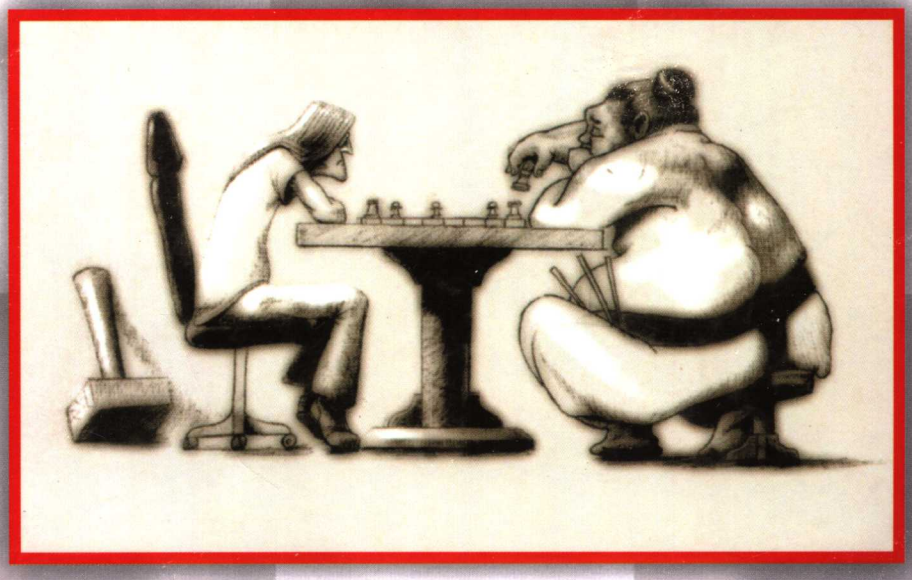
HZ BOOKS

AUERBACH

黑客防范手册

The Hacker's Handbook

The Strategy behind Breaking into and Defending Networks



（美） Susan Young Dave Aitel 著

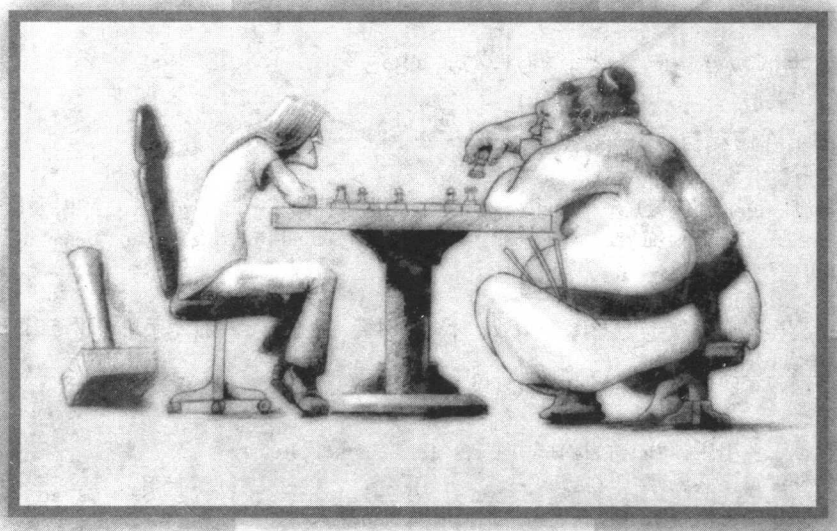
吴世忠 郭涛 李斌 宋晓龙 等译

机械工业出版社
China Machine Press

黑客防范手册

The Hacker's Handbook

The Strategy behind Breaking into and Defending Networks



（美） Susan Young Dave Aitel 著

吴世忠 郭涛 李斌 宋晓龙 等译

机械工业出版社
China Machine Press

虽然市面上已有不少介绍系统和网络安全的书籍，但本书从不同的视角来阐述安全问题，使本书在安全图书领域独具特色。本书使用分析的观点来看待黑客行为和安全，将攻击和防御类比为国际象棋游戏中的对弈，攻与守之间存在着对立统一性。本书适合有一定安全经验的系统管理员、网络管理员和安全管理员阅读，通过揭示黑客行为的技术内幕，让管理员们做到知己知彼，准确地将黑客行为"映射"到未来的防御系统中。

Susan Young and Dave Aitel: The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks(ISBN 0-8493-0888-7).

Original English language edition published by Auerbach Publications, an imprint of CRC Press LLC, 345 Park Avenue South, New York, NY USA 10010.

本书版权登记号：图字：01-2005-4848

图书在版编目(CIP)数据

黑客防范手册/(美)杨(Young, S.)等著；吴世忠等译. -北京：机械工业出版社，2006.1
书名原文：The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks
ISBN 7-111-17508-5

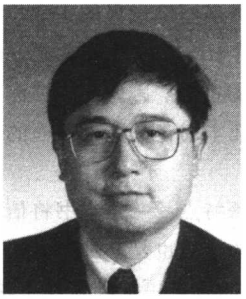
Ⅰ.黑…　Ⅱ.①杨…②吴…　Ⅲ.计算机网络-安全技术-技术手册　Ⅳ.TP393.08-62

中国版本图书馆 CIP 数据核字(2005)第 115346 号

机械工业出版社(北京市西城区百万庄大街 22 号　邮政编码　100037)
责任编辑：盛思源　刘立卿
北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行
2006 年 1 月第 1 版第 1 次印刷
787mm × 1020mm 1/16 · 31.25 印张
印数：0 001-4000 册
定价：59.00 元

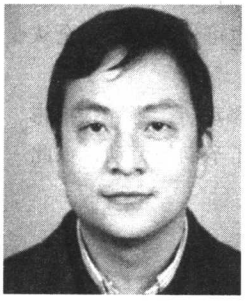
凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：(010)68326294

