[系统安全] 二.如何学好逆向分析及吕布传游戏逆向案例

原创

Eastmount 于 2020-12-13 16:13:13 发布 6491 收藏 37

分类专栏： 系统安全与恶意代码分析 文章标签： 系统安全 逆向分析 游戏逆向 基础普及 恶意代码分析

本文链接：https://blog.csdn.net/Eastmount/article/details/108832086

您可能之前看到过我写的类似文章，为什么还要重复撰写呢？只是想更好地帮助初学者了解病毒逆向分析和系统安全，更加成体系且不破坏之前的系列。因此，我重新开设了这个专栏，准备系统整理和深入学习系统安全、逆向分析和恶意代码检测，“系统安全”系列文章会更加聚焦，更加系统，更加深入，也是作者的慢慢成长史。换专业确实挺难的，逆向分析也是块硬骨头，但我也试试，看看自己未来四年究竟能将它学到什么程度，漫漫长征路，偏向虎山行。享受过程，一起加油~

系统安全系列作者将深入研究恶意样本分析、逆向分析、攻防实战和Windows漏洞利用等，通过在线笔记和实践操作的形式分享与博友们学习，希望能与您一起进步。前文作者先带领大家学习什么是逆向分析，这篇文章将继续普及逆向分析基础知识，告诉大家如何学好逆向分析，并结合作者经验给出逆向分析的路线推荐，最后给出吕布传游戏逆向案例。

该篇文章也是作者学习科锐钱林松老师在华中科技大学的分享视频，这里非常推荐大家去看看。话不多说，让我们开始新的征程吧！您的点赞、评论、收藏将是对我最大的支持，感恩安全路上一路前行，如果有写得不好的地方，可以联系我修改。基础性文章，希望对您有所帮助，作者的目的是与安全人共同进步，加油~

文章目录

作者的github资源：

- 系统安全：https://github.com/eastmountyxz/SystemSecurity-ReverseAnalysis
- 网络安全：https://github.com/eastmountyxz/NetworkSecuritySelf-study

> 声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。（参考文献见后）

一.如何学好软件逆向技能

1.软件逆向前沿

怎么学好软件逆向技能呢？

钱老师说“软件逆向属于搬砖活”。哈哈！的确，任何技术、任何学科方向，都是在你刚开始参与实际工作时，会觉得很好玩，当你做多了之后，就会觉得它是搬砖活。你刚开始接触它，会觉得是技巧，如果你每天都靠这个吃饭，就不再是技巧了。

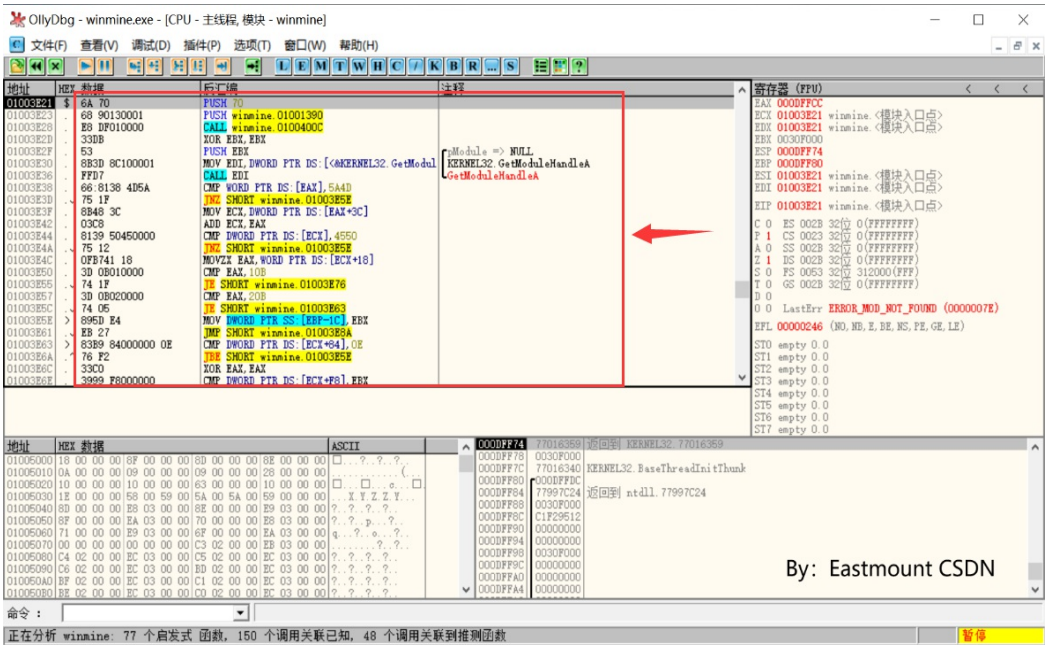
在逆向分析中，很多人都会去网上学习脱壳之类的教程，会教你在哪个地方下断点，按几下F7、F8、F9后，就到了指定位置然后右键脱壳，这一系列操作是大师多年的经验积累。你可能学会了这个最简答的方案，却不理解具体的原理。第一个提出方案的人他需要走过这个壳各种各样的坑，才会形成这个所谓的技巧，它就是为了节约时间和人力成本，无数次重复工作且不影响质量的解决方案。

这种最优解决方案提供给新人看的时候，他会觉得充满了技巧性或不理解，但大家在学习逆向分析的时候，还是少琢磨技巧，干就对了。市面上会有各种各样的工具，比如脱壳，你需要先去学会写壳，写好壳，才会觉得壳有多么的脆弱，我的程序里到处都有BUG，如果别人触发了程序的某个点，我的壳可能就会被摧毁。同时，还有人会研究反调试，甚至汇编出反调试技巧十几则，你为什么发现不了呢？为什么不能自己总结一个呢？只要你自己写一个调试器，就会出现很多方案。当你写完一个调试器之后，你会发现调试器也很脆弱，一不小心某个样本就会把你的调试器给弄奔溃，那么一旦你找到样本规律，对于你的调试器而言就是一种反调试。所以，如果你只是学习网上别人的脱壳、反调试技巧，这是没用的，你需要去深入实践和理解，然后总结属于自己的技巧。

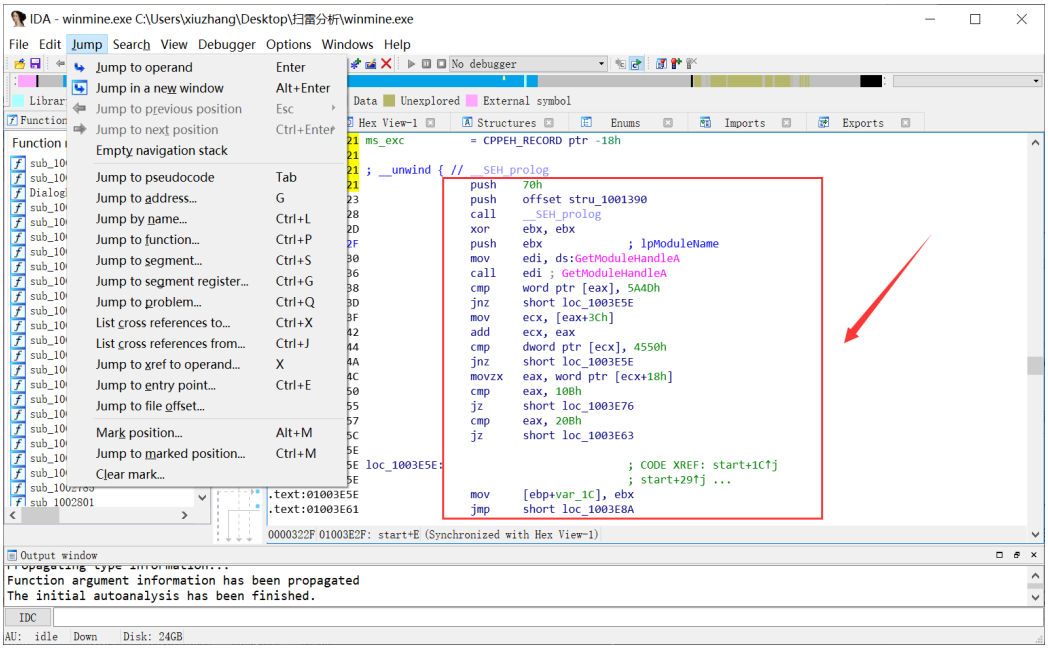
对于对抗行业而言，它是没有一点侥幸而言，你能把对手按在地上摩擦，你就算赢了。同样，很多时候我们只看到安全分析人员光鲜的一面，只看到最后几秒钟那个补丁、攻击的厉害，却不知道分析人员已经被这个壳、调试折磨得不行，反复躺坑最终才能解决。所以，对抗考验的是人的任性和基本功。

