

Hackers Beware

HACKERS

ATTACK

INF

FUTURE TECHNOLOG

BEWARE

黑客

——攻击透析与防范

[美] Eric Cole 著

苏雷 等译

全接触

New
Riders



电子工业出版社
Publishing House of Electronics Industry
www.phei.com.cn

黑 客

——攻击透析与防范

Hackers Beware

[美] Eric Cole 著

苏 雷 等译

電子工業出版社

Publishing House of Electronics Industry

北京·Beijing

内 容 简 介

本书全面、系统地介绍了关于网络安全技术的知识和相关问题。书中主要介绍了能够成功保护网络系统免受攻击的方法,并且对各种攻击的机理进行了全面的论述。本书的突出特点:全面跟踪了当前黑客攻击的关键技术和方法,针对不同对象和情况,提出了不同的防范策略,具有很强的实用性和时效性。本书结构合理、内容翔实,有助于训练安全方面的专门人才,使他们能够更好地对各种威胁做出正确的反应,使防范工作做在攻击者的前面。本书还可以为网络管理员、系统管理员在预防黑客方面提供有效的安全防范与管理策略。

Authorized translation from the English language edition published by New Riders Publishing. Copyright © 2001. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher. Simplified Chinese language edition published by Publishing House of Electronics Industry, Copyright © 2002.
本书中文简体版专有翻译出版版权由Pearson教育集团所属的New Riders Publishing授予电子工业出版社。其原文版权及中文翻译出版版权受法律保护。未经许可,不得以任何形式或手段复制或抄袭本书内容。

图书在版编目(CIP)数据

黑客——攻击透析与防范/(美)科尔(Cole, E.)著;苏雷等译.-北京:电子工业出版社,2002.1

书名原文:Hackers Beware

ISBN 7-5053-7435-4

I. 黑... II. ①科... ②苏... 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(2001)第097835号

书 名:黑客——攻击透析与防范

原 书 名:Hackers Beware

著 者:[美] Eric Cole

译 者:苏 雷 等

责任编辑:谭海平 杜 萌

排版制作:今日电子公司制作部

印 刷 者:北京天竺颖华印刷厂

出版发行:电子工业出版社 www.phei.com.cn

北京市海淀区万寿路173信箱 邮编:100036

经 销:各地新华书店

开 本:787×1092 1/16 印张:37 字数:923千字

版 次:2002年1月第1版 2002年1月第1次印刷

书 号:ISBN 7-5053-7435-4

TP·4287

定 价:59.00元

著作权合同登记号 图字:01-2001-1463

凡购买电子工业出版社的图书,如有缺页、倒页、脱页、所附磁盘或光盘有问题者,请向购买书店调换。若书店售缺,请与本社发行部联系调换。联系电话:88211980 68279077

译 者 序

在 Internet 高速发展的今天，黑客攻击越来越受到全社会的广泛关注，采用适当的安全技术成为保证网络系统正常运转的必要条件。但是由于各种原因，人们对黑客和网络安全存在很多误解。如今，任何计算机都不可能孤立存在，都需要通过网络相互通信。由于各种网络系统以及有关软硬件系统的缺陷、各种系统管理方面的漏洞，导致了許多安全隐患，出现了许多严重的网络安全问题。

本书作者 Eric Cole 曾是美国中央情报局的雇员，现为 SANS（系统管理、网络互联和安全研究机构）的发言人。他在网络安全方面拥有丰富的实践经验和扎实的理论基础。

网络安全并不是一句空话，需要实实在在的防范措施。但是在实施具体的措施之前，必须对黑客攻击进行充分的了解。本书介绍了关于黑客攻防和网络安全的知识，从黑客攻击的原因和方法入手，介绍了黑客在攻击前的准备，详细地讲述了攻击者使用的方法和工具。本书深入研究了黑客的心理并详细描述了攻击过程，对黑客攻击的每个阶段和各个方面，包括原理、功能、实施方法，都有实例加以说明。书中内容与各种漏洞和攻击原理以及攻击所使用的工具有关。本书还对 Windows 和 UNIX 操作系统所存在的主要漏洞，以及各种升级版本和补丁做了深入说明。更有价值的是，本书为系统安全性较脆弱或系统安全方面存在较多漏洞的各种网络提供了一系列的解决方法，并着重强调了根据 SANS 十大漏洞列表，修补主要的网络安全漏洞的必要性。

