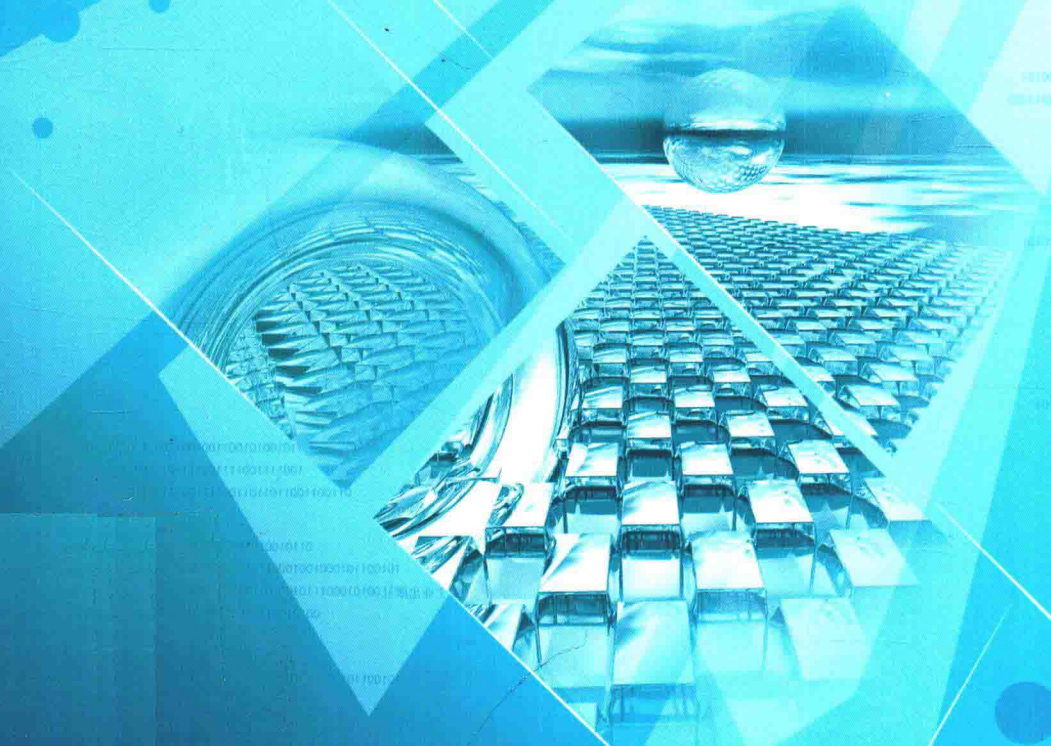
高职应用电子技术专业系列教材
国家骨干高职院校建设项目成果

计算机网络安全项目化教程

主 编◎丁久荣 张玉梅



西北工业大学出版社

计算机网络安全项目化教程

丁久荣　张玉梅　编

西北工业大学出版社

【内容简介】 计算机网络的出现改变了人们使用计算机的方式，也改变了人们的学习、工作和生活方式，“计算机网络安全技术”也已成为高职院校计算机及相关专业的重要必修课程。本书是根据高等职业教育的特点，基于“项目引导、任务驱动”的项目化教学方式编写而成的，体现“基于工作过程”“教、学、做”一体化的教学思想。

本书深入浅出，层次分明，实例丰富，通俗易懂，突出实用，可操作性强。特别适合于作为高职院校计算机类、通信类专业的教学用书，还可作为培训班的教材使用，同时，也可作为从事计算机网络技术应用领域的工程技术人员的参考书。

图书在版编目(CIP)数据

计算机网络安全项目化教程 / 丁久荣，张玉梅主编. —西安：西北工业大学出版社，2015.2

ISBN 978-7-5612-4312-1

Ⅰ. ①计… Ⅱ. ①丁… ②张… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第040230号

出版发行：西北工业大学出版社
通信地址：西安市友谊西路127号　　邮编：710072
电　　话：（029）88493844　88491757
网　　址：www.nwpup.com
印 刷 者：兴平市博闻印务有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：19.5
字　　数：462千字
版　　次：2015年4月第1版　　2015年4月第1次印刷
定　　价：36.00元