译者简介

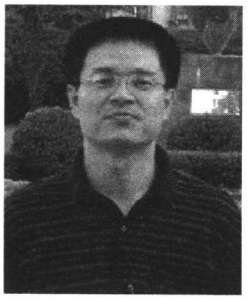


吴世忠：博士、研究员，中国信息安全产品测评认证中心主任。现为全国信息安全标准化技术委员会副主任，中国信息产业商会信息安全产业分会理事长，《信息安全与通信保密》杂志主编。已公开出版文章百余篇，著有《信息系统的互连与互通》、《C3I 系统的安全与保密》、《关贸总协定：中国准备好了吗?》、《首都信息化标准指南·信息安全与保密标准化体系》等专著五部和《应用密码学》、《密码编码和密码分析原理和方法》、《网络世界信息安全的真相》、《密码学的理论和实践》、《中文 Windows 2000 的安全性》、《密码学导引》、《ICSA 密码学指南》等译著七部，同时还主持起草了防火墙、应用网关安全技术要求以及信息技术安全性评估准则等七项国家标准，并主笔撰写了与信息安全战略与技术发展有关的多篇专题报告。

郭涛：1974 年 9 月出生，湖北宜昌人。华中科技大学计算机系统结构专业博士毕业。中国信息安全产品测评认证中心副总工程师，参加多项国家重大科研项目。主要研究方向为信息安全、密码理论、安全测试技术、安全电子支付技术等；曾在《通信学报》、《高技术通讯》等刊物发表论文十几篇，译著有《密码学导引》和《ICSA 密码学指南》。



李斌：1971 年 11 月出生。北京大学信息科学技术学院博士生。中国信息安全产品测评认证中心副总工程师，参加多项国家重大科研项目，包括国家 863 项目、国信办项目、国家发改委项目等。曾经在 ACM 等学术期刊上发表论文多篇。



宋晓龙：1970 年 9 月出生。毕业于中国人民解放军信息工程大学，获理学硕士学位；主要研究兴趣为密码算法与理论、密码分析和密码产品测试技术；曾在《通信学报》、《信息安全与通信保密》等刊物发表论文多篇，译著有《密码编码与密码分析原理和方法》、《密码学导引》和《ICSA 密码学指南》。

译者序

作为人类智慧的结晶，计算机和网络在本质上具有程序性和严谨性。但是，人类是网络世界的主宰，人类思维不会受到这些程序的束缚，具有无限的创造性，这就是信息安全日益成为当今社会的重大问题之一的根本原因所在。所谓道高一尺，魔高一丈，攻与防永远是信息安全领域中恒久不变的主题。因此，能够深入了解黑客如何展开攻击行动，对于更好地实施信息安全保障具有很好的借鉴意义，而本书正是这个方面的一本不可多得的教材。

作为译者，我们得以先睹为快。反复推敲之余，我们感到本书具有以下几个显著特点：一是本书将信息安全的攻与防比喻成国际象棋的博弈，并且把这个思想贯穿于本书始终，国际象棋的本质也是一种思维的艺术，信息安全与国际象棋之间存在很多相似之处，比喻不但非常贴切，而且使本书的行文更加幽默和生动；二是本书从攻和防两个视角来看待信息安全，知己知彼，百战不殆，信息安全工作人员只有更好地了解黑客攻击的动机和行为，才能更好地进行防范；三是本书通过生动翔实的案例来对沉闷乏味的黑客行为进行描述，能够吸引读者的注意力；四是本书在各章中都给出了大量的代码和操作结果，具有很强的实用性和可操作性。

本书分为三个部分：第一部分给出了实施黑客攻击所必需具备的基础知识，包括程序设计、协议以及黑客攻击工具等；第二部分从网络协议、服务、数据库入侵和恶意代码等方面，阐述了黑客是如何对系统和网络进行渗透的；最后一部分详细介绍了黑客在成功破解系统或网络后，通常会如何去扩大“战果”。

值得注意的是，在本书的第18章给出了一个黑客入侵的完整案例，但作者的初衷并不是想要教人们如何去进行攻击和破坏，而是希望人们通过认识黑客攻击的过程来更好地进行防御。

总而言之，本书是一本深入浅出的网络安全技术宝典，具有很强的实用性和可操作性，能够为广大信息安全爱好者起到很好的指导作用。本书不仅适合于信息安全领域的广大科研人员，也可作为信息安全从业人员的参考手册。古人云，开卷有益，我们希望本书对所有读者都有所裨益。

本书由吴世忠、郭涛、李斌、宋晓龙主持翻译，其他参与翻译人员还有吴迪、张动、李淼、张彬彬、易郡、徐惠林、陈庆锋等，田惠文、肖珏、向继志、童俊等同志在文字校对上也付出了辛勤的劳动，在此一并表示感谢。

由于水平所限，不妥或错误之处在所难免，敬请广大读者批评指正。

译　者

2005年10月

致　谢

正如人们所说的，每一本书都有一个故事。本书的历史非常悠久，而且充满很多变数。在本书的撰写过程中，很多人都花费了大量的时间、精力和智慧，或者给予了精神上的支持。

作者对下面这些为本书做出贡献和给予支持的人员致以诚挚的感谢：

- Rich O'Hanley 和 Auerbach 出版社生产部的全体员工，感谢他们对本书的不知疲倦的支持，不管本书的历史有多长(甚至有些令人讨厌)。
- 我们所有的作者——Felix Lindner、Jim Barrett、Scott Brown 和 John Zuena，他们花费了大量的时间和精力撰写了其中非常精彩的几章，涉及黑客社区、恶意软件、目录服务以及网络硬件，这些章节中都包含了非常独特的见解和很有意思的内容。
- 我们的技术审阅人，包括 Jim Tiller、Anton Chuvakin、Sean Cemm、Ben Rothke 和 Ted Shagory，感谢他们卓越的见识，他们花费了大量的时间和精力来帮助完成本书。我们相信此审阅过程将一直持续到本书正式出版为止，同时我们也感谢本书的读者和审阅人对本书质量的关注。

