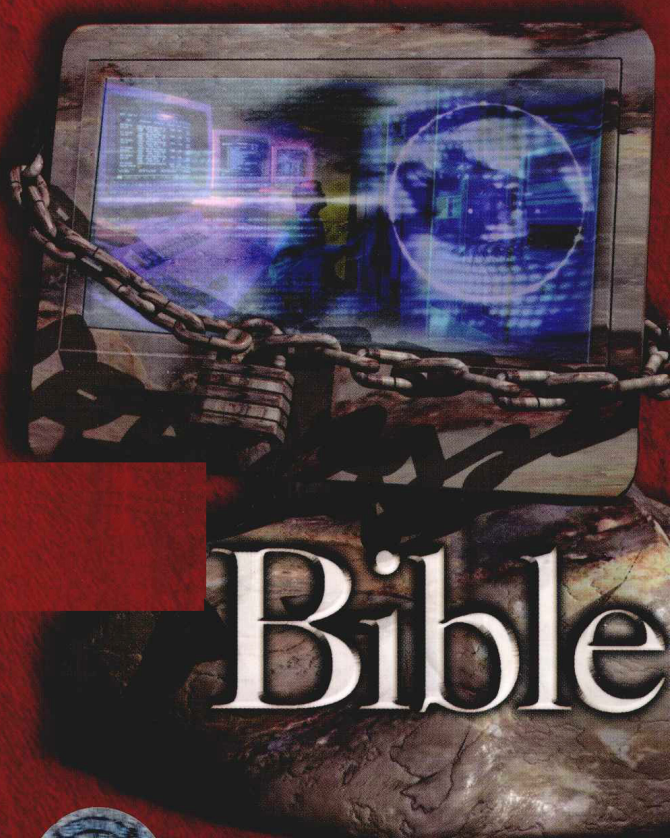
网络安全课堂教学的完美补充

Network Security Bible, 2nd Edition

网络安全宝典

(第2版)

(美) Eric Cole 著
曹继军 译
林龙信 译
李 化 审校



- 了解安全领域的发展
- 学习最新技术和最佳实践
- 保护企业和数据安全

网络安全保护必备书籍

清华大学出版社

网络安全宝典

(第 2 版)

清华大学出版社

北　京

Eric Cole
Network Security Bible, 2nd Edition
EISBN：978-0-470-50249-5

图书在版编目(CIP)数据

网络安全宝典(第 2 版)/(美)科尔(Cole,E.) 著；曹继军，林龙信　译；李化　审校.
—北京：清华大学出版社，2010.11
书名原文：Network Security Bible，2nd Edition
ISBN 978-7-302-23939-0
Ⅰ. 网… Ⅱ. ①科… ②曹… ③林… ④李… 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(2010)第 195695 号

责任编辑：王　军　王滋润
装帧设计：康　博
责任校对：胡雁翎
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：45.25　**字　数**：1129 千字
版　　次：2010 年 11 月第 1 版　　**印　　次**：2010 年 11 月第1 次印刷
印　　数：1～4000
定　　价：98.00 元

产品编号：034808-01

译 者 序

网络技术使得信息资源可以高度共享，同时也使人们面临着巨大的安全风险。黑客入侵事件和计算机病毒常有发生。为此，各国政府、军队、企业和其他相关机构都越来越重视网络安全问题，并不断为解决网络安全问题而投入大量资金和精力。

《网络安全宝典(第 2 版)》是一本介绍网络安全相关知识和方法的经典书籍。与前一版本相比，本书涵盖了网络安全的新技术、新方法和新手段，并尝试由被动安全向主动安全转变。本书可以作为网络安全领域的综合教程，也可以作为实现网络安全的技术手册。

