初探二进制

gnol3

前言

学习二进制是一个周期较长的过程，本文为初探二进制必备的初步知识点。如果你有更好的看法与网课，以你为准。本文出现的**所有书籍会打包上传至百度网盘/夸克网盘**,资源包见文末取。

说明：橙色样式都是超链接，在电脑上用PDF阅读器打开后鼠标点击能够直接打开网站，比如点击此点会跳转到ctf-wiki

C语言基础

> 网课：B站C3程序员入门视频
>
> 教材：《C Pirmer Plus》

对于C语言要熟悉基本语法，了解指针，了解结构体等知识点。

汇编基础

> 网课：汇编语言从0开始 虽然是10元，但是全部都能免费看，只是附件无法下载
>
> 教材：《汇编语言》(王爽) 《x86汇编语言：从实模式到保护模式》《C++反汇编与逆向分析技术揭秘》

对于汇编，前期把几个重点指令功能了解清楚就行，比如mov/test/cmp/push/pop/leave/retn/call，不一定要自己手写一些汇编程序，但一定要知道指令在说什么。且这一部分知识可以直接看王爽著的教材，网课是你遇到不理解的知识点的时候，查看对应视频起辅助理解的作用(所以网课的附件不用管)。经过我们不断的做题学习的过程后，我们的汇编水平也会随之提高。

后面两本书是拔高的时候看的，其中从实模式到保护模式会对之后的操作系统的学习起到部分帮助，而C++反汇编与逆向分析技巧能够让你更加理解C++的原理，且学习到对应的逆向技巧。

Linux使用基础

> 文档：《ctf-all-in-one》一书中`1.3.LINUX基础`

使用VMware Workstation安装好Kali或者Ubuntu，一开始不用配置任何环境，先把Linux常用命令敲熟练。对于`1.3.LINUX基础`中常用基础命令，Bash快捷键，权限管理，字节序，文件描述符，调用约定为初部接触的必看内容。

初探漏洞利用

> 网课：你想有多Pwn CTF-PWN环境初配置
>
> 教材：《从0到1:Ctfer成长之路》《CTF训练营》《深入理解计算机系统》等
>
> 文档：ctf-wiki CTF-PWN虚拟机环境配置

其中，`你想有多Pwn`与`ctf-wiki`皆为教程，初学者因该以视频为主实践为主，文档为辅(当然你的理解能力够强，直接上手wiki也不是不行，但是视频里面的一些调试手法在文档中可能不会体现出来)。当上手后，再以文档为主，跟着文档所写案例来便调试程序边学习知识。教材起到的作用为查漏补缺，因为文档中可能有些知识点文档书写者会默认大家都懂，但是互联网上的资料质量高低不一，教材可能会更加细致且正确的表述。总之就是零星知识看"互联网论文"，系统知识看书。

`CTF-PWN环境初配置`与`CTF-PWN虚拟机环境配置`为配套的Linux下pwn的环境配置教程，如果Linux使用不够熟练的同学可以参考视频中的操作配置，每配置完一个环节后应该检查是否安装成功(安装过程中飘红或者出现Fail，IGN等字样肯定是安装失败了，可能首先需要检查换源是否成功，与github相关的另算)，如果不成功则先在文档中查看是否有解决方案，如果没有可以先尝试百度，如果刚开始学习不知道查询什么内容，可以私聊本文作者。当然你也可以找别的教程，这里单独提这个，仅仅是因为是我暑假花了一周重新安装了各种系统然后总结出来的一个文章，你遇到问题我打概率都遇到过，能够更好的解决问题。

后记

以下书籍会帮助你更好更全面的了解整个计算机学科知识体系。(书籍排名不分先后，但第一本值得最先阅读)

- 《深入理解计算机系统》
- 《程序员的自我修养：链接、装载与库》
- 《操作系统真象还原》
- ......(每个人应该会有每个人心中的答案)

pdf资源包(总共600M+)：

- 百度网盘：点此进入
- 夸克网盘：点此进入

pdf阅读器推荐，万兴pdf，福昕pdf阅读器，drawboard pdf，edge浏览器