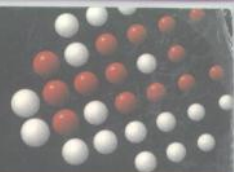


网络安全技术系列丛书



Internet Security Professional Reference, Second Edition



Internet

网络安全

专业参考手册

(美) Derek Atkins 等著

严伟 刘晓丹 王千祥 等译



机械工业出版社

西蒙与舒斯特
国际出版公司



New
Riders

CMP

55183 / 1.5
本书是一本非常有用的网络安全手册，几乎涵盖了 Internet 网络安全的所有方面，包括从特定的技术到特定的策略；以及保护 Internet 连接安全性的企业决策。

全书共分五大部分：管理 Internet 安全、访问并且保护网关、消息机制——创建安全的通道、当前关注的问题及附录。

本书适合计算机网络安全管理人员、大专院校师生及广大网络用户阅读。

Derek Atkins, et al.: Internet Security Professional Reference, Second Edition.

Authorized translation from the English language edition published by New Riders Publishing.

Copyright 1997 by New Riders 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和美国西蒙与舒斯特国际出版公司合作出版，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。

本书封面贴有 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：01-98-1440

图书在版编目 (CIP) 数据

Internet 网络安全专业参考手册 / (美) 艾肯 (Atkins, D.); 严伟等译. - 北京: 机械工业出版社, 1998

(网络安全技术系列丛书)

书名原文: Internet Security Professional Reference, Second Edition

ISBN 7-111-06358-9

I. I... II. ①艾...②严... III. 因特网-安全技术-手册 IV. TP309-62

中国版本图书馆 CIP 数据核字 (98) 第 17579 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: 傅豫波 李云静

北京忠信诚胶印厂印刷·新华书店北京发行所发行

1998 年 8 月第 1 版第 1 次印刷

787mm×1092mm¹/₁₆·40.25 印张

印数: 0 001-8 000 册

定价: 85.00 元 (附光盘)

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

序

你将会发现这本《Internet 网络安全专业参考手册》是一个非常有价值的工具，它能够防止你的 Internet 连接被网络黑客、网络窃贼或其他不幸事件所危害。这本书的适用范围极广，它包括了个人、小型企业、大型企业防止安全性漏洞需要的所有信息。如果你是一位网络安全方面的专家，或者从事咨询、管理及提供 Internet 和网络方面的服务，你会需要这本书，而且会发现它对你非常有帮助。

本书几乎涵盖了 Internet 安全的所有方面，从特定的技术到特定的策略，以及关于保护 Internet 连接安全性的企业决策。作者洞察网络黑客（hacker）所思所想，以子之矛攻子之盾。如果你需要一个安全的 Internet 网络连接，那么这本书再合适不过了。

本书是如何组织的？

本书分为五个部分。

第一部分，管理 Internet 安全，包括在你规划和实现网络连接时需要着重理解的一些主题。第一部分通过 TCP/IP、UUCP、守护程序（daemon）和 audit trails 等章节，使你完全能够处理有关安全策略的问题。

第二部分，访问并且保护网关，这可能是最重要的一步了。如果你的网关不安全，那么其他什么就都不会安全。这一部分要论述电子欺骗（spoofing）、网络窥探（sniffing）和一直都很重要的防火墙，这部分还包括 SATAN 和 Kerberos，因此阅读了第二部分的这些章节之后，你就会清楚有关安全网关的所有问题。

第三部分，消息机制：创建安全的通道，这是问题的核心。如果网络黑客设法通过了你的安全基础设施，你仍然可以保护消息本身。通过详细介绍加密技术和 PGP，你就完全清楚如何充分利用加密方法。

第四部分，当前关注的问题。以深入讨论现代技术如何影响网络安全以及如何实现最佳安全性作为结尾。这部分主要包括 Java 安全性、Windows NT 安全性、CGI 安全性和病毒。

第五部分，附录，包括附录 A 和附录 B。当你查找安全性信息、资源和参考时将会发现这部分非常有用。

New Riders Publishing

New Riders Publishing 的全体员工竭诚为您提供最佳的计算机参考资料。New Riders 出版的每一本书都是作者与工作人员对书中信息经过几个月深入研究和精心筛选的结果。

作为这个承诺的一部分，New Riders 欢迎你的参与。无论是你对这本书爱不释手、对其中提供的信息和例子感到困惑不解，还是对下一个版本有一些忠告，都希望能让我们知道你的意见和建议。

但是请注意：New Riders 的工作人员不能提供有关 Internet 网络安全或软硬件问题方面的技术支持。这方面的问题请参考你的软件附带的文档或者应用程序的帮助系统。

如果你对 New Riders 出版的书籍有疑问或者意见的话，你有多种途径可以与 New Riders Publishing 联络。我们将为尽可能多的读者提供答复。

联系地址如下：

New Riders Publishing

Attn: Publisher

201 W, 103rd Street

Indianapolis, IN 46290

如果你愿意的话，可以按下面这个号码给我们发传真：

317-817-7448

你也可以按照下面的电子邮件地址给我们发电子邮件：

jbelbot @ newriders.mcp.com

New Riders Publishing 是 Macmillan Computer Publishing 的标记，要获得本公司的分类目录或信息；或者要购买本公司的书籍，请拨电话 800-428-5331 或者访问我们的 Web 站点：<http://www.mcp.com>。