此外，Dave Aitel 还要感谢 Justine Bone 的支持和鼓励，Susan Young 也要感谢下列人员：Darklord(Thomas McGinn)，尽管几个月以来他牺牲了大量周末休息时间，而且极度疲劳，但他还是一直信守承诺，对本书给予了大力支持；感谢 Trevor Young 为本书付出了自己的才能、热情、时间和关注，他绘制了本书所有的图表；感谢 Gemma Young 和她的父母——Sylvia 和 Neil，感谢他们在长达两年的长途电话交流中所给予的关心、支持和建议；此外，还要感谢国际网络服务公司(特别是 Steven Marandola、Bob Breingan 和 Shaun Meaney 等人)在为本书的最终完稿上所提供的时间和支持。

目 录

译者序
致谢

第 1 章 导论：国际象棋游戏 …… 1

第一部分 基础材料

第 2 章 案例研究 …… 9
2.1 Dalmedica …… 9
2.2 困境 …… 10
2.3 调查 …… 14
第 3 章 了解对手 …… 19
3.1 术语 …… 19
3.1.1 脚本小子 …… 19
3.1.2 骇客 …… 20
3.1.3 白帽子黑客 …… 20
3.1.4 黑帽子黑客 …… 21
3.1.5 黑客激进主义 …… 21
3.1.6 专业攻击者 …… 21
3.2 历史 …… 22
3.2.1 计算机产业和大学 …… 22
3.2.2 系统管理 …… 23
3.2.3 家用计算机 …… 23
3.2.4 家用计算机：商业软件 …… 23
3.2.5 家用计算机：BBS …… 24
3.2.6 电话系统 …… 26
3.3 道德规范和完全公开 …… 27
3.4 内部对手 …… 29
3.4.1 内部攻击者 …… 29
3.4.2 企业策略 …… 31
小结 …… 31
第 4 章 攻击剖析 …… 32
4.1 概览 …… 32
4.2 探测 …… 32
4.3 社会工程和场所探测 …… 33
4.4 因特网探测 …… 34
4.4.1 因特网搜索引擎和 Usenet 工具 …… 35
4.4.2 财务搜索工具、目录、黄页和其他资源 …… 35
4.5 IP 和网络探测 …… 36
4.5.1 域名注册商和 whois 搜索 …… 36
4.5.2 网络域名注册商搜索(ARIN) … 38
4.6 DNS 探测 …… 38
4.7 映射目标 …… 40
4.8 网络映射(ICMP) …… 42
4.8.1 ICMP 查询 …… 42
4.8.2 TCP ping：ICMP 的替代 …… 43
4.8.3 traceroute …… 44
4.8.4 其他网络映射工具 …… 45
4.9 端口扫描 …… 45
4.9.1 TCP 和 UDP 扫描 …… 46
4.9.2 标志获取 …… 46
4.9.3 包分片选项 …… 46
4.9.4 欺骗扫描能力 …… 47
4.9.5 标识扫描 …… 47
4.9.6 FTP 反弹扫描 …… 47
4.9.7 源端口扫描 …… 47
4.9.8 栈指纹识别技术 …… 47
4.10 漏洞扫描(网络操作系统及应用问询) …… 49
4.11 漏洞的研究和探测 …… 51
4.12 系统/网络穿透 …… 52
4.12.1 账号(口令)破解 …… 52
4.12.2 应用程序攻击 …… 52
4.12.3 缓存利用 …… 52
4.12.4 文件系统攻击 …… 52
4.12.5 恶意和自我复制代码 …… 53
4.12.6 编程策略 …… 53
4.12.7 进程操纵 …… 53
4.12.8 shell 攻击 …… 53
4.12.9 会话劫持 …… 53
4.12.10 哄骗 …… 54
4.12.11 基于状态的攻击 …… 54
4.12.12 流量捕获(嗅探) …… 54