全书共分为 7 个部分共 29 章，各部分的内容如下：第 I 部分概述了网络安全现状；第 II 部分介绍了信息系统安全基础；第III部分讨论了主要操作系统和应用程序中存在的安全问题；第Ⅳ部分介绍了网络安全基础；第 V 部分介绍了与安全通信相关的最佳实践；第Ⅵ部分介绍安全威胁与响应；第Ⅶ部分将前面各部分内容融为一个综合解决方案，并展望了网络安全的未来。本书内容丰富、全面、新颖，适用于信息安全领域的从业人员和在日常工作中需要应对各种网络安全问题的人员。其中深入探讨的问题包括：风险管理、取证、防火墙、入侵检测系统、Windows 安全、UNIX/Linux 安全、万维网、电子邮件、服务器应用、域名系统、安全通信、安全评估、安全评价和安全测试等。

本书由曹继军和林龙信翻译完成。李化负责审校和统稿。在翻译本书的过程中，我们仔细地推敲了相关的术语，并重点参阅了常用的翻译方法，但是在日常交流时，我们常常使用某些英文术语而不是其中文翻译，因此我们推荐读者更多地关注英文术语及其缩写。在翻译过程中，虽然我们竭尽所能，但恐怕仍有不少翻译不当之处，我们希望得到您的批评指正请将您的反馈信息发送到 wkservice@vip.163.com，我们将不胜感激。

译 者

2010 年 2 月

前　言

网络安全跨越众多学科，涉及面覆盖管理和策略主题，以及操作系统内核基本原理。此前，覆盖网络安全各领域的知识通常由多本不同的书籍分别阐述，当用一本书籍进行阐述时总是讨论一些高层次的问题，而与实际应用相差甚远。《网络安全宝典(第 2 版)》所提供的网络安全方法是从那些希望学习并应用有关网络安全最佳实践的用户角度总结的。本书全面总结了网络安全的知识和方法，拥有本书就不需参考其他的网络安全资料。本书所提供的信息是作者在网络安全领域内多年实践经验的总结。

《网络安全宝典(第 2 版)》不只是对上一版本进行了简单的修订，还涵盖了网络安全的新技术、新方法和新手段。与上一版本相比，本书最大的变化之一是向主动安全转变，从而获得任务弹性。网络安全的本质是管理和控制机构的关键性资产所面临的风险。然而，由于威胁的持久性和隐蔽性越来越强，因此机构需要的是在被攻击之前已经预先关闭漏洞，这就是主动安全的基本原理。

本书的目标

《网络安全宝典(第 2 版)》阐述了网络安全的基本概念，以及网络安全的实现过程和方法。本书的目标是为读者理解安全工程过程和网络安全的最佳实践提供支持，本书深入探讨了如下主题：

- 风险管理
- 取证
- 防火墙
- 入侵检测系统
- Windows
- UNIX/Linux
- 万维网(WWW)
- 电子邮件
- 服务器应用
- 域名系统(DNS)
- 通信安全

其他主题包括安全评估、安全评价和安全测试技术等，这些主题旨在让读者通过清楚透彻地了解最新信息而洞察信息保障。商业、政府和工业等部门的网络安全从业人员将从这些

最新的和可应用的知识中受益。

如何使用本书

《网络安全宝典(第 2 版)》可以作为网络安全领域的综合教程，也可以作为实现网络安全的技术手册，还可以作为信息和网络安全从业人员的参考文献，甚至可以作为规划未来网络安全问题和项目的指南。

作为网络安全领域的综合教程

《网络安全宝典(第 2 版)》涵盖了基本原则、标准过程、管理问题和访问控制概念。通过学习本书，读者可以理解信息系统安全的基本原理。在此基础上，本书还讨论了主流的操作系统、Internet 安全、Web 安全等。接着，本书介绍了网络协议、无线通信和网络体系结构，这为理解网络和通信提供了有力支持。同时，本书还探讨了入侵检测和信息安全评价方法学。上述这些主题构成了本书的不同部分，以便于读者依据自己的兴趣进行重点阅读或跳过熟悉的主题。因此，本书为读者提供了一个具有选择性的综合教程，这取决于读者的经验和培训。

作为实现网络安全的技术手册

在分析网络安全问题和实现有效的解决方案方面，本书的作者具有丰富的经验。基于这些经验，作者为现实的从业人员提供了解决实际问题的相关指导和详细的“秘笈”。这些“秘笈”适用于如下领域：

