《网络安全技术》课程标准

课程编码	0404005	课程类别	专业核心课
计划学时	68	课程类型	B 类
适用专业	计算机应用技术	课程性质	必修
开课学期	第四学期	学分	4
先行课程	计算机网络技术、局域网组建与配置	开课单位	信息工程系
平行课程	虚拟化技术与应用	考核类型	考试
后继课程			

一、课程性质与定位

《网络安全技术》是计算机应用专业的专业技能核心课程。尽管在表述的字面上没有提及网络安全技术，但是对网络安全技术的需求实质渗透到上述三方面能力当中。特别是当前网络安全威胁成为网络应用的最大危害，网络安全性成为网络应用的焦点问题。有研究表明，21 世纪人类对网络最大的担忧是网络安全，未来网络行业最大的就业机会在安全领域。因此《网络安全技术》课程是本专业的核心课程，网络安全应用和管理能力则是学生从事网络技术工作应具备的核心能力之一。

二、课程设计与理念

按照“以能力为本位、以职业实践为主线、以项目课程为主体的模块化专业课程体系”的总体设计要求，该门课程以满足一下要求为基本理念

（1）体系性要求：所设计的模块课程，要求能够既能自成体系，又能独立使用。所谓自成体系是指单个模块课程要涵盖该模块所涉及的所有内容领域，不能有遗漏；所谓能够独立使用，是指该模块课程的设计，要以每一任务为单位，对每一节课甚至每个知识点，要设计出适合教学需要的任务课程，它可以独立用于教学。

（2）功能性要求：所设计模块课程在教学过程中，要在如下五个方面起重要作用：一是用于辅助教师教学，重点在于向学生演示和表达知识，突破重点和难点，辅助教师进行知识的传授；二是辅助学生学习，重点帮助学生巩固知识，诱导学生积极思考，帮助学生发现探索知识；三是提供资料参考，重点在于提供教师备课以及学生学习时的相关参考资料；四是用于学生的兴趣扩展，重点用于

帮助学生发展兴趣爱好、增长见识、形成个性。五是能即时测评，重点在于对学习者的学习效果进行评价并即时反馈。

（3）技能性要求：模块教学设计要符合人才培养方案，要有利于激发学生的学习动机和提高学习兴趣，最终达到让学生掌握改课程所传授的技能，并能将这些技能应用的以后的工作中。

三、课程目标

1．总体目标

《计算机网络安全技术》本课程主要面向网络安全管理职业岗位群，通过本课程的学习，使学生掌握网络安全基本原理、基本技能和基本分析方法。学生学完本课程应具备从事网络安全的管理工作的职业素养，可以独立的从事中小型网络安全的配置、管理和维护工作。更高层次的目标是使学生具备一定的网络系统的安全规划和安全评估的能力。

2．技能与知识目标

（1）了解计算机系统所面临的安全问题，理解计算机网络安全体系结构及网络安全管理的基本内容，了解计算机安全所涉及的法律问题；

（2）了解网络攻击和网络入侵带来的问题和危害，理解并掌握常见的网络入侵技术和网络攻击技术，了解安全防范的基本原则以及常见的安全检测技术；

（3）了解计算机病毒基本概念、病毒的危害以及基本原理，理解计算机病毒的检测技术，掌握计算机病毒的防范措施；

（4）掌握数据加密技术的基本概念，了解对称和非对称密码体制常用的加密方法，初步理解 DES 算法和 RSA 算法，掌握数据加密技术的应用；了解数据完整性的概念，理解报文摘要技术和数字签名技术的基本原理及应用；