本书共 20 章，分别介绍了关于信息搜集、欺骗、会话劫持、拒绝服务攻击、缓冲区溢出攻击、口令安全等知识，同时结合实际介绍了口令破解和攻击实例，并讨论了黑客是如何保留访问权限和隐藏踪迹的。书中的案例非常典型，具有现实意义，相信每个读者都会受益匪浅。本书语言生动，内容深入浅出，讲解细致全面，是网络安全人员的必备参考书，也适合具备计算机基础知识的读者。本书的读者应具备有关网络、操作系统、TCP/IP、HTML、Perl 或 C 语言等方面的基础知识。

本书由苏雷等翻译。参加翻译工作的还有：严静东、郭文明、贾振华、李冰、杨晓静、严炎、张立莉、王建东、范卫国、范永欣、章颖。参加审校工作的有：蔡开裕、曹介南、程健、窦勇、葛颖增、耿卫东、李恒年、李晓敏、刘宏伟、柳靖、彭秀文、石雄、孙宁、孙逊、陶菲、田兴彦、汪诗林、韦海亮、伍湘君、肖其英、袁静、徐钦桂、杨文、杨秀合、于贵桃、俞刚、余再祥、张永和、赵立军、郑军、周立、朱东升。该书在翻译和出版过程中得到了许多专家和同行的大力帮助和支持，在此谨向他们表示衷心的感谢，并向所有为本书中文版出版做出贡献的人们表示谢意。

由于本书内容新、翻译难度大、翻译时间非常紧迫，加之译者水平有限，错误和疏漏在所难免，恳请广大读者批评指正。

关于作者

Eric Cole 曾是美国中央情报局的雇员，现为 SANS（系统管理、网络互联和安全研究机构）的高级发言人。他拥有纽约技术学院的理科学士学位和理科硕士学位，现在正在攻读网络安全博士学位，专攻入侵检测与隐蔽技术。Eric Cole 在信息安全的诸多方面都有着广泛的经验，其中包括加密技术、隐蔽技术、入侵检测、NT 安全、UNIX 安全、TCP/IP 和网络安全、Internet 安全、路由器安全、安全评估、渗透试验、防火墙、安全的 Web 事务处理、电子商务、SSL、IPSEC 以及信息战等。他是 SANS 的高级讲师，开设了多门课程，同时针对不同的课题做过系列演讲。Eric Cole 还在纽约技术学院教学，同时担任乔治镇大学的助教。他还创办了 Teligent 公司，并兼任该公司安全部门的领导。

致 谢

感谢在本书写作过程中提供帮助与支持的 New Riders 出版公司，特别是 Jeff Riley、Katherine Pendergast 和 Sean Monkhouse，他们是非常出色的发行人。

同时要感谢 SANS。与 Alan Paller 和 Stephen Northcutt 一起工作令人愉快，他们给我提供了很大的帮助。在本书撰写的整个过程中，他们提出了很好的建议与支持。还要感谢 SANS GIAC 的学生们，他们提供了在实践中获得的极有价值的信息。

现在要感谢帮助我的所有朋友和家人。Tony Ventimiglia 是一个同甘共苦的朋友，他给予了编辑方面的很大支持。Mathew Newfield 提供了各方面的帮助。Jim Conley 提供了编辑建议与指导。Gary Jackson 是一位非常棒的朋友，给予了我不断的指导。Marc Maloof 也同样给予了指导和帮助。

尤其是要感谢上帝赐予我的生命与和睦完美的家庭：Kerry Magee，大力支持我的妻子；Jackson，我可爱的儿子，给我每天的生活带来快乐；Ron 和 Caroline Cole、Mike 和 Ronnie Magee，给予我无数爱和支持的父母。还要感谢我的姐姐、姐夫、侄女、侄子：Cathy、Tim、Allison、Timmy 和 Brianna。

