Windows .NET Server安全指南

Windows .NET Server Security Handbook

[美] Cyrus Peikari 博士，Seth Fogie 著　周 靖 译

清华大学出版社

Windows .NET Server 安全指南

[美] Cyrus Peikari 博士, Seth Fogie 著

周 靖 译

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书是第一本介绍 Windows .NET服务器安全的专业书籍，两名作者均是资深的行业专家，他们将指导读者实现每一项重要的 Windows .NET和 XP 安全特性，从.NET的新型防火墙到最新的加密文件系统。与此同时，还介绍了一些新特性(比如远程桌面和远程协助)在安全方面的意义。另外，还讨论了如何利用微软提供的最新工具，在各种各样的场合配置安全性。学习本书后，读者会掌握如何在各种规模的网络中，最有效地保护任何 Windows .NET系统。

本书适合关心 Windows .NET安全的网管、企业管理人员、超级用户和 IT 安全顾问阅读，也适合欲部署和升级到 Windows .NET的用户参考。

北京市版权局著作权合同登记号：图字 01－2002－4504 号

图书在版编目(CIP)数据

Windows .NET Server 安全指南/(美)佩卡利，(美)福奇著；周靖译.
—北京：清华大学出版社，2002
书名原文：Windows .NET Server Security Handbook

ISBN 7-302-05869-5

Ⅰ. W... Ⅱ. ①佩... ②福... ③周... Ⅲ. 服务器—操作系统(软件)，Windows .NET Server—安全技术 Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2002)第 069247 号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑：文开祺
印 刷 者：北京牛山世兴印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：18.25　**插页**：1　**字数**：396 千字
版　　次：2002 年 10 月第 1 版　2002 年 10 月第 1 次印刷
书　　号：ISBN 7-302-05869-5/TP・3476
印　　数：0001～4000
定　　价：39.00 元

中文版序

安全，对于包括中国在内的整个国际社会，都是一个亟待解决的重要问题。黑客的威胁无时、无处不在。包括 Microsoft 在内的各大公司纷纷推出自己的应对之策。随着 Windows .NET Server 的分布，Microsoft 把服务器平台的安全性提升到了一个新台阶。以这个平台为基础，许多高级安全技术都可轻松实现。

本书正是在这样的背景下问世的，书中全面讲解了 .NET Server 的安全机制，指导您建立一个高度安全、高度可靠的服务器平台。

中国是一个有巨大潜力的国家，一旦潜力被激发，这条巨龙的气势会使整个世界为之震惊。摆在您面前的这本书，以及其他许多讲解领先技术的书籍，将如春雨滋润万物一般，使读者快乐成长。

在与中国留美学生交往的过程中，我们发现他们总能想出一些新鲜的、可行的观点，总能准确地把握重要的新技术的主旨。我们希望有一天能到中国与亲爱的读者面对面地交流。但在这之前，先让本书成为我们跨越重洋建立联系的纽带。

本书英文版的精髓被周靖先生完美译成了中文。他在翻译过程中同我们实时沟通，对原文的许多不足之处进行了改进，使中译本的质量上升到一个新的台阶。在此要感谢他，以及参与本书中文版制作的所有人员。

Cyrus Peikari 博士
Seth Fogie

作者简介

Cyrus Peikari 博士：VirusMD 公司首席技术官，他设计的安全软件屡获殊荣，而且在反病毒领域拥有几项专利。他是 Defcon 大会的发言人，经常在有关 Internet 安全新闻的电视节目中抛头露面。

Seth Fogie：VirusMD 公司高级安全顾问，在达拉斯 KRLD Radio 广播电台（隶属于哥伦比亚广播公司）主持每周一次的 Internet 安全节目。他持有 MCSE 证书，以前是一名美国海军原子能工程师。Peikari 和 Fogie 共同创作了《Windows Internet Security: Protecting Your Critical Data》一书（Prentice Hall PTR）。

首席技术审稿人：Warwick Ford 博士，VeriSign 公司主管研究的副总裁和首席技术官，也是全球知名的 Internet 安全和密码学专家。

前　言

安全是关系 Microsoft 成败的关键。Microsoft 将自己的命运押在了.NET战略上，但黑客却会不遗余力地找出这个精密结构的些许漏洞。Microsoft 自己也承认，要想公众对其安全性树立信心，尚有很长的一段路程。

