《网络安全与防护》省级精品课程

课程代码	0102210141	课程类别	专业课程
课程类型	理实一体课程	课程性质	必修课程
课程学分	4	课程学时	72
修读学期	第4学期	适用专业	计算机网络技术
合作开发企业	吉林中软吉大信息技术有限公司		
执笔人	迟恩宇、刘杰、方欣、郭成刚	审核人	迟恩宇

1. 课程定位与设计思路

1.1 课程定位

本课程是计算机网络技术专业专业的核心课程、专业必修课。本课程通过对企业实际网络安全防护需求的分析,培养学生利用相应软件对企业网络安全性分析、测试、评价的能力,通过企业网络安全管理典型工作任务的分析,培养学生网络安全的设计与实施能力,并逐步具备针对企业新的网络安全需求对企业网络安全策略进行改进、改造或重新设计的能力。

本课程与前修课程计算机网络基础及应用、网络服务器架设、网络组建与互联等课程相衔接,共同培养学生信息化基础设施建设、应用与管理能力;与后续课程毕业设计、顶岗实习相衔接,共同培养网络安全管理相关岗位技术技能。

1.2 设计思路

通过对本专业网络安全管理相关工作岗位分析,网络安全管理员是本专业学生的一个重要岗位之一,也是学生在专业技术领域得以继续发展的重要途径。课程主要是培养学生对网络安全项目的分析、实施和改进能力,为培养“网络安全管理员”服务,因此本课程在网络技术专业中处于非常重要的地位,是专业核心课程和必修课程。

网络安全管理员的工作涉及保护数据安全存贮与传输、防护企业园区网络免于攻击、检测发现入侵行为、对网络流量分析定位安全故障、实施网络及主机渗透攻击测试与加固防护、对网络进行冗余备份等可靠性设计以及安全管理技术综合应用等,是综合性较强的工作,通过对网络安全管理员岗位进一步调研,并经

过行业专家深入、细致、系统地分析，根据学生实际在岗位中要完成的任务，我们将教学内容设计了6个学习情境：

- ◆ 学习情境1-通过流量分析定位网络故障；
- ◆ 学习情境2-保护数据在公网上的传输；
- ◆ 学习情境3-对网络访问行为进行控制；
- ◆ 学习情境4-对入侵进行检测、审计与防护；
- ◆ 学习情境5-网络及主机渗透攻击测试与加固防护；
- ◆ 学习情境6-保护网络安全可靠运行的综合技术。

因此，本课程主要围绕这6个学习情境设计多个工作任务开展教学和训练。

本课程设置了6个学习情境，在真实的职业活动情境中使学生更好地获得职业能力，并获得理论认知水平的发展。因此，本课程打破了传统教学方式，整合工作任务中涉及的专业知识和技能，以真实的网络安全需求为载体来开展教学与训练，彻底改变了学与教的行为，同时通过实际工作任务的接触，让学生感受什么是实践，什么是实际工作任务，并体验企业实际岗位的要求。

本课程注重实际应用能力的培养，以岗位职业能力为依据，同时结合学生的认知特点和教学规律，采用递进与并列相结合来展现教学内容，例如：在保护数据在公网上的传输的学习情境中，遵循从简单到复杂的原则，从常见的加密保护数据工作任务入手，然后安排利用安全协议进行通信工作任务，最后是复杂的基于路由器进行VPN连接工作任务，由此循序渐进，所选项目具有典型性和覆盖性，通过这些工作任务的完成，使学生具备网络安全防护能力，并学会对典型工作任务的分析，为使学生具有广泛的实际适应能力，对不同工作任务进行扩展实现能力的迁移。

依据专业人才培养方案及课程体系整体规划，本课程的参考总学时为72学时，4.5学分。

2. 课程目标

根据网络工程专业面对的职业岗位群，将本课程培养的学生与企事业单位的网络安全管理与维护人员相对应。完成本课程的学习后，学生应该具备能对网络协议及流量进行分析解决网络中由于协议引起的故障的知识与能力、为数据提供有效保护措施的知识与能力、对网络安全进行控制减少攻击的知识与能力、对网

络安全事件进行记录检测及防护的知识与能力、对网络及主机渗透攻击测试与加固防护的知识与能力、对网络整体加以设计优化使网络更可靠的知识与能力。通过工作任务的设计,使学生能按企事业单位网络安全与管理人员的操作标准完成工作任务,在学习过程中注重学生职业素质的培养。通过本课程的学习,使本专业的学生具备从事网络安全管理员等相关工作岗位所必需的专业知识、专业技能,提升学生实际岗位的适应能力,提高学生的职业素质。具体如下:

