目录

第一篇　基础知识

第 1 章　CTF 简介
1.1　赛事介绍
1.2　竞赛模式
1.3　国内外知名赛事
1.4　入门方法
1.5　本章小结

第 2 章　二进制文件
2.1　从源代码到可执行文件
2.1.1　预编译
2.1.2　编译
2.1.3　汇编
2.1.4　链接
2.1.5　GNU 工具链
2.2　ELF 文件格式
2.2.1　ELF 文件的类型
2.2.2　从共享目标文件开始
2.2.3　ELF 文件结构
2.3　静态链接
2.4　动态链接
2.5　本章小结

第 3 章　汇编基础
3.1　CPU 架构与汇编
3.2　汇编开发环境搭建
3.3　x86/x64 汇编基础
3.3.1　寄存器
3.3.2　内存寻址
3.3.3　字节序
3.3.4　指令集
3.3.5　调用约定
3.4　ARM 汇编基础
3.5　MIPS 汇编基础
3.6　本章小结

第 4 章　Linux 安全机制概述
4.1　Linux 基础
4.1.1　常用命令
4.1.2　根目录结构
4.1.3　用户组及文件权限

4.1.4 环境变量
4.1.5 流、管道和重定向
4.1.6 procfs 文件系统
4.2 应用层安全机制
4.2.1 Canary
4.2.2 Fortify
4.2.3 NX
4.2.4 PIE
4.2.5 Relro
4.2.6 ASLR
4.3 内核安全机制
4.3.1 SELinux
4.3.2 KASLR
4.4 本章小结

第二篇 安全工具

第 5 章 分析环境搭建
5.1 虚拟机环境
5.2 Docker 环境
5.3 QEMU 环境
5.4 pwn 环境部署
5.5 本章小结

第 6 章 分析工具简介
6.1 静态分析与动态分析
6.2 IDA Pro
6.3 Radare2
6.4 GDB
6.5 其他常用工具
6.5.1 base64
6.5.2 dd
6.5.3 file
6.5.4 ldd
6.5.5 md5sum
6.5.6 nm
6.5.7 objcopy
6.5.8 objdump
6.5.9 readelf
6.5.10 socat
6.5.11 ssdeep
6.5.12 strace&ltrace
6.5.13 strip
6.5.14 strings

6.5.15 xxd
6.6 本章小结

第 7 章 漏洞利用开发
7.1 shellcode 开发
7.1.1 shellcode 的基本原理
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
7.2.3 开发利用脚本
7.3 zio
7.3.1 简介及安装
7.3.2 使用方法
7.4 本章小结

第三篇 CTF 专题

第 8 章 reverse
8.1 方法概述
8.2 常见加密算法及编码
8.2.1 单向散列函数
8.2.2 对称加密算法
8.2.3 非对称加密算法
8.2.4 常见编码
8.3 代码混淆
8.4 脱壳技术
8.5 反调试技术
8.6 虚拟机指令分析
8.7 C++逆向
8.8 非常规程序逆向
8.9 本章小结

第 9 章 pwn
9.1 方法概述
9.2 格式化字符串
9.3 整数溢出
9.4 栈溢出
9.5 返回导向编程（ROP）
9.6 堆利用
9.6.1 glibc 堆概述
9.6.2 glibc 堆数据结构
9.6.3 glibc 堆管理函数

9.6.4 glibc 堆利用方法
9.7 ARM pwn
9.8 MIPS pwn
9.9 内核利用
9.10 本章小结

第四篇 解题技巧

第 10 章 pwn 技巧
10.1 one-gadget
10.1.1 寻找 one-gadget
10.1.2 ASIS CTF Quals 2017 – Start hard
10.2 通用 gadget
10.3 劫持 hook 函数
10.4 利用 printf 触发 malloc 和 free
10.5 利用 DynELF 泄露函数地址
10.6 利用 environ 泄露栈地址
10.7 利用__stack_chk_fail
10.8 利用_IO_FILE 结构
10.9 利用 vsyscall 和 vDSO
10.10 攻击伪随机数生成器
10.11 本章小结

第 11 章 完善中的 glibc
11.1 关于 tcache 机制
11.1.1 tcache 机制介绍
11.1.2 tcache 安全性分析
11.2 jemalloc 内存分配器
11.3 本章小结

第 12 章 线下赛技巧
12.1 线下赛的基本模式
12.2 流量分析
12.3 二进制文件 patch
12.4 本章小结

第五篇 高级专题

第 13 章 软件漏洞分析概述
13.1 软件分析技术的定义
13.2 软件分析技术的分类
13.3 本章小结

第 14 章 模糊测试

14.1 基本概念
14.2 AFL fuzzer
14.3 在 CTF 中的运用
14.4 本章小结

第 15 章 二进制插桩
15.1 基本概念
15.2 Pin
15.3 在 CTF 中的运用
15.4 本章小结

第 16 章 可满足性模理论
16.1 基本概念
16.2 Z3
16.3 在 CTF 中的运用
16.4 本章小结

第 17 章 符号执行
17.1 基本概念
17.2 angr
17.2.1 安装
17.2.2 快速入门
17.2.3 二进制文件加载器
17.2.4 求解器引擎
17.2.5 程序状态
17.2.6 模拟管理器
17.2.7 VEX IR 翻译器
17.2.8 总结
17.3 一步一步实践 angr
17.4 在 CTF 中的运用
17.5 本章小结

第 18 章 CGC 初探
18.1 CGC 模式简介
18.2 自动化利用生成
18.3 Driller
18.4 本章小结

附录

参考资料