

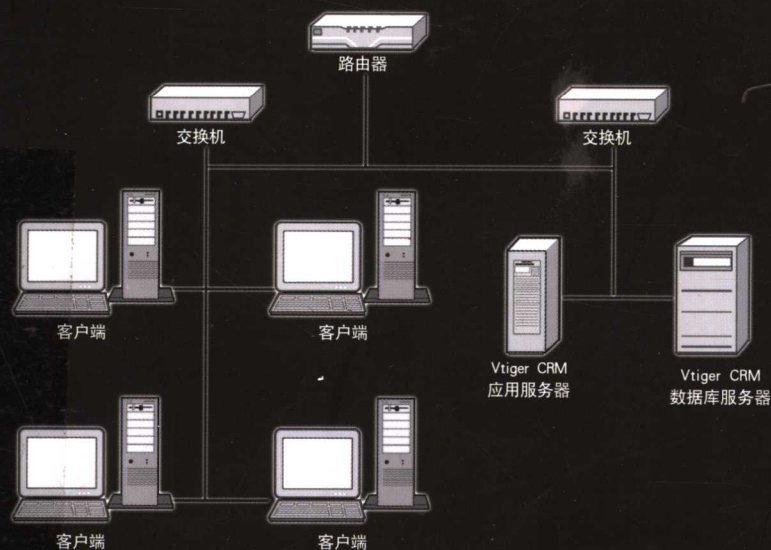


网管宝典系列

网络安全 技术内幕

NETWORK SECURITY TECHNOLOGY EXPOSING

北京希望电子出版社 总策划
肖松岭 编 著



科学出版社
www.sciencep.com



TP393.08/256

2008

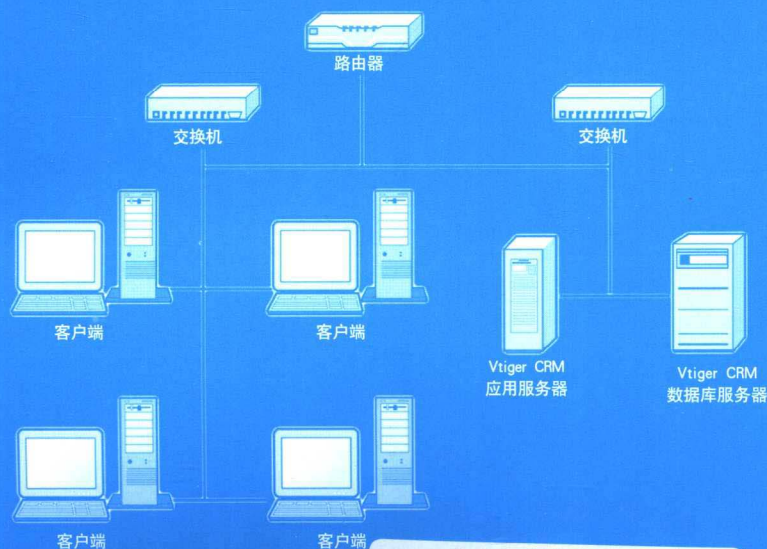
网 管 玉 典 系 列

网络安全 技术内幕

NETWORK SECURITY TECHNOLOGY EXPOSING

北京希望电子出版社 总策划

肖松岭 编 著



科学出版社

www.sciencepress.com

内 容 简 介

破坏操作系统、获得超级用户权限的恶意行为,对所有系统管理员来说都将是—场噩梦。本书主要讨论 Windows、UNIX、Linux 等操作系统,各类黑客入侵的手段及其防护措施。