前　言

从1999年开始，高等学校连续进行了十几年的大规模扩招，大学教育也开始由精英教育转为大众化教育。随着教学对象、教学目标和教学环境的转变，传统的教学内容、教学方法和教学手段已不再适合高职教育的需要。

计算机网络的出现改变了人们使用计算机的方式，也改变了人们的学习、工作和生活方式，“计算机网络安全技术”也已成为高职院校计算机及相关专业的重要必修课程。本书是根据高等职业教育的特点，基于“项目引导、任务驱动”的项目化教学方式编写而成的，体现“基于工作过程”“教、学、做”一体化的教学思想，将全书内容划分为8章，共16个项目。具体内容包括网络安全概论、TCP/IP协议基础、网络入侵初步分析、网络入侵工具分类、网络安全策略、网络安全专题、网络设备安全知识和密码技术。本书具有以下特点。

(1)体现“项目引导、任务驱动”的教学特点。从实际应用出发，从工作过程出发，从项目出发，以企业组网、用网、管网为主线，采用“项目引导、任务驱动”的方式，通过“提出问题”→“分析问题”→“解决问题”→“拓展提高”四部曲展开。在宏观教学设计上突破以知识点层次递进为体系的传统模式，将职业工作过程系统化，以工作过程为参照系，按照工作过程来组织和讲解知识，培养学生的职业技能和职业素养。

(2)体现“教、学、做”合一的教学思想。以学到实用技能、提高职业能力为出发点，以“做”为中心，教和学都围绕着做，在学中做，在做中学，从而完成知识学习、技能训练和提高职业素养的教学目标。

(3)本书体例采用项目/任务形式。全书设有16个项目，每一个项目再明确若干任务。教学内容安排由易到难、由简单到复杂，层次推进，循序渐进。学生能够通过项目学习，完成相关知识的学习和技能的训练。每个项目均来自企业工程实践，具有典型性、实用性。

(4)项目/任务的内容体现趣味性、实用性和可操作性。趣味性可以使学生始终保持较高的学习兴趣和动力，实用性使学生能学以致用，可操作性保证每个项目/任务能顺利完成。本书的讲解力求贴近口语，让学生感到易学、乐学，在宽松环境中理解知识、掌握技能。

(5)紧跟行业技术发展。计算机网络安全技术发展很快,本书着力于当前主流技术和新技术的讲解,与行业联系密切,使所有内容紧跟行业技术的发展。

(6)课程学习与计算机技能考证相结合。项目的内容和难度符合高校计算机三级考试的要求。学生学习完本书内容后,可参加相应的计算机等级及相关认证考试。

(7)符合高职学生认知规律,有助于实现有效教学。本书打破传统的学科体系结构,将各知识点与操作技能恰当地融入各个项目(任务)中,突出现代职业教育的职业性和实践性,培养学生实践动手能力,适应高职学生的学习特点,在教学过程中注意情感交流,因材施教,调动学生的学习积极性,提高教学效果。

本书由丁久荣和张玉梅编写。其中,张玉梅负责编写第1章至第4章,丁久荣负责编写第5章至第8章。

由于水平有限,书中难免存在疏漏与不妥之处,敬请读者批评指正。

编　者

2014年12月

目　录

第 1 章　网络安全概论

项目一　网络安全概述

【项目要点】

☆预备知识

(1)日常生活中的网络安全知识;

(2)计算机病毒知识;

(3)操作系统的安全知识。

☆技能目标

(1)学习网络安全的概念;

(2)了解网络安全主要有哪些威胁;

(3)理解网络安全的体系结构;

