



ICSA 国家信息中心 启明星辰公司 策划

Internet / Intranet

网络安全结构设计

启明星辰公司

许锦波 严望佳 编著

计算机网络安全系列丛书



清华大学出版社

<http://www.tup.tsinghua.edu.cn>



TP393.68

X76

计算机网络安全系列丛书

Internet/Intranet 网络安全结构设计

启明星辰公司

许锦波 严望佳 编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书主要讲述 Internet/Intranet 的安全结构, 首先从构成 Internet/Intranet 的基本部件的安全性着手, 分别叙述了它们各自的安全问题和安全措施, 然后从总体上介绍一个综合运用各部件的实际安全网络方案, 该方案有机地糅合了各个安全部件, 从而使大家进一步认清各个安全部件的相互关系。本书内容覆盖了 TCP/IP 协议、域名系统、防火墙技术、电子邮件系统、WWW 系统、网络管理系统、数据库管理系统和办公自动化系统等各部分的安全。本书行文流畅、示例丰富、讲解清晰、介绍全面, 必能让读者受益匪浅。

版权所有, 翻印必究。

本书封面贴有清华大学出版社激光防伪标签, 无标签者不得销售。

图书在版编目 (CIP) 数据

Internet/Intranet 网络安全结构设计/ICSA 启明星辰公司著. —北京: 清华大学出版社, 1998

(计算机网络安全系列丛书)

ISBN 7-302-03293-9

I.I… II.①I… ②国… III 计算机网络-安全技术-结构设计, IV.TP393

中国版本图书馆 CIP 数据核字 (98) 第 37543 号

出版者: 清华大学出版社 (北京清华大学校内, 邮编 100084)

<http://www.tup.tsinghua.edu.cn>

印刷者: 北京市清华园胶印厂

发行者: 新华书店总店北京发行所

开 本: 787×1092 1/16 印张: 32.25 字数: 573 千字

版 次: 1999 年 2 月第 1 版 1999 年 2 月第 1 次印刷

书 号: ISBN 7-302-03293-9/TP·1766

印 数: 0001~5000

定 价: 53.00 元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设, Internet/Intranet 的发展, 将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击, 同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程, 需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中, Internet/Intranet 安全面临着重大挑战。事实上, 资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展, 计算机网络的资源共享进一步加强, 随之而来的信息安全问题日益突出。据美国 FBI 统计, 美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为, 计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前, 人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现, 随着 Internet 的发展, 现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括: 通过网络监听获取网上用户的帐号和密码; 监听密钥分配过程, 攻击密钥管理服务器, 得到密钥或认证码, 从而取得合法资格; 利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击, 如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等; 利用 Finger 等命令收集信息, 提高自己的攻击能力; 利用 SendMail, 采用 debug、wizard 和 pipe 等进行攻击; 利用 FTP, 采用匿名用户访问进行攻击; 利用 NFS 进行攻击; 通过隐蔽通道进行非法活动; 突破防火墙等等。目前, 已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同, 它们主要的区别是, “蠕虫”寄生于操作系统之上, 而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多, 极易传播, 影响范围广。它动辄删除、修改文件, 导致程序运行错误, 甚至死机, 已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击, 最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件, 从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之,对 Internet/Intranet 安全构成的威胁可以分为以下若干类型:黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等,这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢?主要原因在于 Internet/Intranet 系统内在安全的脆弱性;其次是人们思想麻痹,没有正视黑客入侵所造成的严重后果,因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性,没有采取有效的安全策略和安全机制。另外,缺乏先进的网络安全技术、工具、手段和产品等原因,也导致网络的安全防范能力差。

由于我国网络研究起步晚,网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生,该丛书系统全面地介绍了计算机网络安全各方面的问题,并且从一些新的角度进行探讨,例如,如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略;如何提出 Internet/Intranet 系统安全的整体解决方案;如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术,一定会有所收获。

中国工程院院士 沈昌祥

前言

从国家提出建设“三金工程”以来，因特网（Internet）开始在我国逐渐得到重视。许多部委、事业单位、科研单位等机构开始建立 Internet 的接入网，并在信息科学的推动下开始重组机构内部的信息结构。

但是，当人们真正使用 Internet 的时候，一方面被 Internet 的技术和能跨越空间索取信息所折服，另一方面则对 Internet 网络安全技术感到失望。Intranet 泛指机构内部网，在这里，机构可以是工商企业、事业单位、行业部门和区域部门等。Intranet 其实是指在有限的范围内，利用 Internet 的一系列成熟标准所构筑的机构内部的网络系统。它和数据库技术、多媒体技术以及开放式的群件系统相互融合连接，形成一个能有效地解决信息系统内部信息的采集、共享、发布和交流的，易于维护管理的信息运作平台。与 Internet 相比，Intranet 的安全性则显得更为重要，Intranet 的解决方案应当具有严格的网络资源管理机制、网络安全保障机制，同时还应当具有良好的开放性。

