

## <<内核漏洞的利用与防范>>

### 图书基本信息

书名：<<内核漏洞的利用与防范>>

13位ISBN编号：9787111374299

10位ISBN编号：7111374290

出版时间：2012-3-15

出版时间：机械工业出版社华章公司

作者：Enrico Perla,Massimiliano Oldani

页数：364

译者：吴世忠,郁莲,郭涛,董国伟

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<内核漏洞的利用与防范>>

### 前言

译者序：随着信息技术的飞速发展，互联网日益成为人们生活中不可缺少的一部分，社交网络、微博、移动互联网、云计算、物联网等各种新技术、新应用层出不穷。

但不管是Facebook、twitter等新兴互联网公司的迅速崛起，还是Android日益成为智能手机市场的主流操作系统，信息安全一直都是永恒的话题。

“震网病毒”事件凸显网络武器的实战破坏能力，关键信息基础设施和政府网络保护已成为网络空间防御的新重点；“维基泄密”事件彰显网络空间攻防双方的不对称性，百密难免一疏成为保密防范永远的痛；这些信息安全事件存在一个共同点，那就是信息系统或软件存在的漏洞是问题的根源。

因而，漏洞分析日益成为信息安全领域理论研究和实践工作的焦点，越来越引起世界各国的关注与重视。

随着操作系统安全性逐步提高，安全防护软件日臻完善，攻击者利用用户态漏洞实施攻击变得越来越困难，因此，内核漏洞日益成为攻击的焦点。

内核漏洞的利用将给系统的安全带来巨大的威胁，甚至会彻底瓦解安全防护措施。

因此，内核漏洞的挖掘与利用已成为研究热点。

为推动国内的漏洞分析和风险评估工作，提高国家信息安全保障能力和防御水平，中国信息安全测评中心长期跟踪和关注相关领域的理论进展和技术进步，有针对性地精选一些优秀书籍译成中文，供国内参考借鉴。

本书内容涵盖了开发内核级漏洞利用手段所需的主要理论和方法，包括：内核和内核漏洞利用的基本概念、内核漏洞的分类方法及主要类别、成功利用内核漏洞所需经历的三个阶段等，并在研究UNIX家族、MacOSX和Windows等不同类型操作系统自身特性的基础上，深入探讨了针对它们的利用代码编写方法，并建立了一套面向操作系统内核漏洞利用开发的行之有效的的方法论，从攻防双方不同的视角，介绍了内核漏洞远程利用的方法以及防御措施。

书中大量的实际漏洞利用技术及案例，不但能够帮助读者更好地理解那些深奥的理论，还可以帮助安全研究人员更加深入地了解内核攻击的方式和方法，为防御系统级的攻击，降低安全隐患提供了重要的理论支撑和技术保障。

在本书翻译过程中，译者得到中国信息安全测评中心的张普含、王嘉捷、柳本金、王欣等同志，以及北京大学软件与微电子学院的何建杉、余天天、王斌、万成铨、沈阳、张开元、张任伟、李金诺、彭磊、汤云杰等师生的支持和帮助，在此深表感谢。