- 任性：信念支撑
- 基本功：写代码、读代码

基本功很重要，网上现在三天学会脱壳、两天学会反调试之类的教程很多，我们需要却是基本功。比如，我们在扫雷逆向分析时，关于OllyDbg的教程也非常多，它们详细讲解每个功能干什么，这些功能其实都可以简略学习，**我们需要做的是把下图所示的反汇编窗口的代码搞明白就OK了。** 这些自动化工具可能不是很熟悉，只是工作效率慢点；但换个角度，如果OD工具中的每个功能及快捷键你都会用，但是反汇编窗口的代码看不懂，那你不就废了吗？所以，大家的注意力应该放到反汇编窗口。



同样，对于IDA静态分析也是一个道理，它也有很多的功能，但我们的重点其实还是代码窗口。因为搞安全的人会遇到很多资料，归纳学习总结是必备的技能（通过训练是可以培养出来的），它能帮助你快速的找到重点。所以，技巧不是决定性因素，逆向分析人员真正拼的是基本功。



那么，如何学好编程语言或逆向分析呢？

不要这样学习：

- 只看书，不上机
- 只运行，不调试
- 只做课后练习，不做工程项目

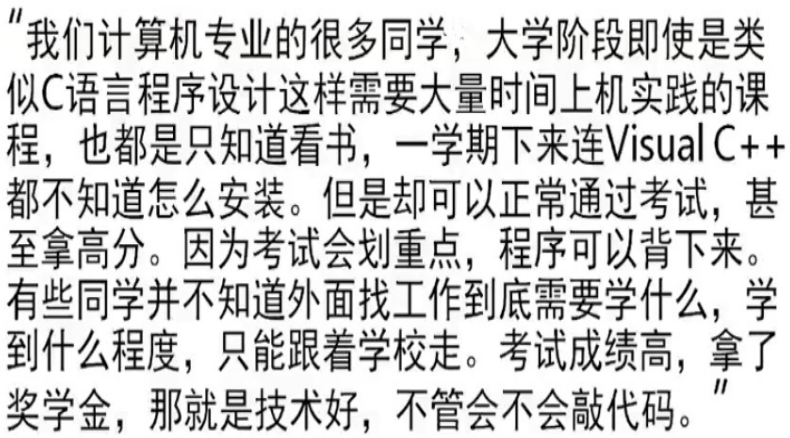
应该这样学习：

- 多敲代码，重要实战
- 程序不是写出来的，是调出来的
- 根据自己的兴趣或者市场的需要多做一些有一定规模的项目

逆向分析底层推荐的三门课程：

- 数据结构
- 操作系统
- 编译原理：逆向的理论知识课程，想要逆向反汇编，还原成高级代码，就需要对编译器有一定了解，否则只能去看别人公布的技巧。

比如《操作系统》课程，你能不能做一个小型的操作系统出来呢？《编译原理》你能不能找到开源的编译器看看词法分析、语法分析的源代码，写点注释呢？2000年之前钱老师是玩黑客工具的，但后来发现学不到本质，学的都是技巧，而技巧是有时效性的，所以想学好还得研究其本质，并且逆向分析底层的知识很少更新，而上层技术更新较快。



2.逆向技能学习路线

在校可以做哪些项目准备呢？

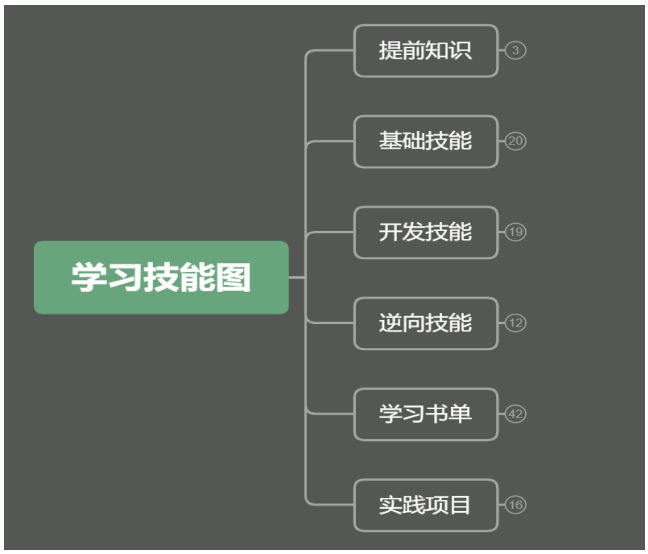
- 关注网络社区，参与技术讨论，推荐看雪论坛
- 搜索安全公司招聘信息，了解技能要求（逆向技能表）
- 针对性开发实际项目

科锐逆向公司在看雪分享的逆向资料推荐大家去学习下。

- 逆向并公开Ollydbg的原理
- 逆向并公开xp版CreateProcess的原理及流程分析
- 逆向并公开Win7 x64版CreateProcess的原理及流程分析
- 逆向并公开xp版ReadProcessMemory原理及流程分析

逆向工程技能树

下面给出软件逆向工程的技能表，包括提前知识、基础技能、开发技能、逆向技能、学习书单和实践项目。



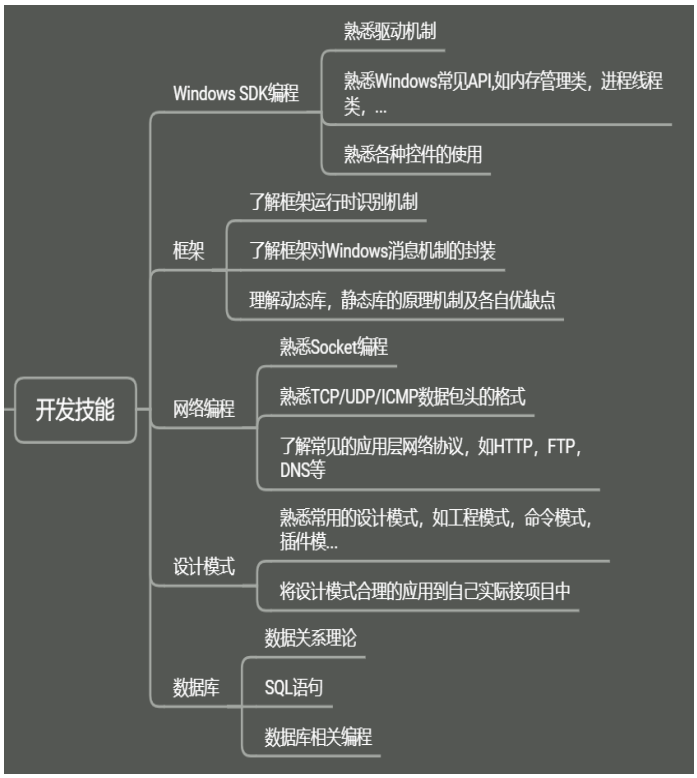
(1) 基础技能

包括汇编语言、C语言、C++语言、数据结构，至少得学一个低级语言和高级语言，然后会一个面向对象语言，重点是数据结构。

(2) 开发技能

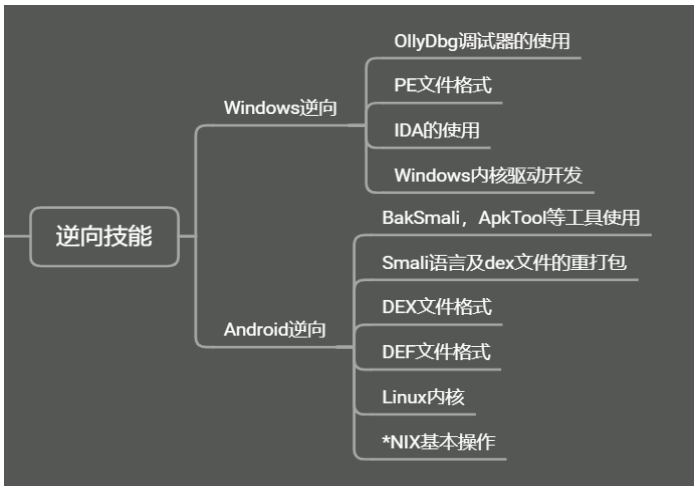
逆向分析需要懂开发，开发至少需要了解一个操作系统平台的编程，可以选择Windows或Linux，如Windows SDK编程；然后至少了解一种框架（Java框架、微软MFC等）。同时，需要懂网络编程（Socket、TCP、HTTP等），有空可以了解下设计模式，学习设计模式前需要有项目经验，因为阅读大型项目代码时会遇到。然后，数据库是必须要学习的技能，非常重要。

