这是一本介绍网络安全的书，从组织结构上说，分为三部分：技术发展、工具软件和参考文献。技术发展部分介绍了安全方面的背景知识，包括Internet的结构、Internet上运行的协议(主要是介绍TCP/IP协议)、一名黑客所具有的知识以及安全的一些概念，如加密算法与标准译码以及信息截取等。工具软件部分详细讲述一些黑客常用的攻击方法，如破坏性装置(邮件炸弹、病毒等)、Internet端口与服务扫描程序、口令攻击程序、特洛伊木马、嗅探器等，并给出了很多黑客常用的攻击工具。在阐述攻击工具之后，作者也对防止攻击提出了很多很好的解决方案，如防火墙、登录与审计工具、各种加密方法等。参考文献部分主要是针对那些要进一步深入研究安全的读者，作者将Internet和各种杂志上的很多有关安全的文章列举出来，以供读者参考。

本书适用于Internet网友和对网络与系统平台的安全有一定要求的信息主管，同时对于国内安全保密研究方面的专家，也具有非常不错的参考价值。

本书版权登记号：图字：01-98-2506

图书在版编目(CIP)数据

网络安全技术内幕 /（美）匿名著；前导工作室译. -北京：机械工业出版社，1999.4
(网络安全技术丛书)
书名原文：Maximum Security (Second Edition)
ISBN 7-111-07182-4

Ⅰ.网… Ⅱ.① 匿…②前… Ⅲ.计算机网络－安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字(1999)第09062号

出 版 人：马九荣 (北京市百万庄大街22号 邮政编码100037)
责任编辑：陈剑颉
北京忠信诚胶印厂印刷 · 新华书店北京发行所发行
1999年4月第1版第1次印刷
787mm × 1092mm 1/16 · 34.25印张
印数：0 001-7 000册
定价：70.00元(附光盘)

译 者 序

由于Internet在国内还是一个新生事物，对其安全方面的研究还刚刚起步，一般Internet使用者根本不了解自身网络或系统存在的安全隐患，出现问题之后，无奈之余，也只好自认倒霉而已。20世纪是信息爆炸的世纪，Internet将在近几年得到更为广泛的发展，然而你并不希望你的信息受到别人的攻击，但却找不到解决安全问题的良药。

当我们拿到这本书的英文版本时，一种难以言表的愉悦心情渗透全身，因为我们可以肯定，这是国内读者迫切需要一本网络安全书籍。无论从内容上，还是组织结构上，本书绝对是一流的。

安全攻击和安全保护是矛与盾的关系，是一种攻击与防守的关系。孙子说“兵者，诡道也”，又说“知己知彼，百战不殆”。安全与反安全之间就是一场斗智斗勇的长期战斗。

我们翻译本书的目的并不是要读者去攻击别人，而是我们必须要对攻击者所采用的技术有很深入的了解，才能知己知彼，百战不殆，才能最终防止别人对自己的攻击。

通过对本书的认真阅读，我们可以说你一定能成为安全方面的高手。当然要成为顶级的安全专家，你还必须对本书中提到的各种安全策略进行仔细的研究，充分利用本书提供的各种安全方面的网上资源。我们相信，你一定能成功的。

全书由陈英武、陈曙晖、黄瑞芳、朱敏主持翻译，前导工作室的全体同仁共同完成了本书的翻译、录排等工作。本书由李志、张巧莉、陈彦海进行了主要的校对工作。

由于时间仓促，且译者经验和水平有限，译文难免有不实之处，恳请读者批评指正!

1998年11月

前　言

关于本书

许多书籍的第2版与第1版并没有很大的差别，作者一般只对链接进行更新，对书的组织结构进行一下改善，并增加20~40页的新内容。当然，也有些作者仅仅修改一些错误，并在篇幅上进行紧缩。尽管是这样一种情况，忠实的读者还是会去购买第2版、第3版以及第4版。