感谢你选择了《Internet 网络安全专业参考手册》！

目 录

序

第一部分 管理 Internet 安全

第 1 章 理解 TCP / IP	1
1.1 TCP / IP 的历史	1
1.2 探究地址、子网和主机名	2
1.2.1 地址分类	2
1.2.2 子网	3
1.2.3 主机名	6
1.3 使用网络接口	7
1.4 网络配置文件回顾	9
1.4.1 /etc/hosts 文件	9
1.4.2 /etc/ethers 文件	10
1.4.3 /etc/networks 文件	10
1.4.4 /etc/protocols 文件	11
1.4.5 /etc/services 文件	11
1.4.6 /etc/inetd.conf 文件	12
1.5 理解网络访问文件	12
1.5.1 /etc/hosts.equiv 文件	12
1.5.2 .rhosts 文件	13
1.5.3 用户和主机的等价性	13
1.6 TCP/IP 守护程序	14
1.6.1 slink 守护程序	14
1.6.2 ldsocket 守护程序	15
1.6.3 cpd 守护程序	15
1.6.4 行式打印机守护程序 (lpd)	15
1.6.5 SNMP 守护程序 (snmpd)	15
1.6.6 RARP 守护程序 (rarpd)	15
1.6.7 BOOTP 守护程序 (bootpd)	15
1.6.8 ROUTE 守护程序 (routed)	16
1.6.9 域名服务守护程序 (named)	16
1.6.10 系统记录守护程序 (syslogd)	17
1.6.11 超级服务器 Inetd	17
1.6.12 RWHO 守护程序 (rwhod)	17
1.7 使用 TCP/IP 实用工具	17
1.7.1 网络管理命令	17
1.7.2 用户命令	28

第 2 章 理解、创建守护程序	36
2.1 什么是守护程序	36
2.2 系统守护程序	40
2.2.1 init 守护程序	40
2.2.2 swapper 守护程序	40
2.2.3 update 和 bdf flush 守护程序	40
2.2.4 lpd 守护程序	40
2.2.5 lpsched 守护程序	41
2.2.6 cpd 和 sco-cpd (sco) 守护 程序	41
2.2.7 cron 守护程序	41
2.2.8 syslog 守护程序	41
2.2.9 sendmail 守护程序	42
2.2.10 getty 守护程序	43
2.2.11 rlogind 守护程序	43
2.2.12 deliver 守护程序	43
2.2.13 inetd 守护程序	44
2.2.14 roudt 守护程序	44
2.2.15 nfsd 守护程序	44
2.2.16 mountd 守护程序	44
2.2.17 pcnfsd 守护程序	44
2.2.18 statd 和 rpc.statd 守护程序	44
2.2.19 lockd 和 rpc.lockd 守护程序	45
2.3 用 Bourne Shell 创建守护程序	45
2.3.1 处理入境和输出	45
2.3.2 处理消息	46
2.3.3 处理信号	46
2.3.4 dfmon 程序	47
2.4 用 PERL 创建守护程序	48
2.4.1 处理入境和输出	49
2.4.2 处理信号	49
2.4.3 procmon 程序	50
2.5 Unix 运行级别	53
2.6 程序清单	55
2.6.1 程序清单 2.1 —— dfmon 程序	55
2.6.2 程序清单 2.2 —— dfmon 的 配置文件	59

2.6.3 程序清单 2.3 —— procmon 命令	64	4.2.1 使用事件查看器	127
2.6.4 程序清单 2.4 —— procmon.cfg 文件	77	4.2.2 记录 ftp 服务器的服务	128
第 3 章 使用 UUCP	78	4.2.3 记录 httpd 事务	129
3.1 UUCP 的历史	78	4.2.4 用 Windows NT 的其他 TCP/IP 应用程序记录	129
3.2 UUCP 网络	80	4.3 DOS 下的审计跟踪	129
3.3 为主机命名	81	4.3.1 PC/DACS	130
3.4 系统 V 基本网络实用工具 UUCP	82	4.3.2 Watchdog	130
3.4.1 UUCP 文件布局	82	4.3.3 LOCK	130
3.4.2 配置 UUCP	83	4.4 使用 System Log 发现入侵者	130
3.4.3 测试连接	85	4.4.1 一般入侵提示	130
3.4.4 Dialers 文件	86	4.4.2 潜在的问题	131
3.4.5 系统文件	87		
3.5 UUCP 交谈脚本	89	第二部分 访问并且保护网关	
3.5.1 使用 uucico 测试连接	92	第 5 章 IP 欺骗与窥探	133
3.5.2 权限文件	95	5.1 窥探	133
3.5.3 允许匿名 UUCP 访问	99	5.1.1 窥探：如何实施	134
3.5.4 UUCP 日志文件	100	5.1.2 窥探：如何威胁安全	135
3.5.5 维护	102	5.1.3 协议窥探：一个案例学习 (case study)	136
3.6 配置版本 2UUCP	103	5.1.4 窥探：如何预防	139
3.6.1 版本 2UUCP 是什么	103	5.1.5 硬件障碍	140
3.6.2 文件布局	103	5.1.6 避免传输口令	146
3.6.3 配置 UUCP	104	5.2 欺骗	149
3.6.4 L-devices 文件	104	5.2.1 硬件地址欺骗	149
3.6.5 测试连接	104	5.2.2 ARP 欺骗	151
3.6.6 L.sys 文件	105	5.2.3 防止 ARP 欺骗	153
3.6.7 用 uucico 测试连接	107	5.2.4 窥探案例学习再讨论	155
3.6.8 版本 2 权限	107	5.2.5 检测 ARP 欺骗	156
3.6.9 日志文件	110	5.2.6 欺骗 IP 路由系统	159
3.6.10 维护	111	5.2.7 基于 ICMP 的路由欺骗	160
3.7 在 TCP/IP 之上配置 UUCP	111	5.2.8 误导 IP 数据报	162
3.8 代码清单	112	5.2.9 防止路由欺骗	163
3.8.1 代码清单 3.1 —— gtimes.c	112	5.2.10 案例学习：涉及外部路由	165
3.8.2 代码清单 3.2 —— genUSER	114	5.2.11 欺骗域名系统的名字	165
第 4 章 审计跟踪	115	5.2.12 欺骗 TCP 连接	171
4.1 Unix 系统的审计跟踪	115	第 6 章 如何构造防火墙	177
4.1.1 一般的 Unix 日志	115	6.1 TIS 防火墙工具箱	177
4.1.2 进程记帐	121	6.1.1 理解 TIS 防火墙工具箱	177
4.1.3 审计中有用的工具	123	6.1.2 如何获得 TIS 防火墙工具箱	178
4.1.4 其他可以联机使用的报告 工具	125	6.1.3 在 SunOS4.1.3 及 4.1.4 下 编译	178
4.2 Windows NT 的审计跟踪	126		