本书共分 4 个部分:第一部分首先介绍了网络安全必备的基本意识和基础知识,接着讨论了 Windows 及其应用程序 IIS、SQL Server 以及 Web 的安全问题及攻击的方法。第二部分讨论了 UNIX 和 Linux 网络的安全问题,包括 Linux 安全硬化、服务器安全策略、虚拟专用网、防火墙技术、OpenSSH 加密以及评估与入侵事件。第三部分主要从网络架构 OSI 各层协议的安全问题着手,对各类操作系统的网络安全及其防护给出了具体实现方法。从技术角度上看,涉及各个操作平台,包括网络安全原理、IP 层安全协议、传输层安全协议、应用层安全协议、防火墙技术以及加密和认证技术等。第四部分重点讨论 Cisco 设备安全问题。网络安全的诸多问题及其安全防护措施,包括防火墙技术,数据加密技术,入侵检测系统,认证、授权和记账以及无线网络的安全性等内容,书中都作了十分详细的剖析,指导性、实用性和可操作性强。

本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读,对网络爱好者也有很好的指导作用。

图书在版编目(CIP)数据

网络安全技术内幕 / 肖松岭 编著. —北京: 科学出版社,
2008
(网络安全技术及应用)
ISBN 978-7-03-021374-7

I. 网... II. 肖... III. —计算机网络—安全技术 IV.
TP 393.08

中国版本图书馆 CIP 数据核字(2008)第 032127 号

责任编辑: 但明天 / 责任校对: 马 君
责任印刷: 密 东 / 封面设计: 梁运丽

科 学 出 版 社 出 版

北京东黄城根北街 16 号
邮政编码: 100717

<http://www.sciencep.com>

北京市密东印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2008 年 5 月第 一 版 开本: 787×1092 1/16
2008 年 5 月第一次印刷 印张: 45 1/2
印数: 1—3000 字数: 1 052 220

定价: 68 元

前言

破坏操作系统——无论是 Windows、UNIX 还是 Linux，并获得超级用户权限的恶意行为，对所有系统管理员来说都将是一场恶梦。

本书重点不在于讨论各个操作系统本身的安全问题，而是讲述它们基于网络方面的安全技术，同时还探讨了各种黑客入侵的手段以及有效的防护措施。

全书共分 4 个部分，下面对各部分作简单介绍。

第一部分 Windows 安全篇

本部分内容由 13 章组成，主要讨论应用最为广泛的 Windows 操作系统的安全问题。

Windows 操作系统最容易上手，但其存在的问题多多，无论是系统本身的漏洞，还是其提供的各种服务：上网有问题，打印有问题，输入有问题，开、关机有问题……但本书不准备讲这些，而是另辟蹊径，首先简单讨论一下 Windows 的安全及其防护，接着转移目标，讲如何攻击这个穷寇。

基于 Windows 系统网络方面的安全问题，主要包括：Windows 安全结构及其防御，踩点、嗅探、扫描，获取控制权，服务攻击——IIS、SQL Server、Web，扩大攻击范围，后门处理以及 DoS 攻击。

第二部分 Redhat Linux 安全篇

本部分内容由 6 章组成，主要讨论网络操作系统 Linux 及 UNIX 方面的安全问题。

毋庸置疑，称得上真正意义上的网络操作系统就是 UNIX 和 Linux，而目前应用较为广泛的要数 Redhat Linux。虽然这两种操作系统都是十分优秀的网络平台，但它们也必然存在诸多安全问题。基于此，本部分单独为这两款操作所存在的安全问题进行了比较详细的讨论，以期帮助读者解决一些较为棘手的难题。

基于 Linux 及 UNIX 操作系统方面的网络安全问题，主要从 6 个方面进行讨论，包括：Linux 安全硬化、服务器安全策略、虚拟专用网、防火墙技术、OpenSSH 加密以及评估与入侵事件。

第三部分 网络安全篇

本部分内容由 6 章组成，主要讨论网络通信协议及数据传输过程方面的安全问题。

网络是现代企业的脊梁骨，数以千米计的铜制或光纤电缆为通信提供了有效的数据传输介质。大多数公司的局域网（LAN）或广域网（WAN）都需要安全保护。网络漏洞绝不是小事情，一旦攻击者控制了你的网络，他们就可以控制数据的传输情况和传输目标。在大多数场合，控制了某个网络意味着攻击者不仅可以监听这个网络上的电子邮件、财务数据等敏感信息，甚至可以把这个网络上的通信重定向到另一个未经授权的系统上去，如果到了这一地步，那么该网络是否使用了虚拟专用网（VPN）或防火墙技术其作用都不大了。

