CISCO SYSTEMS

ciscopress.com

Web 安全实践

Web Security Field Guide

Hands-on techniques for securing Windows® servers, browsers, and network communications

[美] Steve Kalman 著
冯大辉 姚湘怡 译

人民邮电出版社
POSTS & TELECOM PRESS

Web 安全实践

[美] Steve Kalman 著

冯大辉 姚湘怡 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

Web 安全实践/（美）卡尔曼（Kalman, S.）著；冯大辉，姚湘怡译.
—北京：人民邮电出版社，2003.12
ISBN 7-115-11934-1

I. W… II. ①卡… ②冯… ③姚… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2003）第 099847 号

版 权 声 明

Web 安全实践

◆ 著 [美] Steve Kalman
译 冯大辉 姚湘怡
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 ciscobooks@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：27.75
字数：669 千字 2003 年 12 月第 1 版
印数：1-4 000 册 2003 年 12 月北京第 1 次印刷

著作权合同登记 图字：01－2002－3667 号
ISBN 7-115-11934-1/TP・3761
定价：55.00 元

本书如有印装质量问题，请与本社联系 电话：(010) 67129223

内容提要

本书提供了有效的、经过验证的解决方案，以修补端到端网络安全架构中的 Windows Web 服务器和浏览器的常见脆弱之处。本书分为 5 个部分。第一部分是基本背景信息概述，帮助读者实现能够实际应用的网络安全规则与策略。第二到第四部分讲授加固操作系统、Web 服务器和浏览器的技术。第五部分专注于全面的网络安全，着重点在阻止与控制访问上，对成为认证机构、Cisco PIX 防火墙、Cisco IOS 防火墙、访问列表、持续的安全维护以及测试等话题都作了深入的分析，提供了一个能有效地减少企业系统和数据的风险的全面网络安全方案。

本书避免了基本技术的概念性的讨论，而是使用了平实的语言和大量的逐步操作的例子来演示如何保护网络并阻止网络攻击。本书适合负责公司网络安全的网络管理员、系统管理员及其他网络安全技术人员阅读。

献　辞

本书特别要献给致力于公共服务的两个人。

第一个是我的妻子 Gail。她是一名特殊教育教师，为那些有身体或情感障碍的孩子工作。她已经为此工作了 35 年多的时间，燃起了数以百计的学生和他们的父母的希望。

另一个是前纽约市市长 Rudolph Guiliani。在我们最危急的时刻，他体现出了肯尼迪、罗斯福和丘吉尔等国家领导人那样的才干。他给予了我们信念、信任、爱和支持。他不顾个人安危，引领国家走出了黑暗。他成了全美国的市长。

Steve Kalman

于宾夕法尼亚州 Lords Valley

致　谢

当我决定要写这本书时，我给 Cisco Press 的执行编辑 Brett Bartow 发了一封很短的 E-mail。我们已经共事多年，我曾经为几本 Cisco Press 的书做过技术编辑。在那封信中，我问他是否能为出版一本网络安全的书介绍一家出版社，根本没想到 Cisco Press 会对此感兴趣。Brett 立即回复并说我们可以一起做，这样我们就开始着手书的大纲。我很高兴能为 Cisco Press 写书。当你和最好的伙伴合作时总是一段愉快的经历。谢谢你，Brett。

我请求 Brett 做的第一件事就是委任 Chris Cleveland 作为开发编辑。我是从以前的 TE 工作中认识 Chris 的，我很敬重他的技术和奉献精神。现在，作为作者，我看到了他对我发给他的原始材料所做的大量工作。一致性是技术写作中的基本要素，Chris 确实为本书在幕后做了极其大量的工作。

没有一个作者能唱独角戏。好多人和公司在这个项目完成的过程中起到了关键的作用。其中有 Adrian Bryan，他是 Learning Tree 网络安全课程的作者。我也一直讲授这门课程，该课程是本书的灵感之源。Adrian 慷慨地给我提供了附录 B 的材料。

