河南中医药大学课堂教学设计

授课章节	第 11 章：系统安全		授课学时	2 学时
所属课程	操作系统	授课年级	2021 级	
设计者	阮晓龙	授课专业	医学信息工程本科	

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. 让学生了解系统安全；
2. 让学生掌握使用 SELinux 提升内核安全性；
3. 让学生掌握使用 Firewalld 提升系统安全性；
4. 让学生掌握使用 Nmap 进行系统安全检测。

能力目标：

1. 学生能明白操作系统安全的重要性；
2. 学生能使用 SELinux 提升内核安全性；
3. 学生能使用 Firewalld 提升系统安全性。
4. 能够独立使用 Namp 进行系统安全检测；

素质目标：

1. 激发学生对系统安全的兴趣，培养其主动探索知识的欲望；
2. 培养学生的技术理解与应用能力；
3. 培养学生的问题解决与调试能力；
4. 培养学生拥有较强的实践能力与创新精神。

思政目标：

1. 让学生感受到技术实践的挑战和成就感，从而增强自信和自强的思想品质；
2. 让学生明确自己在使用 SELinux 和防火墙等系统安全工具时的责任和义务；
3. 让学生学生树立正确的网络伦理观念，积极传播正能量，共同构建安全、健康的网络社区。

2.教学内容：依据教学大纲；含教学重点难点

教学重点：

1. 系统安全；
2. 使用 SELinux 提升内核安全性；
3. 使用 Firewalld 提升系统安全性；
4. 使用 Nmap 进行系统安全检测。

教学难点：

1. 使用 SELinux 提升内核安全；
2. 使用 Firewalld 提升系统安全；
3. 使用 Nmap 进行系统安全检测。

课堂教学内容:

1、讲述操作系统安全（10 分钟）

结合 PPT 和案例讲述系统安全的概念、安全风险、提升操作系统安全的方法、Linux 内置多种安全保护机制 4 点内容。

Linux 内置多种安全保护机制：PAM 机制、安全审计机制、强制访问控制机制、防火墙机制。

2、讲述使用 SELinux 提升内核安全性（20 分钟）

结合 PPT 和视频演示讲述使用 SELinux 提升内核安全性，包括 SELiux 简介、SELinux 的用途、安全上下文 Security Context、Booleans、案例 5 点内容。

SELinux 简介：SELinux 是美国国家安全局（NAS）项目，旨在增强 Linux 系统的安全性；SELinux 起源于 1980 年开始的微内核和操作系统安全的研究，这两个方向的研究最后形成了分布式信任计算机（DTMach，Distribute Trusted Mach）项目，融合了前期研究项目的成果；美国国家安全局参加了 DTMach 项目，并继续参与了后续安全微内核项目，最终产生了一个新的项目 Flask，支持更丰富的动态类型的强制机制。

SElinux 的用途：作用：采用最小权限原则、最大限度地减小系统中服务进程可访问的资源。

SELinux 的工作模式：工作模式决定 SELinux 是否启用，包括 enforcing：强制模式，启用 SELinux、permissive：宽容模式，启用 SELinux，但不阻止任何操作，只提出警告信息、disabled：关闭模式，关闭 SELinux。

安全上下文 Security Context：SELinux 的工作过程主要通过安全规则和安全上下文协同，包括安全规则、安全上下文（Security Context）。安全上下文介绍是操作系统访问控制是以关联客体和主体的访问控制属性为基础的；SELinux 中，访问控制属性叫做安全上下文；SELinux 中，所有客体（文件、进程间通讯通道、套接字、网络主机等）和主体（进程）都有与其关联的安全上下文；SELinux 启用后，系统中所有的资源都会进行标识，就是安全上下文；SELinux 通过安全上下文信息来完成访问控制。

Booleans 特点：对 Security Context 的修改需要一定的专业能力和丰富的经验；使用 Booleans 可以更改安全规则的部分内容；修改 Booleans 是 SELinux 管理配置的常用操作。

案例：SELinux 为业务提供安全保障：以【任务：使用 Apache 发布多个静态网站】 、【任务：实现远程连接 MySQL 数据库服务器】、【任务：通过 vsftpd 实现 FTP 服务器】、【任务：使用 BIND 实现域名解析服务】为例讲述本部分内容。

3、讲述使用 Firewalld 提升系统安全性（20 分钟）

结合 PPT 和视频演示讲述使用 Firewalld 提升系统安全性，包括防火墙、Firewalld、Zone、Firewalld-cmd、Firewalld Log、案例 6 点内容。

防火墙：防火墙是服务器安全的重要保障系统，遵循允许和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。

Firewalld：firewalld 与 iptables 之间的异同点：

firewalld 防火墙可以动态修改单条规则与管理规则集等，允许更新规则而不破坏现有会话和连接，而 iptables 防火墙在修改规则后必须全部会话刷新后才可以生效；firewalld 防火墙使用区域和服务，而 iptables 防火墙则使用链式规则；firewalld 防火墙规则默认为拒绝。

课堂教学内容:

而 iptables 防火墙规则默认为允许；firewalld 和 iptables 本身均不具备防火墙的功能，实现的均是防火墙的管理；firewalld 和 iptables 的防火墙功能是通过内核 netfilter 来实现的。

Zone：基于用户对网络中设备和通信的信任程度，防火墙将网络分割成不同的区域（Zone）。

Firewalld-cmd：防火墙的配置模式：runtime configuration：运行时配置，就是防火墙当前起效的规则；permanent configuration：存储的配置，就是防火墙启动时会加载的规则。

