【网络管理与安全】

【Network Management and Security】

一、基本信息

课程代码：【0050154】
课程学分：【3】
面向专业：【计算机应用技术】
课程性质：【专业领域课程组、专业限选课】
开课院系：【职业技术学院机电系计算机应用技术专业】
使用教材：

教材【网络安全与管理（第 3 版），石磊 赵慧然 肖建良，清华大学出版社，2021 年 9 月】

参考书目

【计算机网络安全与管理项目教程，张虹霞 王亮，清华大学出版社，2018 年 7 月】
【网络安全技术及应用实践教程（第 3 版），贾铁军等，机械工业出版社，2018.7 .“十三五”国家重点出版规划项目暨上海市高校精品课程教材】
【计算机网络管理与安全，郭峰、董德宝等，清华大学出版社，2016.11】
【网络攻击与防御技术，张玉清，清华大学出版社，2011 年 1 月】
【CCNA 网络安全运营，[美]艾伦.约翰逊，人民邮电出版社，2019 年 8 月】

先修课程：【计算机网络技术 0050064（3）】

二、课程简介

习近平主席多次强调“没有网络安全就没有国家安全”。随着各种网络技术的快速发展和广泛应用，我国在网络化建设方面取得了令人瞩目的成就，电子银行、电子商务和电子政务的广泛应用，使各种网络已经深入到国家的政治、经济、文化和国防建设等各个领域，遍布现代信息化社会的工作和生活每个层面，“数字化经济”和全球电子交易一体化正在形成。网络管理与安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及到国家政治、军事和经济各个方面，而且影响到国家的安全和主权。随着各种网络的广泛应用和网络之间数据传输量的急剧增大，网络管理与安全的重要性尤为突出，已经成为各国关注的焦点，也成为研究热点和人才需求的新领域。

网络管理与安全内容涉及网络管理和网络安全两大方面。主要包括：攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）等多方面的基础理论和实用技术。网络管理与安全属于综合、交叉学科领域，综合利用管理、信息安全和计算机等多学科的长期知识积累和最新发展成果的不断发展和完善。

三、选课建议

该课程的选课建议：适合计算机应用技术等计算机类各专业课程或专业限选课程，通常在大二或大三开设，需要先行修完计算机网络技术等专业基础课程。

四、课程与专业毕业要求的关联性

计算机应用专业毕业要求	关联
L011：表达沟通：能领会用户诉求，正确表达自己的观点，具有专业文档的撰写能力。	
L021：自主学习：能根据环境需要确定自己的学习目标，并主动地通过搜集信息、分析信息、讨论、实践、质疑、创造等方法来实现学习目标。	●
L031：工程素养：掌握数学、自然科学知识，具有工程意识，能结合计算机、计算机网络相关专业知识解决复杂工程问题。	
L032：软件开发：系统掌握基于计算机网络应用系统的设计与开发的基本方法和技能，具备网页设计、网站建设与维护能力。	
L033：系统运维：系统地掌握计算机硬件、软件的基本理论、基本知识，具备保障计算机系统运行与维护基本技能。	
L034：网络工程设计与实施：掌握计算机网络系统的规划、设计方法，具备组建企业或校园网基本技能。	
L035：网络安全管理：系统地掌握信息安全的基本原理和防范策略，具备保障计算机网络安全运行基本技能。	●
L036：网络协议分析：系统地掌握计算机网络协议的基本原理、基本规则，能灵活运用工具实时捕捉数据进行分析。	
L041：尽责抗压：遵守纪律、守信守责；具有耐挫折、抗压力的能力。	
L051：协同创新：能与团队保持良好关系，积极参与其中，保持对信息技术发展的好奇心和探索精神，具有创新性解决问题的能力。	●
L061：信息应用：能发掘信息的价值，综合运用相关专业知识和技能，解决实际问题。	
L071：服务关爱：愿意服务他人、服务企业、服务社会；为人热忱，富于爱心，懂得感恩。	
L081：国际视野：具有基本外语表达沟通能力，积极关注发达国家和地区信息技术发展新动向。	

备注：LO=learning outcomes（学习成果）

五、课程目标/课程预期学习成果

序号	课程预期 学习成果	课程目标 （细化的预期学习成果）	教与学 方式	评价方式
1	LO21：自主学习：能根据环境需要确定自己的学习目标，并主动地通过搜集信息、分析信息、讨论、实践、质疑、创造等方法来实现学习目标。	1、能通过课件、实验文档、实验虚拟化环境、线上课堂、线上作业和测试，开展自我学习，线上线下相结合，完成课下作业和巩固课堂教学内容； 2、能针对课程教学中遇到的疑难问题，课下利用图书馆纸质和电子图书资源以及各类知识型网站，查找各类知识点的解答和实例分析，逐步加深对专业知识的了解和掌握，激发学习的兴趣。	课堂示范、课下练习	实验报告、作业
2	LO35：网络安全管理：系统地掌握信息安全的基本原理和防范策略，具备保障计算机网络安全运行基本技能。	1、了解和掌握信息安全的基本要素，能运用信息安全要素管理社会企业各种类型网络和系统；了解和掌握信息安全基本模型P2DR2，能运用模型设计信息安全保护方案，监控信息安全各个流程环节。 2、能根据不同操作系统的环境和不同服务的类型，进行加固和防御； 3、能根据网络实际情况开展网络设备 ACL 的访问设置，能根据用户和组、文件系统和访问控制权限进行防御设置。 4、能根据不同操作系统的环境和不同服务的类型，掌握日志的位置和分析方法； 5、能根据网络实际情况开展入侵检测的监控，能根据日志和入侵检测警报综合分析入侵来源和入侵行为。	讲授、演练、实践	实验报告、作业、小测验
3	LO51：协同创新：能与团队保持良好关系，积极参与其中，保持对信息技术发展的好奇心和探索精神，具有创新性解决问题的能力。	能够根据现实实际网络系统中的问题，进行分析并解决问题；能够实现协同学习掌握网络管理与安全相关方面的知识、技术和方法与实际应用	视频、讲授、分组协同、线上课堂	体现解决问题的作业、练习