当Sams希望我能对Maximum Security(中文版书名为《网络最高安全技术指南》，机械工业出版社，1998.5,ISBN 7-111-06224-8/TP·72)进行修改时，我一直在思考这个问题。我知道，我可以收集一些有意义的建议，对原书增加那么几页，这样就又出了一本“新”书。我的读者会跑到书店去买书，而我则跑到银行取钱——但是收集建议并不是我的工作。我的工作是将Internet安全方面的最新发展告诉大家。经过长时间的海滩漫步，我终于坐在计算机旁开始写书了，结果就出版了Maximum Security(Second Edition)(中文版书名为《网络安全技术内幕》)。对于本书，我想阐明的第一个观点是:

该版本几乎就是一本完整的新书。

对于该书，我作了很多的修改。

本版所做的完善工作

本书的第1版写得比较草率，它只是一个冲击波，给读者提供一个对Internet安全进行全面了解的机会。但这样的方式有一个缺点，读者不可能拿它来保护自己的网络。

而现在的版本就不同了。

在第四部分“平台和安全”中，我列出了系统的脆弱点、它们存在的原因以及发现这些脆弱点的源代码。在许多示例中，那些脆弱点是按照严重性排列的（换句话说，那些可能导致整个系统崩溃的脆弱点排在所有列表的前面)。这种方式就是一种不小的改进，读者可以使用本书快速地防止最为通常的一些攻击。

但是，要覆盖所有的脆弱点是不可能的。在本书中，只有那些比较严重的脆弱点才列出来了（我们忽略了那些仅仅出于好奇而显示一些信息的问题)。

本版是面向解决方案的

本书的第1版列举了很多脆弱点，而很少有解决方案。第1版讲述了如何破坏网络，却没有提出防止别人破坏的方法。这导致了很多人的批评，因为这样的版本充满着敌意。在本版本中，我对此进行了改变。我对许多攻击提出了修复和防止的方法。

关于选材

在这个版本中，我还省去了一些材料，包括讲述Bell实验室的Plan 9的那一章。

注意 Plan 9是Bell实验室在Lucent技术公司实现的一个实验操作系统。它主要的特性是

层次文件系统(有点像UNIX)、TCP/IP集成以及其本地文件系统和网络文件系统。Plan 9几乎可以运行在任何系统结构上，包括价格便宜的基于Intel的硬件，以及基于位图方式的显示器。Plan 9与其他操作系统的最主要区别在于Plan 9的网络使用方式和CPU服务器。处理器是集中式的，而文件存储在传统的网络上。在第1版中，我讨论Plan 9的安全特性，因为它有一点是其他操作系统所不同的：它没有与NT上的系统管理员(Administrtor)、Netware上的超级用户(Supervisor)以及UNIX上的根用户相类似的用户。

Plan 9是一个令人着迷的操作系统，其在网络处理方式上的构思是非常独特的，但是很少有人使用Plan 9。尽管在第1版中我们对其进行了描述，但是后来很少得知相关的信息了。

事实上，Microsoft的Windows NT现在成为了中小型业务所选用的平台。Internet现在成为了两个操作系统的栖息之所：Windows NT和UNIX。除这两个巨人之外，还有其他一些操作系统(如Windows 95和Mac OS)对Intranet及其子网进行控制。

链接和资源的修改

在第1版中充满着链接和参考文献。这些链接中的很大一部分到去年已经不再存在了。(许多WWW服务器和FTP站点都关闭了，而另外一些可能也重新组织了其结构。这样，导致了有404个资源再也找不到！)在这个版本中，我不但找到了原来资源的新位置，而且增加了几百个新的链接。

结构

本书第1版的结构比较差，在某些方面显得有些冗余，而另外一些内容放置的位置可能不是很适当。我在本版中对该问题进行了修改。本版最开始介绍一些技术的发展过程，然后讲述一些工具软件，最后介绍一些有关安全的参考文献。

注意 如果读者购买了第1版的话，会很高兴地发现本版保持了一些原来的格式。对于所讨论的每一个主题，都有一些在线参考文献的超链被嵌入到了正文之中，这样使得读者在希望详细了解有关主题时非常方便（例如，在讨论口令攻击时，本版给出了很多有关口令攻击的在线文档，如果读者希望对口令攻击进行仔细研究的话，可以下载这些文档，这些文档大多是工程师们书写的）。