6.1.4 在 BSDI 下编译	178	6.14 管理工具	224
6.1.5 安装 TIS 防火墙工具箱	179	6.14.1 portscan	224
6.2 准备配置	181	6.14.2 netscan	225
6.3 配置 TCP/IP	185	6.14.3 报告工具	226
6.4 netperm 表	186	6.15 何处寻求帮助	234
6.5 配置 netacl	187	6.16 netperm-table 文件示例	235
6.5.1 与 netacl 连接	188	6.17 参考手册	239
6.5.2 重新启动 inetd	190	6.17.1 Authmgr——网络认证客户 程序	239
6.6 配置 Telnet 代理	190	6.17.2 authsrv——第三方网络认证守 护程序	239
6.6.1 通过 Telnet 代理建立连接	192	6.17.3 ftp-gw——FTP 代理服务器	245
6.6.2 主机访问规则	193	6.17.4 http-gw——Gopher/HTTP 代理	249
6.6.3 检测 Telnet 代理	194	6.17.5 login-sh——认证登录 shell	254
6.7 配置 rlogin 网关	194	6.17.6 netacl——TCP 网络访问 控制	255
6.7.1 经 rlogin 网关建立连接	196	6.17.7 plug-gw——通用 TCP 插接板 (plug-board) 代理	256
6.7.2 主机访问规则	197	6.17.8 rlogin-gw——rlogin 代理 服务器	258
6.7.3 检测 rlogin 代理	197	6.17.9 smap——sendmail 包装 (wrapper) 客户	260
6.8 配置 FTP 网关	197	6.17.10 smapd——sendmail 包装守 护程序	261
6.8.1 主机访问规则	199	6.17.11 tn-gw——telnet 代理服务 器	263
6.8.2 检测 FTP 代理	199	6.17.12 x-gw——X 网关服务器	265
6.8.3 通过 FTP 代理建立连接	200	第 7 章 如何购买防火墙	267
6.8.4 允许 FTP	201	7.1 防火墙回顾	267
6.9 配置 sendmail 代理: smap 和 smapd	201	7.1.1 体系结构	267
6.9.1 安装 smap 客户程序	202	7.1.2 应了解的三个术语	268
6.9.2 配置 smap 客户	202	7.2 选择防火墙	269
6.9.3 安装 smapd 应用程序	204	7.3 防火墙体系结构	269
6.9.4 配置 smapd 应用程序	204	7.3.1 路由器体系	269
6.9.5 为 smap 配置 DNS	205	7.3.2 先进防火墙体系	271
6.10 配置 HTTP 代理	206	7.4 评估防火墙	272
6.10.1 非代理意识 HTTP 客户	207	7.4.1 选择状态包过滤器或传输防 火墙	273
6.10.2 使用代理意识 HTTP 客户	208	7.4.2 评估通过防火墙的路径	274
6.10.3 主机访问规则	208	7.4.3 评估管理接口和 GUI	275
6.11 配置 X 窗口代理	210	7.4.4 评估灵活性和特征	277
6.12 理解认证服务器	211	7.4.5 评估报告和记帐	278
6.12.1 认证数据库	212		
6.12.2 添加用户	214		
6.12.3 认证 Shell——authmgr	216		
6.12.4 数据库管理	217		
6.12.5 认证如何工作	219		
6.13 其他服务使用 plug-gw	220		
6.13.1 配置 plug-gw	220		
6.13.2 plug-gw 与 NNTP	221		
6.13.3 plug-gw 与 POP	223		

