河南中医药大学课堂教学设计

授课章节	项目十二：openEuler 的安全加固		授课学时	2 学时
所属课程	Linux 操作系统 国产操作系统	授课年级	2022 级	
设计者	互联网技术教学团队	授课专业	计算机类、信息管理与信息系统、智能医学工程专业	

1.教学目标：含知识、技能（能力）、学习态度与价值观（情感）目标

知识目标：

1. 了解 openEuler 的安全机制；
2. 掌握操作系统安全加固的基本操作；
3. 掌握使用 SELinux 提升内核安全性；
4. 掌握使用防火墙提升主机安全性；
5. 掌握使用 Nmap 进行主机安全检测。

能力目标：

1. 逻辑推导能力；
2. 语言表达能力；
3. 复杂问题简化分析能力。

素质目标：

1. 提升学生分析和评估安全风险的能力；
2. 激发学生系统安全的学习兴趣；
3. 强调团队合作、互相学习和分享的精神；
4. 培养严谨的实践态度和问题解决能力。

思政目标：

1. 强调信息安全的法律法规和职业道德，维护信息安全，增强责任感和使命感；
2. 信息安全就是国家安全，激发学生的爱国精神；
3. 鼓励学生批判性地思考和分析 Linux 系统安全问题。

2.教学内容：依据教学大纲；含教学重点难点

教学重点：

1. 如何使用防火墙；
2. 了解 SELinux。

教学难点：

1. 使用防火墙提升安全性；
2. 实现系统内核安全加固；
3. 操作系统的安全评估。

课堂教学内容：

1、操作系统安全加固（20 分钟）

（1）安全风险（10 分钟）

1）硬件设备的安全风险。外部硬件设备的运行情况是否正常，硬件设备所处的环境是否长期正常稳定，在使用过程中应防止因异常关机或设备零件故障造成操作系统的无法正常使用。

2）交互过程的安全风险。系统使用过程中，存在用户权限混乱、服务进程异常等安全风险。

3）网络病毒漏洞的安全风险。当操作系统在网络中提供服务时，将会面临着服务攻击、口令破解攻击、欺骗用户攻击、网络监听攻击、端口扫描攻击等网络安全风险。

（2）openEuler 的安全机制（10 分钟）

1）PAM 机制。PAM（Pluggable Authentication Modules）机制是一套共享库，其目的是提供一个框架和一套编程接口，将认证工作由程序员交给管理员。PAM 允许管理员在多种认证方法之间进行选择，它能够在不重新编译与认证相关应用程序的情况下改变本地认证方法。

2）安全审计机制。虽然 openEuler 不能预测何时服务器会遭受攻击，但是可以记录入侵者的行踪，记录事件信息和网络连接情况，信息保存到日志文件中，为后续复查提供支持。

3）强制访问控制机制。强制访问控制（Mandatory Access Control，MAC）是一种由系统管理员从全系统的角度定义和实施的访问控制机制，它通过标记系统中的主客体，强制性地限制信息的共享和流动，使用户只能访问与其相关的、指定范围的信息，防止信息泄密，杜绝访问权限的交叉混乱。

4）防火墙机制。

2、SELinux（10 分钟）

（1）什么是 SELinux（5 分钟）

SELinux（Security-Enhanced Linux）是强制访问控制机制在 Linux 内核上的实现，旨在提升 Linux Kernel 安全性。Linux Kernel 2.6 及以上版本均集成 SELinux 模块。

（2）SELinux 能够干什么。（5 分钟）

1）操作系统检查用户权限是否允许访问（DAC 控制权限）。

2）如果允许，继续检测 SELinux 强制访问控制策略是否允许（MAC 访问控制）。

3）如果允许，用户进程可访问系统内的对象。

3、SELinux 的工作模式与类型（20 分钟）

（1）强制模式：该模式是默认和推荐的操作模式，在强制模式下，SELinux 正常运行，在整个系统上强制加载安全策略。

（2）许可模式：又叫宽容模式，该模式启用 SELinux，但不阻止任何操作，只提出警告信息和进行记录。该模式下策略规则不被强制执行，只接收审核拒绝信息，不做任何安全策略加固。

（3）停用模式：该模式下，SELinux 是完全关闭的。关闭 SELinux 后，系统不再强制执行 SELinux 策略，还会停止标记任何对象，如果业务系统为正式服务的系统，在关闭 SELinux 的情况下运行一段时间后，由于大量的文件没有进行标记，未来启用 SELinux 是非常困难的强烈建议不要关闭 SELinux，如不需要使用 SELinux，可将工作模式调整为许可模式。

