逆向入门指南

0x00 基础

- 1. 扎实的编程基础(包括**必须会的C语言**、最好还有一门**特别擅长的别的语言比如 Python**)
- 2. 入门时需要对汇编有个**大概了解**,对汇编的深入理解可以放到**逆向进阶**的时候再来
- 3. 有一颗持续学习下去的心(这是最难的一点)

学技术的道路注定是枯燥无味的,而且也会有很多坑,摔残了,出来了就成为了强者;出不来,就断了自己的学技术之路。

0x01 相关书籍

- 1. 《有趣的二进制:软件安全与逆向分析》(这本书用于确定你是否真的想学逆向)
- 2. 《逆向工程核心原理》
- 3. 《C++反汇编与逆向分析技术揭秘》
- 4. 《Android软件安全与逆向分析》《iOS应用逆向与安全》
- 5. 《汇编语言》《intel汇编语言程序设计》(**只针对入门而言不需要学得太深**)

0x02 工具

- 1. IDA 7.0+
- 2. 吾爱破解工具包(里面工具较老,需要自己去寻找新版)
- 3. OllyDbg(吾爱破解有专版)
- 4. x32/64dbg
- 5. 带插件的gdb(peda, gef, pwndbg)

0x03 学习相关网站

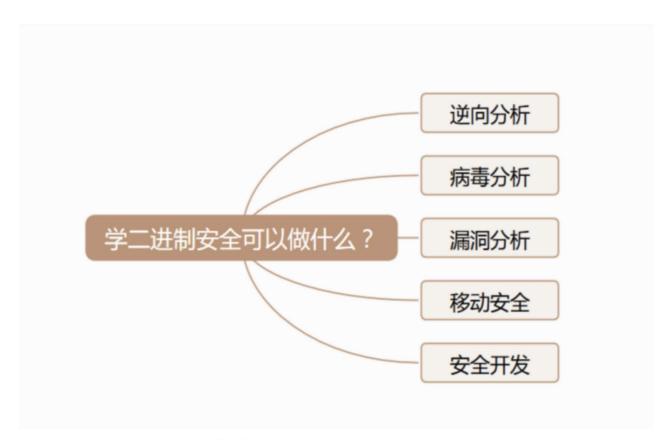
开发相关--菜鸟教程 <https://www.runoob.com/>

吾爱破解 <https://www.52pojie.cn/>

看雪论坛 <https://bbs.pediy.com/>

还有很多网站,不过不是通用适合每一个人的,就需要自己去寻找了。

0x04 学二进制安全可以干什么呢



0x05 来自其他学长的建议

