About us

广东工业大学 A&D 攻防工作室是专注于网络安全技术的学生团队。如果你热爱网络安全，崇尚极客精神，来加入我们吧，一起学习网络安全技术，组队参加各种安全比赛（CTF），参与安全项目，共同成长~

虽然正式招新还没开始，但暑假是一个很好的自主学习的时间，对网络安全感兴趣的同学们可以先加我们的招新群，安全相关的学习上有什么问题和困惑都可以在群里提出，师兄们会尽力解答帮助大家，共同交流。

A&D 攻防工作室 2019 招新群：904533878

逆向入门

从大方面来说逆向就是要了解代码是如何工作和怎样对数据进行处理。

逆向可以走很多有趣的路，如安卓逆向，Windows 逆向，病毒分析，软件漏洞挖掘等等。

最可能已经接触到的小方面逆向的应用：软件的破解（也就是盗版），游戏汉化（脱壳）。

走向其他有趣的道路需要先学一些基础：

c 语言基础（大一如果上过 c 语言程序设计掌握得不差就够了，后续有需要再深入）
汇编语言（推荐 王爽老师的《汇编语言》，b 站上有小甲鱼学习《汇编语言》这本书的视频）
调试器的运用（《加密与解密》这本书有 Windows 上面各个调试器的讲解，Linux 的调试器一般用 gdb，用法自行百度，b 站小甲鱼的调试篇也可以看看）

如果要走 CTF 逆向的学完上面的基础，调试器的运用可以在做 CTF 的题的同时熟悉用法，推荐攻防世界（https://adworld.xctf.org.cn/）对小白比较友好。

如果要学破解软件，可以继续看 b 站小甲鱼的脱壳篇，或者可以转战吾爱破解和看雪论坛

CTF 注重数据的处理（加密算法），破解软件看重代码流程的分析，但这只是浅层次地说，深入点学习就看选择着重的点了。

调试工具：
olly debug（简称 OD）用于动态调试

IDA 用于静态调试和动态调试，功能强大

Windows 专用调试：windbg 可用于调试用户程序和内核程序，或者查看一些内核数据结构

Linux 常用调试：gdb（因为不熟悉请看 pwn 入门，或者自行百度）

建议虚拟机中进行逆向的实践，不要装杀毒，保存个快照。

虚拟机软件-如 VMware Workstation Pro

镜像-http://www.msdn3.com/index.html

---以上是来自学习 Windows 逆向萌新的一点看法，入坑需谨慎。