7.5 评估防火墙性能	279	8.8.1 获取 SATAN	338
7.5.1 包过滤性能问题	280	8.8.2 检查 SATAN 文件	339
7.5.2 传输代理性能问题	281	8.9 构造 SATAN	347
7.5.3 性能测试规则	282	8.9.1 使用 SATAN HTML 界面	348
7.6 评估防火墙的安全	283	8.9.2 运行一个扫描	353
7.7 总结	286	8.9.3 理解 SATAN 数据库记录格式	354
第 8 章 SATAN 与 Internet	287	8.9.4 理解 SATAN 规则集	357
8.1 网络攻击的本质	288	8.9.5 扩展 SATAN	359
8.1.1 Internet 威胁层 (ITL)	289	8.9.6 使用 SATAN 的长期利益	360
8.1.2 普通攻击方法	291	8.10 参考文献	361
8.1.3 安全漏洞概述	293	第 9 章 Kerberos	362
8.1.4 学习新的安全漏洞	297	9.1 Kerberos 如何工作	362
8.2 像入侵者那样思考	297	9.2 Kerberos 网络	363
8.2.1 收集系统信息	298	9.2.1 RFC	363
8.2.2 掌握代码	314	9.2.2 Kerberos 的目标	364
8.2.3 尝试所有已知问题	315	9.3 认证如何工作	364
8.2.4 漏洞与机会匹配	315	9.4 加密	367
8.2.5 查找弱连接	315	9.4.1 私有、公开、秘密或共享密 钥加密	368
8.2.6 总结远程网络攻击	316	9.4.2 私人或私密密钥加密	368
8.2.7 自动搜索	316	9.4.3 DES 及其变体	369
8.3 初次遭遇 SATAN	316	9.4.4 加密出口问题	370
8.3.1 历史	316	9.4.5 加密和校验和规范	371
8.3.2 创造者	317	9.5 Kerberos 版本	375
8.3.3 与其他工具的比较	317	9.5.1 不同的 Kerberos 版本 4	376
8.3.4 厂商反应	317	9.5.2 不同的 Kerberos 版本 5	376
8.3.5 长期影响	318	9.5.3 Bones	377
8.4 检测 SATAN	318	9.6 选择销售商	377
8.4.1 Courtney	318	9.7 销售商的互操作性问题	377
8.4.2 Gabriel	318	9.7.1 DEC ULTRIX Kerberos	377
8.4.3 TCP Wrappers	318	9.7.2 Transarc 的 Kerberos	378
8.4.4 netlog/ TAMU	319	9.7.3 DCE	378
8.4.5 Argus	319	9.7.4 互操作性要求	379
8.5 使用安全的网络程序	319	9.8 命名约束 (naming constraints)	380
8.5.1 Kerberos	319	9.8.1 区域名	380
8.5.2 安全 Shell (ssh)	320	9.8.2 主体名字	381
8.6 SSL	320	9.9 跨区域 (Cross-Realm) 操作	382
8.7 研究 SATAN 做什么	322	9.10 ticket 标志	383
8.7.1 SATAN 的信息收集	322	9.10.1 初始及预认证 ticket	384
8.7.2 搜索的脆弱点	323	9.10.2 无效 ticket	384
8.7.3 其他网络脆弱点	331	9.10.3 可更新的 ticket	384
8.7.4 探讨 IP 欺骗	334	9.10.4 过期 ticket	385
8.7.5 检验结构型 Internet 问题	336	9.10.5 可代理的及代理 ticket	385
8.8 SATAN 集结	338		

9.10.6 可转发的 ticket	386	10.3.6 安全通道	428
9.10.7 认证标志	386	10.3.7 安全 Internet 隧道	429
9.10.8 其他密钥分配中心选项	386	10.3.8 电子商务	429
9.11 消息交换	387	10.4 对称(私钥)密码技术	430
9.11.1 ticket 与认证符	387	10.4.1 转置	431
9.11.2 认证服务交换	389	10.4.2 解密	432
9.11.3 Ticket Granting Service (TGS) 交换	392	10.4.3 置换	433
9.11.4 认证服务器与 Ticket Granting Service 交换规范	396	10.4.4 块密码和流密码	442
9.11.5 客户/服务器认证交换	401	10.4.5 DES(数据加密标准)	442
9.11.6 客户/服务器(CS)消息 规范	403	10.4.6 DES 的其他替代选择	444
9.11.7 KRB_SAFE 交换	405	10.4.7 Blowfish	445
9.11.8 KRB_SAFE 消息规范	406	10.5 非对称(公钥)密码技术	446
9.11.9 KRB_PRIV 交换	407	10.6 攻击和密码学分析	446
9.11.10 KRB_PRIV 消息规范	407	10.7 有关密码技术的地址	448
9.11.11 KRB_CRED 交换	408	10.8 小结	449
9.11.12 KRB_CRED 消息规范	409	第 11 章 PGP 程序	450
9.11.13 名字	410	11.1 PGP 概述	450
9.11.14 时间	411	11.1.1 PGP 的历史	450
9.11.15 主机地址	411	11.1.2 为什么要使用 PGP	451
9.11.16 授权数据	411	11.1.3 加密简短回顾	452
9.11.17 最后请求数据	411	11.2 PGP 的使用	452
9.11.18 错误消息规范	412	11.2.1 在使用 PGP 之前	452
9.12 Kerberos 工作站认证问题	413	11.2.2 产生一个 PGP 密钥	454
9.12.1 Kerberos 的端口号	414	11.2.3 公钥的发布	455
9.12.2 Kerberos 的 Telnet	414	11.2.4 为一个消息签名	456
9.12.3 Kerberos ftpd	414	11.2.5 添加其他人的密钥	457
9.13 其他信息源	415	11.2.6 加密一个消息	458
		11.2.7 解密和验证消息	459
		11.3 PGP 密钥	460
		11.3.1 名字中是什么	460
		11.3.2 PGP 密钥环	461
		11.3.3 Web 的受托性	462
		11.3.4 信任程度	463
		11.4 密钥管理	464
		11.4.1 密钥产生	464
		11.4.2 向公钥环中添加密钥	467
		11.4.3 从公钥环中提取密钥	469
		11.4.4 为密钥签名	470
		11.4.5 查看密钥环的内容	473
		11.4.6 删除密钥和签名	474
		11.4.7 密钥指纹和验证密钥	475
		11.4.8 取消你的密钥	476
		11.5 基本消息操作	477

第三部分 消息机制：创建安全的通道

第 10 章 加密概述	417
10.1 加密技术概述	417
10.2 密码术语	420
10.3 密码技术的应用	421
10.3.1 黑客和窃贼的威胁	421
10.3.2 密码技术的目标	422
10.3.3 数字 ID, 证明和证明机构 (certificate authority)	423
10.3.4 数字签名	425
10.3.5 网络登录和认证的安全性	427

