河南中医药大学课堂教学设计

授课章节	第 11 章：系统安全（Nmap）		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	信息管理与信息系统本科	

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. 让学生了解操作系统安全的重要性；
2. 让学生了解 Namp 的作用；
3. 让学生掌握使用 Nmap 进行系统安全检测；
4. 让学生掌握使用 Nmap 对网站服务器与网站业务进行安全评估。

能力目标：

1. 能简单谈谈操作系统安全的重要性；
2. 能够理解 Namp 检测的作用；
3. 能够独立使用 Namp 进行系统安全检测；
4. 能够独立使用 Namp 对网站服务器与网站业务进行安全评估。

素质目标：

1. 激发学生对操作系统安全的思考，培养其主动探索系统安全领域；
2. 培养学生拥有沟通交流、团队协作、组织管理等能力；
3. 培养学生拥有较强的实践能力与创新精神；
4. 培养学生认真踏实、勇于从事计算机专业研发工作的职业精神。

思政目标：

1. 帮助学生树立正确的价值观；
2. 坚定学生的理想信念，培养学生的创新能力；
3. 培养学生未来作为计算机行业从业人员的责任心和使命感。

2.教学内容：依据教学大纲；含教学重点难点

教学重点：

1. 操作系统安全的重要性；
2. Namp 的作用；
3. 使用 Nmap 进行系统安全检测；
4. 使用 Namp 对网站服务器与网站业务进行安全评估。

教学难点：

1. 使用 Nmap 进行系统安全检测；
2. 使用 Namp 对网站服务器与网站业务进行安全评估。

课堂教学内容:

1、操作系统安全的重要性（10 分钟）

系统安全是指在系统生命周期内，应用系统安全工程和系统安全管理方法，辨识系统中的隐患，采取有效的控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。操作系统是信息系统的重要组成部分，操作系统的安全在整个信息系统的安全性中起到至关重要的作用，没有操作系统的安全，信息系统的安全性将犹如建在沙丘上的城堡一样没有牢固的根基。操作系统位于软件系统的底层，需要为其上运行的各类应用服务提供支持。操作系统是系统资源的管理者，对所有系统软、硬件资源实施统一管理。作为软硬件的接口，操作系统起到承上启下的作用，应用软件对系统资源的使用与改变都是通过操作系统来实施。

2、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。

3、使用 Nmap 进行主机检测（15 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。

4、使用 Nmap 评估域名解析服务的安全风险（15 分钟）

通过 Nmap 工具检测域名解析服务的安全风险。实现 5 个目标：

①使用“dns-nsid”插件检测 DNS 服务运行版本的详细信息；

②使用“dns-brute”插件检测是否能够破解列出 DNS 服务器中“domain.com”域名下的主机记录信息；

③使用“dns-blacklist”插件检测 DNS 服务器是否支持防止 DNS 反垃圾和打开 Proxy 黑名单等安全措施；

④使用“dns-random-srcport”插件检测 DNS 服务器是否存在可预测的端口递归漏洞；

⑤使用“dns-random-txid”插件检测 DNS 服务器是否存在可预测的 TXID DNS 递归漏洞。

5、Nmap 实现自动化安全评估（15 分钟）

使用 Nmap 实现自动化安全评估：

①安装 Nmap；

②关闭受测主机防火墙等安全措施以凸显检测效果（实验目的）；

③安装电子邮件发送客户端工具；

④明确安全检测的内容与计划；

⑤撰写自动化安全评估的脚本程序；

课堂教学内容：

⑥执行并测试结果。

使用 Nmap 工具对网络内主机与域名解析服务进行安全检测，检测完成后通过电子邮件将报告发送给指定的运维管理人员。以达到运维管理人员快速发现安全风险，实现运维管理与安全检测的部分自动化。本步骤通过操作系统的任务计划进行任务调度，安全评估任务实现 4 个目标：

①自动进行安全检测，每天 00:00 执行，检测结果以邮件的形式发送给运维人员；

②对网络内主机运行状态、开启端口、运行软件版本、操作系统信息等内容进行检测；

③实现对域名解析服务的安全性检测；

④检测结果内容通过电子邮件发送给指定电子邮箱。

6、对网站服务器与网站业务进行安全评估（15 分钟）

对网站服务器与网站业务进行安全评估：

①受测主机进行系统与业务安全配置（检测目的）；

②检测操作系统的安全性；

③检测网站服务的安全性；

④检测 PHP 的安全性；

⑤检测 MariaDB 的安全性；

⑥检测 WordPress 的安全性 撰写安全评估报告。

3.思政知识点：

课程思政案例	思政点映射
2006 与 2007 年岁交替之际，网络上最火的动物既不是“狗”也不是“猪”，而是一只拜着三只高香的国宝熊猫。一名为“熊猫烧香”的计算机病毒在互联网上掀起轩然大波。从 2006 年 11 月首次出现至 2007 年 1 月份，短短两个多月，病毒已迅速在全国蔓延，受害用户至少上百万，计算机反病毒公司的热线电话关于该病毒的咨询和求助一直不断，互联网上到处是受害者无奈的求助、怨恨、咒骂，电脑里到处是熊猫烧香的图标，重要文件被破坏， 局域网彻底瘫痪，病毒造成的损失无法估量。在两个多月的时间里，数百万电脑用户被卷进去，那只憨态可掬、颔首敬香的“熊猫”除而不尽，成为人们噩梦般的记忆。	通过介绍安全事件提升学生对系统安全重要性的认知，培养学生追求科学真理、热爱祖国、为保护网络空间安全努力奋斗的情怀。

4.学情分析及教学预测：

学生的知识基础：

1. 计算机操作系统理论；
2. Linux 操作系统。

学生的认知特点：

1. 对 Linux 操作系统有了一定的理解和认识；
2. 对 Linux 操作系统下的常见服务有一定的了解，缺乏系统安全方面的认知。

学生的学习风格：

1. 对新鲜事物充满好奇，对新知识的学习充满激情；
2. 能够积极的对待课堂所讲的内容。

教学预测：

1. 学生了解了 Linux 操作系统下的常见服务，从服务安全性的角度出发，引导学生学习系统安全的检测。

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。

6.板书设计：

① **黑板（白板）设计：**

Nmap 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：是否存在绝对的安全呢?
2. 问题二：操作系统安全该如何保证？
3. 问题三：Nmap 都有哪些作用，能够提升服务安全性吗？

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. 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）