在数据库学习中，大家应该好好学习下数据关系理论（范式、集合等），而大家可能更关注后面的SQL语句。为什么呢？因为语句是可能变化的（如Neo4j和MySQL不同），而关系理论一直在那里。同时，我们的操作系统也可以理解为一个专用型数据库，它的职责是管理和分配硬件资源的。比如，我们的系统有50个以上进程在跑，一个32位进程的理论地址空间假设是2G，这就需要100G的内存，那怎么解决这个问题呢？通过数据关系可以解决。微软的操作系统都用到了数据关系，都会建表和主外键，从而避免空间的无故或重复占用。



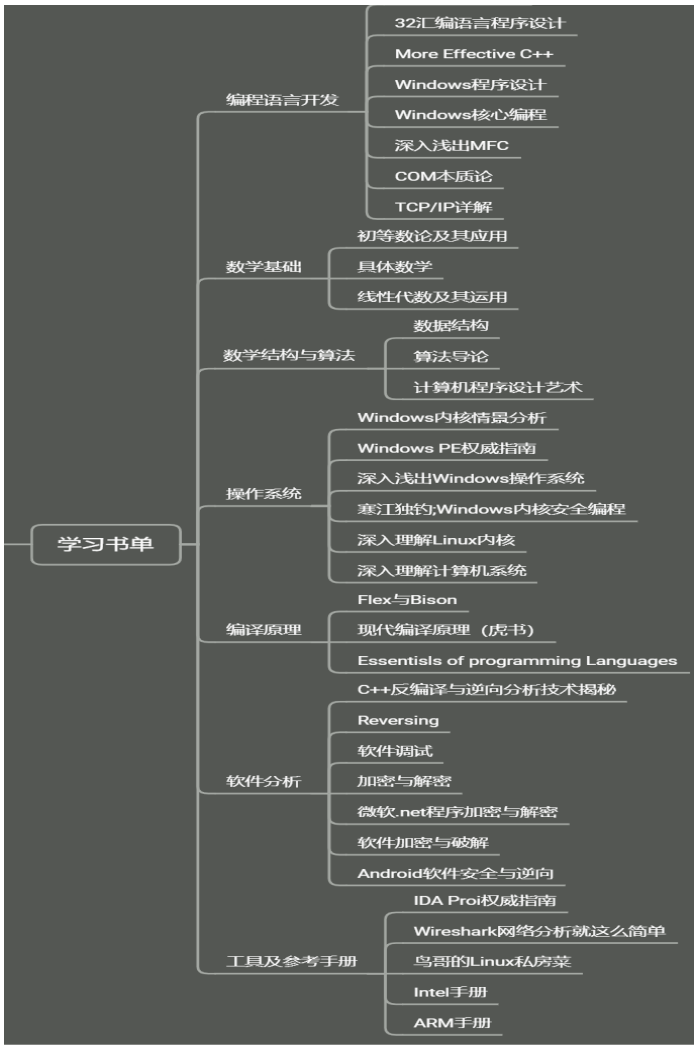
(3) 逆向技能

逆向技能比较偏实战，Windows逆向包括OllyDbg、PE文件格式、IDA使用、Windows内核驱动开发（核心操作系统），Android逆向包括BakSmail、DEX文件格式、Linux内核、NIX操作等。



(4) 学习书单

主要推荐编程语言开发、数学基础、数学结构与算法、操作系统、编译原理、软件分析、、工具及参考手册等书籍。数学基础也非常重要，但我们逆向以应用为主，数学简单了解就好。



(5) 实践项目

这里给出一些推荐的开发项目和逆向项目供大家学习，感觉难度都不小！由于作者开发类的项目很多都做过，所以后面只会详细讲解一个远控软件的实现过程，更多是系统学习和分享逆向项目。远控软件对我们分析木马有帮助，CAD软件能帮助我们分析C++程序，调试器能辅助反调试，PE分析工具帮助对PE文件格式的理解，逆向项目更是直观地提升逆向分析能力。

下面是推荐的一些项目，以及作者的完成情况，这些年确实学得很杂，o(╥﹏╥)o

- [x] 编写一个小游戏，如俄罗斯方块、五子棋、贪吃蛇、坦克（2012年大二完成《坠梦》等多款游戏）
- [x] 编写一个远控软件，支持PC、Android（2014年大四毕设已完成）
- [x] 编写一个CAD，支持图形编辑、图像变换、存储 （2013年大三图形学课完成、2015年完成Android端）
- [ ] 编写一个调试器
- [x] 编写一个小型操作系统（2013年大三小学期C++实现U盘操作系统）
- [x] 编写一个任务管理器，可以对进程、线程等程序活动进行监控（2014年大四毕设已完成）
- [x] 编写一个网络聊天室，支持多人聊天（2015年研一Python实现）
- [ ] 编写一个PE分析工具
- [x] 做一个针对Windows扫雷的作弊程序（2020年博一完成）
- [x] 分析一个RPG游戏存档并写程序修改存档（2013年大三完成《仙剑1》存档器）
- [ ] 通过注入方法，为Windows计算机添加一个菜单程序选项
- [ ] 通过注入内联钩子，实现对指定程序API监控
- [x] 详细逆向分析一个典型的病毒和机理（2020完成年WannaCry蠕虫分析）
- [ ] 不用编译器，只借助十六进制编译器，可以手写一个编译器
- [ ] 从内存中durmp出某应用程序并修复导入表等消息
- [x] 尝试PJ看雪论坛Crakeme模块的各Crakeme习题（2019年正在进行中）
- [ ] 结合安全机理找到安全漏洞并提交CVE漏洞报告

二.安全系列书籍及工具推荐

作为安全初学者，我结合自己和小伙伴们的经验，简单给大家推荐下网络安全、系统安全和人工智能三个方向的书籍，以及相关技术工具，希望大家喜欢！

首先推荐如下书籍，这些都是我读过或正在学习的，都还不错。

- **网络安全**

  《白帽子讲web安全》《Web前端黑客技术揭秘》《XSS跨站脚本攻击剖析与防御》《Web攻防业务安全实战指南》《内网安全攻防渗透测试实战指南》《安全之路Web渗透技术及实战案例解析》《黑客攻防技术宝典浏览器实战篇》《网络攻防实战研究漏洞利用与提权》《CTF训练营》等。

- **系统安全**

  《加密与解密》《恶意代码分析实战》《Windows黑客编程技术详解》《逆向工程权威指南》《软件安全》《windows高级编程》《Windows PE 权威指南》《IDA pro 权威指南》《Android软件安全与逆向分析》《C++反汇编与逆向分析技术揭秘》《0day安全：软件漏洞分析技术》等。

