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

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

段海新 陈俏 译

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　2004 年 1 月第 2 次印刷
书　　号：ISBN 7-302-07207-8/TP · 5249
印　　数：5001－8000
定　　价：39.00 元

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。

攻击难度

攻击难度是指发起攻击的攻击者所需的技术能力和知识。通常我们会看到，环境越复杂越安全，攻击者就越难攻破（当然，这也不是绝对的）。

- ▼ **低/易** 这种层次的攻击一般只是 script-kiddie 级别的人干的。攻击者只需要运行一个攻击脚本，编译一下很容易到手的源代码，或者使用众所周知的攻击方法即可。这种行为缺乏创意，黑客的收获最少。
- ■ **中等** 攻击者使用公开的攻击方法，但是他可能改动一些东西，增加一些自己的创意，比如伪造源地址、稍微修改攻击行为等。
- ■ **难** 攻击者非常聪明，技术熟练。他们所使用的手段可能是公开的也可能是未公开的，攻击者自己可以编写攻击代码。
- ▲ **高** 这种量级的攻击通常出自专家之手。攻击者技术极为高明，使用未公开的攻击方法或者领先的技术。他自己创造新的攻击方法，如果可能，他会抹掉自己的踪迹，留下一个隐蔽的后门。这类攻击者一般不会被抓住，除非真正碰到更为老练的安全管理员，或者自己运气不佳。

预防和补救的难度

预防的难度是指从企业管理者的角度来看，为避免事件的发生而采取措施的难度。补救的难度是指万一事件发生，采取措施防止事件扩散到整个组织网络、降低损失的难度。两者有些相似，而且都可以用下面的术语来分类:

- ▼ **低/易** 预防或补救这一问题非常简单，比如打一个软件补丁或更新，或者增加一条防火墙规则。这种修改非常简单，无需太费功夫。
- ■ **中等** 补救措施可能涉及复杂软件的打补丁或更新操作，可能还需要修改防火墙政策，还必须重新安装受感染的计算机系统，或者对网络结构稍作修改。
- ▲ **难/高** 需要打补丁，更新一台计算机，或者更新一系列计算机。还要对网络结构作重大修改。这种级别的攻击事件涉及非常难以防范和补救的漏洞。

本书的规范

了解本书的行文规范将使你的阅读更加轻松。下面是简单的概要。

在每一章的正文里，你都可以找到日志文件、网络结构图、文件列表、命令输出信息、代码以及多种形式的取证证据。我们尽可能保持这些内容原始的样子，不过出于对版面的限制和保密的考虑，我们对这些证据做了必要的修改。

本书分成两个部分。第1部分，挑战1至挑战19给出了真实的安全事件的细节。每个挑战的开头都用表格形式给出了受害者的行业、攻击、预防和补救的难度。

问题

在每个“挑战”的末尾，你会看到几个问题，这些问题指导你研究事件的细节，把你引向最终的“解决方案”。你可以随意在这一部分、甚至全文中作些标记或记录，这样有助于你找出最终的答案。

答案

在本书第2部分，你会看到对应第1部分的解决方案1至解决方案19。解决方案详细解释了事件是如何发生的，如何解决的，并回答了第1部分提出的问题。

预防

解决方案中包括“预防”部分，在此你可以找到如何在攻击发生之前进行预防的建议（对于与本书中描述的那些不幸的公司类似的企业来说，这部分是非常有用的）。

补救

解决方案包含“补救”部分，在此你可以看到受害的公司在受到攻击后是如何亡羊补牢的。

祝你好运!

