信息安全技术

全国信息技术人才培养工程指定培训教材

网络操作系统安全

信息产业部电子教育中心　组编
祝晓光　编著

清华大学出版社

全国信息技术人才培养工程指定培训教材

网络操作系统安全

信息产业部电子教育中心　组编

祝晓光　编著

清华大学出版社

北　京

内 容 简 介

本书详细介绍了网络操作系统安全方面的有关内容，共分为 7 章，主要内容包括：网络操作系统安全的基本概念和安全机制，Windows 操作系统安全，Windows 2000 安全管理，Linux/UNIX 操作系统安全，Linux/UNIX 安全防范与增强，系统漏洞攻击与安全防范以及信息安全评测与法律法规。

本书结构清晰，内容实用，适合系统安全管理员或从事信息安全的技术人员阅读和参考。

图书在版编目(CIP)数据

网络操作系统安全/ 祝晓光编著.—北京：清华大学出版社，2004.12

全国信息技术人才培养工程指定培训教材

ISBN 7-302-09530-2

Ⅰ. 网… Ⅱ. 祝… Ⅲ. 计算机网络—操作系统(软件)—安全技术—技术培训—教材

Ⅳ. TP316.8

中国版本图书馆 CIP 数据核字(2004)第 094431 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：胡伟卷

文稿编辑：刘金喜

封面设计：王　永

版式设计：康　博

印 装 者：北京鑫海金澳胶印有限公司

发 行 者：新华书店总店北京发行所

开　　本：185×230　**印张**：20.75　**字数**：440 千字

版　　次：2004 年 12 月第 1 版　2004 年 12 月第1 次印刷

书　　号：ISBN 7-302-09530-2/TP・6631

印　　数：1～5000

定　　价：32.00 元

全国信息技术人才培养工程教材编委会

通讯地址：北京 4356 信箱教育中心

http://www.ceiaec.org/

丛书序

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化，以工业化促进信息化”，“优先发展信息产业，在经济和社会领域广泛应用信息技术”。明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势，电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息产业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写的同志们致以诚挚的感谢，并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。

王耀先

二〇〇四年四月十三日

前　言

进入 21 世纪以来，互联网和计算机技术以前所未有的速度迅猛发展，尽管网络和操作系统安全问题得到了各个领域的高度重视，但每年仍然会由于安全问题为全球造成巨大的损失。本书编写的目的在于让读者了解操作系统的功能和安全性设置，对黑客的攻击进行有效的阻挡和预防。Windows 操作系统是迄今桌面用户所使用最广泛的操作系统，UNIX 则以其高稳定性和高安全性的悠久历史占据了大份额的服务器市场。毫无疑问，这是本书以这两种操作系统为核心编写的主要原因。

本书第 1 章主要介绍操作系统的发展史和一些基本概念，第 2 章和第 3 章重点讲述 Windows 系统相关的安全管理、漏洞分析、攻击方法和安全性设置，包括 Windows 安全子系统、账户和文件系统安全及安全策略等。第 4 章和第 5 章介绍 UNIX 系统的工作原理、标识与账户安全，以及 UNIX 的后门查找和系统加固等内容。第 6 章则对典型的黑客攻击手段进行详细的剖析，让读者了解一次有效的攻击是如何发生的，应该如何阻止它。第 7 章介绍相关的系统安全评估标准和相关的法律法规知识。

有关操作系统安全的相关技术不应是一些网管和技术人员的“专利”，所有的计算机用户都有必要了解，因为一个大的网络往往由于一小部分人没有安全防范的意识和必备的基础知识而使整个网络受到严重影响。

本书详细介绍了操作系统的工作原理和关键性技术，并辅以大量的实例和 step by step 的方式来描述，对于系统安全管理员或从事信息安全的技术人员，本书有着极高的阅读和参考价值。

作　者

2004 年 6 月

目　录

第 1 章

概　述

随着各种操作系统不断的开发，服务器和台式机已起到了决策的功能性作用，并且越来越多的计算机和设备通过广域网或局域网相连。连接这些网络可通过多种介质和拓扑结构实现，如以太网和光纤等。尽管这些互连系统最主要的动机是信息和资源共享，但这种连接还是会导致系统及数据被攻击。因为 UNIX 和 Windows 操作系统已被广泛应用，所以它们更容易成为被攻击的目标。公司的 Intranet 和互联网易遭受到黑客的攻击，包括数据被越权访问或恶意修改及删除等。因此，需要在任何一个计算机和网络环境中实现坚固的安全策略和防护手段。

