

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。

Anonymous: Maximum Security (Second Edition).

Authorized translation from the English language edition published by Sams Publishing.

Copyright 1998 by Sams Publishing.

All rights reserved. For sale in Mainland China only.

本书中文简体字版由机械工业出版社出版,未经出版者书面许可,本书的任何部分不得以任何方式复制或抄袭。

本书封底贴有Prentice Hall 防伪标签,无标签者不得销售。

版权所有,翻印必究。

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: 陈剑甬

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)

凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换

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、Microsoft 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

Indianapolis, IN 46290 USA

原书名: Maximum Security (Second Edition)

原书号: ISBN 0-672-31341-3

目 录

译者序
前言

第一部分 开始阶段

第1章 我为什么要写这本书	1
1.1 安全需要的现实性	1
1.2 问题之源	2
1.2.1 目标主机的错误配置	3
1.2.2 系统缺陷或开发商缺乏反应	4
1.2.3 为什么安全培训是重要的	6
1.3 法人方面	6
1.4 政府	7
1.5 孤独的远程网络冲浪	8
1.6 小结	9
第2章 如何使用本书	10
2.1 怎样用本书	10
2.2 几种工具的下载地址	10
2.2.1 FTP客户程序	10
2.2.2 压缩文件格式	11
2.2.3 文本文件格式	11
2.3 编程语言	12
2.4 本书使用方法	13
2.4.1 学习Internet安全的基本知识	13
2.4.2 利用本书保护网络安全	13
2.4.3 利用本书作安全研究	13
2.5 本书的局限性	14
2.5.1 时效性	14
2.5.2 功用性	14
2.6 本书结构	14
2.7 本书的零碎问题	15
2.8 小结	16

第二部分 理解领域范围

第3章 网络的产生: Internet	17
---------------------	----

3.1 产生(1962~1969)	17
3.2 UNIX的产生(1969~1973)	18
3.3 C语言	19
3.3.1 Internet的形成期(1972~1975)	19
3.3.2 进入UNIX时代	20
3.3.3 UNIX和Internet的共同发展	20
3.3.4 UNIX的基本特征	21
3.3.5 X Windows系统	22
3.3.6 UNIX上运行的应用程序	23
3.3.7 UNIX与Internet安全的关系	24
3.4 继续: 现代Internet	24
3.4.1 Internet服务提供者	25
3.4.2 将来	25
3.5 小结	26
第4章 TCP/IP简介	27
4.1 什么是TCP/IP	27
4.1.1 TCP/IP协议包中的协议类型	27
4.1.2 TCP/IP历史	27
4.1.3 哪些平台支持TCP/IP	28
4.2 TCP/IP的工作	29
4.3 协议	29
4.4 TCP/IP就是Internet	39
4.5 小结	39
第5章 黑客和破译者	40
5.1 黑客和破译者之间的区别	40
5.1.1 Mens Rea	40
5.1.2 计算机语言	40
5.1.3 Randal Schwartz	41
5.2 所有这些从何处开始	43
5.3 今日状况: 网络战争	45
5.3.1 黑客举例	46
5.3.2 破译者举例	46
5.4 小结	47
第6章 黑客攻击的对象	48

VIII

6.1 术语“被破译”的意思	48
6.2 政府	48
6.2.1 国防信息系统网络	50
6.2.2 美国的海军和NASA	50
6.2.3 对五角大楼的攻击	51
6.2.4 政府安全	52
6.2.5 总统关键设施保护委员会	53
6.2.6 国家设施保护中心	54
6.2.7 对政府工作漏洞的总结	55
6.3 公共站点	55
6.3.1 StarWave事件	56
6.3.2 其他信用卡案例	56
6.3.3 趋势	57
6.3.4 Farmer的安全综述: Dusting Moscow	57
6.3.5 Ernst & Young LLP/Information Week的信息安全综述	58
6.4 警告	58
6.5 小结	58
第7章 Internet战争	60
7.1 Internet可以改变你的生活	60
7.2 我们不能很好相处吗	60
7.3 朋友或敌人	60
7.4 Internet可以用作间谍活动吗	61
7.5 威胁将更个人化	61
7.5.1 谁掌握了秘密	62
7.5.2 美国能保护国家信息设备的 安全吗	63
7.6 信息攻击将会是什么样子	63
7.7 Y2K	65
7.8 不远的未来	67
7.9 小结	67
7.10 关于信息战的资源	67
7.11 关于信息战的书	69
7.12 关于Y2K的资源	70
7.13 Y2K的书	71
第8章 安全概念	72
8.1 我们迫切需要Internet	72
8.2 评估公司的特殊状况	72