Addie Sheridan 是我的一个学生。给她授课的时候我仍然在想是否做这个项目。当我向她提起这件事，她说“最终，这是一本我们可以实际使用的书”。这真是一句警言。希望我已创作了一些能够称得上实用的东西。

Peter Vogel 是 Learning Tree 教程的技术作品的作者，他用了高强度的 4 天培训我把一本白皮书变成类似于本书所需要的技巧。他教给我的许多知识都提高了这本书的可读性。

Grant Moyle 和 Mike Covington 帮助我完成了最初的大纲。

我为 Learning Tree 讲授关于路由、电信和安全的课程。这给了我机会去更多地了解对学生们来说哪些方面容易或难于理解，以及哪些技术对他们来说更重要。还要感谢创建这家公司的 Eric Garen 和 David Collins，是他们给了我同如此多的行业优秀专家合作的机会。

感谢 ISS 允许我用它的产品作为安全扫描的范例。

感谢 Sanctum 公司允许我用 AppShield 产品来演示网络内容的不安全性。

感谢 Rhinosoft 允许我使用他们的 FTP 安全服务器和客户端软件。

感谢美国安全协会创建了一个有大量极好的实例总结的站点，我采用、编辑了站点的内容并根据本书的读者进行了重新的设计。

感谢技术编辑 Carl、Hank 和 Boles，他们的审校使一切变得不同。他们坐在计算机前好几个月来解决本书的编辑任务问题——跟踪了所有的步骤，提供建议并纠正错误。余下的是我个人的错误，但是我感激他们做得如此好的工作并把所有正确的荣誉给予他们。

最后，毫无疑问最重要的是感谢我 25 年来的贤妻 Gail。当我的工作接近最后期限的时候，我几乎排除了任何其他的事情而全身心地投入到这一任务中。当我们谈话时，我的思维转到一些我应该写或应该写得更好的事情上的时候，她理解并给予支持（她把这称为“程序员模式”——只是把比萨饼从门下滑进去，然后等待他出来）。没有她坚定的支持，我的成就是不可能的——也是毫无意义的。谢谢。

关于作者

Steve Kalman 是 Esquire Micro 顾问公司（该公司提供演讲、撰稿和咨询服务）的主要官员。他在数据处理方面有 30 多年的经验，并具备网络设计和实施的实力。Steve 是 Learning Tree International 的教师和作者，曾撰写并审校过许多与网络相关的文章。他拥有 CISSP、CCNA 和 CCDA 认证证书。

关于技术审稿人

Hank Mauldin 是 Cisco 公司的顾问工程师，为 CTO 办公室工作。他在 Cisco 工作了多年，评估并进行数据网络的设计。他专长的领域包括 IP 路由协议、服务质量及网络安全。Hank 目前是网络设计工具 Cisco Network Designer 的程序经理。在加盟 Cisco 之前，他曾为几家不同的系统集成商工作过。他有超过 15 年的数据网络工作经验。Hank 住在加州的圣迭戈。他获得了乔治·华盛顿大学信息系统技术的硕士学位。

Carl Smigielski 是罗得岛州 Newport 的 Aquidneck 管理协会的一名高级网络工程师。Carl 为军事客户——包括美国海军下属的作战中心——开发 IT 安全解决方案，写过已获奖的海军罪犯研究中心和其他研究机构日常使用的安全分析工具。Carl 讲授关于网络安全技术方面的课程，包括入侵检测、加密、PKI、Web 安全、虚拟专用网和防火墙等。

Boleslav Sykora 是一个著名的安全专家。他做关于网络和系统安全问题的咨询，处理的问题包括入侵检测、脆弱性评估、突破测试、防火墙、VPN、Web 服务器以及 PKI 等。他也在 Learning Tree International 针对这些问题进行授课，在那里他写了关于入侵检测和 Cisco OSPF/BGP 路由方面的教程。Boles 是一名电子工程师，并持有 CISSP 认证。

前　言

似乎每一两天就有关于新的攻击或安全漏洞的报道。管理员们被告知应该采用什么样的补丁或采取什么样的措施。面对如此多的安全警告，我们已经变得不为所动，就像我们面对报纸和电视上报道的重罪的冗文毫无反应一样。而名列 2002 年春季3个月前10名的KLEZ病毒本可以提早用一个叫fourteen months的补丁来预防。

