

【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】

课程性质：【专业限选课】

开课院系：信息技术学院 网络工程系

使用教材：主教材【网络安全技术及应用.贾铁军等.机械工业出版社.2014年9月第2版】

辅助教材【信息安全概论(第二版). 杨义先等】

先修课程：【计算机网络原理】

二、课程简介

网络管理与安全是计算机应用专业的一门专业限选课。通过本课程的学习，学生可以掌握计算机网络管理与安全技术的基本概念，熟悉现行的网络管理标准和安全技术应用，并具有网络管理系统和网络安全工具的实现和实践能力。

三、选课建议

本课程适合计算机应用专业学生，在理解计算机网络等知识，进一步理解信息安全的知识。

四、课程与培养学生能力的关联性

自主学习	表达沟通	专业能力						尽责抗压	协同创新	服务关爱	信息应用	国际视野
		软件开发	系统运维	系统设计	系统测试	撰写技术文档	嵌入式系统开发					
●	●	●	●	●	●	●	●	●			●	●

五、课程学习目标

通过本课程的学习，学生以 TCP/IP 网络管理为主线，系统地讨论了计算机网络管理协议、网络管理系统，并结合网络管理工具深入讨论网络管理技术的应用。本课程对网络安全基础、网络安全技术、操作系统的安全性等进行了较全面的介绍，并以任务驱动的方式，介绍网络安全工具的使用，使学生能够对 Windows 平台上的安全管理问题进行初步分析和解决。

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

六、课程内容

第1章 信息安全简介

知道信息安全的发展历程，定义和涵盖范围。理解网络安全是信息安全的重要组成部分，理解网络安全的主要技术手段。知道信息安全中有关的非技术因素。

本章的重点是网络安全主要的技术手段。

第2章 网络安全技术基础

知道计算机网络协议安全概述；知道网络安全体系结构和安全服务与安全机制。应用虚拟专用网(VPN)技术和无线局域网安全技术；应用常用的网络命令。

本章的重点是掌握虚拟专用网技术和学会常用的网络命令。

第3章 网络安全管理概论

理解网络安全管理概念、内容及功能；理解安全管理的原则及制度、防护体系规范和政策；理解网络安全管理技术、策略及主机网络防护、网络安全管理解决方案；知道实体安全防护有关技术；知道软件安全有关技术。

本章的重点是掌握网络安全管理技术、策略及主机网络防护、网络安全管理解决方案。

第4章 黑客攻防与检测防御

了解黑客攻击的目的及攻击步骤；熟悉黑客常用的攻击方法；理解防范黑客的措施；掌握黑客攻击过程，并防御黑客攻击；掌握入侵检测系统的概念、功能、特点、分类、检测过程和常用检测方法。

通过本章实验使学生学会各类网络监听，端口扫描工具的基本操作及捕获数据包。

本章的重点是理解防范黑客的措施；掌握黑客攻击过程，并防御黑客攻击。

第5章 身份认证与访问控制

理解身份认证技术的概念、种类和方法；了解登录认证与授权管理；掌握数字签名技术及应用；掌握访问控制技术及应用；掌握安全审计技术及应用。

本章的重点是掌握访问控制技术及应用；掌握安全审计技术及应用。学会 Windows 操作系统的 NTFS 权限应用。

第6章 密码及加密技术

理解密码技术相关概念、密码学与密码体制；理解数据及网络加密的方式；知道密码破译方法与密钥管理；综合应用各类实用加密技术，包括：对称/非对称加密、单向加密技术、无线网络加密技术等。知道实用综合加密方法、加密高新技术及发展；知道数据压缩的基本概念和使用方法。

通过本章实验使学生学会各类加密软件的使用。

本章的重点是掌握数据及网络加密方式；掌握实用加密技术。

第7章 数据库安全技术

知道数据库系统安全的概念、组成和安全性要求；知道数据库系统的安全框架与特性；理解数据库的

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

数据保护三个方面：安全性、完整性和并发控制；熟练应用几种常见数据库攻击方法，并能用于防御实践；理解数据库系统的数据备份和恢复概念、策略和方法；知道网络数据库的安全管理措施。

通过本章实验使学生学会在 WEB 应用服务器上实现 SSL 协议访问（包括证书的请求和颁发）。

本章的重点是理解数据库的数据保护三个方面：安全性、完整性和并发控制；掌握几种常见数据库攻击方法，并能用于防御实践。

第 8 章 计算机病毒防范

知道计算机病毒发展的历史和趋势；理解病毒的定义、分类、特征、结构、传播方式和病毒产生；掌握病毒检测、清除、防护、病毒和反病毒的发展趋势；理解恶意软件概念、分类、防护和清除；综合应用个人杀毒软件。

通过本章实验使学生学会手工查杀病毒的方法。

本章的重点是掌握病毒检测、清除、防护、病毒和反病毒的发展趋势。

第 9 章 防火墙应用技术

理解防火墙的概念；知道防火墙的功能；知道防火墙的不同分类；理解 SYN Flood 攻击的方式及用防火墙阻止 SYN Flood 攻击的方法。

本章的重点是掌握防火墙的功能。学会个人防火墙的设置（以天网防火墙为例）。

第 10 章 操作系统与站点安全

理解 Windows 操作系统的安全性的重要性。学会应用 Windows 系统的安全配置；理解 Web 站点的安全和 Web 站点的安全策略；知道系统恢复的过程和方法。对 Windows 系统的各类安全配置熟练掌握。

本章的重点是理解操作系统的安全配置。应用组策略进行管理。

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	网络监听，端口扫描工具使用	学会使用各种网络监听工具进行网络性能监听，并能通过端口扫描软件进行漏洞扫描操作	4	综合型	PC 机 2 台。 建议 2 人/组。
2	加密软件的使用	理解 RSA 算法的加密和解密过程；知道 MD5 算法如何保证数据的完整性；能应用 PGP 软件进行数字签名。	4	综合型	PC 机 2 台。 建议 2 人/组。
3	计算机病毒查杀	学会分析计算机病毒的基本机理，并能通过病毒现象，手工查杀各类计算机病毒	4	综合型	PC 机 2 台。 建议 2 人/组。
4	个人防火墙设置	使用天网个人防火墙进行相关设置，并能通过防火墙实现对内网的保护操作	4	综合型	PC 机 1 台。 建议 1 人/组。

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

八、评价方式与成绩

总评构成 (1+X)	(1)	(X1)	(X2)	(X3)
评价方式	期终闭卷考	课堂测验	实验报告	工作现场评估
1 与 X 两项所占比例%	30%	20%	30%	20%

撰写：朱曙锋

系主任审核：