8.3	认证和承诺	72
8.3.1	Cooper & Lybrand L.L.P., Resource Protection Services	73
8.3.2	The American Institute of Certified Public Accountants	73
8.3.3	International Computer Security Association	74
8.3.4	Troy Systems	74
8.3.5	做为保证而非责任的认证	75
8.4	在哪儿接受训练	75
8.5	一般训练	75
8.5.1	Lucent Technologies, Inc	75
8.5.2	Great Circle Associates, Inc	76
8.5.3	Learning Tree International	76
8.5.4	NSC System Group, Inc	76
8.5.5	Training On Video	77
8.6	高级训练	77
8.7	用Co-Location方法解决	78
8.8	雇佣外面的安全顾问	79
8.8.1	花费	79
8.8.2	根本问题	81
8.8.3	关于你的系统管理员	82
8.9	顾问和其他解决方案	82

第三部分 工 具

第9章 破坏性设备	83
9.1 什么是破坏性设备	83
9.1.1 破坏性设备对安全的威胁	83
9.1.2 电子邮件炸弹	83
9.1.3 电子邮件炸弹程序包	83
9.1.4 电子邮件炸弹的处理	84
9.1.5 电子邮件炸弹对安全的威胁	85
9.1.6 列表链接	85
9.1.7 邮件中继	86
9.1.8 服务拒绝攻击	86
9.1.9 你将会在哪里发现服务拒绝攻击	87
9.1.10 服务拒绝目录	87
9.1.11 著名的服务拒绝攻击	88
9.1.12 对硬件的服务拒绝攻击	94

9.1.13 其他的拒绝服务工具	94	11.1 口令攻击程序的概念	127
9.1.14 其他的拒绝服务资源	96	11.1.1 口令破译者如何工作	127
9.1.15 病毒	96	11.1.2 密码学	128
9.1.16 什么是计算机病毒	96	11.1.3 ROT-13	128
9.1.17 谁编写病毒及其原因	97	11.1.4 DES与Crypt	129
9.1.18 病毒是如何产生的	97	11.2 口令攻击程序的重要性	131
9.1.19 病毒是用何种语言编写的	98	11.3 口令攻击程序	132
9.1.20 病毒是如何工作的	98	11.4 用于Windows NT的口令攻击程序	132
9.1.21 主引导区记录病毒	99	11.4.1 10phtCrack 2.0	132
9.1.22 反病毒工具	102	11.4.2 Midwestern Commerce公司的 ScanNT	132
9.1.23 相关文献及站点	103	11.4.3 Somarsoft的NTCrack	133
9.2 小结	104	11.4.4 Midwestern Commerce公司的 Passwd NT	133
第10章 扫描程序	105	11.5 UNIX上的口令攻击程序	134
10.1 扫描程序怎样工作	105	11.5.1 Crack	134
10.2 哪些平台上有扫描程序	105	11.5.2 Jackal的CrackerJack	136
10.3 运行扫描程序的系统要求	105	11.5.3 PaceCrack95	136
10.4 创建扫描程序的难度	106	11.5.4 Crypt Keeper的Qcrack	137
10.5 扫描程序合法吗	106	11.5.5 Solar Designer的John the Ripper	137
10.6 扫描程序对Internet安全的重要性	106	11.5.6 Remote和Zabkar的Hades	137
10.7 扫描程序对安全所造成的影响	106	11.5.7 Sorcerer的Star Cracker	138
10.8 扫描程序	107	11.5.8 Racketeer和Presense的 Hellfire Cracker	138
10.8.1 Nessus	107	11.5.9 Roche's Crypt的XIT	138
10.8.2 NSS	111	11.5.10 Grenadier的Claymore	139
10.8.3 Strobe	112	11.5.11 Christian Beaumont的Guess	139
10.8.4 SATAN	114	11.5.12 Computer Incident Advisory Capability(CIAC)DOE的 Merlin	139
10.8.5 Ballista	115	11.6 其他类型的口令攻击程序	140
10.8.6 Jakal	116	11.6.1 Michael A.Quinlan的ZipCrack	140
10.8.7 IdentTCPscan	116	11.6.2 Fast Zip 2.0	141
10.8.8 Ogre	117	11.6.3 Gabriel Fineman的Decrypt	141
10.8.9 WebTrends Security Scanner	118	11.6.4 Glide	141
10.8.10 Internet Security Scanner和 SAFEsuite	118	11.6.5 AMI Decode	141
10.8.11 防护墙的另一侧	122	11.6.6 James O' Kane的NetCrack	141
10.8.12 CONNECT	123	11.6.7 Mark Miller的PGPCrack	142
10.8.13 FSPScan	123		
10.8.14 XSCAN	123		
10.9 在其他平台上	124		
10.10 小结	126		
第11章 口令攻击程序	127		