本书得到中国信息安全测评中心“漏洞分析与风险评估”专项工程的支持。

## <<内核漏洞的利用与防范>>

### 内容概要

本书系统地讲解内核级别漏洞利用所需的理论技术和方法，并将其应用于主流操作系统——UNIX家族、Mac OS X和Windows。

本书分4个部分：第一部分介绍漏洞利用的目标、内核以及理论基础；第二部分深入介绍了目前主流操作系统的细节，并针对不同错误类别分别编写了漏洞利用程序。

第三部分将关注点从本地场景转移到远程利用的情景；第四部分介绍未来内核的攻防模式。

本书不仅从软件安全研究人员的角度谈论如何发现软件漏洞，也从软件开发者的角度给出了防止软件出现漏洞的方法，以帮助软件编程人员开发出安全的软件系统。

本书内容详实，实例丰富，可操作性强，涉及主流操作系统内核漏洞利用的各个方面，适合软件开发人员、测试人员、安全工程师等阅读。

## <<内核漏洞的利用与防范>>

### 作者简介

Enrico Perla

目前是Oracle公司的内核开发人员。

他于2007年获得Torino大学学士学位，并于2008年获得Trinity

Dublin大学计算机科学硕士学位。

他的兴趣范围包括底层系统编程、底层系统攻击、漏洞利用和漏洞利用对策等。

Massimiliano Oldani

目前担任Emaze网络的安全顾问。

他主要的研究课题包括操作系统安全和内核漏洞。

### 技术编辑简介

Graham Speake

是Yokogawa电气公司首席系统架构师，该公司是一个工业自动化供应商。

他目前为内核开发人员，并为多个国家的客户提供安全咨询和解决方案。

他擅长工业自动化和过程控制安全、渗透测试、网络安全和网络设计。

Graham经常在安全会议上发表演讲，并经常给世界各地的客户进行安全培训。

Graham的背景包括：BP和ATOS/Origin的安全顾问，以及福特汽车公司的工程师。

Graham拥有位于威尔士的Swansea大学学士学位，并且是ISA的成员之一。

## <<内核漏洞的利用与防范>>

### 书籍目录

译者序

序言

前言

致谢

作者简介

第一部分 内核态

第1章 从用户态利用到内核态利用

引言

内核和内核漏洞利用的世界

漏洞利用的艺术

为什么用户态漏洞利用不再有效

内核态漏洞利用和用户态漏洞利用

一个漏洞利用者的内核观

用户态进程和调度

虚拟内存

开源操作系统和闭源操作系统

小结

相关阅读

尾注

第2章 内核漏洞分类

引言

未初始化的/未验证的/已损坏的指针解引用

内存破坏漏洞

内核栈漏洞

内核堆漏洞

整数误用

算术/整数溢出

符号转换错误

竞态条件

逻辑

引用计数器溢出

物理设备输入验证

内核生成的用户态漏洞

小结

尾注

第3章 成功内核利用进阶

引言

架构级概览

基本概念

x86和x86-64

执行阶段

放置shellcode

伪造shellcode

触发阶段

内存破坏

## <<内核漏洞的利用与防范>>

竞态条件

信息收集阶段

环境告诉我们什么

环境不想告诉我们的：信息泄露

小结

相关阅读

### 第二部分 UNIX家族、Mac OS X和Windows

#### 第4章 UNIX家族

引言

UNIX家族成员

Linux

Solaris/OpenSolaris

BSD衍生操作系统

执行步骤

滥用Linux的权限模型

实战UNIX1

内核堆利用

利用OpenSolaris的slab分配器

利用Linux 2.6 SLAB<sup>H</sup>HUB 分配器

Linux的栈溢出利用

重拾 CVE-2009-3234

小结

尾注

#### 第5章 Mac OS

引言

XNU概述

Mach

BSD

IOKit

系统调用表

内核调试

内核扩展 (kext)

IOKit

内核扩展审计

执行步骤

利用注释

随意的内存重写

基于栈的缓冲区溢出

内存分配符利用

竞态条件

Snow Leopard利用

小结

尾注

#### 第6章 Windows

引言

Windows内核概述

内核信息收集

## <<内核漏洞的利用与防范>>

- DVWD介绍
- 内核内部组织攻略
- 内核调试
- 执行阶段
- Windows验证模型
- 编写shellcode
- Windows 漏洞利用实践
- 重写任意内存
- 栈缓冲区溢出
- 小结
- 尾注

### 第三部分 远程内核漏洞利用

#### 第7章 远程内核漏洞利用面临的挑战

- 引言
- 利用远程漏洞
- 缺少公开信息
- 缺少对远程目标的控制
- 执行第一条指令
- 直接执行流程重定向
- 内核内存的任意写
- 远程payload
- payload迁移
- KEP上下文
- 多级shellcode
- 小结
- 尾注

#### 第8章 一个Linux案例

- 引言
- SCTP的转发块堆内存损坏
- SCTP简要概述
- 漏洞路径
- 远程漏洞利用：总体分析
- 获得任意内存重写原语
- 远程调整堆布局
- 创建SCTP消息：从相对到绝对内存的重写
- 安装shellcode
- 从中断上下文直接跳到用户态
- 执行shellcode
- 检查当前进程，模拟gettimeofday()函数
- 执行反向连接
- 恢复Vsyscall
- 小结
- 相关阅读
- 尾注

### 第四部分 展望

#### 第9章 内核演变：未来内核攻防模式

- 引言

## <<内核漏洞的利用与防范>>

内核攻击

保密性

完整性

可用性

内核防御

内核威胁的分析与建模

内核防御机制

内核保证机制

超越内核bug：虚拟化

虚拟层安全

客户机内核安全

小结



## <<内核漏洞的利用与防范>>

### 章节摘录

版权页：插图：

## <<内核漏洞的利用与防范>>

### 媒体关注与评论

“这是一本非常有趣的书，它不仅仅教授读者内核漏洞利用的技术，而且激发了读者对操作系统内部结构的学习兴趣，这样的学习兴趣远远超出了简单的好奇心。

” ——Golden G. Richard III博士，新奥尔良大学计算机系教授，数字取证咨询公司CTO

## <<内核漏洞的利用与防范>>

### 编辑推荐

《内核漏洞的利用与防范》编辑推荐:全面剖析内核漏洞利用的概念、方法和步骤,深入探讨UNIX、Mac OS X和Windows等操作系统内核的利用代码编写方法,并详细阐述了内核漏洞的防御方法及措施。

《内核漏洞的利用与防范》主要内容: 涵盖主流操作系统——LINUX家族、Mac OS x 和Windows。

详解常见方案,如一般内存损坏(栈溢出、堆溢出等)问题、逻辑错误和竞态条件等。

从用户态漏洞利用引领到内核态漏洞利用的世界中。

专注于漏洞利用实施步骤。

可操作性强。

目前针对用户态漏洞利用的安全对策数量在不断增加,因此,内核漏洞利用在攻击者中变得越来越流行。

与操作系统内核共舞可能是一个危险的游戏:《内核漏洞的利用与防范》涵盖了开发可靠并且有效的内核级别漏洞利用所需要的理论技术和方法。

并将它们运用于主流操作系统中。

利用内核漏洞既需要艺术也需要科学。

每个操作系统都有其特点,所以,充分实现目标需要对每个漏洞进行建模。

《内核漏洞的利用与防范》讨论了最流行的操作系统,并讲解了如何完全控制它们。

## <<内核漏洞的利用与防范>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>