最后，为了所有我忘记提到名字的人，再一次感谢我的所有朋友、家人、同事以及在本书编写过程中给予我一切支持的所有人。

前言

网络安全是一个流行的话题，有关这方面的书籍几乎不用介绍。大约十年以前，大多数人并不知道什么是 Internet 或电子邮件，再早一些时候，大多数家庭和办公室也没有计算机，一些人甚至在怀疑计算机与网络的用处。但是世界变化得太快了，当在写这篇简介的时候，感觉到网络世界的繁荣景象，就像是在迪斯尼世界中一样。十年前我们认为是科幻小说里才会有的东西现在不仅已变成了现实，而且已深入到了我们的生活之中。现在真正是计算机网络的时代了！

从功能的角度来讲，孤立的计算机是非常安全的。如果在家中放一台没有接入网络的计算机，那就不需要什么安全措施。可是现实中人们通过 Internet 把他们的计算机连接了起来，我们在互相信任的基础上建立了这个网。这里仅存在一个问题：人们之间并非完全互相信任。然而，在很多情况下，我们给所有用户完全的信息存取权。基于这一点，我们来追溯一下事情的起因。这其实是由于过去人们只关注于技术与功能，而并不担心安全问题，但事实上当前的安全问题已非常严重。

我还记得十年前在安全部门工作时的情景：人们都不愿搭理我，到处都给我白眼看。为什么会这样？因为人们还没有认识到安全工作的重要性，而是认为安全工作纯粹是在为根本不存在的威胁而浪费金钱。在那时，其他的技术和安全技术比起来，可以很容易地比较它们的效益。比如，扩展网络或安装新服务器可以加快访问速度、增加计算效率、提供更大的存储空间等。而安全技术却没有这些直接效益，它有的只是间接效益：数据和信息得到安全保障。一般情况下，在没有受到损失之前，人们是不会真正认识到安全的重要性的。只有当攻击者侵入了系统并盗走一千万美元的时候，人们才开始重视安全问题。想想看，如果他们一开始就在安全上投入的话，能省多少钱呢！

在越来越多的单位遭受损失的情况下，越来越多的单位认识到提前对安全投资的重要性。汽车保险就是这样，人们在买车的同时也买下了保险，只是为了防备万一车祸发生所带来的损失。我认识一些三十多年都没有发生过车祸的人，但是他们仍然购买保险。这是因为购买汽车保险可以降低出车祸时的损失，这已在人们心中形成了一种共识。同样的道理也适用于网络安全。不管您的公司是从事什么行当的，规模有多大，投资网络安全都是明智之举。

没有系统是安全的。任何接入 Internet 的系统都受到探测并有可能遭到侵入。我们可以做一些简单的实验来验证一下。可以用家中的直接接入或拨号接入 Internet 的计算机来做这个实验。购买或者从网上下载防火墙，这类软件工具有好几种，但 Zone Alarm 是一个免费版本，它可以从 www.zonelabs.com 下载。将这个防火墙安装在计算机系统上，接入 Internet，48 小时后会有吃惊的发现。通常在不到两天的时间内，系统会被探测到数次并可能被侵入。举个例子，当从 Internet 服务提供商（ISP）那里索要到一个 IP 后，接入网络，在不到 30 分钟的时间里就受到了 5 次探测。如果是家用计算机，没有域名，不受到太多关注，但还是被探测并受到攻击。对于公司而言，一定会受到更多攻击的。如果没有良好的防范措施，就会被非法攻入并遭受损失。

有一些公司曾对我说过，他们的系统从来都没有受到过攻击。这些话肯定是不对的。事实上，应该是他们从来都没有检测到攻击。眼不见心不烦并不能解决问题，清楚并能针对自己系

统进行恰当的防范措施是非常关键的。本书就是要介绍黑客们在干什么以及他们所用的工具和技术。通过本书，可以从准确的角度对系统做出更好的防范。

应该明确，成功的防范必须建立在对攻击充分了解的基础之上，这正是本书的目的：介绍黑客攻击与破坏的技术、方法以及工具，让人们利用这些知识建立更安全的网络。安全防范不是一句空话，必须了解威胁是什么。在这个领域只有知识是最有力量的。

