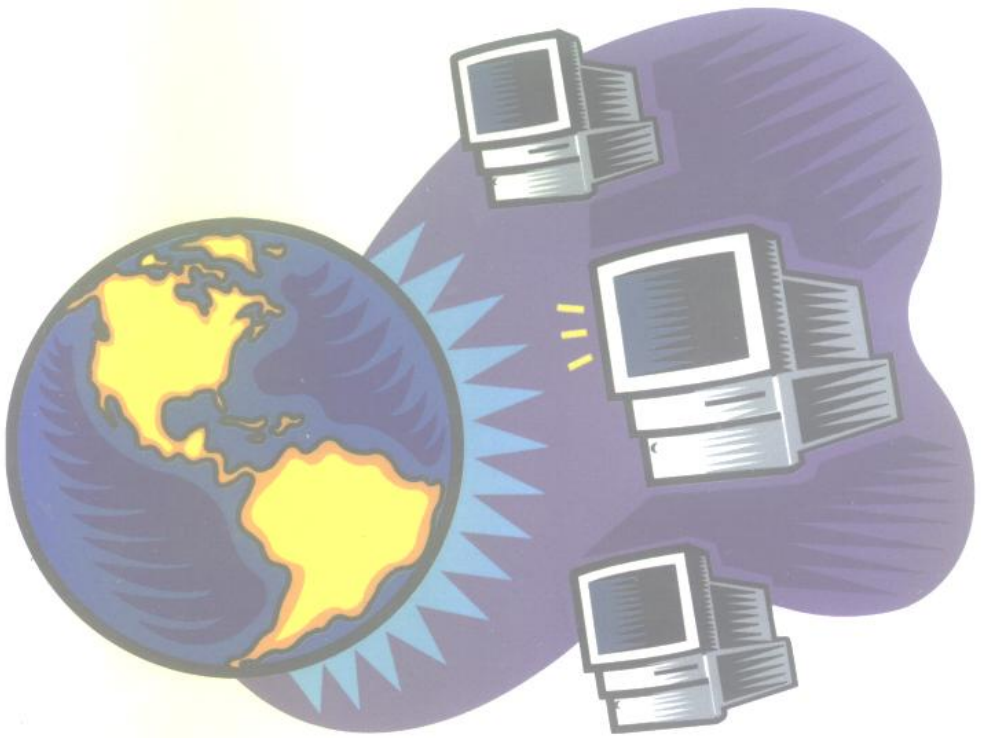
ICSA 国家信息中心 启明星辰公司 策划

Windows NT
系统安全实用技术

启明星辰公司
高鹏 严望佳 编著



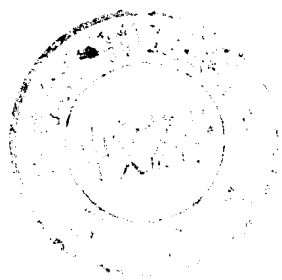
计算机网络安全系列丛书

清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机网络安全系列丛书

Windows NT
系统安全实用技术

启明星辰公司
高 鹏　严望佳　编著



清华大学出版社

(京)新登字 158 号

内 容 简 介

本书讲述 Windows NT 系统的有关网络和系统安全。书中首先介绍了与 Windows NT 安全有关的概念及相关问题，然后详细地介绍了 Windows NT 系统中存在的安全问题，重点介绍了 Windows NT 安全配置的具体方法。最后，介绍了 Windows NT 系统已知的安全漏洞及相应的解决方法。本书针对性强、技术实用，是帮助用户解决 Windows NT 安全问题的不可多得的好书。

图书在版编目(CIP)数据

Windows NT 系统安全实用技术 / 高鹏，严望佳编著.-北京：清华大学出版社，1999
(计算机网络安全系列丛书)
ISBN 7-302-03576-8

Ⅰ.W… Ⅱ.①高… ②严… Ⅲ.计算机网络-操作系统，WindowsNT Ⅳ.TP393

中国版本图书馆 CIP 数据核字 (1999) 第 19504 号

出版者：清华大学出版社(北京清华大学校内，邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者：北京市清华园胶印厂
发行者：新华书店总店北京发行所
开　本：787×1092 1/16　**印张**：12.5　**字数**：222 千字
版　次：1999 年 6 月第 1 版　1999 年 10 月第 2 次印刷
书　号：ISBN 7-302-03576-8/TP・1969
印　数：5001～11000
定　价：27.00 元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击，同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的账号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省账户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 debug、wizard 和 pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

