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

主讲教师

- 教师
  - 姓名：王鹃　教授、博士生导师
    -研究方向：系统和网络安全
  - 电话：18986213038
  - Email：jwang@whu.edu.cn

- 群号：487383343
- 密码：linux

教学内容

- Linux操作系统及内核架构
- Linux内存管理和内存攻防
- Linux进程管理和沙箱机制
- Linux I/O和驱动安全
- Linux内核漏洞分类及实例
- LSM及Selinux机制
- NameSpace及Cgroup机制
- Linux安全进展

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

参考教材

-推荐教材：

- **Linux内核设计与实现**(原书第3版)， (美)Robert Love， 陈莉君等译，机械工业出版社，2011
- **Linux内核安全模块深入剖析**，李志，机械工业出版社，2016

-参考书目：

- 操作系统设计与实现第三版，陈渝等译，电子工业出版社
- 主流操作系统安全实验教程，王鹃主编，武汉大学出版社，2016
- 奔跑吧Linux内核，张天飞，人民邮电出版社，2018
- Linux源代码详解，赵炯，机械工业出版社
- 鸟哥Linux私房菜 （基础篇和服务器架设篇）
- Unix环境编程， W.Richard Stevens，第3版，人民邮电出版社，2014
- 汇编语言入门第二版, 王爽, 清华大学出版社

网络资源

- **内核源码站：http://www.kernel.org/**
- Linux内核之旅http://wwww.kerneltravel.net/
- Linux中国开源社区 https://linux.cn/tech/
- Linux伊甸园 http://www.linuxeden.com/
- 开源操作系统 Minix http://www.minix3.org/
- LINUX内核之旅公众号（微信号：LinuxKernelTravel）
- Syracuse大学Prof Du创建的安全实验室 http://www.cis.syr.edu/~wedu/seed/index.html
- http://www.exploit-db.com/ 上面有不少exploit的源码

成绩计算

- 成绩

  作业 20%

  考勤 10%

  实验 40%

  课堂展示 30%

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内核缓冲区溢出攻击及防御

3、Linux内核系统调用Hook

4、Linux驱动编程及Hook

5、LSM及SeLinux源代码分析

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）