Mc Graw Hill Education

现实生活中安全入侵场景的真实描述，网络安全专业人员的《伊索寓言》

黑客大挑战

检验你的网络安全和取证能力 2

所有的挑战和解决方案都是新的！

Hacker's Challenge 2 :
Test Your Network Security & Forensic Skills

[美] Mike Schiffman
Bill Pennington
Adam J.O'Donnell
David Pollino
著

段海新 陈俏 译

Mc Graw Hill

清华大学出版社

黑客大挑战2

检验你的网络安全和取证能力

[美] Mike Schiffman
Bill Pennington
Adam J. O'Donnell
David Pollino 著
段海新 陈俏 译

清华大学出版社
北京

Mike Schiffman, Bill Pennington, Adam J. O'Donnell, David Pollino

Hacker's Challenge 2:Test Your Network Security & Forensic Skills

EISBN: 0-07-222630-7

图书在版编目（CIP）数据

黑客大挑战 2：检验你的网络安全和取证能力/（美）迈希夫曼等著；段海新等译.
－2版－北京：清华大学出版社，2003.9

书名原文：Hacker's Challenge 2: Test Your Network Security & Forensic Skills

ISBN 7-302-07207-8

I.黑… II. ①迈…②段… 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 080281 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

组稿编辑：成昊

文稿编辑：安静

封面设计：杨月静

版式设计：房利萍

印 刷 者：北京市耀华印刷有限公司

发 行 者：新华书店总店北京发行所

开　　本：异 16　　印张：21.25　　字数：438 千字

版　　次：2003 年 9 月第 1 版　2003 年 9 月第 1 次印刷

书　　号：ISBN 7-302-07207-8/TP · 5249

印　　数：1～5000

定　　价：39.00 元

内容提要

本书以一种生动惊悚的记事手法讲述了19个真实的网络安全入侵案例，让读者身临其境地检验自己的应急响应和计算机取证能力。书中的案例覆盖了当今世界常见的攻击类型，包括拒绝服务攻击、恶意代码、Web应用攻击、内部攻击和外部攻击等，还覆盖了无线网络安全等当前热点技术。

本书分为“挑战”和“解决方案”两部分内容。“挑战”部分详细描述了每一起安全事件的所有证据和取证信息（日志文件、网络拓扑图等），并提出了一些问题引导读者自己分析入侵的原因；“解决方案”部分深入案例分析，用详细的证据来透彻解释入侵的来龙去脉，并回应了“挑战”部分的问题，另外还提供了相应的预防手段和补救措施，以降低风险并减少损失。

书中的场景都是资深的网络安全专业人员的真实遭遇，对于提高技术人员的事件分析能力和应急响应能力极有教益，适合网络管理员、系统管理员、信息安全官等研习及参考。

技术在道德上是中性的，只有在我们用它的时候才分为好坏。如果把它用于正义，它就是好的；如果用于邪恶，它就是坏的。

—— William Gibson

关于作者

Mike D. Schiffman 是 @stake 公司的安全设计部主任。@stake 公司是世界领先的安全咨询公司，该公司众多的安全专家和安全权威人士可以为企业设计和构建安全的业务解决方案。Schiffman 在到 @stake 公司工作之前，是 Guardent 公司研发部主任，负责公司内部的研发与其他部门的整合，包括交付、取证和安全服务管理。在到 Guardent 公司工作之前，Schiffman 在 Internet Securidty Sytems（ISS）和 Cambridge Technology Partners 公司都担任过较高的职务。

Schiffman 的主要工作领域是研发、咨询和写作，他是著名的网络安全工具 firewalk 和一个普遍使用的底层软件包 libnet 的作者之一。Schiffman 曾经领导过财富 500 强的大企业的安全咨询项目，包括关键的基础设施、金融、汽车业、制造业、软件行业。Schiffman 在安全界颇受欢迎，还在许多政府机构作过报告，包括 NSA、CIA、DOD、FBI、NASA、AFWIC、SAIC 以及一些军事部门。

Schiffman 曾写过几本关于计算机安全的书，包括“Building Open Source Network Security Tools”（Wiley & Sons 出版），以及有关计算机取证和应急响应“Hacker's Challenge”系列（McGraw-Hill/Osborne 出版）。他还与别人合写了几本书，包括“Hacking Exposed”（McGraw-Hill/Osborne出版），“Hack Proofing Your Network: Internet Tradecraft”（Syngress Media 公司出版）。他还为许多技术期刊撰文，写过多篇技术白皮书，涉及内容包括从 Unix 内核到网络协议缺陷。