虽然网络漏洞不如系统漏洞那么多，但其数量和潜在破坏力却年年在增加。从 MIB

(Management Information Base, 管理信息库) 信息泄露到设计缺陷和强大的 SNMP (Simple Network Management Protocol, 简单网络管理协议) 读/写操作, 当黑客把这些网络漏洞结合起来运用时, 网络管理员就不得不面对一个到处是陷阱的蛮荒世界了。

ISO/OSI 网络安全问题可以从 6 个方面来解决, 包括: 网络安全原理、IP 层安全协议、传输层安全协议、应用层安全协议、防火墙技术以及加密与认证技术。

第四部分 Cisco 安全篇

本部分内容由 5 章组成, 主要讨论使用 Cisco 设备组建的网络安全问题。

在众多网络设备供应商中, 由于 Cisco 的设备遍布网络世界的各个角落, 因此它是无可争议的龙头老大。在网络安全方面, Cisco 提供了一套完善的解决方案。凡是使用 Cisco 设备的网络, 或多或少都在使用 Cisco 安全方案中的技术。

Cisco OSI 网络安全方案主要由 5 部分组成, 包括: 认证、授权和记账 (AAA), 安全服务器协议, 流量控制和防火墙, IP 安全和加密技术以及网络设备安全。

关于网络安全技术, 包括身份认证、防火墙技术、入侵检测技术、加密技术、公钥基础设施、虚拟专用网络、恶意代码和病毒防治以及无线网络所涉及的网络安全技术, 书中都进行了详细的讨论, 同时指导读者进行一些尝试和探索。

本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读, 对网络爱好者也有很好的指导作用。

由于新技术发展、更新迅速, 尽管作者做了不懈努力, 但书中难免存在不妥和遗漏之处, 敬请广大读者批评、指正。

目 录

第一部分 Windows 安全篇

第1章 初识 Windows 安全.....	3
1.1 网络安全服务.....	3
1.2 安全策略的重要性.....	4
1.3 网络安全主要技术.....	4
1.4 Windows 安全配置初步方案.....	5
1.5 Windows 安全配置中级方案.....	8
1.6 Windows 安全配置高级方案.....	12
第2章 Windows Server 安全结构.....	17
2.1 Windows Server 安全结构.....	17
2.2 安全内容.....	17
2.2.1 操作用户.....	17
2.2.2 用户分组.....	20
2.2.3 计算机账户.....	22
2.2.4 操作权限.....	22
2.2.5 账户安全管理器.....	23
2.3 森林、树和域.....	24
2.3.1 本地、全局和通用.....	25
2.3.2 信任关系.....	25
2.3.3 管理边界.....	26
2.4 安全标识符.....	28
2.5 身份验证与授权.....	30
2.5.1 权限令牌.....	30
2.5.2 网络身份验证.....	31
2.6 审计.....	33
第3章 Windows Server 安全防御.....	35
3.1 对 Windows Server 平台进行硬化.....	36
3.1.1 安装前的安全准备.....	36
3.1.2 以手动方式进行硬化.....	37
3.1.3 连接防火墙因特网.....	38
3.2 安全模板和安全配置分析.....	39
3.2.1 安全模板.....	40
3.2.2 安全配置分析.....	42
3.3 组策略.....	43
3.3.1 组策略.....	43

