挑战黑客

——网络安全的最终解决方案

HACKER PROOF

The Ultimate Guide to Network Security

- [美] 拉斯·克兰德 著
- 陈永剑 沈兰生 任鲲鹏 等译
- 刘咏亭 刘咏新 审校

JAMSA

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

URL: http://www.phei.com.cn

73.97
318

挑 战 黑 客

——网络安全的最终解决方案

HACKER PROOF
The Ultimate Guide to Network Security

[美] 拉斯·克兰德 著

陈永剑 沈兰生 任鲲鹏 等译

刘咏亭 刘咏新 审校

2011005

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

2011005

内容简介

本书面向网络用户，全面介绍了网络安全性方面的基本问题。首先给读者介绍了几种常见的网络协议，如 TCP/IP，HTTP，S－HTTP。接着谈到了防火墙、加密及数字签证方面的知识。作者还分析了黑客种种攻击网络弱点的方法，并指出我们应该怎样预防。最后，逐个比较各种网络在安全性上的优缺点，并提出一个可行的安全方案。

本书内容详实、编排得当，适应用户阅读习惯，是一本献给网络管理员、MIS 专家、程序员及终端用户的，不可多得的网络安全性方面的最新图书。

Copyright©1997 by Jamsa Press. All rights reserved.

本书中文简体专有翻译出版权由美国 Jamsa Press 授予电子工业出版社，并可在全球出版发行。该书专有出版权受法律保护。

图书在版编目(CIP)数据

挑战黑客——网络安全的最终解决方案/(美)拉斯·克兰德(Lars Klander)著；陈永剑等译．
－北京：电子工业出版社，2000.6
ISBN 7－5053－4990－2

Ⅰ．挑… Ⅱ．①兰… ②陈… 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(2000)第 07682 号

书　　名：**挑战黑客——网络安全的最终解决方案**
原 书 名：**HACKER PROOF　The Ultimate Guide to Network Security**
著　　者：[美]拉斯·克兰德
译　　者：陈永剑　沈兰生　任鲲鹏　等
审 校 者：刘咏亭　刘咏新
责任编辑：吴剑锋
特约编辑：黄亚昌
印 刷 者：北京京安达明印刷厂
装 订 者：三河市金马印装有限公司
出版发行：电子工业出版社　　URL：http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036　发行部电话 68214070
经　　销：各地新华书店
开　　本：787×1092 1/16　印张：32.5　字数：825.6 千字
版　　次：2000 年 6 月第 1 版　2000 年 9 月第 2 次印刷
书　　号：ISBN 7-5053-4990-2 / TP·2462
印　　数：2000 册　　定价：52.00 元
著作权合同登记号　图字：01－97－1858

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。电话　68279077

译 者 序

随着网络使用的日益广泛，其安全性成为人们关注的焦点。而对安全性的最大威胁就是所谓的网络“黑客”。为了让不同层次的读者对黑客的危害及防御方法有一个清楚的认识，我们合力翻译了《挑战黑客》一书。

全书的内容可分为四大块：一、网络与网络协议；二、不同类型网络的特点及其安全漏洞；三、黑客的种类及防御方法；四、安全的网络方案。

参加本书翻译的人员有：陈永剑、沈兰生、任鲲鹏、甘荃、吴炜、刘小光、滕广松、董恩广、鲍治国、付勇军、王梅玲、徐杨勇、邢燕。由于时间仓促，书中难免有不妥之处，敬请广大读者不吝指正。

最后，我们感谢电子工业出版社对我们工作的大力支持，并向《Haker Proof》的原作者表示敬意。

译 者

2000 年 2 月

目　录

第一章　认识危机——接入 Internet 的计算机网络 …… (1)

1.1　1988 年的 Internet 蠕虫事件 …… (1)
1.2　Internet worm 的机理 …… (3)
1.3　Internet worm 的影响 …… (4)
1.4　不断增长的危险 …… (4)
1.5　什么是 Internet …… (6)
1.6　报文交换:网络的"建材" …… (9)
1.6.1　用报文交换来传送数据 …… (9)
1.7　Internet 的先驱:ARPANET …… (11)
1.8　ARPANET 通信功能的扩展:TCP/IP …… (12)
1.9　WWW 的介绍 …… (12)
1.10　作为商业机遇的、不可或缺的工具——Web …… (14)
1.11　考虑危险 …… (14)
1.12　关于黑客定义的争论 …… (15)
1.13　威胁的种类:概述 …… (15)
1.14　企业内部网(Intranet)——Internet 的表弟 …… (19)
1.15　回顾黑客的种类及更多信息 …… (20)
1.16　与安全性相关的邮件列表和新闻组 …… (20)
1.17　总结 …… (22)
1.18　附加的 Internet 资源: …… (23)