4.12.13 可信关系滥用 …… 55
4.13 拒绝服务攻击 …… 55
4.14 巩固 …… 56
4.15 安全 …… 56
参考文献 …… 58
第5章 防御武器库 …… 60
5.1 防御武器库 …… 62
5.1.1 访问控制 …… 62
5.1.2 系统访问控制 …… 68
5.2 鉴别 …… 69
5.2.1 IP 鉴别 …… 70
5.2.2 口令鉴别 …… 71
5.2.3 窃听攻击 …… 72
5.2.4 口令猜测攻击 …… 73
5.2.5 基于令牌的鉴别 …… 73
5.2.6 会话鉴别 …… 73
5.2.7 客户端会话/ID 窃取 …… 77
5.2.8 密码(基于密钥的)鉴别 …… 77
5.2.9 密钥传输和密钥管理漏洞 …… 80
5.2.10 密钥绑定和假冒漏洞 …… 83
5.2.11 针对弱密钥的字典攻击和蛮力攻击 …… 83
5.2.12 集中式鉴别服务器 …… 83
5.2.13 人体特征鉴别(生物测定学) … 87
5.3 资源控制 …… 88
5.4 抗抵赖性 …… 89
5.5 私密性 …… 91
5.5.1 虚拟专用网 …… 92
5.5.2 会话和协议加密 …… 95
5.5.3 文件系统加密 …… 99
5.6 入侵检测 …… 100
5.6.1 NIDS 和 HIDS …… 100
5.6.2 基于异常(基于行为)的 IDS …… 101
5.6.3 基于特征(基于知识)的 IDS …… 102
5.6.4 针对 IDS 的攻击 …… 102
5.6.5 文件系统完整性检查器 …… 104
5.6.6 安全信息管理 …… 105
5.7 数据完整性 …… 105
参考文献 …… 106
第6章 程序设计 …… 108
6.1 语言 …… 108
6.2 速度和安全的折衷 …… 108
6.2.1 本地的编译代码：C/C++/汇编语言 …… 109
6.2.2 字节码/JIT 编译代码(“受控”代码)：C#/Java …… 109
6.2.3 解释语言(通常在运行时编译成字节码)：Perl、Python(脚本语言)，PHP、VB、.ASP、Lisp、JSP(Web 语言) …… 110
6.3 具体语言的缺陷和防止受到这些缺陷影响的策略方法 …… 110
6.4 缓冲区溢出和其他内存分配错误的基础知识 …… 111
6.5 历史 …… 111
6.5.1 基本的栈溢出 …… 111
6.5.2 栈溢出后黑客的选择 …… 112
6.5.3 什么是栈 canary …… 113
6.5.4 堆溢出 …… 113
6.5.5 格式字符串缺陷 …… 114
6.5.6 整数溢出 …… 115
6.5.7 UNIX 上的信号竞争 …… 115
6.5.8 什么是 shellcode …… 115
6.6 解释器缺陷 …… 116
6.7 文件名规范化 …… 116
6.8 逻辑错误问题 …… 117
6.9 特定平台的编程安全问题 …… 117
6.10 应用的类型 …… 118
6.11 跨站脚本漏洞 …… 119
6.12 Java J2EE …… 119
6.13 传统的 ASP …… 120
6.14 .Net …… 120
6.15 LAMP …… 120
6.16 创建一个 RPC 程序 …… 121
6.17 特殊情况 …… 121
6.17.1 UNIX 上的 setuid 应用 …… 121
6.17.2 DCOM 服务 …… 122
6.18 审查技术 …… 122
6.18.1 协助代码审查的工具 …… 123
6.18.2 反向工程可用的工具 …… 124
6.18.3 fuzzing 审查工具 …… 124

6.18.4 Web 安全性审查工具 …… 125
6.18.5 一般的安全工具 …… 126
6.19 加密和鉴别 …… 126
6.20 分级防御 …… 127
6.21 特定平台的防御 …… 127
6.21.1 非执行栈 …… 127
6.21.2 使用不同的平台 …… 127
6.21.3 文件系统用户访问控制 …… 128
6.21.4 进程日志 …… 128
6.22 内部的问题、后门和逻辑炸弹 …… 128
6.23 购买应用评估服务 …… 129
小结 …… 129
参考文献 …… 129
第 7 章 IP 和第 2 层协议 …… 130
7.1 第 2 层协议 …… 131
7.1.1 地址解析协议 …… 131
7.1.2 反向地址解析协议 …… 135
7.2 第 3 层协议 …… 136
参考文献 …… 154
第 8 章 协议 …… 156
8.1 第 3 层协议 …… 156
8.2 第 4 层协议 …… 167
8.2.1 传输控制协议 …… 167
8.2.2 用户数据报协议 …… 175
参考文献 …… 179

第二部分 系统和网络渗透

第 9 章 域名服务器 …… 181
9.1 DNS 协议 …… 181
9.1.1 DNS 协议和包结构(包数据攻击) …… 181
9.1.2 DNS 漏洞 …… 184
9.2 DNS 的利用和 DNS 攻击 …… 185
9.2.1 基于协议的攻击 …… 185
9.2.2 基于应用的攻击 …… 190
9.2.3 缓存中毒攻击 …… 193
9.2.4 DNS 劫持 …… 194
9.3 DNS 的安全和控制 …… 195
9.3.1 漏洞利用对应的防御方法 …… 195
9.3.2 防御策略 …… 196
9.3.3 Microsoft Windows 2000 DNS 日志控制 …… 200
9.3.4 分层 DNS 拓扑结构(和 DNS 代理) …… 201
参考文献 …… 203
第 10 章 目录服务 …… 205
10.1 什么是目录服务 …… 205
10.2 目录的构成 …… 205
10.2.1 架构 …… 205
10.2.2 叶对象 …… 206
10.2.3 容器对象 …… 206
10.2.4 命名空间 …… 206
10.2.5 目录信息树 …… 206
10.2.6 目录信息库 …… 206
10.3 目录的特点 …… 206
10.3.1 目录安全 …… 206
10.3.2 单点登录 …… 207
10.4 目录系统的使用 …… 207
10.4.1 使用目录的网络 …… 207
10.4.2 连接准备 …… 207
10.4.3 全球目录 …… 207
10.4.4 公钥基础设施 …… 207
10.5 目录模型 …… 208
10.5.1 物理与逻辑 …… 208
10.5.2 扁平的与分等级的 …… 208
10.6 X.500 目录 …… 209
10.6.1 X.500 架构 …… 209
10.6.2 X.500 分区 …… 210
10.6.3 X.500 对象和命名 …… 210
10.6.4 关于别名 …… 211
10.6.5 X.500 后端处理 …… 211
10.6.6 X.500 目录访问 …… 213
10.6.7 X.500 安全 …… 213
10.6.8 访问控制 …… 214
10.6.9 权限 …… 214
10.6.10 小结 …… 215
10.7 轻量级目录访问协议 …… 215
10.7.1 LDAP 架构 …… 216
10.7.2 LDAP 分割 …… 216
10.7.3 LDAP 对象和命名 …… 217
10.7.4 LDAP 查询 …… 218
10.7.5 LDAP 数据相互交换格式 … 218
10.7.6 LDAP 安全 …… 218