本书就是介绍黑客攻击的内幕以及如何防范黑客的关键。保护网络安全是一次没有终点的旅行，但就我的经验来看，它也是一次非常令人愉快而且回报相当大的旅行。快让我们开始在网络安全世界中的美妙旅途吧！

目 录

第 1 章	简介	1
1.1	进行攻击的黄金时期	1
1.2	问题的严重程度	2
1.2.1	总的趋势	3
1.2.2	为什么问题变得如此严重	7
1.3	公司正在做什么	9
1.3.1	零忍耐	9
1.3.2	侥幸的安全意识	10
1.3.3	试着修复已经建立起来的系统	10
1.3.4	过于重视或者极不重视	11
1.4	公司现在应该做些什么	11
1.4.1	预防和检测投资	11
1.4.2	给予监测技术更多的关注	12
1.4.3	注意对员工的培训	14
1.5	深度防御	14
1.6	本书的目的	14
1.7	合法的使用	15
1.8	本书的内容	15
1.9	小结	16
第 2 章	攻击目的和方法	17
2.1	什么是攻击行为	17
2.2	攻击的步骤	18
2.2.1	被动的侦察	19
2.2.2	主动的侦察	20
2.2.3	入侵系统	21
2.2.4	上传程序	24
2.2.5	下载数据	24
2.2.6	保持访问	24
2.2.7	隐藏踪迹	25
2.3	攻击的种类	26
2.4	入侵行为的种类	27
2.4.1	在 Internet 上	27

2.4.2	在局域网上	29
2.4.3	本地	33
2.4.4	离线	35
2.5	攻击者进入的途径	37
2.5.1	端口	37
2.5.2	服务	39
2.5.3	第三方软件	40
2.5.4	操作系统	41
2.5.5	口令	42
2.5.6	社会工程	42
2.5.7	特洛伊木马	43
2.5.8	推论引导	43
2.5.9	秘密通道	43
2.6	攻击者想要达到的目标	44
2.6.1	机密性	44
2.6.2	完整性	45
2.6.3	可用性	45
2.7	小结	45
第3章	信息搜集	46
3.1	信息搜集的步骤	46
3.1.1	找到初始信息	47
3.1.2	找到网络的地址范围	52
3.1.3	找到活动的机器	57
3.1.4	找到开放端口和入口点	59
3.1.5	弄清操作系统	62
3.1.6	弄清每个端口运行的服务	64
3.1.7	画出网络图	65
3.2	信息搜集总结	67
3.3	实际应用	67
3.3.1	Whois	68
3.3.2	Nslookup	69
3.3.3	ARIN Web Search	70
3.3.4	Traceroute	71
3.3.5	Ping	73
3.3.6	绘制网络图	75
3.3.7	端口扫描和指纹鉴别	75
3.3.8	攻击系统	77
3.4	小结	77

第4章 欺骗	78
4.1 欺骗的理由	78
4.2 欺骗的类型	78
4.2.1 IP 欺骗	79
4.2.2 电子邮件欺骗	87
4.2.3 Web 欺骗	92
4.2.4 非技术欺骗	104
4.3 小结	108
第5章 会话劫持	109
5.1 欺骗和劫持	109
5.2 会话劫持的种类	110
5.3 TCP/IP 概念	111
5.3.1 TCP	111
5.4 会话劫持的细节	113
5.4.1 发现目标	114
5.4.2 执行顺序预测	114
5.4.3 寻找一个动态的会话	116
5.4.4 猜测序列号	116
5.4.5 使对方下线	116
5.4.6 接管会话	117
5.5 ACK 风暴	117
5.6 会话劫持攻击的程序	117
5.6.1 Juggernaut	118
5.6.2 Hunt	127
5.6.3 TTY Watcher	133
5.6.4 IP Watcher	134
5.7 劫持攻击的危害	134
5.7.1 大多数计算机都易受攻击	135
5.7.2 没有较成功的防范措施	135
5.7.3 劫持攻击非常简单	135
5.7.4 劫持攻击非常危险	135
5.7.5 大多数反劫持攻击方法都不起作用	136
5.8 会话劫持攻击的防范措施	136
5.8.1 进行加密	136
5.8.2 使用安全协议	137
5.8.3 限制引入连接	137
5.8.4 减少远端连入	137
5.8.5 拥有完善的认证措施	137

