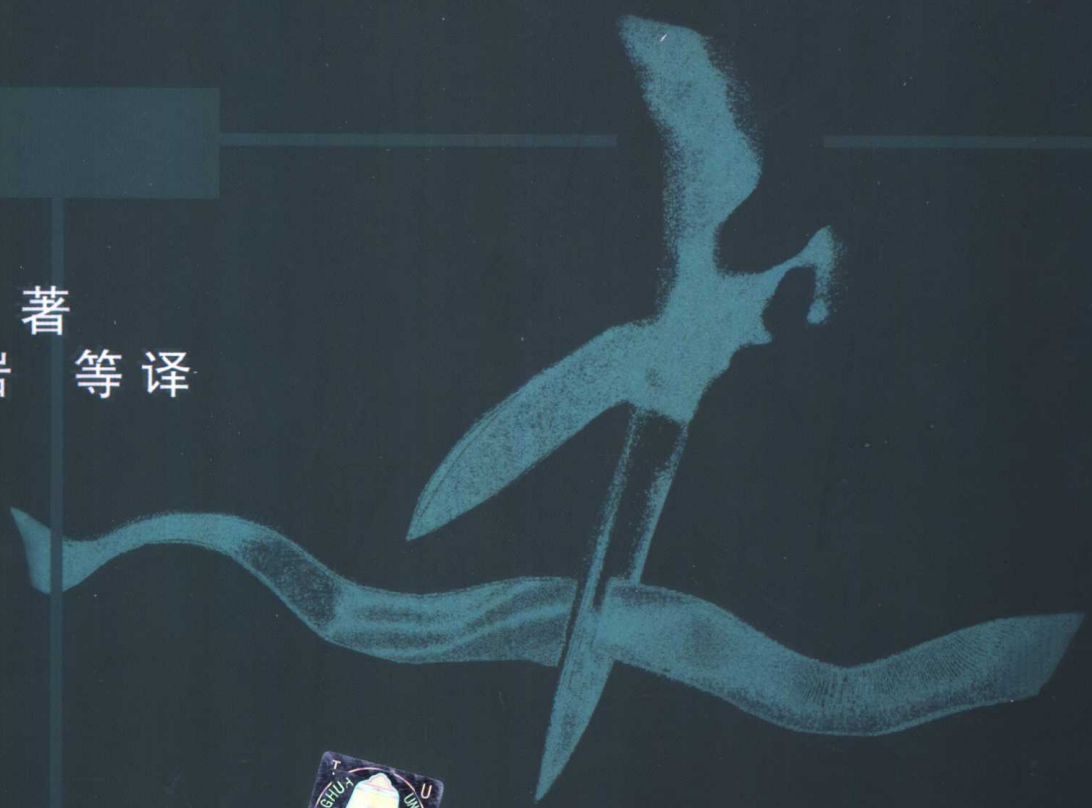
THOMSON

Guide to Network Defense and Countermeasures

网络防御与安全对策

Greg Holden 著
黄开枝 孙岩 等译



清华大学出版社

网络防御与安全对策

Greg Holden 著

黄开枝　孙　岩　等　译

清　华　大　学　出　版　社

北　京

Greg Holden
Guide to Network Defense and Countermeasures
EISBN: 0-619-13124-1

图书在版编目（CIP）数据

网络防御与安全对策/ 赫顿（Holden, G.）著；黄开枝等译. —北京：清华大学出版社，2004.4
书名原文：Guide to Network Defense and Countermeasures
ISBN 7-302-08210-3

I. 网… II. ①赫… ②黄… 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（2004）第 015568 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社总机：010-62770175　　**客户服务**：010-62776969
责任编辑：冯志强
封面设计：付剑飞
印 刷 者：世界知识印刷厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：26.5　**字数**：657 千字
版　　次：2004 年 4 月第 1 版　2004 年 4 月第 1 次印刷
书　　号：ISBN 7-302-08210-3/TP・5927
印　　数：1～4000
定　　价：48.00 元

前　言

进入21世纪，入侵检测成为与保护计算机和网络有关的最重要和最急迫的概念之一，本书将对此进行介绍。

从狭义上来说，入侵检测是硬件和软件提醒用户注意可疑连接企图的能力，这些企图可能就是对计算机及/或计算机上的资源进行未授权访问的企图。本书中有几章内容将广泛论述这一特定功能。