本书主要讲述 Internet/Intranet 的安全结构。首先从构成 Internet/Intranet 的基本部件的安全性着手，分别叙述它们各自的安全问题和安全措施，然后从总体上介绍一个综合运用各部件的实际安全网络方案，该方案有机地结合了各个安全部件，从而使人们进一步认清各个安全部件间的相互关系。

本书内容主要分为十二个部分：

第一部分：Internet/Intranet 安全基础（第一章至第七章）

第二部分：域名系统的安全（第八章）

第三部分：防火墙技术（第九章至第十五章）

第四部分：电子邮件系统的安全（第十六章至第十九章）

第五部分：WWW 系统的安全（第二十章）

第六部分：网络管理系统（第二十一和第二十二章）

第七部分：数据库管理系统的安全（第二十三章至第二十五章）

第八部分：高可用技术（第二十六章）

第九部分：办公自动化系统的安全（第二十七章至第三十章）

第十部分：报表系统（第三十一章）

第十一部分：综合应用实例（第三十二章）

第十二部分：附录

除了最后一个部分外，其余各部分内容基本上是独立的，阅读每一部分都不需要其他部分的知识。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目 录

第一章 Internet/Intranet 解决方案综述	1
1.1 概述	2
1.1.1 Intranet 在中国的诞生	2
1.1.2 Intranet 的实质	2
1.1.3 Intranet 解决方案的基本结构	3
1.1.4 面向业务系统的解决方案	4
1.2 网络建设背景	4
1.2.1 系统目标及任务	4
1.2.2 设计原则	6
1.3 Internet/Intranet 的组成、结构与功能	6
1.3.1 Intranet 的网络逻辑构成	6
1.3.2 操作系统及应用系统结构逻辑图	8
1.4 网络系统连接结构	9
1.4.1 主干网技术的选择	9
1.4.2 网络拓扑结构	12
1.4.3 网络通信协议	13
1.5 本章小结	13
第二章 TCP / IP 介绍	15
2.1 OSI 参考模型	16
2.2 TCP/IP	17
2.3 IP 层	19
2.3.1 IP 数据包格式	20
2.3.2 IP 地址	21
2.3.3 子网	21
2.3.4 网络掩码	22

2.3.5	IP 冲突.....	23
2.3.6	IP 欺骗攻击的防范.....	23
2.3.7	IP 层其他控制协议.....	24
2.4	TCP 和 UDP.....	25
2.5	应用层.....	26
2.6	端口.....	27
2.7	本章小结.....	29
第三章	标准和非标准的 TCP/IP 服务.....	31
3.1	远程登录.....	32
3.2	文件传输协议.....	33
3.2.1	FTP.....	33
3.2.2	提供匿名 FTP 服务.....	33
3.2.3	TFTP.....	38
3.2.4	UUCP.....	38
3.2.5	FSP.....	38
3.2.6	RCP.....	38
3.3	电子邮件.....	39
3.4	Usenet 新闻.....	41
3.5	万维网.....	42
3.5.1	WWW.....	42
3.5.2	Gopher.....	43
3.5.3	广域网信息服务.....	43
3.5.4	Archie.....	43
3.6	网上成员信息查询.....	44
3.6.1	finger.....	44
3.6.2	whois.....	45
3.7	实时会议服务.....	45
3.7.1	talk.....	45
3.7.2	IRC.....	46
3.7.3	MBONE.....	46
3.8	名字服务.....	46
3.9	网络管理服务.....	47
3.10	时间服务.....	48

3.11 NIS 系统	49
3.11.1 NIS 结构	49
3.11.2 NIS 安全脆弱性	50
3.11.3 攻击 NIS 的例子	51
3.11.4 可能的解决方法	52
3.12 网络文件系统	53
3.12.1 NFS 的协议层次	53
3.12.2 RPC	53
3.12.3 XDR	54
3.12.4 NFS 的两个协议	55
3.12.5 客户端的 NFS 相关进程	55
3.12.6 服务器端的 NFS 进程	55
3.12.7 从服务器端调出文件系统	56
3.12.8 客户端的相关信息	57
3.12.9 NFS 的 RPC 认证	57
3.12.10 不安全的 NFS 对系统的危害	58
3.12.11 安全 NFS	59
3.13 窗口系统	59
3.14 打印系统	60
3.15 编写安全的守护程序	60
3.15.1 程序安全的重要性	61
3.15.2 SUID/SGID 程序的设计	63
3.15.3 root 程序的设计	64
3.15.4 编写安全的网络程序	64
3.16 本章小结	65
第四章 广域网络连接技术	67
4.1 广域网的连接方式	68
4.2 连接广域网常用网络设备	70
4.2.1 调制解调器	70
4.2.2 通信服务器	72
4.2.3 网桥和路由器	72
4.3 VSAT	73
4.4 PPP 和 SLIP	74