本版更为清晰和简洁

最后，我要说的是第1版写得并不是很好。我希望这本书的这次改版能够给读者提供更多的经验和阅读的兴趣。

希望你以健康的心态和高尚的目的来阅读本书。

作者简介

作者把他自己描述成一个“UNIX螺旋桨头部”，一个Perl编辑语言、Linux和FreeBSD的忠实拥护者。

作者在加利福尼亚两家健康服务公司当了4年的系统管理人员。之后，便开始了他自己的安全咨询生意。现在，他专门测试各种网络平台的安全性，即闯入计算机网络，并发现导致

非法闯入的“漏洞”(hole)。他测试的平台包括Novell NetWare、Micrsoft WindowsNT、Sun OS、Solaris、 Linux和Microsoft Windows95。目前，他的主要任务是负责一个横跨洛杉矶到蒙特利尔的广域网的安全。

现在，作者同他的妻子平静地生活在南加利福尼亚州，他的家中有一台Sun SPARC工作站，一台IBM RS/6000,两台Pentiums，一台Macintosh和一台MicroVAX机。

在80年代末，作者曾因开发了一种破坏银行自动取款机系统安全性的技术，而被控犯有一系列经济罪行，因此作者选择使用匿名写书。

与原出版社联系

作为本书的读者，你是我们最为重要的评论家。我们非常重视你的观点，希望知道我们应该怎样做才对、如何才能做得更好，你希望看一些什么样的书籍，以及其他一些你认为对我们有所帮助的观点。

我们非常希望得到你的建议。你可以给我们发传真、发电子邮件，或者给我们写信，以便让我们知道你对本书优缺点的评价——这样我们才能把我们的书籍做得越来越好。

请注意，我不能对本书的技术问题提供帮助，而这却是我每天收到的邮件中的很大一部分，但是我却不能对每一封信都进行回复。

当你与我联系的时候，请确保在你的信函中包含本书的名称、作者，以及你的姓名、电话或传真的号码。我将非常仔细地了解你的观点，并告知书的作者和责任编辑。

FAX: 317-817-7070
E-mail: webdev@mcp.com
Mail: Mark Taber
Executive Editor,Web Development
Macmillan Computer Publishing
201 west 103rd Street
Indianspolis,IN 46290 USA

原书名: Maximum Security (Second Edition)
原书号: ISBN 0-672-31341-3

目　录

第三部分 工 具

第四部分 平台和安全

第五部分 进 阶

第六部分 远程攻击

第七部分 附 录

第一部分 开始阶段

第1章 我为什么要写这本书

当Sams要我写这本书的时候，我犹豫了一下。确实，这个题材对我而言是个巨大的机会，我自己十分乐意干这件工作。但我也知道这本书将会给自己招致相当大的批评。在我动笔以前，我打电话给编辑，向他们列举了我不能写这本书的理由。其中包括：

- 读者可能会出于不正当的目的而使用本书的内容。
- Internet安全协会的反对。
- 开发商会控告我们暴露他们软件中的缺陷。

编辑重视这些事件的后果，但并没有因此而气馁。他们认为公众应该知道这些信息。我同意他们的观点。这样，我们就开始同舟共济了。这结果是令人愉快的。

媒介分成了两派。一派认为这本书有新意，并且具有大量有用的信息，虽然它对安全确实带来了挑战。来自ZDNET的Ben Elgin就表达了这种观点。他写道：

“虽然本书中的许多章节中的黑客的观点被认作是非法的，但它确实给网站管理者提了个醒，通过对特定平台上和特定配置下的大量应用软件的恰如其份的评价，Web站点管理员将能更好地懂得如何保护他们的网络，如何检测何时何地安全出了问题。是处于最大安全状态下，还是处于致命的危险之中？”(1997年9月8日 Ben Elgin)

很多人赞同Ben Elgin的观点，说公开这样的信息将能加强Internet的安全性。一个来自Library Journal的充满实用主义的评论家甚至认为本书应该是系统管理员的必备手册：

“网络管理员应该仔细地阅读一下本书，因为有许多黑客将会认真地研读本书，并将找个地方来实践一下这些新技能，这些地方很可能就是你的LAN或Web服务器。”

当然，并不是每个人都喜欢本书的内容。在许多时候，本书被认为是投市场所好，是为了冲击一下现有的网络秩序，是一种耸人听闻文化的典型。因此，在写第2版之际，我将用更多的笔触来强调我为什么要写这本书。

