MyDEC 专业教育机构

本书可作为本科、专科、高职高专院校计算机职业技能教育课程的教学用书

信息产业IT职业技术培训指定教材

网络安全

NS 实用教程

Network Security

总策划　MyDEC专业教育机构
审　定　信息产业部电子行业职业技能鉴定指导中心
主　编　崔英敏
副主编　陈　康　李纪标

中国青年出版社
中国青年电子出版社
http://www.21books.com　http://www.cgchina.com

信息产业IT职业技术培训指定教材

网络安全实用教程

崔英敏　主　编
陈　康　李纪标　副主编

中国青年出版社
中国青年电子出版社
http://www.21books.com http://www.cgchina.com

图书在版编目(CIP)数据

网络安全实用教程 / 崔英敏，李纪标，陈康编. —北京：中国青年出版社，2006

ISBN 7-5006-7028-1

Ⅰ.网… Ⅱ.①崔…②李…③陈… Ⅲ.计算机网络—安全技术—教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2006）第 091612 号

书　　名：网络安全实用教程

主　　编：崔英敏

副 主 编：陈　康　李纪标

出版发行：中国青年出版社

地址：北京市东四十二条 21 号　　邮政编码：100708

电话：（010）84015588　　传真：（010）64053266

印　　刷：中国农业出版社印刷厂

开　　本：787×1092　1/16　　印　　张：26.25

版　　次：2006 年 9 月北京第 1 版

印　　次：2006 年 9 月第 1 次印刷

书　　号：ISBN 7-5006-7028-1/TP・594

定　　价：38.00 元

网络安全实用教程编委会名单

前　言

网络安全技术作为信息安全技术的一个方面，在互联网络的大规模应用中发挥着越来越重要的作用，随着计算机网络的广泛使用和网络之间信息传输量的急剧增长，TCP/IP 的开放性和透明性等特点给网络安全造成了威胁。而现代操作系统日渐复杂也导致出现了越来越多的网络安全问题。

网络安全是一门技术交叉密集的学科，它综合利用了数学、物理、生物、通信技术和计算机技术等多种学科。从本质上讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受恶意或偶然的原因而遭到破坏、更改、泄露，能确保系统连续可靠地正常运行。

网络安全是一门发展迅速的年轻学科，网络信息安全领域的“攻”与“守”的高智商对抗不断丰富着网络信息安全技术，网络安全涉及的内容既有技术方面，也有管理方面。两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。现在，如何更加有效地保护重要的信息数据，提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

全书系统详细地介绍了网络安全基础知识、风险分析、安全策略、网络安全服务、网络安全处理、Internet 安全、防火墙技术、黑客技术、病毒技术、系统平台、安全需求分析，安全基础设施、安全与风险管理，以及网络安全实战等内容。

本书为信息产业 IT 职业技术培训指定教材，重点面向所有参加信息产业 IT 职业技术培训的人员，同时也适合大中专院校相关专业师生以及对网络安全应用技能有不同程度培训需求的人员阅读学习。

参加本书编写的有：张昱、贾治国、叶宏帅、李建芳、庞琨、张忠狮、赵学工、王大印、姜中华、刘在强、赵季卫、赵松岩、成宝栋、朱东锋、靳梅、张霄、李哲、王为等。由于时间仓促加之水平有限，书中难免会有差错及不足之处，敬请广大专家和读者给予批评指正。

最后，祝广大读者学有所成、学习愉快！

编　者

2006 年 7 月

目　录

第一篇　网络安全基础

第四篇 网络安全工程

第一篇　网络安全基础

第 1 章　网络安全概述

本章重点：

- 网络安全的基本概念
- TCP/IP 协议的网络安全问题
- 网络安全的基本属性
- 网络安全的体系结构
- 网络安全模型
- 网络安全处理的过程
- 密码学的基本概念

本章对网络安全的基本问题进行了介绍，使读者对网络安全的基本知识有一个初步的了解，为后续的学习打下基础。

1.1　网络安全简介

随着计算机和通信技术的发展，计算机网络已成为全球信息化基础设施的重要组成部分，它彻底改变了人们交换信息的方式，对科学、技术、文化、教育、生产的发展及现代人类生活质量的提高，都带来了深刻的影响。同时，计算机网络作为一把双刃剑，在推动人类进步的同时，也给国家安全和个人隐私带来了极大的威胁。计算机网络犯罪事件已屡见不鲜，且呈上升趋势。在人类进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求显得越来越迫切和重要，它不仅关系到战争的胜负、国家的安危、科技的进步、经济的发展，而且也关系到每个人的切身利益。