但是从广义上来说，入侵检测的实践实际上包括网络安全的所有方面，本书同样要研究这些活动——如风险分析、安全策略、损失评估、入侵响应、预测将来的攻击和起诉入侵者。

编写本书的目的有两个。第一个目的是为学生在网络安全基础原理方面打下坚实的基础；虽然本书的重点在于入侵检测，但是也涉及到一些必要的实践，如开发安全策略，然后通过执行NAT（网络地址转换）和数据包过滤，以及通过安装代理服务器、防火墙和VPN（虚拟专用网络），实现该策略。第二个目的是为学生参加网络防御和对策考试作准备，这个考试是Security Certified Network Professional（注册网络安全人员）认证考试的第二个考试。

从何入手

本书的读者对象是那些需要具有安装防火墙和入侵检测系统内行实习经验的学生和专业人员。本书假定读者已经对Internet和基本的网络互联概念有所了解，如TCP/IP、网关、路由器和以太网。本书还假定学生符合SC0-402考试的前提条件，其中包括IP故障检修、子网技术、子网掩码、IP数据报结构、路由、Web服务和常见的攻击技术。

本书的第1章和第2章让学生进行复习，其内容包括IP寻址技术、子网技术、路由技术、IP数据包结构以及周边安全配置应当防御的不同类型的网络攻击。第3章~第11章介绍严格定义的安全策略的开发、加密、身份验证、VPN、防火墙和其他有助于入侵检测和对策的安全概念。

本书不需要按顺序进行学习。但是由于前两章详尽地介绍了网络安全，所以强烈建议首先阅读这两章。不过，如果你主要关注的是入侵检测，那么就可以直接跳到第8章~第11章学习。如果主要关注防火墙，可以转到第4章~第6章；如果主要关注的是VPN，可以转到第7章。下面将对每一章进行更详细的说明。

章节说明

第1章　“网络安全基础”，介绍开发网络安全程序的原因，包括黑客、病毒和心怀不

满的员工。本章还分析了网络安全程序的目的，这种程序将连通性和访问的需要与维护隐私权和完整性的需要平衡起来。本章还介绍了在阻挡入侵和攻击中发挥作用的基本TCP/IP网络互联概念，其中包括IP寻址技术、子网技术、IP数据包结构、DNS以及路由和访问控制。本章最后介绍了保护各个工作站的技术，以及维护World Wide Web的安全技术。

第2章 “设计网络防御”，介绍常见的安全威胁，以及需要由入侵检测系统和其他安全设备解决的薄弱点。同时概括介绍了阻挡这些威胁的基本工具，包括数据包过滤器、反病毒软件、日志文件及分析日志文件的软件、入侵检测系统。

第3章 “风险分析和安全策略设计”，介绍基本的但经常被忽略的主题：告诉机构成员开发如何保护系统资源以及在发生入侵的情况下如何响应的安全策略。由于安全策略源自于全面的风险分析和风险评估，所以本章还研究了计算机资源和安全方面的风险分析概念。

第4章 “选择和设计防火墙”，首先介绍如何配置堡垒主机，这是一种受到高度保护的计算机，它运行防火墙或入侵检测系统。本章还概括介绍了不同种类的防火墙及其主要功能，以便你可以根据需要选择正确的防火墙。

第5章 “配置防火墙”，介绍基本的防火墙安全功能——数据包过滤。本章还介绍了防火墙执行的其他通用的安全功能，包括NAT、身份验证和加密。

第6章 “加强和管理防火墙”，介绍代理服务器如何通过影响内部网络上的各个主机来屏蔽它们。本章还介绍了如何管理和定制防火墙所收集的、通常容量很大的日志文件，以及如何提高防火墙的性能。最后介绍了如何安装和启动3种流行的防火墙配置：Check-Point NG、Microsoft ISA Server和iptables。

第7章 “建立虚拟专用网络”，介绍VPN的建立，它为公司通过公共Internet进行安全的通信提供了费用低廉的途径。由于VPN使用加密和身份验证，所以在学习本章以前最好先阅读第5章。