这些理由可以简化成：Sams出版了本书(当然我同意写这本书)，是因为现实中确实有对它的真正的需求。在后面的段落中，我将解释这些需要。

1.1 安全需要的现实性

每天，有成千上万的研究所、商家和个人上网。这种现象——它已经有了一打以上的不同的名字——通常被叫作Internet爆炸，这种爆炸已经彻底改变了Internet的构成。

10年以前，绝大多数服务器维护人员具有最起码的安全知识。当然，这并不能防止入侵，只是与潜在的目标相比，被入侵的比例很小而已。

而今天，普通人就可以建立Internet服务器，他们中的绝大多数都没有安全方面的经验。这样的服务器每天都在增长。然而，那些公司无视于这种危险的状态，而只是一味地强调上

网的数量。他们说，Internet是安全的，不必担心会发生什么事。这是真的吗？其实并非如此。

那些市场营销人员总是在信口开河。因为，他们甚至搞不清楚他们在说些什么。事实是，Internet并不安全，它连中等的安全都达不到。

而使这种情况变得更加糟糕的是那些计算机工业界的权威们还在对公众进行误导。他们异乎寻常地宣称他们的安全产品，使普通的消费者信以为真。我担心的是事实可能要比我们想象的更为严重：黑客或网络破译者每个月都在攻破新的工业安全机制。

Microsoft PPTP

一个典型的例子是Microsoft 公司的点对点通道协议(PPTP,Point-to Point Tunneling Protocol)。PPTP协议用于在Internet上建立虚拟个人网(VPN,Virtual Private Nerwork)。VPN具有安全机制，在共用的两点之间进行加密传输，这样，就可以减少租用线路(通过VPN公司就可以把Internet当作自己的租用线路)。

Microsoft 对PPTP的实现方式被称为是用户所能得到的最佳安全标准。实际上，PPTP已经获得了不少荣誉。在计算机杂志上，它总是被作为一种工业标准的解决方案。这真不赖!

在本书付印之前的一个月，Microsoft 的PPTP就被一个著名的密码专家给破译了。这则消息震惊了整个计算机安全界。这里有一个评论：

“难道Microsoft 不能做得更好吗？也许你认为他们会的。他们所犯的错误并不小。他们所提供的保密机制任何一个蹩脚的密码破译者都能够破译。这种加密机制根本就没有考虑到它的效果。他们的文档宣称密匙有128位长，但实际上并没有使用那么长。并且，由Hash函数所保护的口令是如此的糟糕，以致在大多数时候它们可以很容易地被发现。还有，PPTP控制通道的设计是如此草率，以致每个人都可以造成PPTP服务器‘胀死’。”(Microsoft 的PPTP 实现，常用问题解答技术小组。地址：http://www.counterpane.com/pptp-faq.html)

这看上去好像Microsoft的PPTP并不安全，是吧？研究人员发现了PPTP实现方式中的五个缺陷，包括口令杂凑中的漏洞以及验证和加密中的不足。简而言之，他们发现Microsoft的PPTP的实现方式简直就是一场灾难。

我可以打赌你从不知道这种意见。若你没有，那么你就像全国各地的公司中的信息官员一样。他们相信他们所使用的产品是安全的。毕竟，Microsoft是一个巨大的、有着良好声誉的公司。如果他们宣称他们的产品是安全的，那就准是安全的。

这就是当今普通网络管理员的心态，成千上万的公司因此而处于危险之中。

注意　像上述类型的错误总在发生着。这里有一个有趣的例子：最近发现，Microsoft的Windows NT中的加密机制可以被有效地关闭。这个攻击方法现在已被称作是“You Are Now in France”。其工作方式是：由于法国不允许普通公众对具有高度保密信息的站点进行访问，因此如果Windows NT把用户的工作地点解释为法国，那么，NT强大的加密机制就被禁止了。NT也不安全，是吧？

最佳的保密方式是自己的命运由自己掌握。也就是说，只有自己才能掌握自己数据的安全尺度。不要指望任何一个开发商来为你解决问题，若你一定要这样做，那么你将成为一个十分不幸的人。

1.2 问题之源

软件开发商的虚假广告只是问题的一个方面，而问题的根本原因则在其他地方。其中三