3.3.2 使用组策略.....	43
3.3.3 组策略生效.....	44
3.3.4 策略效果.....	45
3.3.5 软件限制策略.....	46
3.4 IPSec 过滤器.....	47
3.4.1 IPSec 过滤器优点.....	47
3.4.2 IPSec 过滤机制缺陷.....	47
3.4.3 IPSec 策略创建步骤.....	49
3.5 其他配置.....	51
3.6 保护 IP 和端口.....	52
3.6.1 设置代理服务器.....	52
3.6.2 关闭端口.....	53
3.6.3 配置安全策略保护端口.....	55
3.7 防范木马程序.....	60
3.7.1 木马伪装手段.....	60
3.7.2 识别木马.....	62
3.7.3 防范木马的入侵.....	63
3.8 驱逐间谍软件.....	64
3.8.1 Ad-aware.....	64
3.8.2 安博士.....	66
第4章 踩点、扫描.....	69
4.1 踩点.....	69
4.1.1 whois 和 Sam Spade 查询工具.....	69
4.1.2 由 IP 获取地理位置.....	70
4.1.3 了解网站备案信息.....	71
4.1.4 搜索引擎工具.....	72
4.2 命令行扫描工具.....	73
4.2.1 扫描原理与分类.....	74
4.2.2 ping 扫描工具.....	75
4.2.3 ScanLine 扫描工具.....	77
4.2.4 netcat、telnet 和 nmap 扫描工具.....	79
4.3 视窗扫描软件.....	80
4.3.1 SuperScan 扫描软件.....	80
4.3.2 MBSA 检测系统.....	87
4.3.3 X-Scan 扫描软件.....	94
4.3.4 IP Scanner 扫描软件.....	101

4.3.5 LanSee 搜索软件.....	102	6.1.4 人工猜口令.....	140
4.3.6 LanExplorer 扫描软件.....	104	6.1.5 FOR 循环字典.....	141
第 5 章 查点嗅探.....	108	6.1.6 NAT 字典工具.....	143
5.1 分析扫描结果.....	108	6.1.7 SMBGrind 字典工具.....	143
5.2 NetBIOS Name Service 查点.....	109	6.1.8 enum 字典工具.....	144
5.2.1 net view 查点工具.....	109	6.1.9 “猜测口令字”攻击对策.....	144
5.2.2 nbtstat 查点工具.....	110	6.2 窃取 Windows 身份验证过程.....	147
5.2.3 nbtscan 查点工具.....	110	6.2.1 KerbSniff 和 KerbCrack 工具.....	147
5.2.4 nlttest 查点工具.....	111	6.2.2 SMB 重定向服务器.....	147
5.3 RPC 查点.....	111	6.3 拦截 Windows 身份验证过程.....	149
5.3.1 epdump 查点工具.....	111	6.3.1 SMBRelay 工具设立的非法 验证服务器.....	149
5.3.2 rpcdump 查点工具.....	111	6.3.2 SMBRelay 工具 MITM 攻击.....	150
5.4 SMB 查点.....	112	6.4 攻击手段回顾.....	150
5.4.1 net use 建立空连接.....	112	第 7 章 谋取控制权.....	152
5.4.2 net view 查看共享卷.....	113	7.1 命令行控制权.....	152
5.4.3 nltest 查看域信任关系.....	113	7.1.1 remote 工具.....	152
5.4.4 local 和 global 查看账户名单.....	113	7.1.2 rsetup/rclient 工具.....	153
5.4.5 DumpSec 查点工具.....	114	7.1.3 netcat 工具.....	154
5.4.6 enum 查点工具.....	114	7.1.4 Wsremote 工具.....	155
5.4.7 nete 查点工具.....	115	7.1.5 PsExec 工具.....	156
5.4.8 user2sid 查点工具.....	116	7.1.6 Telnet 入侵.....	157
5.4.9 Userinfo 查点工具.....	118	7.1.7 命令行控制的防范措施.....	160
5.4.10 UserDump 查点工具.....	118	7.2 注册表入侵.....	163
5.4.11 GetAcct 查点工具.....	118	7.2.1 修改注册表实现远程监控.....	163
5.4.12 walksam 查点工具.....	119	7.2.2 开启远程注册表服务.....	165
5.4.13 SMB 查点对策.....	119	7.2.3 通过注册表开启终端服务.....	167
5.5 SNMP 查点.....	124	7.3 GUI 图形控制权.....	168
5.5.1 snmputil 工具.....	125	7.3.1 VNC 工具.....	168
5.5.2 SNMP 查点对策.....	125	7.3.2 网络执法官.....	169
5.6 活动目录查点.....	126	7.4 远程控制任我行.....	178
5.7 网络嗅探.....	127	7.4.1 配置“远程控制任我行”.....	179
5.7.1 Sniffer Portable.....	127	7.4.2 植入木马.....	182
5.7.2 CaptureNet.....	133	7.4.3 监视并控制远程计算机.....	182
5.8 探查疑点对策.....	136	第 8 章 扩大范围.....	188
第 6 章 开始攻击.....	138	8.1 关闭目标审计.....	188
6.1 猜口令字.....	138	8.1.1 auditpol 工具.....	188
6.1.1 分析查点结果.....	138	8.1.2 防止关闭审计.....	188
6.1.2 关闭“空连接”.....	139	8.2 收集应用服务口令字.....	189
6.1.3 避免账户被锁定.....	139		