(4)掌握网络安全管理原则。

【项目案例】

小孟在某一学院信息中心实习,常常遇到下面几种情况:下载一些有用的东西,常常遭受病毒的困扰;有时重要的文件莫名丢失;网上有些美丽的图片竟然有木马程序;有时候自己没有操作,但桌面的鼠标却在动;有时候明明 IP 地址正确,却上不了网? 小孟想系统学习网络安全的基本知识,他就请教网络中心的张主任。张主任说,我们的网络并不安全。如何保证上网的安全? 如何保证我们的信息安全? 如何防范恶意黑客的攻击? 这得从最基本的网络安全知识讲起,今天我就给你介绍一下网络安全的基本概念和网络安全的体系结构。

【知识点讲解】

1.1.1 网络安全的概念

随着 Internet 的发展，网络安全越来越成为一个敏感的话题。网络安全有很多基本的概念。我们先来简单地介绍一下。

1.1.1.1 网络安全威胁

目前，计算机互联网络面临的安全性威胁主要有以下几个方面。

(1)非授权访问和破坏(“黑客”攻击)。

非授权访问：没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。操作系统总不免存在这样那样的漏洞，一些人就利用系统的漏洞，进行网络攻击，其主要目标就是对系统数据的非法访问和破坏。“黑客”攻击已有十几年的历史，黑客活动几乎覆盖了所有的操作系统，包括 UNIX，Windows NT，VM，VMS 以及 MVS。

我们后面会对这一节的内容进行详细讨论。

(2)拒绝服务攻击(Denial Of Service Attack)。

一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(3)计算机病毒。

计算机病毒程序有着巨大的破坏性，其危害已被人们所认识。单机病毒就已经让人们“谈毒色变”了，而通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面都是单机病毒不能比拟的。

(4)特洛伊木马(Trojan Horse)。

特洛伊木马的名称来源于古希腊的历史故事。特洛伊木马程序一般是由编程人员编制，它提供了用户所不希望的功能，这些额外的功能往往是有害的。把预谋的有害的功能隐藏在公开的功能中，以掩盖其真实企图。

(5)破坏数据完整性。

破坏数据完整性指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重

要信息，可以修改网络上传输的数据，以及销毁网络上传输的数据，替代网络上传输的数据，重复播放某个分组序列，改变网络上传输的数据包的先后次序，使攻击者获益，以干扰用户的正常使用。

(6)蠕虫(Worms)。

蠕虫是一个或一组程序，可以从一台机器向另一台机器传播，它同病毒不一样，它不需要修改宿主程序就能传播。

(7)活板门(Trap Doors)。

活板门是为攻击者提供“后门”的一段非法的操作系统程序，这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。

(8)隐蔽通道。

隐蔽通道是一种允许违背合法的安全策略的方式进行操作系统进程间通信(IPC)的通道，它分为隐蔽存储通道和隐蔽时间通道，隐蔽通道的重要参数是带宽。

(9)信息泄露或丢失。

信息泄露或丢失指敏感数据在有意或无意中被泄露出去或丢失，它通常包括信息在传输中丢失或泄露(如“黑客”们利用电磁泄露或搭线窃听等方式截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等)，信息在存储介质中丢失或泄露，通过建立隐蔽隧道窃取敏感信息。

在所有的操作系统中，由于 Linux 系统的核心代码是公开的，这使其成为最易受攻击的目标。攻击者可能先设法登录到一台 UNIX 的主机上，通过操作系统的漏洞来取得特权，然后再以此为据点访问其余主机，这被称为“跳跃”。攻击者在到达目的主机之前往往会先经过几次这种跳跃。这样，即使被攻击网络发现了攻击者从何处发起攻击，管理人员也很难顺利找到他们的最初据点，而且他们在窃取某台主机的系统特权后，退出时会删掉系统日志，用户只要能登录到 Linux 系统上，就能相对容易地成为超级用户。所以，如何检测系统自身的漏洞，保障网络的安全，已成为一个日益紧迫的问题。