- **人工智能**

  推荐《机器学习》《深度学习》《统计学习方法》《Malware Data Science》等。

下图是作者的一些书籍，感觉还挺多的，建议大家一定结合实战进行阅读，坚持就是胜利。

常见安全网站及论坛：

- 看雪（https://bbs.pediy.com/）
  看雪论坛是个软件安全技术交流场所，为安全技术爱好者提供一个技术交流平台和资源。
- freebuf（https://www.freebuf.com/）
  国内关注度最高的全球互联网安全媒体平台，爱好者们交流与分享安全技术的社区。
- 吾爱PJ（https://www.52pojie.cn/）
  吾爱PJ论坛是致力于软件安全与病毒分析的非营利性技术论坛。
- i春秋（https://www.ichunqiu.com/）
  由国内网络安全机构永信至诚打造的信息安全在线教育平台，非常多的在线网络安全资源。
- 安全客（https://www.anquanke.com）
  提供权威信息发布的漏洞信息,发布安全资讯,分享安全知识和精彩的安全活动直播。
- 先知社区（https://xz.aliyun.com/）
  一个开放型技术平台，包括非常优秀的安全技术文章。
- Bilibili网站（https://www.bilibili.com/）
  B站真的提供了非常多的各类学习资源，去B站学习安全课程真是不错的选择。
- CSDN网站（https://blog.csdn.net/Eastmount）
  全国最大的编程社区，可惜安全文章比较少，但上面有正在进步的我，哈哈！更重要也有很多不错的安全分享，比如冰河、谢公子等，作者谋篇文章会详细总结CSDN的那些白帽子。
- 微信公众号
  微信公众号也提供了非常便捷的安全学习环境，包括很多安全资源，推荐安全+、Gcow、谢公子、看雪、渗透云等公众号。
- 安全牛（https://www.aqniu.com/）
- 安全内参（https://www.secrss.com/）
- 绿盟（http://www.nsfocus.com.cn/）
- 阿里聚安全（https://xlab.tencent.com/cn/）

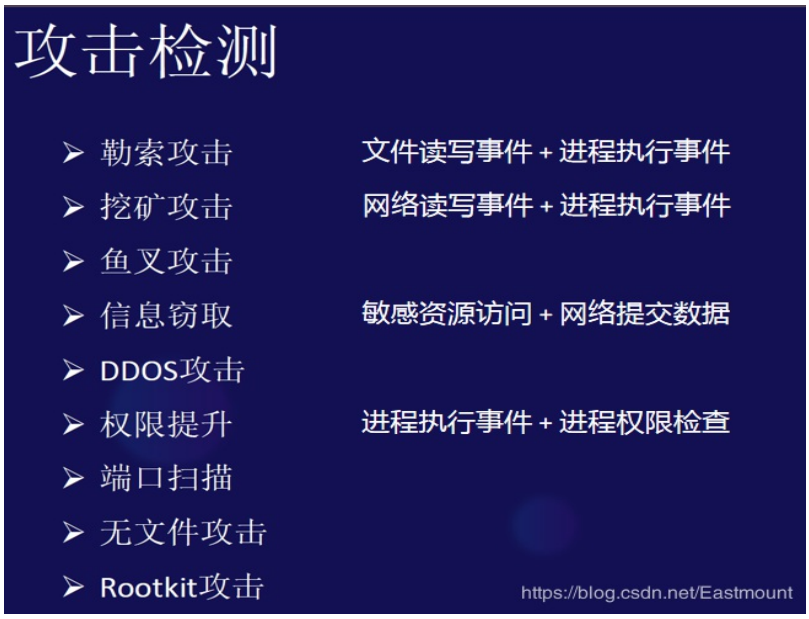
网络安全常用工具推荐如下，其中加粗字体是作者学习或使用过的优秀工具。

- **Fiddler（网络漏洞扫描器）**
- **Burpsuite（网络漏洞扫描器）**
- **NMap（端口扫描器）**
- **Nessus（漏洞扫描程序）**
- **Wireshark（手动分析包工具）**
- **SQLMAP（渗透测试工具）**
- **Metasploit（漏洞监测工具）**
- **Cobalt Strike（渗透测试框架）**
- Hydra（密码破J工具）
- Acunetix（网络漏洞扫描软件）
- pangolin（SQL注入测试工具）
- Ettercap（中间人攻击工具）
- Maltego（取证工具）
- OWASP Zed（攻击代理工具）
- Caidao（网站渗透工具）
- 中国蚁剑（网站渗透工具）
- 冰蝎Behinder（网站渗透工具）

系统安全分析常用工具推荐如下：

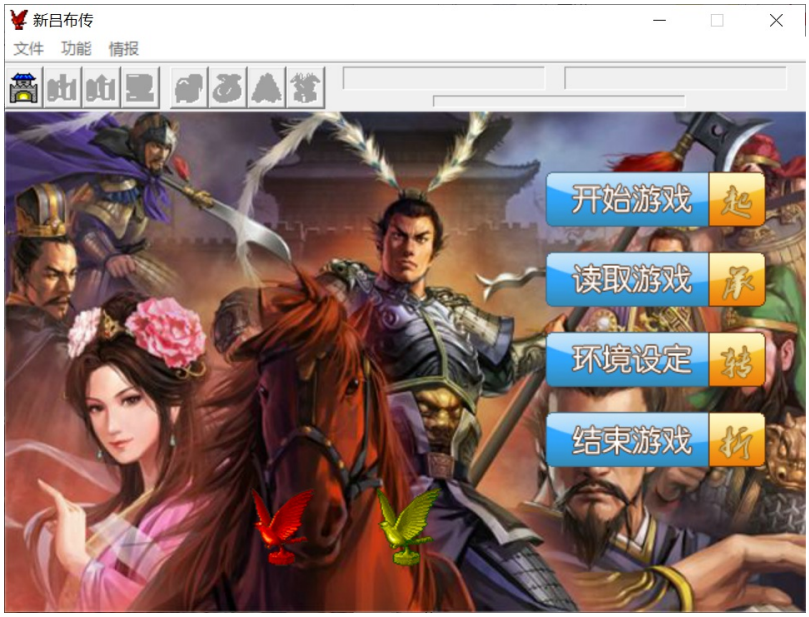
- **OllyDbg（动态分析工具 倚天剑）**
- **IDA Pro（静态分析工具 屠龙刀）**
- **Windbg（微软内核级调试工具）**
- **PEiD（查壳工具）**
- **Cuckoo sandbox（开源沙箱系统）**
- PEView（PE文件查看工具）
- 010Editor（二进制分析）
- Process Monitor（Windows监视工具）
- **Process Explorer（文件进程查看器）**
- **Cheat Engine（内存修改编辑工具）**
- Outpost Firewall（共享软件）
- hex editor（十六进制编辑工具）
- Ubertooth（蓝牙嗅探工具）
- 汇编语言编译器

