《网络安全技术》
课程标准

适用于中等职业学校

目 录

一、课程性质

1. 课程定位

《网络安全技术》课程是一门新兴科学，属于计算机网络技术专业的专业课程，为学生的必修课。实施网络安全的首要工作就是要进行网络防范设置。深入细致的安全防范是成功阻止利用计算机网络犯罪的途径，缺乏安全防范的网络必然是不稳定的网络,其稳定性、扩展性、安全性、可管理性没有保证。

2. 课程任务

本课程在介绍计算机网路安全基础知识的基础上，深入细致的介绍了网络安全设置的方法和经验。目的是使学生通过学习网络安全的基础知识和基本操作，培养学生使用网络安全的方法解决学习和工作中实际问题的能力，并且配合必要的实验，和具体的网络安全案例，使学生顺利掌握网络安全的方法，提高网络安全的意识。

二、教材编写

教材编写体现了项目课程的特色与设计思想，教材内容应体现现有企事业单位的需求，充分体现学有所用。教材呈现方式应要图文并茂，文字表述规范、正确等。

1. 与前导课程的联系

《计算机网络技术》培养学生网络基础知识与技能。

《网络构建》培养学生局域网组建、广域网连接能力。

《网络管理》培养学生网络操作系统安装、设置及基本管理能力。

2. 与后续课程的联系

《数据恢复技术》《网络攻击与防范》提供网络安全基本知识与技能。

三、教材的选用

1. 教材选取的原则

教学内容要占教材篇幅的80%以上。

涉及的概念讲解深入浅出，并配有大量实例，以帮助学生对知识的理解。

理论偏多，为了学生以后高职或者入企打好基础。

2. 推荐教材

《网络安全技术》校本教材

《网络安全技术》 常彩虹，程延周 机械工业出版社

3. 参考的教学资料

《计算机网络基础与应用》 人民邮电出版社

四、课程目标

1. 总体目标

提升学生的网络安全素养，安装好杀毒软件和防火墙并及时更新；养成良好的上网习惯，培养学生的网络安全意识；定期对电脑进行清理杀毒，对电脑安装补丁和更新；学习网络安全法律法规等知识。

2. 三维目标

根据三年制中职计算机网络技术专业人才培养方案的要求，本课程应该达到以下教学目标。

课程目标	职业能力目标
知识目标	掌握网络安全的意义和特征
	掌握网络安全的主要技术
	掌握网络安全受到的威胁和解决对策
	了解网络安全法律法规
技能目标	具备网络安全需求分析能力
	具备网络安全规划设计能力，包括分析项目总体方案、网络安全规划
	具备网络安全防范的能力
	具备熟练使用相关网络安全工具软件的操作
	具备网络安全管理与维护的能力
素养目标	学习体验课堂理论知识在实际网络安全项目中的应用，积累项目实战经验
	培养良好职业道德，做合格的网络安全卫士
	培养自主学习能力、交流沟通能力、创新能力
	培养团队协作精神、基本的组织协调能力、责任心和服从意识
	加速由学生向员工的身份转变，增强就业能力和信心

