• 设计 • 实现 • 管理

IIS

安全技术

- 配置和管理安全的IIS Web服务器
- 获取实用的建议，以防御新型的IIS攻击，包括：缓冲区溢出、跨站点脚本执行、ISAPI扩展和蠕虫等
- 展示有用的工具和行业最佳安全实践
- 学习使用IIS身份验证、加密、授权、筛选、限制和其他主要安全功能

Marty Jost
Michael Cobb 著
肖国尊 杨征 王元钢 译

Mc Graw Hill

清华大学出版社

IIS 安全技术

Marty Jost
Michael Cobb 著

肖国尊 杨征 王元钢 译

清华大学出版社
北京

北京市版权局著作权合同登记号：01-2002-4657

内 容 简 介

本书专门介绍了 IIS 安全技术。本书的第 I 部分首先介绍了网络在给人们带来便捷的同时所带来的不安全因素，并着重介绍了 IIS Web 服务器所面临的安全问题以及应该采取的预防措施。第 II 部分按照 Web 站点的生命周期分别从站点的规划、设计、实现、后期运行等方面阐述了各个阶段所面临的安全问题及其解决方案。第III部分则介绍了一些比较高级的安全主题，包括 Windows NT/2000 上的服务以及活动目录的安全性等。由于 IIS Web 站点的安全是一项系统工程，它需要综合运用一整套技术，所以这样一本全面的、专门的介绍书籍是非常实用的。

本书适合于希望了解并掌握 IIS 安全技术及其解决方案的 Web 站点管理人员和设计人员阅读。

EISBN：0-07-222439-8

图书在版编目(CIP)数据

IIS 安全技术/(美)约斯特，(美)科布著；肖国尊，杨征，王元钢译. —北京：清华大学出版社，2003
书名原文：IIS Security
ISBN 7-302-06607-8

Ⅰ.I… Ⅱ. ①约…②科…③肖…④杨…⑤王… Ⅲ. 互联网络—网络服务器—安全技术 Ⅳ.TP368.5
中国版本图书馆 CIP 数据核字(2003)第 032610 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.com.cn
责任编辑：陈宗斌
封面设计：康博
版式设计：康博
印 刷 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　**印张**：22　**字数**：563 千字
版　　次：2003 年 6 月第 1 版　2003 年 6 月第 1 次印刷
书　　号：ISBN 7-302-06607-8/TP・4948
印　　数：0001～3000
定　　价：48.00 元

前　言

新闻媒体经常在突出位置报道新病毒的出现、入侵和一些不幸的公共机构或公司所遭受的窃取事件(这些机构或公司的站点缺少恰当的安全)。这些新闻听起来让人感到有些惊慌，而这还只是您所听说过的新闻。有谁知道有多少站点由于认证或目录安全存在缺陷，而丢失代价昂贵的数字资产或知识产权呢？这些损失甚至有可能是这些站点的 Intranet 上的雇员所造成的，只是他们不知道罢了。

那么，该怎么办呢？不再使用 Internet 还是关闭自己的 Web 站点？当然不能这样。如果关闭 Web 站点并且不再使用 Internet，那么您在业务上又怎么跟别人竞争呢？很明显，应当采取相应的对策，解决的办法是了解存在的威胁和弱点，然后采取恰当的措施来减少风险。

本书是一本指南性书籍，介绍了读者应当知道的有关站点安全的需求、方法、实践和过程，其目的是帮助您保护自己的 Microsoft IIS Web 站点，使其不成为下一个不幸的受害者。与此同时，我们进行了逐步的阐述，解释如何使用由 Microsoft 提供的安全特性。然而，我们认为应当在安全方面采取更为广泛的方法，因此我们将用比较多的篇幅来讨论 Web 安全措施，以便帮助您计划并实现安全，从而保护所有与其 Microsoft IIS Web 环境进行交互的系统和应用程序。

保护 Web 环境并非只需要在 Web 服务器上进行少数非默认特性的配置，还需要计划、实现、测试、维护和监控的协同工作，以达到整个系统的安全。我们编写本书的目的是提供一些背景知识，这些背景知识将有助于您构思与实现一个用来保护自己的站点的实用和可行的安全框架。因此，我们在本书中会花费一些时间来解释站点面临的危险、为避免这些危险应遵循的最佳安全专业习惯、安全专家使用的许多工具、这些工具的配置及帮助组织机构时刻保持警惕的一些方法。

我们将这本书分为 4 个部分，前 3 个部分讲述了上面的所有问题，此外，我们还在本书的第Ⅳ部分介绍了一些附录和一个参考表，在您学习完本书之后，这些附录与安全设置参考表可能有助于您继续有关安全的研究。

