Mc Graw Hill Education

国外经典初学者入门教程系列

网络安全

实用教程(第二版)

Networking Security

A Beginner's Guide

Eric Maiwald 著
李庆荣 黄开枝 等译

清华大学出版社

网络安全实用教程

（第二版）

Eric Maiwald 著

李庆荣　黄开枝　等 译

清华大学出版社

北　京

Eric Maiwald
Network Security: A Beginner's Guide
EISBN: 0-07-222957-8

北京市版权局著作权合同登记号 图字 01-2003-4891 号

图书在版编目(CIP)数据

网络安全实用教程/(美)麦伍德(Maiwald, E.)著；李庆荣等译. —2 版. —北京:清华大学出版社，2003.11
书名原文：Network Security: A Beginner's Guide
ISBN 7-302-07366-X

Ⅰ. 网… Ⅱ. ①麦…②李… Ⅲ. 计算机网络—安全技术—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2003)第 090487 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社总机：010-62770175　　**客户服务**：010-62776969
责任编辑：冯志强
封面设计：张范云
印 刷 者：世界知识印刷厂
装 订 者：北京鑫海金澳印刷厂
发 行 者：新华书店总店北京发行所\清华大学出版社出版发行
开　　本：185×230　**印张**：25　**插页**：1　**字数**：554 千字
版　　次：2003 年 11 月第 1 版　2003 年 11 月第 1 次印刷
书　　号：ISBN 7-302-07366-X/TP·5346
印　　数：1～4000
定　　价：45.00 元

致　谢

本书得以出版，得到了众人的帮助，包括：Lee Kelly、John Alexander、Rob Fike、Dave Henning、Sam Hinson、Robert Burnett 和 Lauren Schuler。当然也包括 McGraw-Hill/Osborne 的人员，包括：Jane Brownlow、Athena Honore 和 Jody McKenzie 等。

前　言

本书书名已经指出了本书的内容。但是本书并不仅仅是一本入门教程。在编写本书的时候，我还挑选了我作为安全官员和顾问时在日常工作中遇到的那些棘手的问题。这些问题曾经困扰了我多年，在编写本书时对我整理资料起了很大的帮助作用。

安全仍然是各种机构面临的大问题。我们不仅仅听说过成功侵入网站和机构的事例，而且还知道现在已经制订了新的法律和规则来保护信息。为了解决这些问题，越来越多的公司开发了安全保护工具。从这些情况看来，似乎安全方面的最大问题通过技术就可以解决。遗憾的是，安全问题远远比此复杂。最低限度讲，安全也是人的问题。不管我们开发了多少技术，但是最好的做法莫过于简化安全从业人员的工作难度。我们不应仅通过技术解决基本的安全问题，还必须通过应用深思熟虑的安全进程和过程来管理安全问题。

本书第二版增加了许多新信息和新功能。项目、思考与练习和自测题可以帮助读者完整地理解安全。本书还提供了必要的基本工具来管理安全问题。

作者简介

Eric Maiwald 是 Bluefire Security Technologies 公司的产品管理和技术支持负责人。Eric 在信息安全领域具有长达 15 年的丰富阅历。他既在政府部门工作过，也为商业公司工作过。他为大型金融机构、保健公司和制造商从事工作评估、开发策略，并实现安全解决方案。Eric 获得了 Rensselaer Polytechnic Institute 的电子工程学士学位，获得了 Stevens Institute of Technology 的工程硕士学位，并且是信息系统安全认证专家(CISSP)。他在大量著名的安全会议上作过发言，并编写了 *Security Planning and Disaster Recovery*(与 William Sieglein 合作，此书由 McGraw-Hill/Osborne 出版)，与他人合作编写了 *Hacking Linux Exposed* and *Hackerr's Challenge*(由 McGraw-Hill/Osborne 出版)。他的电子邮箱是 emaiwald@ fred. net。

本书合作作者

Philip Cox 是 SystemExperts Corporation 的顾问。他是业界公认的顾问、作家和演讲人，作出过许多业绩。Phil 是权威图书 *Windows* 2000 *Security Handbook*(由 McGraw-Hill/Osborne 出版)的主要作者。他获得了 College of Charleston 的计算机专业理学学士学位，还是 Microsoft Certified Systems Engineer(微软认证系统工程师，MCSE)。

本书技术编辑

John Bock 是一位 CISSP，是 Foundstone 的研发工程师，主要研究方向是网络评估技术和网络安全。他负责设计 Foundstone Enterprise Risk Solutions 产品线新的评估特征。John 在网络安全方面具有深厚的顾问阅历，领导了一个企业安全小组。在加入 Foundstone 之前，他完成了攻击测试和安全评估，是 Internet Security Systems(ISS)的网络安全顾问。