2.1 知识目标

网络安全技术涉及的领域很广,不易讲求知识的全面性,因此课程在知识内容设计上选取当前企业应用技术,强调以点代面,设计6个学习情境,辐射当前企业实际应用的6个领域网络安全主流技术。每个学习情境在知识设计上能满足工作任务需要为目标,培养学生具备同一领域知识的学习方法与技巧,通过学生自主学习来扩展知识面,从而具备完成新的工作任务所需知识。互联网对网络专业的学生来说,是传授知识最好的老师,网络上有最新的知识、技术与教程。因此本课程在知识传授的目标是:不求传授给学生更多知识,但求传授给学生学会更多知识的方法。

- ◆ 具备网络协议底层结构与原理的知识与新的协议的学习方法;
- ◆ 学习数据加密和VPN技术相关知识以及对新知识的学习方法;
- ◆ 学习防火墙技术与原理和对新知识的学习方法;
- ◆ 学习入侵检测/防御技术与原理和对新知识的学习方法;
- ◆ 学习网络及主机渗透攻击测试与加固防护相关知识与概念和对新知识的学习方法;
- ◆ 学习保障网络安全可靠运行的相关技术与知识。

2.2 能力目标

课程以培养企事业单位园区网络的安全管理与防护人员为目标,能保护企事业单位网络及其中的路由器、交换机、防火墙、主机、服务器等网络设备与运行其中的网络协议和传输其上的数据的安全。不仅仅是技能有较高的要求,难点在学习技能的实训环境及条件上。因此课程根据多年积累将在工作任务设计上引入了很多的工具软件,使学生在一台主流配置的计算机上即可完成对实验设备及环境要求苛刻的网络安全工作任务,例如虚拟机软件、路由模拟软件、防火墙模拟软件

等，使学生不受实验条件的限制（当然也要适当安排学生接触真实的网络安全设备），课程的全部工作任务都可以在这样的实训条件下完成，学生可以在课内多人协作完成课内工作任务，并且教师注重培养学生学习新技能的方法与技巧，使学生在课外还可以独立学习拓展新的工作任务。这种设计对学生技能的培养提供了保障。当然课程的最终目标是要将学生培养成为具备解决企业安全防护需求方面技能的安全管理人员。

- ◆ 学会协议分析技术，能利用协议分析软件定位协议及流量引发的安全问题，具备实施有效的防护措施的方法与能力；
- ◆ 学会数据加密技术与 VPN 技术为数据提供保护，并能设计规划 VPN 方案，具备对数据机密性、完整性、合法性保护的方法与能力；
- ◆ 学会防火墙在网络中的设计、规划与部署，能对网络访问行为加以控制，具备利用防火墙保护网络的能力；
- ◆ 学会利用入侵检测/防御技术对网络行为进行审计与防护，并能部署入侵检测/防御方案；
- ◆ 学会网络及主机渗透攻击测试与加固防护的方法与能力，保障企业网络和主机不被渗透；
- ◆ 学会对网络部署不同层面的安全防护技术，保障网络安全可靠运行的相关技能与方法。

通过工作任务的完成使学生学会利用主流安全技术为企业网络中的主机系统及网络设备提供安全防护，对网络进行安全设计实施与维护，并能进行安全风险评估。针对每一项安全技术为学生设计工作任务，这些技术包括：协议分析技术、加密技术、认证技术、VPN 技术、防火墙技术、IDS/IPS 技术、加固防护技术及冗余备份技术等。会对安全需求选取特定的安全技术加以解决，能对相关任务的安全技术的资料进行搜集与整理，并能独立完成工作任务。独立获取和利用信息，也要通过团队或小组完成 6 个网络安全技术与实施学习情境中的每个工作任务，能够以准确的专业语言进行沟通。在充分考虑技术安全的前提下，自觉承担并完成工作任务。

2.3 素质目标

通过课程的学习来培养学生良好的劳动纪律观念、养成正确的工具设备使用

习惯、培养认真做事，细心做事的态度、培养团队协作意识、培养表述、回答等语言表达能力。作为一名企事业单位网络的安全管理与维护人员，道德品质是非常关键的，他能保护网络的安全，也可能会威胁到单位及其它员工的隐私。另外网络安全的防护工作涉及资金的投入，如何培养学生注重单位利益，经济、高质、高效地完成工作任务，是一名网络安全管理与维护人员必备的素质。另外一名高素质网络安全管理与维护人员要具备很强的沟通能力、协作能力和责任心，这样才能与其团队共同完成其服务对象提出的工作任务需求。最后由于将来工作岗位的性质决定了学生要具备吃苦精神和较高的专业技能，来保障工作任务高效高质完成。因此，对学生素质培养上，课程把“德、能、勤、技”当作是最好的排序。

