Pwn入门指北

欢迎大家点进来这个文档，可能大家都是带有Pwn是个啥玩意的疑问才点进来这个文档的，既然如此，就别急着离开，让我给大家讲讲Pwn这方面的内容。

Pwn指南参上！

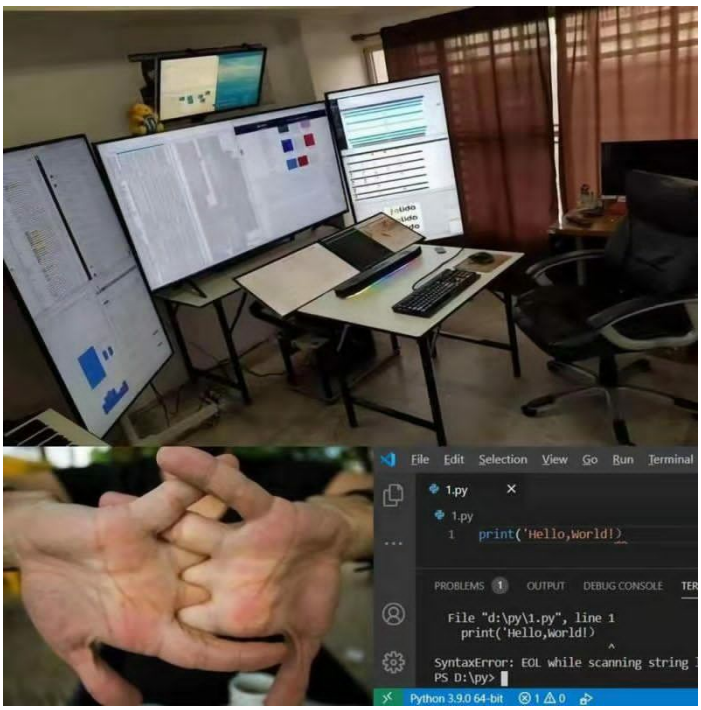
介绍一下Pwn

Pwn是什么，Pwn在中文里面又叫**二进制漏洞挖掘**。这个词最早源于网络游戏社区，起初是一种拼写错误，后来逐渐被接受为一种表达方式，用来表示在游戏中击败了对手。在计算机安全领域之中，Pwn用来描述成功地攻击或控制计算机系统、服务器或应用程序，实现了对目标的控制。（是不是有些像我们平时刻板印象上的黑客）

在CTF的比赛中一般如以下形式：

出题人会给你一个二进制的程序，再给你一个挂载了这个程序的靶机，而我们所需要做的就是在本地找到这个程序的漏洞，运用所学通过发送攻击代码去攻击远程靶机，从而获取靶机的控制权，找到flag，简直就是黑客帝国的感jio，有木有？

是不是听起来很酷？有种想学的冲动？[doge]



这个方向虽然看起来很NB，但是需要**很牢固的计算机底层知识作为基础，研究的东西难，门槛相对于其他几个方向来说比较高（先别急着退出去，我好不容易敲那么多字，起码看完再做选择吧o(┬﹏┬)o）**。

但你先别急，~~让我先急~~，虽然研究的东西难，但是你可以很清楚的知道程序底层是如何实现的，这个程序又是如何跑起来的，还有各种各样的漏洞是怎么出现的，我相信你学了之后肯定会对计算机的了解站在一个更高的角度，可以满足你的好奇心。

基础知识与工具

Pwn前置知识的多，决定了这个方向的门槛高，那具体要学啥基础知识与工具呢？大致有以下几部分：

- C语言基础，推荐《C Premier Plus》（这是基础中的基础，一定得学的，怎么说也至少得看的懂程序大概吧）
- C语言与内存，推荐《C与指针》
- 汇编语言基础，推荐《汇编语言》王爽版（这个同上，大概看得懂就行）
- 有一个能做Pwn题的Linux环境，同时需要点Linux知识（这边建议使用WSL2+VScode，系统选用Ubuntu，当然直接装kali或debian之类的虚拟机也是可以的）
- 会用Python写简单的脚本
- 会用一些工具如：IDA Pro，GDB，Pwntools等，这里只是举了几个基本工具，还会有很多工具要求你在后期学习过程中自行挖掘（大部分工具在github上都可以找到）
- Typora的使用,这里其实不一定得这个，只要能记录你学习过程的都可以（写心得之类的），记录很重要，它不仅能在后期帮你快速回忆与许久未用的已学知识点，同时也记录你学习的过程十分有意义

学习序列

当你们掌握好上面C语言与汇编，准备好工具之后就可以正式开始学习Pwn相关知识啦(^O^)/

1. ELF文件结构
2. X86-C语言惯用函数调用约定
3. Linux进程空间结构
4. 栈溢出原理
5. ROP技术

... ...

怎么学

---

1. 在学习的过程中，一定要先**学会自己使用搜索引擎（这个真的很重要）（魔法真的很重要）**，找不到的时候可以换换搜索引擎（像谷歌，Bing，ChatGPT啥的），说不定就出来了

2. 多动手，什么地方不明白的时候可以自己动手试试，还有就是学习了新知识也得多动手敲代码练习，**不要学了很多理论知识但不实操**，学一点练一点才能让你弄明白这些知识
3. 遇到了难以解决的问题，可以向学长寻求帮助（学长们都很友善的，尊嘟），但提问前记得注意下提问的方式，建议可以看看《提问的智慧》（别到时候和问问题的时候，学长反手给你甩个《提问的智慧》就gg了）
4. 保持记笔记，写心得的习惯（可以写在个人空间里也可以写在其他地方），及时记录下来学习的内容以及遇到的什么问题，这在自己回头看时会是很大的资源

其实不管什么是什么方向，耐心和恒心才是最重要的，只有在这条路真正能坚持下去，才有可能走的远。

资源网站

- CTFwiki（这里面有很详细的技能树）
- ctfhub（这里面的技能树可以配合ctfwiki使用）
- buuctf
- nssctf
- Pwncollege
- pwnable
- ...

剩下的就等你们自行探索吧（~~前面的区域以后再来探索吧bushi~~）

其他（~~学长吹水~~）

jyx：Pwn方向非常有趣，剩下我想说的大多都在上面写给你们了，就等你们自己来探索这个领域了，有啥事都可以来找我（~~乐子人就喜欢找乐子~~），最后我只想说欢迎学习这个方向，也欢迎你们加入我们实验室。（~~实验室里个个都是人才，说话又好听~~）

dyl: 学习pwn一定要多动手调试和写脚本，不要一直看理论不实践(血泪教训），多动手能加深印象并且更好的理解学到的理论知识，希望你们可以在感兴趣的方向上所向披靡

Hyrink：虽然总是说pwn的学习门槛高，但其实所有方向最后的难度都是相似的，或者说最后都会通往一个方向全栈。所以如果你对pwn感兴趣，那么请坚持下去，秉持着好奇与激情不断往其中发起挑战。go！go！go！

结尾

最后还是希望大家能够进入Pwn这个方向来学习，愿各位选择该方向的新手能够在这条道路上不断前行，在这个领域里不断深耕。