目录

一.基本知识储备

1. 了解什么是linux 操作系统，熟悉linux 操作系统的一些基本命令，如: ls nc rm cat 等
2. 掌握常用寄存器的及其作用，如：rax,rsp，rdi等，尤其是对于rip(PC)的理解
3. 掌握常用的汇编指令，如： mov,add,sub,xor,push,pop,call,ret,je,jmp等
4. 掌握linux的内存布局，尤其是栈的布局，并且结合汇编指令（pop,push,call,ret)等，熟悉栈的基本操作

二.熟悉常用工具

1. 掌握ida-pro的基本操作，如：f5反汇编，n 重命名，g 根据地址查询指令，x 交叉饮用，等等
2. 掌握gdb 的基本操作，如：b 打断点， c Continue, r run, x/gx 以8字节为一个单位查询内存，等
3. 掌握pwntools 的基本语法

一般这个模块不单独列出来讲，而是在讲题的过程中，用到哪个命令就顺带讲解

三.栈入门

1. 理解栈上返回地址的作用，并且知道什么情况下可以覆盖返回地址，学会如何覆盖返回地址为指定地址，完成例题ret to addr
2. 懂得编写自己的shellcode，知道如何使用shellcode 进行调用execve("/bin/sh",0,0), 使用shellcode 进行orw,使用shellcode 进行socket 连接等
3. 了解aslr 和 nx机制 ， plt 和got 表机制
4. 学习几个基础的rop 技巧：ret to gadget ,ret to libc, ret to csu
5. 了解canary , pie , RELRO 等更进一步的保护机制，学会绕过canary 和 pie 的基本技巧
6. 了解格式化字符串漏洞及其基本利用方式
7. 掌握更高级的rop技巧，ret to dlresolve

在此过程中，应该注意32位程序和64位程序的不同之处

四.堆入门

1. 了解堆的数据结构
2. 理解malloc 和 free 的基本过程
3. 熟悉fastbin attack
4. 熟悉off by one , off by null , unlink 等基本技巧
5. 熟悉house of XXX 系列

在学习堆的过程中，常利用iofile 结构体，所以需要对该结构体有一定了解，尤其是如何修改stdout ， 来泄漏libc