11.5.1 PGP 是程序还是过滤器	478	名字转换	508
11.5.2 压缩消息	478	12.4.3 在 Intranet 中使用 WINS 服务器	508
11.5.3 处理文本和二进制文件	478	12.5 连接到 Internet 上的考虑	509
11.5.4 通过电子邮件发送 PGP 消息 ..	479	12.5.1 使用 IIS 的公共 Web 服务器 连接	510
11.5.5 常规加密	479	12.5.2 代理服务器连接	511
11.5.6 为一个消息签名	480	12.5.3 在 Windows NT 中配置服务	512
11.5.7 用公钥加密消息	481	12.5.4 在 Windows NT 中配置端口	513
11.5.8 为一个消息签名和加密	482	12.6 Microsoft Internet Information Server	513
11.5.9 消息的解密和验证	483	12.7 Microsoft 代理服务器	517
11.6 高级消息操作	485	12.8 新的 Windows NT 目录服务模型	518
11.6.1 净签	485	12.9 总结	521
11.6.2 分离签名	486	第 13 章 Java 的安全性	522
11.6.3 For Her Eyes Only	487	13.1 Java 的功能	523
11.6.4 清除文件	487	13.1.1 Java 是可移植的	524
11.7 PGP 配置文件	488	13.1.2 Java 是健壮的	524
11.8 PGP 的安全性	491	13.1.3 Java 是安全的	524
11.8.1 蛮力攻击	492	13.1.4 Java 是面向对象的	525
11.8.2 私钥和通过短语	492	13.1.5 Java 是高性能的	525
11.8.3 对公钥环的攻击	493	13.1.6 Java 是容易使用的	526
11.8.4 程序的安全性	493	13.2 Java 语言的历史	526
11.8.5 对 PGP 的其他攻击	494	13.3 Java 环境的主要功能特性	528
11.9 PGP 的扩充	494	13.3.1 Java 语言的特性	529
11.9.1 PGP 公钥服务器	494	13.3.2 Java 体系结构	531
11.9.2 PGPMenu: PGP for Unix 的 菜单界面	495	13.4 从类文件到执行	535
11.9.3 Windows 前端	495	13.4.1 代码的编译	535
11.9.4 Unix 邮件程序	496	13.4.2 运行代码	537
11.9.5 Mac PGP	496	13.5 Java 虚拟机	539
		13.5.1 要建立一个新的机器代码 规范	540
		13.5.2 Java 虚拟机描述	540
		13.6 设置 Java 安全性功能	543
		13.6.1 使用 Appletviewer	543
		13.6.2 Netscape 3.0	545
		13.6.3 使用 Java 程序的其他方面 问题	546
		第 14 章 CGI 安全性	548
		14.1 CGI 接口介绍	548
		14.1.1 为什么 CGI 是危险的	549
		14.1.2 CGI 如何工作	549
		14.1.3 CGI 数据: 编码和解码	550

第四部分 当前关注的问题

第 12 章 Windows NT 的 Internet

安全	497
12.1 Windows NT 概述	497
12.2 Windows NT 操作环境	500
12.2.1 域	501
12.2.2 用户帐户、组、权利和权限 ..	503
12.3 Windows NT 的登录和认证	505
12.4 Windows NT 中与 Intranet 有关 的特性	508
12.4.1 在 Intranet 中使用 DNS 服务器	508
12.4.2 在 Intranet 中使用 NetBIOS	

14.1.4 CGI 库	550	15.4.7 文件感染病毒的潜在破坏	595
14.2 理解 CGI 的脆弱性	551	15.4.8 宏病毒	597
14.2.1 HTTP 服务器	551	15.4.9 蠕虫	599
14.2.2 HTTP 协议	551	15.5 网络和 Internet 对病毒的敏感性	599
14.2.3 环境变量	552	15.5.1 网络对文件病毒的敏感性	600
14.2.4 GET 和 POST 输入数据	552	15.5.2 引导病毒	601
14.3 尽量减小 CGI 的脆弱性	553	15.5.3 宏病毒	601
14.3.1 限制对 CGI 的访问	553	15.6 病毒类型	602
14.3.2 用最小的特权运行 CGI	554	15.6.1 多态病毒	602
14.3.3 在一个改变根文件系统的环境 中运行	554	15.6.2 Stealth 病毒	603
14.3.4 保护 HTTP 服务器所在的 机器	555	15.6.3 Slow 病毒	606
14.4 CGIWRAP: 另一种模型	555	15.6.4 Retro 病毒	607
14.5 越过 CGI	555	15.6.5 多头病毒 (Multipartite Viruses)	607
14.6 服务器方包含 (SSI)	556	15.7 反病毒程序如何工作	607
14.6.1 限制对 SSI 的访问	556	15.7.1 病毒扫描程序	608
14.6.2 SSI 的替代	556	15.7.2 内存扫描程序	612
14.7 语言问题	557	15.7.3 完整性检查器	613
14.7.1 PERL	557	15.7.4 行为阻止者	615
14.7.2 C 和 C++	559	15.7.5 启发式扫描器	616
14.7.3 安全语言	559	15.8 预防措施和治疗	616
14.8 保护敏感数据	560	15.8.1 防止和修复引导记录病毒	617
14.9 日志记录	561	15.8.2 防止和修复可执行文件病毒	618
第 15 章 病毒	562	15.8.3 修复读取隐藏病毒感染的文 件	619
15.1 用户的角度	562	15.8.4 防止和修复宏病毒	620
15.2 什么是计算机病毒	563	15.9 Windows NT 下病毒行为概况	620
15.3 最可能的目标	564	15.9.1 Windows NT 下的主引导记录 病毒	620
15.3.1 关键硬件	564	15.9.2 Windows NT 下的引导记录 病毒	621
15.3.2 关键软件	565	15.9.3 Windows NT DOS 框内的 DOS 文件病毒	623
15.3.3 软引导记录 (FBR)	566	15.9.4 Windows NT 下的 Windows 3.1 病毒	625
15.3.4 硬盘主引导记录	567	15.9.5 Windows NT 下的宏病毒	625
15.3.5 分区引导记录	568	15.9.6 本机的 Windows NT 病毒	626
15.3.6 系统服务	569	15.10 总结	626
15.3.7 程序文件	570		
15.3.8 带有宏能力的数据文件	572		
15.4 IBM PC 计算机的病毒类型	574		
15.4.1 引导记录病毒	574		
15.4.2 软引导记录病毒	575		
15.4.3 分区引导记录病毒	581		
15.4.4 主引导记录病毒	583		
15.4.5 程序文件病毒	585		
15.4.6 伙伴病毒	595		
		第五部分 附录	
		附录 A 安全性信息来源	627
		附录 B Internet 安全性索引	630

