# Pwnの引导

~~CTF最強伝説とBinaryの漏洞挖掘！PWN一郎です 参上 ！~~

正经一点，欢迎来到MoeCTF 2023，更欢迎你抱着各种好奇心来到pwn的领域:grinning:

既然你点开了这份文档，我在这里就很期望你读完（里面会有一些我不知道到底算不算废话的东西）然后对pwn这个领域有一个小小的了解，如果读完了对pwn有兴趣是作者最想看到的:heart:，如果不感兴趣的话，也希望你能在Moe中找到你感兴趣的那一部分，希望玩得开心:happy:

## 0x00 介绍一下Pwn

如同上面那句话一样，pwn在中文里叫做**二进制漏洞挖掘**，在CTF中普遍的形式如下：

出题人会给你一个二进制程序，还会再给你一个环境/靶机，你需要在本地找到这个程序的漏洞，然后运用各种攻击手段向远程发送攻击代码，从而打通远程的靶机，得到它的控制权，并且找到flag:grinning:

是不是听起来就有一点大伙理解中的黑客气息了？

但是先别急，这个方向与计算机底层的知识联系密切，需要你对底层的知识有丰富深刻的了解，研究的东西很难很复杂，门槛是有点高的，例如：

- c语言中某些函数的机制漏洞
- 对于某些保护机制的绕过方法
- 对于代码执行流的恶意攻击手段

然后再别急，如果你很坚定的想要成为一个带嘿客，喜欢挖漏洞，喜欢破解软件想要写点诸如游戏外挂这一类的什么东西，或者想要做CTF队伍里面珍稀且很有排面的pwn爷爷，或者我们正经一点，坚定不移的走安全的这条路，那我更希望你可以耐心看下去，并且对它产生兴趣，来了解一下这个神奇的领域

## 0x01 前言

在讲pwn的各种东西之前，我想说一些自己学过来的一些废话：

我个人觉得，对于0基础pwn这个方向的入门门槛非常高，非常硬核，如果你看到这个文档的时候不知道什么是Linux，不知道什么是shell，再甚至如果你对c语言的掌握还没有那么好的话，很可能你要花出相比于其他方向更多的时间去入门（对，仅仅是入门）pwn:cry:

**听起来很劝退对吧，但是万事开头难，无论你决定学什么东西什么方向都一定要带着你的觉悟，如果遇到一个问题就想着放弃或者搁置的话在这里一定不会学到什么知识的**

在pwn的路上你可能会遇到各种与你之前的学习生活非常割裂的各种名词，或者都不用说在这条路上，接下来的指北里估计就有不少你看不懂的名词，**勤用搜索引擎**，多用搜索引擎然后狠狠地钻研就一定会得到你的答案

劝退过后我也说一些稍微有点安慰意义的话，大伙大可以把学pwn的过程当做是打怪升级的过程，当你把零零散散的一些东西学明白且做出了这个方向的一道题之后一定会感受到那种突然通畅了一样的快感，且时常会伴随着“这东西现在看上去这么简单为什么我当时学花了好多时间”的感觉，这都是学习的珍贵成果

同时也要记住多实践多动手，在硬核的领域里面实机操作一定是第一准则，比如一个漏洞的攻击方法和具体实现你去思考的话一定是不如去自己动手动态调试一遍的，拿我举个例子，直到今年3月份我的动态调试水平都是非常拉垮的，但是进入堆的领域之后感觉到上手动调非常重要于是现在逐渐掌握了基本的动调方法并且也确

实意识到了动调对于后续学习的重要性且开始应用于实战，所以很建议大伙从头开始就一直动手调试实践而不是一直啃书本看帖子思考

## 0x02 基础知识

为什么要说学pwn的门槛高呢，因为基础知识如下：

- 首先一定要学会c语言，书推荐《c primer plus》
- 汇编语言，我的方法是从王爽的汇编语言->《深入理解计算机系统》的第三章
- 搭建一个可以做pwn题的linux环境同时学一些基础的linux知识
    - 可以使用wsl/vmware
    - 系统建议选择Ubuntu，22.04即可
- 要学会用python和pwntools写一些简单的脚本，称之为exp
- 还会涉及到一些工具的使用诸如ida pwndbg 等等等等
- 同时很建议学会使用markdown编辑器，这种语言适合于记一些学习过程以及心得

实际上你在真正学习的时候，既不可能有一个确定的学习目标（或者说任务，再解释一下就是说不可能学到卡到某一个确定的位置），又需要逐渐的多方向扩展学习，(**其实好像对于每个方向都是如此，这可能也是CTF的魅力所在**），与此同时：

**千万不要真的去看完所有知识点再来做题，请注重实践和理论的分配**

pwn中最简单的题可能只需要上述知识中的一项，拿接下来的moe题目里面来说，很多题都是入门难度，不需要你真的看懂很多c/薄纱python/看懂很多汇编/完全熟悉linux

