网络安全技术系列丛书

Windows NT Server 4 Security Handbook

Windows NT Server 4 安全手册

(美) Lee Hadfield
Dave Hatter
Dave Bixler 著

高杏生 等译

机械工业出版社
西蒙与舒斯特国际出版公司

QUE® CMP

网络安全技术系列丛书

Windows NT Server 4 安全手册

Lee Hadfield
(美) Dave Hatter 等著
Dave Bixler
高杏生 等译
王建华 审校

机 械 工 业 出 版 社
西蒙与舒斯特国际出版公司

Windows NT服务器安全手册由五部分19章组成：第一部分概述网络安全性应关注的问题；介绍了Windows NT服务器安全结构及Windows NT提供的各种安全工具的使用。第二、第三部分着眼于理解并实施Windows NT 的许多安全特性，如域的概念、文件系统和用户帐户安全性问题。通过具体实施主域模式，学习设计域，规划域控制器，创建用户组，建立委托关系。第四部分解释Windows NT 网络与其他网络操作系统组网时，如何在内部网络、外部网络使用TCP/IP或与Internet 连接时确保Windows NT网络的安全性。第五部分讨论Windows NT怎样达到国防部C2级安全标准。

本书版权登记号：图字：01-98-0129

图书在版编目(CIP)数据

Windows NT Server 4安全手册/(美)哈德菲尔德(Hadfield,L.)等著；高杏生等译。-北京：机械工业出版社，1998.6
(网络安全技术系列丛书)
书名原文：Windows NT Server 4 Security handbook ISBN 7-111-06146-2

I.W… Ⅱ.①哈…②高…Ⅲ.计算机网络-安全技术-手册Ⅳ.TP393

中国版本图书馆CIP数据核字(98)第06017号

出 版 人：马九荣(北京市百万庄大街22号 邮政编码100037)
责任编辑：江 颖
三河永和印刷有限公司印刷 • 新华书店北京发行所发行
1998年6月第1版第1次印刷
787mm × 1092mm 1/16 •18.75印张
印 数：0001-8000册
定 价：32.00元

译 者 序

1993年Microsoft 公司推出新型32位操作系统以来，计算机网络领域出现了一系列的变化和发展。Windows NT 已经逐步发展成为一种世界级的网络操作系统，从而对网络和网络的安全产生了重大的影响。

本书将全面分析你的网络所面临的各种安全问题，告诉你如何评估和监控网络的安全性。通过详细介绍Windows NT 采用的功能强大的安全模式，使你了解应该采取哪些方法和技巧来保护Windows NT 网络和它所包含的各种信息的安全。此外，本书还讲述了如何将Windows NT 的安全功能与NetWare、UNIX和 Maciutosh 操作系统结合起来运行的方法。

全书分为5个部分共19章。第一部分综合介绍 Windows NT 的安全性，使你了解网络安全的基本概念和要求，Windows NT 安全性的模式以及Windows NT 操作系统的结构。第二部分介绍如何实现Windows NT 的安全性，包括运用域、域的委托关系、用户帐户和新型文件系统等来保护系统的安全。第三部分讲述一个如何建立主控域模式的实例。第四部分介绍如何将Windows NT 的安全性应用于BackOffice产品、Internet和其他网络平台。第五部分介绍如何在Windows NT环境中实现美国国防部规定的安全标准。

本书由Lee Hadfield Dave Hatter和Dave Bixler 共同撰写。他们在软件开发、网络设计和管理等方面具备丰富的经验，并且参加了多部计算机专著的编写工作。本书既包含了系统的理论知识，又配有详细的实例介绍，因此是一本非常实用的参考手册。

本书由高杏生、高波、徐军和刘孜群翻译。参加翻译和录排工作的还有赵永国、杨武臣、王爱晶、杨宝明、王卫峰、吴小红、潘青、吕晨波、吴炳林、侯丽坤、陈晓明等。全书由王建华审校。