Mariana Hentea 是印第安那州 Calumet 的 Purdue University 的助教，她是 IEEE 和 SWE 的成员。她获得了 Chicago 的 Illinonis Institute of Technology 的计算机硕士和博士学位，以及 Romania 的 Polytechnic Institute of Timisoara 的电子工程学士学位和计算机硕士学位。她发表了关于通信、冶金和化学工业领域计算机软件和工程应用方面的大量论文。1995 年，Mariana 参与设计和实施了美国国防部的计算机和网络安全。

目　录

第一部分　信息安全基础知识

第 1 章　信息安全 …… 3
1.1　信息安全定义 …… 4
1.2　安全是一个过程，而不是静止产品 …… 10
1.2.1　防病毒软件 …… 10
1.2.2　访问控制 …… 10
1.2.3　防火墙 …… 11
1.2.4　智能卡 …… 11
1.2.5　生物统计学系统 …… 11
1.2.6　入侵检测 …… 12
1.2.7　策略管理 …… 12
1.2.8　薄弱点扫描 …… 12
1.2.9　加密 …… 13
1.2.10　物理安全机制 …… 13
项目 1　检查计算机安全认证 …… 13
1.3　思考与练习 …… 14

第 2 章　攻击类型 …… 15
2.1　定义访问攻击 …… 16
2.1.1　监听 …… 16
2.1.2　窃听 …… 16
2.1.3　截听 …… 18
2.1.4　访问攻击是如何完成的 …… 18
2.2　定义修改攻击 …… 21
2.2.1　更改攻击 …… 21
2.2.2　插入攻击 …… 21
2.2.3　删除攻击 …… 22
2.2.4　如何完成修改攻击 …… 22
2.3　拒绝服务攻击 …… 23

2.3.1 拒绝对信息进行访问 …… 23
2.3.2 拒绝对应用程序进行访问 …… 23
2.3.3 拒绝对系统进行访问 …… 23
2.3.4 拒绝对通信进行访问 …… 23
2.3.5 如何实现 DoS 攻击 …… 24
2.4 否认攻击 …… 25
2.4.1 伪装 …… 25
2.4.2 否认事件 …… 25
2.4.3 如何实现否认攻击 …… 25
项目 2 检查系统的薄弱点 …… 26
2.5 思考与练习 …… 27

第 3 章 黑客技术 …… 28
3.1 黑客的动机 …… 29
3.1.1 挑战 …… 29
3.1.2 贪婪 …… 30
3.1.3 恶意 …… 30
3.2 学习历史上的黑客技术 …… 31
3.2.1 开放共享 …… 31
3.2.2 糟糕的密码 …… 32
3.2.3 编程中的漏洞 …… 33
3.2.4 社会工程 …… 34
3.2.5 缓存溢出 …… 35
3.2.6 拒绝服务 …… 37
3.3 学习高级技术 …… 41
3.3.1 嗅闻交换网络 …… 41
3.3.2 IP 哄骗 …… 43
3.4 识别恶意代码 …… 46
3.4.1 病毒 …… 46
3.4.2 特洛伊木马病毒 …… 47
3.4.3 蠕虫病毒 …… 47
3.4.4 Slapper 蠕虫示例 …… 47
3.4.5 混合体 …… 48
3.5 识别无目标黑客的方法 …… 49
3.5.1 目标 …… 49

3.5.2　侦察 …… 49
3.5.3　攻击手段 …… 51
3.5.4　利用已受攻击的系统 …… 51
3.6　识别有目标黑客的方法 …… 56
3.6.1　目标 …… 56
3.6.2　侦察 …… 56
3.6.3　攻击方法 …… 59
3.6.4　利用被攻击的系统 …… 60
项目3　完成对你的站点的侦察 …… 61
3.7　思考与练习 …… 62

第4章　信息安全服务 …… 63
4.1　定义机密性 …… 64
4.1.1　文件的机密性 …… 64
4.1.2　传输中信息的机密性 …… 65
4.1.3　通信数据流的机密性 …… 66
4.1.4　可以防止的攻击 …… 67
4.2　定义完整性 …… 67
4.2.1　文件的完整性 …… 67
4.2.2　信息传输的完整性 …… 68
4.2.3　可以预防的攻击 …… 68
4.3　定义可用性 …… 69
4.3.1　备份 …… 69
4.3.2　故障还原 …… 69
4.3.3　灾难还原 …… 70
4.3.4　可以预防的攻击 …… 70
4.4　定义责任性 …… 70
4.4.1　识别和认证 …… 70
4.4.2　审核 …… 72
4.4.3　可以预防的攻击 …… 72
项目4　保护信息 …… 72
4.5　思考与练习 …… 73

