网络工程师实用技术培训教材

网络安全实用技术

叶丹　编著

清 华 大 学 出 版 社

（京）新登字 158 号

内 容 简 介

随着网络越来越深入到人们的生活和工作当中，网络安全变得越来越重要了，尤其是用于商业目的的内部网络。本书旨在介绍一些关于网络安全的基本技术。本书对于网络安全内容的覆盖面很广，有基本的网络安全定义、系统安全级别、网络安全的策略和基本原则、主机系统的安全、网络服务与应用的安全、网络系统与设备的安全等，并配以精致的图片和例子，每章后附有小结和习题。全书行文流畅、示例丰富、讲解清晰、介绍全面，必能让读者受益匪浅。

本书以实用为目的，使学员可以在很短的时间内，熟悉、了解计算机网络安全方面的理论和实用技术。在已经具有一定计算机网络基础知识的基础上，再通过学习本书，基本上可以满足一般的网络管理和网络安全方面的工作需要。

图书在版编目(CIP)数据

网络安全实用技术/叶丹编著. —北京：清华大学出版社，2002.10
（网络工程师实用技术培训教材）

ISBN 7-302-05793-1

I. **网**… II. **叶**… III. **计算机网络-安全技术** IV. TP393.08

中国版本图书馆 CIP 数据核字（2002）第 062473 号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
责任编辑：闫红梅
印 刷 者：北京市
发 行 者：新华书店总店北京发行所
开　　本：787×1092　1/16　**印张：**22.5　**字数：**543 **千字**
版　　次：2002 **年** 10 **月第** 1 **版**　　2002 **年** 10 **月第** 1 **次印刷**
书　　号：ISBN 7-302-05793-1/TP · 3426
印　　数：0001~5000
定　　价：33.00 **元**

序

信息技术飞速发展，IT 行业突飞猛进，我国的 IT 行业已经历了网络时代的萌芽期，正在逐渐壮大和成熟，目前正朝着高速、宽带、移动、多元化应用的方向发展。

IT 业的发展需要大量的高素质的技术人才，虽然我国的高校在不断扩大招生，每年都有相当数量的各种 IT 专业的毕业生走上工作岗位，然而对于迅速增长的 IT 人才的需求，仍然供不应求。而且大部分 IT 在职人员随着日新月异的技术发展，也越来越不能适应市场的需求，也需要进行进一步系统性的技术培训。

网络技术是 IT 领域的核心技术，是带动整个 IT 技术发展的龙头。近十余年来，我国的网络产业、网络基础设施建设以及网络应用获得迅速发展，但在我国具有一定基础知识和工程实践经验的基层网络规划、设计人员和网络管理人员的长期缺乏，制约了网络业乃至整个 IT 业进一步地高速发展。

如何进行网络系统的规则、方案设计和工程实施，如何进行网络的维护和管理，如何进行网络产品的开发，如何提供网络服务，这些问题都有待于拥有一定知识和实践经验的技术人员去解决。

通过调研，我们发现目前市场上有关网络技术书籍中的内容多偏于一般性或基础理论的论述，实践性不强，更缺乏建网与网络管理中实用技术的内容，致使建网及网管人员买不到适用的书籍。为了推广和发展我国的信息技术，为培养 IT 行业技术人才提供一条快捷之路，我们根据目前我国网络人才培训的需求，组成编委会，组织、策划并编写了这套丛书——《网络工程师实用技术培训教材》。

这套丛书包括了宽带 IP 网络、接入网、网络安全、网络管理、网络平台与服务、社区数字化系统、网络多媒体七方面内容，根据这些内容组织有关的人员分别编写了每本教材，组成这套丛书。

这套丛书的作者选自既有理论功底，又有实践经验的技术人员，且还包括有教学和培训经验的专家，并组成编委会，统一规划选题，并设专人负责每本教材的审稿工作。每本教材的大纲和目录均经过多次研讨。

全套书形成一个系统，内容上既包括原理与技术基础，又包括了网络各方面的实用技术，还有网络发展的一些热点技术；既适合于刚涉足网络工作的技术人员，更适合正在从事网络建设与管理的中级技术人员，对高级技术人员也有参考价值；也能作为高等院校有关网络课程的教材和参考用书。

张公忠

2002 年 7 月于清华园

编　委　会

前　言

安全性是目前每一位网络管理员都关心的一个主要问题。因特网目前正在以惊人的速度发展。在 20 世纪 90 年代初期，多数人如果不是通过报纸或杂志的报道，不会知道一些关于网络安全方面存在的薄弱环节。即使看了新闻报道，其中所针对的软件也已经是很老的版本，多数人已经不再使用了。而现在，成千上万的人可以在不到 1 小时之内，了解某种网络的弱点。

人们对问题的认识越清醒，也就越能够担负更多的责任。不仅软件公司希望弥补软件中的缺陷，网络管理员或负责安全的专家也希望修补自己的系统。任何在邮件群中订阅了邮件的人都能够与网络从业人员同时获得关于系统弱点的信息。这样，就更迫切需要在软件开发的时候，进行与安全保护相关的软件修改（因为我们已经没有多少回旋的余地）。

