推荐点书,说点学习路线...

转载

我是一只大菜鸟 于 2012-10-24 09:26:25 发布 792 收藏
[乱弹学习] by Tbit

;==========

0.扯淡的一些话

;==========

写出这个图书目录的作者的水平,就比你高一点点..哈哈,就是在论坛混的日子比你久一点,而且一些书过期了,比如:

<windows 深入剖析>,这本书 是清华社出的,当年的确很强大,那个时代同样强大的书还有;matti <未公开的windows核心技术>,walter oney的

<windows95系统奥秘>,多是9X系统下的东西了,NT结构变化比较大,过时了,但是依然膜拜作者...我也很无聊的翻过,西电图书馆有

而且分类也没分好..真是浪费啊.

;==========

1.大概的一个路线

;==========

我也写个我当年混过来的一些书:

+====>MFC路线:(这条路没走下去,MFC的书倒是买了<VC++深入详解>,<MFC深入浅出>

C/C++ --->asm-->SDK/API------ +

+====>系统底层:<undocumented win nt> <驱动开发技术详解> <寒江独钓><深入解析windows操作系统>

;==========

2.具体的书目:

;==========

2.1基础知识:

C/C++: <21天学通C语言>第六版,人民邮电出版社(我选这个没有办法,当年那个书店就只卖这个,结果我很悲剧的学着使用DevC++开始写程序...)

<C++ primer plus> 第五版,蓝皮书,人民邮电出版社.(讲的比较详细,而那个所谓<C++ primer> 第四版当时我觉得我可能看不大懂,现在

倒是想把<C++ primer> 第三版 搞过来了看看..)

asm: <汇编语言>第二版,王爽 清华社.(入门好书,把16位的汇编讲的很清楚,比那些IBM-PC汇编要强大点)

<Intel32位汇编语言程序设计>第四版,第五版均可以.罗云彬,温玉杰(hume)等译,(很强大的一本书啊,作者把不少函数写好了,嘿嘿封装起来,理解

起来就很容易了,这就是整体和细节的把握啊....)

;==========

2.2 ring3下:

;==========

SDK/API:<windows 程序设计> 第五版,Charles Petzold写的.(很经典的一本书,只有电子版的,虽然很多关于GDI操作的,但是看看也无妨,依然在看.)

<windows环境下32位汇编语言程序设计> 第二版,罗云彬编著(现在出到第三版了,看的时候配合下iczelion的教程,这个书比较强大了看这个,

你搞破解,学逆向多不是啥问题..哈哈,学着些PE文件感染型病毒..这个相当有意思,这本书YY掉了,必然上一个台阶..)

<加密与解密>第三版,段钢 编著,电子工业出版社.(也是相当不错的一本书啊,起码让我开始认识到很多调试器了,什么OD啊,IDA之类的,

也知道破解逆向是什么回事了.再配合看雪论坛,真的很强大,很多资料自己可以找找)

<加密与解密技术内幕>,这个是很老的一本书了,我看的只有电子版的..呵呵,也不错..

PS: 貌似我在学习的过程中,还七零八落的看了些其他的书,比如<黑客反汇编揭密>,<黑客调试技术>,电子工业出版社,karpaskey写的.

还有个<逆向工程揭密>(说实话,看这个的时候比较讨厌西电的那个陈贵敏(现在是西电的副教授..机电院的..),

(唉 team509那群牛真的不容易呢..BS国内的一些SB学者..)

<windows核心编程> jerry Richard著,现在出到第五版了,清华社有翻译.(翻译质量不错),英文名字叫<windows via C/C++>)

这本书看了两遍了,嘿嘿,相当经典啊,还是得继续看下去,很值得收藏..

;==========

2.3 ring0下:

;==========

系统底层:其实也不见得搞系统底层的就有多牛B,呵呵..但是牛B的人一般多搞系统底层..废话不说,看书目

<undocumented windows NT> 这个网上有中文电子版的,虽然是windows nt4.0架构下的东西,但那些思想以及关于NT的架构

可以让我们有个清晰的概念..(这个是俺不久前看完的...)

<windows驱动开发技术详解>,这本书讲的比较浅,算是个入门书吧,看了一半了..能让我们对NT驱动,WDM驱动的流程熟悉,

另外就是熟悉一些native api...把这个看完再来好好评论下)

<深入解析windows操作系统>MarkE.Russionovich和David A.Solomn著,潘爱民翻译(这个书绝对是无敌的,搞windows内核的不看这个,
那就没道理可言,强烈推荐!!! 鄙人看到第三章,由于种种原因 耽搁了一段时间,当我看完一遍的时候再来说话...)