五、教学模块

以教师指导下的活动体验、训练实操两条路径相互渗透，强调理实一体化，课内

与课外相结合，学业与职业相结合，考核过程与结果相结合。

第一章：网络安全的基本概念

第二章：防治计算机病毒和木马

第三章：网络应用中的密码技术

第四章：口令攻击与防御

第五章：网络安全产品的应用

第六章：网络安全的法律法规

第七章：综合安全方案设计与实施

模块	项目	教学内容	学时
第一章 网络安全的基本概念	网络安全的基本含义	1. 案例研讨	3
		2. 网络危害的原因	
		3. 网络安全的基本要求	
	网络安全现状及发展趋势	1. 网络安全形式的研讨	4
		2. 了解防护产品	
		网络安全防护整体框架	3
第二章 防治计算机病毒和木	杀毒软件的使用	1. 案例研讨	6
		2. 下载杀毒软件	
	防范网络病毒入侵	1. 预防措施	6
		2. 规范使用计算机网络的习惯	
		3. 使用专门技术防范网络病毒入侵。	
	了解计算机木马及清除	网络安全防病毒与木马的制定与实施	2
	预防木马侵入	1. 防范木马的措施	6
		2. 使用 360 预防木马	
		3. 使用 360 修复漏洞	
第三章 网络应用中的密码技术	数据加密技术	1. 密码的基本原理	6
		2. 代替密码和换位密码	
		3. 消息认证	
		4. 认证协议与数字签名	
		5. 实体认证	
	Windows 系统密码的保护	1、Windows 系统的口令设置与解除	4
		2、文件和文件夹的加密、解密操作	
		3、了解常用办公软件的加密、解密操作	
	电子邮件的加解密	1. 使用压缩软件加密电子邮件	4
		2. 使用 PGP 加密电子邮件	
		3. 利用 Outlook 加密邮件	
第四章 口令的攻击与防御	认识口令以及口令的破解方式	1、口令的概述	4
		2、口令的破解方式	
	口令破解工具	1. 口令破解的原理。。	4

		2.账号口令破解实验。	
	口令攻击与防御	1.强口令的选取方法。	4
		2.口令安全的管理策略	
	攻击与防御的实战演练	1.基于 Windows 的口令破解与防御	4
		2.WIFI 密码的破解与防御	
第五章 网络安全产品应用	常用的网络安全	1.案例研讨	4
		2. 防火墙的工作原理	
		3.入侵检测技术	
	使用软件防火墙	1.天网防火墙	4
		2.天网防火墙端口	
	使用硬件防火墙	1.配置硬件防火墙	4
		2.管理硬件防火墙	
		3.监控网络	
	了解入侵检测产品	1.瑞星入侵检测系统	4
		2. 天阗入侵检测系统	
第六章 网络安全的法律规范	网络安全管理的基本方法	1、安全事件的案例研讨	4
		2、制定网络安全管理制度	
		3、网络安全的管理工作方法	
		4、了解网络安全的审计工作	
	网络安全保护与评价	1.了解信息安全等级保护	4
		2 了解网络安全风险评估	
		3. 常用网络攻击手段与对策	
	网络应用中的法律规范	1.案例研讨	2
		2.网络应用中的法律责任	
	网络应用中的道德规范	1.侵权案例研讨	2
		2.基本道德规范	
第七章 综合安全方案设计与实施	综合安全方案设计与实施	1、综合安全方案设计基本原则	6
		2、安全策略设计与实施要点	
		3、综合安全方案文档撰写要求	
操作考核	要求：方案合理、操作熟练		2
	学时合计		96

六、课程改革思路

1.课程内容方面的改革

随着网络设备和网络协议的不断升级，将课程内容做了整合，进行了增减处理。

2.授课方式的改革

课堂采用信息化教学手段，利用教学软件进行教学操作过程，达到了更佳的教学

效果，使枯燥乏味的攻防过程变得生动而丰富。同时依托校园网建立的专业网络教学的教学资源库、电子课件、教案、在线联系等平台，为学生的学习提供了多种途径。

3.课时分配

课程内容由理论教学、实践教学两大部分组成，建议课程总学时为 96 学时。

七、课程理念

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,打破了传统的学科体系的模式,将《计算机网络基础》、《Windows 2003Server 服务器安全配置》、《计算机网络管理》、《Internet 安全设置》等学科内容按计算机高级网络安全管理员岗位的实际项目进行整合，按“理论+实践”要求设计。它体现了职业教育“以就业为导向，以能力为本位”的培养目标，不仅强调计算机网络管理维护岗位的实际要求，还强调学生个人适应劳动力市场的发展要求。

1.“工学结合”的理念

网络安全中的一些实际应用，以职业技能培养为重点，以项目为导向设计大量的应用实例。在教学过程中提出真实的有代表性的工作任务，教师分析任务需求，提出“解决方案”，然后教师详细讲解“任务实现”的操作步骤和方法，完成后进行“效果展示”，培养学生分析问题、解决问结合现代社会工作单位实际工作岗位中题的能力。

