空天信息安全与可信计算
教育部重点实验室

# Linux分析与安全设计

# 教学内容

- Linux操作系统及内核架构
  - 内核架构、内核源代码组成、内核基本数据结构
- Linux内存管理
  - 物理内存管理、虚拟内存管理、交换机制、Cache
- Linux进程管理
  - 进程控制块、进程创建流程分析、进程调度算法（CFS）
- Linux I/O和驱动安全
  - 驱动模型和开发、键盘过滤、内核模块调试方法

# 教学内容

- Linux内核漏洞分类及实例（包括了内存攻防）
  - 缓冲区溢出及防御（Stack Protection、DEP、ALSR等）、整数溢出、空指针、竞态条件、内核Hook
- LSM及Selinux机制
  - LSM Hook架构、Selinux模块
- NameSpace及Cgroup机制(进程沙箱机制）
  - NameSpace和Cgroup进程资源隔离机制
- Linux安全进展
  - 顶会论文分析

# 教学目标

- ✓熟悉Linux内核基本架构
- ✓熟悉Linux内存管理及保护机制
- ✓熟悉Linux进程管理机制
- ✓熟悉NameSpace及Cgroup机制
- ✓熟悉Linux I/O及驱动安全
- ✓熟悉内核漏洞类型及利用方法
- ✓熟悉LSM及Selinux强制访问控制实现原理
- ✓熟练掌握Linux内核调试方法

# 实验

以下5各实验中选做4项

1、Linux内核架构基本数据结构源代码分析

2、Linux驱动编程及Hook（两个实验：字符设备和键盘过滤）

3、Linux内核缓冲区溢出攻击及防御

4、Linux内核系统调用Hook

5、LSM及SeLinux源代码分析（结业报告）

# 课堂展示

- 要求：每组不超过3人
- 展示内容可以是以下其中一项

（1）LINUX操作系统某个漏洞，最好能够展示如何利用该漏洞攻击操作系统并可能的提出防御方法。

（注：以操作系统漏洞为主，最好不是展示网络漏洞、Web漏洞）

（2）分析Linux内核源代码,如ALSR等

（3）课堂展示内容也可以是实验内容，如果是展示实验作业，则为一人单独展示，并且同一选题，不超过2个人讲解。

- 时间：10-15分钟（第3周开始，每次课的最后一节课）
- 方法：PPT原理讲解+实际演示

（注：防御方法可以不实现）

# 成绩计算

- 成绩

  考勤 10%

  实验 40%

  结业报告 30%（Selinux源代码分析）

  课堂展示 20%

# 后续学习

- 源代码阅读与分析
- 修改内核代码
- 从安全功能入手，去分析相关源代码
- 鸿蒙OS、安卓、IOS、FreeRT OS
- 关注Linux内核安全漏洞，研究检测防御方法
- Linux内核之旅公众号（http://www.kerneltravel.net/）