10.7.7 小结 …… 219
10.8 活动目录 …… 219
10.8.1 Windows NT …… 220
10.8.2 Windows 2000 架构 …… 221
10.8.3 Windows 2000 分区 …… 221
10.8.4 Windows 2000 对象和命名 … 221
10.8.5 Windows 2000 的命名标准和解析 …… 222
10.8.6 活动目录的后端处理过程 … 223
10.8.7 Windows 2000 安全 …… 224
10.9 利用 LDAP …… 227
10.9.1 Sun ONE 目录服务器 5.1 …… 227
10.9.2 微软活动目录 …… 230
10.10 小结 …… 237
10.11 未来发展方向 …… 237
10.12 深入读物 …… 237
第 11 章 简单邮件传输协议 …… 238
11.1 SMTP 协议 …… 238
11.1.1 SMTP 协议和包结构(包数据攻击) …… 238
11.1.2 SMTP 漏洞 …… 242
11.1.3 SMTP 协议命令和协议扩展 …… 244
11.2 SMTP 漏洞利用和 SMTP 攻击 …… 246
11.2.1 SMTP 协议攻击 …… 247
11.2.2 ESMTP 和命令集的漏洞 …… 251
11.2.3 蠕虫和自动攻击工具 …… 258
11.2.4 基于应用的拒绝服务 …… 258
11.2.5 对邮件信任模型的攻击 …… 259
11.2.6 数据完整性的攻击 …… 261
11.2.7 投递状态通知的操纵 …… 261
11.3 SMTP 安全性和控制 …… 262
11.3.1 漏洞利用与防御 …… 262
11.3.2 防御策略 …… 264
参考文献 …… 268
第 12 章 超文本传输协议 …… 271
12.1 HTTP 协议 …… 271
12.1.1 HTTP 协议与数据包的构造(包数据攻击) …… 271
12.1.2 HTTP 漏洞 …… 273
12.1.3 HTTP 协议的方法(以及相关漏洞) …… 275
12.2 HTTP 漏洞利用和 HTTP 攻击 …… 276
12.2.1 HTTP 协议攻击 …… 276
12.2.2 缓存技术漏洞利用 …… 280
12.2.3 基于应用的攻击 …… 281
12.2.4 对 HTTP 信任模型的攻击 … 286
12.3 HTTP 安全和控制 …… 288
12.3.1 漏洞利用与防御的对应 …… 288
12.3.2 防御策略 …… 290
参考文献 …… 293
第 13 章 数据库入侵和安全 …… 296
13.1 简介 …… 296
13.2 弱点列举 …… 296
13.3 SQL 注入 …… 297
13.3.1 简介 …… 297
13.3.2 SQL 注入的阶段 …… 298
13.4 攻击微软 SQL Server …… 298
13.4.1 微软 SQL Server 中的溢出 …… 298
13.4.2 微软 SQL Server 鉴别后漏洞 …… 299
13.4.3 微软 SQL Server 的 SQL 注入漏洞 …… 299
13.4.4 攻击 Cold Fusion Web 应用程序的一个注释 …… 300
13.4.5 默认的账号和配置 …… 300
13.5 攻击 Oracle …… 301
13.5.1 Oracle Server 中的缓冲区溢出 …… 301
13.5.2 Oracle 中的 SQL 注入漏洞 … 302
13.5.3 默认的用户账号 …… 302
13.5.4 Oracle 评估的工具和服务 … 303
13.6 其他数据库 …… 303
13.7 向后连接 …… 304
13.8 证明和例子 …… 304
13.8.1 阶段 1：发现 …… 305
13.8.2 阶段 2：有漏洞的应用程序的逆向工程 …… 307
13.8.3 阶段 3：得到任意查询的结果 …… 309
13.9 小结 …… 312
第 14 章 恶意软件和病毒 …… 313
14.1 再论道德 …… 314

14.2 目标平台 …… 315
14.3 脚本恶意软件 …… 315
14.4 从 Anna Kournikova 中学习脚本病毒的基础知识 …… 315
14.5 二进制病毒 …… 317
14.5.1 二进制文件病毒 …… 317
14.5.2 二进制引导型病毒 …… 319
14.5.3 混合型病毒 …… 320
14.5.4 二进制蠕虫 …… 321
14.6 祸不单行 …… 323
14.7 广告软件感染 …… 323
14.8 小结 …… 324
第 15 章 网络硬件 …… 325
15.1 概述 …… 325
15.2 网络基础设施 …… 325
15.2.1 路由器 …… 325
15.2.2 交换机 …… 325
15.2.3 负载均衡设备 …… 326
15.2.4 远程访问设备 …… 326
15.2.5 无线技术 …… 326
15.3 网络基础设施漏洞利用与攻击 …… 326
15.3.1 设备策略攻击 …… 327
15.3.2 拒绝服务 …… 328
15.3.3 网络映射 …… 330
15.3.4 信息窃取 …… 331
15.3.5 哄骗 …… 332
15.3.6 口令或配置漏洞利用 …… 332
15.3.7 日志攻击 …… 333
15.3.8 网络端口和协议的漏洞利用与攻击 …… 334
15.3.9 设备管理攻击 …… 335
15.3.10 管理协议 …… 336
15.3.11 设备配置安全攻击 …… 337
15.3.12 特定路由器漏洞利用 …… 337
15.3.13 访问控制列表攻击 …… 339
15.3.14 特定交换机漏洞利用 …… 339
15.3.15 MAC 地址漏洞利用 …… 340
15.3.16 负载均衡设备——特定漏洞利用 …… 341
15.3.17 远程访问设备——特定漏洞利用 …… 341
15.3.18 家庭用户系统漏洞利用 … 341
15.3.19 无线技术——特定漏洞利用 …… 342
15.4 网络基础设施安全和控制 …… 344
15.4.1 防御策略 …… 344
15.4.2 路由协议安全选项 …… 344
15.4.3 管理安全选项 …… 344
15.4.4 操作系统加固选项 …… 344
15.4.5 配置审计和验证工具 …… 349
15.4.6 无线网络控制 …… 350
参考文献 …… 351

