[转自看雪]新手学习计划

转载

weixin_30314813 于 2013-03-17 22:30:00 发布 48 收藏
原文链接：http://www.cnblogs.com/Wzqa/archive/2013/03/17/2965131.html

无意在sudami大神的Blog看到对初学者的一些建议。想想自己也才初学，如果就跑去驱动尝试理解Windows这套精密的仪器，应该是一件吃力不讨好的事情，我这样的拙劣的水平还是定一个低一点的起点，从最基础的部分开始学习吧。

sudami对初学者的一点建议

1．若对Windows底层开发没有兴趣，不建议继续深究， 若有些兴趣可以继续。

2．先广泛打基础，比如C/ASM/C++/MFC，再学习Windows核心编程，对R3上的一些开发有所熟悉，再系统的学习《操作系统》等书籍，理解整个系统的原理，构架，实现。

3．有了以上基础，可以开始阅读一些驱动入门书籍，如《Windows内核情景分析》， 多上google搜索资料，下一份WRK/ReactOS，没事翻一翻，搭好驱动编译环境后，可以尝试写些小驱动，在蓝屏中摸索总结，从而积累初级的经验。

4．等成了驱动开发初级工后，可开始学习Windbg，IDA的使用，多看源码多F1看帮助文档。

5．等熟练以上工具后，开始Windbg动态调试，IDA静态逆向其他驱动(包括微软自己的)。 在这一过程中，你又会接触到脚本语言，汇编知识点，Intel手册，加密解密，Vmware等一堆的东西，同样你需要熟悉它们。

6．等你熟悉以上东西后，可以给自己提些需求，并实现该需求，比如写个小型ARK，在这个过程中，你可以切实感受到开发一个程序是一个系统的东西，你又需要回到R3写界面，重温MFC，WTL等设计与使用。当然又要写驱动程序，保证兼容性等问题，这个过程是漫长的，期间你会发现写一小部分功能，你可以扩展收获很多知识点。

7．等你熟悉以上东西后，已经可以自己独立解决问题了，基本不需要到网上求助。
遇到问题，会利用WRK / Windbg / IDA / Google 等方式自行搞定，如网上有现成的解决方法，借用之，取其精华，唾其糟粕。 若网上没有现成的，则需要你IDA 系统文件，Load pdb；Windbg动态调试内核等手段自行挖掘，若网上只有类似的程序，你可以逆向其关键部分参考之，而后变成自己的东西。

8 .等你经历了以上7个阶段,你可以开始系统的了解Windows的构架，站在产品的角度思考问题，分析问题，解决问题，对自己多提需求，进而再去实现之，这阶段是积累经验的阶段。

9．基本能够胜任大多数公司的项目需求了。

想来能在看雪注册帐号，都是有兴趣的童鞋吧，就是缺少一颗坚持的心，希望自己能够坚持把这条路走下去。

在看雪不乏我这样的学习贴、计划贴、目标贴，不过我想我要坚持下去，争取2012结束时，能完成sudami大神建议中的第二条，“先广泛打基础，比如C/ASM/C++/MFC，再学习Windows核心编程，对R3上的一些开发有所熟悉，再系统的学习《操作系统》等书籍，理解整个系统的原理，构架，实现”，并有一篇自己的精华帖。

分解一下大神提出的学习计划，大概是两部分

基础学习：C语言，汇编语言，C++基础部分（不涉及C++中的高级技巧，STL，泛型等，只能够看懂C++封装的类就好）。
操作系统：Windows API，部分Windows系统特性，核心编程。

目标：能熟练掌握并应用C语言，对OD下的汇编指令能够阅读，使用C++的封装特性；熟悉常用的Windows API（函数，结构），熟悉Windows系统特性，能看懂大牛的文章。

此帖的内容主要是把sudami大神的学习心得从他Blog留言板拷贝来此跟大家共享。每天都要在工地搬砖，能用来学习的时间也不是很多，而且基础知识都是重复性的内容，我会尽量发在自己的帖子里，不占用论坛版面，也希望新手区的朋多多多帮助。

2012/3/21 revfish

原帖链接：

http://bbs.pediy.com/showthread.php?t=148217