3、防火墙（20 分钟）

（1）什么是防火墙（5 分钟）

课堂教学内容：

防火墙是服务器安全的重要保障系统，遵循允许或拒绝业务来往的网络通信机制，提供网络通信过滤服务。从保护对象上区分，防火墙可分为主机防火墙和网络防火墙。

（2）主机防火墙（5 分钟）

主机防火墙是安装在一台计算机操作系统上的软件，属于典型的包过滤防火墙。将网络层作为数据监控对象，对每个数据包的头部、协议、地址端口及类型信息进行规则分析与数据包的处理（如进入、丢弃或拒绝等），从而实现针对单个主机进行防护。

（3）网络防火墙（5 分钟）

网络防火墙是部署在两个网络之间的设备或一整套装置，针对一个网络进行防护。通常部署在网络边界以加强访问控制，其将网络划分为可信与不可信区域，对流入流出的网络流量进行过滤，实现对网络的防护。

（4）防火墙的局限性（5 分钟）

防火墙是重要的系统安全防护措施之一，但也不能过分依赖防火墙，因为防火墙自身具有一定的局限性。

4、安全审计（10 分钟）

为什么要安全审计。没有绝对的安全，即便 SELinux 和防火墙同时使用，也无法绝对保障操作系统无任何安全风险。只有持续性、周期性对操作系统进行安全评估，及时发现安全漏洞并进行修复，才能持续提高主机的安全性。

3.思政知识点：

课程思政案例	思政点映射
上海某政府信息系统技术承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据泄露，以致成为境外不法分子窃取政务数据的“供应链”入口。 上海市网信办协调有关部门已要求该公司立即下线政府网站页面、关闭相关云服务端口、配合开展网络资产清查，并对该公司作出行政处罚。	网络信息安全、爱国意识教育。

4.学情分析及教学预测：

学生的知识基础：

1. 防火墙的工作原理；
2. Linux 操作系统。

学生的认知特点：

1. 学生认识防火墙但应用不充分；
2. 学生对系统安全的认识不足。

学生的学习风格：

1. 通过课堂上知识点的讲解，学生更倾向于深入理解安全加固的理论基础和原理；
2. 为了深化理解，学生通过实际操作在真实的 Linux 环境中进行安全加固来学习。

教学预测：

1. 通过案例式教学和探究式教学等方法，培养学生的创新意识和思维能力；
2. 学生的学习兴趣和动机提升：通过引导学生进行实际的操作和互动交流；
3. 学生的合作与沟通能力培养：在课程中鼓励学生进行小组合作，分享经验和解决问题。

5.教学策略与方法：

教学策略：

1. 通过多媒体演示文稿进行讲解，并结合板书进行关键难点的介绍和原理过程的讲解；
2. 课后留练习题目或作业，引导学生对课程内容进一步巩固和复习。

教学方法：

1. 通过课前预习，让学生对相关基础知识及概念有基本的了解；
2. 理论课通过讲解、与学生互动了解学生知识掌握情况，对学生较为薄弱的环节进一步强化介绍。

6.板书设计：

① **黑板（白板）设计：**	② **现代信息媒体设计：**
防火墙 SELinux	使用多媒体教学课件开展。 基于虚拟化平台开展教学演示。

7.教学互动环节设计：

课堂上的提问和互动交流：

1. 问题一：可以通过哪些方式提升系统安全性?
2. 问题二：防火墙与 SELiux 在提升系统安全性方面有什么不同?
3. 问题三：使用防火墙和 SELinux 操作系统就没有安全风险了吗?

8.学习资源，课外自主学习设计：

自建学习资源：

1. 课程学习平台：https://internet.hactcm.edu.cn/linux
2. 课堂派：https://www.ketangpai.com

网络学习资源：

1. OpenEuler 官网：https://www.openeuler.org/zh/
2. OpenEuler 镜像仓库列表：https://www.openeuler.org/zh/mirror/list/

官方文档：

1. OpenEuler 官方文档：https://docs.openeuler.org/zh/

9.教学测量与评价：

课堂教学测量评价：

1. 课堂测试：使用课堂派开展阶段性测试。
2. 课堂提问：通过提问及利用课堂派与学生互动，及时了解学生知识点掌握情况。

课外学习测量评价：

1. 课前预习：通过课程学习平台开展预习。
2. 课后作业：通过课堂派布置作业，每个章节 1 个作业，内容见课堂派。

10.教学反思与改进：（授课后教师总结）

11.授课教师认为尚未包含在内的设计内容：（授课后教师总结）