1.1.1.2 网络安全策略

在网络安全中，加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠的运行，将起到十分有效的作用。

安全策略是指在一个特定的环境里，为提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的一个重要组成部分，即：

威严的法律：安全的基础是社会法律、法规与手段，这是建立一套安全管理的标准和方法，即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

先进的技术：先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，根据安全服务的种类，选择相应的安全机制，然后集成先进的安全技术。

严格的管理：网络的安全管理策略包括确定安全管理等级和安全管理范围；制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。各网络使用机构、企业和单位应建立相关的信息安全管理办法，加强内部管理，建立

审计和跟踪体系，提高整体信息安全意识。

1.1.1.3 网络安全的五要素

安全包括五个基本要素：机密性、完整性、可用性、可控性与可审查性。

机密性：确保信息不暴露给未授权的实体或进程。

完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。

可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。

可控性：可以控制授权范围内的信息流向及行为方式。

可审查性：对出现的网络安全问题提供调查的依据和手段。

1.1.1.4 网络安全服务、机制与技术

安全服务：包括控制服务、数据机密性服务、数据完整性服务、对象认证服务、防抵赖服务。

安全机制：包括访问控制机制、加密机制、认证交换机制、数字签名机制、业务流分析机制、路由控制机制。

安全技术：包括防火墙技术、加密技术、鉴别技术、数字签名技术、审计监控技术、病毒防治技术。

在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术来实现的。应当指出，同一安全机制有时也可以用于实现不同的安全服务。

1.1.1.5 网络安全工作目的

安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理借施，完成以下任务：

(1)使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

(2)使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

(3)使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

(4)使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性。

(5)使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

1.1.2 网络安全体系结构

关于网络安全体系结构的划分有很多种。下面介绍一种比较有代表性的体系结构划分。

1.1.2.1 物理安全

物理安全是指用一些装置和应用程序来保护计算机硬件和存储介质的安全。比如在计算机下面安装将计算机固定在桌子上的安全托盘、硬盘震动保护器等。下面详细地谈一下物理安全。

物理安全非常重要,它负责保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故,以及人为操作失误、错误和各种计算机犯罪行为导致的破坏过程。它主要包括三个方面:

(1)环境安全。对系统所在环境的安全保护,如区域保护和灾难保护。参见国家标准 GB50173 -93《电子计算机机房设计规范》、国标 GB2887 -89《计算站场地技术条件》、GB9361 -88《计算站场地安全要求》。

(2)设备安全。主要包括设备的防盗、防毁、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及电源保护等。

(3)媒体安全。包括媒体数据的安全及媒体本身的安全。

显然,为保证信息网络系统的物理安全,除在网络规划和场地、环境等要求之外,还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多,在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示,给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散,通常在物理上采取一定的防护措施,来减少或干扰扩散出去的空间信号。这是政府、军队、金融机构在新建信息中心时的首要设置条件。

正常的防范措施主要体现在三个方面:

(1)对主机房及重要信息存储、收发部门进行屏蔽处理,即建设一个具有高效屏蔽效能的屏蔽室,用它来安装运行的主要设备,以防止磁鼓、磁带与高辐射设备等的信号外泄,为提高屏蔽室的效能,在屏蔽室与外界的各项联系、连接中均要采取相应的隔离措施和设计,如信号线、电话线、空调、消防控制线,以及通风管道、门的开关等。

(2)对本地网、局域网传输线路传导辐射的抑制,由于电缆传输辐射信息的不可避免性,现均采用了光缆传输的方式,大多数均在 Modem 出来的设备用光电转换接口,用光缆接出屏蔽室外进行传输。

