高职高专21世纪规划教材
GAOZHI GAOZHUAN 21 SHIJI GUIHUA JIAOCAI

网络安全与实训教程

■ 邓志华 朱庆 主编 ■
■ 胡长坤 李祥 副主编 ■

人民邮电出版社
POSTS & TELECOM PRESS

高职高专21世纪规划教材

网络安全与实训教程

邓志华　朱庆　主编

胡长坤　李祥　副主编

人民邮电出版社

图书在版编目（CIP）数据

网络安全与实训教程 / 邓志华，朱庆主编. —北京：人民邮电出版社，2005.4
高职高专 21 世纪规划教材

ISBN 7-115-13097-3

Ⅰ. 网… Ⅱ. ①邓…②朱… Ⅲ. 计算机网络－安全技术－高等学校：技术学校—教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 011298 号

内 容 提 要

本书围绕网络安全的定义、国际国内的安全标准以及常见的网络安全威胁与攻击等问题，从防病毒、防火墙、入侵检测、数据加密、身份认证及网络监控等多个方面对网络安全系统作了全面的分析和讨论；安排了 10 个详尽而具体的实际操作训练,从实用及操作的角度探讨了个人计算机的网络安全。

本书可作为高职高专院校相关专业的教材，也可供各行各业从事计算机网络应用和管理的读者阅读和参考。

高职高专 21 世纪规划教材

网络安全与实训教程

◆ 主　　编　邓志华　朱　庆
副 主 编　胡长坤　李　祥
策划编辑　滑　玉
执行编辑　祁　云

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn

读者热线　010-67170985
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：14.75
字数：346 千字　　2005 年 4 月第 1 版
印数：1－5 000 册　　2005 年 4 月北京第 1 次印刷

ISBN 7-115-13097-3/TP・4427

定价：20.00 元

编者的话

在过去的 10 年间，Internet 以前所未有的速度发展起来，它的开放性虽然使得信息能够高度共享和迅速传递，但同时也带来了系统入侵、泄密等网络安全问题。只要有网络存在，网络安全问题就会作为一个极其重要和极具威胁性的问题存在。

近几年来，有关计算机网络安全的书籍逐渐增多，有翻译国外的著作，也有国内专家自己编著的，这些书各有各的特点，为各层次读者提供了宝贵的资料，也指导着国内计算机网络安全技术的应用与研究。

本书的主要特点包含以下两个方面。

首先是通俗易懂。计算机网络的技术性很强，网络安全的技术也比较晦涩难懂，这可能是初学者的共同心理。本书根据高职高专学生的特点,紧紧抓住“入门”和“实用”这两个中心，以通俗的语言和清晰的图文叙述方式，向读者介绍计算机网络安全的基本理论、基本知识、常用技术和方法。

其次是注重实用。阅读本书，可使读者掌握计算机网络安全的基本概念，并了解设计和维护网络及其应用系统安全的基本手段和方法。本书在编写形式上注重介绍使用方法，突出应用的需求，尽量避开原理性的介绍和一些基本数学理论内容，力争反映网络安全技术的新发展，主要是想满足构造安全的网络应用系统的实际需要。

计算机应用技术和网络技术的发展是非常迅速的，为了使本书能反映较新的理论和技术，我们结合多年的教学积累,参阅了大量的资料，力图尽量靠近新知识、新技术的前沿。

全书共分两部分：基础篇与实训篇。本书的第 1 、3、5 章由朱庆编写，第 2 章由邓志华编写,第 4 章由胡长坤编写，实训篇由邓志华和朱庆编写,李祥老师、熊江华老师和刘伟老师参加了全书大纲的讨论和部分内容的编写，全书由邓志华负责总撰。

本书可作为高职高专院校相关专业的教材，也可供各行各业从事计算机网络应用和管理的读者阅读和参考。

笔者在向读者推荐本书的同时，也感到计算机网络安全技术的博大精深和迅速发展，因此对本书中的错误和疏漏之处，恳请读者和有关专家批评指正。

目　录

基　础　篇

实 训 篇

基　礎　篇

第 1 章

网络安全概述

网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题，也是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学和信息论等多种学科的边缘学科。当今，网络安全的重要性已有目共睹。