目　录

第2部分 解决方案

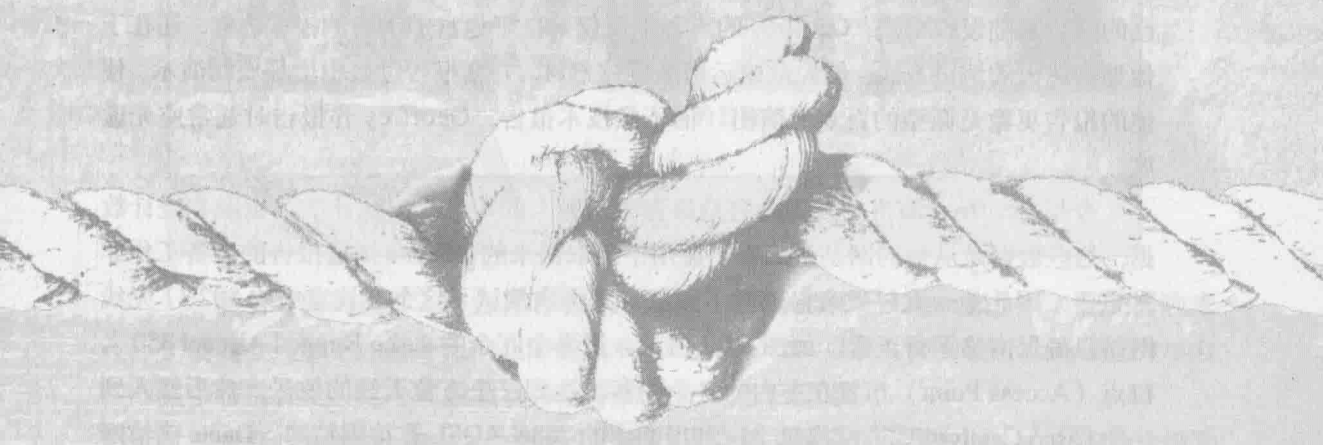
第1部分

挑　战

读后感

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

THURSDAY, AUGUST 15, 2002, 09:15

一个夏天的清晨，风和日丽，Dante看上去的确很招眼：花100美元收拾的发型和黑色的Prada西装，使Dante看上去光彩照人。有人问他为何总是打扮得衣冠楚楚，他说这是职业需要。Dante是世界首屈一指的计算机安全会议“漏洞演示会（The Vulnerability Monologues，TVM）”的会议推广人。TVM每年可带来超过30 000 000美金的收益。如果纯粹从规模和魄力方面而言，它远远超越了任何其他的安全会议。

TVM将它的安全季度会议安排在全球最繁华的地方。这次会议安排在内华达州拉斯维加斯。Dante只不过是负责主持此次会议的小人物，也许有人说他有点刻薄，但是人们不得不整天都要迎合他。然而今天这个特殊的早上，却没人愿意再买他的账。Dante一副圆滑的外表也无法掩饰住他的不悦。

Dante看了看他的劳力士总统铂金表，现在是上午9:15。“见鬼！他到哪里去了？”他的主讲人Geoffrey Cooper目前已经迟到了整整15分钟。今年的主题是“不确定世界中的业务连续性”。在这个领域里，Geoffrey是国内的顶级权威之一。现在，3000位来自世界各地的信息安全经理人在Bellagio酒店的大厅里不耐烦地等着，Dante孤独地站在空旷的舞台前面，焦急地等待着那个令人尊敬的演讲人。

每个人都渴望聆听Geoffrey的新报告，并期望能把他充满梦幻色彩的原理应用到自己的网络基础设施中去。Geoffrey的声誉不仅仅来自于他富于创新的报告内容，还在于他那种迷人的演讲方式。他大量地运用多媒体素材，并在报告过程中增加现场演示，使他的报告更像是微型的百老汇演出，而不像技术报告。Geoffrey作报告时通常座无虚席。

今年Geoffrey演讲的关键内容是报告中所融入的动态人口统计学、金融和统计数据，这些数据是从他的网站上的客户应用中提取出来的。Dante知道报告的准备工作非常重要，因此他一大早就亲自进行了测试，并再次测试了这个会议室中的802.11无线网络以确保网络运行正常，如图C1-1所示。用多个冗余的Cisco Rugged Aironet 350入口点（Access Point）布置在室内的各个角落，达到了全方位天线的效果，然后接入到一个Cisco Catalyst 3550交换机上，利用酒店的768K ADSL连接因特网。Dante确信网络的连通性肯定万无一失。

Dante知道静态WEP的安全问题，于是他不厌其烦地搭建一个LEAP服务器进行802.1x认证和WEP密钥分配，以确保仅允许已注册的与会人员连接无线网络。Dante环顾四周，看到很多与会者正在浏览电子邮件、网站和其他在线娱乐；他对网络能够正常