本文档由广东工业大学A&D攻防工作室的2017级pwn手根据自己的学习历程和心得所写，是一篇关于二进制安全/操作系统安全/CTF-pwn的入门指南。由于是面向小白、新手，因此着重介绍关于ctf中的pwn。授之以鱼不如授之以渔，本文档不涉及具体技术，而是告诉你pwn该如何去学，如何入门。虽然本人水平非常有限，但还时希望能对师弟师妹们了解、学习二进制安全起到指引的作用。

另外，我们工作室会在十月份/十一月份招新，欢迎对安全感兴趣的同学们来参与。如果对二进制安全感兴趣的话，根据本文档在暑假就可以开始学习。

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

什么是pwn

”Pwn”是一个黑客语法的俚语词 ，是指攻破设备或者系统 。发音类似“砰”，对黑客而言，这就是成功实施黑客攻击的声音——砰的一声，被“黑”的电脑或手机就被你操纵了。[来自百度百科]

CTF中的pwn

CTF中的pwn是一个关于二进制漏洞挖掘与利用的方向。通过对二进制程序进行逆向分析，挖掘程序中存在的漏洞并进行漏洞利用，最终获取目标主机的shell或读取flag。

学pwn以后能干啥?

PWN是CTF比赛中一个非常重要的方向。

通过CTF中的pwn，可以学习到很多关于操作系统方面的知识以及漏洞原理，为日后转向实战的二进制漏洞挖掘/利用/分析打下基础。

本方向的同学以后可以进入各大厂商的安全实验室，从事二进制漏洞挖掘/利用、病毒分析、系统安全研究等工作。

PWN入门指南

学习方法概述

我个人建议的学习方法是，首先要将下面列举的基本内容学习好，然后开始pwn的学习时，仍然会有很多不熟悉甚至没见过的东西，这是二进制安全学习路上的常态，无论是入门还是进阶，学习时都会遇到很多新的东西，一定要利用好搜索引擎，遇到不会的不要怕，百度google就完事了，要养成这种自主查找资料学习来解决技术盲区的习惯。

基础知识及对应书籍资料

在进行pwn学习之前，需要一些基础知识，下面列举了一下最基本的知识，按基础程度来顺序排列。并推荐了一些相关的书籍资料，这里提醒一下，并不是说要看完全书，而是要根据目录和自己需要的东西选择性的学习。后面学习pwn的时候，不同类型的漏洞需要不同的知识点，需要啥，就学啥。

- **C语言**（大家大一都学过C语言，对于指针、结构体等概念一定要熟悉）
- **汇编语言** - 《汇编语言 第三版》
- **函数调用惯例** - 《程序员的自我修养》《加密与解密》
- **程序的装载与链接**（静态链接、动态链接、动态链接库等概念）《程序员的自我修养》《深入理解计算机系统》
- **内存管理**（linux下为Glibc内存管理机制）《glibc内存管理ptmalloc源代码分析》（PDF文件，百度获取）
- **pwntools** 这是一个python第三方库，写解题脚本一般用它会非常方便。这个其实不需要专门学，看别人的代码，然后不懂的函数查询官方文档就行了，慢慢就会用了。官方文档：http://docs.pwntools.com/en/stable/intro.html#making-connections 还有一个非常好的pwntools新手教程：https://bbs.pediy.com/thread-247217.htm

逆向分析基础

逆向能力是二进制安全的基础，所以，在学习pwn之前，需要具备一定的逆向能力。推荐以下两本书籍入门：

- **《加密与解密》**
- **《逆向工程权威指南》**

一些必备的工具（这里只讨论linux下的pwn需要的两个最基本的）

- **gdb** gdb是linux平台下的调试器，因为现在的CTF-PWN一般都是在linux平台下的，所以一定要会使用它的一些基本操作，也推荐几个非常好用的gdb插件：**pwndbg**、**gef**、**peda**。 学习栈的利用的时候，用peda插件就可以很好的支持了，到学习堆的利用时，建议从gef和pwndbg中选一个使用。插件的使用上网搜也有很多入门资料的。