由于译者水平所限，书中难免存在不妥之处，敬请读者批评指正。

译者

1997年12月

引　言

微软公司1985年步入网络领域时，起步很小，只是增强MS-DOS 3.1的网络功能；而1991年迈出了具有重要意义的一步：推出了Windows for Workgroups 3.11(WFW)。但真正使 微软公司走上网络界统治地位的是1993年发行的内置网络功能和图形用户界面(GUI)的新32位操作系统。这个新的操作系统名为Windows New Technology，简称 Windows NT。尽管它在业界分析家和企业用户中受到的欢迎程度说好了也不过是不冷不热，但却呈现出很好的发展前景。

自从Windows NT 推出以来，网络界已经发生了很大变化。在发生的所有变化和进步之中，两样东西对Windows NT 网络以及随之而来的网络安全产生了最重大的影响。一是 Windows NT 成为成熟的世界级网络操作系统(NOS)；二是广域网(WAN's)、互联网络及Internet的爆炸性发展。

本书遵循这样的前提：积极进攻就是最好的防御。尽管没有一个系统能够做到百分之百的安全，但是，如果你的系统与一般的系统相比更难被大多数计算机黑客闯入，那么计算机黑客就会猎取更容易打击的目标。Windows NT Server 安全手册通过介绍网络面临的安全威胁，帮助你加强防御措施(如果保护这些操作系统是你的责任，那么这些威胁令人惧怕)。本安全手册向你展示Windows NT的强大安全模式，教给你为保护网络而采用的技术措施以及它们所包含的关键性任务信息。

微软公司以极快的速度不断增强 Windows NT 的功能和性能。增强的功能很多，其中一些如下：

- 以 Windows 95用户界面代替旧的 Windows 3.x 界面。
- 重写操作系统结构以提供数量更多、质量更好的性能。
- 吸收了 Internet Information Server (IIS)，包括 HTTP、FTP 和 Gopher服务程序。
- 本机 TCP/IP 过滤功能使你能够筑起一堵花钱不多的基本防火墙。
- NetWare 的 Gateway Services 现已包括了对 NetWare Directory Services(NDS)的支持。
- 新的点对点之间管道连接协议使你能够通过 TCP/IP 网络发送非 TCP/IP数据。
- 改善了注册(Registry)的使用和安全性。
- 增加了系统策略编辑器，从而可以更好地控制用户网络环境。
- 采用了 Domain Name Service (DNS)服务器服务程序，使你可以方便地在网络中添加DNS服务程序。
- 增加了 Administrative Wizards，极大地简化了管理工作，对新的管理员来说尤其如此。
- 大大改善了 Task Manager，使其更加有用。
- 增加了一个 Multi-Protocol Router (MPR)服务程序。

尽管 Windows NT 3.51 版本的功能有了明显增强，使它成为“受人崇拜的有名”产品，但是实际上只有4.0版本才真正实现了它努力要达到的目标。Windows 4.0是一个可伸缩的、强大的、功能丰富的、安全的操作系统，因为它提供了最好的“货真价实”的高档操作系统，才使之正迅速成为高档客户机和服务器的精选操作系统。

维护安全性

Windows NT 的销售数字说明了它在维护系统安全方面具备的能力。1995年Windows NT Server 销量增长了86%，根据国际数据公司(IDC)公布的1996年销售结果，Windows NT Server 的销量比 Novell 的 NetWare 3.x，4.x 和 NetWare Loadable Modules 合起来还多!前者销售732000台，而后者加在一起才669 000台。

但是随着功能的扩充，安全隐患也增加了，基本原因有两个：一是开发小组感到要消除黑客搜寻和可利用的漏洞变得越来越困难；二是系统管理员要面面俱到地实施全面管理变得越来越困难。对于像 Windows NT Server 这样功能丰富、结构复杂的产品，很难保证能堵塞所有的安全漏洞。因此网络管理员必须经常保持警惕。

Windows NT Server 增加 Internet Information Server (IIS)以后，情况尤其如此。IIS 是在 Windows NT 结构基础上建立起来的功能异常强大的工具，它使Windows NT 非常容易用于 Internet。但记住，把一个网络与TCP/IP 网络(尤其是 Internet 网络)连网，就为用户(包括黑客)访问你的系统打开了大门。

另一个令人关切的问题是使用计算机的人越来越多，更多的用户对计算机的了解越来越深入，这意味着，如果不采取适当的安全措施，用户或出于好奇心理，或出于有意伤害的邪念，可能会经常破坏系统，毁掉数据。

