第 1 章 CTF 简介
1.1 赛事介绍
1.1.1 赛事起源
1.1.2 竞赛模式
1.1.3 竞赛内容
1.2 知名赛事及会议
1.2.1 网络安全竞赛
1.2.2 网络安全会议
1.2.3 网络安全学术会议
1.3 学习经验
1.3.1 二进制安全入门
1.3.2 CTF 经验
1.3.3 对安全从业者的建议
第 2 章 二进制文件
2.1 从源代码到可执行文件
2.1.1 编译原理
2.1.2 GCC 编译过程
2.1.3 预处理阶段
2.1.4 编译阶段
2.1.5 汇编阶段
2.1.6 链接阶段
2.1.7 LLVM 编译过程
2.2 ELF 文件格式
2.2.1 ELF 文件的类型
2.2.2 ELF 文件的结构
2.2.3 可执行文件的装载
2.3 静态链接
2.3.1 地址空间分配
2.3.2 静态链接的详细过程
2.3.3 静态链接库
2.4 动态链接
2.4.1 什么是动态链接
2.4.2 位置无关代码
2.4.3 延迟绑定
第 3 章 汇编基础
3.1 CPU 架构与指令集
3.1.1 指令集架构
3.1.2 CISC 与 RISC 对比
3.2 x86/x64 汇编基础
3.2.1 CPU 操作模式
3.2.2 语法风格
3.2.3 寄存器与数据类型
3.2.4 数据访问
3.2.5 算术和逻辑运算

3.2.6 跳转指令
3.2.7 栈与函数调用
第 4 章 Linux 安全机制
4.1 Linux 基础
4.1.1 常用命令
4.1.2 流、管道和重定向
4.1.3 根目录结构
4.1.4 用户组及文件权限
4.1.5 环境变量
4.1.6 procfs 文件系统
4.1.7 字节序
4.1.8 调用约定
4.1.9 核心转储
4.1.10 系统调用
4.2 Stack Canaries
4.2.1 简介
4.2.2 实现
4.2.3 NJCTF 2017 - messager
4.2.4 sixstars CTF 2018 - babystack
4.3 Non-eXecute
4.3.1 简介
4.3.2 实现
4.3.3 示例
4.4 ASLR 和 PIE
4.4.1 ASLR
4.4.2 PIE
4.4.3 实现
4.4.4 示例
4.5 FORTIFY_SOURCE
4.5.1 简介
4.5.3 实现
4.5.3 示例
4.5.4 安全性
4.6 RELRO
4.6.1 简介
4.6.2 示例
4.6.3 实现
第 5 章 分析环境搭建
5.1 虚拟机环境
5.1.1 虚拟化与虚拟机管理程序
5.1.2 安装虚拟机
5.1.3 编译 debug 版本的 glibc
5.2 Docker 环境
5.2.1 容器与 Docker

5.2.2 Docker 安装及使用
5.2.3 pwn 题目部署
第 6 章 分析工具
6.1 IDA Pro 6.1.1 简介
6.1.2 基本操作
6.1.3 远程调试
6.1.4 IDAPython
6.1.5 常用插件
6.2 Radare2
6.2.1 简介及安装
6.2.2 框架组成及交互方式
6.2.3 命令行工具
6.2.4 r2 命令
6.3 GDB
6.3.1 组成架构
6.3.2 工作原理
6.3.3 基本操作
6.3.4 增强工具
6.4 其他常用工具
6.4.1 base64
6.4.2 dd
6.4.3 file
6.4.4 ldd
6.4.5 md5sum
6.4.6 nm
6.4.7 objdump
6.4.8 readelf
6.4.9 socat
6.4.10 ssdeep
6.4.11 strace/ltrace
6.4.12 strip
6.4.13 strings
6.4.14 xxd
第 7 章 漏洞利用开发
7.1 shellcode 开发
7.1.1 基本原理
7.1.2 编写简单的 shellcode
7.1.3 shellcode 变形
7.2 pwntools
7.2.1 简介及安装
7.2.2 常用模块和函数
7.3 zio
7.3.1 简介及安装
7.3.2 使用方法