第一部分 管理 Internet 安全

第 1 章 理解 TCP/IP

TCP/IP 是数据通信协议集。这些协议包括从一台机器到另一台机器传递信息的路由、电子邮件和新闻的发送，甚至远程登录功能的使用。

从名字来看，TCP/IP 是指两个主要的协议：传输控制协议（Transmission Control Protocol）和网际互连协议（Internet Protocol）。尽管还有其他一些协议提供操作在 TCP/IP 之上的服务，但这两个协议则是最普遍使用的。

1.1 TCP/IP 的历史

通过 TCP/IP 实现网际互连已经进行了很多年，甚至几乎以 Unix 最初应用就开始了。TCP/IP 或者说传输控制协议/网际互连协议的发展已经超出了国防部高级研究项目机构（Defense Advanced Research Projects Agency, DARPA）的工作。在 1969 年，DARPA 发起了一项称为 ARPANET 的项目。这个网络主要为政府、教育研究性实验室的主要计算机站点提供高带宽的网络互连。ARPANET 为那些用户提供以一个站点传送电子邮件和文件到另一个站点的能力，而 DARPA 则为整个项目提供研究基金。随着项目的发展，人们清楚地意识到可以从中获取广泛的利益和优势，并且有可能提供跨国的网络链接。

1970 年左右，DARPA 继续资助和支持关于 ARPANET 的研究，这时的研究主要集中于点对点租用线路的互连。DARPA 还开始推动各种方式通信连接的研究，例如卫星通信和无线广播通信。就是在这个时候开始形成了公共网络互连技术的框架，由此产生了 TCP/IP。为了使这些协议获得广泛的接受和应用。DARPA 降低费用为用户实现协议。协议的实现主要在加州大学伯克利分校的 BSD Unix 上进行。

DARPA 出资创建 Bolt Beranek and Newman 公司（BBN）来开发 TCP/IP 在 BSD Unix 上的实现。在这个开发项目进行时，许多计算机站点正在采用和开发局域网技术，这时的局域网技术只是基于对以前使用的单个计算机环境的扩展。到了 1983 年 1 月，所有连接到 ARPANET 的计算机都已经运行新的 TCP/IP 协议。除此之外，许多没有连接到 ARPANET 的站点也正在使用 TCP/IP 协议。

因为 ARPANET 一般仅限于一组选择的政府部门、机构使用，所以国家科学基金会创建了 NSFNet。这个网络使用已成功运行于 ARPANET 网络上的协议，并且在某些方面可以说是 ARPANET 网络的扩展，它是连接美国所有超级计算机中心和一些与其互联小型网络的主干网。

由于 NSFNet 所使用的方法，它可以采用各种网络拓扑，而且 TCP/IP 协议并不只限于其中一种网络拓扑。这意味着 TCP/IP 协议可以运行在令牌环、以太网、各种总线结构、点对点租用线路和其他各种拓扑结构之上。然而，TCP/IP 与以太网有着非常紧密的联系，以

致这两个词甚至可以互换使用。

从那时起, TCP/IP 的使用以罕见的速率增长, 到全球性网际网 Internet 的连接数目也以近乎指数的速率增大。无数人开始通过 Internet 牟利, 而且随着当前信息传播的趋势, Internet 将会深入到发达国家中每个人的生活里。

TCP/IP 不是一个单一的协议。事实上, 它是由一组协议组成的, 其中的每个协议提供一些特定的服务。本章的其余部分将探讨 TCP/IP 的地址使用、网络配置、文件控制与其他各种管理命令和守护程序。

注意 守护程序 (daemon) 是完成特定功能的程序。它与许多执行后就退出的命令不同, 守护程序完成它的任务之后还会等待其他任务。例如 sendmail 是一个守护程序, 即使没有邮件处理时, 它仍然处于活动状态。

1.2 探究地址、子网和主机名

Internet 上的每台机器必须有一个唯一的地址, 就像你的邮寄地址一样, 这样发送给每台机器的信息才可以正常传递。这个地址机制由网际互连协议 (IP) 控制。

每台机器有自己的 IP 地址, IP 地址由两部分组成: 网络部分和主机部分。地址的网络部分用于描述主机所在的网络, 主机部分则用于标识特定的主机。为了保证网络地址的唯一性, 由一个中心机构负责分配地址。

因为 Internet 的最初设计人员不知道 Internet 会发展成什么样, 所以他们把地址机制设计得很灵活, 使这种机制既适用于带有许多主机的大型网络, 也适用于仅有几台主机的小型网络。这种寻址机制引入了地址分类, 目前分为 4 类。

IP 地址可以通过几种不同形式表示。第一种是圆点分隔的十进制数表示 (dotted decimal notation), 对每个字节用一个十进制数字表示, 用圆点分隔开, 例如 192.139.234.102。另外, 这个地址也可以用十六进制数表示, 例如 0xC08BEA66。然而最常用的还是圆点十进制数表示法。