所有这些说明了什么？涉及到安全问题，适当全面考虑问题是件好事!如果你看问题全面，可能不仅要采取适当的预防措施来保护网络安全，而且还会保持警惕，寻找安全隐患。关键是权衡安全保障、性能和可用性之间的关系。如果安全规则太严，则用户无法利用系统完成工作。另一方面，尽管使用的网络是世界上最快最容易使用的网络，但黑客偷掉你的数据，破坏你的系统，给你的企业造成无法挽回的损失。那样，你能得到什么呢？

有关安全问题，须要理解两个关键概念：第一，疏忽通常是安全的最大威胁。如果你不知道存在安全漏洞，或者不知道有堵漏洞的工具，那么你会遇到麻烦，因为有人知道这些漏洞，而且乐于闯入你的系统。第二，提高警惕。安全是个不断发展的过程，它不会在你建立了用户帐户或安装了防火墙后而停止。为了确保系统安全，你必须经常寻找并堵塞安全漏洞。

最后，请记住，每个网络环境是不一样的。本书讨论的一些技术和策略可能不适合你的环境。在采用本书提出的建议以前，务必备份你的系统，在非实用系统上检验这些变动情况。

本手册的读者对象

本书主要为 Windows NT Server 管理人员所写。他们须要彻底了解网络所面临的安全威胁。本书介绍了相应的策略，帮助你保护你们机构中最重要的资源——信息。同时你将掌握 Windows NT Server 提供的许多健全的安全措施，如新技术文件系统 (New Technology File System——NTFS)、审查、TCP/IP 过滤和帐户设置原则等。此外，你还可以了解到许多非文档的或常常被忽略的安全漏洞，以及使你能够有效堵塞这些漏洞的提示、方法和技巧。

本书可供正在考虑或正在使用 Windows NT Server，并想确保企业系统和信息安全的经理和企业家们使用。

如何使用本书

本书分成五个部分，很容易理解。第一部分介绍网络安全问题。对于初学者来说，第一

部分是有关安全问题的最好的启蒙教科书；而对于老练的网络管理人员来说，第一部分是很好的温故知新的读物，同时也是深入研究 Windows NT 结构的好教材。第二和第三部分着眼于理解 Windows NT 的许多安全特性。第四部分集中阐述 Windows NT 网络、Internet 网络和其他网络操作系统连网后 Windows NT 网络的安全问题。最后第五部分讨论 Windows NT 怎样达到国防部C2级的安全要求。

第一部分　Mircosoft Windows NT 安全性概述

第一部分概述了网络安全性关注的问题，以及 Microsoft 公司的Windows NT Server 如何解决这些问题。Windows NT Server的安全结构提供了许多安全工具，可以帮助你完成安全性目的。

第1章“了解安全性的基本知识”　介绍网络安全的基本知识，如：什么是安全性，谁需要安全，如何设计安全。

从第2章“Microsoft Windows NT 安全性概述”　中可以了解到强大的 Windows NT 安全模式，以及 Windows NT 提供的许多安全特性和操作工具。

第3章“Windows NT 操作系统的结构”　把你领进 Windows NT 的系统结构内部，详细阐述了 Windows NT 3.51 的结构，Windows NT 4.0 发生的变化，以及这些变化与Windows NT 网络安全性的关系。了解 Windows NT系统结构，对于确保网络安全至关重要。

第二部分　Microsoft Windows NT 的安全性实施

第二部分详细叙述了 Windows NT 安全模式的许多特性功能。你将会学习Windows NT域、文件系统、用户帐户及与安全性相关的许多有用提示和技巧。也可以了解网络客户对 Windows NT 安全性的影响。

第4章“Windows NT 域的概念”　揭开了 Windows NT 域的神秘面纱。你将会了解什么是域，为什么需要域，域与用户帐户有何关系，以及如何有效地管理它们。

第5章“用域委托关系维护安全性”　本章解释了经常引起混乱的域和委托关系的概念，教你如何利用域之间的委托关系进一步改善 Windows NT 网络上的安全性。

第6章“用户帐户的安全性与 Window NT”　为确保 Windows NT 用户帐户安全，Windows NT提供了许多手段供选择。本章还介绍了如何利用组使管理变得更加容易。