- **IDA Pro** 目前最广泛使用的反汇编、反编译软件，安全分析人士不可缺少的利器
- 工具下载：https://tools.pediy.com/ 看雪的工具库

PWN的学习资源

当掌握一定的以上基础知识后，就可以开始尝试pwn的学习了，下面推荐两个非常好的平台，可以说是一条龙学习路径都铺好了。

- https://ctf-wiki.github.io/ctf-wiki/pwn/readme-zh/

  首先是CTF Wiki，这是一个非常好的开源项目，基本上涵盖了pwn的基本面，跟着学就行，遇到没见过的概念就搜索引擎解决。

- https://github.com/firmianay/CTF-All-In-One

  最近发现的一个类似于CTF Wiki的项目，也是非常棒的学习资源。

- **建议的学习顺序：**栈溢出(Stack overflow) -> 格式化字符串漏洞(formart string) -> 释放后重用(UAF) -> 堆的利用(heap)

  上面的两个平台，这里讲到的几种类型都有涉及到，建议按照这个顺序学习，由浅入深。

PWN环境搭建

由于现在的ctf-pwn大部分是在linux平台下的，所以要安装linux虚拟机系统，这里推荐Ubuntu 16.04 ，虚拟机的操作百度google就行了，这里不赘述。装好之后再安装pwntools包和gdb插件，然后就可以了开始基本的学习了，学习过程中遇到需要什么工具再安装就行了。

- pwntools的安装： http://docs.pwntools.com/en/stable/install.html
- gdb插件的安装：https://blog.csdn.net/kevin66654/article/details/86773517

练习平台

下面是几个练习平台（其实在上面CTF Wiki里，每个知识点都会有例题，下面的平台是自己拓展练习必备的，网上都能搜到write up）

- https://adworld.xctf.org.cn/ [国内比较好的练习平台，XCTF联赛官方平台]
- https://pwnable.kr/play.php [非常基础，小白强烈推荐，由浅入深，可以通过它学习到很多非常基础的概念]
- https://pwnable.xyz/ [据说是面向新手]
- https://pwnable.tw/ [有一定难度]
- https://github.com/scwuaptx/HITCON-Training [Hitcon Training]

论坛平台

没事多逛论坛博客，经常能学到不少东西

- https://bbs.pediy.com/ 看雪论坛
- https://www.52pojie.cn/ 吾爱破解
- https://xz.aliyun.com/ 先知社区

- https://www.anquanke.com/ 安全客
- https://paper.seebug.org/ paper.seebug
- https://www.freebuf.com/ freebuf

个人的学习心得

我是在大二的时候开始学pwn的，实不相瞒，大一的时候就没学好C语言，因此基础非常的差，学习起来真的很困难，但是最后还是坚持下来了。这里想告诉大家的是，学习的时候处处碰壁，举步维艰是很正常的。当你遇到了我说的这种情况时，不要慌，这些困难总是要克服的，而且也不是啥大问题，看不懂、不会 又怎么样呢，百度google就完事了，利用好搜索引擎、养成自主查找资料解决问题的习惯，会让你的学习事半功倍。最重要的是，一定要有毅力有恒心，不要急躁。

这里借用《逆向工程权威指南 - 李承远》书中的一段话，将作者话中的“逆向分析技术”换成任何技术，这段话都是成立的，共勉。

> 逆向分析技术涵盖的内容很多，学习过程中有时会出现这样的想法：“我学习逆向分析技术都几天了，怎么到现在连这种问题都解决不了！”有些问题还解决不了是正常的。用吃的打个比方，逆向分析技术不是快餐（Fast food），而是有益于健康的慢餐（Slow food）。做起来要花费相当长的时间，需要足够的耐心。只要熬过了这段等待的时间，谁都可以成为优秀的逆向分析专家。