教学目标

通过本章的学习，读者应了解并掌握在 UNIX 和 Windows 环境下实现安全的必要性；清楚安全管理的范围和实施策略，并且能够识别确定 3 种安全级别的准则。

教学重点与难点

- 3 种安全级别的准则
- 实施安全系统的安全机制
- 安全的必要性
- 安全操作系统的重要性

1.1 安全的基本概念

1.1.1 安全的定义

国际标准化组织(ISO)早已对安全进行了定义，ISO7498-2 文献中提出安全就是最大程度地减少数据和资源被攻击的可能性。ISO 进一步定义了另一术语“资产”，就是存在于任一计算机系统的数据、应用程序和资源。ISO 所描述的漏洞是指能够被一些人对那些资产取得访问权限的任何事情。通常，漏洞是指系统的各种弱点，系统安装和操作时所未注意的方面。威胁即任何能对系统安全造成危害的活动。ISO7498-2 文献定义了对于所有等级的本地和远程系统及应用程序访问的主要安全服务，如表 1-1 所示。

表 1-1 安 全 服 务

服　务	描　述
认证	如何确定自己的身份，如利用一个带有密码的用户账号登录
访问控制	赋予用户对文件和目录的权限
数据保密性	保护系统或主机上的数据不被非认证的用户访问
数据完整性	提供类似网络中“劫持”这种手段的攻击的保护措施
不可否定性	当两个系统交互时，如果一方拒绝承认发生过这种交易，另一方就需要拿出证据来证明交易确实发生过。不可否定性也是提供防止欺骗的安全服务

安全是什么？

简单地说，在网络环境里的安全指的是一种能够识别和消除不安全因素的能力。安全的一般性定义也必须解决保护公司财产的需要，包括信息和物理设备(如计算机本身)。安全的想法也涉及适宜性和从属性概念。负责安全的任何一个人都必须决定谁在具体的设备上进行合适的操作，以及什么时候进行操作。当涉及公司安全的时候，什么是适宜的且在公司与公司之间是不同的，但是任何一个具有网络的公司都必须具有一个解决适宜性、从属性和物理安全问题的安全策略。

1.1.2 安全等级

UNIX 和 Windows NT 操作系统提供了很大范围的安全选项。它们允许用户在每个系统上定做符合所需要的安全尺度。通过本书用户将会利用多种方法来使 UNIX 或 Windows NT/2000 系统更加安全。尽管安全的实现是由很细微的工作组成的，不过为了讨论，我们将安全等级大致地分成了 3 类，即低、中、高 3 个级别。

表 1-2 安 全 等 级

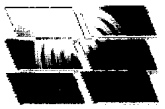
安全等级	适 用 于	实 施
低	计算机在一个安全的区域里； 计算机不包含和访问敏感信息	操作系统安全未应用； 使用防病毒软件； 防止计算机遭遇偷窃行为
中	计算机含有或访问公司数据； 计算机可被一人以上访问	能够审计； 使用文件级权限保护； 实施账号策略； 操作系统提供反措施和保护对策
高	计算机含有高度敏感或极有价值的数据； 计算机处在一个高风险的位置	操作系统为满足选择性功能被分成最小部分； 在操作系统上使用额外的更严格的策略和保护措施

1.1.3 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措施，完成以下任务：

- 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。
- 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。
- 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。

- 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。
- 使用审计、监控和防抵赖等安全机制，使攻击者、破坏者和抵赖者“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。



1.2 安全机制

根据 ISO 提出的观念，安全机制是一种技术、一些软件或实施一个或更多安全服务的过程。

ISO 把安全机制分成特殊的和普通的。一个特殊的安全机制是在同一时间只对一种安全服务上实施一种技术或软件。加密就是特殊安全机制的一个例子。尽管可以通过使用加密来保证数据的保密性、完整性和不可否定性，但实施在每种服务时却需要不同的加密技术。一般的安全机制都列出了在同一时间实施一个或多个安全服务的执行过程。特殊安全机制和普通安全机制不同的另一个要素是普通安全机制不能应用到 OSI 参考模型的任一层上。普通的安全机制包括以下方面。

- 信任的功能性：指任何加强现有机制的执行过程。例如，当升级 TCP/IP 堆栈或运行一些软件来加强 Novell、NT 或 UNIX 系统认证功能时，使用的就是普遍的机制。
- 事件检测：检查和报告本地或远程发生的事件。
- 审计跟踪：任何机制都允许你监视和记录你在网络上的活动。
- 安全恢复：对一些事件做出反应，包括对于已知漏洞创建短期和长期的解决方案，还包括对受危害系统的修复。