2. 4 其他目标

通过课程的学习使学生具备一定的能力和社会能力，如处理问题的技巧、自主学习能力、团队协作能力、利用网络解决问题能力和与人沟通能力等。也可通过课程学习获得各厂商网络安全专项职业资格证书。目前安全知识急需普及，人们对此还没有足够的重视，引导学生通过课程学习对网络安全防护加以重视，并将网络安全知识加以普及，让身边使用计算机及网络人引起重视，避免由于网络安全造成不必要的损失。信息是有价值的，保护信息安全也就具有了价值，虽然网络安全与防护课程的主要目标不是为社会创造价值，但它能通过对学生的培养为社会价值提供保护。

3. 教学内容

本课程要培养的不是安全领域里的信息安全技术专家或专业人员，也不是安全产品研发与设计人员，是要培养能利用现有的安全技术和产品来维护企业内部网络安全、能排除网络安全故障、能为网络资源进行保护、能对网络进行安全防护的规划与设计、通过对网络中的关键设备及服务的合理配置保护网络安全可靠运行的企业网络安全管理人员。网络安全与防护课程不同于机电和软件类课程，也不同于本专业的网络组建与互联课程，网络安全技术是一个系统工程，它涉及多个领域的知识与技能，每一项知识与技能可以完成一项工作任务，解决特定的网络安全问题。所以本课程具有很强的服务性，即根据特定的需求去完成某项工作任务，所以适合于工作过程与任务的形式进行学习情境设计，更具有可实施性。

网络安全技术类课程的特点就是专业知识的深度与广度，一味地追求知识的全面性就会走入误区。恰当地选取和运用知识解决实际工作中的任务需求成为关键。强调以知识为引导，用知识解决实际问题，完成相应工作任务。针对企业网络中对不同网络安全防护方面的实际需求，课程设计了6个学习情境，每个学习情境内设置若干工作任务，将原本的章节知识分解到不同类型的工作任务需求中去。让学生对工作任务及需求加以完成，在完成工作任务中学习。使学与做相连，知识与工作需求相接，技术与能力相融，学生与员工身份相合。并通过学院网络中心的支持将学生引入到学院的网络安全管理与维护工作中去。

课程围绕企业在网络安全技术与实施的六个方面的需求设计了6个学习情境，每个情境下设置若干工作任务。其中主要内容是：

- ◆ 通过对网络协议及流量的深入分析理解网络协议的安全性，并能定位网络故障；
- ◆ 保护重要的企业数据或文件在公网上的传输的安全性，不被非法修改、破坏和查看；
- ◆ 合理选择与配置防火墙，保护企业内部网络的安全，并能对网络合理进行控制；
- ◆ 对网络中发生的入侵行为进行检测、审计与防护；
- ◆ 对内网主机服务器进行多角度的安全测试，并能根据渗透攻击测试结果对网络及主机进行加固；
- ◆ 合理设计网络，利用冗余备份技术保障网络可靠运行。

在课程内容设计上与吉林中软吉大信息技术有限公司合作一线专家合作，同时也聘请学院网络中心技术主管，为整体安全方案提供技术指导，并将其聘为本课程课外学习小组的兼职教师；聘请安全产品与技术集成商的网络安全高级工程师对课程进行技术指导；同时深入企业进行调研分析，对教学内容进行了充分的调查与分析以求设计上能满足多数企事业单位网络对网络安全防护的需求。

同时，将以上企业人员一起请进来对课程内容进行讨论，以研讨会的形式对设计的每一个工作任务的设计加以指导，并对全部内容进行排序。按这些企业实践人员成长过程对学习情境进行排序，并按他们完成具体工作任务的流程对每个工作任务流程加以分析、设计。具体如表1所示。