我们的基础题可能只需要：

- 熟悉几个简单的linux指令
- 会写一个python的简单的交互脚本
- 弄懂最简单的栈溢出原理

所以也不要被这么多的学习项目吓到或者劝退，moe的这些题会以一种梯度的形式来帮助你了解我上述的这些东西，**真的如同“打怪升级”，所以请保持你的激情和觉悟加油做下去**

在这里推荐一些资源：

- ctfwiki，一个很全面的教程资料网站，当你学会一些基础知识之后可以看看ctfwikipwn分区
- 好用的题库网站，供刷题巩固知识点：
    - buuctf，题量非常全
    - nssctf，里面有最近的各大比赛的原题，网站题库里附有一些师傅的wp（writeup即题解）方便随时参照解题
    - 攻防世界
    - pwnable.tw（似乎有点进阶）
    - 等等

## 0x03 How to

说完了“是什么”和“该做什么”，接下来先适应性的谈谈“怎么做”

**首先我重申一个核心观点就是，学什么方向什么东西都需要觉悟和坚持，学pwn也是如此，这一定是一个长期的过程，同时可能你也会被其中的一两个知识点卡住持续短则几天长则一月，还是上面的话，如果你轻言放**

**弃无论我告诉你怎么做都帮不到你**

而且可能也会和前面说的话会有一些重复，见谅，可能是我希望在这里更多解释一下前面的话，~~也可能是我这个大语言有点混乱~~

- :one:，这个领域主要的学习方式不同于你以前的“不会就去问别人/翻书”，你要去学习自己使用搜索引擎，搜索其他师傅的帖子等等来解决你的问题，这需要你使用一些合适的搜索引擎（必应/谷歌），同时掌握一定的搜索方法，搜不到先去改一改关键词，改一改引擎
- :two:，循序渐进，学一点东西就立刻动手实践，而不是攒一大堆知识之后才开始做题，这样通常会得到一个不怎么样的结果就是**你需要反复递归回来看以前的知识，同时你可能也会对它失去兴趣**，我个人还是觉得升一级就去打一级的怪对于这个领域而言更加合适也更加让自己有满足感，当然后续知识点复杂的话可能也会出现第二个知识点卡住导致你第一个知识点的掌握也变得不那么牢靠的情况
- :three:，广撒网，在技术方面的学习中途径非常多，书籍，大佬的blog以及各种有用的网站都是你的目标，多看多汇总对你的学习还是有很大帮助的，甚至你都可以去询问一下万能的AI..
- :four:，找一些好的题库网站且积极寻找适合你自己水平的比赛，以刷各种题来练习来提升自己的水平，在pwn中，即使是同一个知识点也能在不同的师傅手中发挥出不同的姿势，同时知识点的本质是不变的，所以刷题练习可以让你一边学到各种利用手段一边加深对某一点的理解
- :five:，如果遇到了自己很难解决的情况或者是找不到方向了这种自己难以解决的困难，向学长/资深师傅提问也是一个不错的方法，但是提问之前**建议先去看看《提问的智慧》，掌握友好且高效的提问方式**
    - pwn方向的几位管理都是非常友好的，遇到问题的话欢迎各位新生朋友来找我们提问

## 0x04 其他

到这里，大伙已经可以着手去准备自己的基础知识且开始跟随着我们在moe中设置的梯度开始做题享受CTF的美好了，如果读到这里的你对pwn还是持有一些好奇和激情，想要步入这条道路的话，我更想看到你带着这份激情与你的觉悟去向我们在moe中的题目不断坚持发起挑战:heart:

好像结尾写成了励志文章，感觉和这样子的硬核安全比赛的一篇入门文章不是很搭，但是如果我把一个指北单纯的写成一个描述任务或者描述方向的文章，那估计这种语气的指北萌新朋友看了就扔，效果会更差，也更劝退，单纯描述任务什么的可能只需要几句话，各种知识与步骤网上也有许多师傅写过了，我这种菜鸡不如说点自己的话循循善诱一下

虽然开头很不正经，但是结尾我希望用一种正经的方式结束，用《进击的巨人》中希斯特利亚摔针的一首《Zero Eclipse》中的一句歌词来说，歌挺好听的，大伙甚至可以试试：

**“Make a promise that I cannot regret”**

flag：moectf{M4ke_A_Promi5e_7hat_1_C4nn0t_Re9ret}

希望看到这里的新生萌新朋友们，不管是对这个方向有没有兴趣，想来学pwn或是想学别的方向或是别的东西，或者是什么大佬学长出于好奇想来看看这个指北里有什么东西，我希望都请“许下一个不会后悔的诺言”，找到自己的方向，玩得开心，学得开心，同时祝各位能够取得成功--

**最后，欢迎来到MoeCTF 2023，更欢迎大家来到pwn的领域。**

**By Pwn-luo。**