1.1.1　网络安全的背景

Internet 为人类交换信息，促进科学、技术、文化、教育、生产的发展，提高现代人的生活质量提供了极大的便利。据中国互联网络信息中心（China Internet Network Information Center，CNNIC）发布的“第十四次中国互联网络发展状况统计报告”显示，截止到 2004 年 6 月 30 日，我国上网用户总数为 8700 万，比 2003 年同期增长 27.9%，如图 1.1 所示，上网计算机达到 3630 万台。网络国际出口带宽增长飞速，总数达到 53.9G，比 2003 年同期增长 190.3%。CN 下注册的域名数、网站数分别达到 38 万和 62.7 万。报告中的主要数据说明，经过十年的发展取得了丰硕成果，我国互联网事业正在持续快速地发展，并在普及应用上进入崭新的多元化应用阶段。互联网的影响正逐步渗透到人们生产、生活、工作、学习的各个角落。

但随着 Internet 进一步国际化、社会化、开放化和个性化，Internet 在促进科学、技术、文化、教育发展，提高现代人的生活质量，为人类交换信息等提供方便的同时，也带来了一些不安全的阴影。由于计算机网络和信息系统的全球性、开放性、无缝连接性、共享性、动态性等特征，使得任何人都可以自由地接入，其中不乏恶意破坏者，对计算机网络的信息资源和软、硬件资源存在着已知的或潜在的各种威胁。例如，对银行、保险公司、证券公司等金融机构的网络犯罪；各企事业单位内部的商业秘密不胫而走；计算机网络病毒的泛滥与侵扰等。网络安全问题已经成为一个全世界人民必须面对的重要问题。

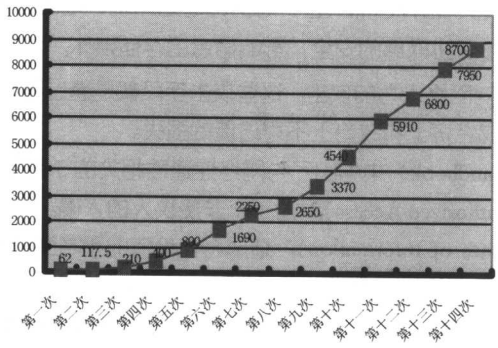

图 1.1 历次 CNNIC 互联网调查的网民数

1.1.2 网络安全的概念

1. 网络安全的定义

目前为止，还没有人针对网络安全给出一个统一的定义，但计算机科学界普遍存在以下一些观点。

（1）网络安全是指网络系统的硬件、软件及数据受到保护，不能因为偶然的或恶意的原因而遭到破坏、更改和泄漏，系统连续可靠正常地运行，网络服务不中断。

（2）网络安全从其本质上来讲就是网络上的信息安全，从广义来说，凡是涉及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网络安全所要研究的领域。

（3）网络安全是一个关系国家的安全、主权和社会稳定、民族文化的继承和发扬等的重要问题。网络安全正随着全球信息化步伐的加快而变得越来越重要。

（4）网络安全是一个综合、交叉的学科领域。它要利用数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果。

（5）网络安全研究的内容很多，它涉及安全体系结构、安全协议、密码理论、信息分析、安全监控、应急处理等内容，其中密码是网络安全的关键技术。

从不同的角度来看，网络安全有以下不同的含义。

（1）从用户的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

（2）从网络运行和管理者角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现后门、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

（3）对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，同时避免由于这类信息的泄密而对社会产生的危害，对国家造成的巨大经济损失。

（4）从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成障碍，必须对其进行控制。

2. 网络安全威胁

网络安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为自然威胁和人为威胁两类。

（1）自然威胁。可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些事件有时会直接威胁网络的安全，影响信息的存储媒体。

（2）人为威胁。也就是对网络人为的攻击。这些攻击手段都是通过寻找系统的弱点，以便达到破坏、欺骗、窃取数据等目的，造成经济上和政治上不可估量的损失。

在 RFC1244（Security Handbook）中指出了与网络连通性相关的 3 种不同类型的安全威胁。

（1）非授权访问（Unauthorized Access）。指一个非授权人的入侵。

（2）信息泄露（Disclosure of Information）。造成将有价值的和高度机密的信息泄露给无权访问该信息的人的所有问题。

（3）拒绝服务（Denial of Service）。使得系统难以或不可能继续执行任务的所有问题。

3. 网络安全研究的对象

计算机网络安全研究的对象主要包括保密性、安全协议设计和接入控制。

（1）保密性。为用户提供安全可靠的通信是计算机网络最为重要的任务。尽管计算机网络安全不仅局限于保密性，但是不能提供保密性的网络肯定是不安全的。网络的保密性机制除为用户提供通信保密之外，也是许多其他安全机制的基础，如访问控制中登录口令的设计、安全通信协议的设计以及数字签名的设计等，这些设计的实现都离不开密码机制。