第二章　网络和 TCP/IP …… (25)

2.1　基本网络和 TCP/IP 的简单描述 …… (25)
2.1.1　定义 TCP/IP 协议的组成部分 …… (26)
2.2　ISO/OSI 网络模型 …… (26)
2.2.1　定义协议栈 …… (26)
2.2.2　数据是怎样在各层之间传输的 …… (27)
2.2.3　TCP/IP 对 ISO/OSI 模型的实现 …… (28)
2.2.4　物理层 …… (30)
2.2.5　数据链路层 …… (30)
2.2.6　网络层 …… (30)

试读结束，需要全本PDF请购买 www.ertongbook.com

2.2.7 传输层 …… (31)
2.2.8 应用层 …… (32)
2.3 TCP/IP选址方案 …… (33)
2.3.1 地址分类 …… (33)
2.3.2 定义地址类型 …… (34)
2.4 传输控制协议 …… (35)
2.4.1 可靠性 …… (35)
2.4.2 滑窗 …… (36)
2.4.3 定义 TCP 消息 …… (37)
2.4.4 创建一个 TCP 连接 …… (38)
2.4.5 起始顺序号 …… (39)
2.4.6 响应数据的传输 …… (39)
2.4.7 建立正式连接 …… (39)
2.4.8 理解顺序号 …… (39)
2.4.9 使用全双工服务 …… (40)
2.4.10 终止一个 TCP 连接 …… (40)
2.4.11 TCP 文件头 …… (41)
2.4.12 源端口和目的端口 …… (41)
2.4.13 顺序号 …… (42)
2.4.14 应答号 …… (42)
2.4.15 头文件长度 …… (42)
2.4.16 标识位 …… (42)
2.4.17 滑窗大小 …… (42)
2.4.18 TCP 校验和 …… (43)
2.4.19 紧要指针 …… (43)
2.4.20 选项 …… (43)
2.4.21 从概念到设计 …… (44)
2.5 网络拓扑结构 …… (44)
2.5.1 星型拓扑 …… (44)
2.5.2 环型拓扑 …… (45)
2.5.3 总线型拓扑 …… (45)
2.5.4 总线仲裁 …… (45)
2.5.5 令牌传送 …… (46)
2.6 各种网络技术 …… (46)
2.6.1 以太网 …… (47)
2.6.2 ARCNET …… (47)
2.6.3 IBM 令牌环网 …… (47)
2.6.4 ATM 网 …… (48)
2.7 连接计算机网 …… (48)

2.7.1 转发器和信号消弱 …… (48)
2.7.2 错误控制和校验和 …… (48)
2.7.3 用网桥来改进网络 …… (49)
2.7.4 理解和使用路由器 …… (50)
2.7.5 理解和使用网关 …… (50)
2.8 网络物理结构 …… (51)
2.8.1 广播波段的不同种类 …… (51)
2.9 总结 …… (53)
2.10 与 ISO/OSI 及 TCP/IP 相关的 Internet 资源 …… (53)

第三章 了解和使用防火墙 …… (56)

3.1 安全性的不同形式 …… (56)
3.1.1 防止外部侵扰 …… (57)
3.1.2 防止内部系统的侵犯 …… (58)
3.2 介绍防火墙的构造 …… (59)
3.3 防火墙 …… (60)
3.3.1 冒险区 …… (61)
3.3.2 防火墙的局限性 …… (62)
3.3.3 三种类型的防火墙 …… (63)
3.3.4 网络层防火墙 …… (63)
3.3.5 应用层防火墙 …… (65)
3.3.6 链路层防火墙 …… (66)
3.4 防火墙结构 …… (67)
3.4.1 双主机防火墙 …… (67)
3.4.2 主机屏蔽防火墙 …… (68)
3.4.3 子网屏蔽防火墙 …… (69)
3.5 最小化的安全性等级分类 …… (70)
3.6 总结 …… (74)
3.7 与防火墙相关的 Internet 资源 …… (74)