第8章 “入侵检测：概述”，介绍入侵检测的概念，并概括介绍组成典型网络IDS（入侵检测系统）的组件。你要逐步地遵循入侵检测的过程，并学习基于网络的、基于主机的和混合的IDS实现方式的特点。最后，本章将介绍一些可供使用的最流行的IDS程序包，从免费的软件到价格昂贵的、使用多个网络传感器检测可疑通信的硬件系统。

第9章 “入侵检测：预防措施”，深入研究IDS硬件和软件实际用于检测未授权访问企图和阻止它们的方法。本章将特别介绍各种类型的入侵检测签名——标识已知可疑数据包的特性集合。你将学习如何捕获数据包，以及如何比较正常的通信签名和可疑的通信签名。最后本章将介绍如何基于这些签名的独有特性开发过滤器。

第10章 “入侵检测：突发事件响应”，介绍一组人员的开发和活动，这组人员的任务是响应安全突发事件，并将可能发生的损害减少到最低限度。本章将介绍组织这样一个小组的各种选项，以及如何处理发生的假警报。最后，你将了解计算机侦破，以及如何处理入侵的证据，以便在法庭上起诉被告时使用。

第11章 “通过前进式的管理加强防御”，介绍与有效管理现有IDS有关的问题，以便

它不仅能有效地继续运行，而且能继续阻止新的攻击。另外将介绍实时监视，以及通过添加内存、硬件和软件发展IDS，使其跟上不断发展的网络。最后，你将学习如何通过加强你自己的知识跟上快速发展的挑战。

附录A “SC0-402的目标”，描述了在SCP（安全认证专业人员）的SC0-402网络防御和对策教程中规定的目标，并提供了在本书中涉及这些目标的章节的标题。如果你在准备这个考试时需要针对某个特定题目提高，并且想要了解什么地方涉及该题目，你就可以使用这一部分作参考。

附录B “安全资源”，简要介绍了在写作本书时仍然有效的一些与安全有关的主要组织、团体和信息来源。如果你要寻找有关遇到的病毒攻击或者安全问题的最新新闻和观点，你可以看一下这一部分列出的资源。


注意

我们还鼓励读者研究许多有关本书中引用的附加信息的联机和纸面资料来源的线索。

本书特点

为了帮助你充分理解网络互联安全概念，本书加入了许多用于增强你学习经验的特点。

- 每章的学习目标：每一章的开始都详细地列出了在本章中要掌握的概念。该列表不仅可以让你快速查阅这一章的内容，而且可以作为一个有用的学习助手。
- 插图、表格和图：大量互联配置的插图可以帮助你直观地浏览通用的周边防御设置和体系结构。此外，大量表格使用实际和理论信息提供了细节和比较。有些表格提供了可以用于建立防火墙规则库的数据包过滤规则的特定示例。由于大多数校园实验室都使用 Microsoft 公司的操作系统，所以我们将它们的产品用于本书的图和大部分实习项目。
- 每章小结：每章的课文后面都有一个对已经介绍的概念的小结。这些小结对于概述和回顾每一章涉及的理念很有帮助。
- 关键术语：每一章所介绍的所有术语都归纳在该章后面的关键术语表中。这可以帮助你检查对所有已介绍的术语的理解。
- 复习题：关键术语表后面是一组复习题，它们强化了每章介绍的理念。对这些问题的回答将确保你掌握重要的概念。
- 实习项目：虽然了解互联技术背后的理论非常重要，但是没有什么可以比现实世界的经验更好。除了那些纯理论的章节以外，每一章都提供了一系列练习，其目的是为你提供实习的实现经验。
- 案例项目：这一部分是每章的最后一部分，它提出了某些入侵检测和与安全有关的情况。这些项目将要求你评价情况，并决定解决所述问题要采取的一系列动作。这一有价值的工具可以帮助你加强决策和故障检修技术——网络安全系统管理的重要方面。

指导教师的资料

当本书在课堂环境中使用时，可以使用下列补充资料。随本书提供给指导教师的所有补充资料都在一张CD-ROM上，请从www.tupwq.net下载“教师教辅资料申请表”。