- 风险管理
- 信息安全系统生命周期过程
- 培训
- 业务连续性/灾难恢复
- 备份
- 远程认证
- Windows
- UNIX
- Linux
- 攻击
- 电子邮件
- 服务器安全
- 无线安全
- 入侵检测和处理
- 保证评估

作为信息和网络安全从业人员的参考文献

本书包含了网络安全及其相关主题的基础和前沿知识。这些内容可以作为信息安全从业人员日常安全工作的一套有价值的参考文献。本书关于操作系统、访问控制、无线安全、Web 安全、入侵检测与响应，以及评估方法学的章节将对现在和未来的应用特别有用。

作为规划未来网络安全问题和项目的指南

本书强调了重点讨论未来规划以及预测网络安全问题的主题。这些主题涉及的相关问题和重要领域如下：

- 如何将好的系统工程原则应用于信息安全系统的开发
- 提出关于安全标准和指南的建议——这些标准和指南非常有用，应该将其应用于实现和达到所需的网络安全
- 如何实现机构的安全策略，并且如何确保这些安全策略被理解和制度化
- 如何确保机构对灾难有所准备
- 如何防止未来可能的责任诉讼
- 如何规划扩展的、安全的远程访问需求
- 如何实现无线安全
- 如何防止未来的攻击
- 如何处理未来的攻击
- 如何评估新提出的安全体系结构的有效性

在本书最后一章，将总结上述问题和方法。

本书的读者对象

《网络安全宝典(第 2 版)》不仅适合于信息安全专业人员，也适合于日常需要处理网络安全问题的人员。本书以简明的语言描述了为什么需要以及如何获得安全网络。这是一本包罗万象的参考文献。

在任何规模的机构中，对于涉及网络安全的所有人(从管理者到技术工程师)而言，通过阅读此书，他们将能够更好地了解网络安全的重要方面，并获得高效构建安全网络的方法。

本书的组织结构

《网络安全宝典(第 2 版)》全文由如下所示的 7 个部分组成：

- 第 I 部分：网络安全现状
- 第 II 部分：安全原则与实践

- 第III部分：操作系统和应用
- 第IV部分：网络安全基础
- 第V部分：通信
- 第VI部分：安全威胁与响应
- 第VII部分：综合网络安全

本书各个部分之间的顺序体现了从网络安全基本原则和基础知识到实践细节的平滑过渡。就此而言，本书不仅可以为经验丰富的专业人员提供有价值的参考和指导，也可以为该领域的初学者提供学习机制。

第 I 部分：网络安全现状

第 I 部分内容为网络安全现状的基础，读者可以通过学习这部分内容而理解网络安全的关键问题和重点领域。第 I 部分也是本书其他部分的基础，为学习网络安全建立起坚实的知识基础。

- **第 1 章：网络安全的状态**。为了正确地保护机构，我们需要理解网络安全现状、网络中正在发生的情况，以及机构最需要关注的风险。尽管网络安全问题引起了极大的关注，但是许多机构对其重要性的认识还不够。
- **第 2 章：网络安全的新方法**。目前，网络安全问题所关注的焦点正在向提供具有更高成本效益和主动式的安全解决方案转变。重要的是要记住，并不存在一种适合所有网络安全的解决方案。网络安全原则和概念需要依据存在的威胁和漏洞来应用并适用于各个机构。
- **第 3 章：机构的安全问题**。安全的本质是管理和缓解机构的关键性资产所面临的风险。为了计划能够成功，必须具备预算和人手；而为了获得预算和人手，必须明确当前怎样的风险是不可接受的，而且需要以成本效益的方式进行修复。显然，如果机构管理人员未能理解该问题，则不会为修复工作分配所需的资源。