下面分享2019年看雪安全峰会关于攻击检测和对抗的常见技术。



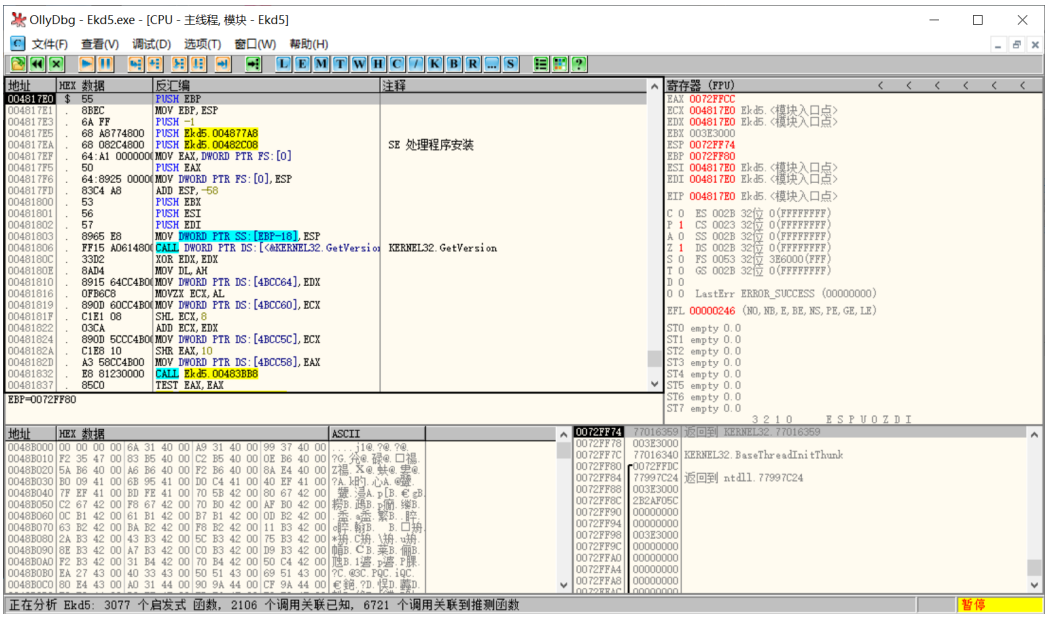
三.吕布传游戏逆向分析

下面以老游戏《新吕布传》为例，这是非常老的一款游戏。

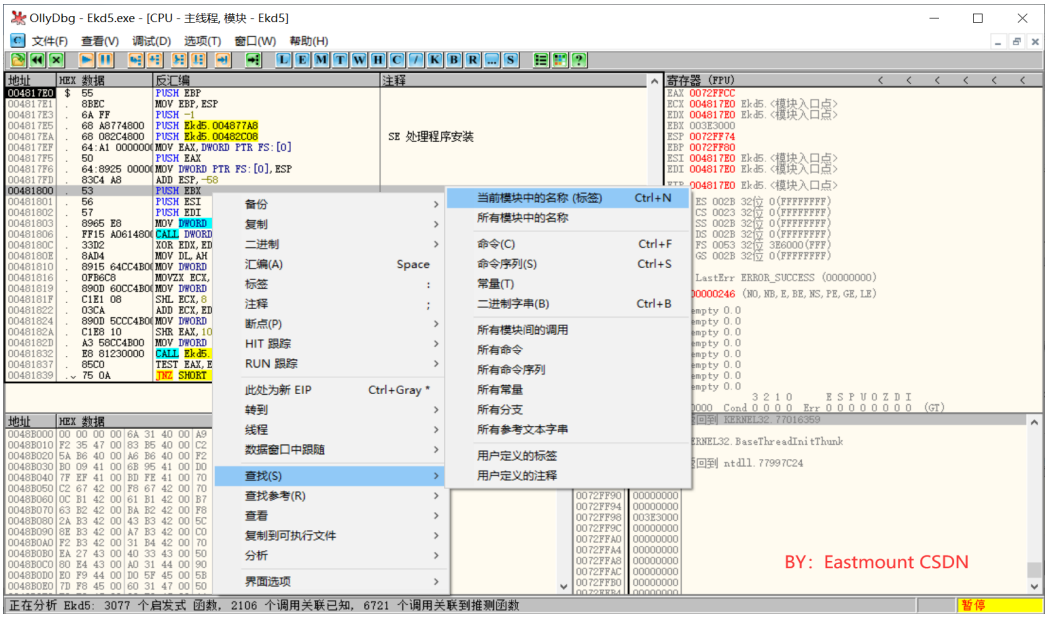


我们在玩这个游戏的时候会遇到一个问题，就是NPC说话太慢，在不断地过剧情，我们想逆向分析让它迅速完成对话，加快我们游戏的进程。

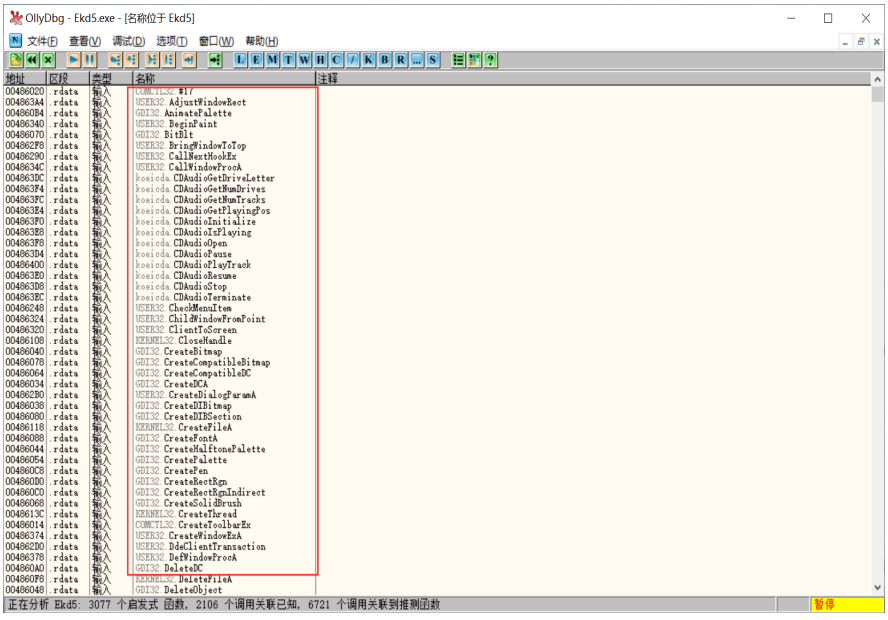
第一步，通过OllyDbg软件打开吕布传游戏“Ekd5.exe”。



第二，右键点击“查找”，选择“当前模块中的名称”查看该游戏打开了哪些函数。



返回界面如下图所示，包括该游戏需要调用的各种函数，并且猜测各种函数的应用场合。



第三步，发现两个异常函数。

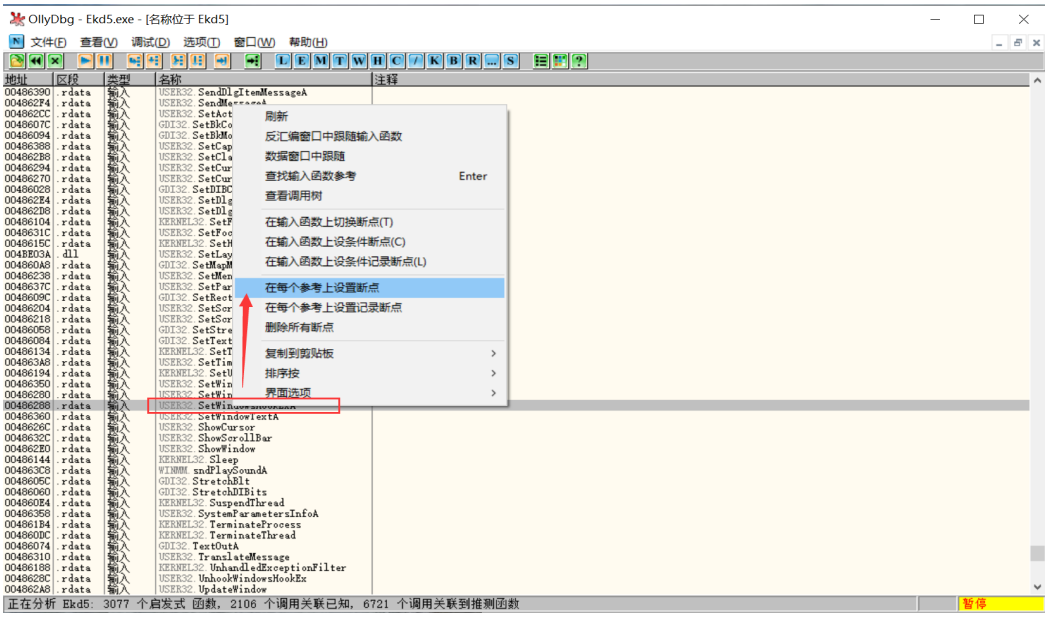
作者在游戏中设置两个钩子函数做什么呢？难道想检测我们的键盘吗？

- UnhookWindowsHookEx：卸载钩子消息函数
- SetWindowsHookExA：安装钩子消息函数

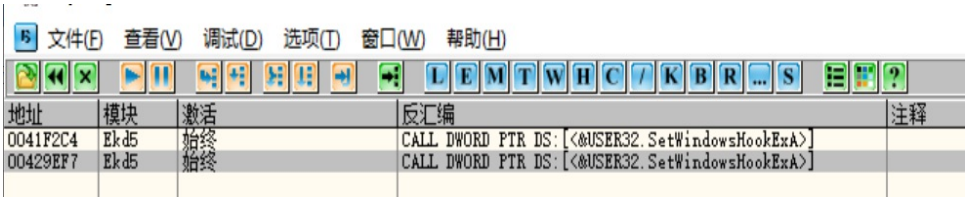
> PS：这些分析经验需要我们不断地实践来总结，这是一个大量反复训练的过程，目前作者也还在学习的过程，一起加油！

```
00486194 .rdata 输入 KERNEL32.SetUnhandledExceptionFilter
00486350 .rdata 输入 USER32.SetWindowLongA
00486280 .rdata 输入 USER32.SetWindowPos
00486288 .rdata 输入 USER32.SetWindowsHookExA
00486360 .rdata 输入 USER32.SetWindowTextA
0048626C .rdata 输入 USER32.ShowCursor
0048632C .rdata 输入 USER32.ShowScrollBar
004862E0 .rdata 输入 USER32.ShowWindow
00486144 .rdata 输入 KERNEL32.Sleep
004863C8 .rdata 输入 WINMM.sndPlaySoundA
0048605C .rdata 输入 GDI32.StretchBlt