11.6.8 Richard Spillman的ICS Toolkit	142	13.6.8 NetMinder Ethernet	164
11.6.9 E.Kuslich的EXCrack	142	13.6.9 IBM的DatagLANce网络分析器	164
11.6.10 Lyal Collins的CP.EXE	143	13.6.10 LinkView Internet监视器	165
11.7 资源	143	13.6.11 ProConvert	165
11.7.1 关于UNIX口令安全	143	13.6.12 LANdecoder32	165
11.7.2 其他资源和文档	145	13.6.13 NetXRay Analyzer	166
11.8 小结	146	13.6.14 NetAnt协议分析器	166
第12章 特洛伊木马	147	13.7 可免费获取的嗅探程序	166
12.1 什么是特洛伊木马	147	13.7.1 Esniff	166
12.2 特洛伊是来自何处	148	13.7.2 Gobbler	166
12.3 特洛伊出现在哪里	149	13.7.3 ETHLOAD	168
12.4 特洛伊被真正发现的频度	150	13.7.4 Netman	168
12.5 特洛伊表明什么层次的危险	151	13.7.5 LinSniff	169
12.6 怎样检测特洛伊	151	13.7.6 Sunsniff	169
12.6.1 MD5	153	13.7.7 linux_sniffer.c	169
12.6.2 Hobgoblin	156	13.8 抵御嗅探器的攻击	170
12.6.3 在其他平台上	157	13.9 检测和消灭嗅探器	170
12.7 资源	157	13.9.1 安全的拓扑结构	171
12.8 小结	158	13.9.2 会话加密	172
第13章 嗅探器	159	13.10 小结	172
13.1 嗅探器的安全危害	159	13.11 关于嗅探器方面更多的资料	172
13.1.1 局域网与数据流量	159	第14章 防火墙	174
13.1.2 报文发送	160	14.1 防火墙简介	174
13.2 嗅探器能够造成的危害	160	14.2 防火墙执行的其他任务	174
13.3 是不是真的有人发现过嗅探器的攻击	160	14.3 防火墙构件	174
13.4 嗅探器获取的信息	161	14.4 防火墙的类型	175
13.5 嗅探器在何处出现	162	14.4.1 网络级防火墙	175
13.6 从何处可以得到嗅探器	162	14.4.2 应用-代理防火墙(应用网关)	175
13.6.1 商用嗅探器	162	14.4.3 确信信息系统防火墙工具包	176
13.6.2 Network Associates公司的ATM嗅探式网络分析器	162	14.5 防火墙综述	177
13.6.3 Shomiti系统公司的Century LAN分析器	162	14.6 创建防火墙的重要步骤	178
13.6.4 Klos Technologies公司的PacketView	163	14.6.1 确定拓扑结构、应用和协议需求	178
13.6.5 Network Probe 8000	163	14.6.2 分析本组织中的可信任关系	178
13.6.6 LANWatch	163	14.6.3 制定规则并选择合适的防火墙	179
13.6.7 EtherPeek	164	14.6.4 使用及测试防火墙	179
		14.6.5 防火墙的安全问题	179
		14.6.6 Cisco PIX DES漏洞	179
		14.6.7 Firewall-1保留关键字漏洞	180