第 8 章 整数安全
8.1 计算机中的整数
8.2 整数安全
8.2.1 整数溢出
8.2.2 漏洞多发函数
8.2.3 整数溢出示例
第 9 章 格式化字符串
9.1 格式化输出函数
9.1.1 变参函数
9.1.2 格式字符串
9.2 格式化字符串漏洞
9.2.1 基本原理
9.2.2 漏洞利用
9.2.3 fmtstr 模块
9.2.4 HITCON CMT 2017 - pwn200
9.2.5 NJCTF 2017 - pingme
第 10 章 栈溢出与 ROP
10.1 栈溢出原理
10.1.1 函数调用栈
10.1.2 危险函数
10.1.3 ret2libc
10.2 返回导向编程（ROP）
10.2.1 ROP 简介
10.2.2 ROP 的变种
10.2.3 示例
10.3 Blind ROP
10.3.1 BROP 原理
10.3.2 HCTF 2016 - brop
10.4 SROP
10.4.1 SROP 原理
10.4.2 pwntools srop 模块
10.4.3 Backdoor CTF 2017 - Fun Signals
10.5 stack pivoting
10.5.1 stack pivoting 原理
10.5.2 GreHack CTF 2017 - beerfighter
10.6. ret2dl-resolve
10.6.1 ret2dl-resolve 原理
10.6.2 XDCTF 2015 - pwn200
第 11 章 堆利用
11.1 glibc 堆
11.1.1 内存管理
11.1.2 堆概述
11.1.3 重要概念与结构体
11.1.4 各类 bin 介绍

11.1.5 chunk 相关源码
11.1.6 bin 相关源码
11.1.7 malloc_consolidate()函数
11.1.8 malloc()相关源码
11.1.9 free()相关源码
11.2 tcache 机制
11.2.1 数据结构
11.2.2 使用方法
11.2.3 安全性分析
11.2.4 HITB CTF 2018 - gundam
11.2.5 BCTF 2018 - House of Atum
11.3 fastbin dup
11.3.1 fastbin dup
11.3.2 fastbin dup consolidate
11.3.3 0CTF 2017 - babyheap
11.4 house of spirit
11.4.1 house of spirit
11.4.2 LCTF 2016 - pwn200
11.5 unsafe unlink
11.5.1 unsafe unlink
11.5.2 HITCON CTF 2016 - Secret Holder
11.5.3 HITCON CTF 2016 - Sleepy Holder
11.6 off by one
11.6.1 off by one
11.6.2 poison null byte
11.6.3 ASIS CTF 2016 - b00ks
11.6.4 Plaid CTF 2015 - PlaidDB
11.7 house of einherjar
11.7.1 house of einherjar
11.7.2 SECCON CTF 2016 - tinypad
11.8 overlapping chunks
11.8.1 extend free chunks
11.8.2 extend allocated chunks
11.8.3 hack.lu CTF 2015 - bookstore
11.8.4 0CTF 2018 - babyheap
11.9 house of lore
11.9.1 house of lore
11.10 house of force
11.10.1 house of force
11.10.2 BCTF 2016 - bcloud
11.11 unsorted bin attack
11.11.1 unsorted bin into stack
11.11.2 unsorted bin attack
11.11.3 国赛分区赛 - oneTwothree

11.12 large bin attack
11.12.1 large bin attack
11.12.2 0CTF 2018 - heapstorm2
第 12 章 pwn 技巧
12.1 one-gadget
12.1.1 寻找 one-gadget
12.1.2 ASIS CTF Quals 2017 – Start hard
12.1.3 XNUCA 2018 - gets
12.2 通用 gadget 及 Return-to-csu
12.2.1 Linux 程序的启动过程
12.2.2 Return-to-csu
12.2.3 LCTF 2016 - pwn100
12.3 劫持 hook 函数
12.3.1 内存分配 hook
12.3.2 0CTF 2017 - babyheap
12.4 利用 DynELF 泄漏函数地址
12.4.1 DynELF 模块
12.4.2 DynELF 原理
12.4.3 XDCTF 2015 - pwn200
12.4.4 其他泄漏函数
12.5 SSP Leak
12.5.1 Stack Smashing Procetor（SSP）
12.5.2 __stack_chk_fail()
12.5.3 32C3 CTF 2015 - readme
12.5.4 34C3 CTF 2017 - readme_revenge
12.6 利用 environ 泄露栈地址
12.6.1 HITB CTF 2017 - Sentosa
12.6.2 SECCON CTF 2016 - jmper
12.7 利用_IO_FILE 结构
12.7.1 FILE 结构体
12.7.2 FSOP
12.7.3 FSOP（libc-2.24）
12.7.4 HITCON CTF 2016 - House of Orange
12.7.5 HCTF 2017 - babyprintf
12.8 利用 vsyscall
12.8.1 vsyscall 和 vDSO
12.8.2 HITB CTF 2017 - 1000levels