2.“任务驱动”的理念

从学校、企事业单位“信息化办公”的实际工作出发，培养目标选取了六个项目，按照“学习情境----提出任务---分析任务-----解决办法----操作过程-----效果展示”的过程，带领学生逐步完成任务，通过这些任务全面训练学生的计算机操作能力。以学习情境为基础，实施“理论—实践一体化”的课堂教学，融“教、学、做”为一体。

八、课程改革思路

1.课程内容方面的改革

随着网络设备和网络协议的不断升级，将课程内容做了整合，进行了增减处理。

2.授课方式的改革

课堂采用信息化教学手段，利用教学软件进行教学操作过程，可以达到更佳的教学效果，使枯燥乏味的攻防过程变得生动而丰富。同时依托校园网建立的专业网络教

学的教学资源库、电子课件、教案、在线联系等平台，为学生的学习提供了多种途径。

3.课时分配

课程内容由理论教学、实践教学两大部分组成，建议课程总学时为 96 学时，其中理论教学 64 学时，实训 32 学时，理论和实践教学的比例约为 2：1。

注：另建议在教学中安排 1 周左右的综合实训。

九、教学组织和方法

这门课程理论偏多，针对课程的培养目标和特点，教学的方式和手段需要灵活多样。以下是采取的教学手段:

1.理论教学应注重讲、练结合，利用多媒体教学方式可以将基础知识讲解、实例演示有机结合，提高授课效率。

2.为了发挥学生的主观能动性，提高学生的职业素质，教师不在课堂上讲授所有的知识要点，将一些简单的、雷同的内容分配给学生，要求他们以组为单位完成预习、实践、甚至上台给其他组讲解，并能回答其他同学的提问，最后由教师给予全面总结。

3.本课程重点在于培养学生的计算机网络安全基础知识，后续课程、实习、课程设计、毕业设计中应继续培养和提高学生的计算机网络安全设置的能力以达到教学计划对学生计算机网络安全的认识。

十、课程考核

1.考核评价方式

我们对网络工程师等岗位所需的职业能力进行分析，从中提炼出核心素质(沟通能力、团队合作、学习能力)、知识、技能作为主要考评的依据。

目前考评方式分为以下两部分：**(1)阶段性考评　(2)期末考评**

教师可采用纸质作业、电子作业、小组成果展示、课堂提问等多种形式在学习情境的全过程中实施评价。我们今后将通过技术手段逐步细化学习情境考评的内容，包括核心素质考评、基础知识考评和技能考评。教师将来在完成评价的同时还要为学生互评提供明确的、适合当前学习情境的评判标准。学生将可以在教师指导下对其他同学或小组的作品、成果等进行评价。每个学习情境的阶段性考评结束后要公开成绩明细，确保评定的透明、公正。

2.考核评价内容

考核评价内容主要包括:基本概念的理解程度，具体技能方法的掌握程度，相关法律法规的认知水平，工作方案设计实施能力，团队合作能力，工作态度(包括出勤)，工作效率(包括进度)，工作质量(失误率、正确率)等。

3.考核评价方法

(1)过程性考核

①平时出勤、作业、实训表现、实训报告等占20%

②平时实操测试占40%

(2)总结性考核

理论考核:占40%，考试成绩由三部分组成，平时成绩(作业、课堂学习的情况)、平时实践考核和期末理论考试成绩。即本课程成绩=平时表现成绩+实践考核成绩+期末理论成绩。

十一、改革与创新

1.加强校企合作，实行订单培养

根据人才培养目标和职业岗位的能力分析，建立以工作过程导向的课程体系，改革课程教学内容，理论教学和实践教学体系整体优化，对专业技能课和专业技能训练课以“突出、强化”为特色，加强针对性、实用性和先进性。

2.积极开展教学方法研究

根据高技能人才的培养要求，以突出培养学生职业能力为核心，积极开展教学方法研究，大胆改革，探讨混合学习模式，探索理论教学、实践教学、网络教学相结合的新模式。根据课程特点开展以项目导向的课程改革，探索游戏式、项目导向式等教学方法，创新教学机制，并不断总结经验，提高质量，逐步推广。同时，注意培养学生综合素质和职业道德。目前我们已经编写《计算机网络安全》实训指导书，并不断创新，实践出它的特色。