Adam J. O'Donnell 是德雷克赛尔大学电子工程系博士研究生，他在 Drexel 大学电子系获得了电子工程学士学位并获最高荣誉毕业生称号。Adam 目前主要从事学术研究和创作工作，同时为信息行业提供安全咨询。Adam 在 Lucent 公司优化过 RF 放大器，并因此获得专利，同时 Guardent 公司还为他提供一个研究职位。Adam 还是本书第 1 版的作者之一。

Bill Pennington 是认证的信息系统安全专家（Certified Information Security Systems Practitioner，CISSP），目前受雇于 WhiteHatSec 公司，该公司是 Web 应用安全服务的主要提供商。Bill 有 12 年的 IT 工作经验和 6 年的信息安全专业工作经验。他熟悉 Linux、

Solaris、Windows 和 OpenBSD，他是 CISSP、CCNA（Certified Network Administrator）、CISS（Certificate Internet Security Specialist）和 Windows NT 4.0 微软认证的产品专家。他主要从事计算机取证、Web 应用安全、网络体系结构设计、安装和配置 VPN、Cisco Pix 防火墙、IDS 和监控系统等工作。Bill 经常在安全领域作报告，他是本书第 1 版的作者之一。

David Pollino 领导 @stake 公司的无线研究中心专门从事无线技术的研究，如 WLAN、WAP、蓝牙技术、GPRS。他的网络工作经验丰富，从一级的 ISP 雇员到财富 500 强企业的网络安全设计师都能胜任。David 发表过许多论文并出版了多本书，他是本书第 1 版的作者之一，还是“RSA Press： Wireless Security”的作者之一。

关于技术审阅人

Tom Lee（MSCE）是 Foundstone 公司的 IT 经理。他目前负责 Foundstone 公司的系统正常运行和阻止入侵者的攻击和内部人员的破坏。Tom 有 10 年的系统管理和网络管理经验，他维护过许多不同的系统的安全，从 Novell 网、Window NT/2000 到 Solaris、Linux 和 BSD。在加盟 Foundstone 之前，Tom 是加州大学里弗赛德分校的 IT 主任，他是“Windows XP Professional Security”（McGraw-Hill/Osborne 出版）的作者。Tom 是本书第 1 版的技术审阅人，另外还是“Haking Exposed”（《黑客大曝光》）第 3 版和“Hacking Linux Exposed”（《Linux 黑客大曝光》）第 2 版的技术编辑。

引 言

2001 年秋天，为了推出“Hacker's Challenge”（《黑客大挑战》），我们查询了美国有线新闻网（cnn.com），发现安全事件经常成为 CNN 的头条新闻，其中关于形形色色的系统滥用事件的报道数不胜数。在本书写作时的 2002 年冬天，网络安全的形势并没有出现任何好转：

- ▼ 媒体给美国计算机安全打分 F（即不及格）
- ■ 美国公开审理军方网络黑客
- ■ 英国政府起诉军方黑客事件
- ■ 对因特网心脏地带的攻击被挫败
- ■ 中国的计算机面临病毒泛滥的危险
- ■ 黑客称系统漏洞泄漏了零售业数据
- ■ Bugbear 病毒攻击计算机安全
- ■ 美国计算机系统易受攻击吗？
- ▲ 黑客攻击——你是怎样成为攻击目标的？

总之，这个世界很不安全（无论是现实世界，还是电子空间）。感到恐惧吗？亲爱的读者。《黑客大挑战 2：检验你的网络安全和取证能力》这本书把当前现实世界中的常见的几种攻击场景呈现在你面前：

- ▼ 中间人攻击
- ■ 新的无线网络攻击
- ■ 第二层攻击
- ■ 安全政策的实施
- ▲ 品质恶劣的雇员

如果你没有读过本书的第 1 版，你可能会问为什么这本书称为《黑客大挑战 2》。随

着因特网规模和用户的发展，计算机安全事件也愈演愈烈。媒体上的新闻没有告诉我们这些攻击事件究竟是怎样发生的，导致事件的原因是什么？攻击是怎样进行的？怎样防范？如何降低事件的破坏程度？对于所有的事件，我们也许都要问是怎么发生的？如果你对这些安全事件感兴趣，那么这本书肯定对你有用。

在《黑客大挑战 2》中，与第 1 版相同的核心团队将带给你一个个真实的计算机安全战的故事，每个故事都给你展示了事件的详细信息，并要求你解决其中的问题。

不同行业中负责网络和网络安全的人员都可以从类似行业的实际安全事件中吸取教训，可以从书中提供的信息中学到各种情况下需要考虑的因素，并了解黑客的惯用伎俩。而且这本书非常有意思。