第 I 部分　暴露、风险与预防

第 I 部分提供了一些背景知识，这些背景知识将帮助您了解一些常见的 Web 站点弱点、解释黑客的工作原理，并仔细分析攻击事件以展示站点上的入侵可能发生的方式。这些信息将为对防御策略的相关讨论打下基础。

在第 I 部分的阐述过程中，我们会讨论如何设置和加固服务器并对硬件和软件配置提供一些建议。您还将看到如何克服一些已知的弱点，并知道在 Internet 和 Intranet 上应该开展一些什么工作，而哪些工作是不应该做的。

第 1 章“Web 安全威胁”将讨论并对 Web 站点所面对的所有外部和内部威胁进行分类。在这一章中，我们将定义和解释各种类型的安全事件。您将进入一个黑客的世界，并且能够透视这些事件的发生过程。这一章的讨论将列出黑客使用的方法、工具和资源。

第 2 章“丑化、破坏与拒绝”将分析一些由黑客发现的最常见的 Web 站点弱点。本章的讨

论将考虑恶意代码攻击(如病毒、蠕虫和特洛伊木马)。示例和案例研究将分析一些众所周知的攻击方法，如缓冲区溢出和分布式拒绝服务攻击。我们将解释为什么这类攻击方法中的一些方法能够攻破某些保护机制，同时我们还将提供一些工具和步骤来帮助防止发生危及未来安全的事件。

第 3 章“准备与加固 Web 服务器”将阐述如何排除常见的管理疏忽、易受攻击的默认设置、为未经授权的入口打开通道的错误配置、信息窃取、数据修改以及恶意代码或程序的引入。这一章将逐步展示如何排除漏洞，排除方法包括：最初禁用所有的服务，而只启用需要的最低限度的服务，然后只在应用程序需要时才添加相应的服务。在这些过程中，我们会讨论每种服务的作用，以便帮助 Web 管理员完全理解配置所带来的后果。第 3 章还将讨论如何使用 Microsoft 工具和核对清单来设置安全的底线，并提供最好的实践建议来对这个基础加以改进。

第 4 章“账号、授权和安全策略”将讨论物理访问限制、多级管理、目录安全以及站点上角色的权利与权限。您将需要进行匿名用户账号和认证机制的配置。我们将特别注意 Windows 2000 和 IIS 中的账号管理、授权和访问控制。

第 5 章“安全审核与日志”将讨论对日志与审核特性的配置，目的是监控 Web 站点，从而检测攻击或入侵的迹象。我们将学习如何设置和配置安全日志文件以及如何开展维护过程。这一章同时包括了审核设置的每个过程，这样您可以建立一种正当的、可实施的(您的站点上的)用户活动审核跟踪方法。

第 II 部分　管理

第 II 部分讨论在第 I 部分中没有包含的计划、策略和过程的实现。这一部分包含了使用 Microsoft IIS 来配置安全的网络以及 Web 环境的其他细节，并将提供许多与安全问题有关的建议。

第 6 章“部署问题”包含在将站点投入使用之前最后要进行的准备工作。本章将讨论最后的检查、备份和恢复措施，这些措施对于确保 Web 服务器配置正确是必需的。这些讨论将包括域的安全、流量过滤以及对 Internet 地址的屏蔽。在这一章中还将讨论用于边界防护的 DMZ 的正确使用方法，以此来增强您在第 1 到 5 章中学习到的安全措施。最后，这一章还将讨论将站点托管在 ISP 或需要托管服务时所需的远程管理。

第 7 章“安全管理的生命周期”将介绍站点的后期部署(post-deployment)——管理生命周期，并将讨论用于监控 Web 站点状态的方法和工具，以及如何对可能的攻击加以应对。我们将讨论 Web 站点的正常配置方法，并对使用系统警告和其他特性与工具提供建议，以此来帮助您系统地掌握方法。这一章还包括用于响应安全事件的建议以及一些最好的习惯。我们还讨论了审核，通过审核可以跟踪和识别站点有可能遇到的破坏以及产生这些破坏的原因。

第 8 章“加密应用”将讨论 Windows 2000 和 IIS 可以用来保护站点和站点内容的加密特性。在这一章中，我们解释了加密系统、公钥加密术、数字证书和公钥的基础结构。您将学习如何获取和安装 Microsoft 和第三方数字证书。最后，您将学习如何配置 IIS 服务器上的 SSL 和/或 TLS 加密会话。

第 9 章“使用第三方工具增强安全”将集中讨论可以用来增强 IIS 的物理安全、软件安全

和日志与审核功能的大多数非 Microsoft 硬件和软件产品，这些产品包括防火墙、VPN、日志分析器、加密加速器等等。

第III部分　高级主题

在您已经成功安装和配置了基本的 IIS Web Services 之后，还存在大量您可能添加到 Web 站点的其他服务、介质和特性，这些服务、介质和特性同样必须进行安全配置。这一部分包含这些高级服务和功能，以及保护这些服务和功能可以采取的措施。