第四章 利用加密保护你的信息传递 …… (76)

4.1 为什么说加密是非常重要的 …… (76)
4.2 加密基础知识 …… (77)
4.2.1 常规单密钥加密体系的局限性 …… (77)
4.3 公用密钥系统 …… (80)
4.3.1 RSA 算法 …… (81)
4.3.2 RSA 算法本身 …… (82)

4.4 DIFFIE 和 HELLMAN 简介 …… (84)
4.4.1 Diffie – Hellman 加密算法 …… (84)
4.4.2 公用密钥协议中的信息认证 …… (85)
4.5 安全性只能如此 …… (86)
4.5.1 怎样有效管理公用密钥加密 …… (86)
4.5.2 密钥证书和密钥链 …… (87)
4.6 消息摘要算法 …… (88)
4.7 机密增强型邮件(PEM) …… (89)
4.7.1 用 PEM 产生认证 …… (89)
4.7.2 PEM 中的信息机密性 …… (89)
4.7.3 PEM 中的数据完整性 …… (89)
4.8 对主要加密程序的简短讨论 …… (90)
4.8.1 完美的加密(PGP) …… (90)
4.8.2 PGP 使用多种加密方式 …… (90)
4.9 复习公用密钥的结构 …… (91)
4.9.1 PGP 的广泛使用 …… (92)
4.9.2 密码和谜 …… (93)
4.9.3 SMTP 与解码 …… (93)
4.10 微软的 CryptoAPI …… (93)
4.11 对加密系统的计时入侵 …… (96)
4.12 加密新法:椭圆曲线加密 …… (97)
4.12.1 椭圆曲线的安全性 …… (97)
4.13 总结 …… (97)
4.14 文档加密和传送方面的 Internet 资源 …… (98)

第五章 利用数字签名证实消息源 …… (100)

5.1 数字签名的建立 …… (100)
5.2 数字签名的重要性 …… (102)
5.3 数字签名与手写签名的对比 …… (104)
5.4 使用数字签名 …… (105)
5.5 美国数字签名标准(DSS) …… (106)
5.5.1 关注 DSS …… (106)
5.5.2 NSA 的作用 …… (107)
5.5.3 卷入安全标准发展的 NSA …… (107)
5.5.4 在 DSS 上的进展 …… (108)
5.5.5 数字签名和机密增强型邮件(PEM) …… (109)
5.6 重温 Diffie – Hellman 算法 …… (110)
5.6.1 数字签名的未来 …… (111)

5.7 数字签名和文件标识 …… (112)
5.7.1 认证机构 …… (114)
5.8 总结 …… (116)
5.9 与数字签名有关的 Internet 资源 …… (116)

第六章 超文本传输协议 …… (118)

6.1 HTTP——Web 的基本协议 …… (118)
6.2 MIME …… (119)
6.2.1 在网上使用 MIME …… (120)
6.2.2 MIME 类型及其子类型 …… (120)
6.2.3 测试 MIME 类型 …… (122)
6.3 深入了解 HTTP …… (123)
6.3.1 HTTP 是无状态的 …… (123)
6.3.2 无状态通信的高效性 …… (123)
6.3.3 HTTP 支持动态格式 …… (124)
6.3.4 HTTP 头信息 …… (124)
6.3.5 HTTP 是可读的 …… (124)
6.4 HTTP 怎样进行查找、检索和注释 …… (125)
6.4.1 查找资源 …… (125)
6.4.2 检索资源 …… (126)
6.4.3 注释资源 …… (126)
6.5 HTTP 四步处理法 …… (126)
6.5.1 第一步:建立客户端与服务器的连接 …… (126)
6.5.2 第二步:客户端向服务器发出请求 …… (127)
6.5.3 第三步:服务器的响应 …… (127)
6.5.4 第四步:服务器与客户端断开连接 …… (128)
6.6 HTTP 响应代码类型 …… (128)
6.7 进一步了解 URI …… (130)
6.8 回顾 URL …… (130)
6.8.1 URL、协议和文件类型 …… (131)
6.8.2 URL 部件 …… (131)
6.9 URL 和 HTML …… (131)
6.10 绝对 URL 和相对 URL …… (132)
6.10.1 绝对 URL …… (132)
6.10.2 相对 URL …… (132)
6.10.3 进一步了解相对 URL …… (133)
6.11 HTTP 请求方法 …… (133)
6.11.1 GET 方法 …… (134)

