pwn学习资源

转载

SkYe231_ 于 2019-07-28 15:32:47 发布 230 收藏 5

分类专栏： PWN 文章标签： PWN PWN学习资料

pwn学习资源

> 原文链接：https://www.jianshu.com/p/a955ff04534e

学习思路：

- 学习各种套路
- 写有漏洞的程序 -> pwn

CTF练习网站：

- http://pwnable.kr
- https://pwnable.tw
- https://www.jarvisoj.com
- https://github.com/ctfs
- Wargames
- ROP Emporium
- exploit-exercises
- google搜索：xxx ctf 、xxx writeup

常用工具：

- gdb：Linux调试中必要用到的
- gdb-peda：gdb方便调试的工具，类似的工具有gef，gdbinit。peda安装
- pwntools：写exp和poc的利器，类似的有zio。pwntools安装
- checksec：可以很方便的知道elf程序的安全性和程序的运行平台，peda已集成
- objdump和readelf：可以很快的知道elf程序中的关键信息
- IDA pro ：强大的反编译工具
- ROPgadget：强大的rop利用工具
- one_gadget：可以快速的寻找libc中的调用exec('bin/sh')的位置
- libc-database： 可以通过泄露的libc的某个函数地址查出远程系统是用的哪个libc版本
- 参考链接

shellcode生成&搜索：

- pwntools
- msf
- shell-storm
- exploit-db

入门之前：

- 汇编语言：程序执行、函数栈帧、函数调用等
- 防护措施：CANARY, ASLR, NX
- 编译、链接、装载、执行
- x86&x64寄存器
- ELF文件结构
- Linux系统相关：文件描述符、系统调用、socket编程、shell命令

栈溢出入门：

- 手把手教你栈溢出从入门到放弃（上）
- 手把手教你栈溢出从入门到放弃（下）
- 一步一步ROP：x86
- 一步一步ROP：x64

博客：

- 蒸米(ROP经典)
- Swing
- muhe

文章：

- pico-ctf-2013
- rop和rop2的题目的wp
- 【技术分享】ROP技术入门教程
- 栈溢出学习入门总结
- 2017广东红帽杯pwn1_writeup：简单ROP
- Chybeta
- jarvisoj writeup