（5）理解并掌握主机访问控制的基本原理及访问控制政策，理解防火墙的体系结构及工作原理，掌握 ISA 软件防火墙的配置；

（6）了解入侵检测的基本概念和工作原理，初步掌握一种入侵检测系统的配置与管理；

（7）了解 Windows 服务器所存在的安全隐患，掌握 Windows 服务器的安全管理技术；

（8）了解 VNP 技术的基本概念和原理，初步掌握 VPN 的配置与管理技术；

（9）了解网络安全体系的基本概念，了解构建网络安全体系的基本原则，初步学习运用所学的安全技术构建安全的网络系统。

3．能力与素质目标

（1）理解网络安全威胁的发生机理和网络安全技术原理，具备分析和解决网络安全问题的能力；

（2）熟练掌握各种网络安全实用工具和网络安全产品的使用方法，能够针对不同环境下的网络应用规划设计并实施有效的安全管理。

（3）理解计算机网络安全系统的基本概念及设计原则，初步具备网络安全体系的评估、分析与设计能力。

四、课程教学内容及学时分配

序号	项目名称	学习任务	学习目标	学习内容	学时
1	网络安全概述	1、信息安全概况	了解网络安全的定义，及网络安全状态	信息安全概况、安全产品市场与需求	2
		2、安全人才需求	培养学生正确的网络安全理念和社会责任心	学术研究与开发、安全人才需求	2
2	网络安全扫描技术	1、网络扫描技术概述 2、网络安全扫描的步骤分类 3、常用扫描工具的使用：X-Scan	掌握扫描器的使用方法，能够通过扫描器写出系统漏洞的报告。	网络扫描技术概述、网络安全扫描的步骤分类、常用扫描工具的使用：X-Scan	2
		4、常用扫描工具的使用：Super-Scan 5、常用扫描工具的使用：流光 5	了解网络监听的原理，掌握防御网络监听的方法。	常用扫描工具的使用：Super-Scan、常用扫描工具的使用：流光 5	4
		6、常用扫描工具的使用：NC 7、其它扫描工具、常用命令和抓包分析	掌握常用命令和抓包分析的方法	常用扫描工具的使用：NC、其它扫描工具、常用命令和抓包分析	4
3	windows 密码与权限的安全管理	1、Windows 安全基本知识 2、Windows 安全策略的配置	了解 Windows Server 2003 的新特性与安全机制；	Windows 安全基本知识、Windows 安全策略的配置	2
		3、Windows 注册表安全	了解 Windows Server 2003 的注册表的原理与结构	Windows 注册表安全	2

		4、Windows 服务安全	了解 Windows Server 2003 的安全认证过程	Windows 服务安全	2
		5、Windows 2003 server 域的管理与组策略	掌握 Windows Server 2003 的账户管理	Windows 2003 server 域的管理与组策略	2
		6、Windows 2003 serverWEB 服务器安全管理	掌握 Windows Server 2003 的系统日志的管理；掌握 Windows Server 2003 系统的安全模板的使用	Windows 2003 serverWEB 服务器安全管理	4
4	远程控制与木马安全	1 远程控制基本原理 2、常用远控软件的使用：PCAnywhere	理解远程控制的原理	远程控制基本原理 、常用远控软件的使用：PCAnywhere	4
		3、木马的控制原理 4、常见木马的使用：冰河 5、常见木马的使用：灰鸽子	理解木马的控制原理；掌握常见木马工具的使用	木马的控制原理；常见木马的使用：冰河；常见木马的使用：灰鸽子	4
		6、利用系统漏洞进行远控：3389 攻击 7、利用系统漏洞进行远控：IPC$ 攻击 8、病毒木马的防治与查杀	掌握病毒木马的防治与查杀	利用系统漏洞进行远控：3389 攻击；利用系统漏洞进行远控：IPC$ 攻击；病毒木马的防治与查杀	4
5	网络安全体系	1、网络安全层次体系结构 2、网络安全过程分析	熟悉网络安全体系结构；掌握网络管理的基本功能、网络安全管理基本概念和内涵	网络安全层次体系结构、网络安全过程分析	2
		3、网络安全关键技术 4、网络安全产品简介	了解网络安全的关键技术；熟悉网络安全产品；掌握一种网络管理系统的使用方法	网络安全关键技术、网络安全产品简介	2
6	数据加密与数字签名技术	1、数据加密与数字签名基础 2、常见数据加密算法	掌握密码学的有关概念；了解常见的古典密码加密技术；理解对称加密算法和公开密钥算法的基本思想以及两者的区别。	数据加密与数字签名基础、常见数据加密算法	2

		3、使用 PGP 加密/解密数据 4、使用证书认证的方式访问 WEB 站点	掌握对称加密算法和公开密钥算法在网络安全中的具体应用；掌握数据签名技术、报文鉴别技术的实际应用。	使用 PGP 加密/解密数据、使用证书认证的方式访问 WEB 站点	4
7	防火墙、VPN 与入侵检测技术	1、防火墙的概念及基本功能 2、防火墙的分类和优缺点 3、常用软件防火墙配置：天网	了解防火墙的功能和分类；掌握防火墙的工作原理；掌握包过滤防火墙的工作原理以及优缺点	防火墙的概念及基本功能；防火墙的分类和优缺点；常用软件防火墙配置：天网	4
		4、常用软件防火墙配置：ISA 防火墙 5、入侵检测技术的概念和作用	了解防火墙的产品；掌握代理服务器的应用	常用软件防火墙配置：ISA 防火墙；入侵检测技术的概念和作用	4
		6、入侵检测技术的主要功能和工作原理 7、VPN 技术概述	了解入侵检测的概念；了解入侵检测技术的基本实现原理；掌握一种入侵检测技术的应用方法	入侵检测技术的主要功能和工作原理；；VPN 技术概述	4
		8、Windows 2003 server 下 VPN 配置与连接 9、网络安全评估	了解 VPN 的概念和发展；了解第二层隧道协议（L2F、PPTP 和 L2TP176）；掌握一种 VPN 实现技术的应用	Windows 2003 server 下 VPN 配置与连接；、网络安全评估	4
9	综合实训	网络安全评估	掌握网络安全评估的方法	网络安全评估报告	8