5.9 小结	137
第6章 拒绝服务攻击	139
6.1 拒绝服务攻击的概念	139
6.1.1 拒绝服务攻击的类型	139
6.2 分布式拒绝服务攻击的概念	140
6.3 难以防范的原因	141
6.4 拒绝服务攻击类型	142
6.4.1 Ping of Death	142
6.4.2 SSPPing	145
6.4.3 Land 攻击	147
6.4.4 Smurf	149
6.4.5 SYN Flood	152
6.4.6 CPU Hog	155
6.4.7 Win Nuke	157
6.4.8 RPC Locator	160
6.4.9 Jolt2	163
6.4.10 Bubonic	168
6.4.11 Microsoft 不完整 TCP/IP 数据包的脆弱性	172
6.4.12 HP Openview 节点管理器 SNMP DOS 的脆弱性	172
6.4.13 NetScreen 防火墙 DOS 的脆弱性	173
6.4.14 Checkpoint 防火墙 DOS 的脆弱性	174
6.5 DOS 攻击工具	175
6.5.1 Targa	175
6.6 DDOS 攻击工具	176
6.6.1 TFN2K	177
6.6.2 Trinoo	179
6.6.3 Stacheldraht	181
6.7 防范拒绝服务攻击	181
6.7.1 有效完善的设计	182
6.7.2 带宽限制	182
6.7.3 及时给系统安装补丁	182
6.7.4 运行尽可能少的服务	182
6.7.5 只允许必要的通信	183
6.7.6 封锁敌意 IP 地址	183
6.8 防范分布式拒绝服务攻击	183
6.8.1 保持网络安全	184
6.8.2 安装入侵检测系统	184
6.8.3 使用扫描工具	185

6.8.4 运行 Zombie 工具	186
6.9 小结	186
第 7 章 缓冲区溢出攻击	187
7.1 缓冲区溢出攻击的概念	187
7.2 缓冲区溢出的细节	188
7.3 缓冲区溢出攻击类型	190
7.4 存在大量易受攻击程序的原因	190
7.5 缓冲区溢出样例	191
7.6 如何保护例子程序	191
7.7 十种缓冲区溢出攻击	192
7.7.1 NetMeeting 缓冲区溢出	192
7.7.2 Outlook 缓冲区溢出	196
7.7.3 Linuxconf 缓冲区溢出	200
7.7.4 ToolTalk 缓冲区溢出	204
7.7.5 IMAPD 缓冲区溢出	206
7.7.6 AOL Instant Messenger 缓冲区溢出	209
7.7.7 AOL Instant Messenger BuddyIcon 缓冲区溢出	210
7.7.8 Microsoft Windows 2000 ActiveX 控件缓冲区溢出	211
7.7.9 IIS 4.0/5.0 Phone Book 服务器缓冲区溢出	212
7.7.10 SQL Server 2000 扩展存储程序缓冲区溢出	214
7.8 防范缓冲区溢出攻击	217
7.8.1 关闭端口或服务	217
7.8.2 安装厂商的补丁	217
7.8.3 在防火墙上过滤特殊通信	218
7.8.4 检查关键程序	218
7.8.5 以需要的最少权限运行软件	218
7.9 小结	218
第 8 章 口令安全	219
8.1 典型攻击	219
8.2 口令现状	220
8.3 口令的历史	221
8.4 口令的未来	222
8.5 口令管理	224
8.5.1 口令的必要性	224
8.5.2 口令策略的必要性	225
8.5.3 强口令的概念	225
8.5.4 选取强口令的方法	226

