PWN入门指北

前言

PWN是一个非常硬核的方向，需要学的东西很多，也很难理解，但是这也是一个学习计算机底层实现的极佳途径，而且能很好地帮助你理解一些难懂的东西，比如C语言的指针。

PWN是什么

PWN指的是二进制漏洞挖掘和利用，很多时候与web类似，都是审计代码，找到漏洞，想办法进行攻击，从而控制系统或者拿到系统的权限。

PWN能做什么

PWN能做的东西很多，比如最近米哈游的反外挂服务存在漏洞，如果你的室友是一个OP，那么你就有办法控制他的电脑，往他们电脑中塞入一些奇奇怪怪的东西；又或是安卓手机获取root权限，以及苹果手机的越狱，很多时候都是PWN手负责的范围。

怎么学PWN

基础知识

二进制方向的基础知识基本一样，都是c语言和汇编语言，具体的学习推荐可以看逆向入门指北中的介绍

前置知识

1. 基本的程序逆向。毕竟我们叫做二进制漏洞挖掘和利用，和二进制文件打交道，程序逆向的技能是必不可少的（至少要会使用IDA Pro，教程可以参考逆向中的IDA Pro教程）。
2. 基本的Linux操作。毕竟Windows用户占有量巨大，相对来说攻击价值更高，但是相对应的Windows也有更加多样的内存保护措施，另外Windows闭源的特性也增加了代码审计的难度。相反，Linux的内存保护比较简单，同时很多组件开源，代码审计难度比较低，对于PWN学习来说门槛也相对更低。

PWN入门

以我自己的经验来看，PWN最开始的以实践入门会相对简单一点，在对做题有点感觉后，在去补足一些理论性的知识。
教程或是内容值得学习的网站：
ctf-wiki
20级PWN爷chuj的博客

刷题网站：
攻防世界 题目有难度划分，适合入门
buuoj 题目量比较大，一般是看到一道题后上buuoj找相关环境
pwnable.tw 题目质量比较高

`VIDAR{7his_is_4_new_st4rt}`