14.7 商用防火墙	180
14.7.1 Alta Vista Firewall 98	180
14.7.2 ANS InterLock	180
14.7.3 Avertis	180
14.7.4 BorderManager	181
14.7.5 Conclave	181
14.7.6 CSM Proxy/Enterprise Edition	181
14.7.7 CyberGuard防火墙	181
14.7.8 CyberShield	182
14.7.9 Elron防火墙/Secure	182
14.7.10 FirewallA 3.0	182
14.7.11 Gauntlet Internet防火墙	182
14.7.12 GNAT防火墙盒	182
14.7.13 Guardian	183
14.7.14 IBM eNetwork防火墙	183
14.7.15 Interceptor防火墙工具	183
14.7.16 NETBuilder	183
14.7.17 NetRoad TrafficWARE防火墙	183
14.7.18 NetScreenA0	184
14.7.19 PIX防火墙4.1	184
14.7.20 Raptor防火墙	184
14.7.21 Secure Access	184
14.7.22 SecurIT防火墙	185
14.7.23 SunScreen	185
14.8 小结	185
第15章 日志和审计工具	188
15.1 日志工具	188
15.2 使用更多日志工具的原因	188
15.3 网络监视和数据收集	189
15.3.1 SWATCH	189
15.3.2 Watcher	189
15.3.3 lsof	190
15.3.4 WebSense	190
15.3.5 适用于防火墙和VPN的 WebTrends	190
15.3.6 Win-Log V1	191
15.3.7 MLOG	191
15.3.8 NOCOL/NetConsole V4.0	192
15.3.9 PingLogger	192

15.4 分析日志文件的工具	192
15.4.1 NestWatch	192
15.4.2 NetTracker	192
15.4.3 LogSurfer	193
15.4.4 VBStats	193
15.4.5 Netlog	193
15.4.6 Analog	193
15.5 特别日志工具	194
15.5.1 Courtney	194
15.5.2 Gabriel	194
15.6 小结	195

第四部分 平台和安全

第16章 漏洞	197
16.1 漏洞的概念	197
16.2 关于时间性	197
16.3 漏洞如何出现	198
16.4 开采数据	198
16.5 究竟需要多大的安全度	199
16.6 一般资源	199
16.6.1 计算机紧急事件反应小组	199
16.6.2 美国能源部计算机事件咨询库	200
16.6.3 国立标准和技术协会计算机 安全资源交换所	201
16.6.4 美国国防部网络信息中心	201
16.6.5 BUGTRAQ文档	202
16.6.6 事件响应和安全小组论坛	202
16.6.7 Windows 95 bug文档	202
16.7 邮件列表	203
16.8 usenet新闻组	204
16.9 厂家安全邮件列表、补丁仓库以及 资源	204
16.9.1 Silicon Graphics安全总部	204
16.9.2 Sun安全公告文档	205
16.9.3 ISS NT安全邮件列表	205
16.9.4 国立健康协会	205
16.9.5 计算机和网络安全参考目录	205
16.9.6 Eugene Spafford的安全活动表	205
16.10 小结	205