第 II 部分：安全原则与实践

第 II 部分介绍了信息系统安全基础的背景。具体而言，这部分内容共包括三章，分别涉及信息系统安全原则、信息系统安全管理和访问控制。

- **第 4 章：信息系统安全原则**。对于网络安全从业人员而言，非常熟悉信息系统安全的基本原则，特别是机密性、完整性和可用性(CIA)的概念是很重要的。本章详细解释了这些主题及其相关的威胁、漏洞和威胁可能产生的影响等。在阐述这些基本主题后，本章还解释了系统工程(Systems Engineering, SE)、信息系统安全工程(Information Systems Security Engineering, ISSE)、系统开发生命周期(Systems Development Life Cycle, SDLC)的规范过程，以及网络安全和系统开发生命周期的关系。这些知识有助于读者更好地将包含信息系统安全的标准规则应用于系统开发活动。对于需要上述方

法提供规范的大型公司的个人和需要将正规信息系统安全方法应用于日常运作的政府机构而言，这些技巧是非常有价值的。

- **第 5 章：信息系统安全管理**。为了进一步为研究网络安全问题提供基础，本章探讨了管理在实现良好的网络安全过程中所扮演的角色问题，这个问题非常重要，但有时会被忽视。机构的每一名员工都应该了解信息安全策略、过程和指导方针，并始终贯彻和执行。对于机构而言，这些规章制度文档和实践的存在是极其重要的，它们应该被纳入该机构的日常运作中。例如，关键人员需要休假一周或更多时间，这需要新的人员替代他们的工作，这个看似普通的需求可能招致隐蔽的非法活动。同时，如果公司管理者没有为保护该机构的知识产权和其他重要信息制定相关策略，那么他们将被追究相关法律责任。本章还提供了确保机构的关键业务不被灾难中断的简明指导。本章还解释和说明了业务连续性计划(Business Continuity Planning, BCP)和灾难恢复计划(Disaster Recovery Planning, DRP)方法，这两种方法可以为关键业务功能和网络信息系统的连续性运作提供支持。
- **第 6 章：访问控制**。对于任何机构而言，对关键的网络和计算机资源进行访问控制是最重要的需求之一。本章定义和说明了识别访问信息系统的用户和进程、验证用户或进程的身份(认证)、授予访问特定资源的权限(授权)等概念。此外，本章内容还涵盖了从远程站点安全访问信息系统的实现方法。
- **第 7 章：攻击与威胁**。理解攻击是优化防御的唯一方法。本章将关注机构面临的各种威胁，并将威胁分解为针对机构发起的特定攻击。通过了解具体攻击，可以知道机构存在的重要漏洞，从而制定安全方针。

第III部分：操作系统与应用

第III部分首先详细介绍了 Windows、UNIX 和 Linux 操作系统的相关安全问题和解决方案。然后探讨了 Web 浏览器安全、Web 安全、电子邮件安全、域名系统和服务器应用。基于在本领域的丰富经验，作者在实现操作系统和 Web 安全方面提供了见解和方向。

- **第 8 章：Windows 安全**。各种版本的 Windows 操作系统得到了广泛应用，其安全漏洞也对主机产生了严重威胁。第 8 章阐述了这些安全问题，以及安装 Windows、固化操作系统、安全操作和维护安全系统的步骤。
- **第 9 章：UNIX 和 Linux 安全**。由于 Windows 操作系统存在可靠性问题，UNIX 和开源的 Linux 操作系统越来越受到广大用户的欢迎。因此，第 9 章阐述了 UNIX 和 Linux 操作系统的网络安全方面的问题，包括内核问题、外部服务以及具体服务(如 NFS、Sendmail、BIND 和 RIP)等。
- **第 10 章：Web 浏览器和客户端安全**。Web 浏览器会对主机的安全产生严重威胁，本章将基于通用浏览器探讨这些威胁的来源。作者为实现 Web 浏览器安全和保护企业门户提供了解决方案。