第 10 章“保护 FTP、NNTP 和其他 IIS 服务”将概要地描述安全使用 IIS FTP、NNTP 和 SMTP 服务、Windows Media Services 以及 FrontPage 服务器扩展的过程。

第 11 章“活动内容安全”将讨论用于保护交互脚本(可添加到 Web 站点中，为站点提供更为新式的和动态的画面)、服务器页面和应用程序的方法和工具。这一章中将要学习的安全技术可以帮助确保活动内容的部署，而不是损害 IIS 服务器的安全。

第 12 章“Web 隐私”。隐私是一个与安全相关的主题，它是 Web 站点的衍生物。许多 Web 站点保存有关顾客和客户的详细信息，您要在自己的站点上提供业务和法律上的可信度，维护这些信息的保密性，并进行适当的管理。本章会讨论这个问题，并对如何处理隐私管理提供实用的建议。

第IV部分　附录

第IV部分提供一些帮助和资源信息，这些信息应该可以使您对本书中学到的内容加以充分利用。以一种安全的方式安装和配置 Web 环境只是安全管理过程的一部分。因为您是自己的 Web 环境的保护人，在管理自己的 Web 环境的过程中应当具备勤勉的态度，尽可能提前采取措施。

附录 A“安全资源”。只靠一个人的力量保护一个站点是远远不够的。本附录将为您介绍其他的安全资源、专业组织、培训和公共域信息的网址，获取它们的信息有助于您及时了解最新的安全威胁、提示、研究、产品、培训和其他有用信息。

附录 B“词汇表”提供了许多安全术语，这些术语不一定出现在本书中，但在安全文献中比较常见。本附录还包括这些术语的首字母缩略词，以此来帮助查找(在本书中或者您所看到的其他安全信息中遇到的)某个术语的定义。

附录 C 安全设置“参考表”，正如这个标题所示意的那样，这个附录(为了方便)通过表格列出了 Windows 2000 和 IIS 的访问控制、审核以及其他安全设置。

附录 D“Microsoft IIS 认证方法”。在第 4 章中，除了提到匿名认证外，我们只是简略提到了 Web 站点的认证设置，而这个附录中对此进行了深入讨论，这是因为这些认证方法是特定于 Windows 环境的。这个附录完善了第 4 章中关于 Web 站点认证的讨论。

小结

在安全方面，有一句比较好的名言(但笔者不记得出处了)，“安全是一段旅程，而不是目的地”。解释一下这句话，安全是一个不断完善的过程，在这个过程中，您运用自己的知识和经验来部署(您可以提供的)最好的保护措施，然后根据状态变化来监视和调整这些措施。在本书中，我们已经尝试帮助您打下必要的知识基础，以便您为自己的 Web 站点规划、部署和管理一组实际的和合理的安全措施，这样，您就可以开始您的安全之旅了。

关于作者

Marty Jost 是一位有经验的安全专家与顾问，擅长于 Windows NT/2000、IIS、防火墙、PKI 及认证。他经常在业界的安全会议上发表演讲，并且已经出版和发表了若干关于计算机网络和安全的书籍和文章。

Michael Cobb(MCDBA、CISSP)是一位公认的信息安全专家，他有显赫的金融系统背景，擅长网络、数据库和 Internet 安全。作为 E-Business Security Advisor Magazine 杂志的有贡献的编辑之一，Mike 定期报告最新的安全技术和威胁。

致谢

我要向本书的合作者 Mike Cobb 表示感谢，谢谢他的努力工作和贡献。感谢我的好朋友 Stephen Cobb，他提供了第 12 章中大量关于 Web 隐私的材料。感谢 Matt Berry，谢谢他对本书中的细节表现出的耐心与重视。感谢 Marjorie Jost，谢谢他对本书所作的最后的润色。感谢 Osborne 的优秀人才，他们一直跟踪和关注着这本书的整个出版流程。

目　　录

第 I 部分　暴露、风险与预防

第II部分 管　理

第III部分　高 级 主 题

第Ⅳ部分　附　　录

第Ⅰ部分　暴露、风险与预防

第1章　Web安全威胁

Web 站点是组织机构面对世界的界面。对于客户而言，Web 站点给出了商标和产品信息。它是一个营销与支持工具，用于同客户进行交流。对于雇员而言，Web 站点是他们可以发现新闻和有关福利与培训材料信息的场所。组织机构的合伙人可能将其用于许多信息收集目的。简而言之，Web 站点是客户、雇员和重要的第三方借以实现交易的信息中心。因此，很自然，对 Web 站点进行保护是很重要的，不仅仅是保护 Web 页面，还应当保护站点所连接的任何东西；通过网站显示、发布和收集的所有信息；还可以是为客户保留的图像。