第二部分 基础工作

第5章 信息安全的法律问题 …… 77
5.1 美国刑法 …… 78
5.1.1 计算机诈骗与滥用(18 US Code 1030) …… 78
5.1.2 信用卡诈骗(18 US Code 1029) …… 79
5.1.3 版权(18 US Code 2319) …… 79
5.1.4 截听(18 US Code 2511) …… 79
5.1.5 对电子信息的访问(18 US Code 2701) …… 80
5.1.6 其他犯罪条款 …… 80
5.1.7 Patriot 法案 …… 80
5.1.8 国土安全法案 …… 82
5.2 州法律 …… 82
5.3 其他国家的法律 …… 83
5.3.1 澳大利亚 …… 83
5.3.2 巴西 …… 83
5.3.3 印度 …… 84
5.3.4 中华人民共和国 …… 84
5.3.5 英国 …… 84
5.4 起诉 …… 84
5.4.1 收集证据 …… 85
5.4.2 联系执法机关 …… 86
5.5 民事问题 …… 86
5.5.1 员工问题 …… 87
5.5.2 连带责任 …… 87
5.6 隐私问题 …… 88
5.6.1 客户信息 …… 88
5.6.2 HIPAA …… 89
5.6.3 “可选择的”与必要的组成部分 …… 89
5.6.4 安全规则的要求 …… 89
5.6.5 Graham-Leach-Bliley 财务服务现代化法案 …… 91
项目5 起诉违法人员 …… 92
5.7 思考与练习 …… 93

第6章　策略 …… 94
6.1　策略的重要性 …… 95
6.1.1　定义安全性 …… 95
6.1.2　让所有人看到 …… 95
6.2　不同的策略 …… 96
6.2.1　信息策略 …… 96
6.2.2　安全策略 …… 98
6.2.3　计算机使用策略 …… 101
6.2.4　Internet 使用策略 …… 102
6.2.5　邮件策略 …… 102
6.2.6　用户管理过程 …… 103
6.2.7　系统管理过程 …… 104
6.2.8　备份策略 …… 105
6.2.9　应急响应过程 …… 106
6.2.10　配置管理过程 …… 109
6.2.11　设计方法论 …… 109
6.2.12　灾难还原计划 …… 110
6.3　制订正确的策略 …… 112
6.3.1　定义重要策略 …… 112
6.3.2　定义可接受的行为 …… 113
6.3.3　确认利益相关人 …… 113
6.3.4　定义正确的大纲 …… 113
6.3.5　制订策略 …… 113
6.4　部署策略 …… 114
6.4.1　策略被接受 …… 114
6.4.2　教育 …… 114
6.4.3　实现 …… 115
6.5　有效使用策略 …… 115
6.5.1　新的系统和项目 …… 115
6.5.2　现有系统和项目 …… 115
6.5.3　审核 …… 115
6.5.4　策略复查 …… 116
项目6　制订机构内部使用策略 …… 116
6.6　思考与练习 …… 116

第7章 管理风险 …… 118
7.1 风险定义 …… 119
7.1.1 薄弱点 …… 119
7.1.2 威胁 …… 120
7.1.3 威胁 + 薄弱点 = 风险 …… 123
7.2 确认机构的风险 …… 124
7.2.1 确认薄弱点 …… 125
7.2.2 确认真正威胁 …… 125
7.2.3 检查防范措施 …… 126
7.2.4 确认风险 …… 126
7.3 评估风险 …… 127
7.3.1 金钱 …… 127
7.3.2 时间 …… 128
7.3.3 资源 …… 129
7.3.4 形象 …… 129
7.3.5 业务损失 …… 129
7.3.6 评估风险的方法 …… 130
项目7 确认机构的电子风险 …… 131
7.4 思考与练习 …… 131

第8章 信息安全过程 …… 133
8.1 评估 …… 134
8.1.1 网络 …… 136
8.1.2 物理安全 …… 137
8.1.3 策略和过程 …… 138
8.1.4 预防措施 …… 139
8.1.5 安全意识 …… 140
8.1.6 人员 …… 140
8.1.7 工作量 …… 141
8.1.8 态度 …… 141
8.1.9 遵守情况 …… 141
8.1.10 业务 …… 142
8.1.11 评估结果 …… 142
8.2 制订策略 …… 142
8.2.1 选择制订策略的顺序 …… 143