1.1 网络安全的概念

1.1.1 安全定义

从狭义的保护的角度来讲，网络安全是指计算机及其网络系统资源和信息资源不被未授权用户访问，即计算机、网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改或泄露，系统能连续、可靠、正常地运行，使网络服务不中断。

从广义来说，凡是涉及到计算机网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是计算机网络安全的研究领域。

1.1.2 安全标准

1. OSI 安全体系结构的安全技术标准

国际标准化组织（ISO）在它所制定的国际标准 ISO7498-2 中描述了 OSI（开放系统互连基本参考模型）安全体系结构的 5 种安全服务，各服务的名称及用途如表 1.1 所示。

表 1.1　　安 全 服 务

服　务	用　途
身份验证（Authentication）	身份验证是证明用户及服务器身份的过程
访问控制(Access control)	一旦用户身份被验证就发生访问控制，这个过程决定用户可以使用、浏览或改变哪些系统的资源
数据保密(Data confidentiality)	这项服务通常使用加密技术保护数据免于未授权的泄露，可避免被动威胁
数据完整性(Data integrity)	这项服务通过检验或维护信息的一致性，避免主动威胁
抗否认(Non-reputation)	否认是指否认参加全部或部分事务的能力。抗否认服务提供关于服务、过程或部分信息的起源证明或发送证明

2. 可信计算机评估标准（Trusted Computer System Evaluation Criteria，TCSEC）

在美国，国家计算机安全中心（NCSC）负责建立可信计算机产品的准则。NCSC 建立了可信计算机评估标准，TCSEC 指出了一些安全等级，被称作安全级别，它的范围从级别 A 到级别 D，其中 A 是最高级别。高级别在低级别的基础上提供进一步的安全保护。级别 A、

B 和 C 还分数字标明的子级别，各级别的名称及描述如表 1.2 所示。

表 1.2　　TCSEC 安全级别

级别	名　称	描　述	例　子
A1	可验证的安全设计	此级别要求严格的数学证明，证明系统不会危及安全	Honeywell SCOMP
B3	安全域机制	提供数据隐藏和分层，保护层与层之间的所有交互信息	Honeywell、Federal、Systems XTS-200
B2	结构化安全保护	支持硬件保护，内存区域被虚拟分段，并进行严格保护	XENIX、Honeywell MULTICS
B1	标号安全保护	除 C2 的保护级别外，把用户隔离成各个单元以提供进一步的保护	AT&T System V
C2	访问控制保护	以用户为单位的存储控制，广泛的审计、跟踪，对资源、数据、文件和进程提供系统级别的保护	Windows 2000、UNIX
C1	选择的安全保护	用户与数据分离，不区分用户群，以用户组为单位	早期的 UNIX
D	最小保护	无内在的安全保护	MS-DOS

3. 我国计算机安全等级划分与相关标准

对信息系统和安全产品的安全性评估事关国家安全和社会安全，任何国家不会轻易相信和接受由别的国家所作的评估结果。没有一个国家会把事关本国安全利益的信息安全产品和系统的安全可信性建立在别人的评估标准、评估体系和评估结果上。为保险起见，通常要通过本国标准的测试才被认为可靠。1989 年公安部在充分借鉴国际标准的前提下，开始设计和起草法律和标准，制定了《计算机信息系统安全保护等级划分准则》（以下简称为《准则》）的国家标准，并于 1999 年 9 月 13 日由国家质量技术监督局审查通过并正式批准发布，已于 2001 年 1 月 1 日执行。

《准则》将计算机信息系统安全保护能力划分了 5 个等级，计算机信息系统安全能力随着安全保护等级的增高，逐渐增强。高级别的安全要求是低级别要求的超集。各级别的描述如表 1.3 所示。

表 1.3　　《准则》的安全等级

等级	名　称	描　述
第一级	用户自主保护级	它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏
第二级	系统审计保护级	除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己行为的合法性负责
第三级	安全标记保护级	除具备前一级所有的安全保护功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制访问
第四级	结构化保护级	除具备前一级所有的安全保护功能外，还将安全保护机制划分为关键部分和非关键部分，对关键部分可直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力
第五级	访问验证保护级	除具备前一级所有的安全保护功能外，还特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动