4.4.1	PPP	75
4.4.2	SLIP	76
4.5	帧中继	77
4.6	X.25	78
4.7	ATM	79
4.8	路由	80
4.8.1	静态路由	80
4.8.2	动态路由	82
4.8.3	外部路由	82
4.9	本章小结	83
第五章	Windows NT 的安全机制	85
5.1	Windows NT 的安全概述	86
5.2	Windows NT 中的术语	87
5.2.1	Windows NT 中的对象	87
5.2.2	Windows NT 服务器和 Windows NT 工作站	88
5.2.3	工作组	88
5.2.4	域	88
5.2.5	域控制器	88
5.2.6	Windows NT 注册表	89
5.3	Windows NT 的安全模型	89
5.3.1	Windows NT 的安全子系统	90
5.3.2	Windows NT 中的登录上网	92
5.3.3	登录标志	92
5.3.4	Windows NT 登录的过程	93
5.3.5	可根据需要选择的存取控制	93
5.3.6	存取标识	94
5.4	Windows NT 环境中的用户帐户	95
5.5	NT 文件系统的安全性	96
5.6	Windows NT 域	98
5.7	域委托关系的安全概念	99
5.8	本章小结	101
第六章	UNIX 系统的安全性	103
6.1	UNIX 的用户帐户	104

6.2	UNIX 文件系统.....	104
6.3	UNIX 的 NIS	107
6.3.1	NIS 与分布环境的管理	107
6.3.2	NIS 组成.....	108
6.3.3	NIS 映射的数据	110
6.4	本章小结.....	111
第七章	认证和加密	113
7.1	认证	114
7.1.1	认证的种类	114
7.1.2	认证服务器存在的问题.....	116
7.1.3	认证服务器的商用解决方案.....	116
7.2	网络级加密.....	117
7.2.1	加密层次	117
7.2.2	加密对象	118
7.2.3	加密地点	119
7.2.4	密钥分配	119
7.3	本章小结.....	120
第八章	域名系统.....	121
8.1	域名系统的结构.....	122
8.2	名字服务器.....	124
8.3	解析器	125
8.4	地址到名字的映射	128
8.5	UNIX 名字服务——BIND	130
8.5.1	named 的配置.....	130
8.5.2	标准资源记录	133
8.5.3	缓存初始化文件	134
8.5.4	自反地址映射文件.....	136
8.5.5	反向域文件	136
8.5.6	名字到地址的转换文件.....	137
8.6	名字欺骗技术.....	139
8.7	本章小结.....	141
第九章	防火墙技术	143

9.1 Internet 上的安全性问题	144
9.2 防火墙简介	144
9.3 防火墙的一般组成	145
9.4 防火墙的不同实现技术	147
9.4.1 数据包过滤技术	148
9.4.2 过滤 FTP 会话	151
9.4.3 应用层网关	153
9.4.4 应用层网关的优缺点	154
9.4.5 代理服务	154
9.4.6 数据包过滤和代理服务的比较	156
9.5 网络拓扑结构和防火墙技术的关系	157
9.6 本章小结	160
第十章 名字服务器和防火墙的配合	161
10.1 名字服务器的数据包特性	162
10.2 名字服务器的代理特性	164
10.3 分散的名字服务器策略	165
10.3.1 外部计算机的名字服务器	165
10.3.2 堡垒主机的名字服务器	166
10.3.3 内部计算机的名字服务器	167
10.4 名字服务器的位置	167
10.5 非透明防火墙网络的名字服务器	169
10.5.1 内部名字服务的配置	170
10.5.2 外部名字服务器的配置	171
10.5.3 堡垒主机的名字服务器配置	172
10.6 透明防火墙的名字服务器	175
10.6.1 外部名字服务器	176
10.6.2 内部名字服务器	177
10.6.3 数据包过滤	180
10.7 设置名字服务器来隐藏信息	181
10.7.1 在堡垒主机上建立伪名字服务器供外界使用	182
10.7.2 内部名字服务器客户机查询内部服务器	183
10.7.3 堡垒名字服务器客户机查询内部服务器	183
10.7.4 数据包过滤	184