第7章“新技术文件系统(NTFS)的安全性”　介绍了保护 NTFS 文件系统须要理解并最终实施时所需的知识。

第8章“使用 Windows NT 安全性为域资源提供保护”介绍了如何利用 Windows NT Server 提供的工具，如User Manager for Domains，Event Viewer 和 Registry Editor，来确保你的 Windows NT网络的安全。

第9章“Windows NT Workstation的安全性”　介绍 Windows NT Workstation特有的安全问题和提示。

第三部分　创建主域模型实例

第三部分全面介绍为实施 Windows NT 主控域模式须要知道的知识。将要学习如何设计域，规划域控制器，创立用户、组以及建立委托关系。

仔细规划你的主域对于成功地使用非常重要。

第10章“规划主域” 帮助理解有关要求和面临的挑战。

第11章“实施步骤” 介绍如何配置 Windows NT 环境的主域模式，内容包括准备域控制器、创建用户帐户和组帐户以及配置资源服务器。

第12章“建立委托关系” 讲述配置域之间的委托关系。

第四部分 Windows NT 安全性与BackOffice 产品，Internet 和其他网络平台的结合

不管是 Intranet 还是Extranet(外延网)，现在是一个特别热门的话题，安全对于连网的机构来说，具有也应该具有极重要的意义。第四部分介绍了Windows NT网络与其他网络操作系统、在Intranet(内部网)、Extranet(外部网)使用TCP/IP或与Internet连网时如何确保Windows NT网络的安全性。

第13章“安全性与 Internet概述” 介绍了与Internet 连网时如何确保Windows NT网络的安全。讨论的问题包括Internet面临的威胁，已知的安全问题，防火墙，代理服务程序和IP过滤功能。

第14章“Internet安全性和BackOffice” 介绍如何确保可在Internet上运行的BackOffice应用程序的安全性；如微软公司的Internet Information Server和Microsoft Exchange。

第15章“Windows NT与NetWare 和其他网络操作系统的集成” 介绍如何把Windows NT Server 与其他网络操作系统相连接，如Novell NetWare和Banyan VINES，以及一旦连接，如何确保网络安全。

第16章“让Macintosh 客户访问Windows NT资源” 介绍如何通过安装 Macintosh 服务程序、配置访问权，把Apple Macintosh与客户机Windows NT服务器连接。

第17章“Windows NT与UNIX环境的集成” 介绍了如何把 Windows NT Server与UNIX网络，讨论了有关的安全问题。

第五部分 在 Windows NT 环境中实施美国国防部安全标准

第五部分使你进入Windows NT绝密领域——C2级安全标准。你可以了解到C2级安全性的含义，哪些部分与国防部可信任计算机系统评估标准吻合，以及在你的Windows NT网络中如何实施这一等级的安全标准。

第18章“美国国防部可信计算机系统评估标准概述” 介绍网络安全的政府标准(这是由美国国家安全署的一个机构——全国计算机安全委员会——开发的标准)。这个标准为受到信赖的计算机产品定义了安全标准。

第19章“在Windows NT中实现C2级安全标准” 介绍如何使你的Windows NT 网络达到C2级标准。

本书中的体例、结构与字符约定

Que公司具有十多年撰写和开发最成功的计算机书籍的经验。根据这些经验，我们了解到哪些特性功能对读者的帮助最大。在全书寻找这些具体的特性功能，以增进你的学习经验。

每一章都以导读开始，简要列举本章要阐述的内容，使你一眼就能看到这一章包含的信息，可以当作本章的主要提纲。

提示:

“提示”对经常容易忽视的操作步骤提供简短的忠告。这些提示包括一些快捷操作方式，可以帮助你节省时间。

注意:

“注意”为你提供额外的信息，可以帮你避免操作中出现的问题，或提供与内容有关的建议。

警告:

“警告”可以提醒你某个操作步骤可能引起的潜在的问题、未预料到的结果或可以避免的错误。

上网:

在阅读本书过程中，你会发现一些Internet参考信息，为你提供World Wide Web的网址，或补充本书内容的其他在线资料。Internet参考信息的形式如下:

