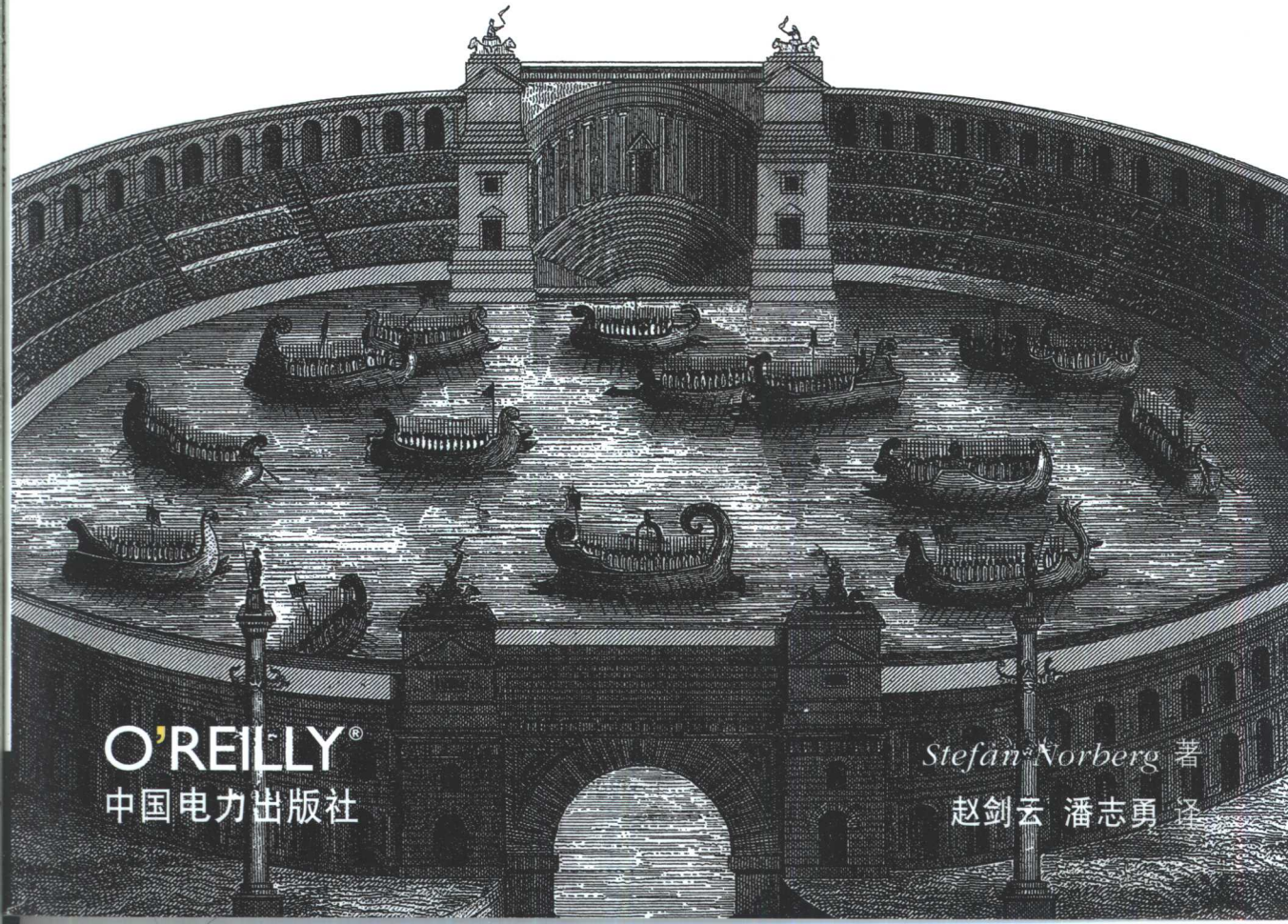
Securing Windows NT/2000 Servers for the Internet