第17章 微软	206	Agent	213
17.1 DOS	206	17.10.16 Fortres 101	213
17.2 IBM兼容	206	17.11 微软应用软件的新弱点	213
17.3 键盘捕获工具	207	17.11.1 Microsoft Internet Explorer	213
17.4 DOS访问控制软件	207	17.11.2 Microsoft Frontpage	216
17.4.1 Secure 1.0	207	17.11.3 Microsoft Exchange	217
17.4.2 Secure File System(SFS)	207	17.11.4 其他应用软件及其附件	218
17.4.3 Sentry	207	17.11.5 其他微软应用软件	220
17.4.4 Encrypt-It	208	17.11.6 其他应用软件	221
17.4.5 LCK2	208	17.11.7 小结	221
17.4.6 Gateway 2	208	17.11.8 Windows NT	221
17.5 DOS安全工具	208	17.11.9 IIS	221
17.5.1 Simtel DOS安全索引	208	17.11.10 Windows NT的常见安全弱点	224
17.5.2 CIAC DOS安全工具主页	208	17.12 Windows NT内部安全	225
17.5.3 Cypher.net的DOS安全工具	208	17.12.1 内部安全概述	225
17.5.4 Oakland.edu的仓库	208	17.12.2 RDISK漏洞	225
17.6 Windows for Workgroups及		17.12.3 改善内部安全	226
Windows 95	208	17.12.4 重新设置一个安全的NT	
17.7 password list (PWL)口令方案	209	服务器	226
17.8 破译pwl文件	209	17.12.5 工具	226
17.9 Flushing高速缓存中的口令	209	17.12.6 一些极好的在线信息资源	231
17.10 基于Windows 95的访问控制软件	210	17.12.7 Windows NT安全参考书	233
17.10.1 Cetus StormWindows	210	17.13 小结	234
17.10.2 Clasp 97	210	第18章 UNIX	235
17.10.3 Assist技术公司的		18.1 从头开始	235
Configsafe 95	210	18.2 物理安全问题的提出	235
17.10.4 DECROS有限公司的DECROS		18.3 控制台安全	236
安全卡	211	18.3.1 控制台口令	236
17.10.5 Desktop Surveillance 97	211	18.3.2 根口令	236
17.10.6 Nerds Unlimited的Future Lock	211	18.4 安装媒介	237
17.10.7 HD95 Protect	211	18.5 缺省配置	237
17.10.8 Secure 4U	211	18.6 口令安全	237
17.10.9 PCSL的Stoplock 95	212	18.7 安装口令预检程序	239
17.10.10 Posum的Windows Task-Lock	212	18.7.1 passwd+	239
17.10.11 Cyber Watch	212	18.7.2 anlpaswd	240
17.10.12 WP WinSafe	212	18.7.3 npaswd	240
17.10.13 Safe Guard	212	18.8 补丁	240
17.10.14 Secure Shell	213	18.9 特殊的脆弱性	241
17.10.15 Formlogic Surveillance		18.9.1 AIX的严重的远程弱点	241

18.9.2 IRIX的严重的远程弱点	243	19.16 保护和管理Novell网络的工具	278
18.9.3 SunOS和Solaris的严重的 远程弱点	243	19.16.1 审核追踪	279
18.9.4 linux的严重的远程弱点	244	19.16.2 ProtecNet for NetWare	279
18.10 下一步: 检查服务	245	19.16.3 LatticsNet网络管理系统	279
18.10.1 rServices	245	19.16.4 LT Auditort+ V6.0	279
18.10.2 finger Service	246	19.16.5 Novell NetWare Kana安全 分析工具	280
18.10.3 Telnet	246	19.16.6 来自Baseline Software公司的 信息安全策略	280
18.10.4 FTP	247	19.16.7 MenuWorks	280
18.10.5 常规FTP	248	19.16.8 AuditWare for NDS	281
18.10.6 TFTPDP	249	19.16.9 WSetPass 1.55	281
18.10.7 Gopher	250	19.16.10 WnSyscon 0.95	281
18.10.8 网络文件系统	250	19.16.11 BindView EMS	281
18.10.9 HTTP	251	19.16.12 SecureConsole	281
18.10.10 保持文件系统的—个记录	252	19.16.13 GETEQUIV.EXE	282
18.11 关于X	253	19.17 破译Novell网络或测试它们安 全性的工具	282
18.12 检查列表及指南	254	19.18 Getit	282
18.13 部分UNIX攻击工具	255	19.19 Burglar	282
18.14 出版物和一些其他工具	271	19.20 Spooflog	282
18.14.1 书	271	19.21 Setpass	282
18.14.2 在线出版物	271	19.22 NWPCRAK	283
18.15 小结	272	19.23 IPXCntrl	283
第19章 Novell	273	19.24 Crack	283
19.1 Novell的内部安全	273	19.25 Snoop	283
19.2 缺省口令	274	19.26 Novelbfh.exe	283
19.3 标识弱点	274	19.27 其他Novell破译工具	284
19.4 登录脚本弱点	274	19.28 资源	284
19.5 嗅探器和Novell	275	19.28.1 资源集合	284
19.6 NetWare远程攻击	275	19.28.2 Usenet新闻组	285
19.7 PERL漏洞	275	19.28.3 书	285
19.8 登录协议攻击	276	第20章 VAX / VMS	286
19.9 欺骗	276	20.1 VMS	288
19.10 服务拒绝	277	20.2 VMS的安全性	288
19.11 Novell Net Ware 4.x上的TCP/IP 服务拒绝	277	20.3 一些老的漏洞	290
19.12 对于服务拒绝攻击的FTP脆弱性	278	20.3.1 Mountd漏洞	290
19.13 第三方问题	278	20.3.2 监视器工具的漏洞	290
19.14 Windows漏洞	278	20.3.3 历史上的问题: Wank 蠕虫	
19.15 Windows NT漏洞	278		

