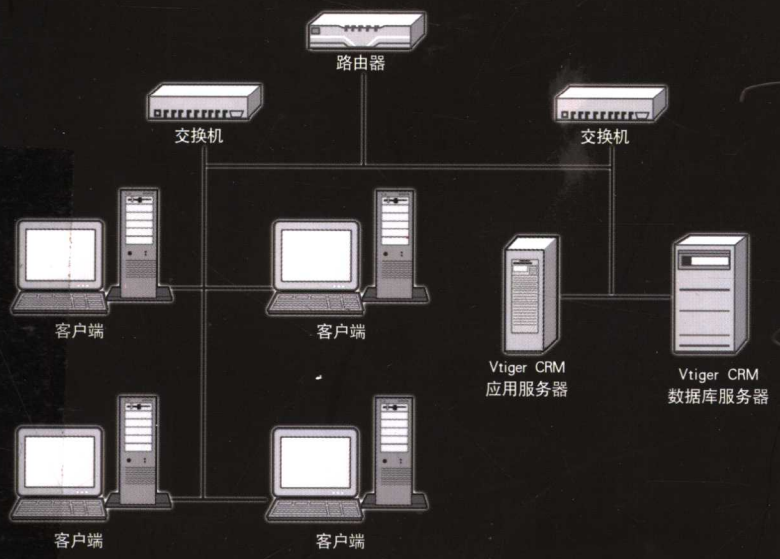
网管宝典系列

网络安全技术内幕

NETWORK SECURITY TECHNOLOGY EXPOSING

北京希望电子出版社 总策划
肖松岭 编 著



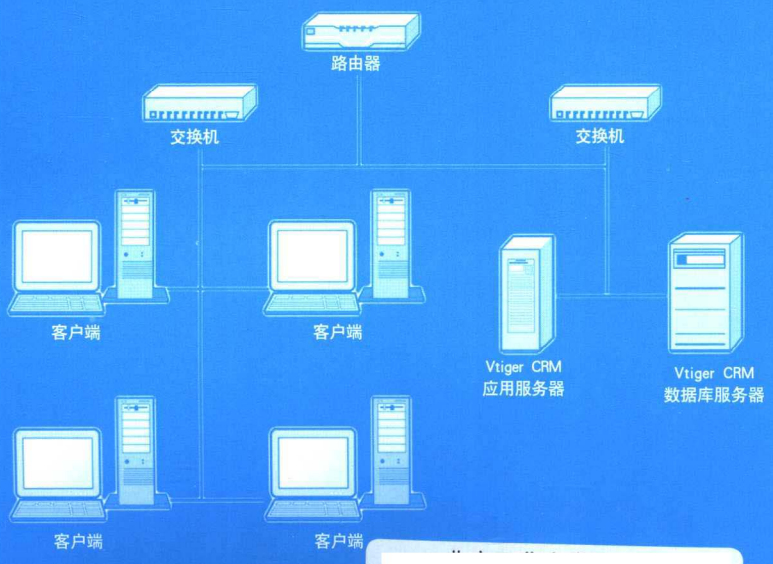
科学出版社
www.sciencep.com

网管宝典系列

网络安全技术内幕

NETWORK SECURITY TECHNOLOGY EXPOSING

北京希望电子出版社 总策划
肖松岭 编 著



科学出版社
www.sciencep.com

内 容 简 介

破坏操作系统、获得超级用户权限的恶意行为，对所有系统管理员来说都将是一场噩梦。本书主要讨论 Windows、UNIX、Linux 等操作系统，各类黑客入侵的手段及其防护措施。

本书共分 4 个部分：第一部分首先介绍了网络安全必备的基本意识和基础知识，接着讨论了 Windows 及其应用程序 IIS、SQL Server 以及 Web 的安全问题及攻击的方法。第二部分讨论了 UNIX 和 Linux 网络的安全问题，包括 Linux 安全硬化、服务器安全策略、虚拟专用网、防火墙技术、OpenSSH 加密以及评估与入侵事件。第三部分主要从网络架构 OSI 各层协议的安全问题着手，对各类操作系统的网络安全及其防护给出了具体实现方法。从技术角度上看，涉及各个操作平台，包括网络安全原理、IP 层安全协议、传输层安全协议、应用层安全协议、防火墙技术以及加密和认证技术等。第四部分重点讨论 Cisco 设备安全问题。网络安全的诸多问题及其安全防护措施，包括防火墙技术，数据加密技术，入侵检测系统，认证、授权和记账以及无线网络的安全性等内容，书中都作了十分详细的剖析，指导性、实用性和可操作性强。

本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读，对网络爱好者也有很好的指导作用。

图书在版编目（CIP）数据

网络安全技术内幕 / 肖松岭 编著. —北京：科学出版社，2008

（网络安全技术及应用）

ISBN 978-7-03-021374-7

Ⅰ. 网… Ⅱ. 肖… Ⅲ. —计算机网络—安全技术 Ⅳ. TP 393.08

中国版本图书馆 CIP 数据核字（2008）第 032127 号

责任编辑：但明天 / 责任校对：马 君

责任印刷：密 东 / 封面设计：梁运丽

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市密东印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2008 年 5 月第 一 版 开本：787×1092 1/16