00486060 .rdata 输入 GDI32.StretchDIBits
004860E4 .rdata 输入 KERNEL32.SuspendThread
00486358 .rdata 输入 USER32.SystemParametersInfoA
004861B4 .rdata 输入 KERNEL32.TerminateProcess
004860DC .rdata 输入 KERNEL32.TerminateThread
00486074 .rdata 输入 GDI32.TextOutA
00486310 .rdata 输入 USER32.TranslateMessage
00486188 .rdata 输入 KERNEL32.UnhandledExceptionFilter
0048628C .rdata 输入 USER32.UnhookWindowsHookEx
004862A8 .rdata 输入 USER32.UpdateWindow
004861E8 .rdata 输入 KERNEL32.VirtualAlloc
0048614C .rdata 输入 KERNEL32.VirtualFree
0048616C .rdata 输入 KERNEL32.WideCharToMultiByte
00486328 .rdata 输入 USER32.WindowFromPoint
0048610C .rdata 输入 KERNEL32.WriteFile
004862C0 .rdata 输入 USER32.wsprintfA
0048635C .rdata 输入 USER32.wvsprintfA
```

第四步，选中该函数右键点击“在每个参考上设置断点”。

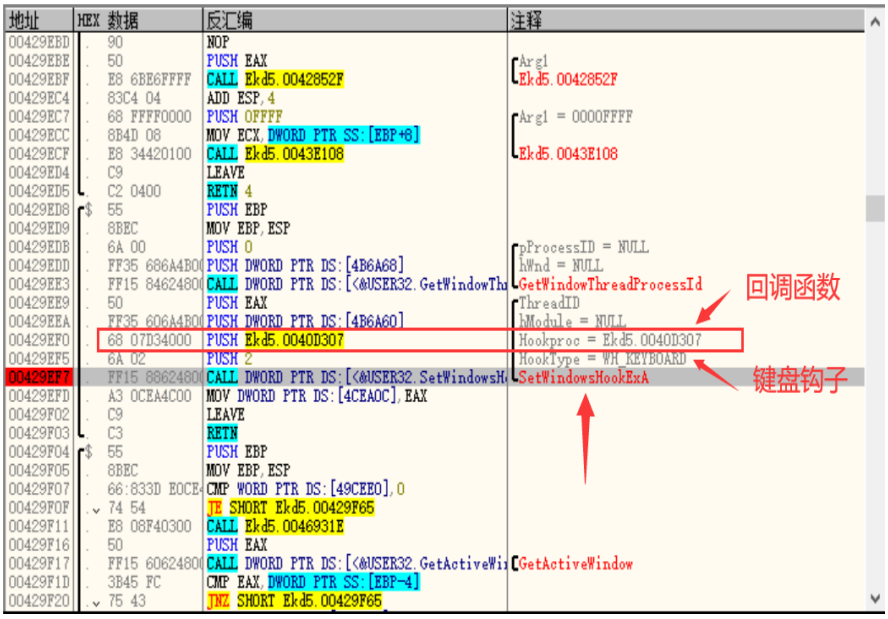


可以看到已经设置了两个断点。

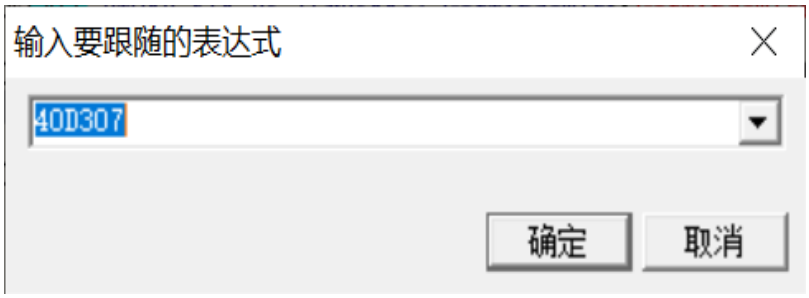


第五步，运行程序或双击断点可以进入反汇编窗口具体位置，可以看到它是一个键盘钩子，并且回调函数为0x0040D307。

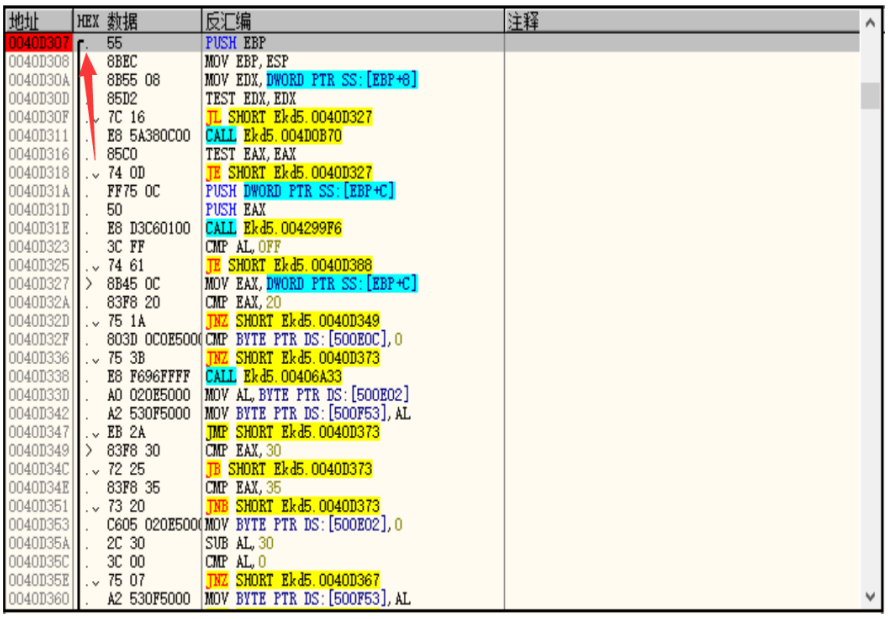
- Hookproc Ekd5.0040D307
- HookType WH_KEYBOARD
- CALL SetWindowsHookExA



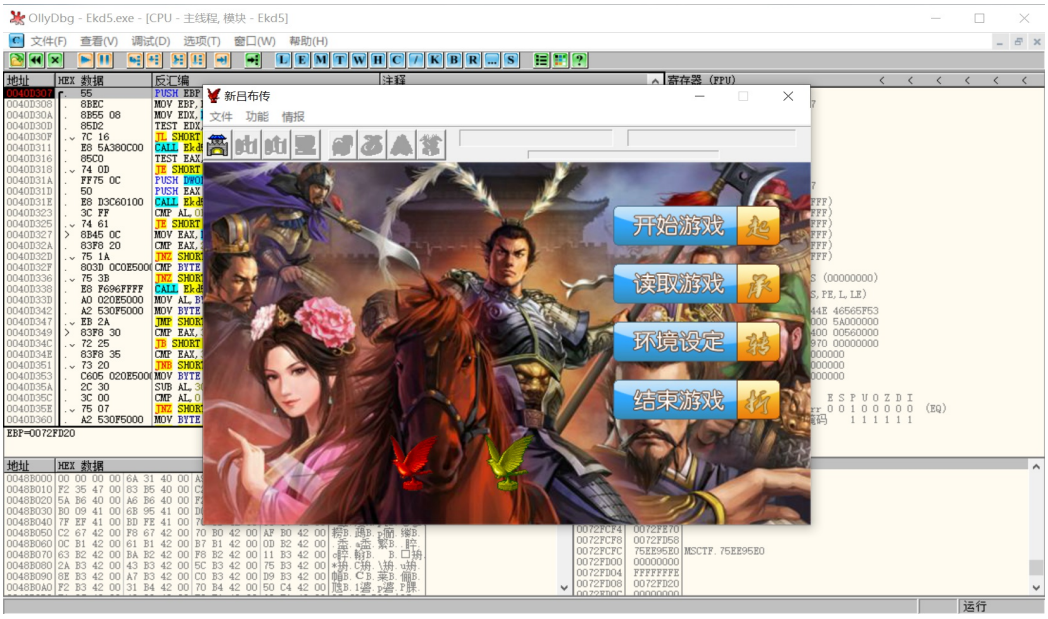
第六步，双击回调函数那行，复制地址40D307，输入Ctrl+G跟随到指定位置。