8.2.1 逆向还原解密口令.....	189	9.4.6 修改文件关联.....	221
8.2.2 pwdump2/3 工具.....	190	9.4.7 捆绑文件.....	221
8.3 破解口令字.....	190	9.5 木马的捆绑生成.....	221
8.3.1 John the Ripper 工具.....	191	9.5.1 使用 Exebinder 捆绑木马.....	221
8.3.2 MDcrack 工具.....	192	9.5.2 免杀捆绑器.....	223
8.3.3 L0phtcrack4 工具.....	192	9.5.3 网页木马生成器.....	224
8.3.4 Lsadump 工具.....	193	9.6 “冰河”木马.....	225
8.4 密码搜索.....	193	9.6.1 “冰河”简介.....	226
8.4.1 命令行.....	193	9.6.2 配置“冰河”木马服务端程序.....	227
8.4.2 键盘记录器.....	194	9.6.3 使用“冰河”木马遥制计算机.....	228
8.5 种植木马.....	194	9.6.4 卸载和清除“冰河”木马.....	231
8.5.1 木马的特征.....	195	9.7 木马清除软件.....	233
8.5.2 木马的种类.....	196	9.7.1 使用“Windows 进程管理器”.....	233
8.5.3 “广外女生”木马.....	197	9.7.2 软件清除木马.....	236
8.6 捕获数据.....	209	9.7.3 Trojan Remover 清除木马.....	241
8.6.1 FakeGINA 木马工具.....	209	9.8 掩盖入侵痕迹.....	242
8.6.2 dsniiff for Win32 工具.....	210	9.8.1 删除日志.....	242
8.6.3 Ethereal 工具.....	210	9.8.2 attrib +h 命令隐藏文件.....	243
8.7 跳板双网攻击.....	210	9.8.3 Elitewrap 工具.....	244
8.8 端口重定向.....	213	9.9 计算机犯罪证据的收集分析.....	244
8.8.1 rinetd 工具.....	213	9.9.1 谁在监听那些端口.....	244
8.8.2 fpipe 工具.....	214	9.9.2 pulist 和 sclist 工具.....	245
8.9 怎样扩大攻击范围.....	215	9.9.3 定期检查文件系统.....	245
第9章 后门处理.....	216	9.9.4 审计、账户和日志维护.....	246
9.1 偷建用户账户.....	216	9.10 小心后门.....	246
9.2 远程控制工具.....	216	第10章 攻击 IIS.....	247
9.2.1 SubSeven 工具.....	217	10.1 IIS 缓冲区溢出.....	247
9.2.2 Back Orifice(BO2K).....	217	10.1.1 HTR 堆溢出漏洞.....	247
9.3 后门和木马程序种植位置.....	218	10.1.2 HTRchunked 编码对策.....	249
9.3.1 启动文件夹.....	218	10.2 源代码泄露攻击.....	249
9.3.2 Windows 注册表中的启动项.....	218	10.2.1 +.htr 漏洞.....	250
9.3.3 Web 浏览器初始页面下载代码.....	219	10.2.2 Translate:f 漏洞.....	251
9.3.4 计划任务.....	219	10.2.3 WSDL 和 DISCO 泄露.....	252
9.4 木马常用的入侵手法.....	220	10.3 Web 服务器安全评估工具.....	253
9.4.1 在 win.ini 文件中加载.....	220	10.4 防御措施.....	254
9.4.2 在 system.ini 文件中加载.....	220	第11章 攻击 SQL Server.....	258
9.4.3 在 Winstart.bat 中启动.....	220	11.1 SQL Server 安全概述.....	258
9.4.4 启动组.....	220	11.2 扫描 SQL Server.....	259
9.4.5 *.ini.....	221	11.2.1 端口扫描.....	259