第三部分 攻击防范

第 16 章 了解攻击者的巩固策略 …… 353
16.1 概述 …… 353
16.2 巩固(操作系统和网络设施) …… 354
16.2.1 账户和权限管理工具 …… 354
16.2.2 文件系统和 I/O 资源 …… 360
16.2.3 文件系统(操作系统)攻击 … 364
16.2.4 基于应用程序的文件系统攻击 …… 372
16.2.5 服务和进程管理工具 …… 373
16.2.6 进程、服务和权限标识 …… 374
16.2.7 缓冲区溢出、格式化字符串和其他应用程序攻击 …… 383
16.2.8 进程调试和内存操纵 …… 383
16.2.9 设备和设备管理工具 …… 387
16.2.10 库和共享库 …… 388
16.2.11 shell 访问和命令行工具 … 392
16.2.12 注册表工具(NT/2000) …… 393
16.2.13 客户端软件 …… 394
16.2.14 监听器和网络服务 …… 396
16.2.15 网络信息服务探测 …… 400
16.2.16 SNMP 探测 …… 402
16.2.17 网络信任关系 …… 406
16.2.18 应用/可执行环境 …… 406
16.3 巩固(外来代码) …… 406
16.3.1 特洛伊木马 …… 407
16.3.2 后门(和特洛伊后门) …… 410
16.3.3 后门程序 …… 412
16.3.4 rootkit …… 415
16.3.5 内核级 rootkit …… 417

16.4 安全性 …… 419
16.5 漏洞利用与防御的对应 …… 419
参考文献 …… 425
第17章 取证调查中的问题 …… 429
17.1 日志、审计和IDS逃避 …… 430
17.1.1 日志和审计逃避 …… 430
17.1.2 IDS逃避 …… 447
17.2 取证逃避 …… 448
17.2.1 环境清理 …… 449
17.2.2 文件隐藏和文件系统操纵 … 450
17.2.3 隐蔽的网络活动 …… 458
17.3 调查、取证和安全控制 …… 462
参考文献 …… 466
第18章 结论 …… 468
18.1 结论：案例研究 …… 469
18.1.1 Dalmedica的观点 …… 483
18.1.2 接入点 …… 483
18.1.3 堡垒主机 …… 484
18.1.4 探测活动 …… 485
18.1.5 目标系统 …… 485
18.2 小结(最后的看法) …… 486
参考文献 …… 486

第 1 章　导论：国际象棋游戏

当你看到一步好棋时，请寻找一步更好的走法。

——Emanuel Lasker

国际象棋，就像任何创造性活动一样，只有通过那些具有创造性天赋和有能力组织创造性工作的人的努力，才能够存在。

——Mikhail Botvinnik

好的进攻和好的防守都源于好的“创造”。

——Bruce A. Moon

Botvinnik 曾试图解开国际象棋之谜，并将它与日常生活中的情形联系起来。他将国际象棋称为一个典型的不确定问题，与人们日常生活中必须解决的问题类似。

——Garry Kasparov

国际象棋游戏就像是一次对话——棋手和他的对手之间的对话。对手的每一步棋都可能极具威胁，也可能铸成大错，但是棋手如果不首先自问“对手每一步之后的计划如何”，那他就不可能很好地防守威胁和利用失误。

——Bruce A. Moon

从很多方面看，本章几乎都是书中最难的一部分；在写这一章时，我被迫去重新体验站在书店迅速翻阅技术书籍的感觉，以确定它对我当前所从事的技术领域的价值如何。我通常从前言开始阅读。对于这本十分特别的书，整理出一篇精确的、有代表性的序言是一项令人气馁的任务；因为本书涉及面非常广。

本书是一本讨论黑客行为的书，但它更是直接针对安全社区的。在作者开始创作本书时(2001 年 5 月)，已经出版了大量有关数字黑客行为和安全的书籍。为了使本书能够有一些“空间”，我们浏览了很多此类书籍，并发现尚有一些空白的领域，可以使用一种分析的观点来看待黑客行为和安全，并且向读者揭示黑客行为的技术内幕，至少要让系统管理员、网络管理员和安全管理员心中有数。

这里，我们列出了一些目标，这些目标真实地反映了本书的组织结构：

- 每一章都一分为二地看待黑客行为和安全，以便向读者揭示两者的含义。大多数章节都分为三个部分：(1)技术性(背景)；(2)黑客行为；(3)安全。采用这种方法的目的，就是通过在同一技术领域对黑客行为的利用和防御进行探索，来揭示管理员防御系统和网络的构筑方式。
- 每一章都包括特定的技术性和管理性部分(例如，特定的服务，如 SMTP、HTTP、DNS、目录服务，特定管理任务，系统加固和取证调查等)，以便将本书作为技术性的安全参考手册来使用。例如，如果你是一名 DNS 管理员，你应该能够迅速地找到 DNS 黑客行为和 DNS 安全的相关材料。
- 强调提供一种合理的技术和概念性框架，以便读者能够在整个书中应用。关键的基础章节如下：
  — 攻击剖析(第 4 章)
  — 安全技术(第 5 章)
  — 程序设计(第 6 章)
  — 传输控制协议/网际协议(TCP/IP)攻击(第 7、8 章)
  — 了解攻击者的巩固策略(第 16、17、18 章)
- 本书主张以双重角度看待理论和工具，目的是为读者提供一套全面的解决方案。每章中的材料作为一种参考框架，可以为读者提供合适的理论基础。文中对工具、应用代码和黑客“技术”都进行了分析，但是大量事实都表明，黑客行为仍然是一项“创造性”的活动。