1.2　常见的安全威胁与攻击

在讨论安全问题之前，我们先来看一下目前网络上存在着的一些安全威胁与攻击，了解一下攻击者（俗称黑客）一些常用的攻击方法。

网络上已经存在着无数的安全威胁与攻击，对于它们，也存在着不同的分类方法。在这

里我们将威胁分为两大类：意外威胁和故意威胁。

意外威胁是指由系统管理员和无知的用户因为没有预先思考或计划而引起的威胁。故意威胁是有企图的行为导致的结果，它是执行计划好的活动。故意威胁还可进一步分为：被动威胁和主动威胁。被动威胁包括在网络上使用探测器读取正在被发送的数据包，但不修改包内容或改变目标地址。数据的合法用户往往不知道这种活动的存在，这种类型的活动通常不会被系统记录。主动威胁包括的行为有：反复尝试访问和修改存储在操作系统中的信息；还包括生成若干的包用来阻塞网络。

常见的攻击方式有以下几种。

1.2.1 窃取机密攻击

窃取机密攻击是指未经授权的攻击者非法访问网络、窃取信息的情况，一般可以通过在不安全的传输通道上截取正在传输的信息或利用协议或网络的弱点来实现。

1.2.2 电子欺骗

电子欺骗是指攻击者伪造源于一个可信任地址的数据包以使机器信任另一台机器的电子攻击手段。它包含 IP 电子欺骗、ARP 电子欺骗和 DNS 电子欺骗 3 种类型。

IP 电子欺骗是攻击者攻克 Internet 防火墙系统的最常用的方法，也是许多其他攻击方法的基础。IP 电子欺骗技术就是通过伪造某台主机的 IP 地址，使得某台主机能够伪装成另外一台主机，而这台主机往往具有某种特权或被其他的主机所信任。

ARP 电子欺骗是一种更改 ARP Cache 的技术。Cache 中含有 IP 与物理地址的映射信息，如果攻击者更改了 ARP Cache 中的 IP 与物理地址连接，来自目标的数据包就能直接被发送到攻击者的物理地址。

DNS 电子欺骗是指攻击者危害 DNS 服务器并明确地更改主机名和 IP 地址映射表。当这些改变被写入 DNS 服务器上的转换表后，当一个客户机请示查询时，用户只能得到这个伪造的地址，该地址是一个由黑客输入的地址。因为网络上的主机都信任 DNS 服务器，所以一个被破坏的 DNS 服务器可以将客户引导到非法的服务器上，也可以欺骗服务器相信一个 IP 地址确实属于一个被信任客户。

1.2.3 拒绝服务攻击

拒绝服务攻击（Denil of Service，DOS）是一种很简单而又很有效的进攻方式。其主要目的是拒绝服务访问，破坏组织的正常运行，最终使系统的部分 Internet 连接和网络系统失效。DOS 的攻击方式很多，最基本的 DOS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。

分布式拒绝服务（Distributed Denial of Service，DOS），它是一种基于 DOS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，利用一批受控制的机器向一台机器发起进攻，具有很大的破坏性。

1.2.4 社会工程

社会工程是一种低技术含量的破坏网络安全的方法，但它其实是高级黑客技术的一种，

往往使看似严密防护的网络系统出现致命的突破口。社会工程往往被大家认为是黑客群体中最无赖的方法，但多年使用，仍是很有效果。这种技术是利用说服或欺骗的方式，让网络内部的人来提供必要的信息从而获得对信息系统的访问。攻击对象通常是一些安全意识薄弱的公司职员，攻击者可以采用与之交流或其他互动的方式实现。

1.2.5　恶意代码攻击

从 2003 年各国计算机犯罪和安全调查来看，恶意代码攻击是对信息系统最大的威胁，恶意代码包括计算机病毒、蠕虫病毒、特洛伊木马程序、移动代码及间谍软件等。

计算机病毒是一段附着在其他程序上的可以实现自我繁殖的程序代码，它可以在未经用户许可，甚至在用户不知道的情况下改变计算机的运行方式。计算机病毒必须满足两个条件：即能够自动执行和自我复制。

蠕虫病毒与传统病毒既有类似之处又有自身的特点。蠕虫病毒也具有传播性、隐蔽性及破坏性等传统病毒的共性，但蠕虫病毒不利用文件来寄存即可在系统之间复制自身的程序，这点与传统病毒不同。