8.2.2　升级现有的策略 …… 144
8.3　实现安全 …… 144
8.3.1　安全报告系统 …… 145
8.3.2　身份验证系统 …… 145
8.3.3　Internet 安全 …… 146
8.3.4　入侵检测系统 …… 146
8.3.5　加密 …… 147
8.3.6　物理安全 …… 148
8.3.7　工作人员 …… 148
8.4　安全意识培训 …… 148
8.4.1　员工 …… 149
8.4.2　管理员 …… 149
8.4.3　开发人员 …… 149
8.4.4　主管人员 …… 149
8.4.5　安全人员 …… 150
8.5　审核 …… 150
8.5.1　策略遵守情况的审核 …… 150
8.5.2　定期的项目评估和新的项目评估 …… 150
8.5.3　入侵测试 …… 151
项目 8　部署安全意识程序 …… 151
8.6　思考与练习 …… 152

第 9 章　信息安全最佳实践 …… 153
9.1　管理性安全 …… 154
9.1.1　策略和过程 …… 154
9.1.2　资源 …… 155
9.1.3　责任 …… 156
9.1.4　教育 …… 157
9.1.5　突发事故计划 …… 159
9.1.6　安全项目计划 …… 160
9.2　技术性安全 …… 162
9.2.1　网络连接性 …… 162
9.2.2　恶意代码的防护 …… 163
9.2.3　验证机制 …… 164
9.2.4　监控 …… 165

9.2.5 加密 …… 166
9.2.6 补丁系统 …… 166
9.2.7 备份和还原 …… 167
9.2.8 物理安全 …… 167
9.3 ISO 17799 应用 …… 169
9.3.1 此标准中的关键概念 …… 169
9.3.2 如何使用此标准 …… 170
项目9 缺口分析 …… 170
9.4 思考与练习 …… 171

第三部分 安全技术

第 10 章 防火墙 …… 175
10.1 防火墙的类型 …… 176
10.1.1 应用层防火墙 …… 176
10.1.2 数据包过滤防火墙 …… 177
10.1.3 混合型 …… 179
10.2 防火墙的配置 …… 180
10.2.1 体系结构 1：防火墙之外 Internet 可以访问的系统 …… 180
10.2.2 体系结构 2：单一防火墙 …… 181
10.2.3 体系结构 3：双重防火墙 …… 182
10.3 设计防火墙规则集 …… 184
项目 10 学习各种防火墙之间的区别 …… 184
10.4 思考与练习 …… 185

第 11 章 虚拟专用网络 …… 186
11.1 虚拟专用网络 …… 187
11.2 部署用户 VPN …… 188
11.2.1 用户 VPN 的优点 …… 189
11.2.2 用户 VPN 的问题 …… 190
11.2.3 管理用户 VPN …… 191
11.3 部署站点 VPN …… 192
11.3.1 站点 VPN 的优点 …… 192
11.3.2 站点 VPN 的问题 …… 193
11.3.3 管理站点 VPN …… 194

11.4 标准 VPN 技术 …… 194
11.4.1 VPN 服务器 …… 195
11.4.2 加密算法 …… 197
11.4.3 认证系统 …… 197
11.4.4 VPN 协议 …… 198
11.5 VPN 系统的类型 …… 199
11.5.1 硬件系统 …… 199
11.5.2 软件系统 …… 200
11.5.3 基于 Web 的系统 …… 200
项目 11 研究不同 VPN 的区别 …… 200
11.6 思考与练习 …… 201

第 12 章 加密 …… 202
12.1 加密的基本概念 …… 203
12.1.1 加密的术语 …… 203
12.1.2 针对加密系统的攻击 …… 204
12.2 私钥加密 …… 205
12.2.1 私钥加密 …… 205
12.2.2 替换密文 …… 206
12.2.3 一次性便条 …… 206
12.2.4 数据加密标准 …… 207
12.2.5 三重 DES …… 209
12.2.6 密码加密 …… 210
12.2.7 高级加密标准：Rijndael …… 211
12.2.8 其他私钥算法 …… 211
12.3 公钥加密 …… 212
12.3.1 公钥加密 …… 213
12.3.2 Diffie-Hellman 密钥交换 …… 213
12.3.3 RSA …… 214
12.3.4 其他的公钥算法 …… 216
12.4 数字签名 …… 217
12.4.1 数字签名概述 …… 217
12.4.2 安全的哈希函数 …… 218
12.5 密钥管理 …… 219
12.5.1 创建密钥 …… 219

