CTF中pwn的入门指南

原创

影子019 于 2019-09-13 13:50:31 发布 23171 收藏 468

分类专栏： ctf_pwn 教程指南 文章标签： ctf pwn 入门

本文链接：https://blog.csdn.net/qinying001/article/details/100802002


ctf_pwn 同时被 2 个专栏收录

20 篇文章 10 订阅

订阅专栏


教程指南

2 篇文章 0 订阅

订阅专栏

CTF中pwn的入门指南

pwn简介：

CTF中的pwn指的是通过通过程序本身的漏洞，编写利用脚本破解程序拿到主机的权限，这就需要对程序进行分析，了解操作系统的特性和相关漏洞，是是一个难度比较大的分支。

接下来介绍相关的学习思路(自己总结的，当作参考)

0x01 基础知识准备

pwn相对于web，更需要专业的技能和知识，最主要的是要学会如何分析程序，这就需要有足够的准备

- c语言
- 汇编语言
- python
- 操作系统
- linux操作

C语言是最基础的，当下的比赛大部分的pwn题目使用的程序都是利用C语言或者C++完成的，IDA的反编译功能也是变成C/C++，理解并能运用C语言，对于分析程序有很大的帮助。

汇编语言，pwn是绕不过汇编的，分析程序首先面对的就是汇编，对于汇编需要有一定的基础，按照当下来说，使用的最多的是x86的汇编，然后就是IA32，掌握这两种汇编基本上就足够了。

python，用来exp，实际上exp每种语言都可以写，但是python集成了一个专门用于pwn的库–pwntools，更方便使用。

操作系统的知识也需要有一定的了解，特别是linux，栈和堆以及一些操作系统特性造成的漏洞都是我们解题的思路。

linux操作，基础的掌握就行。

0x02 主流工具的使用

分析pwn会用到许多的工具，掌握并使用这些工具也是十分重要的。

- IDA pro　静态分析神器，必备。
- ollydbg　动态分析使用，分析程序的流程。
- windbg　windows下的动态分析神器，可以调试内核态，谨慎使用。
- gdb　linux下的调试程序，同样作用很大。
- pwntools　python第三方库，用于开发exp。
- pwndbg　gdb调试的一个插件，可以显示一些调试信息很有用。

上面列举的工具对于pwn来说都有很大的作用，刚开始学习的建议从IDA和gdb开始。

0x03 经典漏洞学习

pwn的几大主流漏洞一定要掌握，深层掌握，后续的题目基本上是这些漏洞的深化和结合。

- 栈溢出
- 堆溢出
- ROP
- 格式化字符串漏洞
- 其余漏洞

前四种漏洞是大部分程序都存在，且很难避免的，是必须掌握的内容。

0x04 Shellcode编码

Shellcode是破解软件的一种方法，对于一些没有办法通过程序内部函数获取系统权限的软件，可以编写Shellcode来获取系统权限。

0x05 学习资料总结

书籍推荐：

- 汇编语言第三版
- 鸟哥的linux私房菜
- 深入理解计算机系统
- 黑客攻防技术宝典(系统实战篇)　一本老书，但是很经典。
- IDA pro权威指南　IDA学习的书籍
- 黑客反汇编解密　关于反汇编和分析软件的知识
- 加密与解密　windows平台的逆向分析

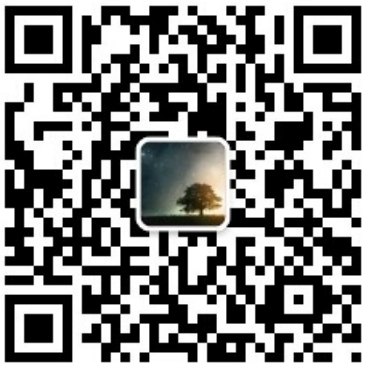
学习网站推荐：

- 看雪论坛 https://bbs.pediy.com
- 学破解论坛 https://www.xuepojie.com
- 吾爱破解 https://www.52pojie.cn
- i春秋 https://www.ichunqiu.com
- 实验吧 http://www.shiyanbar.com
- 漏洞银行 https://www.bugbank.cn/live

ctf刷题网站推荐

- 实验吧 http://www.shiyanbar.com
- i春秋 https://www.ichunqiu.com
- bugku https://ctf.bugku.com
- 攻防世界 https://adworld.xctf.org.cn
- pwnable http://www.pwnable.kr/

建议大家在开始的时候多刷题，多动手。



新建微信公众号，欢迎各位安全爱好者关注，一起学习。