安全机制用于实施安全系统，主要存在两种形式的安全机制，即特殊安全机制和广泛安全机制。

1.2.1 特殊安全机制

某些技术可以实施在不同的级别来提供安全。这些技术如下。

- 加密机制：对流动在系统或网络之间的数据加行加密(或在本机的两个进程之间)。
- 数字签名机制：与加密极为相似，但另一个好处是检验发送者和内容是可信的，这种

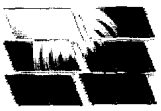
交易是由第三方来做的。

- 访问控制机制：通过简单的检查来确保在完成一个任务或程序时发送方和接收方是通过认证的。例如，网络允许一个有资格的用户在远程登录时访问资源。
- 数据完整性机制：一种确保每片数据的顺序、编号和时间戳的技术。
- 认证机制：就像用户级的这种简单密码验证方法一样。认证也可以应用到程序中，要求每次访问都要通过验证。
- 数据填充机制：额外的针对网络上进出的数据流，为了防止那些熟悉数据包的大小并以取得访问权限为目的的人对网络进行监视。例如，当一个新的登录会话建立后，在会话开始时主要有几个较小的数据包传输和接收。对这些包头进行分析可以提防那些网络监视者捕获下面一些数据包(因为较小的数据包和主字段都存在于包头中)。数据填充可以使所有的数据包看起来都是相同大小的，所以可避免某一个数据包被单独地摘出分析。

1.2.2 广泛安全机制

其他不受限于特殊级别的安全机制，有下列一些内容。

- 信任的功能性建立。某些服务或主机在各方面都是安全的而且可以信任。
- 安全标签的应用。指出数据敏感性的级别，例如，一个文件可以有附加的标签在读/写特权旁，只允许那些完全符合标签登录的账号才能访问。
- 审计跟踪经常在不同级别上使用，监视易受到入侵的活动和安全侵害。例如，UNIX的系统文件日志能够记录企图访问重要账号的事件。

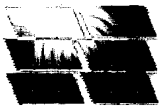


1.3 安全管理

为了协助管理者开发一种方案和策略，可以指定不同范围的安全管理，这些范围有：

- 安全管理，从事整个计算机环境和安全的管理。在此范围，策略已事先定义，服务提供商为顾问，选择特殊安全机制。这个部门还要负责审计和恢复的工作以及所有更深入的安全工作。
- 安全服务管理，包括那些实际的安全服务提供商。

- 安全机制管理，包括那些负责以下活动的人们。
  - ◊ 数据流量添充
  - ◊ 产生或分配数字签名
  - ◊ 加密的密钥
  - ◊ 数据完整性
  - ◊ 访问控制工作



1.4 安全操作系统的重要性

安全操作系统是信息安全的基础。操作系统作为各种安全技术的底层，信息交换都是通过操作系统提供的服务来实现的。当前，各种安全需求(如黑客通过操作系统的安全漏洞绕过防火墙等)普遍增长，对操作系统的安全性要求日益明显。各种应用程序要想获得运行的高可靠性和信息的完整性、机密性、可用性和可控性，必须依赖于操作系统提供的系统软件基础，任何脱离操作系统的应用软件的高安全性都是不可能的。计算机网络信息系统中，系统的安全性依赖于网络中各主机系统的安全性，而各主机系统的安全性是由其操作系统的安全性所决定的。没有安全的操作系统的支撑，安全保密性也就无从谈起，因此，操作系统的安全是计算机网络信息系统安全的基础。

1.5 安全操作系统的发展状况

安全操作系统的研究历程可以划分为以下 4 个时期。

- 开始时期：1967 年安全 Adept-50 项目的启动开始产生第 1 个安全操作理念。在这个时期，安全操作系统经历了从无到有的探索过程，安全操作系统的基本思想、理论、技术和方法逐步建立。
- 发展时期：始于 1983 年美国的 TCSEC[DOD1983]标准颁布之时，这个时期的特点是人们以 TCSEC 为蓝本研制安全操作系统。
- 多安全策略时期：始于 1993 年，这个时期的特点是人们超越 TCSEC 的范围，在安

全操作系统中实现多种安全策略。

- 动态策略时期：始于 1999 年，特点是使安全操作系统支持多种安全政策的动态变化，实现安全政策的多样性。

1.6 信息系统的脆弱性

随着我国国民经济与科学技术的发展，计算机信息技术在各个领域的应用越来越广泛，计算机信息系统的建立与运行大大提高了工作效率。然而，随着各种敏感机密信息和大量资金等重要计算机数据在计算机及其网络上的处理、传递、交换和存储，计算机信息系统的脆弱性越来越突出，一旦计算机信息系统在安全和可靠运行方面发生问题，将直接影响到经济建设和社会稳定，甚至会造成巨大的、无可挽回的损失。