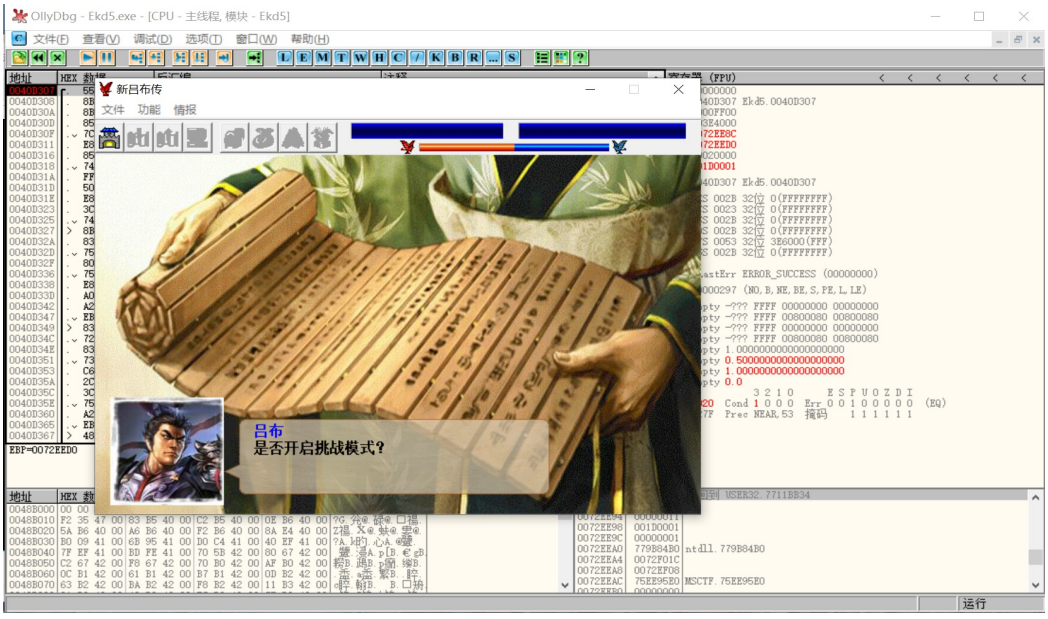
第七步，再跳转的地址0x0040D307位置按下F2，增加新的断点。



第八步，按下F9运行程序，并进入对话界面。

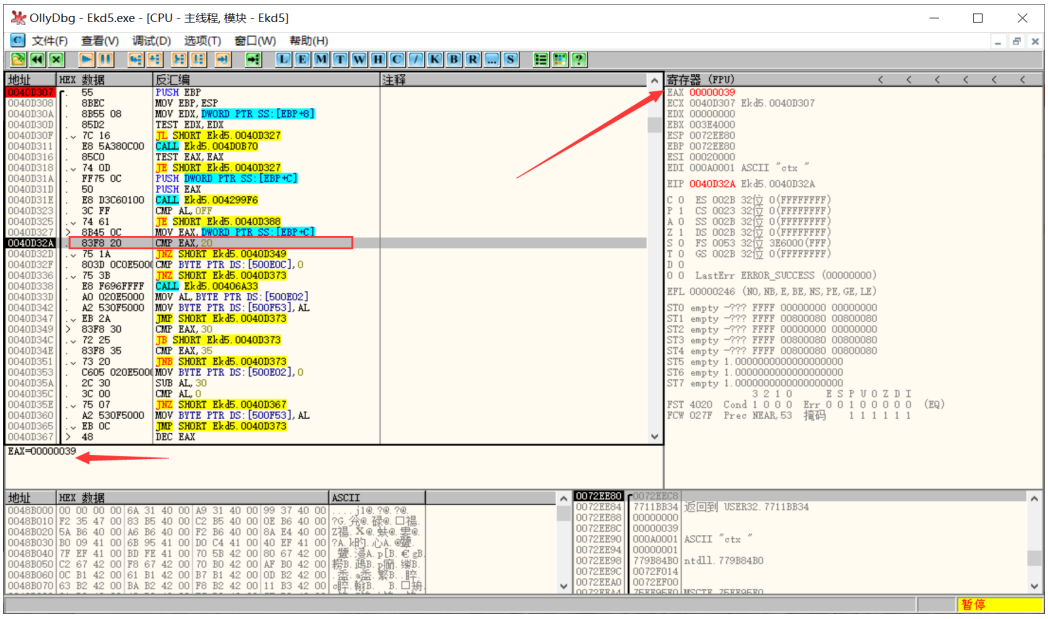


第九步，按下某个按键，我们来详细分析这段汇编代码。



作者按下的是数字“9”，其输出结果存储在EAX寄存器中，对应的十六进制为0x39，然后它会检测我按键的ASCII码是否等于0x20（空格）。

- CMP EAX, 20



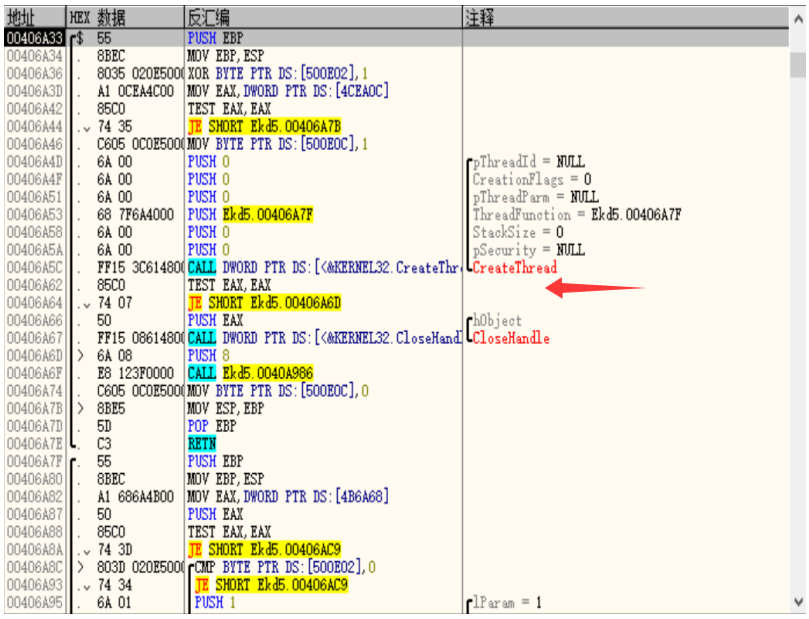
第十步，给该位置0x0040D32A下个断点，继续运行和分析代码。
当输入空格相等后，它会比较一个全局变量的值是否为0，然后进入新的CALL。