特洛伊木马程序是具有欺骗性的文件。这种程序表面上是执行正常的操作，但实际上隐含着一些破坏性的指令。它与病毒的最大区别在于特洛伊木马程序并不像病毒那样复制自身。特洛伊木马程序包含能够在触发时导致数据丢失甚至被窃的恶意代码。要使特洛伊木马程序传播，必须在计算机上有效地启动这些程序。

移动代码指能够从主机传输到客户计算机上并且执行的代码。一般利用 VBA、Javascript 和类似的技术编写。大多数网站都使用移动代码来增强实用性、功能性和吸引力，但是黑客却通过它让用户的计算机感染病毒，偷窃私人信息，甚至重新格式化硬盘。移动代码与病毒的本质区别是，它并不复制自己，也不只是简单地破坏数据，而是盗窃数据或使系统瘫痪。

间谍软件是一种能够在用户不知情的情况下偷偷进行安装，安装后很难找到其踪影，并悄悄把截获的一些机密信息发送给第三者的软件。

1.3　近期网络安全发展趋势展望

系统漏洞问题、混合了黑客攻击和病毒特征于一体的网络攻击和以窃取用户机密数据为目的的威胁，将成为近期网络安全的 3 大发展趋势。

除了微软的漏洞外，目前，像思科路由器、Oracle 数据库、Linux 操作系统、移动通信系统以及很多特定的应用系统中，均存在着大量的漏洞。系统漏洞从出现到被利用之间的时间将会越来越短，直至零时间。2003 年 8 月份出现的“冲击波”病毒利用的是仅公布了 26 天的漏洞。控制系统中的漏洞已成为人们必须要考虑的首要问题。

目前的病毒早已不再是传统的病毒了，而是集黑客攻击和病毒特征于一体的网络攻击行为。针对这种混合性的威胁仅仅靠反病毒产品是无法对付的，必须增加防火墙、IDS 以及反病毒等综合防范措施。

此外，虽然近来的一些恶意代码只是阻塞网络，引起网络速度的极端下降，但是，一些以窃取用户机密数据的威胁开始在网上流行。

1.4 小　　结

本章介绍了网络安全的定义，国际国内的安全标准，以及常见的网络安全威胁与攻击，并对近期网络安全的发展趋势进行了预测。

总之，网络安全并不只有防病毒一个方面，其涵盖的领域包括防杀毒、防火墙、入侵检测、数字加密、网络监控、信息审计、灾难恢复和身份认证等多个方面。因此，网络安全系统作为一个整体的解决方案也应该由多个安全系统整合而成，多个单独的系统相互协作才能构成一个好的网络安全解决方案。

第 2 章

计算机病毒

计算机病毒（Computer Vires）其实是某些计算机高手利用计算机所固有的弱点编制的具有特殊功能指令的一种程序，是具有恶意攻击并破坏计算机软硬件的程序。这种程序和生物医学上的“病毒”一样，也有传染性和破坏性，并具有再生能力。它会自动地通过修改其他程序并把本身嵌入其他程序或者将自身复制到其他存储介质中，从而“感染”其他程序。在满足一定条件时，该程序可干扰计算机正常工作，搞乱或破坏已存储的信息，甚至引起整个计算机系统不能正常工作。本章将讨论计算机病毒的原理、发展趋势和防范措施。

2.1 计算机病毒的原理

2.1.1 计算机病毒的产生过程

计算机病毒的产生过程是：设计→传播→潜伏→触发→破坏。

（1）设计：计算机高手花费一段时间编写出可扩展的病毒指令程序。

（2）传播：编写者将含有病毒代码的程序放在 Internet 的 FTP 站、单位、学校或者盗版光盘中，进行广泛地传播。

（3）潜伏：设计完美的病毒可以潜伏很长的时间，不断地复制与传染，使其传染到更多的地方，造成巨大和无法挽回的损失。

（4）触发和破坏：当病毒发作的条件满足时，病毒就开始进行破坏，效果与病毒的能力有关。

2.1.2 计算机病毒的基本特征

一般说来，计算机病毒基本具有以下特性。

（1）传染性：对于绝大多数计算机病毒来讲，传染性是它的一个重要特性。病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机，病毒一旦进入计算机并得以执行，便会搜寻符合其传染条件的程序和存储介质，它通过修改别的程序，并将自己全部代码复制在外壳中，从而达到扩散的目的。