如果你看过第 1 版，你肯定还想看第 2 版，因为第 2 版并不是第 1 版的修订，而是一本全新的书，其中，挑战和解决方案都是新的。

本书的结构

《黑客大挑战 2》包括两部分，第 1 部分包括所有案例研究，即“挑战”。每个挑战都详细描述了所有的证据和取证信息（日志文件、网络图等），这些信息对于判断攻击是必须的。为简洁起见，许多章节中的证据信息都做了删节，留下的是最为关键的信息（而不是把冗长的原始日志全部列出来）。每个案例研究中都提出了具体的问题来引导读者正确地取证分析。

第 2 部分是第 1 部分所有挑战的解决方案。这部分深入分析案例，用详细的证据信息透彻解释案情，并回答了挑战中的问题。另外还提供了一些关于预防和降低风险的信息。

保护隐私

为了保护相关组织的隐私，本书修改或删除了每个故事中的许多信息；同时，为保证案例研究的完整性，保留了重要的信息。改动的信息包括：

- ▼ 公司名称
- ■ 雇员姓名
- ■ IP 地址
- ■ 日期
- ■ 网页的被黑细节（修改了信息，去掉了淫秽或不合适的内容）
- ▲ 没必要的故事情节

漏洞信息

只要有可能，本书从头到尾，对涉及到的漏洞信息都给出了外部的参考资源（参见每个解决方案中的“其他资源”部分）。另外，MITRE 和 SecurityFocus 公司提供的稍有不同的漏洞数据库也是非常有用的资源。

MITRE（http://cve.mitre.org）是非盈利的国家技术资源，对政府部门提供系统工程、研发、信息技术支持。CVE（Common Vulnerabilities and Exposures）是一个清单或者一个字典，它为常见的安全漏洞指定一个公共的名字。使用公共的名字，独立的数据库或工具之间可以非常容易地共享信息，而在此之前，共享这些数据则极为困难。因此，CVE 对于信息共享极为关键。

SecurityFocus（http://www.securityfocus.com）是信息安全服务行业中领先的服务提供商。该公司管理着业界最大也是最活跃的安全群体，运行着安全界首屈一指的门户网站，每月有 20 多万的用户访问量。SecurityFocus 的漏洞数据库是公开的漏洞库中最为全面的。

难度分类

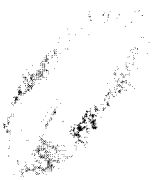
每个案例可以分为 3 个不同的级别，在挑战的开始给出，描述该章的难度。这些难度既包括攻击的难度，也包括安全管理人员防范的难度。

目　录

第2部分 解决方案

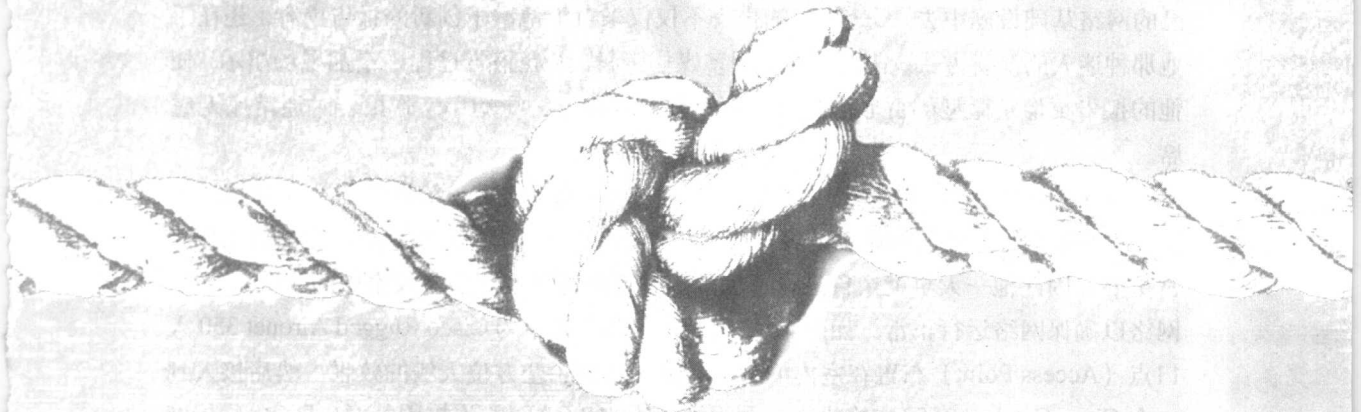
第1部分

挑　战



挑　战 1

拜占庭式故障



行业:	专业会议和培训
攻击难度:	低
预防难度:	难
补救难度:	低