- **第11章：Web安全**。第11章研究了超文本传输协议(Hypertext Transfer Protocol，HTTP)和通用网关接口(Common Gateway Interface，CGI)的安全问题，与Cookie、隐藏字段和URL跟踪有关的隐私保护，以及电子商务应用程序的安全实现。这部分内容也与构建安全的Web浏览器密切相关。
- **第12章：电子邮件安全**。由于电子邮件得到广泛应用，因此本章所涵盖的安全知识可以直接适用于用户、IT专业人员和安全人员等。本章介绍了不同类型的电子邮件协议，包括SMTP、POP3和IMAP。作者描述了如何正确配置电子邮件系统，以及如何处理上述各种类型电子邮件协议的安全问题。
- **第13章：域名系统**。本章描述了域名系统和主/从名称服务器的概念，以及域名系统的设计(包括分离式DNS和双分离式DNS)。并且介绍了如何建立不同类型的域名服务器，讨论了递归查询和区域传输问题。
- **第14章：服务器安全**。关于网络安全的另一个重要知识点是理解不同类型的服务器和与其相关的应用。本章描述了关于建立服务器的一些有待进一步观察的通用原则，并就服务器通用应用给出了有价值的评论。

第Ⅳ部分：网络安全基础

第Ⅳ部分阐述了各种网络协议，尤其是针对OSI和TCP模型。解释了无线通信和无线安全的基本概念，包括编码方案、不同的无线技术代和无线漏洞。然后，描述了网络体系结构的各个组成部分，并为实现各部分的安全提出了详细建议和指导。

- **第15章：网络协议**。本章详细阐述了OSI和TCP模型，以及IP、ICMP、TCP和UDP协议。还回顾了地址解析的概念和方法，以及与其相关的网络安全的一般目标。
- **第16章：无线安全**。通过无线通信连接Internet已经越来越普及。本章涵盖的主题包括：无线频谱、无线传输基础、不同的编码机制、无线技术的代、无线应用相关的安全问题。
- **第17章：网络体系结构基础**。在实现网络安全过程中，网络组件及其相应的配置是保护信息系统的关键因素。本章清晰地描述和解释了网桥、路由器、交换机以及其他重要网络设备。还探讨了上述网络设备的功能以及网络设备与网络整体安全之间的关系，并提供了应用的指导方针。
- **第18章：防火墙**。在网络上部署防火墙是主要预防措施之一。防火墙在任何网络中都发挥着重要作用，因而必须对其进行正确地设计和配置。本章探讨了如何正确部署防火墙，以及如何避免常见的错误等问题。
- **第19章：入侵检测/防御**。“防御是理想的，而检测是必须的”是网络安全的名言之一。尽管防火墙是主要的防御措施，但是往往需要对其辅以入侵检测系统(Intrusion Detection System，IDS)和入侵防御系统(Intrusion Prevention System，IPS)。最重要的是理解如何将各种系统组合起来以形成一个综合的网络安全解决方案。

第Ⅴ部分：通信

第Ⅴ部分揭示了与通信安全相关的最佳实践和方法。

- **第 20 章：保密通信**。保密通信包括加密和解密消息的方法，以及验证消息发送者的身份。本章介绍了密码术的历史，阐述了对称加密和非对称加密的基础，解释了数字签名，最后概述了普遍认可的加密公理。
- **第 21 章：隐蔽通信**。隐蔽通信是指掩盖了传输秘密信息事实的通信。在第 20 章所描述的保密通信中，攻击者知道敏感信息正在以混杂的方式传输。攻击者面临的问题只是如何通过解密消息而获取信息。在隐蔽通信中，敏感信息会隐藏在一幅图像或者一段时间出现的句子末尾的句号中。除非攻击者检查传输的所有信息以获取隐藏信息，否则无法知道隐藏了信息。这种隐蔽的通信类型称为隐写术。本章描述了隐蔽的目标、优缺点、将敏感信息嵌入图像等其他部件的方法，以及检测隐藏信息的工具。
- **第 22 章：保密/隐蔽通信应用**。本章详细描述了获得保密/隐蔽通信的方法。这些主题包括：电子邮件安全、虚拟专用网络(Virtual Private Network, VPN)的实现、为保护 Internet 传输信息而采用多种协议。本章也介绍了寻找数字证书以证明个人的公共密钥和管理公共密钥的方法。