五、考核评定办法

改革传统的学生评价手段和方法，采用阶段性评价、过程性评价与目标评价相结合、项目评价、理论与实践一体化评价模式。关注评价的多元性，将课堂提问、学生作业、平时测验、项目考核、技能目标考核作为平时成绩，占总成绩的 60%，期末作品汇报占总成绩的 40%。

评价中应注意学生动手实践中分析问题、解决问题能力的考核，对在学习和应用上有创新的学生应予特别鼓励，全面综合评价学生能力。

六、教学建议

1. 教学条件

本课程中实践内容居多，要求课堂教学应在实训室上课，教师边讲解，学生

边实践。同时为了实验要求，需配备相应的网络设备和软件。如：交换机、路由器、防火墙、入侵检测系统、安全日志等；软件包括网络操作系统、抓包软件、网络探测工具等。

2.师资要求

本课程需要教师具有一定的基础理论知识、较广泛的专业知识以及相关学科的基本知识，以便解决教学、科研、实践工作中不断涌现出的新的问题；要求教师具备较高的教学能力，良好的知识传导能力和系统的教学设计能力；还要求教师具有同行业的实践经验或经历，与行业系统密切联系的沟通渠道，具备善于实践并指导学生实践的能力。

3.教学方法

本课程改变原有的“以教师为主，单一课堂教学”的传统教学模式，采用“以教师为主导，以学生为主体，以培养学生能力为本位，教学做一体化”的教学模式。

课堂教学采用四步教学法

在课堂教学中突出“项目导向”的设计理念，采用四步教学法，并对每单元教案都设计了目标说明、范例预览、知识讲解、课堂练习、要点总结、实验作业、单元测试八个教学环节。

第一步，任务导入：老师首先展示一些能够与本单元教学内容相关的企业实际的作品，然后从中选取具有代表性的作品作为本单元要完成的教学目标。通过展示范例的实际功效，让学生了解需要完成的项目与任务，并激发学生对新知识的学习兴趣。

第二步，讲解示范：以操作演示为主，对制作方法、操作步骤等进行示范演示，重点讲解关键步骤，便于学生掌握。

第三步，模仿操作：学生进行素材下载后，在课堂的上边学边练，按照教师的示范，自己动手模仿操作。

第四步，总结练习：教师对本单元能力涉及的重点难点进行归纳总结，并渗透相关的知识点，让学生理解新知识的应用机理，使学生了解实现的方法和原理。然后布置单元测试与实验作业，让学生通过练习与测试，掌握所学知识与技能，并激发学生的创新意识

通过四步教学法，将实操教学中的“赏——教——学——做——创“的教学环节有机融合在一起，提高学习的效率与质量。

在教学中采用项目教学与任务驱动相结合的方式，学生既可以接触到真实的项目，又可以将项目分成小的学习任务应用在教学中；除此之外还采取理论与实践相结合的教学方法，自主学习与小组合作学习相结合的教学方法。

4.教学资源的开发与利用

本课程是我系教师与神州数码有限公司合作，并编写了网络安全实训教程。教学中可以将整个网络安全工程分解为多个任务，选出典型案例作为教学的资源，按照实际工程实施过程制作。

5.评价标准

总分 100 分。其中考勤占 30%，平时作业 20%，结课作业占 50%

考情：全勤 30 分，旷缺课 1 次扣 1 分。

平时作业：全交的 20 分，少 1 次作业扣 1 分，学生自己可保存，随堂检查。

结课作业：满分 50 分

版面设计排列合理；文字排版设置，突出重点；颜色搭配合理得 40--50 分，中等得 30--40 分，差得 20--30 分。

七、推荐选用教材

选用教材:《计算机网络安全技术》主编：王其良 高敬瑜 出版时间：2008-5 北京大学出版社

参考用书：1.《网络安全技术》；作者：李拴保 等 ISBN 编号：9787302280248 出版时间：2012-5-1

2. 《网络信息安全技术》；周明全；西安电子科技大学出版社

参考文献（含课程网站）

1. http://www.nsdtarena.com/baidutgzt/dnpp/index.html?360

2. http://www.2cto.com/ebook/safe/

3. http://netsecurity.51cto.com/

4. http://soft.yesky.com/security/