- 每一章都提供详细的参考材料，以便为读者提供一条继续学习的“途径”，并且为通过因特网和其他资源获得可用信息、掌握更多的黑客行为和安全知识提供向导。提供这些信息也确保了本书中的技术性材料能够禁得起时间的考验。

本书面向具有一定安全经验的系统管理员、网络管理员和安全管理员，他们希望能够拓展黑客技术和应用方面的知识，并以此作为一种解决系统和网络安全问题的方案。这种定位使得本书具有相当多的读者，也反映了所采用材料的广泛性。为了保证本书能够实现该目标，每一章都给出了大量的图表，并根据内容分节进行介绍，以便管理员们能够将黑客行为准确地“映射”到未来的防御，而且，在每章的结尾处都给出了未来安全防御的处理方法。

在实用性方面，书中材料惟一的局限就在于作者将精力主要集中于微软的 Windows NT/2000 和 UNIX 平台，因为篇幅和深度所限要求必须设定范围。作者认为，限制平台的范围可能有利于增加这些黑客应用资料的技术深度。这样比选择某些其他平台要好，例如 Novell 或者 Mainframe/Midrange，所以最终我们决定将它们排除在外。

为了在本书中更好地安排黑客行为和安全材料，“国际象棋游戏”类比将会贯穿于整个材料之中(顺便说一句，所有作者都不是国际象棋高手)。作者认为，国际象棋的动力和策略与本书的主题有很多相似之处：

- 与很多其他策略游戏一样，国际象棋游戏中一方能够获胜的诀窍在于他能够增强自己的实力。
- 国际象棋棋手会设法预测对手的走法，这样才能压制对手，直至最后取胜。
- 国际象棋实际上就是一项走子和反向走子的游戏；也可认为黑客行为和安全策略采用了类似的方式。
- 防御策略存在于黑客行为和安全之中，但是一个具有侵略性和创造性的攻击者能够战胜它们。
- 进攻策略也存在于黑客行为和安全之中，但是聪明和警惕的防御者还是能够阻止它们。
- 执行欠佳的计划或者僵化地执行计划，就不如学习和调整有效果，这一点和国际象棋游戏是很类似的。
- 黑客行为和安全之间的“国际象棋”比赛的结果可能就取决于某一步。

使用这种类比，也可证明通常的黑客社区在寻求新的漏洞和利用代码上的足智多谋。这不是一个完美的类比(例如，防御者通常不会攻击进攻者)，但也很贴切了。国际象棋游戏的主题通过一系列的阐述(Trevor Young)，而被融入本书之中，也为我们的课题增添了一些艺术性(和幽默感)。

Susan Young
2003 年 3 月

本书结构

本书从结构上分为三个部分，以便帮助读者更好地理解书中的材料(参见表 1-1)。

表 1-1　本书的内容布局

章　节	标　题	章　节	标　题
第 1 章	导论：国际象棋游戏	第 10 章	目录服务
第一部分	基础材料	第 11 章	简单邮件传输协议
第 2 章	案例研究	第 12 章	超文本传输协议
第 3 章	了解对手	第 13 章	数据库入侵和安全
第 4 章	攻击剖析	第 14 章	恶意软件和病毒
第 5 章	防御武器库	第 15 章	网络硬件
第 6 章	程序设计	第三部分	攻击防范
第 7 章	IP 和第 2 层协议	第 16 章	了解攻击者的巩固策略
第 8 章	协议	第 17 章	取证调查中的问题
第二部分	系统和网络渗透	第 18 章	结论
第 9 章	域名服务器		

本书的第一部分介绍了程序设计、协议以及攻击的概念，这些概念将贯穿全书。本书的第二部分提出了一些特殊的主题域(协议、服务、技术、黑客工具和恶意代码)，它们都与系统和网络穿透密切相关。本书的最后一部分详细介绍了一旦黑客成功渗透进入系统或网络，建立并扩大“战果”，他们将采用的巩固措施的类型。

下面给出了每一章内容的详细分类。

第 2 章：案例研究

本章将介绍一些案例研究，阐述从管理员的角度来看待复杂的网络攻击。本书的结论(第 18 章)又从攻击者的角度回顾了开始的案例研究，从而贯穿整本书中介绍的材料。

该案例研究采用了一对虚构的角色(黑客和网络管理员)，并使用系统和设备的日志文件、截屏等材料，以及基于合理安全体系的相当复杂的网络，来制定攻击展开的步骤。

第 3 章：了解对手

第 3 章讲述了黑客的历史和构成黑客社区的不同成分，并对潜在的黑客进行了概述——脚本小子、黑客、骇客、竞争对手、政治激进分子、计算机恐怖分子、灰帽子和黑帽子等。

本章希望能够提供一些关于黑客心理和动机方面的认识。

第 4 章：攻击剖析

第 4 章给出了对各种类型攻击的“剖析”，以及攻击过程所用工具的分类。本章给出了一个模型来描述攻击策略的五个组成部分：

- 探测
- 锁定目标
- 系统或网络穿透
- 拒绝服务攻击
- 巩固

本章简要地回顾了“普通”类型的攻击，以此作为后续技术章节的背景知识，包括账户攻击、缓冲区溢出、拒绝服务攻击、会话劫持、欺骗等。

本章每节都有一个部分专门讨论“工具”，以表格形式列出了所有可用工具以及源代码和 Web 参考的索引。

第 5 章：防御武器库

本章仔细分析了管理员在联网环境中用来防御的工具，并对漏洞和可能会被利用的漏洞类型进行了介绍。

本章中提到的安全技术按照下面的框架进行组织：

- 访问控制
- 鉴别
- 审计和日志
- 资源控制
- 抗抵赖
- 私密性
- 入侵检测
- 数据完整性
- 平台完整性

第 6 章：程序设计

第 6 章是技术“基础”章节，可以认为是后面“协议”章节的技术性补充。本章给出了一些程序设计缺陷，黑客可利用它们来构建攻击代码、方法论以及其他一些程序设计工具。

为了照顾非程序员读者，本章详细介绍了各种类型的编译和解释语言，并对如下类型的程序设计缺陷和黑客工具进行了研究：

- 特定语言的缺陷

- 缓冲区溢出和内存分配错误
- 格式字符串错误
- 解释器错误
- 标准化攻击
- 逻辑错误
- 特定平台的安全问题
- Web 应用程序问题
- 远程过程调用(RPC)漏洞

