CTF『Pwn』版块精选帖分类索引

https://bbs.pediy.com/thread-262816.htm

基础知识

- ubuntu安装各种pwn工具
- Docker搭建pwn环境
- CTF Pwn环境搭建
- 一步一步学pwntools
- 第一个mips pwn搭建环境，逆向，调试，最终exp的过程
- 深入窥探动态链接
- PLT&GOT 表以及延迟绑定机制
- 栈迁移原理（图示）
- rop链攻击原理与思路(x86/x64)

漏洞保护机制

- Linux 二进制程序保护机制详解
- printf函数leak与canary绕过原理及利用方式
- Safe-Linking机制分析及绕过

整数溢出

- 数组越界之入门向
- 由寄存器位数差异引发的漏洞利用
- 经典整数溢出漏洞示例 XCTF int_overflow

格式化字符串

- printf格式化漏洞魔术公式
- Pwn-WereWolf
- 通过堆上的格式化字符串利用剖析函数栈帧的建立与还原
- Pragyan CTF 最高分Unbreakable encryption--AES加密的WriteUp
- pwn-格式化字符串学习笔记

- 格式化字符串漏洞简介
- 格式化字符串漏洞解析
- 格式化字符串漏洞

栈溢出

- 栈溢出学习笔记
- TAMUCTF 2018 pwn writeup
- 小白学pwn——ret2libc
- ret2csu学习
- 通过一道pwn题详细分析retdlresolve技术
- 记一道简单难度ret2shellcode中遇到的坑
- SROP分析及例题

堆利用

- dlmalloc、ptmalloc与glibc堆漏洞利用
- ptmalloc代码研究
- heap related data structure && ptmalloc2
- how2heap调试学习（一）、（二）、（三）
- 堆入门攻略-how2heap学习总结
- 堆的六种利用手法
- Asis CTF 2016 b00ks
- 2015 plaidctf datastore(off by one)
- PWN入门（Off-By-One）
- glibc2.29下的off-by-null
- LCTF 2018 easy_heap
- Chunk Extend and Overlapping笔记
- unlink 系列
- ctf ptmalloc pwn unlink
- 堆利用之unlink小结
- PWN：unsafe unlink
- 协程切换的临界区块控制不当而引发的UAF血案
- 2014 hack.lu oreo
- 0ctf2017 - babyheap

- 关于fastbin合并问题的研究
- PWN：fastbin attack学习
- ctf pwn中的unsorted bin利用及chunk shrink——0ctf2018 heapstorm2 writeup
- Large bin attack--LCTF2017-2ez4u--writeup
- ctf中的large bins attack及lctf2017 2ez4u writeup
- 西湖论剑storm_note Large bin Attack
- largebin attack原理学习
- Tcache利用总结
- Tcache Attack原理学习
- 从BookWriter看house of orange原理
- 借助gdb调试glibc代码学习House of Orange
- 一道house of storm的heap题目
- [CTF堆利用]House Of Force
- House Of Force实例
- 堆利用-House Of Force
- Tinypad Seccon CTF 2016(House Of Einherjar)
- House Of Einherjar学习

IO_FILE 相关

- IO-FILE中的stdin介绍
- hctf2018 the end（IO FILE attack和exit hook attack）

浏览器相关

- 强网杯2020线下GooExec

虚拟化相关

- SECCON 2018 kindvm writeup
- 2019强网杯线下赛qemu虚拟机逃逸

Linux 内核

- KERNEL PWN状态切换原理及KPTI绕过
- linux kernel pwn 分析(一) 强网杯core + ciscn babydriver
- kernel pwn入门 强网杯 core

- Linux kernel pwn （一）：ROP&&ret2usr
- kernel pwn -- UAF
- InCTF-Internationals-2019-pwnbox分析
- Linux Kernel Pwn 学习笔记(栈溢出)
- Linux Kernel Pwn 学习笔记 (UAF)

Windows 相关

- windows10下的堆结构及unlink分析

实用技巧

- 关于不同版本glibc强行加载的方法
- 关于不同版本 glibc 更换的一些问题
- pwn中one gadget的使用技巧
- 如何在pwn题中更有效地使用GDB
- Linux内核驱动调试遇到的一些坑以及解决方法
- Libc-Database 本地搭建实战

专题系列

- Linux PWN从入门到熟练： part1、part2、part3
- 从0开始CTF-PWN： part1、part2、part3、part4
- pwnable.tw新手向write up： part1、part2、part3、part4、part5、part6、part7
- Pwn从入门到放弃： part1、part2、part3、part4、part5
- Pwn堆利用学习： part1、part2、part3、part4、part5

经验分享

- 写下你的 CTF Pwn 个人经验谈

赛制相关

- 强网杯出题思路-solid_core-HijackPrctl
- 强网杯线下赛堆分配检查机制(lowbits leak check)
- Pwn 的比赛环境配置
- 如何安全快速地部署多道ctf pwn比赛题目

题解集锦

- readme-revenge details
- readme_revenge - 34C3 2017 CTF
- pwnable.tw 之 unexploitable 解题思路分享
- pwnable.kr 之 ascii 解题思路分享
- 读取popen输出结果时未截断字符串导致的命令行注入
- HITCTF 2018 pwn writeup
- Teaser Dragon CTF 2018 pwn
- X-NUCA revenge骚思路getshell
- 2018-XNUCA steak 涨姿势
- WarGame-narnia 解题思路
- WarGame-behemoth 解题思路
- ROPEmporium全解
- ByteCTF Pwn部分题解
- Layer7 CTF Pwn题部分Writeup
- hctf 2018 部分pwn writeup
- 2018科来杯PWN复现
- 2018redhat_gameserver 记一次较为详细的解题过程
- seccomp沙箱机制 & 2019ByteCTF VIP
- 由一道ctf题目 对一个另类upx壳的一次探究
- 2020-HackTM 题目学习
- Hackergame 2020 pwn writeup
- 字节跳动ByteCTF2020 两道堆题（glibc2.31）

学习资源

- **资料搜索**：LibGen、Sci-Hub、Google Scholar
- **Wargames**：CTFtime、Awesome-Hacking-Resources、awesome-ctf
- **在线文档**：CTF Wiki、CTF-All-In-One
- **书籍**：《CTF特训营》、《从0到1：CTFer成长之路》、《CTF竞赛权威指南（Pwn篇）》