事件	290
20.4 审计与监视	291
20.4.1 watchdog.com	292
20.4.2 Stealth	292
20.4.3 GUESS_PASSWORD	292
20.4.4 WATCHER	292
20.4.5 Checkpass	293
20.4.6 Crypt	293
20.4.7 DIAL	293
20.4.8 CALLBACK.EXE	293
20.4.9 TCPFILTER(G.Gerard)	293
20.5 时代变了	294
20.6 小结	294
20.7 资源	294
第21章 Macintosh	296
21.1 建立一个Macintosh Web 服务器	296
21.1.1 WebSTAR的挑战	296
21.1.2 Blue World的Lasso	297
21.1.3 挖掘自己的潜能	298
21.2 Macintosh 平台的弱点	298
21.2.1 FoolProof弱点	298
21.2.2 由于端口溢出而服务拒绝	299
21.2.3 MacDNS 错误	299
21.2.4 Death序列和WebSTAR	299
21.2.5 DiskGuard 错误	300
21.2.6 Retrospect 弱点	301
21.2.7 At Ease 错误	301
21.2.8 NetWork Assistant	301
21.2.9 MacOS 8.0升级版的口令 安全性	302
21.3 关于文件共享及安全性	302
21.3.1 服务器管理以及安全性	303
21.3.2 AG Group 的EtherPeek v.3.5	303
21.3.3 Dartmouth Software Development 的InterMapper 2.0	304
21.3.4 Interlink Computer Sciences公司的 NetLock	304
21.3.5 Cyno 的MacRadius	305
21.3.6 Network Security Guard	305

21.3.7	Network Scout 1.0	306
21.3.8	Timbuktu Pro 4.0	306
21.3.9	内部安全	306
21.4	口令破译以及相关的工具	309
21.4.1	PassFinder	309
21.4.2	FirstClass Thrash!	309
21.4.3	FMPProPeeker1.1	310
21.4.4	FMP Password Viewer Gold 2.0	310
21.4.5	MasterKeyII	310
21.4.6	Password Killer	310
21.4.7	Killer Cracker	310
21.4.8	MacCrack	310
21.4.9	Remove Passwords	311
21.4.10	RemoveIt	311
21.5	小结	311
21.6	资源	311
21.6.1	书和报告	311
21.6.2	工具和军需品站点	312
21.6.3	电子杂志和电子在线杂志	312

第五部分 进阶

第22章 谁是主管	315
22.1 一般概念	315
22.2 关于访问控制	317
22.3 关于得到根	318
22.3.1 许可系统的Pros和Cons	318
22.3.2 破译根	319
22.4 根也许会成为历史	319
22.5 其他操作系统的根	320
22.6 小结	320
第23章 内部安全	321
23.1 内部安全	321
23.2 我们确实需要内部安全吗	321
23.3 为什么内部攻击如此普遍	321
23.4 关于规定	322
23.5 硬件考虑	322
23.6 驱动器、目录以及文件	325
23.7 一般内部安全评估	326
23.8 内部安全扫描器	326