指导教师的电子手册：随本书提供的指导教师手册包括辅助课堂准备的附加指导资料，包括对课堂活动、讨论题目和附加项目的建议。

解决方案：解决方案包括在所有的章后资料中，包括复习题。在合适的地方，还包括实习项目和案例项目。

ExamView：随本书提供的ExamView是一个功能强大的测试软件程序包，它可以使指导教师创建和管理纸面印刷的、计算机（基于LAN的）和Internet考试。ExamView包括数百个与本书所述题目相对应的问题，使学生可以获得详细的学习指南，其中包括进一步复习时使用的书面参考资料。基于计算机和Internet的测试组件允许学生在他们的计算机上参加考试，并且通过对每次考试进行自动评分，还可以节省指导教师的时间。

PowerPoint演示工具：本书的每一章都提供有Microsoft PowerPoint幻灯片。它们作为课堂准备的教学辅助工具，可以在网络上供学生在进行章节复习时使用，也可以打印出来，在课堂上分发。指导教师可以任意添加自己的幻灯片，向学生介绍其他的题目。

图形文件：本书中的所有图形都以位图格式复制在指导教师的资源CD上。和PowerPoint演示工具一样，这些文件是作为课堂准备的教学辅助工具提供的，可以提供给学生进行复习，或者打印出来后在课堂上分发。

处理 Web 上的变化

本书中提到的所有基于Web的特定资源迟早会过时，或者被更新的信息所代替。在有些情况下，你将发现书中的URL会把你带到它们的置换URL；而在另外一些情况下，URL不会指引到任何地方，而只是出现404错误消息“File not found”（文件未找到）。

当出现这种情况时，千万不要放弃！如果你愿意花一些时间和精力的话，你总能在Web上找到你想要的东西。首先，大多数大型或者复杂的Web站点会提供搜索引擎。只要你可以到达这个站点本身，你就可以使用这个工具来帮助你找到所需要的东西。

要敢于使用像www.google.com、www.hotbotcom或者www.excite.com这样的通用搜索工具来寻找有关的信息。虽然某些标准组织可以联机提供有关他们标准的最准确和最具体的信息，但是在这一领域还有大量的第三方信息、培训和帮助来源。关键在于：如果你不能在本书介绍的地方找到某些信息，一定要开始四处查看。你肯定能在某个地方找到这些信息！

访问我们的 World Wide Web 站点

在World Wide Web可能存在专用于你们教程的其他资料。请定期访问www.course.com，搜索本书的题目，以获取更多的信息。

致谢

我要感谢Course Technology公司的团队给我提供了创作这本主题如此有价值和重要的书籍，这也是我为他们创作的第一本书。这个团队包括（但不限于）产品经理Amy Lyon；优秀的制作编辑Elena Montillo；质量保证人员Sean Franey和Stephen Connor。还要感谢策划编辑Jill Batistick，感谢她一贯出色的编辑、对我的鼓励以及经常提醒我不要离题。感谢技术编辑Ron Milione，他根据自己的经验，在本职工作之外为我提供了详细的建议。我还要感谢下列评论家，他们对每一章提出的精辟和有益的反馈为我指明了方向：

Timothy Culhane New England Institute of Technology
Max Josquin Spokane Falls Community College
Eileen Vidrine Northern Virginia Community College

特别感谢我最好和最诚挚助手Ann Lindner、我的女儿Lucy和Zosia，她们的耐心的支持使我成功地完成了这个项目。

在开始学习前应当阅读下列内容

本书包含65个以上的实习项目，其中许多项目都需要你安装和使用不同的与安全有关的软件程序。你需要访问一台连接到Internet并且可以运行软件程序的计算机。下面将描述建议的硬件和软件要求。

硬件要求

计算机的CPU至少应当是Pentium II，运行速度为300MHz以上。要运行Check Point NG的话，RAM最少应当为128MB；要同时运行Web浏览器、字处理应用程序和其他应用程序的话，RAM至少应当为192MB（256MB以上的RAM为理想情况），可用硬盘空间最少为75MB。

软件要求

使用运行Windows 2000、Windows XP、Red Hat Linux 7.3或更新版本的计算机，可以完成本书中的大部分项目。设计的Check Point NG是在Windows 2000上运行；它在Windows XP上运行时，功能将受到限制。

在本书中使用的许多程序都需要你下载和安装软件。你的计算机起码应当配备Web浏览器和归档实用程序WinZip（可以在www.winzip.com上得到）。你还需要有字处理程序或文本编辑器，用来记录实习项目的答案。其中有几个项目还需要使用电子邮件应用程序，如Outlook Express或Netscape Messager。

目　录