5 篇文章 0 订阅

订阅专栏



[OllyDBG](#)

3 篇文章 0 订阅

订阅专栏

看雪学院-OllyDBG入门系列（四）内存断点 笔记

原作地址: <http://bbs.pediy.com/showthread.php?threadid=21378>

作者: CCDebugger

在 OllyDBG 中一般我们用到的内存断点有内存访问和内存写入断点。内存访问断点就是指程序访问内存中我们指定的内存地址时中断, 内存写入断点就是指程序往我们指定的内存地址中写东西时中断。

内存断点的特性就是不管你选几个字节, OllyDBG 都会分配 4096 字节的内存区。而硬件断点最多只能选 4 个字节。

更多关于断点的知识大家可以参考 [论坛精华7->基础知识->断点技巧->断点原理](#) 这篇 Lenus 兄弟写的《如何对抗硬件断点之一 --- 调试寄存器》文章, 也可以看这个帖: <http://bbs.pediy.com/showthread.php?threadid=10829>。