<寒江独钓--windows内核安全编程>,感觉也是一本入门书,只看了第一章关于WDK..但是已经买了有好几个月了..呵呵,也是值得推荐

(有讨论文件透明加密,和NDIS..看完再说话..)

;==========

其他关于系统底层我看过的一些书:

<rootkit--- windows内核安全>,也算是一本驱动入门书籍,如果从来没接触过内核ring0层次的话,这个倒不错的选择...

<kmd教程> 这个主要是讲使用asm开发驱动的,俄罗斯强男 Four-F整理出来的开发包..膜拜...和<驱动开发技术详解>一个层次上的书,

不过一个是讲C,一个讲asm...而已..

<Programmming windows Driver Model>,walter oney写的,很详细的一本驱动入门书,打算接下来就看这个了....

其他还没看的:

<windows内核情景分析> 毛德操编著.这个比较厚,没看过..不知道怎么评论好...

<软件调试> 电子工业出版社,张银奎著,很无敌的一本书啊,我觉得作者很牛X,这本书很为国人争光...

<windows NT/2000 native API reference> 昨天刚把这玩意儿打印完,480多页呢..35RMB...唉..纯英文的..哈哈..

<undocemented windows 2000 secrets> <windows file system internals> 这两本也是 很强大啊...

参考网站:bbs.pediy.com www.debugman.com forum.sysinternals.com www.rootkit.com www.openrce.org

;==========

;3.Others

;==========

其他的一些:

MFC: 买了孙鑫的<VC++深入详解>,那个时候学完api的时候,玩了下MFC啊,还买了本 侯杰的<深入浅出MFC>第二版呢..没怎么看

另外就是潘爱民翻译的<VC++技术内幕>,有第四版和第六版的,也是本MFC的入门和参考书籍,第六版多了个.NET...

shellcode: 当年可是有当网络hacker的梦啊,所以觉得这玩意儿很神秘,当时把<加密与解密>看了大半后,玩了下shellcode,看了科普书

<0day:软件漏洞分析>(应该是这个名字) 电子工业出版社,failwest编著的,西电图书馆有两本...貌似两天把这本书看完了..

其他的关于shellcode的,觉得比较厉害的就<安全编程修炼之道> 还有个S级的<网络渗漏技术>这可是暗礁的四头牛写的,

跨4个操作系统平台...,windows,linux,power pc,solaris...膜拜ing...

病毒: 这个书籍不好推荐,一般多是网上资料..有一本倒是不错<计算机病毒防范艺术>,另外关于病毒的书多是些垃圾...

virus方面的资料,中文的:看雪上有一点,cvc当年出过一本精华帖的集合,还有个NE365的书

主要还是国外的病毒杂志,最牛B的就是29A了,呵呵,http://vx.netlux.org/上可是有不少资料啊..很强大

要知道病毒中的多态和变形技术是很能和加壳软件结合起来的,我可也是个初学者..正在学习ing...

数学方面: 先说说密码学这块吧,其实我自己也没怎么看,有本<密码学的原理与实践> 第二版 ,第三版 均可以,电子工业出版社,冯国登译

貌似这人,还是西电杰出校友.这本书我就看了个古典密码啊,有点线性代数知识就可以了.另外就是<程序员密码学>很多C的例子,

沈晓斌翻译的,还有个看雪的密码学版块,可以参考.

再说点算法类的,这个我还真不敢乱说话啊,自己就看本<离散数学>,电子工业出版社.数据结构就翻了两下,有本<数据结构(C语言描述)>

貌似不错啊,<算法导论>,kuth的三卷书(貌似出了第四卷了?)这些看了,你就无敌了...哈哈..估计程序界能和你比算法的没几个...

电子书籍下载: www.shubulo.com, 邪恶八进制的电子书区,看雪的资料下载吧,貌似就这些....

;==========

;the end

;==========

最后好像没什么好说的了,路线大概是个这样子,其实有时候想想,搞MFC,做VC程序员也不错,但是我感觉自己真没什么艺术天分,看到图形设计就头大的很...

自己乱七八糟看的书也不少,显然上面推荐的路线,应该还算是比较规矩吧,呵呵,应该不会走火入魔,其实说到底,什么路线多是一样的,该会的你自然就会了

不明白的你永远多明白不了,学习感觉没有太多章法好说的,关键还是在于自己坚持,坚持久了,你自然也就懂的多了.看书翻书的时候,其实注重看看前言

序,和目录,有些话其实作者讲的很清楚了.对于资料,尽量还是买实体书吧,这样自己看起来也方便,也算是对作者版权的一个尊重.(别以为书很贵,其实珍贵的是

自己的时间,关键在于自己肯不肯花时间上去学习...把这些书静下心来好好看完..) 很显然我这些做的很不够

Author: by Tbit

Email: ttchen7#gmail#com