11.2.2	SQLPing 工具.....	259
11.2.3	查找 SQL Server.....	260
11.3	SQL 查询工具.....	261
11.3.1	Query Analyzer 工具.....	261
11.3.2	osql 工具.....	261
11.3.3	sqldict 工具.....	262
11.4	SQL 攻击方式.....	262
11.4.1	sqlbf 工具.....	262
11.4.2	sqlpoke 工具.....	263
11.4.3	恶意 ASP 页面.....	263
11.4.4	源代码泄露.....	265
11.5	SQL 代码注射攻击.....	265
11.6	SQL Sewer 防御措施.....	267
第 12 章	攻击 Web.....	271
12.1	缓冲区溢出.....	271
12.1.1	DirectX 缓冲区溢出.....	271
12.1.2	HTML 转换器缓冲区溢出.....	272
12.1.3	Outlook/OFFICE vCard 缓冲区 溢出.....	272
12.1.4	WMP 对.asx 缓冲区溢出.....	273
12.2	执行命令.....	274
12.3	写本地文件.....	276
12.3.1	WMP 皮肤下载.....	276
12.3.2	写入 Telnet 客户日志.....	276
12.4	VBS 地址簿蠕虫.....	278
12.4.1	Senna Spy Worm Generator.....	278
12.4.2	Outlook 蠕虫防范措施.....	279
12.5	通用防范措施.....	279
第 13 章	DoS 拒绝服务攻击.....	280
13.1	Windows 拒绝服务攻击.....	280
13.1.1	TCP 连接洪水.....	280
13.1.2	应用服务层 DoS 攻击.....	281
13.1.3	LAN 的 DoS 攻击活动.....	281
13.1.4	DDoS 傀儡.....	282
13.2	如何防范 DoS 攻击.....	284

第二部分 Redhat Linux 安全篇

第 14 章	Linux 安全硬化.....	289
14.1	BIOS 和引导程序安全.....	289

14.1.1	BIOS 口令.....	289
14.1.2	引导装载程序口令.....	289
14.2	口令安全.....	290
14.2.1	创建强口令.....	291
14.2.2	内部创建口令.....	292
14.3	管理控制.....	293
14.3.1	允许根权限.....	294
14.3.2	禁止根存取权限.....	294
14.3.3	限制根存取权限.....	296
14.4	可用网络服务.....	298
14.4.1	对服务的威胁.....	298
14.4.2	识别和配置服务.....	299
14.4.3	不安全服务.....	300
第 15 章	Linux 服务器安全.....	301
15.1	TCP 会绕和 xinetd 增加安全.....	301
15.1.1	TCP 会绕增强安全.....	301
15.1.2	xinetd 加强安全.....	302
15.2	Portmap 安全.....	303
15.3	NIS 安全.....	304
15.4	NFS 安全.....	305
15.5	Apache HTTP 安全.....	306
15.6	FTP 安全.....	307
15.7	Sendmail 安全.....	308
15.8	校验监听端口.....	309
第 16 章	虚拟专用网.....	311
16.1	IPSecs.....	311
16.2	IPSecs 主机到主机配置.....	312
16.3	IPSecs 网络到网络配置.....	315
第 17 章	防火墙.....	319
17.1	防火墙安全级别配置工具.....	320
17.2	使用 IPTables.....	322
17.3	常用 iptables 过滤.....	323
17.4	FORWARD 和 NAT 规则.....	324
17.5	病毒和假冒 IP 地址.....	326
17.6	iptables 和连接跟踪.....	326
第 18 章	OpenSSH 加密.....	327
18.1	配置 OpenSSH 服务器.....	327
18.2	配置 OpenSSH 客户.....	328
18.2.1	使用 ssh 命令.....	328

