CENGAGE Learning

CompTIA

国际高等教育精品教材引进项目

Network Security Principle and Application

网络安全原理与实务

◎ 主　编　邓春红
◎ 副主编　朱士明　庄城山　唐仪省

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

CENGAGE Learning
CompTIA
国际高等教育精品教材引进项目

网络安全原理与实务

Network Security Principle and Application

◎ 著　Mark Ciampa
◎ 主　编　邓春红
◎ 副主编　朱士明　庄城山　唐仪省
◎ 参　编　查　宇　孙　飞　周　浩
杨德超　孙　俊

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

Network Security Principle and Application, 2e
Mark Ciampa 著，邓春红　主编

EISBN：0619215666

Cengage Learning Asia Pte Ltd
5 Shenton Way, #01 - 01 UIC Building Singapore 068808

北京市版权局著作权合同登记号　图字 01 - 2008 - 3459 号

图书在版编目（CIP）数据

网络安全原理与实务/邓春红主编. —北京：北京理工大学出版社，2011.1
ISBN 978 - 7 - 5640 - 4196 - 0

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

中国版本图书馆 CIP 数据核字（2011）第 008468 号

出版发行／北京理工大学出版社
社　　址／北京市海淀区中关村南大街 5 号
邮　　编／100081
电　　话／(010)68914775(办公室)　68944990(批销中心)　68911084(读者服务部)
网　　址／http：// www. bitpress. com. cn
经　　销／全国各地新华书店
印　　刷／保定市中画美凯印刷有限公司
开　　本／787 毫米 ×1092 毫米　1/16
印　　张／17.25
字　　数／405 千字
版　　次／2011 年 1 月第 1 版　2011 年 1 月第 1 次印刷　责任编辑／高　芳
印　　数／1 ~ 2500 册　责任校对／王　丹
定　　价／42.00 元　责任印制／边心超

Preface

前言

随着网络高新技术的不断发展，社会经济建设与发展越来越依赖于计算机网络，与此同时，网络安全的威胁也日益严重。加快培养网络安全方面的应用型人才、广泛普及网络安全知识和掌握网络安全技术突显重要并迫在眉睫。本书的编写目的在于帮助学生和专业人士掌握实用网络和计算机安全方面的知识。

本书内容的编写与实践案例的选取，注重以能力为中心，以培养应用型和技能型人才为根本，遵循认识、实践、总结和提高这样一个认知过程，通过提供一个真正的交互式学习方式来帮助读者学习网络和计算机安全知识与技能。本书涵盖了计算机技术工业协会（CompTIA's）安全管理员（Security + ）认证的考试科目，以及全国信息安全技术水平考试（NCSE）项目内容。

为了帮助读者全面了解和掌握计算机和网络安全知识，本书特意设计了许多专题来加强读者的学习。

本章学习目标：每章开始都有本章概念的详细列表。本列表为读者快速介绍本章所涉及的概念，提供了有用的学习辅助。

图表：安全缺陷、攻击及防御的众多图片为读者直观地描述了安全组件、理论和概念。此外，众多表格也为读者提供实践和理论信息的详细资料和对比。

本章小结：每章结尾都有本章概念的总结。这些总结可以帮助读者复习本章的内容。

思考练习题：思考练习题包括了针对于本章内容的一系列复习问题。这些问题帮助读者检验和应用本章所学内容。回答这些问题可以加深对概念的理解，也对安全管理员考试有重要的帮助。

实践项目：虽然了解网络技术的理论知识是相当重要的，但也需要学习实践经验。因此，每章最后都为读者提供了若干个实践项目来了解实际安全软件和硬件的运行经验。这些

项目包含了 Windows 和 Linux 操作系统及网上下载的软件。

本教材由邓春红担任主编，并负责全书的统稿，由朱士明、唐仪省、庄城山担任副主编。具体分工是：查宇第 1 章、孙飞第 2 章、邓春红第 3 章，周浩第 4 章、朱士明第 5 章，唐仪省第 6 章、杨德超第 7 章，庄城山第 8、9 章，孙俊第 10 章。

在本书的编写过程中参考了相关文献和网站，在此向这些文献的作者和网站管理者深表感谢。由于作者水平有限，本书不足之处在所难免，欢迎广大读者批评指正。

编　者

Contents

目录

■ Part 1

第1章 网络安全基础

情境引入

根据中国互联网络信息中心《第25次中国互联网络发展状况统计报告》统计：截至2009年12月，中国网民已经达到3.84亿人。按照每户家庭有两个网民保守计算，即使按照每户家庭使用1台计算机计算，网民所使用的计算机数量近两亿。如此庞大的计算机数量及各种网络应用的快速发展所带来的网络安全问题也将与日俱增。媒体经常报道一些有关网络安全威胁的令人震惊的事件，而且更多不知名的黑客正在互联网上制造着破坏。