Windows NT/2000 Internet服务器安全



O'REILLY®
中国电力出版社

Stefan Norberg 著
赵剑云 潘志勇 译

Windows NT/2000 Internet服务器安全

Stefan Norberg 著

赵剑云 潘志勇 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

Windows NT/2000 Internet服务器安全/（美）诺博格（Norberg, S.）编著；赵剑云，潘志勇译．-北京：中国电力出版社，2001.12

书名原文：Securing Windows NT/2000 Servers for the Internet

ISBN 7-5083-0851-4

Ⅰ.W... Ⅱ.①诺... ②赵... ③潘... Ⅲ.服务器－操作系统（软件），Windows NT/2000－安全技术 Ⅳ.TP316.86

中国版本图书馆CIP数据核字（2001）第088257号

北京市版权局著作权合同登记

图字：01-2001-4696号

书　　名/ Windows NT/2000 Internet服务器安全

书　　号/ ISBN 7-5083-0851-4

责任编辑/ 程璐

封面设计/ Ellie Volckhausen，张健

出版发行/ 中国电力出版社（www.infopower.com.cn）

地　　址/ 北京三里河路6号（邮政编码100044）

经　　销/ 全国新华书店

印　　刷/ 北京市地矿印刷厂

开　　本/ 787毫米×1092毫米　16开本　14.5印张　202千字

版　　次/ 2002年1月第一版　2002年1月第一次印刷

印　　数/ 0001-5000册

定　　价/ 29.00元（册）

Windows NT/2000 Internet服务器安全

O'Reilly & Associates 公司介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly & Associates公司授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly & Associates 公司是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的《The Whole Internet Use's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly & Associates一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates依靠他们及时地推出图书。因为O'Reilly & Associates紧密地与计算机业界联系着，所以O'Reilly & Associates知道市场上真正需要什么图书。

目录

前言

直到现在，仍然只有少数系统管理员相信Windows NT是一个相当不错的平台，可以用做Web服务器，或用于Internet上各种类型的系统。由于某种历史原因，绝大部分Internet服务器都是基于Unix的，而且绝大部分经验丰富的系统管理员都认为Windows NT并不安全——作为一种文件服务器或打印服务器是足够了；然而用于严格的商业应用，则是不可信赖的。

Unix仍然是Internet服务器平台的首选，但随着Windows NT安全性的逐步提高，管理员们使用它的经验日益丰富，Windows NT（以及Windows 2000）系统逐渐被用做一种可行的Internet服务器平台。已经有越来越多的单位把他们所有的商业活动都委托给了Windows NT。今天，大约20%的Internet上的Web服务器在使用Windows NT（注1），其中许多服务器是用于电子商务的。

本书假设你已经决定使用Windows NT或2000。为此提供了十分详尽的指导来帮助你安装和配置软件，尽量使你的系统安全，尤其当系统被用做一台暴露在公共网络上的主机时——例如，一台Internet上的Web服务器。

注1：　见Netcraft Web Server Survey（*http://www.netcraft.com/survey/*）。

注意： 如果你遵循本书给出的建议，你的Internet服务器在面对已知的Internet威胁时都会非常安全。不过，要牢记新类型的攻击总是层出不穷的。另外，如果系统要求极为严格的安全性，那么你就需要考虑使用额外的措施了。

本书并不是一本完全手册，也没有全面阐述Windows NT/2000安全性的所有方面。我处心积虑地缩减了文字，所以本书将以一种检查清单的叙述方式提供安装和配置方面的指导。我认为你应该通读本书，然后，当你真正建设Windows NT/2000安全性的时候，应该把本书带在身边，对照本书一步一步地检查你的工作。我假设你已经熟悉Windows NT/2000的基本操作，并且已经对这些系统的安全性有了相当的了解。这并不是一本写给新手的书。如果你现在还没掌握Windows NT/2000和网络安全性的基础知识，我强烈建议你阅读一下下面列出的参考书，或至少选择一本，你还可以根据第七章中的邮件列表查找参考书目。

注意： Email地址和URL经常变化。本书中的信息是出版时的信息。我会尽量在O'Reilly的网站上给出本书中参考书目和其他联系方式的最新更新。

《Building Internet Firewalls》（第二版）Elizabeth D.Zwicky、Simon Cooper、D. Brent Chapman著，O'Reilly&Associates公司2000年出版（ISBN 1-56592-871-7）。这本书是一个实用的详细指导，它一步一步地介绍了如何设计和安装防火墙，以及如何配置Internet服务，使其与防火墙协同工作。