表1

学习情境描述

序号	学习情境	任务	知识	能力	素质	学时
1	通过流量分析定位网络故障	在本学习情境中设计了3个工作任务。任务1：利用 Packet Tracer 分析协议工作过程；任务2：基于 Sniffer Pro 进行协议、模拟攻击分析；任务3：利用深信服流量控制设备分析与定位网络故障。	TCP/IP 网络协议封装及数据结构；网络协议及原理的安全性分析。	学会协议分析的技术、工具软件及方法；初步会使用深信服流量控制设备。	对网络协议深层次的理解与认识，养成自学习惯。	12
2	保护数据在公网上的传输	在本学习情境中设计了7个工作任务。任务1：利用 PGP 实施非对称加密；任务2：利用数字证书保护通信；任务3：利用隧道技术连接企业与分支；任务4：基于 Windows 实现 VPN 连接；任务5：基于路由器实现分支与总部 VPN 连接；任务6：基于 INODE 实现出差员工通过 VPN 访问总部；任务7：对无线连接进行认证与数据加密保护。	对称与非对称加密原理；数字信封工作原理；数字签名实现原理；CA 数字证书实现原理；GRE 隧道封闭技术与原理；VPN 技术与公网传输数据的保护方法；无线技术。	能利用 PGP 软件实现非对称加密，来保护传输文件的机密性及真实性；能基于 Windows 服务器操作系统实现 CA 数字证书申请、颁发、撤销的全过程；能在路由器上配置 GRE 隧道；能基于主机或路由器配置 VPN 虚拟专用网络，来保护公网数据传输的安全性；会对无线网络进行简单的安全配置。	养成计算机网络安全使用的意识，加强对数据保护意义的认识。通过 VPN 实验养成团队协作能力。	24

3	对网络访问行为进行控制	<p>在本学习情境中设计了5个工作任务。任务1：基于路由器配置基本防护功能；任务2：软件防火墙配置保护主机与内部网络；任务3：基于思科路由器的IOS防火墙防护功能配置；任务4：基于天融信硬件防火墙对网络进行防护；任务5：基于深信服设备进行网络行为控制。</p>	<p>培养学生对防火墙功能、主要技术、体系结构与配置方法的理解；能完成基本的包过滤防护功能的设计。掌握防火墙软件的和硬件配置方法。</p>	<p>至少掌握一款软件和硬件防火墙的配置；能对网络访问控制、网络攻击等需求提供有效的安全措施，能为中小型企业网络提供有效、经济的防火方案。</p>	<p>养成严谨的工作态度，对潜在风险的评估能力。</p>	8
4	对入侵进行检测、审计与防护	<p>在本学习情境中设计了3个工作任务。任务1：基于Snort入侵检测功能配置；任务2：基于思科路由器的IOS入侵检测功能配置；任务3：基于深信服实施网络审计。</p>	<p>培养学生对入侵检测系统产品及功能、构成、分类、及部署方法的理解；能对入侵检测的术语加以解释，知道IDS的部署条件；对IDS的工作原理及各组件之间如何协同工作熟悉，能合理选择IDS的安放位置；理解网络审计。</p>	<p>能利用SNORT、思科路由器的IOS配置入侵检测功能，对特定的行为进行入侵检测并报警；会配置深信服的网络审计。</p>	<p>养成严谨的工作态度，及处理复杂问题的能力。</p>	4
5	网络及主机渗透攻击测试与加固防护	<p>在本学习情境中设计了2个任务，共计10个子任务。任务1：网络及主机渗透攻击测试；子任务1：</p>	<p>学会网络及主机渗透攻击测试的方法；</p>	<p>对基于主流操作系统的主机进行渗透</p>	<p>养成严谨的工作态度，及</p>	8

		主机扫描技术；子任务 2：远程控制技术；子任务 3：操作系统漏洞攻击；子任务 4：应用程序漏洞攻击；子任务 5：数据库漏洞攻击；任务 2：网络及主机加固防护；子任务 1：运用 NEUSS 扫描软件检测主机漏洞；子任务 2：主机基本防护与加固；子任务 3：病毒防护；子任务 4：系统漏洞防护与加固；子任务 5：服务及应用防护与加固。	正确理解网络及主机加固防护方法；学会常见黑客工具软件的使用方法。	攻击测试和加固防护；能正确安装和使用常见黑客工具软件；能综合利用各种工具软件对网络及主机进行安全测评，并能制定改进方案。	处理复杂问题的能力。	
6	保护网络安全可靠运行的综合技术	在本学习情境中设计了 6 个工作任务。任务 1：数据备份与恢复；任务 2：磁盘冗余配置与实现；任务 3：服务器冗余配置与实现；任务 4：网络冗余配置与实现；任务 5：AAA 实现认证、授权与审计配置与实现；任务 6：基于 SNMP 协议实现网络管理。在内容设计上考虑了对安全技术综合与补充，重点是对网络及数据可靠性的设计，任务的完成也主要是由学生实现。	学会数据备份与恢复的相关技术与方法；磁盘冗余技术 RAID 原理；网络与服务器高可靠性设计方法；AAA 技术原理；网络管理技术实现方法。	引导学生独立完成保障网络可靠运行的工作任务，并能独立进行实施；实现不同层面的网络可靠性设计；能为网络持续安全可靠运行提供新的解决方案。	养成严谨的工作态度，及处理复杂问题的能力。同时培养学生自学能力及独立解决问题的能力。	16