(3)对终端设备辐射的措施。终端机,尤其是 CRT 显示器,由于上万伏高压电子流的作用,辐射有极强的信号外泄,但又因终端分散使用不宜集中采用屏蔽室的办法来防止,故现在的要求除在订购设备上尽量选取低辐射产品外,目前主要采取主动式的干扰设备如干扰机来破坏对应信息的窃取,个别重要的首脑或集中的终端也可考虑采用有窗子的装饰性屏蔽室,这样虽降低了部分屏蔽效能,但可大大改善工作环境,使人感觉像是在普通机房内一样工作。

1.1.2.2 网络安全

网络安全主要包括系统(主机、服务器)安全、网络运行安全、局域网和子网安全等几个方面。

(1)内外网隔离及访问控制系统。

在内部网与外部网之间,设置防火墙(包括分组过滤与应用代理)实现内外网的隔离与访问控制是保护内部网安全的最主要、最有效、最经济的措施之一。防火墙技术可根据防范的方式和侧重点的不同分为很多种类型,但总体来讲有两大类较为常用:分组过滤、应用代理。

1)分组过滤(Packet Filtering)。作用在网络层和传输层,它根据分组包的源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端,其余数据包则被从数据流中丢弃。

2)应用代理(Application Proxy)。也叫应用网关(Application Gateway),它作用在应用层,其特点是完全"阻隔"了网络通信流,通过对每种应用服务编制专门的代理程序,实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。无论何种类型防火墙,从总体上看,都应具有以下五大基本功能:

①过滤进、出网络的数据;

②管理进、出网络的访问行为;

③封堵某些禁止的业务;

④记录通过防火墙的信息内容和活动;

⑤对网络攻击的检测和告警。

应该强调的是,防火墙是整体安全防护体系的一个重要组成部分,而不是全部。因此必须将防火墙的安全保护融合到系统的整体安全策略中,才能实现真正的安全。

(2)内部网不同网络安全域的隔离及访问控制。

在这里,防火墙被用来隔离内部网络的一个网段与另一个网段。这样,就能防止影响因一个网段的问题而穿过整个网络传播。针对某些网络,在某些情况下,它的一些局域网的某个网段比另一个网段更受信任,或者某个网段比另一个更敏感。而在它们之间设置防火墙就可以限制局部网络安全问题对全局网络造成的影响。

(3)网络安全检测。

网络系统的安全性是网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节,如何最大限度地保证网络系统的安全,最有效的方法是定期对网络系统进行安全性分析,及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件,其功能是用实践性的方法扫描分析网络系统,检查报告系统存在的弱点和漏洞,建议补救措施和安全策略,达到增强网络安全性的目的。

(4)审计与监控。

审计是记录用户使用计算机网络系统进行所有活动的过程,它是提高安全性的重要工具。它不仅能够识别谁访问了系统,还能指出系统正被怎样地使用。对于确定是否有网络攻击的情况,审计信息对于确定问题和攻击源很重要。同时,系统事件的记录能够更迅速和系统地识别问题,并且它是后面阶段事故处理的重要依据。另外,通过对安全

事件的不断收集与积累，并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

(5)网络反病毒。

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消毒三种技术。

1)预防病毒技术。它通过自身常驻系统内存，优先获得系统的控制权。监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏，这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

2)检测病毒技术。它是通过计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

3)消毒技术。它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测；在工作站上使用防病毒芯片和对网络目录及文件设置访问权限等。

(6)网络备份系统。

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有场地内高速度、大容量自动的数据存储、备份与恢复；场地外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

一般的数据备份操作有三种：一是全盘备份，即将所有文件写入备份介质；二是增量备份，只备份那些上次备份之后更改过的文件，它是最有效的备份方法；三是差分备份，备份上次全盘备份之后更改过的所有文件，其优点是只需两组磁带就可恢复最后一次全盘备份的磁带和最后一次差分备份的磁带。在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。“热备份”是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。“热备份”的优点是投资大，但调用快，使用方便，在系统恢复中需要反复调试时更显优势。

“热备份”的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是将数据备份到另一个子系统中，通过主机系统与子系统