6.11.2 HEAD 方法 …… (134)
6.11.3 POST 方法 …… (135)
6.12 介绍其他 HTTP 方法 …… (135)
6.13 总头域 …… (136)
6.13.1 HTTP 数据域 …… (136)
6.13.2 MIME 版本域 …… (136)
6.13.3 Pragma 域 …… (136)
6.14 请求头域 …… (137)
6.14.1 接受域 …… (137)
6.14.2 认证域 …… (137)
6.14.3 缘起域 …… (137)
6.14.4 If - Modified - Since 域 …… (138)
6.14.5 参考域 …… (138)
6.14.6 用户代理域 …… (138)
6.15 实体头域 …… (138)
6.15.1 允许域 …… (138)
6.15.2 内容加密域 …… (139)
6.15.3 内容长度域 …… (139)
6.15.4 内容类型域 …… (139)
6.15.5 期限域 …… (140)
6.15.6 扩展头域 …… (140)
6.15.7 最新修改域 …… (140)
6.16 响应 …… (140)
6.16.1 HTTP 响应头域 …… (140)
6.16.2 位置域 …… (141)
6.16.3 服务器域 …… (141)
6.16.4 WWW 认证域 …… (141)
6.17 实体主体 …… (141)
6.18 关于网络数据通信 …… (142)
6.19 考察一个 HTTP 处理范例 …… (142)
6.20 总结 …… (143)
6.21 HTTP 编程方面的 Internet 资源 …… (143)

第七章 安全超文本传输协议 …… (146)

7.1 介绍 S - HTTP …… (146)
7.1.1 S - HTTP 如何创建消息 …… (146)
7.1.2 S - HTTP 怎样恢复消息 …… (148)
7.1.3 S - HTTP 的加密方法 …… (149)

7.2 S-HTTP的详述 …… (152)
7.3 S-HTTP增加的内容 …… (153)
7.3.1 S-HTTP的密码算法和数字签名模式 …… (153)
7.4 数字签名与S-HTTP …… (154)
7.4.1 密钥交换和加密 …… (154)
7.4.2 消息完整性和发送者认证 …… (155)
7.4.3 S-HTTP事务处理的新鲜度 …… (155)
7.4.4 HTTP封装 …… (155)
7.4.5 S-HTTP的请求行 …… (155)
7.4.6 S-HTTP的响应行 …… (156)
7.4.7 S-HTTP的头域行 …… (156)
7.4.8 S-HTTP接受的内容类型 …… (156)
7.4.9 解析S-HTTP头域:Prearranged-Key-Info …… (157)
7.4.10 MAC-Info头域 …… (157)
7.5 S-HTTP消息内容 …… (158)
7.6 S-HTTP和Content-Privacy-Domain:PEM …… (158)
7.7 PEM和S-HTTP模式的一致性 …… (159)
7.8 S-HTTP的协商内容 …… (159)
7.8.1 协商头域格式 …… (159)
7.8.2 S-HTTP的协商头域 …… (160)
7.8.3 密钥模式参数 …… (161)
7.8.4 S-HTTP缺省值 …… (163)
7.8.5 S-HTTP的头域行 …… (163)
7.8.6 Certificate-Info头域行 …… (164)
7.8.7 Key-Assign头域 …… (164)
7.8.8 使用Inband密钥分配法 …… (165)
7.8.9 使用Kerberos密钥分配法 …… (165)
7.8.10 S-HTTP Nonce的用法 …… (165)
7.8.11 S-HTTP服务器状态错误报告的处理 …… (165)
7.8.12 S-HTTP的重试行为 …… (166)
7.8.13 S-HTTP自动重试的局限性 …… (166)
7.8.14 自动加密的重试 …… (166)
7.9 S-HTTP HTML元素 …… (166)
7.9.1 S-HTTP HTML和URL的扩展 …… (167)
7.9.2 CERTS元素 …… (167)
7.9.3 CRYPTOPTS元素 …… (167)
7.10 总结 …… (168)
7.11 相关的Internet资源 …… (168)