本书的目的是向读者展示如何保护 Microsoft Internet Information Server(IIS) Web 站点及其服务，确保它正确执行其关键的功能，避免由于安全破坏而引起负面的客户影响或营业亏损。归根结底，我们希望帮助您为您所在的组织设计一个安全框架，该安全框架将针对(您的 Web 站点在 Internet 世界中所面临的)威胁来保护它，这些威胁可能是已知的，也可能是未知的。开始设计该框架的最好方法是详细考虑安全威胁，从而获得一些认识，这些认识将有助于您计划最终的防御方案。

1.1　安全事件

您可能记得一个称为 Code Red(红色代码)的恶意蠕虫程序的快速传播特征。这种特殊蠕虫的传播方式是：首先感染一个服务器，然后从这个服务器开始自动向其他附近的服务器发动攻击，最终传播到成千上万的 Microsoft 操作系统。Code Red 设计的目的是用数据来泛洪 Web 服务器，它可以如此成功地泛洪 Web 服务器，以致它能够导致 Internet 上的大部分网站关闭，因为站点由于数据泛洪而过载，无法对这些数据进行相应的处理。

像 Code Red 这样的蠕虫只是用来妨碍、破坏 Web 的正常工作，或者从 Web 进行窃取的许多知名方法之一。因为这些威胁是无法改变的事实，所以 Web 管理员必须要么准备随时排除威胁来保护他们的站点，要么等着遭受由这些威胁所带来的后果。

1.1.1　威胁源

从 Code Red 事件可以看出 Web 服务器受 Internet 袭击的容易程度。您还有可能通过阅读信息来获悉 Internet 上的公司间谍、信息战、计算机恐怖主义以及有组织的犯罪。确实，在 Internet 上存在许多威胁和坏家伙。

安全警告

威胁可以存在于组织内部，也可以存在于外部，组织内部的威胁同样可怕。在花费了大量的精力和资源来确保对外部威胁进行防御后，还可能让自己暴露在恶意的内部用户面前，使自己易受内部用户的攻击。

根据美国联邦调查局提供的情况，安全管理员通常忽略这样一个事实：大多数的计算机犯罪都是由组织机构里面的成员和雇员所为。内部保护不充分可能是一种代价惨重的失误。假设某个人可以获得对 HR Web 内部站点的机密薪水信息的访问权，即使这种安全问题是由于普通的过失(如对文件目录没有加上充分的限制)所引起的，考虑一下这种情况会导致什么样的后果。我们是不是应该讨论一个不满的或者不诚实的雇员可能通过欺骗、窃取或怠工等手段所导致的破坏？很清楚，在您的 Intranet 上，对企业的威胁和对安全的需求是一个严重的问题。

1.1.2 事件分类

对 Web 站点的安全威胁可以分为几种事件类别。有些事件可以影响站点的可访问性和可靠性，这些事件通常属于拒绝服务式(Denial of Service，DoS)事件。Code Red 事件是 DoS 的一个很好的例子。其他事件则可以对站点内容和数据产生消极的影响，因为入侵者会设法破坏、欺骗、探听、窃取、修改或者存储站点上的一些信息。这样的事件通常称为破解(cracking)事件。

破解(hacking)描述 DoS 事件犯罪与破解事件犯罪的术语。为了您参考的方便，我们将美国国家安全局(National Security Administration)所提供的术语表中的一些术语(在附录 B 中包含了一个不完整的形式)列在下面：

- 拒绝服务(Denial of Service) 是一种行为，它使得自动化信息系统的任何部分的功能与其预期目标不一致。
- 破解(Hacking) 绕过计算机信息系统或网络的安全机制的未经授权的用法或尝试。
- 破坏(Cracking) 侵入计算机系统或者网络的行为。

“攻击(attack)”一词常用于描述破解事件的过程。在 DoS 和破坏(Cracking)事件中，可以使用许多不同的攻击技术。

提示

在信息技术(Information Technology，IT)和学术界中的一些人认为破解(hacking)与破坏(cracking)具有明显的不同，因为黑客(hacker)(与骇客(cracker)相对)的动机不是恶意的。黑客相信通过暴露弱点可以帮助受害者，从而使受害者在遭受任何真正的伤害之前进行安全加固。我们当然相信：随着组织机构对其 IT 产品中的缺陷知道得更多，安全实践水平也就会相应提高。我们一直试图确定一个通用的、无歧义的破解(hacking)的定义。

1.1.3 社会攻击和物理攻击

黑客和骇客在获取对受口令保护的系统的访问权限时，他们使用的最有效方法之一是：获取不受怀疑的个别人的信任，获取信任的途径是：他们假装是需要这个用户的口令的技术支持人员。社会工程(*Social engineering*)是用于描述这类攻击技术的术语，它基于对人类行为的探索和操纵来达到目的。