令人遗憾的是，Microsoft 的安全性每前进一步，黑客似乎就会迫使它后退一步。事实上，对.NET的威胁已变得如此严重，以至于比尔·盖茨也被迫重新调整整个公司的策略，将安全问题摆在首要位置。2002 年 1 月，在盖茨的一个备忘录中，明确宣布 Microsoft今后会将安全性视为首先需要解决的问题。这一“可信计算”备忘录表明盖茨在多年来面对众人对其产品安全性的批评后，终于有所表示。他最后的表态也反映了黑客们多年来所说的：Microsoft 必须变得更安全，否则注定会失败。

.NET基于三个重要支柱。第一个是仍有许多人持怀疑态度的.NET 框架。这种分布式编程技术可使软件成为网上的一种服务。但在它尚未正式发布之前，一些独立工作的专家就在.NET 框架中发现了安全漏洞。另外，将来的问题可能会更糟。.NET 框架的核心是分布式编程，从理论上讲，会进一步加大来自分布式黑客攻击、病毒和拒绝服务攻击的威胁。

.NET的第二个支柱是改善用户体验。通过.NET，Microsoft 试图在增强功能的同时，提高产品易用性。在很大程度上，这是对公共关系的一个挑战。.NET确实能增强用户体验，但假如存在安全问题，会使其黯然失色，就很难将其作为卖点进行大力宣传。

本书重点讨论.NET的第三个支柱，即为.NET概念指明方向的基本操作系统。.NET Server 不仅是一个支柱，还是整个.NET 框架赖以生存的基础。本书讨论了.NET Server 安全结构，并讲解了如何使企业免受黑客的侵害。

.NET Server 经常被作为一个常规术语使用，它覆盖了 Microsoft 的所有企业管理工具，包括 Exchange Server，SQL Server，BizTalk Server 等。但真正的“Windows .NET Server”只是我们所熟悉的一种基本 OS。它是在 Windows 2000 Server 基础上发展起来的下一代产品。

由于易被攻破的客户端是安全服务器最大的突破口，所以本书也介绍了 Windows XP Professional，它是.NET Server 首选的客户端。具有讽刺意味的是，随着人们越来越

普遍地使用经由 IPSec 加密的“隧道”(虚拟专用网络),远程的、功能较弱的客户端也会打开一个后门,黑客可通过它抵达企业网络的心脏。既然有一个无人防守的后门可供进入,为何还要如此费劲地攻打一个守卫森严的堡垒正门呢?为此,本书还强调了 Windows XP Professional 特有的一些安全问题,它们可能会对.NET Server 有负面影响。

Windows .NET Server 是 Microsoft 在服务器市场,为遏制 UNIX/Linux 而推出的。至于两种平台哪一种更有优势,安全性可能是决定一切的因素。由于.NET Server 提供了大力改进的安全体系结构,所以 Microsoft 第一次有了获胜的机会。

本书面向的读者

如关心自己的 Windows .NET企业的安全,应阅读本书。网管、经理、超级用户和 IT 安全顾问如果要部署或即将升级到 Windows .NET,也可参考本书的内容。

和 Windows .NET平台本身一样,我们也使本书的内容能根据实情进行扩展。通过将各章分解成较小的、富有条理的部分,可对本书的信息进行更细的理解和消化。如果您是一名网管,对以前版本的 Windows 有丰富的经验,可浏览一下章节标题,了解哪些是 Windows .NET Server 安全领域的新内容。例如,第 10 章“智能卡”列出了通过 Microsoft公司认证的智能卡阅读器,它们能与最新的 Windows 服务器系列兼容。类似地,如果您是一名超级用户或小型企业主管,正在为网络安全问题而忧虑,也可参照本书的示范步骤进行操作,试着去战胜黑客。

这是市面上第一本全面讲述 Windows .NET Server 平台安全问题的书。除 Windows .NET Server 之外,本书还探讨了有关客户端安全的一些重要概念。甚至用独立的章节,讲解了远程桌面和影响 Windows XP 专业版平台的其他关键问题。

迟早都要把现在的网络升级成 Windows .NET。Microsoft 把 .NET 定义为其以前所有操作系统的一个替换产品。然而,要想安全升级,必须全面掌握最新的安全特性。所以,本书提供了其他地方不易找到的大量第一手 .NET Server 材料,其中包括对位置敏感的防火墙/连接共享、VPN 安全性以及最新的“加密文件系统”(EFS)。除此之外,还探讨了如何对付一些新的以及正在成形的安全威胁,比如怎样锁定无线网络,以防范 802.11b 黑客(战争驾驶)。考虑到广大读者的迫切需要,本书还增加了篇幅较长的第 13 章,讲解如何保护 IIS 6 Web 服务器。第 15 章,甚至面向执行人员,讲解了一些高级的反间谍技术。