为此，本书将为网络管理员和具有一定的网络管理基础并对网络安全感兴趣的读者提供一份及时的“网络安全快餐”，不但可以解决上述问题，还可以帮助读者走得更远。网络安全是一个整体——人们不能只注意网络的某一个方面，而寄希望于所处的环境是安全的。通过这本书，读者可以获得如何制定网络安全策略和如何对网络进行安全管理的基本理论和有效方法。

本书从系统安全过程的角度出发，在介绍计算机网络基本概念的基础上详细阐述如何识别计算机网络中存在的危险，并根据系统安全中危险评估方法确定其安全登记，根据系统安全理论来设计安全策略，即设置 Internet 防火墙；并结合基于 UNIX、Windows NT 等操作系统的具体网络来设置防火墙，对网络进行安全管理。

本书将首先介绍网络安全的基本知识，以便于读者更好地理解后续内容；然后结合实例分析主机系统中的安全问题，提出制定安全策略的安全方案；其次介绍了各种网络服务与应用的安全，并提出一些防范措施；最后结合具体的防火墙技术介绍如何制定具体的安全策略和如何进行实际的网络安全管理。

本书内容如下：

第 1~2 章是网络安全基础，其中第 1 章简单介绍了网络安全的基础知识，着重介绍了 TCP/IP 参考模型和系统安全级别的问题；第 2 章则介绍了常用的增强网络安全的策略和方法。

第 3~5 章，讲述的是主机系统的安全。其中第 3 章简要讲解了 Windows NT 的安全知识，第 4 章则讲述了 UNIX 操作系统的安全机制的相关知识，第 5 章介绍了一般的系统攻击方法以及一些预防和补救的措施。

第 6~9 章，介绍了各种网络服务与应用的安全。其中第 6 章介绍的是 WWW 服务的安全性，第 7 章介绍的是域名系统（DNS）的安全性，第 8 章介绍的是电子邮件的安全性，第 9 章则扼要介绍了其他一些常见网络服务与应用的安全性。

第 10~12 章，重点讲述了网络系统的安全。其中第 10 章重点介绍了物理安全与人员安

全的问题，第 11 章重点介绍了防火墙技术，同时简单评述了一些目前常见的软硬件防火墙产品，最后我们介绍了密码学与 PKI 的有关知识以及信息安全技术在电子商务中的应用。

本书对象

本课程面向具有一定计算机和网络基础知识的网络管理人员、网络安全技术人员和网络技术爱好者。对书中的少量内容来说，一定的计算机软件开发经验可以帮助学员更深入地理解讲授的知识，但是完全没有计算机编程经验的学员同样可以顺利地学习本书所有的内容。

本书的技术基础

学习本课程要求学员具有一定的计算机使用经验和网络方面的基础知识，但是并不要求任何软件开发方面的知识和经验，当然具有一定的编程基础无疑可以帮助读者更深入地理解本书的某些内容。

教学要求、教学时数和参考进度建议

建议按照 15 天授课，4 学时/天，不需要上机辅导练习，但是学生需要独立完成每章后面的练习，教师应该在每次作业后讲解习题答案，有条件的培训中心可以适当安排一些专题的集体讨论时间。

作　者

2001 年 12 月于北京邮电大学

目　　录

第 1 章　网络安全概述

知识要点：

- **网络安全的概述；**
- **网络安全的含义，不同情况下网络安全所指的内容，网络安全的特征，网络安全关键技术；**
- **网络安全的重要性，它与我们国家建设的关系，网络安全问题的分析和防范方法；**
- **系统的安全级别及其描述，系统级别的分类标准；**
- **理解和掌握网络的结构和网络协议；**
- TCP/IP **各层的安全性和提升方法：网络层，应用层，传输层的安全性问题；**
- **使用** IPX/IP **网页的安全问题。**

教学目标：

本章是网络安全的引导篇，首先提出了网络安全的基本概念，使读者对于网络安全的特征和一些关键技术进行简单了解，并结合国家建设讲述网络安全的重要性和紧迫性。接下来掌握系统安全级别的分类，了解部分级别的划分方法和特点。然后介绍了网络模型的结构特点、内部协议，以及 TCP/IP **各层的安全性和提高安全性的方法。读者应注意结合** TCP/IP **和** OSI **模型的比较深入理解。最后我们介绍了使用** IPX/IP **网关的安全问题。总而言之，本章属于入门知识的一般性了解，但这也是今后深入学习网络安全的必要基础。**

1.1 网络安全基础知识

网络安全从其本质上来讲就是网络上的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从广义来说，凡是涉及到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。下面给出网络安全的一个通用定义：

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，系统连续可靠正常地运行，网络服务不中断。

1. 网络安全的含义

从用户（个人、企业等）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。

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“陷门”、病毒、非法存取、拒绝服务和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。

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危害，对国家造成巨大的经济损失。

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。

因此，网络安全在不同的环境和应用会得到不同的解释：

- 运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄露、干扰他人、受他人干扰。本质上是保护系统的合法操作和正常运行。
- 网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限，方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。
- 网络上信息传播安全，即信息传播后果的安全。包括信息过滤，不良信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用通信网络上大量自由传输的信息失控。本质上是维护道德、法则或国家利益。
- 网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在