2008 年 5 月第一次印刷 印张：45 1/2

印数：1—3000 字数：1 052 220

定价：68 元

前　言

破坏操作系统——无论是 Windows、UNIX 还是 Linux，并获得超级用户权限的恶意行为，对所有系统管理员来说都将是一场恶梦。

本书重点不在于讨论各个操作系统本身的安全问题，而是讲述它们基于网络方面的安全技术，同时还探讨了各种黑客入侵的手段以及有效的防护措施。

全书共分 4 个部分，下面对各部分作简单介绍。

第一部分　Windows 安全篇

本部分内容由 13 章组成，主要讨论应用最为广泛的 Windows 操作系统的安全问题。

Windows 操作系统最容易上手，但其存在的问题多多，无论是系统本身的漏洞，还是其提供的各种服务：上网有问题，打印有问题，输入有问题，开、关机有问题……但本书不准备讲这些，而是另辟蹊径，首先简单讨论一下 Windows 的安全及其防护，接着转移目标，讲如何攻击这个穷寇。

基于 Windows 系统网络方面的安全问题，主要包括：Windows 安全结构及其防御，踩点、嗅探、扫描，获取控制权，服务攻击——IIS、SQL Server、Web，扩大攻击范围，后门处理以及 DoS 攻击。

第二部分　Redhat Linux 安全篇

本部分内容由 6 章组成，主要讨论网络操作系统 Linux 及 UNIX 方面的安全问题。

毋庸置疑，称得上真正意义上的网络操作系统就是 UNIX 和 Linux，而目前应用较为广泛的要数 Redhat Linux。虽然这两种操作系统都是十分优秀的网络平台，但它们也必然存在诸多安全问题。基于此，本部分单独为这两款操作所存在的安全问题进行了比较详细的讨论，以期帮助读者解决一些较为棘手的难题。

基于 Linux 及 UNIX 操作系统方面的网络安全问题，主要从 6 个方面进行讨论，包括：Linux 安全硬化、服务器安全策略、虚拟专用网、防火墙技术、OpenSSH 加密以及评估与入侵事件。

第三部分　网络安全篇

本部分内容由 6 章组成，主要讨论网络通信协议及数据传输过程方面的安全问题。

网络是现代企业的脊梁骨，数以千米计的铜制或光纤电缆为通信提供了有效的数据传输介质。大多数公司的局域网（LAN）或广域网（WAN）都需要安全保护。网络漏洞绝不是小事情，一旦攻击者控制了你的网络，他们就可以控制数据的传输情况和传输目标。在大多数场合，控制了某个网络意味着攻击者不仅可以监听这个网络上的电子邮件、财务数据等敏感信息，甚至可以把这个网络上的通信重定向到另一个未经授权的系统上去，如果到了这一地步，那么该网络是否使用了虚拟专用网（VPN）或防火墙技术其作用都不大了。

虽然网络漏洞不如系统漏洞那么多，但其数量和潜在破坏力却年年在增加。从 MIB

（Management Information Base，管理信息库）信息泄露到设计缺陷和强大的 SNMP（Simple Network Management Protocol，简单网络管理协议）读/写操作，当黑客把这些网络漏洞结合起来运用时，网络管理员就不得不面对一个到处是陷阱的蛮荒世界了。

ISO/OSI 网络安全问题可以从 6 个方面来解决，包括：网络安全原理、IP 层安全协议、传输层安全协议、应用层安全协议、防火墙技术以及加密与认证技术。

第四部分　Cisco 安全篇

本部分内容由 5 章组成，主要讨论使用 Cisco 设备组建的网络安全问题。

在众多网络设备供应商中，由于 Cisco 的设备遍布网络世界的各个角落，因此它是无可争议的龙头老大。在网络安全方面，Cisco 提供了一套完善的解决方案。凡是使用 Cisco 设备的网络，或多或少都在使用 Cisco 安全方案中的技术。

Cisco OSI 网络安全方案主要由 5 部分组成，包括：认证、授权和记账（AAA），安全服务器协议，流量控制和防火墙，IP 安全和加密技术以及网络设备安全。

关于网络安全技术，包括身份认证、防火墙技术、入侵检测技术、加密技术、公钥基础设施、虚拟专用网络、恶意代码和病毒防治以及无线网络所涉及的网络安全技术，书中都进行了详细的讨论，同时指导读者进行一些尝试和探索。

本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读，对网络爱好者也有很好的指导作用。

由于新技术发展、更新迅速，尽管作者做了不懈努力，但书中难免存在不妥和遗漏之处，敬请广大读者批评、指正。

目　录

第一部分　Windows 安全篇

第三部分 网络安全篇

第四部分 Cisco 安全篇

第一部分

Windows 安全篇

本部分内容由 13 章组成，主要讨论应用最为广泛的 Windows 操作系统的安全问题。

Windows 操作系统最容易上手，但其存在的问题多多，无论是系统本身的漏洞，还是其提供的各种服务：上网有问题，打印有问题，输入有问题，开、关机有问题……但本书不准备讲这些，而是另辟蹊径，首先简单讨论一下 Windows 的安全及其防护，接着转移目标，讲如何攻击这个穷寇。

基于 Windows 系统网络方面的安全问题，主要从以下方面进行讨论：

- Windows 安全结构及其防御。
- 踩点、嗅探、扫描。
- 获取控制权。
- 服务攻击——IIS、SQL Server、Web。
- 扩大攻击范围。
- 后门处理。
- DoS 攻击。

SECTION 1