本书假定读者具有基本的网络知识,经验多寡并不重要,任何人都能从中找到适合

自己的信息。本书的目标读者是中、高级从业人员。读完本书后，应能在任何规模的网络中，充满自信地管理 Windows .NET Server 的安全性。

本书的特色

本书宗旨是提供最好的指导，帮助您有效保护 Windows .NET企业的安全。为此，我们通过各种方式使这本书大为增色。本书的一些特色包括：

- 提供逐步骤的指导，帮您锁定 Windows .NET服务器。
- 展示如何比 Bugtraq 还要提前 7 天掌握黑客情报。
- 解释如何设置安全的 . NET 虚拟专用网络(VPN)。
- 展示如何对 Windows XP 新的远程桌面特性进行安全保护。
- 介绍如何防范最新的 802. 1x 无线黑客攻击。
- 详细介绍如何保护 IIS Web Server 的安全，其中大部分内容以最新的 IIS 6 为基础。
- 提供大量建议，帮您挑选和安装通过认证的 Windows .NET兼容智能卡。
- 支持在线“Ask the Author”功能，便于您从作者那里直接获得帮助。

本书能提供的帮助

本书将帮助您在 Windows .NET安全领域打下一个良好的基础，并针对各种安全需求，提供快速的解答。各章进行了有序的组织，所有部分都易于查找和参考。本章首先概述了 Windows .NET安全性的新特点。接着，第Ⅱ部分介绍了新的远程管理工具，即“远程桌面”和“远程协助”。同时，提供了大量的安全提示，便于锁定系统，防范黑客。第Ⅲ部分讲解如何在网络客户端保证安全，展示了如何有效地保护 Windows XP 专业版平台。除此之外，还介绍了如何设置和保护无线网络，防范那些移动中的黑客。第Ⅳ部分重点讲述 Windows .NET Server 的安全结构，并通过大量实例，指导您逐步完成和安全有关的配置。最后，第Ⅴ部分强调了 Windows .NET和 Internet 安全问题。在此将学习强化自己的 IIS Web 服务器，甚至会学到一些反间谍技术，以便深入黑客群体，和黑客交朋友，掌握第一手情报。

为增强本书的可读性，每章开头都列举了关键主题。此外，用以下图标使读者便于识别关键的安全提示或警告。

提示

给出重要或有用的提示，便于配置 Windows .NET安全性。

警告

针对潜在的安全隐患或错误的配置，发出警告。

目　录

第Ⅰ部分
Windows .NET安全导论

第1章 概 述

1.1 战争驾驶

周五晚上是我们的“狂欢之夜”。我们像幽灵一样潜入黑沉沉的街道，冰冷的空气丝毫没有降低我们的热情。今晚，我们要把达拉斯黑掉！

蜷缩在一辆多功能运动车里——黑色的车身，浅色的车窗——伸出窗外的奇形怪状的天线，里面的人不知在干什么勾当。车子沿着理查森电信公司外面一条路缓缓滑行，在一台笔记本电脑发出的微光中，我们脸上都闪烁着期待的神情。几乎马上就开始了，网络安全的壁垒在我们周围像冰一样融化。只过了一小会儿，这个城市最大的网络便展现在我们面前。Nortel——28个访问点——全部向我们敞开。再开远一点，我们的天线发出了快乐的嗡嗡声。富士通、爱立信、阿尔卡特……几百个没有安全措施的门户就这样一个接一个在我们面前暴露出来。有的进行了加密，但未免太脆弱，大多数连最起码的密码都没有。我们知道，它们是我们的了。我们觉得自己在上升，高高盘旋在这些钢筋混凝土构筑的建筑物上方，我们凝视着它们，带着嘲弄和怜悯的眼光。然后，我们进入了……

——原文摘自 www.dalascon.com

1.2 现状分析

1.2.1 正在浮现的威胁

拜黑客所“赐”，信息安全已成为目前发展速度最快的一个技术领域。安全已变成价值数十亿美元的一个巨大产业。所以，对公司而言，能确保网络安全的网管是一笔巨大财富。对于网管，学习和掌握信息安全技术，则可提升自己对于公司的价值。此外，在就业市场，个人价值也会大增。安全专家是目前迫切需要的人才。据权威机构的预测，安全咨询产业会以每年35%的保守速度，迅猛增长。