试读结束，需要全本PDF请购买 www.ertongbook.com

第八章　用 SSL 安全地传送信息 …… (171)

8.1　介绍 SSL …… (171)
8.2　理解 SSL 是怎样提供信息的安全传送 …… (172)
8.2.1　SSL 用数字证书来鉴别服务器 …… (173)
8.2.2　SSL 应用 RSA 加密机制 …… (175)
8.2.3　SSL 建立安全的连接 …… (175)
8.3　SSL 浏览器和服务器的特点 …… (175)
8.3.1　如何判定你是通过安全的连接进行通讯的？ …… (175)
8.3.2　验证 Navigator 和 Internet Explorer 通讯的安全性 …… (175)
8.3.3　SSL 服务器 …… (176)
8.4　SSLD——SSL DAEMON …… (178)
8.4.1　SSLD 的配置文件 …… (179)
8.4.2　SSLD 安全性中一些值得注意的事件 …… (180)
8.5　SSL 和防火墙管道 …… (180)
8.5.1　SSL 管道和连接的方法 …… (181)
8.5.2　SSL 管道与安全性考虑 …… (182)
8.5.3　SSL 管道和可扩充性 …… (182)
8.6　S/MIME …… (184)
8.7　Netscape 的对象标识 …… (184)
8.8　Netscape 的安全性 API …… (185)
8.9　总结 …… (187)
8.10　与 SSL 相关的 Internet 资源 …… (187)

第九章　鉴别与防御“黑客”入侵 …… (189)

9.1　最简单的“黑客”入侵 …… (189)
9.2　TCP 协议劫持入侵 …… (191)
9.3　嗅探入侵 …… (191)
9.4　主动的非同步入侵 …… (192)
9.4.1　非同步后劫持入侵 …… (193)
9.4.2　TCP ACK 风暴 …… (195)
9.4.3　前期非同步入侵 …… (195)
9.4.4　空数据非同步入侵 …… (196)
9.4.5　Telnet 会话入侵 …… (197)
9.4.6　进一步了解 ACK 风暴 …… (198)
9.4.7　检测及其副作用 …… (198)
9.4.8　防卫非同步后劫持入侵 …… (199)

9.5 另一种嗅探——冒充入侵 …… (199)
9.6 关于作假的详述 …… (200)
9.6.1 冒充 e-mail …… (201)
9.7 检测作假 …… (202)
9.8 防止作假 …… (202)
9.9 关于劫持会话入侵 …… (203)
9.9.1 检测劫持会话 …… (203)
9.9.2 防卫劫持会话 …… (203)
9.10 超级链接欺骗:SSL 服务器认证中的一种入侵 …… (203)
9.10.1 超级链接欺骗的背景 …… (204)
9.10.2 实施超级链接欺骗 …… (204)
9.10.3 防卫超级链接欺骗的方法 …… (205)
9.10.4 对超级链接欺骗的长远考虑 …… (207)
9.11 网页作假 …… (209)
9.11.1 网页作假的后果 …… (209)
9.11.2 作假整个 Web …… (210)
9.11.3 入侵过程 …… (210)
9.11.4 重访表格和安全连接 …… (211)
9.11.5 开始网页作假入侵 …… (212)
9.11.6 制造错觉——状态条 …… (212)
9.11.7 位置行 …… (213)
9.11.8 查看文档信息 …… (213)
9.11.9 对网页作假入侵的补救措施 …… (213)
9.11.10 对网页作假入侵的长远解决方案 …… (214)
9.12 总结 …… (214)
9.13 与一般黑客入侵相关的 Internet 资源 …… (215)

第十章 在分布式系统中使用 Kerberos 密钥交换 …… (218)

10.1 介绍 kerberos …… (218)
10.1.1 从不同的角度观察 …… (221)
10.1.2 回顾 kerberos 认证过程 …… (222)
10.2 kerberos 协议 …… (222)
10.3 kerberos 跨领域操作 …… (224)
10.3.1 领域间密钥 …… (224)
10.3.2 认证路径 …… (225)
10.4 票据标志使用和请求 …… (227)
10.4.1 初始化票据 …… (227)
10.4.2 认证前票据 …… (227)