23.8.1 SysCAT	326
23.8.2 SQLAuditor	327
23.8.3 System Security Scanner(S3)	328
23.8.4 RSCAN	329
23.9 控制雇员访问Internet	329
23.9.1 Bess School and Business Filters 的N2H2	330
23.9.2 WebSENSE	331
23.9.3 X-STOP	331
23.9.4 Sequel Net Access Manager	331
23.9.5 SmartFilter	332
23.10 开发最实用的核对表	332
23.11 小结	334

第六部分 远程攻击

第24章 远程攻击	335
24.1 何谓远程攻击	335
24.2 第一步骤	335
24.3 获取网络概况	335
24.3.1 WHOIS	337
24.3.2 finger和rusers	338
24.4 操作系统	339
24.5 考察阶段	340
24.5.1 识别系统中的关键弱点	340
24.5.2 系统弱点的数据收集	341
24.6 进行测试运行	343
24.7 小结	343
第25章 攻击级别	345
25.1 攻击何时发生	345
25.2 破译者使用什么操作系统	346
25.2.1 Sun	346
25.2.2 UNIX	347
25.2.3 Microsoft	347
25.3 攻击的起源	347
25.4 典型的攻击者是什么样的人	347
25.5 典型的目标是什么样子	348
25.6 他们为何要攻击	349
25.7 关于攻击	349
25.8 Sams破译级别索引	352

25.8.1 敏感级	352
25.8.2 响应级	357
25.9 小结	358
25.10 资源	358
第26章 电子欺骗攻击	361
26.1 什么是电子欺骗	361
26.2 Internet 安全基础	361
26.2.1 认证的方法	361
26.2.2 RHOSTS	361
26.3 电子欺骗攻击机制	363
26.4 一次成功电子欺骗攻击的因素	364
26.5 猜序数	364
26.5.1 打开一个更合适的漏洞	364
26.5.2 谁能受欺骗	364
26.5.3 电子欺骗攻击普遍吗	365
26.6 关于IP电子欺骗的文档	366
26.7 我们怎样防止IP电子欺骗	367
26.8 其他奇怪和不规则的电子欺骗攻击	368
26.8.1 ARP电子欺骗	368
26.8.2 DNS电子欺骗	368
26.9 小结	369
第27章 基于远程登录攻击	370
27.1 Telnet	370
27.1.1 虚拟终端	370
27.1.2 Telnet安全的历史	371
27.1.3 修改环境	373
27.1.4 终端仿真	374
27.1.5 这些攻击不再有效了吗	377
27.1.6 Telnet作为一种武器	377
27.2 小结	379
27.3 资源	380
第28章 语言、扩展和安全	382
28.1 WWW崛起	382
28.2 CGI和安全	382
28.2.1 实用摘要和报告语言 (Perl)	383
28.2.2 Perl安全	383
28.2.3 特权方式下运行脚本程序的 问题	385
28.2.4 文件产生	385

28.2.5 服务器侧includes	385
28.2.6 Java	386
28.3 ActiveX	388
28.4 脚本语言	390
28.4.1 JavaScript	390
28.4.2 VBScript	391
28.4.3 走近脚本语言	391
28.5 小结	391
第29章 隐藏身份	392
29.1 暴露程度	392
29.2 Web浏览和侵权	393
29.2.1 Internet与隐私	393
29.2.2 用户信息在服务器上是怎样 存储的	393
29.2.3 finger	394
29.2.4 MasterPlan	396
29.2.5 除finger外的其他途径	397

29.3 浏览器的安全性	397
29.4 cookie	399
29.5 用Lucent技术解决隐私问题	402
29.6 用户Email地址和Usenet	405
29.6.1 DejaNews	407
29.6.2 WHOIS服务	407
29.7 警告	411

第七部分 附 录

A 安全图书书目——进一步读物	415
B 如何得到更多信息	426
C 安全顾问	447
D 参考文献	485
E 实质性内容：计算机安全与法律	497
F CD-ROM上的内容	509
G 安全术语	522

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 Network)。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。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。他们的文档宣称密钥有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