1.2.1 地址分类

前面提到过, 地址有 4 种类型: A 类地址、B 类地址、C 类地址和 D 类地址。A 类、B 类和 C 类地址用于标识共用一个公共网络的计算机。D 类地址, 或称多点 (multicast) 地址, 用于标识一组共用一个公共协议的计算机。因为前三类地址的应用非常广泛, 所以本章将集中讨论这三类地址。无论哪种类型的地址, 都是由 32 位, 即 4 个字节组成的, 每个字节通常称为一个 8 位位组 (octet), 因此一个 IP 地址包括 4 个 8 位位组。

每个 8 位位组的数值介于 0 到 255 之间。某些特殊的值有特定的含义, 如本章后面的表 1-1 所示。

1.A 类地址

在 A 类地址中, 第 1 个 8 位位组表示网络部分, 其他 3 个 8 位位组表示主机部分 (见图 1-1)。

这类地址表示这个网络可以连接几百万台主机, 因为可以使用 24 位 (bit) 来标识主机地址。在图 1-1 中, 你会看到第一个 8 位位组的第 1 位设置为 0, 这表示地址的网络部分必

须小于 128。实际上，A 类地址的网络部分范围从 1 到 127。

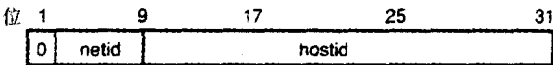


图 1-1 A 类地址的格式

2.B 类地址

B 类地址的结构同 A 类地址很相似，不同之处在于 B 类地址用 2 个 8 位位组表示网络部分，2 个 8 位位组表示主机部分（见图 1-2）。这意味着可以有更多的 B 类网络，每个 B 类网络可以连接几千台主机。

如图 1-2 所示，在 B 类地址的配置中，网络部分和主机部分具有同样数量的地址。网络地址的前 2 位被设置为 1 和 0，表示网络部分的范围从 128 到 191。按照这种格式，每个 B 类地址的网络可以有几千台主机。

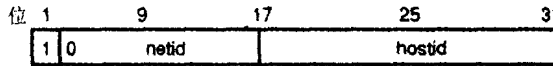


图 1-2 B 类地址的格式

3.C 类地址

C 类地址使用 3 个 8 位位组表示网络部分，使用 1 个 8 位位组表示主机部分。这种安排的结果是可以有更多的 C 类地址的网络，而每一个网络则只能连接少量的主机。因为每个 8 位位组的最大值是 255，而且还要有 2 个保留值，所以每个 C 类地址的网络最多只能连接 253 台主机。这类网络地址的格式如图 1-3 所示。

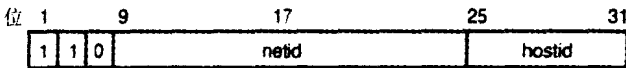


图 1-3 C 类地址的格式

如图 1-3 所示，网络地址的前 2 位均设置为 1。这表明 C 类地址的范围从 192 到 223，其余的值从 224 到 255 用于第 4 类地址。

4. 特殊地址

前面已经提到，有些地址用于特殊目的。这些地址见表 1-1。

表 1-1 保留地址

十进制地址	说 明
0.0.0.0	老式 Sun 网络的所有主机广播地址
num.num.num.0	标识整个网络
num.num.num.255	特定网络的所有主机。(广播地址)
255.255.255.255	对当前网络的所有主机广播

这些保留地址不能用于任何主机或者网络，它们已经被特别保留了下来。你在本章后面将会看到还有一些地址因为其他原因被保留了下来。

1.2.2 子网

网络中的每一台主机都有一个特定的 IP 地址，这样其他主机就可以与它通信。根据网

络类型，一个网络可以连接从 253 台到上百万台主机。然而，如果把 A 类地址或 B 类地址限制于具有千台或百万台主机的一个网络中，则是不现实的。为了解决这个问题，人们开发出子网（subnet）以便把地址的主机部分划分给其他网络。

子网采用网络的主机部分，并通过网络屏蔽（netmask）划分地址空间。网络屏蔽实际上把地址中网络部分和主机部分之间的分隔线从一个地方移动到另一个地方。这样做的作用就是增加可以使用的网络数目，而减少每一个网络可以连接的主机数目。

子网的使用带来很多好处。许多稍小一些的机构只能得到一个 C 类地址，而它们却有许多相互独立的办公室需要连接到一起。如果它们只有一个 IP 地址的话，一台路由器（router）就无法连接两个位置，因为路由器要求每个网络有一个单独的地址。通过把网络划分为子网，就可以使用路由器连接两个网络，因为现在这两个网络具有不同的网络地址。

子网要通过网络屏蔽或者子网络屏蔽来解释。对于处于网络屏蔽范围内的位，地址中对应的位解释为网络位（network bit），对于地址中不在网络屏蔽范围内的位，则作为主机地址部分。要注意的是子网只在一个局部范围内起作用；对于 Internet 的其他部分，这个地址看起来仍然是一个标准的 IP 地址。

如下表所示，每一种 IP 地址类型都有一个与之相关联的缺省网络屏蔽。

表 1-2 标准网络屏蔽

地址类型	缺省网络屏蔽
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

为了清楚地理解这种机制的工作方式，考虑一个例子：假如你有一个网络地址 198.53.64.0，而你想要把它划分成子网，为了进一步划分这个 C 类网络，你必须使用地址主机部分，或者地址中最后一个字节（byte）的一些位作为网络部分。尽管这样会增加可以使用的网络数目，然而却会减少每个子网能够连接的主机数目。

Internet RFC 950 还要求保留每个子网的第 1 个和最后 1 个划分（division）。这表示实际可用的子网络数目比全部划分总和还要少两个。例如，如果你要把一个 C 类网络划分成 2 个部分，你就不能连接任何一台主机。如果你想要有六个子网络，那么你必须把你的网络分隔成 8 个划分。

