Pwnの引导

介绍一下Pwn

中文一般称作**二进制漏洞挖掘**，在ctf中的题型如下：

办赛方会给你一个程序，你要通过各种手段找出它的漏洞。你的目标电脑上运行着这个程序，你可以利用这个漏洞得到那台电脑的控制权，并且在上面找到flag！

听起来可太酷了😄

特点

比较硬核，需要很多相对其他方向更加底层的知识，如操作系统、汇编语言等等

适合这样的人：

- 坚定走网安的道路，或者想成为帅气的大黑客
- 对计算机偏底层的知识感兴趣，想搞明白它如何运转
- 想破解软件、写游戏外挂、挖漏洞
- 想成为ctf战队中珍稀的Pwn爷爷
- 喜欢硬核的东西
- ……

而且很多知识是各个计算机方向都需要、而且重要的，了解一下绝对不亏！

前言/方法论

0基础的最好看看，不感兴趣可以跳过

这是一个指北，而不是系统的入门教程，不可能覆盖到方方面面。如果你不知道Linux是什么，你甚至很可能觉得连这个文档都是天书，这很正常，因为我自己当初就是这样。

> 但请你别急

你不可能认识所有名词，我也不可能解释所有名词，但如果你看到它们的第一反应不是去查而是感到害怕、选择放弃，那谁也帮不了你。

相信我，这个文档写的都是最最最最基础的东西，有什么不懂的**上网搜索**一定能找到答案。

在学习的过程中会不断有“这东西这么简单怎么我当初还学得那么艰难”的想法出现，请习惯这种感觉。

勇于做必要但不那么容易的事情（或者说跳出舒适区？有点营销鸡汤味，不喜欢），下面是我自己的例子：

- 为了熟悉Linux的用法，我只用vim和终端写过一段时间代码
- 为了提高英语能力，我强迫自己看英文原版书（当然只是技术书）、用英语搜索问题、看官方英文文档，大一刚开始时看到大段英文会害怕头疼、看书必须要中英文对照，但现在我基本能脱离中文进行计算机学习
- 以前十几年间的寒暑假我从来没有学习过，但现在我开始尝试在放假期间学习
- 尝试早睡（虽然今天又寄了）

我想重点说一下英语，现在的我依旧听不懂六级听力，看不懂其他领域的英文文章，但我成功把英语提高到了我需要的水平（说白了就是能看懂计算机术语），这也给我带来了很多好处：各种优质的网站（Stack Overflow）、更容易理解的课本（相比中文生硬的翻译）、质量极高的在线课程（https://csdiy.wiki）...其实没有那么难，这种单纯堆熟练度就能做到的事情也许反而是最容易的。

而且英语是躲不掉的，因为害怕它而逃避只是没有意义的拖延，学习中生活中有很多这样的事情，我将它们概括为“必要但不那么容易”，Linux的操作也是、平日里学习的能力也是...意识到这一点之后，要做的当然就是勇敢面对、慢慢改变，稍微坚持一下，时间就是最强大的帮手（我真的不是在写鸡汤...）。

动手能力至关重要：

- 分配好理论和实践的比重，只看书一定会枯燥，并且掌握不牢
- 遇到问题先自行搜索，大部分问题都已经有人给出过答案，这时候找人问反而降低两个人的效率
- 下面的环境配置没有给出详细步骤，不如把它们当成一些锻炼

我也走了很多弯路，和其他几个写指北的大佬相比是大概最菜的ToT，现在有很多能力不足、很多东西想学。虽然时常对这些弯路感到惋惜和后悔，但转念一想，它们也是我成长到现在这样的必经之途。

我好像把指北写成了励志文...但不管了捏，任务几句话就能描述完，详细的步骤网上一定遍地都是，用它们水大量篇幅不如说点真正想说的^_^。

希望能帮到那些想学但感到迷茫的人...纠结一天“我以后要做什么”不如立刻行动一个小时，反正它们都是一定要做的，为什么要在完成它们之前想以后的事情呢?

总之，大家好好学习、一起努力!

基础知识

书都在群文件里

- C语言：《C程序设计语言》
- 汇编语言：《深入理解计算机系统》第三章
- Linux：最最基本的操作，能配好环境那就够了
- Python：只是写简单的脚本，会C语言之后基本不用学

实践：在你的Linux下写一个C语言程序并编译运行

不要试图先把所有东西学完才开始做题!

不要试图先把所有东西学完才开始做题!

不要试图先把所有东西学完才开始做题!

学完够用的知识后即刻动手做一道最基础的Pwn题，比如BUUCTF中Pwn分类下解出次数最高的几题。

Pwn没有那么可怕，入门难度的题并不需要你是一个C语言大师/汇编大师/Linux大师/Python大师，不然又怎么能叫入门? 学习和做题穿插，可以在成就感中体验打怪升级的快乐。

环境配置

推荐程度由高到低，默认你使用Windows系统

- WSL：安装 WSL | Microsoft Docs
- 虚拟机：Download VMware Workstation Pro（激活码怎么找？）
- Docker：skysider/pwndocker: A docker environment for pwn in ctf
- 物理机：有这种想法的大概不需要看这个文档

需要的工具：IDA Pro、pwntools、pwndbg

后面两个是Linux下的工具，你可能需要换源或者配置网络才能成功安装，这些都是很好的实践。我当初也觉得这很困难，但请利用搜索引擎、动手尝试！这也是一种学习和提高！

参考：pwn 环境搭建（wsl/vmware），一样的道理，一开始并不需要用到所有东西，学习过程中会慢慢接触。

其他

- 实用的网站？请看群公告
- 有实在查不到的问题？找Pwn方向的管理员，比如Limiter
- moectf{QwQ_We1com3_t0_pwn_ToT}