六、课程内容

第 1 单元 网络管理与安全概述

理解网络安全的概念；知道网络安全与信息安全、数据安全的区别；理解信息安全要素；分析网络安全的主要威胁；理解网络安全研究内容及相互关系；知道网络安全策略；理解网络安全模型；能分辨网络安全与信息安全的关系，能根据 P2DR2 模型分析网络安全管理流程。

重点：信息安全三要素，P2DR2 模型

理论课时数：2

实践课时数：0

第 2 单元 网络安全的基本配置

理解 OSI 模型；知道路由器交换机的基本功能；知道路由的类型；理解 ACL 的概念；理解 VLAN 的概念；理解 VTP 的概念；能熟练使用 Packet Tracer 模拟器配置交换机、路由器、ACL、VTP。

重点：ACL 配置，VTP 配置

理论课时数：0

实践课时数：4

第 3 单元 操作系统安全的基本配置

理解操作系统用户与工作组的概念；能进行 Windows 本地用户和组、本地安全策略、组策略的基本配置；理解访问控制的基本原理，能进行文件访问控制的配置；知道文件夹加密的原理，能进行加密证书的导出和导入。知道 RWX 的含义，知道/etc/passwd 等文件的内容，能进行 Linux 文件权限的设置与修改；知道 ssh 的功能，能进行 ssh 远程登录加固的配置。

重点：账户管理策略，文件访问控制权限，文件夹加密

理论课时数：4

实践课时数：4

第 4 单元 数据库安全的基本配置

理解 SQL Server 数据库登录的两种方式；知道数据库账户管理策略；知道数据库权限设置的方法；理解数据库系统加固的概念；能进行服务器角色和数据库角色的设置，能进行角色的权限设置。

重点：服务器角色设置，数据库角色设置

理论课时数：2

实践课时数：2

第 5 单元 软件安全漏洞分析

知道缓冲区溢出漏洞的成因；理解堆和栈在数据存储和读取等方面的主要区别；能运用 IDA pro 和 OllyDBG 进行静态和动态分析，能进行分步调试，能观察栈区数据变化。

重点：堆溢出漏洞，栈溢出漏洞

理论课时数：2

实践课时数：6

第 6 单元 密码学基本原理

理解对称加密和非对称加密的区别；理解混合加密对于信息机密性、完整性、不可抵赖性的保证；知道大数分解；知道求余运算和幂运算；能进行简单的 RSA 算法计算和验证；能分析混合加密的各个阶段。

重点：RSA 算法，混合加密

理论课时数：4

实践课时数：0

第 7 单元 入侵检测的原理与实践

知道日志的不同类型；知道日志记录的内容；知道正则表达式；知道日志文件的存放位置；知道数据抓包；能熟练运用 Wireshark 进行数据抓包实验，能分析数据包内容；理解入侵检测的基本概念；理解 snort 基本工作原理；能熟练运用 snort 开展入侵检测监控。

重点：日志格式，snort

理论课时数：6

实践课时数：8

序号	教学内容	课时分配		
		理论	实验	合计
1	第 1 章 网络管理与安全概述	2	0	2
2	第 2 章 网络安全的基本配置	0	4	4
3	第 3 章 操作系统安全的基本配置	4	4	8
4	第 4 章 数据库安全的基本配置	2	2	4
5	第 5 章 软件安全漏洞分析	2	6	8
6	第 6 章 密码学基本原理	4	0	4
7	第 7 章 入侵检测的原理与实践	6	8	14
8	复习及机动	4	0	4
总 计		24	24	48

七、课内实验名称及基本要求

序号	实验名称	主要内容	实验时数	实验类型	备注
1	网络设备的基本安全配置	（1）路由器 ACL 配置 （2）交换机 VTP 配置	4	验证	
2	操作系统安全的基本配置	（1）用户与组 （2）文件系统权限 （3）系统加固	4	验证	
3	数据库安全的基本配置	（1）SQL Server 数据库安全配置 （2）MySQL 数据库安全配置	2	验证	
4	软件安全漏洞分析	（1）堆溢出漏洞分析 （2）栈溢出漏洞分析	6	验证	
5	入侵检测的原理与实践	（1）Snort 与防火墙规则 （2）日志文件分析 （3）PCAP 提取文件	8	验证	
合计	5 次		24		

八、评价方式与成绩

总评构成（1+X）	评价方式	占比
1	期终闭卷考试	60%
X1	实验记录	20%
X2	随堂测验	10%
X3	课堂笔记	10%

撰写人：周胜利　　系主任审核签名：

审核时间：2023.2