《Inside Microsoft® Windows® 2000》（第三版） David A.Solomon、Mark E.Russinovich著，微软出版社2000年出版（ISBN 0-7356-1021-5），如果你想要深入了解Windows NT/2000，本书可以满足你的要求。

《TCP/IP Illustrated》（第一卷：协议）W.Richard Stevens著，Addison-Wesley于1994年出版。这本书是TCP/IP协议族的权威指南，它是我所读过的最好的书之一，我向所有想要了解TCP/IP网络通信的人推荐此书。

《MS Windows NT Server from a UNIX Point of View》，微软公司1997年出版（*http://www.microsoft.com/ntserver/nts/techdetails/overview/WpGlobal.asp*）。这本白皮书阐述了在建设Windows NT系统时的一些核心设计决策，以及对操作系统的技术性指导。

《Windows 2000 Server Resource Kit》，微软公司2000年出版（ISBN 1-57231-805-8）。这套资料手册由七本书（大约七千多页!）和一张实用工具的光盘组成。该书的技术性很强，几乎涵盖了Windows管理的各个方面，且具有极其丰富的细节描述。

本书内容

总体而论，本书分为三部分。第一章介绍了周边网络设计，并讨论了在这种环境下Windows所特有的问题。第一章提供了理解以下各章所必需的背景知识。第二、三章是一个关于如何将Windows NT/2000的安全性提升到一个较高层次的实用指南。第四章至第七章着重于系统管理的主题，例如远程管理、备份和远程登录。

下面列出了每一章的综述：

第一章 “Windows NT/2000安全性”，介绍了Internet安全的问题，介绍了周边网络（Perimeter Network）的概念及其组件（着重于堡垒主机，bastion host）。本章包括Windows NT/2000系统结构的概要，以及与这种结构相关的特有的安全性。

第二章 “构建Windows NT堡垒主机”，本章推荐了构建Windows NT堡垒主机的策略。

第三章 “构建Windows 2000堡垒主机”，本章概括了Windows NT和Windows 2000的不同点，并介绍了IP安全性协议（IPSec）在Windows 2000上的实现。

第四章 “配置安全远程管理”，提供了三种安全远程管理的解决方案。其中两种已获得业界的支持，另外一种则是基于与平台无关的产品和协议的。

第五章 “备份和还原堡垒主机”，讨论了备份堡垒主机过程中的问题，并给出了Windows自带备份软件的简要概述。

第六章“审核并监视周边网络”，解释了Windows的审核和事件日志系统的机制。本章提供了远程登录和时间同步的策略，并介绍了入侵检测（intrusion detection）。

第七章“维护周边网络”，描述了一些有助于维护周边网络及其组件安全性的方法。

附录一“Windows NT/2000的常用端口”，列出了较常使用的Windows NT/2000和微软Back Office应用软件的TCP/IP端口号。

附录二“关于安全性的文章”，列出了引自Microsoft Support Knowledge Base（微软支持软件知识库）的文章。

附录三“Cygwin上OpenSSH的创建指令”，包括了从损坏状态重建OpenSSH二进制文件的指令。（特别提一下，在O'Reilly的网站上有一个预编译的版本。）

排版约定

本书中英文采用如下的字体约定：

斜体（*Italic*）

用于文件名、目录名和URL（FTP、HTTP等等）。也用于强调和技术名词第一次出现。

等宽（`Constant Width`）

用于文件内容和命令输入/输出。

“**注意：**”表示一条窍门、建议或一般的提示。例如，在讨论Windows NT 4.0时，我会告诉你Windows 2000中用来改进安全性的新特性。

“**警告：**”是提醒你要注意的地方。例如，当某一安全设置对系统有负面影响时我会提出警告。

本书中所提到的自由软件

在O'Reilly的主页（*http://www.oreilly.com/catalog/securwinserv*）上有本书中提到的所有自由软件的信息和链接。预编译的版本也可由O'Reilly的网站获得。