你可以按下列地址访问QUE公司的Web网址:

http: //www.que corp.com

▲参见.....P.xxx 表示相互参照第几节上有关主题的更多信息。

附文

与本章思路不完全一致的更多内容的讨论被置于附文之内。阅读附文的内容，以找出甚至更多的信息。

下划线热键或助记符:

本书使用的热键(热键使你很快能访问菜单、按钮和命令)均带有下划线，就像屏幕上显示的那样。例如菜单选项File中的F就是个热键，也叫做快捷键，可以打开File菜单。要访问某个热键，只要按住ALT键，同时按下跟你要选内容相应的热键即可。例如，要打开Edit 菜单，只要按住ALT键，然后按E键即可。

快捷键组合:

快捷键组合与使用热键一样，使你能够用键盘快捷键取代鼠标的点击引导你找到有关菜单来完成操作。例如，假如你要将信息拷贝到剪贴板，再把信息贴到当前文档中去，你可以采用两种方法来完成: 用鼠标选择Edit 和Paste 来完成，也可以按住CTRL键，再按V键来达到同样效果。大多数情况下，键盘快捷键都在它们要执行的功能的菜单选项边上标出。本书使用的快捷键组合在文本中以CTRL+V表示。

菜单命令:

选择菜单命令的指令呈下列格式:

Choose File Properties。

这意味着，你应该点击File 菜单选项中的 F 打开菜单， 然后点击File菜单中的Properties中的P。

由于Windows NT采用Windows 95的用户界面，因此Start按钮也在Windows NT中出现。你要从Start菜单中选择某个项目时，在文本中其形式如下:

打开Start菜单，选择Settings，Control Panel，Internet。

网络安全性的其他信息资源

尽管本书试图作为介绍Windows NT Server安全性的一本全面的指导手册，但是下面的任

何书籍以及 Web 地址都是对本书内容的很好补充。

Internet Firewalls and Network Security, Second Edition, New Riders Publishing, Chris Hare and Karanjit S. Siyan, Ph.D.1996, ISBN: 1562056328.

Implementing Internet Security, New Riders Publishing, New Riders Development Group, 1995, ISBN: 1562054716.

Internet Security: Professional Reference, New Riders Publishing, Derek Atkins (Editor), Paul Buis, Chris Hare, Robert Kelley, 1996, ISBN: 1562055577.

Network and Internetwork Security: Principles and Practice, Prentice Hall, William Stallings, 1995, ISBN: 0024154830.

Web网址:

美国国家计算机安全协会	http://www.ncsa.com
电子保密信息中心	http://www.epic.org
微软公司	http://www.microsoft.com
Netscape	http://www.netscape.com
网络专业人员协会	http://www.npa.org
Windows NT 杂志	http://www.winnt mag.com
RSA 数据安全	http://www.rsa.com
加密策略资源页	http://www.crypto.com

目　录

第五部分 在 Windows NT环境中实施美国国防部安全标准

第一部分 Microsoft Windows NT 安全性概述

第1章 了解安全性的基本知识

本章重点介绍安全性的基本含义，安全性与使用 Windows NT 4.0 Server的现代计算机网络的关系。为保证硬件安全，本章讨论了一些对硬件安全造成的常见的威胁，以及你怎样才能保护硬件免遭这些威胁。

• 安全概念

了解在设计或维护网络环境中运行的Microsoft公司的Windows NT操作系统时的安全性及其功能。我们将回答“什么是网络安全性”这个问题，并介绍安全性给网络带来的好处和不足。

• 安全措施

介绍需要采取安全措施的环境，这一部分内容讨论了网络面临的多种威胁，以及这些威胁引起的危害。

• 保护范围

下一部分集中讨论需要保护的网络操作系统（NOS）的构成部分，介绍了不同类型资源的基础内容。

• 设计安全性

介绍新的网络或现存网络内部安全设计的基本指导原则，观察不同网络层的安全问题以及在各个层次为保护网络免遭损害而应采取的措施。

• 容错

解释介绍安全网络设计中容错所起的作用，研究容错纳入系统部件的一些方法，以保证网络资源随时可供使用。

1.1 什么是网络安全性

在了解网络安全性以前，你也许首先想给整个企业环境中分布式信息处理系统的“安全性”这个词下个定义。简单说来，安全性就是保护你的程序、数据或者设备免遭他人在非授权情况下使用或访问。