使规则永久生效的两种配置方式：使用--runtime-to-permanent 选项：将当前运行的防火墙规则永久保存；使用--permanent 选项：配置防火墙规则，并永久存储；举例：# firewall-cmd --zone=public --add-port=80/tcp --permanent。

Firewalld Log：全局日志配置是对防火墙日志规则进行配置：防火墙日志服务由系统 rsyslog 服务进行管理、日志默认存放在/var/log/firewalld 日志文件中、日志文件基于日期时间自动归档。规则日志配置是设置防火墙触发特定防火墙规则时记录日志的方式。全局日志配置案例：通过修改防火墙与 rsyslogd 配置文件，对防火墙日志字段、日志文件存放路径、日志文件分割方法等进行自定义配置、完成对防火墙全局日志的配置。规则日志设置案例：在配置防火墙规则时，可定义由该规则产生的日志的记录方式。

案例：防火墙为业务提供安全防护：以【任务：通过 vsftpd 实现 FTP 服务器】为例，通过对防火墙规则设置提升文件传输服务的安全性、以【任务：使用 BIND 实现域名解析服务】为例，通过对防火墙规则设置提升域名解析服务的安全性。

4、安全审计与信息安全测评（10 分钟分钟）

安全审计是对目标主机的整体审计，主要包含以下内容与步骤：

①实施端口扫描与服务探测：如果目标主机处于开机状态，通过扫描与探测，可得到目标主机的端口状态（监听/关闭）、目标主机中服务程序列表和版本信息以及目标主机操作系统版本和内核信息等。

②以攻击渗透等方式进行模拟探测：根据获取到目标主机上的服务列表和版本信息，查询安全漏洞数据库，获取有针对性的攻击脚本，开展对目标主机系统的尝试性攻击，并记录目标主机对攻击的响应信息。

③对数据进行分析并产生报告：对获取的响应信息进行分析，并比对安全漏洞信息数据库，明确目标主机确实存在的安全漏洞信息，形成安全审计报告。

④安全风险处理：系统管理员根据安全审计报告的内容，逐项对照解决安全风险。

5、使用 Nmap 进行主机检测（10 分钟）

使用 Nmap 工具对指定网络范围内的主机运行状态、开启的服务端口、运行软件及版本信息、操作系统信息进行检测。实现 4 个目标：

①检测网络内主机的开启状态；

②检测开启主机的端口信息；

③检测开启主机的业务服务信息；

④检测开启主机的操作系统信息。

6、总结（5 分钟）

让学生自主回顾本节课所讲述的知识，标记重点。下达任务，课后自主按照本节课所讲述的内容，进行课后练习。

课堂教学内容:

3.思政知识点:

课程思政案例	思政点映射
随着技术的不断进步，国内的操作系统开发能力也越来越强，2023 年，国内首个自主研发的操作系统——“麒麟操作系统”正式上线发售，这标志着国内操作系统的制造商终于走出了一个新的天地。而在其之后，不断涌现的国产化操作系统，如“中标麒麟”、“龙芯”等，正在不断扩大着自己的市场份额。相对应的是，随着国内 IT 产业不断加速发展，网络攻击事件也愈加频繁，而操作系统国产化后，国内安全技术人才的不断涌现，则成了保障网络安全的重要力量，并且不断推陈出新地吸取国外先进技术，以追赶甚至超越国外操作系统的技术水平。	通过引入操作系统国产化后，国内网络安全的力量增强，提高了学生对网络安全的认知，让学生体会中国科技进步的动态增长，感受到中国的强大发展。

4.学情分析及教学预测：

学生的知识基础：

1. 掌握了 Linux 操作系统方面的知识；
2. 在安全方面了解相关知识。

学生的认知特点：

1. 对系统安全方面缺少相关知识；
2. 对使用 SELinux、Firewalld 提升系统安全性缺少相关知识。

学生的学习风格：

1. 学生对于新课程、新事物都持有很高的学习兴趣，有利于课程的学习，学生思维活跃，课堂气氛较好；
2. 学生具备一定的独立理解思考的方法与能力。

教学预测：

1. 通过对系统安全的讲解，可增加学生对系统安全方面的学习兴趣；
2. 通过 PPT+视频操作演示，可以更加有效的提高授课效率；
3. 本节课讲述的内容实操过程较少，理论知识较多，要更加留意学生的听课状态。

5.教学策略与方法：

教学策略：

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. 通过使用 PPT+视频案例演示的教学方法，激发学生的学习兴趣。

教学方法：

1. 讲解法、演示法、举例法：课堂上使用 PPT 对理论知识进行讲解，并且进行视频举例演示；
2. 练习法：课后让学生按照上课所讲内容，在自己本机上进行实操演示。

6.板书设计：

① **黑板（白板）设计：**

SElinux
Firewalld
安全审计
没有绝对的安全

② **现代信息媒体设计：**

使用多媒体教学课件开展。
课件版本：操作系统-CentOS.2023

7.教学互动环节设计：

课堂上的提问和互动交流：

1. 问题一：SELinux 的策略规则是如何限制和控制进程和资源访问的？可以举个例子说明吗？
2. 问题二：你认为防火墙在系统安全中的地位和作用是什么？为什么防火墙是必需的安全措施？
3. 问题三：操作系统安全该如何保证？

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. 速学 150 个 Linux 常用命令：https://www.bilibili.com/video/BV12L411a7Ne
2. 韦东山手把手教你嵌入式 Linux 快速入门到精通：
   https://www.bilibili.com/video/BV1w4411B7a4

官方文档：

1. RedHat Enterprise Linux Doc：
   https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9
2. CentOS Stream Doc：https://docs.centos.org/en-US/docs/

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）