下面的例子说明如何设置最后 1 个 8 位位组中的位，以及对于每一种情况可以创建多少个子网和主机。地址中代表主机部分的可变部分用字母 V 来标识。

8	7	6	5	4	3	2	1	Divisions	Subnets	Hosts/Subnets
F	V	V	V	V	V	V	V	2	0	0
F	F	V	V	V	V	V	V	4	2	62
F	F	F	V	V	V	V	V	8	6	30
F	F	F	F	V	V	V	V	16	14	14
F	F	F	F	F	V	V	V	32	30	6
F	F	F	F	F	F	V	V	64	62	2
F	F	F	F	F	F	F	V	128	126	0

上面的例子说明，可以有效使用的最小划分是4，其中包括2个子网，每个子网包括62台主机。最多则可以分成64个部分，包括62个子网，每个子网连接2台主机。第1个例子可以用于2个分离的以太网，而第2个则可以用于一组点到点的协议链路（link）。

然而子网类型的选择要根据每个子网要求的最大用户数目和所需的最小子网数目来确定。

对地址进行划分而得到的网络部分是根据最后一个字节中固定部分的价值形成的。回顾上面的例子，要把一个C类地址分成8个部分或6个子网，必须固定最后一个八位位组中的前3位。地址中的主机部分是根据最后一个字节中非固定部分的价值来确定的。考虑下面这个例子，在这个例子中列出了位的组合，并且说明地址是如何划分成子网的。

Network			Host					Decimal Values
8	7	6	5	4	3	2	1	

0	0	1		0	0	0	0	32
0	1	0		0	0	0	0	64
0	1	1		0	0	0	0	96
1	0	0		0	0	0	0	128
1	0	1		0	0	0	0	160
1	1	0		0	0	0	0	192

如前面的例子所示，3个高位——第8、7和6位——是固定的，因此这三位位用作主机地址的一部分。这意味着会有下面这些网络：

Network

N.O.P.32

N.O.P.64

N.O.P.96

N.O.P.128

N.O.P.160

N.O.P.192

C类地址的标准网络屏蔽是255.255.255.0。对于经过子网处理的网络，前3个字节仍然是相同的，第4个字节则是把网络部分设置为1同时把主机部分设置为0，回头看一下前面的例子，你就会清楚网络地址应该是什么。你要使用同样的格式确定网络屏蔽。这些子网的网络屏蔽如下所示：

Network	Broadcast	Netmask
N.O.P.32	N.O.P.31	255.255.255.32
N.O.P.64	N.O.P.63	255.255.255.64
N.O.P.96	N.O.P.95	255.255.255.96

N.O.P.128 N.O.P.127 255.255.255.128

N.O.P.160 N.O.P.159 255.255.255.160

N.O.P.192 N.O.P.191 255.255.255.192

最后结果就是把这个 C 类地址划分成了 6 个子网，因而在不必申请额外网络地址的情况下增加了可用地址空间。

再来看看网络屏蔽，不难发现为什么许多管理员喜欢使用面向字节 (byte-oriented) 的网络屏蔽——因为这种方式更容易理解。然而若使用面向位的网络屏蔽，则可完成许多不同的配置。例如对一个 C 类地址使用网络屏蔽 255.255.255.192，可以创建 4 个子网络；如果把同样的网络屏蔽用于 B 类网络则可以创建超过 1000 个子网。

1.2.3 主机名

必须给每一个连接到 Internet 的设备分配一个唯一的 IP 地址，但是 IP 地址难于记忆。因而，又通常为每一个设备分配一个主机名，可以通过该主机名来访问设备。网络本身并不需要使用名字，但是这样会使网络更加易于使用。

为了使 TCP/IP 正常地工作，要把主机名翻译成相应的 IP 地址。这项工作可以通过几种不同的方法来完成。例如可以在一个称为主机表 (host table) 的文件中查找主机名，也可以使用域名服务 (DNS) 解析名字。

注意 把主机名翻译成相应 IP 地址的方法和 DNS 将在本章后面讨论。

一个组织机构内部的主机名必须唯一。主机名由两部分组成：实际主机名和 TCP/IP 域名，域是由一个核心注册机构根据你所在的国家和你所注册的组织类型来分配的。最常用的域包括 .com, .edu 和 .gov，它们分别代表美国的商业、教育和政府机构。尽管有可能在美国以外获得一个使用这些名称的域，但最好不要这样做。

对于美国以外的组织，还有其他一些规则指导域的分配。例如加拿大一家名为 Widgets 的公司可以申请 widgets.ca，这里 .ca 表示这家机构在加拿大。如果同样的公司在英国，那么这个域很可能是 widgets.co.uk，表示这是英国国内的一家商业性机构。

至于主机的实际名称，Internet Request for Comments (RFC) 第 1178 款提供了一些非常好的关于如何命名系统的指导。下面列出一些应牢记的指导原则：

- 使用那些简短、易拼写、易记忆的实际单词。使用主机名而不使用 IP 地址的根本原因就是主机名更容易使用。如果主机名难于拼写和记忆的话，那么就与其初衷背道而驰了。

- 使用主题性的名字。一个小组中的所有主机可以使用人类的一些动作命名，诸如 fall、jump 或者 hop，也可以使用卡通人物、食物或者其他分类方式命名。主题名字比那些无规则的随意名字更容易想出来。

- 要避免使用项目名称、个人名字、缩写词或者其他这类隐密性的术语。一般说来，这类主机名在将来要重新命名，这样做可不像听起来那么容易。

注意 对主机名唯一的要求就是在它所在的域内必须唯一。无论如何选择一个好的