10.8 本章小结.....	185
第十一章 穿越防火墙的远程登录和远程执行.....	187
11.1 Telnet 及它的代理性.....	188
11.2 远程命令执行.....	191
11.2.1 BSD r 命令的数据包特性.....	192
11.2.2 BSD r 命令的代理特性.....	193
11.3 远程执行命令 rexec.....	193
11.3.1 rexec 的数据包过滤特性.....	193
11.3.2 rexec 的代理特性.....	194
11.4 远程执行命令 rex.....	194
11.4.1 rex 的数据包过滤特性.....	194
11.4.2 rex 的代理特性.....	194
11.5 本章小结.....	194
第十二章 穿越防火墙的文件传输.....	197
12.1 文件传输协议.....	198
12.1.1 FTP 的数据包特性.....	198
12.1.2 FTP 的代理特性.....	201
12.2 简单文件传输协议.....	202
12.2.1 TFTP 的数据包过滤特性.....	202
12.2.2 TFTP 的代理特性.....	202
12.3 文件服务协议.....	203
12.3.1 FSP 的数据过滤特性.....	203
12.3.2 FSP 的代理特性.....	203
12.4 网络文件系统.....	204
12.4.1 NFS 的数据包过滤特性.....	204
12.4.2 NFS 的代理特性.....	205
12.5 本章小结.....	205
第十三章 网络管理服务与防火墙的配合.....	207
13.1 简单网络管理协议.....	208
13.1.1 SNMP 的数据包特性.....	208
13.1.2 SNMP 的代理特性.....	209
13.2 路由信息协议.....	209

13.2.1	RIP 的数据包特性	209
13.2.2	RIP 的代理特性	209
13.3	ping	209
13.3.1	ping 数据包过滤特性	210
13.3.2	ping 的代理特性	210
13.4	traceroute	210
13.4.1	traceroute 数据包特性	211
13.4.2	traceroute 的代理特性	212
13.5	其他 ICMP 数据包	212
13.6	网络信息服务/黄页	212
13.6.1	NIS/YP 的数据包过滤特性	213
13.6.2	NIS/YP 的代理特性	213
13.7	网络上的信息查询	213
13.7.1	finger 的数据包过滤特性	214
13.7.2	finger 的代理特性	214
13.7.3	whois	214
13.7.4	whois 的数据包过滤特性	214
13.7.5	whois 的代理特性	215
13.8	本章小结	215
第十四章	穿越防火墙的新闻服务	217
14.1	NNTP 的数据包特性	218
14.2	NNTP 的代理性	219
14.3	NNTP 的数据包过滤	220
14.4	本章小结	221
第十五章	防火墙之外	223
15.1	网络安全检查——Secure Test 和 Security Health Check	224
15.2	防火墙安全分析	225
15.2.1	SecureVIEW 体系结构	226
15.2.2	丰富的分析和报告	226
15.2.3	灵活的和可定制的输出	228
15.2.4	SecureVIEW 的重要特性	229
15.3	网络传输内容安全性域网络过滤软件	229
15.3.1	MIMESweeper	229

15.3.2 SurfWatch	230
15.3.3 WebSENSE	230
15.4 入侵检测和扫描	230
15.4.1 SAFEsuite	230
15.4.2 扫描工具	231
15.4.3 其他	233
15.5 本章小结	233
第十六章 电子邮件系统	235
16.1 电子邮件	236
16.2 电子邮件的地址	237
16.3 邮件网关	239
16.4 邮件格式	240
16.4.1 非 ASCII 码数据的 MIME 扩展	240
16.4.2 MIME 多部分报文	242
16.5 简单邮件传送协议	243
16.6 MX 记录	244
16.6.1 MX 算法	246
16.6.2 设置 MX 记录	247
16.6.3 构造 MX 列表	252
16.7 本章小结	254
第十七章 企业邮件和 Internet 的连接	255
17.1 概述	256
17.2 邮件网关的选择	257
17.3 为局域网邮件用户传入邮件	258
17.4 传出邮件方案	259
17.4.1 传出的局域网邮件方案一	259
17.4.2 传出的局域网邮件方案二	260
17.4.3 传出的局域网邮件方案三	261
17.5 本章小结	262
第十八章 Notes 的邮件规划	263
18.1 Notes 邮件特性	264
18.2 Domino 邮件服务器	264