



中國人民大學

RENMIN UNIVERSITY OF CHINA

信息学院

SCHOOL OF INFORMATION

操作系统内核 分析与实践

0. 课程概览

授课教师：游伟 副教授

授课时间：周五16:00 – 17:30（公教三楼3505）

上机时间：周五18:00 – 19:30（理工配楼208B机房）

课程主页：<https://www.youwei.site/course/kernel>

教学团队

- 教师：游伟 副教授

- Email: youwei@ruc.edu.cn

- Office: 理工配楼104A

- 助教：谢冬晨（2023级硕士研究生）

- Email: dongchenx@ruc.edu.cn

- Office: 理工配楼301B

课程目标

- 分析：对Linux内核有一个整体的把握，理解Linux的设计思路，掌握源代码中的关键数据结构和核心算法
- 安全：对Linux内核安全机制的设计与实现有基本的认知，对内核漏洞的挖掘、利用、修复与防御有基本的了解
- 实践：亲自动手玩转Linux内核，能够修改/新增内核功能，能够分析/检测内核安全问题

课程特色

■ 与操作系统入门课程的区别

- 简要回顾操作系统的基本概念
- 以Linux内核为例，深入探究操作系统概念的实现

■ 与Unix环境高级编程的区别

- 不关注用户态程序如何使用内核对外提供的API
- 关注内核如何安全地实现系统资源的管理

■ 理论和实践相结合

- 课程讲解+实验展示
- 请同学们上课时带上笔记本电脑

课程内容

模块	周次	章节
内核分析	1	第1章. Linux内核概述
	2	第2章. Linux源码导读
	3	第3章. 进程管理与调度
	4	第4章. 内存管理与进程地址空间
	5	第5章. 中断与系统调用
	6	第6章. 文件系统与磁盘管理
	7	第7章. 进程间通信
	8	第8章. 内核并发与同步
个人汇报	9	第9章. 实践一：内核Rootkit的实现与检测
内核安全	10	第10章. 内核安全机制概述
	11	第11章. 内核安全漏洞
	12	第12章. 内核漏洞的挖掘与触发
	13	
	14	第13章. 内核漏洞的利用
	15	
小组汇报	16	第14章. 实践二：内核漏洞的挖掘、触发与利用

章节	实验	大作业
一、Linux 内核概述	DebugKernel	-
二、进程管理与调度	ProcessShow / ScheduleObserver	HideProcess
三、系统调用	打印列表 / AddSyscall	劫持系统调用
四、存储管理	MemoryStatus / 修改 VMA 属性	HideVMA
五、文件系统	查看 fs 状态 / 修改 proc 节点内容	RedirectFile
六、进程间通信	BinderIPC / 修改 IPC 消息	SignalBlocker
七、内核同步	RaceCondition / VisitShared	-
八、中断机制	查看中断向量 / IRQ 使用情况	IDTHook

课程考核

- 平时成绩：70%
 - 课程作业（40%）
 - 大作业（40%）
 - 课堂表现（20%）
- 期末考试：30%
 - 笔试
- 大作业：30%
 - 任务1：内核Rootkit的实现与检测（个人）
 - 任务2：内核漏洞的挖掘、触发与利用（小组）

任务1概览

课程学习方法

- 理解内核设计思想
- 掌握关键数据结构和核心算法
- 动手实践

课程资源

- 网站: <https://www.youwei.site/course/kernel>

- 虚拟机:

<https://pan.ruc.edu.cn/link/AA1903991E4FC64A9688453C30F95B0E4C>

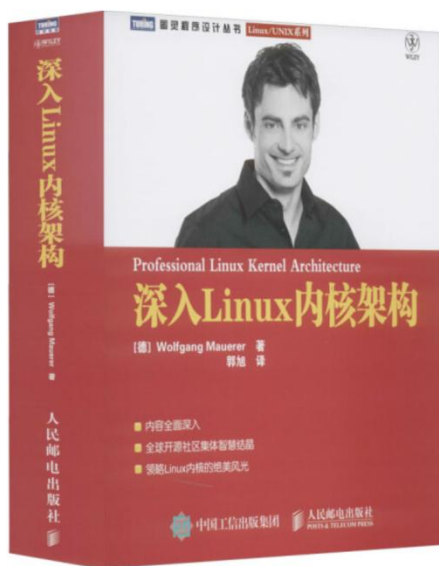
(提取码是1234, 用户名user, 密码abcd1234)

- 内核环境仓库: https://github.com/CheUhxg/RUC-OS_Kernel_Experiment-2025

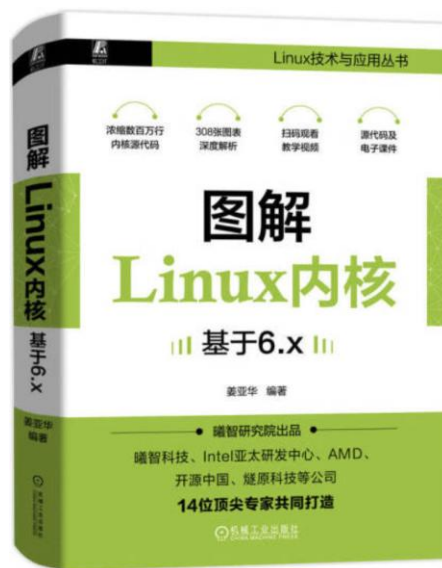
推荐图书



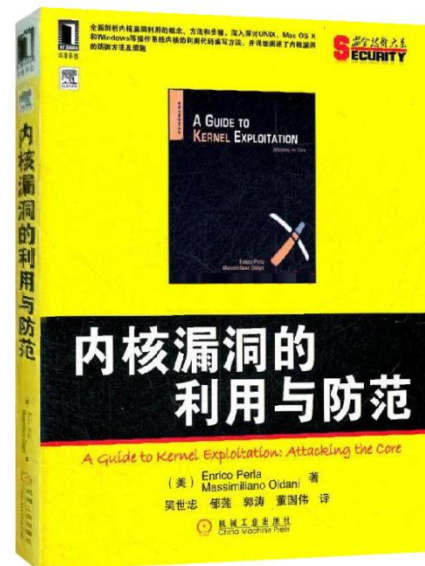
《Linux内核设计与实现》
机械工业出版社



《深入Linux内核架构》
人民邮电出版社



《图解Linux内核》
机械工业出版社



《内核漏洞的利用与防范》
人民邮电出版社