例如，信息安全顾问李明曾在一家拥有700台计算机的财务机构中做过网络接入调查。他发现该财务机构存在严重的安全问题：个人密码过于简单；Windows系统没有升级；运行一些没有必要的程序或服务器；允许用户远程连接到办公计算机而没有任何保护，他甚至发现网络入侵者曾用远程服务器监视网络管理员，并进而登录副主席的计算机。入侵者获得了管理员的登录信息（他的用户名、密码都是3个相同的字母）并进入了网络。

李明分析了网络日志文件，并建立了入侵者的档案。他发现，入侵者们已经进入银行网络系统一个多月了，每次入侵都用不同的IP地址，除节假日或银行休息日外，每次都停留少于一个小时的时间。通过这些IP地址，李明追踪到了在欧洲的同一个网络服务器提供商。

针对这些安全问题，李明向该财务机构职工提出了若干建议。李明建议，运行一个网络测试来检查安全漏洞；把700台计算机全部更新成Windows最新版本；关闭不必要的服务器；建立和强化有效的用户密码政策及严格的远程登录规则。该机构全部采纳并实施。

本章内容结构

本章内容结构如图1-0所示。

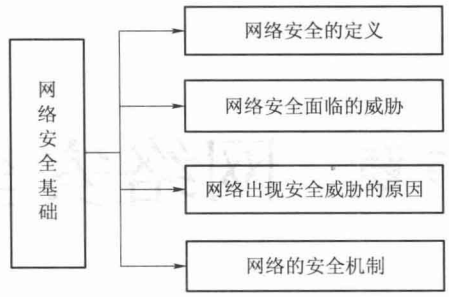

图 1-0　本章内容结构图

本章学习目标

◎ 明确信息安全面临的挑战；
◎ 掌握信息安全的定义；
◎ 了解信息安全的重要性；
◎ 掌握信息安全机制；
◎ 了解安全员认证考试；
◎ 描绘信息安全的职业规划。

1.1　网络安全所面临的挑战

不论国内还是国外，网络安全不断恶化的趋势都没有得到有效的遏制，它带给全球经济社会发展的负面影响越来越大。

我国发布的《2009 年网络安全报告》显示，2009 年网络威胁呈现多样化的特征。除传统的病毒、垃圾邮件外，危害更大的间谍软件、广告软件、网络钓鱼等纷纷加入到互联网安全破坏者的行列，成为威胁计算机网络安全的帮凶。尤其是间谍软件，其危害甚至超越传统病毒，已成为互联网安全最大的威胁。目前网络安全存在的主要威胁如图 1-1 所示。

当前网络安全事件的特点可归纳为以下几点：

（1）入侵者难以追踪。有经验的入侵者往往不直接攻击目标，而是利用所掌握的分散在不同网络运营商、不同国家或地区的跳板机发起攻击，使得对真正入侵者的追踪变得十分困难，需要大范围的多方协同配合。

（2）拒绝服务攻击频繁发生。入侵目标主机需要一定的技术和运气，因此很多攻击者选择使用分布式拒绝服务的攻击方法，严重干扰了目标的网络服务。由于这种攻击往往使用虚假的源地址，因此很难定位攻击者的位置。

（3）攻击者需要的技术水平逐渐降低但危害增大。由于在网络上很容易下载到攻击工

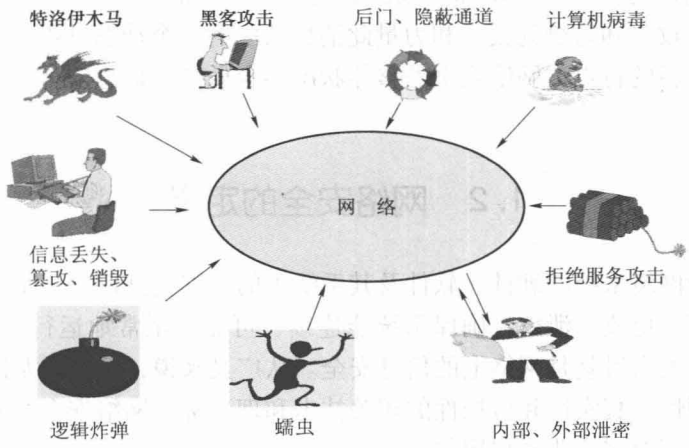

图 1-1 网络安全目前存在的威胁

具，而且一个新的操作系统漏洞被公布后，相应的攻击方法一般在两个月内就会被发布到互联网上。

（4）攻击手段更加灵活，联合攻击急剧增多。网络蠕虫越来越发展成为传统病毒、蠕虫和黑客攻击技术的结合体，不仅具有隐蔽性、传染性和破坏性，还具有不依赖于人为操作的自主攻击能力。新一代网络蠕虫的攻击能力更强，并且和黑客攻击、计算机病毒之间的界限越来越模糊，带来更为严重的多方面的危害。