Cygwin

用于Windows NT/Windows 2000的POSIX仿真层。

NTP

以GPL许可证发布的NTP（Network Time Protocol，网络时间协议）的实现。

NTsyslog

NT系统日志服务的事件日志。

OpenSSH

网络连接工具SSH（Secure Shell，安全外壳）的免费版本。

OpenSSL

实现了安全套接层（SSL v2/v3）和传输层安全（TLS v1）协议的开源工具包，它也是一个通用的加密库。OpenSSH是OpenSSL加密库的后继版本。

TCP Wrappers（TCP包装）

一个程序库，监视并筛选那些与该库相连的网络服务请求。

VNC（Virtual Network Computing，虚拟网络计算）

可以运行在多个平台的远程后台系统。

建议与评论

本书的内容都经过测试，尽管我们做了最大的努力，但错误和疏忽仍然是在所难免的。如果你发现有什么错误，或者是对将来的版本有什么建议，请通过下面的地址告诉我们:

美国:

O'Reilly & Associates,Inc.
101 Morris Street
Sebastopol, CA 95472

中国:

100080 北京市海淀区知春路 49 号希格玛公寓 B 座 809 室
奥莱理软件（北京）有限公司

你也可以给O'Relly发电子邮件。如果想要将自己加入邮件列表或索取一份书目，请访问:

http://elists.oreilly.com/

如果有技术方面的问题或对本书提出指正，请发 Email 到:

bookquestion@oreilly.com/

下面是本书的主页，在那里你可以找到软件和勘误表（以前所发现的错误及其更正），请访问网址:

http://www.oreilly.com/catalog/securwinserv/

最后，您可以在 WWW 上找到我们:

http://www.oreilly.com
http://www.oreilly.com.cn

你也可以直接同我联系:

Stefan@norberg.org

致谢

本书源于一位O'Reilly的编辑Deborah Russell的建议，她看到了我在网上发布的一篇研讨Windows NT安全性的论文（注2）之后与我联系。我非常感谢她在内容、结构和写作风格上所提出的指正。没有她的支持和指导，本书只能是一些杂乱的章节。

我写那篇论文是得到了同事Kevin Steves的研究工作（注3）的启发。Kevin审阅了本书的几次初稿，在这个项目上他还是我的导师。没有他的支持，本书不可能如此完美。我还要感谢本书的技术审校：Simson Garfinkel、Greg Hoglund、David LeBlanc、Kevin Steves和Elizabeth Zwicky。

我衷心地感谢深爱我并支持我的妻子Mavianne，她耐心地阅读并推敲了书中的每一个句子——而且是读了两遍。

特别感谢我以前在惠普公司的同事，他们为我提供了极为专业的帮助，他们也是我的好朋友。我感谢那些从网上下载了我那篇论文并提出建议的人们。Internet真是一个分享思想和结识新朋友的好地方。

注2：“Building a Windows NT bastion host in practice”，可在*http://People.hp.se/stnor/*上找到。

注3：“Building a Bastion Host Using HP-UX 11”，可在*http://people.hp.se/stevesk/*上找到。

本章内容：

- Internet 威胁
- 在 Internet 上建立一个安全的站点
- Windows NT/2000 系统结构
- 周边网络中的 Windows NT/2000
- 加密基础

第一章 Windows NT/2000 安全性

如果使用Windows系统作为Internet服务器，则会面临安全性的挑战。相对大多数内部系统来说，与Internet相连接的系统直接暴露在安全性攻击面前。这些攻击有的来自于新手，有的来自技术娴熟的攻击者。Windows NT（以及Windows 2000）的典型安装将会使Windows服务器轻易地成为这些攻击的目标。确保用于Internet的Windows NT/2000操作系统的安全性是一项复杂的工作。本书的目的是提供一种策略，使基于Windows的服务器配置尽可能地安全。这一策略分为两个基本部分：

1. 对可能遭受Internet攻击的Windows服务器进行加固，尽可能使其安全。这种暴露的系统通称为堡垒主机（bastion host）。
2. 通过安装一个附加网络 —— 通称为周边网络（Perimeter Network）来提供额外的安全保护。它可以把外部网络（通常是Internet）和公司内部网络分离开来。

后面各个章节会专门讲述如何加固 Windows NT/2000 系统，使其可以在周边网络中充当一台安全的堡垒主机。在我逐步给出安全性细节之前，这一章将会简要地描述一下系统将会面临什么样的安全性威胁、Windows NT/2000操作系统的基础结构，以及在周边网络中 Windows 服务器的推荐配置。