8.5.5 保护口令的方法	226
8.6 口令攻击	229
8.6.1 口令破解的概念	229
8.6.2 口令破解的重要性	231
8.6.3 口令攻击的类型	233
8.6.4 其他攻击类型	235
8.7 小结	236
第9章 Microsoft NT 口令破解	238
9.1 NT 中口令的存放	238
9.2 破解 NT 口令的方法	239
9.3 所有的口令都能破解	239
9.3.1 LAN 管理器哈希	239
9.3.2 没有添加成分	240
9.4 NT 口令破解程序	241
9.4.1 L0phcrack	241
9.4.2 NTSweep	251
9.4.3 NTCrack	253
9.4.4 PWDump2	254
9.5 比较	254
9.6 提取口令哈希	255
9.7 预防 NT 口令破解	255
9.7.1 禁用 LAN 管理器认证	256
9.7.2 贯彻强口令	258
9.7.3 拥有强口令策略	259
9.7.4 使用 SYSKEY	260
9.7.5 使用一次性口令	261
9.7.6 使用生物技术	261
9.7.7 审计关键文件访问	262
9.7.8 搜索破解工具	262
9.7.9 保存活动账号清单	262
9.7.10 限制拥有域管理员权限的用户	262
9.8 小结	263
第10章 UNIX 口令破解	264
10.1 UNIX 中口令的存放	264
10.1.1 Shadow 文件	266
10.2 UNIX 加密口令的方法	267
10.3 UNIX 口令破解程序	269
10.3.1 Crack	269
10.3.2 John the Ripper	277

10.3.3	XIT	281
10.3.4	Slurpie	283
10.4	比较	285
10.5	防止 UNIX 口令破解	287
10.5.1	采用强口令策略	287
10.5.2	使用 Shadow 文件	288
10.5.3	使用一次性口令	288
10.5.4	使用生物技术	289
10.5.5	使用 Passwd+ 以实现强口令	289
10.5.6	审计关键文件访问	290
10.5.7	扫描破解工具	290
10.5.8	保存活动账号清单	290
10.5.9	限制拥有根权限的用户	290
10.6	小结	290
第 11 章	Microsoft NT 基础	291
11.1	NT 安全概述	291
11.2	源代码可用性	292
11.3	NT 基础	293
11.3.1	NT 的组织方式	294
11.3.2	物理安全	295
11.3.3	注册表	295
11.3.4	运行的服务	299
11.3.5	账号管理	300
11.3.6	网络设置	300
11.3.7	审计	303
11.3.8	NetBIOS	306
11.3.9	服务包	307
11.3.10	资源工具箱	307
11.3.11	系统增强指导	312
11.4	小结	312
第 12 章	NT 攻击	313
12.1	NT 攻击工具	313
12.1.1	GetAdmin	314
12.1.2	SecHole	317
12.1.3	Red Button	320
12.1.4	Microsoft IIS 中的 RDS 安全漏洞	322
12.1.5	Microsoft Shares	327
12.1.6	Legion	332
12.1.7	相对 Shell 路径弱点	345