（5）系统漏洞发现加快，攻击爆发时间变短。近年来，新的计算机系统安全漏洞不断被发现。网络攻击者热衷于攻击新发现的漏洞，在所有新攻击方法中，64% 的攻击针对一年之内发现的漏洞。2005 年，ZOTOB 爆发为漏洞利用过程创建了一个令人难以置信的记录——从漏洞发现到成功利用仅用了 5 天的时间，以至于很多网络管理员还来不及给系统打补丁。

（6）垃圾邮件问题严重。电子邮件的安全问题层出不穷，垃圾邮件和病毒的勾结更加重了对网络安全的威胁。在垃圾邮件中不仅有毫无用处的信息，还有病毒和恶意代码。从传播的范围和速度来说，垃圾邮件是蠕虫病毒的“最佳搭档”。调查显示，蠕虫病毒制造的邮件已经占全球电子邮件通信量的 20%～30%，造成了严重的网络拥塞。

（7）间谍软件、恶意软件威胁安全。间谍软件在用户不知情的情况下监控用户的网络连接，收集并发送有关用户访问的网址、IP 地址、用户计算机存储的信息。间谍软件一般隐藏在其他的应用软件中，用户在网上下载这些实用程序、游戏、媒体播放器和计费软件时，间谍软件就随之在用户的计算机中驻留，收集、监控并发送有关用户计算机的信息。另外，广告软件、密码窃听、恶意脚本程序等有害软件，在过去的几年里数量增长迅速。这些软件通过不同方式盗取用户的信息，并且威胁用户计算机的安全。

（8）无线网络、移动电话渐成安全重灾区。在无线网络中被传输的信息没有加密或者加密很弱，很容易被窃取、修改和插入，存在较严重的安全漏洞，因此无线网络正在成为黑客的理想目标。而无线网络的安全标准在保护无线网络安全方面的作用如何，还需要经过时间检验。另外，手机病毒利用普通短信、彩信、上网浏览、下载软件与铃声等方式传播，还

将攻击范围扩大到移动网关、WAP 服务器或其他的网络设备。

网络安全是在攻击和防御的技术和力量此消彼长中的一个动态过程。综上分析，当前的信息安全具有很多新的特点，网络安全的整体状况不容乐观，信息安全需要寻找更好的解决之道。

1.2 网络安全的定义

网络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，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。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的研究领域。

保密性：信息不泄露给非授权用户。

完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。

可用性：可被授权实体访问并按需求使用的特性。即当需要时能存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

可控性：对信息的传播及内容具有控制能力。

网络安全包括物理安全、逻辑安全、操作系统安全、联网安全。

1.2.1 物理安全

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括多方面的内容。

1. 防盗

像其他的物体一样，计算机也是偷窃者的目标，如盗走软盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员操作不慎，吸烟、乱扔烟头等，使充满易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。还可能使大规模集成电器损坏，这种损坏可能是在不知不觉间造成的。

4. 防雷击

随着科学技术的发展，电子信息设备的广泛应用，对现代闪电保护技术提出了更高、更新的要求，利用传统的常规避雷针，已不能满足微电子设备的要求，而且带来很多弊端。利

用引雷机理的传统避雷针防雷，不但增加雷击概率，而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。

雷击防范的主要措施是，根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点做分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多级层保护。

5. 防电磁泄露

电子计算机和其他电子设备一样，工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。例如，从20世纪80年代开始，美国市场上出现了一种符合TEMPEST标准的军用通信设备，并逐渐形成商品化、标准化生产。TEMPEST技术是综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及多个学科领域。

屏蔽是防电磁泄露的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽三种类型。

1.2.2 逻辑安全

计算机的逻辑安全需要用口令字、文件许可、查账等方法来实现。防止计算机黑客的入侵主要依赖计算机的逻辑安全。

可以限制登录的次数或对试探操作加上时间限制；可以用软件来保护存储在计算机文件中的信息，该软件限制了用户存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止；限制存取的另一种方式是通过硬件完成，在接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次登录或请求别人的文件。

1.2.3 操作系统安全

操作系统是计算机中最基本、最重要的软件。同一计算机中可以安装几种不同的操作系统。如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以便于防止他们相互干扰。例如，多数的多用户操作系统，不会允许一个用户删除属于另一个用户的文件，除非第二个用户明确地给予允许。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。通常，一个用户有一个账户。操作系统不允许一个用户修改由另一个账户产生的数据。

1.2.4 联网安全

联网的安全性只能通过以下两方面的安全服务来达到：

（1）访问控制服务。用来保护计算机和联网资源不被非授权使用。

（2）通信安全服务。用来认证数据机要性与完整性，以及各通信的可信赖性。例如，基于互联网或WWW的电子商务就必须依赖并广泛采用通信安全服务。

1.3 网络安全面临的威胁

计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。影响计算机