（2）隐蔽性：有些病毒是编程技巧极高的短小精悍的程序，一般只有几百个字节或 1～2KB，并巧妙地隐藏在正常程序或磁盘的隐蔽部位。若不经过代码分析，无法将病毒程序与正常程序区分开来。

（3）破坏性：凡是软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏。任何病毒只要侵入计算机，一旦发作，都会对系统及应用程序产生不同程度的破坏，轻者降

低计算机性能；重者可导致系统崩溃、破坏数据，造成无法挽回的损失。其表现主要在于：占用 CPU 时间和内存开销，从而造成进程堵塞；对数据或文件进行破坏；打乱屏幕的显示等。

（4）潜伏性：病毒在感染计算机后，一般不会马上发作，需要等一段时间，它可长期隐藏在计算机中，当满足其发挥条件时才发挥其破坏作用。几年前，大多数病毒主要通过软盘传播，但是，随着因特网的发展，现在的病毒正越来越多地通过网络进行传播。附着在电子邮件信息中的病毒，仅仅在几分钟内就可以侵染整个企业的信息系统，给企业造成巨大的损失。据美国国家计算机安全协会发布的统计资料可知道，已有超过 10 000 种病毒被辨认出来，而且每个月都在产生 200 种新型病毒。为了安全，大部分机构必须常规性地对付病毒的突然爆发。计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。

2.1.3 计算机病毒的产生背景

计算机病毒是计算机犯罪的一种新的衍化形式。计算机病毒是高技术犯罪，具有瞬时性、动态性和随机性，且不易取证，从而刺激了犯罪意识和犯罪活动。这是某些人恶作剧和报复心态在计算机应用领域的表现。

微型计算机的普及应用为计算机病毒的产生提供了必要环境。由于微型计算机的广泛普及，以及其硬件资料和操作系统的开放性，且基本上没有什么安全措施，使得能够透彻了解它内部结构的用户日益增多，对其存在的缺点和易攻击处也了解得越来越清楚，计算机软硬件产品的脆弱性是根本的技术原因。计算机是电子产品，数据从输入、存储、处理及输出等环节，易误入、篡改、丢失、作假和破坏；程序易被删除、改写；计算机软件设计的手工方式，效率低下且生产周期长；人们至今无法事先了解一个程序有没有错误，只能在运行中发现、修改错误，并且不知道还有多少错误和缺陷隐藏在其中。这些脆弱性就为病毒的侵入提供了方便。

2.1.4 计算机病毒的来源及危害性

计算机病毒是那些非法分子自己设计制造的，家用计算机感染病毒的途径主要有两个：一是使用带有病毒程序的盗版光盘或软盘；二是计算机上网时通过网络受到病毒攻击，比如病毒附在电子邮件里，打开电子邮件，病毒就感染计算机。

计算机病毒的来源包括以下几方面。

（1）计算机专业人员和业余爱好者的恶作剧、寻开心制造出的病毒，例如圆点一类的良性病毒。

（2）软件公司及用户为保护自己的软件不被非法复制而采取的报复性惩罚措施。因为他们发现对软件上锁，不如在其中藏有病毒对非法拷贝的打击大，这更加助长了各种病毒的传播。旨在攻击和摧毁计算机信息系统和计算机系统而制造的病毒。例如，1987 年底出现在以色列耶路撒冷西伯莱大学的犹太人病毒，就是雇员在工作中受挫或被辞退时故意制造的。它针对性强，破坏性大，产生于内部，防不胜防。

（3）用于研究或有益目的而设计的程序，由于某种原因失去控制或产生了意想不到的效果。现在有上万种病毒在网络上传播，其危害是极其恶劣的。病毒可以破坏软件系统，使某些软件运行缓慢，并占用系统资源，最终导致系统资源耗尽而死机；有的病毒甚至可以破坏硬件设备，如主板和硬盘等，造成巨大的经济损失。

对于计算机病毒，主要采取以“防”为主，以“治”为辅的方法，阻止病毒的侵入比病