但是网络安全性的实际含义远远超出这个简单的定义范围，它还包括若干复杂的、难以理解的系统管理方面的问题。安全网络的目标不仅是保护网络系统的部件、程序、数据免遭他人未经授权而使用或访问，而且安全计划的目标是保护企业。

应当说，安全计划必须保护系统的数据、程序，设备和网络部件的安全，使其免遭损坏、偷窃或误用。它同时也必须保证需要时网络能提供服务。这项任务可以通过使用网络操作系统提供的安全工具、实施系统设计中的冗余以及通过提供必要物理屏障阻止非授权人员访问系统部件等手段得以完成。

现代企业解决问题的办法正在变得针对性越来越明确，越来越依赖分布式计算机网络允许群体人员一起更加有效地工作。随着技术的发展，并且变得越来越复杂一样，对于技术上更加复杂的保护方法的要求也越来越高。此外，网络系统越复杂，要想达到预期的安全效果所需的努力也越大。这通常意味着需要作出更多的高强度的努力才能达到所需的安全水平。在实施安全计划的开始阶段，若能适当计划、周密思考，则你能既省时又省钱，而且可最大限度地减少投入就能给网络提供高度的安全性和稳定性。

在实施网络安全计划的同时又出现问题的另一个方面——它限制了系统的最终用 户对系统资源的访问。 说到底，对网络实施安全计划的最终目的是保证企业运营不中断；主要目标应该是允许网络用户为完成他们手头的任务而访问所需数据和程序，而不受不必要的限制。它的目标肯定不是限制系统过严以致阻碍生产力的发展，而是使得他们能以快速有效的方式访问他们授权访问的资源。 与此同时，你必须以一种容易控制、容易管理、容易监督的方式保证网络资源的完整无损。

警告 你会发现,如果以非常严格的方式锁定系统，用户会绕过你的安全措施，通过共享口令或把数据拷贝到公共区域等办法来找到访问资源的办法。

如果你有幸为一个新网络进行安全设计，你就有机会在设计阶段为安全打下一个坚实的基础，从而避免许多设计不好的网络出现的安全隐患。如果你被指派主管或清理现存的网络安全工作，不要急，继续往下读,你会找到相应的解决办法。

1.2 谁需要安全

随着我们的社会日益依赖你开发的信息系统，你更加需要依靠我们开发的安全保障措施来保护你的系统。安全保障措施不仅保护网络系统本身，而且可以保护更有价值的东西——网络系统里面所包含的信息。数据的丢失远比可以更换的网络部件的损失更具破坏性。关键数据的丢失往往会引起企业的倒闭，至少，对用户的工作效率和财务盈亏产生重大影响。

谁需要安全？我们这么说吧：如果你有信息储存于分布式网络环境之中，而你企业的运营天天需要这些数据，那么你就需要实施某种程度的网络安全措施。数据的性质是否敏感没有关系，为了使企业避免数据无法获取、丢失、被窃或误用，数据仍然必须得到保护。

随着数据量的增大和敏感度的提高，采取足够安全措施的必要性更为迫切。必须实时访问关键信息时，足够的安全措施非常重要。

1.2.1 安全威胁源

那么威胁来自何方？这取决于你谈论的安全威胁的类型。简单说来，你可以把分布式网络系统碰到的安全威胁分成两个基本的类别：

- 人为威胁源：人为威胁源产生于人们的错误操作与不操作，从而导致网络数据和资源的改动、丢失、被窃或误用。
- 物理威胁源：网络物理威胁源产生于网络关键部件的故障，从而造成无法获取数据或系统资源。

人为威胁源以及你能采取的防范措施是本手册讲解的重点。在提供存放关键数据的安全、可靠、网络平台方面，Microsoft 公司的 Windows NT Server的性能件非常出色。但是要做到万无一失，你还得在网络安全的物理环境方面多下功夫。如果因为服务器上数据没有备份而