前　言

Windows NT 越来越受欢迎。因特网上采用 Windows NT 平台作为服务器的站点越来越多，同时，众多企业已经采用 Windows NT 平台作为企业计算和企业内部网(Intranet)的解决方案的基础。

与网络连接，尤其是与因特网连接，就不得不考虑到系统的安全问题。作为新一代操作系统的Windows NT，在系统的安全性方面远远超过了Windows 95和 DOS 等操作系统，可以与 UNIX 系统媲美。但是，与 UNIX 系统一样，Windows NT 也存在着不少的安全漏洞。如果对这些漏洞不了解，不采取相应的对策，就会使自己的系统完全暴露在入侵者的入侵范围之内，随时有可能遭受系统攻击。因此，在使用 Windows NT 操作系统时，一定要对系统的安全性有一定的了解，这样才不会或能更少地遭受入侵者的攻击。

本书是专门针对 Windows NT 系统的有关网络和系统安全的书，它侧重并深入地介绍一些内容，使读者在读了之后，感觉有收获。

本书的实用性非常强，它面向对 Windows 95/Windows NT 稍有了解但对安全性不很清楚的用户。各层次、各水平的读者都可以从本书中获取有关 Windows NT 安全的重要信息。

根据本书介绍的方法配置自己的 Windows NT 系统，一定会更加安全、有效。

本书导读

本书可以分为三个部分：

第一部分介绍与 Windows NT 有关的安全概念、基础知识和安全策略等。

第二部分介绍 Windows NT 安全的具体配置方法，这是本书的重点。读者在读完本部分后就应该能够配置出相当安全的 Windows NT 系统环境。

第三部分介绍 Windows NT 系统已知的安全漏洞，并根据书中介绍的解决方法除掉这些漏洞。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目　录

第一章
安全基础

随着社会信息化程度的日益提高，人们越来越依赖于计算机来完成各种事务。从日常文档处理到商业交易事务处理，从简单的数学计算到航天、导弹等高科技技术，计算机都在其中发挥着关键作用。无论从应用的深度还是广度，其他任何工具都无法和它相比。计算机已经并将进一步影响人们生活的各个方面。

在计算机不断地深入到人类活动的过程中，它带来的安全问题同时也显而易见。由于安全性而引发的问题，像黑客入侵盗取重要信息等，已经严重影响了计算机系统正常地发挥作用，因此人门更加关注如何增强计算机系统的安全性。

操作系统是计算机系统中最重要的软件系统，在保证系统安全中具有重要的作用。微软公司的新一代操作系统——Windows NT 具有很高的安全性能，在 Windows NT 最初的设计计划书中就已包括安全性并将其渗透在整个操作系统中。

本章主要介绍 Windows NT 安全的基本概念和基础原理，旨在使读者对它有一个基本的认识和把握。

第 1 节简述 Windows NT 的安全框架。

第 2 节从 Windows NT 的体系结构角度简述它的安全子系统及其构成。

第 3 节介绍安全子系统如何在登录、访问控制和安全措施中发挥作用。

第 4 节介绍美国国防部 C2 级安全标准以及 Windows NT 如何达到这个标准。

第5节简要说明安全基础的问题，为管理员制订相应的安全政策提供依据。

1.1 安全基础

下面介绍 Windows NT 的安全基础。

设计 Windows NT 的目的是为了帮助机构完善它们的安全策略。这些策略详细说明了该机构对访问控制、信息保护及审计的要求。用 Windows NT 来配置网络，使用户能够按需要知道的部门或用户群来分类信息并控制“外来者”的访问。同时，Windows NT 还使得人们能够将网络和有组织的资源作为对象组来进行管理，并改善访问控制和身份确认的安全措施。

既然 Windows NT 可以用来增强系统的安全，是不是就可以不必担心别人来破坏自己的系统了呢？回答是否定的。因为操作系统本身并不能够自己解