（2）安全协议设计。计算机网络的安全协议是网络安全的一个重要方面。如为了防止假冒问题，就需要一种对等实体鉴别协议。如果网络通信协议存在通信安全上的缺陷，攻击者就可能不必攻破密码体制即可获得所需要的信息或服务。人们一直希望能够设计出安全的计算机网络系统，但不幸的是系统的安全性是不可判定的。目前对安全协议的设计，主要是针对具体的攻击设计安全的通信协议。协议安全性的保证通常有以下两种方法。

- 用形式证明一个协议是安全的。
- 用设计者的经验来判定协议的安全性。对复杂通信协议的安全性，主要采取找漏洞的分析方法，也可以开发一些人工智能工具来辅助分析。对于简单的协议，可以通过限制攻击者的操作来对一些特定情况进行形式化的证明，但这种方法有很大的局限性。

（3）接入控制。接入控制（Access Control）计算机网络的一大优点就是能够资源共享，用户可通过网络来共享系统提供的各种资源。但如果这种接入没有什么限制，将会带来许多安全问题。所以有必要对接入网络的权限加以控制，并规定每一个用户的接入权限。由于网络是一些地理上分散的计算机系统通过通信线路互相连接起来的一个复杂的系统，它的接入控制机制比操作系统的访问控制机制更复杂，尤其在高安全性级别的多级安全性（Multilevel Security）情况下更是如此。

1.1.3 网络安全级别

NCSC 领导着计算机和网络安全的研究工作，研制计算机安全技术标准，它在 1983 年提出了“可信计算机系统评测标准”（Trusted Computer System Evaluation Criteria，TCSEC），规定了安全计算机的基本准则。1987 年又发布了“可信网络说明”（Trusted Network Interpretation，TNI），规定了一个安全网络的基本准则，根据不同的安全强度要求，将网络分为 4 级安全模型。

注意：

NCSC（US National Computer Security Commission，美国国家计算机安全中心）的主要目标是促进可信计算机系统的推广。为了达成这一目标，NCSC 创建了一项标准，《国防部可信计算机系统评测标准（TCSEC）》，根据此标准对计算机系统进行评测。

在 TCSEC 标准中将计算机系统的安全分为了 4 级，依次为 D 级、C 级、B 级和 A 级，其中 A 级是安全性最高的一类，每一类都代表一个保护敏感信息的评判准则。在 C 和 B 中又分若干个子级，具体介绍如下。

（1）D 级：最小的保护。这是安全性最低的一级，不再分子级，指那些通过评测但达不到较高级别安全要求的系统。早期商用系统属于这一级，DOS 和 Windows 9x 系列操作系统都属于 D 级。

（2）C 级：无条件的保护。即“需要则知道”（need-to-known）的保护。C 级又分 C1 级和 C2 级两个子级。

- C1 级：自选安全保护系统。这是 C 级中安全性较低的一个子级，提供的安全策略是无条件的访问控制，具有识别与授权的责任。所有的用户都被分组；对于每个用户，必须登记后才能使用系统；系统必须记录每个用户的登记；系统必须对可能破坏自身的操作发出警告。早期的 UNIX 系统属于这一级。
- C2 级：有控制的存取保护。这是 C 级中安全性较高的一个子级，除了提供 C1 中的策略与责任外，还有访问保护和审计跟踪功能。所有的对象都有且仅有一个物主；对每个对象的访问操作，必须检验权限，不符合要求访问的权限，必须予以拒绝；有且仅有物主和物主指定的用户有更改权限；管理员可以获得对象的所有权，但不能归还；系统必须保证自身不能被管理员以外的用户改变；系统必须有能力对所有的操作进行记录，并且只有管理员和由管理员指定的用户可以访问该记录。SCO UNIX 和 Windows NT 及其后继版本 Windows 2000/XP/2003 属于 C2 级。

（3）B 级：属强制保护。要求系统在其生成的数据结构中带有标记，并要求提供对数据流的监视，B 级又分 3 个子级。

- B1 级：称为标志安全保护，是 B 级中的最低子级，除满足 C 级要求外，要求提供数据标记。不同的组成员不能访问对方创建的对象，但管理员许可的除外；管理员不能取得对象的所有权。Windows NT 的定制版本可达 B1 级要求。
- B2 级：结构安全保护，是 B 级的中间子级，除满足 B1 级要求外，要实行强制性的控制。所有的用户都被授予一个安全等级；安全等级较低的用户不能访问高等级用户创建的对象；银行的金融系统通常能达到 B2 级。
- B3 级：安全域保护，是 B 级中的最高子级，提供可信设备的管理和恢复，即使计算机崩溃，也不会泄露系统信息。

