【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

【网络安全与管理实验与实训，石磊 赵慧然 肖建良，清华大学出版社，2021 年 9 月】

【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（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
LO1：品德修养：拥护中国共产党的领导，坚定理想信念，自觉涵养和积极弘扬社会主义核心价值观，增强政治认同、厚植家国情怀、遵守法律法规、传承雷锋精神，践行“感恩、回报、爱心、责任”八字校训，积极服务他人、服务社会、诚信尽责、爱岗敬业。	
LO2：专业能力：具有人文科学素养，具备从事某项工作或专业的理论知识、实践能力。	●
LO3：表达沟通：理解他人的观点，尊重他人的价值观，能在不同场合用书面或口头形式进行有效沟通。	
LO4：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。	●
LO5：健康发展：懂得审美、热爱劳动、为人热忱、身心健康，耐挫折，具有可持续发展的能力。	
LO6：协同创新：同群体保持良好的合作关系，做集体中的积极成员，善于自我管理和团队管理；善于从多个维度思考问题，利用自己的知识与实践来提出新设想。	●
LO7：信息应用：具备一定的信息素养，并能在工作中应用信息技术和工具解决问题。	
LO8：国际视野：具有基本的外语表达沟通能力与跨文化理解能力，有国际竞争与合作的意识。	

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	LO41：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	LO25：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； 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、理解网络监控的基本原理，能够利用网络监控工具 Sniffer Pro 开展网络监控实验。 4、掌握基本的信息加密算法，并能利用 PGP 软件进行通讯加密测试； 5、理解并掌握 VPN 技术的基本原理，学习通过虚拟机对 Windows Server 2003 中的 VPN 功能进行配置，学习 IPsec VPN 隧道，熟悉移动办公方式下的 VPN 隧道的建立。 6、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	LO61：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 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 3 单元 网络监控的原理与实践

理解 OSI 网络模型；了解网络监控的原因及目标；理解网络监控的分类方法及各类监控方法基本原理。掌握 Sniffer 的基本原理、攻击方法及防御方案。能进行 Sniffer Pro 的配置及使用；能进行网路岗软件的配置和使用。

重点：Sniffer Pro 配置，网路岗软件配置

理论课时数：2

实践课时数：4

第 4 单元 密码学基本原理及验证

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：2

第 5 单元 VPN 服务的配置与使用

理解并掌握 VPN 技术的基本原理；知道常用的 VPN 技术；学习通过虚拟机对 Windows Server 2003 中的 VPN 功能进行配置，学习 IPsec VPN 隧道，熟悉移动办公方式下的 VPN 隧道的建立。理解 PPTP 与 L2TP 之间的区别

重点：VPN 技术的基本原理，VPN 功能配置

理论课时数：2

实践课时数：4

第 6 单元 病毒技术与病毒防控

知道病毒的概念及发展；理解常见的病毒、木马、蠕虫的概念及异同；理解流氓软件的定义及防止方法；掌握基本的病毒检测方法，并能够利用火绒安全软件实现常用的访问控制功能。

重点：网络病毒的概念及原理，病毒防控技术

理论课时数：2

实践课时数：4

第 7 单元 入侵检测的原理与实践

掌握入侵检测系统的基本概念，理解常用的入侵检测系统及评价方法。理解并掌握常用的入侵检测方法。理解 IDS 和 IPS 的部署方案。根据教材中介绍的 ZoomEye 及 FOFA 的功能和步骤完成实验。在掌握基本功能的基础上，实现网络空间搜索引擎的使用，并能给出实验报告。

重点：ZoomEye，FOFA

理论课时数：4

实践课时数：6

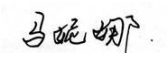
序号	教学内容	课时分配		
		理论	实验	合计
1	第 1 章 网络管理与安全概述	2	0	2
2	第 2 章 操作系统安全的基本配置	4	4	8
3	第 3 章 网络监控的原理与配置	2	4	6
4	第 4 章 密码学基本原理及验证	4	2	6
5	第 5 章 VPN 服务的配置与使用	2	4	6
6	第 6 章 病毒技术与病毒防控	2	4	6
7	第 7 章 入侵检测的原理与实践	4	6	10
8	复习及机动安排	4	0	4
总 计		24	24	48

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	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	
2	Sniffer 网络监控实践	(1) 数据报文解码 (2) 网络流量监控 (3) 监控广播风暴	4	验证	
3	PGP 软件的安装与使用	（1）PGP 软件的安装 （2）PGPmail 的使用 （3）PGPdisk 的使用	2	验证	
4	VPN 服务的配置与使用	（1）PPTP 实现 VPN 服务 （2）在 PPTP VPN 的基础上配置 L2TP/IPSec VPN	4	验证	
5	火绒安全软件的使用	（1）了解安全防御软件的原理 （2）熟练使用火绒软件进行安全配置	4		
6	网络空间搜索引擎的使用	（1）ZoomEye 的 安全与配置 （2）FOFA 的安装与配置	6	验证	
合计	6 次		24		

八、评价方式与成绩

总评构成（全 X）	评价方式	占比
X1	随堂测验	40%
X2	实验记录	20%
X3	作业完成	20%
X4	课堂展示	20%

撰写人：王松　　系主任审核签名： 

审核时间：2023 年 9 月