12.1.8	使用 ODBC 数据源工具拦截 NT DSN	348
12.1.9	Winfreeze	354
12.1.10	Microsoft Windows 媒体播放器 JavaScript URL 弱点	355
12.1.11	Microsoft Internet Explorer Mstask.exe CPU 占用弱点	356
12.1.12	Microsoft MSHTML.DLL 崩溃弱点	357
12.1.13	2001 IIS 5.0 允许文件浏览	358
12.1.14	媒体播放器 7 和 IE Java 弱点	358
12.1.15	IE 5.x/Outlook 允许执行任何程序	360
12.1.16	IIS 5.0 允许执行任何网站服务器命令	361
12.1.17	Microsoft WINS 域控制器欺骗弱点	362
12.2	小结	363
第 13 章	UNIX 基础	364
13.1	Linux	364
13.2	UNIX 的弱点	364
13.2.1	示例脚本	365
13.2.2	无关软件	366
13.2.3	开放端口	366
13.2.4	未打补丁的系统	366
13.3	UNIX 基础	367
13.3.1	重要命令	367
13.3.2	文件许可	368
13.3.3	Inetd	369
13.3.4	Netstat	371
13.3.5	Tripwire	371
13.3.6	TCP Wrappers	372
13.3.7	Lsof	372
13.3.8	Suid	373
13.4	小结	373
第 14 章	UNIX 攻击	374
14.1	UNIX 攻击	374
14.1.1	Aglimpse	374
14.1.2	Campas	378
14.1.3	NetPR	380
14.1.4	DTprintinfo	389
14.1.5	Sadmind 攻击	397
14.1.6	XWindows	402
14.1.7	Solaris Catman Race Condition 漏洞	412
14.1.8	Multiple Linux Vendor RPC.STATD 攻击	412
14.2	小结	414

第 15 章	保留访问权限	415
15.1	后门和特洛伊木马程序	416
15.1.1	QAZ	417
15.1.2	后门监听代理	417
15.2	Rootkit	418
15.2.1	文件级 Rootkit	419
15.2.2	内核级 Rootkit	420
15.2.3	NT Rootkit	420
15.2.4	UNIX Rootkit	421
15.3	NT 后门	423
15.3.1	Brown Orifice 攻击	423
15.3.2	Donald Dick 1.55	428
15.3.3	SubSeven	435
15.3.4	Back Orifice	443
15.3.5	包装程序	445
15.4	小结	445
第 16 章	隐藏踪迹	447
16.1	隐藏攻击踪迹的方法	447
16.1.1	日志文件	448
16.1.2	文件信息	460
16.1.3	附加文件	462
16.1.4	隐藏网络上的踪迹	463
16.2	小结	465
第 17 章	其他类型的攻击	466
17.1	Bind 8.2 NXT 攻击	466
17.1.1	攻击细节	466
17.1.2	协议描述	466
17.1.3	变种描述	467
17.1.4	攻击原理	467
17.1.5	使用方法	468
17.1.6	攻击特征	469
17.1.7	防范措施	471
17.1.8	源代码 / 伪代码	471
17.2	Cookie 攻击	471
17.2.1	攻击细节	472
17.2.2	CGI 协议描述	472
17.2.3	CGI 协议工作原理	472
17.2.4	CGI 协议弱点	472

17.2.5	Cookie 协议描述	472
17.2.6	Cookie 协议工作原理	473
17.2.7	Cookie 协议弱点	473
17.2.8	攻击原理	473
17.2.9	成功原因	473
17.2.10	攻击图解	474
17.2.11	攻击特征	474
17.2.12	怎样防止攻击	475
17.2.13	防范措施	475
17.2.14	源代码 / 伪代码	475
17.3	SNMP 团体字符串	479
17.3.1	攻击细节	479
17.3.2	协议描述	479
17.3.3	历史回溯	479
17.3.4	SNMP 结构	480
17.3.5	SNMP 消息	480
17.3.6	SNMP 验证	482
17.3.7	攻击原理	482
17.3.8	使用方法	482
17.3.9	攻击特征	487
17.3.10	防范措施	487
17.3.11	攻击图解	488
17.3.12	源代码 / 伪代码	488
17.3.13	脆弱的设备	489
17.3.14	附加信息	489
17.4	Sniffing 与 Dsniff	490
17.4.1	攻击细节	490
17.4.2	协议描述	490
17.4.3	攻击变种	490
17.4.4	回顾	491
17.4.5	详细描述	491
17.4.6	使用 Dsniff 及其应用	492
17.4.7	进行攻击	494
17.4.8	攻击特征	495
17.4.9	防范措施	495
17.4.10	源代码 / 伪代码	496
17.4.11	附加信息	496
17.5	PGP ADK 攻击	496
17.5.1	攻击细节	496
17.5.2	协议描述	497
17.5.3	攻击原理	498