第Ⅵ部分：安全威胁与响应

第Ⅵ部分主要解决网络入侵检测和响应，并确保安全控制已经到位实际地提供预期结果等方面的问题。这部分内容详细描述了网络安全、安全解决方案和规划未来情况的最常见问题。

- **第 23 章：入侵检测与响应**。网络安全从业人员必须熟悉并理解恶意代码的各种类型及其影响。第 23 章解释了不同类型的恶意软件，讨论了常见的攻击类型和来源，揭示了如何检测并处理对网络及其资源的入侵。
- **第 24 章：数字取证**。因为攻击的复杂程度不断增加，所以至关重要的是能够确定事件的发生，以便能采取适当的补救措施。无论是对于确定发生了什么，还是对于预防未来事故的发生，数字取证都是理解和确定已利用的漏洞的核心。
- **第 25 章：安全评估、测试与评价**。私人机构和政府机构都需要确保其网络和信息系统是安全的。这两种实体拥有关键敏感信息，其机密性、完整性、可用性必须受到保护。因此，这些机构已经开发出评估和评价方法，以确保网络安全(即使已经对网络实施了适当的控制)。本章讨论了这些方法，包括：系统安全工程能力成熟度模型(Systems Security Engineering Capability Maturity Model，SSE-CMM)、不同类型的认证和鉴定方法、美国国家标准和技术研究所(National Institute for Standards and Technology，NIST)的信息安全出版物，以及各类测试和审计实践。

第Ⅶ部分：综合网络安全

本书最后部分的章节将前面所述内容融合为一个综合的解决方案。网络安全不是部署产品或技术，而是要提供主动安全解决方案来降低关键性资产面临的风险以确保任务的弹性。

- **第 26 章：安全验证。**许多机构为网络安全投入了大量精力并付出很大努力，以确保网络的安全性。每一个机构必须认识到：网络安全是一个活动的目标，必须不断地进行验证。攻击者会不断地测试机构的安全，而且是隐秘进行的。因此，机构需要通过不断验证和改进他们的安全，这样才能与攻击者并驾齐驱。
- **第 27 章：数据保护。**安全的本质是缓解和降低机构的关键数据所面临的风险。数据保护是维护机构安全的核心。坦率而言，安全就是维持数据处于受保护的状态。
- **第 28 章：安全整合。**《网络安全宝典(第 2 版)》前面的各个章节已经涵盖了网络的构成要素、安全体系结构、安全威胁、安全对策、事故处理和安全评估等内容。本章描述了十大网络安全问题及其解决方案、信息安全和 IT 从业人员易犯的十大错误，以及如何为未来的活动和挑战设计框架，从而将上述实体有机地整合在一起。
- **第 29 章：未来展望。**一个机构今天是安全的并不意味着未来也是安全的。风险及其相应的漏洞时刻变化，所以机构需要关注的是任务的弹性，即确保无论面临何种威胁关键业务流程都能继续运作。

约定和排版特征

为了便于从书中获取信息，本书约定了一些排版特征。

提示、注释和警告

文中出现的提示、注释和警告是作者为了让读者注意相关信息。

警 告 ——该信息非常重要，它以独立段落的形式出现，并以一个特殊的图标开始。警告提供的信息都是值得关注的，不论对数据或系统是危险的或存在潜在危害。

提 示 ——提供的信息可以使您的工作变得更容易，是比普通方法更方便的捷径。

注 释 ——提供其他的辅助信息，但其内容有些超出当前本书的讨论范围。

阅读前的问题

通过阅读此书，您会为所在机构实现有效的主动安全而具备坚实的基础和清晰的思路。

请时刻牢记，安全意味着缓解关键性资产所面临的风险。所以，在为安全花费时间和金钱之前，请首先思考如下三个问题。

- 什么是风险？
- 它是优先级最高的风险吗？
- 最具有成本效益的降低风险方法是什么？

目　录