10.4.3 非法票据 …… (228)
10.4.4 更新的票据 …… (228)
10.4.5 过期的票据 …… (228)
10.4.6 代理的和代理票据 …… (229)
10.4.7 前趋的票据 …… (230)
10.4.8 其他的认证服务器选项 …… (231)
10.5 kerberos 数据库 …… (231)
10.5.1 数据库内容 …… (231)
10.5.2 附加的数据库域 …… (232)
10.5.3 频繁改变的数据库域 …… (232)
10.6 领域名 …… (232)
10.7 当事人名 …… (233)
10.8 kerberos 已知的易感染性 …… (234)
10.8.1 实施 kerberos 必需的设想 …… (234)
10.9 kerberos 邮件列表 …… (235)
10.10 总结 …… (236)
10.11 与 kerberos 相关的 Internet 资源 …… (236)

第十一章 保护你在电子商务中的传输信息 …… (239)

11.1 回顾电子商务的基本问题 …… (239)
11.2 数字现金 …… (241)
11.2.1 数字现金怎样解决隐私问题 …… (241)
11.2.2 数字现金的安全性 …… (243)
11.2.3 数字现金存在的问题 …… (244)
11.3 进一步理解"隐藏"签证的原理 …… (245)
11.4 信用卡的使用和 Internet …… (246)
11.4.1 浏览证书 …… (249)
11.5 总结 …… (249)
11.6 与电子商务相关的 Internet 资源 …… (250)

第十二章 利用审计跟踪并击退入侵 …… (252)

12.1 简化审计跟踪 …… (252)
12.1.1 关于审计问题 …… (253)
12.2 审计跟踪和 UNIX …… (254)
12.2.1 用 lastlog 来检查用户的最后访问 …… (254)
12.2.2 用 UTMP 来跟踪用户 …… (255)
12.2.3 用 WTMP 跟踪先前登录者 …… (255)

12.2.4 使用 syslog 日志 …… (256)
12.2.5 用 sulog 跟踪用户的变换 …… (259)
12.2.6 用 aculog 来跟踪 dial-out 访问 …… (259)
12.2.7 记录指定时间的事务 …… (259)
12.2.8 用 sendmail 日志来跟踪 SMTP 入侵者 …… (260)
12.2.9 外壳(shell)历史日志 …… (260)
12.3 Windows NT 的审计 …… (260)
12.3.1 激活 NT 的安全日志 …… (260)
12.3.2 用 NT 审计基层对象 …… (262)
12.3.3 基层对象审计 …… (263)
12.3.4 用 NT 进行特权审计 …… (264)
12.3.5 关闭 FullAuditLog 选项 …… (265)
12.4 Novell NetWare 审计 …… (266)
12.4.1 NetWare 怎样定义审计服务 …… (266)
12.4.2 浏览审计记录 …… (267)
12.4.3 使 NetWare 中的审计器有效 …… (267)
12.4.4 使卷审计有效 …… (268)
12.4.5 使 NDS 容器(Container)的审计有效 …… (269)
12.5 总 结 …… (270)
12.6 与审计跟踪相关的 Internet 资源 …… (271)

第十三章 关于 Java 的安全性问题 …… (273)

13.1 掌握 Java …… (273)
13.2 Java 怎样在浏览器中执行 …… (276)
13.3 Java 组件 …… (277)
13.3.1 Applet 类载入器 …… (277)
13.3.2 类校验器 …… (277)
13.3.3 Applet 安全性管理器 …… (279)
13.4 基本的安全性问题 …… (279)
13.5 掌握 Java 基本原理 …… (280)
13.5.1 Java applet 的功能性限制 …… (280)
13.5.2 使用 Applet 读写文件 …… (281)
13.5.3 编辑读文件的访问控制列表 …… (281)
13.5.4 编辑写文件的访问控制列表 …… (282)
13.6 使用 Applet 读系统属性 …… (283)
13.6.1 隐藏系统信息 …… (284)
13.6.2 显示受保护的系统信息 …… (284)
13.7 通过 Applet 打开与另一台机器的连接 …… (284)