12.5.2 密钥发布 …… 220
12.5.3 密钥证书 …… 221
12.5.4 密钥保护 …… 222
12.5.5 密钥注销 …… 222
12.6 系统中的信任问题 …… 223
12.6.1 分层模型 …… 223
12.6.2 Web 模型 …… 225
项目 12 设计加密系统 …… 226
12.7 思考与练习 …… 227

第 13 章 入侵检测 …… 229
13.1 入侵检测系统(IDS)的类型 …… 231
13.1.1 基于主机的 IDS …… 231
13.1.2 基于网络的 IDS …… 234
13.1.3 是否某种 IDS 更优 …… 235
13.2 安装 IDS …… 236
13.2.1 定义 IDS 的目标 …… 236
13.2.2 选择监视内容 …… 238
13.2.3 选择响应方式 …… 240
13.2.4 设置临界值 …… 243
13.2.5 实现系统 …… 244
13.3 管理 IDS …… 245
13.3.1 理解 IDS 可以提供的信息 …… 245
13.3.2 调查可疑事件 …… 248
13.4 理解入侵预防措施 …… 251
13.4.1 如何使用 IDS 预防入侵活动 …… 251
13.4.2 入侵预防问题 …… 251
项目 13 部署网络 IDS …… 253
13.5 思考与练习 …… 254

第四部分 实际应用与特定平台的实现

第 14 章 Unix 的安全问题 …… 257
14.1 安装系统 …… 258
14.1.1 启动文件 …… 258

14.1.2　允许的服务 …… 259
14.1.3　系统配置文件 …… 261
14.1.4　补丁程序 …… 266
14.2　用户管理 …… 267
14.2.1　向系统中添加用户 …… 267
14.2.2　从系统中删除用户 …… 269
14.3　系统管理 …… 269
14.3.1　审核系统 …… 269
14.3.2　日志文件 …… 270
14.3.3　隐藏文件 …… 271
14.3.4　SUID 和 SGID 文件 …… 271
14.3.5　所有人都可以写的文件 …… 271
14.3.6　查找可疑迹象 …… 272
项目 14　审核 Unix 系统 …… 275
14.4　思考与练习 …… 276

第 15 章　Windows 2000/Windows 2003 Server 的安全问题 …… 278
15.1　安装系统 …… 279
15.1.1　本地安全策略设置 …… 279
15.1.2　系统配置 …… 283
15.1.3　Windows 2003 中的特殊配置问题 …… 288
15.2　用户管理 …… 291
15.2.1　向系统中添加用户 …… 291
15.2.2　设置文件权限 …… 292
15.2.3　从系统中删除用户 …… 293
15.3　系统管理 …… 294
15.3.1　secedit 命令 …… 294
15.3.2　审核系统 …… 296
15.3.3　日志文件 …… 297
15.3.4　查找可疑迹象 …… 298
15.4　使用活动目录 …… 300
15.4.1　安全设置和安装 …… 300
15.4.2　管理 …… 301
15.4.3　组策略和安全 …… 301
15.4.4　AD 用户和组管理 …… 307

项目 15 使用 secedit 管理 Windows 2000 安全配置 …… 308
15.5 思考与练习 …… 309

第 16 章 Internet 体系结构 …… 310
16.1 提供的服务 …… 311
16.1.1 邮件 …… 311
16.1.2 加密的电子邮件 …… 311
16.1.3 Web …… 312
16.1.4 对 Internet 的内部访问 …… 312
16.1.5 从外部访问内部系统 …… 313
16.1.6 控制服务 …… 313
16.2 不应该提供的服务 …… 314
16.3 开发通信体系结构 …… 315
16.3.1 单线访问 …… 315
16.3.2 对单个 ISP 的多线访问 …… 317
16.3.3 对多个 ISP 的多线访问 …… 319
16.4 设计非军事区 …… 322
16.4.1 定义 DMZ …… 322
16.4.2 应该放入 DMZ 中的系统 …… 323
16.4.3 合适的 DMZ 体系结构 …… 325
16.5 理解网络地址转换 …… 328
16.5.1 网络地址转换 …… 328
16.5.2 专用类地址 …… 329
16.5.3 静态 NAT …… 329
16.5.4 动态 NAT …… 330
16.6 伙伴网络 …… 331
16.6.1 使用伙伴网络 …… 331
16.6.2 安装 …… 332
16.6.3 寻址问题 …… 333
项目 16 创建 Internet 体系结构 …… 334
16.7 思考与练习 …… 334

第 17 章 电子商务安全要求 …… 336
17.1 理解电子商务服务 …… 337
17.1.1 电子商务服务与常规 DMZ 服务的区别 …… 338