大多数网络管理员所做的事情都如同没有上保险的驾驶。这不是他们没有能力或者不谨慎，对他们的要求就是在今天显示出积极的结果——扑灭正在燃烧的火。他们没有奢侈的时间去创建防火计划。

本书为他们而写，书中用平实的语言配以大量范例说明了如何保证 Web 服务器的安全，以及如何保护网络使其免受大量的攻击。

本书重点

本书集中讨论要做什么和如何去做，而不是它如何运行。本书的读者是那些要对安全负责却没有足够的专门时间去培训如何正确地做这项工作的管理员。这些读者需要的是解决方案而不是理论，本书就提供这些解决方案。

在假定读者只阅读和他们有关的那部分内容的前提下，一些材料有必要重复。偶尔这些重复在同一章节里（IIS4/IIS5 安装就是一例）。其余情况下，这样的内容会跨越几个章节（证书在 3 处被描述和定义——虽然是在不同的上下文环境中）。

读者

本书的主要读者是那些对公司网络的许多独立的部分负责的网络管理员——在较大的公司中，这一工作可能由几个人来负责。本书假设这些读者群更愿意学习如何做而不是学习为什么。为了使向导部分容易理解，许多技术话题都用充足的信息来处理。

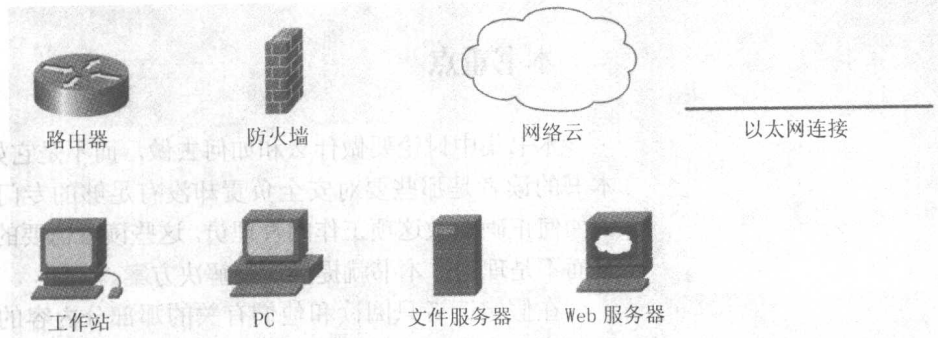
命令语法规定

本书中用于介绍命令语法的规定如下：

- 竖线(|)表示两个单独的选择，互斥的元素。
- 方括号[ ]表示可选的元素。
- 花括号{ }表示一个必须的选择。
- [{ }]表示在一个可选的元素中必须的选择。
- **黑体字**表示按照字面输入的命令和关键字。在实际的配置范例和输出中（不是一般的命令语法），黑体字表示用户手工输入的命令（如 **show** 命令）。
- 斜体字表示你为之提供实际值的变量。

书中的图标

整本书中，你会看到很多用来指示 Cisco 和一般网络设备、外围设备和其他项目的图标。紧接着图标的图例解释这些图标代表着什么。



世界上最安全的计算机是一台完全配置好的机器，然后拔去电源放在塑料袋里，然后再放到银行的保险库中。这也是世界上最没有用的计算机了。如果你负责计算机的安全，应该记住两件事：

第一——你为了提高计算机的可用性所做的每一件事都会降低它的安全性。

第二——这种交替不是一对一的。有些操作降低了一点儿安全性却大大提高了可用性。

另外一些操作大大降低了安全性却仅仅提高了一点点可用性。你的工作就是要倾向于前者而坚定不移地防止后者。在这一部分，你会弥补一些关于数据通信功能方面的知识空白，并学习安全策略的有关内容。

目　录

第一部分　Web 安全基础

第二部分 加强服务器

第三部分 IIS 安装与保护

第四部分　保护用户

第五部分 保护网络