13.7.1 打开一个同 Applet 源服务器的网络连接 …… (285)
13.7.2 维持永久的 Applet …… (286)
13.8 从 Applet 生成程序 …… (286)
13.9 使用 Java 创建安全的 Applet …… (288)
13.10 理解差异所在 …… (289)
13.11 创建可信任的运算基础体制 …… (289)
13.11.1 Kimera Java 安全工程 …… (290)
13.11.2 使用 Kimera 反汇编和字节校验码测试类 …… (290)
13.12 回顾一些有害的 Applet …… (291)
13.13 Jigsaw 服务器 …… (292)
13.14 总结 …… (292)

第十四章 预防病毒 …… (296)

14.1 病毒是如何工作的 …… (296)
14.2 最一般的传染威胁 …… (299)
14.2.1 通过电子邮件传输病毒的威胁 …… (300)
14.3 病毒的类型： …… (301)
14.3.1 特洛伊木马 …… (301)
14.3.2 多态病毒 …… (301)
14.3.3 行骗病毒 …… (302)
14.3.4 慢效病毒 …… (303)
14.3.5 制动火箭病毒 …… (304)
14.3.6 多成份病毒 …… (304)
14.3.7 装甲病毒 …… (304)
14.3.8 同伴病毒 …… (305)
14.3.9 噬菌体病毒 …… (305)
14.3.10 回顾蠕虫事件 …… (305)
14.3.11 病毒对网络和 Internet 的威胁 …… (306)
14.3.12 关于文件病毒 …… (306)
14.4 关于宏病毒 …… (307)
14.4.1 一些流行的宏病毒 …… (309)
14.4.2 宏病毒的最佳解决办法 …… (312)
14.5 互联网上的病毒欺骗 …… (313)
14.5.1 IRINA 病毒 …… (313)
14.5.2 Good Times 病毒 …… (313)
14.5.3 aol4free.com …… (314)
14.5.4 怎样分辨出一个真正的病毒警告 …… (314)
14.6 防止病毒从 Internet 上感染你的网络 …… (315)

14.6.1 反病毒软件如何检测病毒 …… (315)
14.6.2 反病毒软件的主要出版商 …… (315)
14.7 总结 …… (316)
14.8 与病毒有关的 Internet 资源 …… (317)

第十五章 加强 Windows NT 的网络安全性 …… (319)

15.1 Windows NT 简介 …… (319)
15.1.1 共享 …… (320)
15.1.2 NTFS 的脆弱性 …… (320)
15.2 Windows NT 安全模式的原理 …… (321)
15.2.1 SAM 怎样对用户授权 …… (324)
15.3 更好地理解工作组和权限 …… (326)
15.3.1 NT 缺省的域工作组 …… (326)
15.3.2 Windows NT 缺省的本地组 …… (327)
15.3.3 Windows NT 缺省的目录权限 …… (328)
15.3.4 Administrators 及其同等物 …… (328)
15.3.5 使用安全性 Administrator ID …… (329)
15.3.6 使 Administrators 组安全可靠 …… (329)
15.3.7 NT 怎样存储口令 …… (330)
15.3.8 黑客如何破译密码 …… (331)
15.3.9 使用 Brute - Force 攻击方法 …… (331)
15.3.10 防备字典式破译 …… (332)
15.3.11 没有使用锁定功能的 Windows NT …… (332)
15.3.12 不加口令的 Windows NT 系统管理员帐号 …… (332)
15.3.13 Windows NT 系统管理员帐号 …… (333)
15.3.14 Windows NT 中没有密码的 Guest 帐号 …… (333)
15.4 NT 与 TCP 和 HTTP 的联系 …… (333)
15.5 Windows NT 支持多个安全性协议接口 …… (334)
15.5.1 安全消息块服务简介 …… (335)
15.6 认识 Windows NT 的一些缺陷 …… (336)
15.6.1 NT 的示警和消息服务 …… (337)
15.6.2 防备 NetBIOS 完全访问共享 …… (337)
15.6.3 掌握 LAN Manager 的安全性 …… (337)
15.6.4 Windows NT 网络监视器 …… (337)
15.6.5 Windows NT RSH 服务 …… (338)
15.6.6 Windows NT Schedule 服务 …… (338)
15.7 Windws NT 注册表 …… (338)
15.8 NT 系统和计算机病毒 …… (339)

试读结束，需要全本PDF请购买 www.ertongbook.com