- CMP ptr [500E0C], 0
- CALL Ekd5.00406A33

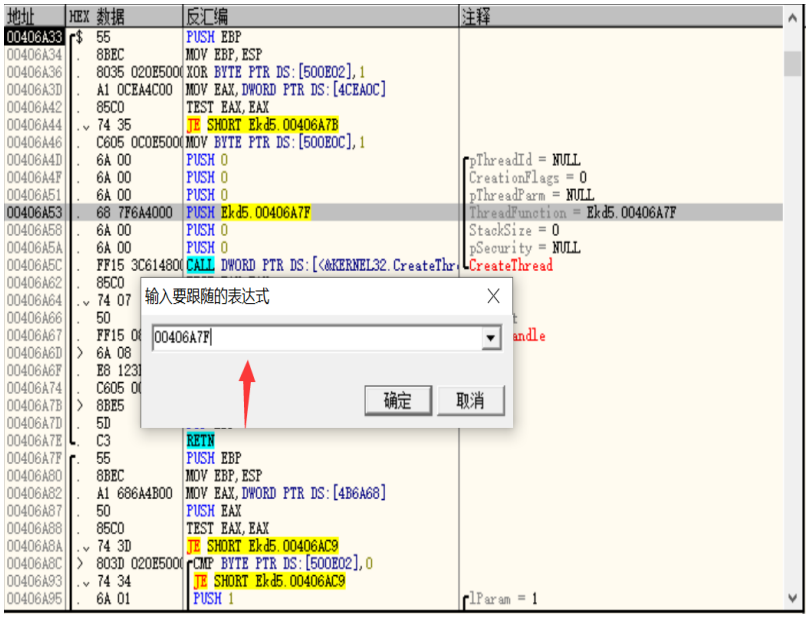
```
0040D30A   .  8B55 08      MOV EDX,DWORD PTR SS:[EBP+8]
0040D30D   .  85D2         TEST EDX,EDX
0040D30F   .v 7C 16        JL SHORT Ekd5.0040D327
0040D311   .  E8 5A380C00  CALL Ekd5.004D0B70
0040D316   .  85C0         TEST EAX,EAX
0040D318   .v 74 0D        JE SHORT Ekd5.0040D327
0040D31A   .  FF75 0C      PUSH DWORD PTR SS:[EBP+C]
0040D31D   .  50           PUSH EAX
0040D31E   .  E8 D3C60100  CALL Ekd5.004299F6
0040D323   .  3C FF        CMP AL,0FF
0040D325   .v 74 61        JE SHORT Ekd5.0040D388
0040D327   >  8B45 0C      MOV EAX,DWORD PTR SS:[EBP+C]
0040D32A   .  83F8 20      CMP EAX,20
0040D32D   .v 75 1A        JNZ SHORT Ekd5.0040D349
0040D32F   .  803D 0C0E5000 CMP BYTE PTR DS:[500E0C],0
0040D336   .v 75 3B        JNZ SHORT Ekd5.0040D373
0040D338   .  E8 F696FFFF  CALL Ekd5.00406A33
0040D33D   .  A0 020E5000  MOV AL,BYTE PTR DS:[500E02]
0040D342   .  A2 530F5000  MOV BYTE PTR DS:[500F53],AL
0040D347   .v EB 2A        JMP SHORT Ekd5.0040D373
0040D349   >  83F8 30      CMP EAX,30
0040D34C   .v 72 25        JB SHORT Ekd5.0040D373
0040D34E   .  83F8 35      CMP EAX,35
0040D351   .v 73 20        JNB SHORT Ekd5.0040D373
0040D353   .  C605 020E5000 MOV BYTE PTR DS:[500E02],0
0040D35A   .  2C 30        SUB AL,30
0040D35C   .  3C 00        CMP AL,0
0040D35E   .v 75 07        JNZ SHORT Ekd5.0040D367
0040D360   .  A2 530F5000  MOV BYTE PTR DS:[500F53],AL
0040D365   .v EB 0C        JMP SHORT Ekd5.0040D373
0040D367   >  48           DEC EAX
0040D368   .  C1E0 08      SHL EAX,8
0040D36B   .  B0 01        MOV AL,1
```

运行代码进入CALL函数，然后去到0x00406A33位置，如下图所示，发现它开启了一个线程。我们接着需要定位到线程的处理函数。

- CreateThread
- PUSH Ekd4.00406A7F

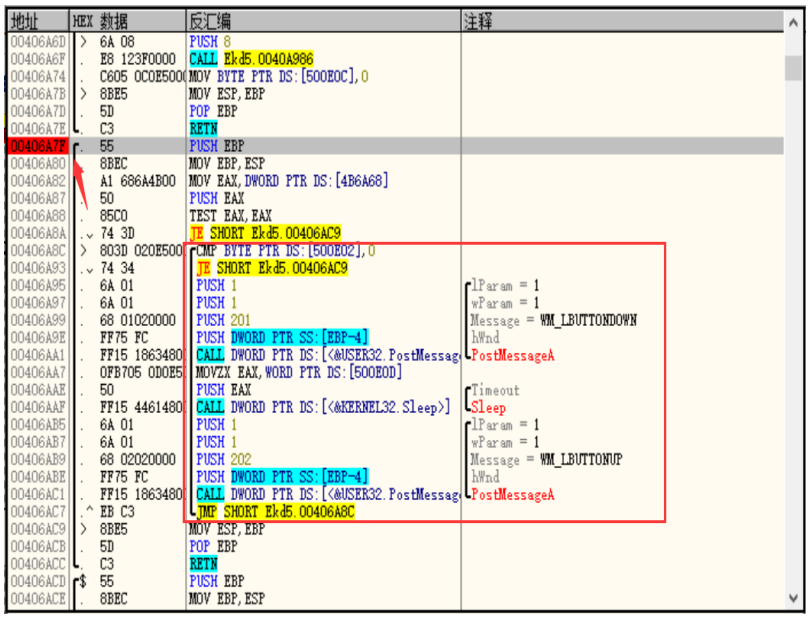


第十一步，按下Ctrl+G跟随到0x00406A7F位置，接着分析汇编代码。



给该位置下个断点，然后分析该函数内容。发现它首先比较状态，如果状态为0就设置个WM_LBUTTONDOWN消息，即点击鼠标。

- Message = WM_LBUTTONDOWN
- Message = WM_LBUTTONUP



然后间隔一个Sleep函数，时间为100毫秒，接着又设置一个UP消息，相当于左键按下后又弹起来了。

写到这里，我们发现空格的效果就是反复按下鼠标左键又弹起右键，原来该游戏已经自带了过场景的功能，就是按下“空格”，哈哈！但是该游戏的说明书并没有讲述这个按键的情况，相当于一个隐藏功能，这里大家也可以进一步修改制作游戏辅助器。这里主要是带领大家来学习下游戏逆向的过程，尤其是OD工具的基础用法。

总之，如果你喜欢逆向分析，会非常有意思，包括玩游戏也会从另一个角度思考；但如果你不喜欢逆向，千万别进这个行业，每天逆向代码看到想吐，可以换个喜欢的行业，因为逆向分析工作就是每天泡在代码堆里。

四.总结

写到这里，这篇文章就介绍完毕，希望对您有所帮助，最后进行简单的总结下。

学安全一年，认识了很多安全大佬和朋友，希望大家一起进步。这篇文章中如果存在一些不足，还请海涵。作者作为网络安全初学者的慢慢成长路吧！希望未来能更透彻撰写相关文章。同时非常感谢参考文献中的安全大佬们的文章分享，深知自己很菜，得努力前行。

《珈国情》
明月千里两相思，
清风缕缕寄离愁。
燕归珞珈花已谢，
情满景逸映深秋。

2020年8月18新开的“娜璋AI安全之家”，主要围绕Python大数据分析、网络空间安全、人工智能、Web渗透及攻防技术进行讲解，同时分享论文的算法实现。娜璋之家会更加系统，并重构作者的所有文章，从零讲解Python和安全，写了近十年文章，真心想把自己所学所感所做分享出来，还请各位多多指教，真诚邀请您的关注！谢谢。

(By:娜璋AI之家 Eastmount 2020-12-13 星期天 写于高铁)

参考文献：

真心推荐大家好好看看这些视频和文章，感恩这些大佬！

- 科锐逆向的钱林松老师受华中科技大学邀请-“逆向分析计算引导”
- c++学习笔记——VS2015中添加graphics.h头文件 - 行歌er
- https://www.bilibili.com/video/BV1J5411x7qz
- [网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
- [网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向