（4）A 级：经过验证的保护，是安全系统等级的最高级，这级系统可建立在具有结构、规范和信息流密闭的形式模型基础之上。A 级在 B2 级的基础上还增加了有系统的整体安全策略，这一策略一经建立便不能修改。A 级的安全性要求过高，目前商品化的操作系统没有达到 A 级要求的。

1.2 TCP/IP 协议

1.2.1 TCP/IP 协议简介

TCP/IP（Transmission Control Protocol/Internet Protocol，即传输控制协议/网际协议）是 Internet 最基本的协议。实际上，TCP/IP 协议不单单包括 TCP 协议和 IP 协议，而是一组网络通信协议的统称，它可以将由异构计算机组成的网络连接成为一个整体。目前覆盖范围最广的 Internet 就是建立在 TCP/IP 协议之上的计算机网络。除了 Internet 之外，TCP/IP 协议还是建立企业内联网（Intranet）的基础，是当今网络协议世界里当之无愧的盟主。

1.2.2 TCP/IP 参考模型

在 Internet 没有形成之前，各个地方已经建立了很多小型的网络，称为局域网，Internet 实际上就是将全球各地的局域网连接起来而形成的一个“网络之间的网”，即“网际网”。然而，在连接之前的各式各样的局域网中存在不同的网络结构和数据传输规则，将这些小网连接起来后各网之间要通过什么样的规则来传输数据呢？

这就像世界上有很多个国家，各个国家的人说各自的语言，世界上任意两个人要怎样才能互相沟通呢？如果全世界的人都能够说同一种语言（即世界语），这个问题不就解决了吗？TCP/IP 协议正是 Internet 上的“世界语”。TCP/IP 协议的开发工作始于 20 世纪 70 年代，是用于互联网的第一套协议。

TCP/IP 参考模型共有 4 层：应用层、传输层、Internet 层、网络层，如图 1.2 所示。

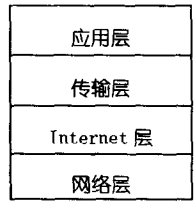

图 1.2 TCP/IP 参考模型

（1）网络层。全称为网络接口层。由于 TCP/IP 在设计时考虑到要与具体的物理传输媒体无关，因此在 TCP/IP 协议中并没有对数据链路层和物理层做出定义，而是将最底层称为网络层，或者网络接口层。它定义了将数据组成正确帧的规程和在网络中传输帧的规程，帧是指一串数据，它是数据在网络中传输的单位。

（2）Internet 层。也称作网际层，是整个体系结构的关键部分，其功能是使主机可以把分组发往任何网络并使分组独立地传向目标（可能经由不同的网络）。这些分组到达的顺序和发送的顺序可能不同，因此如果需要按顺序发送和接收时，高层必须对分组进行排序。

（3）传输层。传输层的功能是使源主机和目标主机上的对等实体可以进行会话，为端到端应用程序间提供通信。在计算机通信中常常是多种应用程序访问 Internet，为区别各个不同应用程序，传输层在每一分组中增加了识别信源和信宿应用程序的信息，对信息流进行格式化。为了可靠传输，在每一分组都附加校验码，以便信宿机接收分组时进行校验。

（4）应用层。在 TCP/IP 模型的最上层是应用层，它向用户提供一些常用的应用程序，如电子邮件、文件传输等，当然，用户可以根据自己的需要建立自己的专用程序。

1.2.3 TCP/IP 中的协议

1. IP 协议

IP 协议（Internet Protocol，即 Internet 协议），是 TCP/IP 协议族中的网络层数据报文服务，用于通过互联网络在主机之间传输数据包。IP 协议的另一个主要特性是拥塞控制。比起 TCP 所提供的拥塞控制，IP 提供的基本的拥塞控制功能是相对简单的。

IP 协议在 RFC791 中定义，该 RFC 定义了跨网络进行通信的一系列规则，同时还定义了允许 IP 数据包在网络上被路由到它们的目的地的寻址和控制信息。

RFC791 定义了两个基本规则，简要描述如下。

（1）一个无连接、尽力而为的跨网络数据包传递路由服务。

（2）提供数据包的分段和重组，使数据包能通过最大传输单元（MTU）不同的网络，这是基本的拥塞控制功能。

IP 协议提供了一个无连接、尽力而为的数据包传输系统，从逻辑上来看，这一服务具有 3 个重要的特点，通过它们可理解 IP 路由的行为。