PWN入门

转载

weixin_30257433 于 2019-03-24 18:39:00 发布 712 收藏 1
文章标签： 操作系统 shell python
原文链接：http://www.cnblogs.com/null1/p/10589482.html

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。以上是从百度百科上面抄的简介，而我个人理解的话，应该就是向目标发送特定的数据，使得其执行本来不会执行的代码，前段时间爆发的永恒之蓝等病毒其实也算得上是pwn的一种。

pwn介绍

CTF pwn中的目标是拿到flag，一般是在linux平台下通过二进制/系统调用等方式编写漏洞利用脚本exp来获取对方服务器的shell，然后get到flag

前置技能

- 汇编语言，函数调用约定，大小端，函数栈帧
- python语言，gdb调试，IDA pro分析
- linux相关：32位与64位，各类防护机制（NX，ASLR，Canary，Relro），ELF文件格式，系统调用，shell命令
- 编译，链接，装载，执行

常见漏洞简介

- 缓冲区溢出(Buffer overflow)
- 栈溢出，堆溢出，bss溢出等
- 整数溢出(Integer overflow)
- 整数的加减乘法
- 有符号与无符号的转换
- 整数溢出一般可以转换成其它漏洞
- 格式化字符串(Format string)
- printf(s)，sprint f(s)，fprintf(s)可以修改地址也可以用来leak信息
- 使用后释放(Use-after-free)
- 释放掉的内存可能会被重新分配，释放后使用会导致重新分配的内存被旧的使用所改写
- Double free是一种特殊的UAF

工具

- IDA
- pro
- gdb
- pwntools
- zio
- peda
- readelf
- ropgadget
- string
- objdump

利用方法

- 注入代码
  - 溢出后在栈上执行代码
- 伪造函数
  - 修改.got.plt地址，替换掉正常函数
  - 布置gadget将ret地址指向libc中的其它函数

学习网站

如何开始你的CTF之旅

PWN总结

p4-team

uaf

ddaa

二进制漏洞学习

sploitfun

CTF Writeup Github(Note:百度搜不到github Pages的)

pwnable.kr

pwnable.tw

ROPemporium

学习资料

《有趣的二进制》
《深入理解计算机系统》
《程序员的自我修养》
《深入理解Linux内核》

转载于:https://www.cnblogs.com/nul1/p/10589482.html