4. 实施建议

4.1 师资队伍

教学的专任主讲教师需由计算机、网络工程、通信工程与信息安全相关专业本科及以上学历人员组成。教学采用理论与实践“一体化”的教学模式，安排在专用的网络技术实训室进行，每个班安排 1 名专任主讲教师，可根据需求选择来自企业的实训指导教师。建议专任教师及兼职教师要具有一定的网络组建与互联课程的讲授经验或网络工程项目实施经验及网络安全产品调试或测试能力，并已经具备网络工程师认证。

4.2 教材及相关资源

本课程已经有配套教材，内容也与本课程标准相符，但还需要与企业人员一道研究教材内容的完善，目前教材于2015年1月由高等教育出版社正式版，并已经确定为国家“十二五”规划教材。教材由主讲教师和企业人员共同开发，要充分体现项目课程设计思想，以任务为载体实施教学，同时要考虑实训条件的可操作性。同时本课程相关教学资源已经在公网发布，为课程提供了电子课件、视频录像等网络资源，建议每一轮授课过程中进行不断完善。另外，可以推荐学生学习线上的一些企业开发的视频教学课程。

4.3 教学组织模式

(1) 课内理实一体，课外拓展学习

结合课程设计的6个情境中的每一个任务，学生以小组方式完成任务，任务的学习从知识引导、任务规划设计、任务实施的思路先知识学习再进行任务实训的方式开展课内教学。课外安排学生完成拓展任务及企业提供一在线教学资源。

(2) 充分利用虚拟仿真技术结合真实设备提高学生实践能力

为了能够高质量实现课程目标，要求网络实训室具备华三、华为及Cisco等厂商相应的交换机、路由器、防火墙、无线等网络及安全设备，同时每一台实验计算机中安装模拟软件HCL、eNSP及GNS等。网络安全实验由于其专业性较强，实验工具及软件很难实现统一。本课程及教材在设计过程中充分考虑了实践与工作的结合，并特别重视实践环境的设计，通过借助一些工具软件来完成情境的设计，即使只有一台计算机也可以完成复杂的安全实验。当然这就需要实训室配备一些工具软件：如VMware Workstation、Sniffer Pro、Wireshark以及网络多媒体教学软件等。

4.4 教学方法与手段

课程教学过程中应充分利用现代信息技术方法与手段，注重每一次教学任务的设计、充分调动学生学习的兴趣，加强学生对每一个任务的理解。建议采取的任务驱动、问题探究、引导文、小组协作等教学方法。充分利用虚拟仿真技术为学生课外自主学习提供方便，制作多媒体课件并利用多媒体技术实施教学。

4.5 教学考核与评价

课程在实施中应按任务对学生的知识理解、技能掌握进行考核与评价，遵循目标考核与评价、理论与实践考核与评价一体化原则。体现考核与评价的多元性，其中过程性考核与终结性考核的权重比建议为4:6。在考核过程中，突出强调技能的操作，充分体现综合应用能力，加强过程性考核。

(1) 形成性考核 (40%)

平时成绩 (20%)：学习态度 (10%) + 问题回答 (30%) + 出勤纪律等 (60%)，培养职业道德和素养。

实践成绩 (20%)：实践任务参与态度 (50%) + 实践任务完成情况 (50%)，具体分值见下表，培养职业素养和责任心。

(2) 期末考核 (60%)

期末考核以理论笔试为主。

表 2 考核评价表

评分内容	评价目标	评分标准	评价方式	评价分值
平时成绩	学习态度、问题回答、出勤纪律等	30%、40%、30%	过程性考核	20
实践成绩	态度与完成情况	25%、25%、50%	过程性考核	20
期末考核	笔试	100%	终结性考核	60
综合得分	100			

4.6 其他

课程在实施过程中应注意对仿真软件的利用，但也要结合企业实际工作任务的环境。

网络安全与防护课程组

2017 年 2 月