本章结尾分析了一些在程序员之间引起争议的不同程序设计思想，是什么东西引起程序员之间的相互对立和竞争，以及一些软件程序员可以用来验证他们所开发软件安全性的工具。

第 7 章：IP 和第 2 层协议

第 8 章：协议

本章重点讨论 TCP/IP 协议，并介绍了一些“普通”的 TCP/IP 利用漏洞、拒绝服务攻击以及相关的防御措施。在某些情况下要使用的特殊协议将放在后续章节中介绍。本章将关注 TCP/IP 中会被黑客利用的基础漏洞，以及一些现有的 IP 安全动机。

使用 OSI 参考模型，按照下文来考察每一条协议：

- 第 2 层协议：地址解析协议(ARP)、反向地址解析协议(RARP)
- 第 3 层协议：网际协议(IP)、网际控制报文协议(ICMP)；路由协议，例如路由选择信息协议(RIP)、开放最短路径优先(OSPF)、增强的内部网关路由协议(EIGRP)，以及第 15 章中提到的边界网关协议(BGP)；第 5 章中详细介绍的 IP 安全协议(IPSec)
- 第 4 层协议：传输控制协议(TCP)、用户数据报协议(UDP)
- 第 5 层协议：第 5 章中提到的安全套接字层(SSL)
- 第 7 层协议：在各自章节中提到的每一条协议(DNS、HTTP、轻量级目录访问协议[LDAP]、开放数据库互连[ODBC]、远程过程调用[RPC]、SMTP、简单网络管理协议[SNMP]、结构化查询语言[SQL]等)

大量的材料都是有关 IP 协议的，IP 协议具有一些基础安全缺陷，使其很容易被作为网络攻击的载体。

第 9 章：域名服务器

本章的重点是域名系统(DNS)，它是一种重要的因特网“目录”服务，也是因特网安全中的脆弱环节。本章将 DNS 作为黑客行为、拒绝服务攻击、探测攻击和应用程序攻击的目标，来探索它的重要性。本章分析了下列各种利用漏洞进行的攻击：

- 探测攻击
- 缓存中毒攻击
- 应用程序攻击
- 拒绝服务攻击
- 动态域名注册攻击
- 客户端/服务器欺骗攻击
- 域名服务器劫持攻击

本章的最后一部分提供了一系列保护、验证和监控域名服务基础设施的工具，并且包括了有关分层 DNS 实现、域名服务器冗余、动态客户端安全，以及使用数字签名来保护域名服务器内容的相关信息。

第 10 章：目录服务

本章给出了网上通用的各种类型的目录服务的信息，以及易被攻击和探测的漏洞的类型。本章将详细讨论下列目录服务和目录服务协议：

- Microsoft 活动目录
- LDAP
- X.500 目录服务

和前面的章节一样，本章探讨了一些普通类型的黑客利用行为，它们能够影响目录服务和某些特定实现中的漏洞细节。本章还回顾了目录安全，并介绍了目录服务（例如，公共密钥基础设施）中特定应用程序内容的目录安全问题。

第 11 章：简单邮件传输协议

第 11 章分析了简单邮件传输协议（SMTP），并将它作为一种核心的因特网和专用网络服务，为传播恶意代码和进行拒绝服务（DoS）攻击提供重要的“引航”作用。

SMTP 协议中的密钥漏洞被作为黑客材料内容进行了详细的阐述，此外，还通过分析各种攻击、利用代码和分组数据对邮件黑客行为进行了探讨，其中包括：

- 邮件窃听和探测
- ESMTP 攻击
- 拒绝服务攻击
- 垃圾邮件和中继攻击
- 邮件哄骗
- MIME 攻击

本章最后给出了管理员可以用来加固 SMTP 服务器的工具，以及定位协议（例如，安全/多功能因特网邮件扩充协议[S/MIME]）中特定漏洞的安全工具。

第 12 章：超文本传输协议

由于因特网商务，以及通过超文本传输协议（HTTP）传输各种敏感的个人和商务数据的出现，本章强调 HTTP 作为黑客攻击目标的重要性。HTTP 服务器通常可以提供可访问的 Web 前台、复杂的后台数据库和传统应用程序，这些为黑客提供了一个装载应用程序和进行数据探测攻击的“渠道”。

HTTP 黑客攻击分为以下几种类型：

- 窃听和探测
- 账号破解和鉴别证书捕获
- HTTP 方法利用（POST、PUT 等）
- HTTP 的缓存利用
- 拒绝服务攻击
- 目录遍历攻击
- 会话 ID 黑客攻击
- 中间人攻击

本章最后总结了 HTTP 的安全机制，例如 SSL、缓存控制、数字认证或签名安全和会话 ID 安全选项等。

第 13 章：数据库入侵和安全

数据库黑客攻击和数据库安全方面的资料可以说是汗牛充栋。本章主要观注特定类型数据库技术（SQL Server、Oracle、MySQL）中的漏洞，从而阐述数据库黑客攻击和数据安全的一些基本知识。数据库黑客攻击常见的主题包括：

- SQL 注入
- 溢出
- 默认账号利用

本章使用有代表性的数据库应用程序和范例来增加材料的“深度”，并列出了识别和利用脆弱的数据库应用程序的过程。