



中國人民大學

RENMIN UNIVERSITY OF CHINA

信息学院

SCHOOL OF INFORMATION

# 操作系统内核 分析与安全

## 0. 课程概览

授课教师：游伟 副教授

授课时间：周五14:00 – 16:30（立德楼807）

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](mailto:youwei@ruc.edu.cn)

- Office: 理工配楼104A

- 助教：袁江风（2020级硕士研究生）

- Email: [202225feng@ruc.edu.cn](mailto:202225feng@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

- 每堂课前2/3课时课程讲解，后1/3课时实验展示
- 请同学们上课时带上笔记本电脑

# 课程内容

模块	周次	时间	章节
基础知识	1	2/23	第1章. 操作系统与Linux内核概述
	2	3/1	第2章. Linux内核源代码导读
内核分析	3	3/8	第3章. 进程管理与调度
	4	3/15	
	5	3/22	第4章. 内存管理与进程地址空间
	6	3/29	
	7	4/5	第5章. 内核并发与同步
	8	4/12	第6章. 文件系统与磁盘管理
	9	4/19	第7章. 进程间通信
	10	4/26	第8章. 中断与系统调用
	12	5/10	第9章. 实践一：内核Rootkit的实现与检测
内核安全	13	5/17	第10章. 内核安全机制概述
	14	5/24	第11章. 内核安全漏洞
	15	5/31	第12章. 实践二：内核漏洞的挖掘与利用
课堂报告	16	6/7	课堂报告1
	17	6/15	课堂报告2

# 课程考核

- 平时课堂：30%
  - 考勤互动
  - 实验报告
- 实践任务：30%（三选一）
  - 任务1：内核Rootkit的实现与检测
  - 任务2：内核漏洞的挖掘与利用
  - 任务3：内核安全机制实现的探索
- 课程报告：40%
  - 报告一篇顶会论文
  - 将报告整理成文字材料

# 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

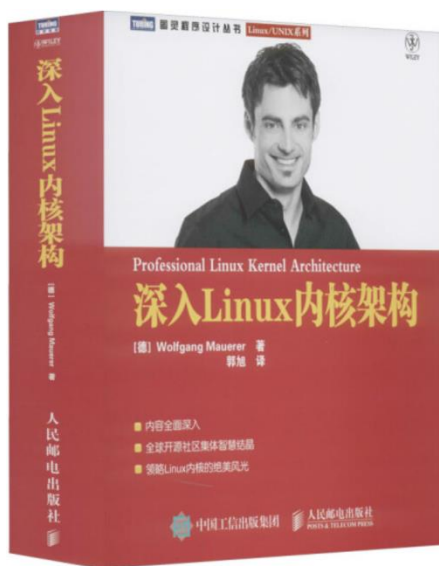
- 网站: <https://www.youwei.site/course/kernel>
- 虚拟机: <https://pan.baidu.com/s/1kO3VDHuol118-Nbo-Kb5DA?pwd=mgp3> (用户名user, 密码abcd1234)



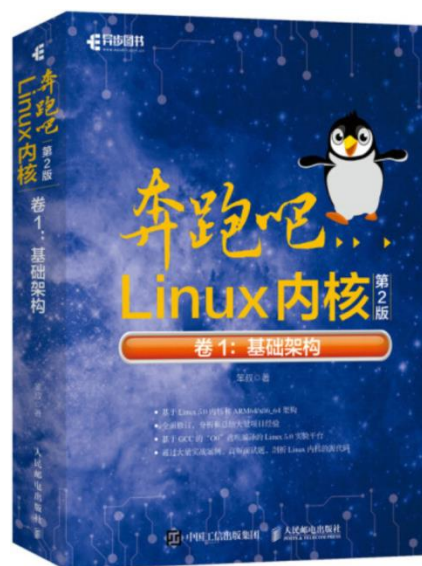
# 推荐图书



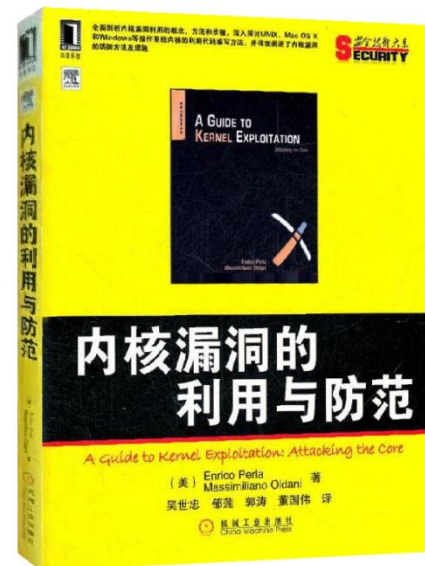
《Linux内核设计与实现》  
机械工业出版社



《深入Linux内核架构》  
人民邮电出版社



《奔跑吧Linux内核》  
人民邮电出版社



《内核漏洞的利用与防范》  
人民邮电出版社