18.2.2 使用 scp 命令	328
18.2.3 使用 sftp 命令	329
18.2.4 生成钥匙对	329
第 19 章 评估与入侵事件	332
19.1 评估工具	332
19.1.1 使用 Nmap 来扫描主机	332
19.1.2 其他评估工具	333
19.2 基于主机入侵检测系统 IDS	333
19.2.1 RPM 作为 IDS	333
19.2.2 其他基于主机的 IDS	335
19.3 基于网络的 IDS	335
19.3.1 tcpdump	336
19.3.2 Snort	337
19.4 调查恢复	337
19.4.1 收集证据映像	337
19.4.2 收集入侵后的信息	338
19.4.3 恢复资源	339
19.5 常见被攻击和利用的漏洞	339
19.6 常用端口	341

第三部分 网络安全篇

第 20 章 TCP/IP 协议簇	347
20.1 OSI 网络结构模型	347
20.1.1 OSI 模型结构	347
20.1.2 OSI 安全服务	349
20.1.3 安全机制	352
20.1.4 安全管理	353
20.2 TCP/IP	354
20.2.1 TCP/IP 分层结构	354
20.2.2 互联网 IP 地址	356
20.2.3 端口	356
20.2.4 IP 子网	357
20.3 ARP/RARP 地址和逆向解析	358
20.3.1 ARP 数据包格式	359
20.3.2 使用 ARP	359
20.3.3 免费 ARP 和 ARP 代理	361
20.3.4 ARP 命令	361
20.4 ICMP 报文控制协议	361
20.4.1 ICMP 报文格式	362

20.4.2 ICMP 报文应用示例	363
20.5 ping 程序	364
20.5.1 ping 命令	365
20.5.2 IP 协议的记录路由选项	365
20.5.3 示例	366
20.6 net 命令	368
20.6.1 netstat 指令	368
20.6.2 net 指令	369
20.6.3 at 指令	369
20.7 Traceroute 命令	370
20.7.1 Traceroute 的原理	370
20.7.2 Traceroute 的使用	370
20.8 IP 路由	371
20.8.1 路由	371
20.8.2 路由选路	373
20.8.3 路由表动态更新	376
20.9 动态选路协议	377
20.9.1 选路信息协议 (RIP)	377
20.9.2 边界网关协议 (BGP)	379
20.10 UDP 用户数据包协议	379
20.10.1 UDP 数据包格式	379
20.10.2 分片	380
20.11 广播和多播	381
20.11.1 广播	382
20.11.2 多播	382
20.11.3 多播地址转换	383
20.12 IGMP 组管理协议	383
20.12.1 IGMP 报文	384
20.12.2 组播作用域	385
20.13 域名系统	385
20.13.1 域名分级	385
20.13.2 域名转换过程	386
20.14 BOOTP 和 DHCP	387
20.14.1 BOOTP 报文格式	387
20.14.2 DHCP 动态地址分配	387
20.14.3 DHCP 地址获取过程	388
20.14.4 DHCP 报文格式	389
20.14.5 Linux DHCP 服务器配置	389
20.15 TCP 协议	390

20.15.1 TCP 通信过程	390	22.3 私有通信技术	433
20.15.2 TCP 报文格式	391	22.4 传输层安全协议	434
20.15.3 建立 TCP 连接	392	22.5 SSL/TLS 在 Windows 上的实现	435
20.15.4 终止 TCP 连接	392	22.5.1 微软证书服务	436
20.15.5 一个例子	393	22.5.2 安装证书服务	436
20.16 SNMP 协议	394	22.5.3 生成证书申请文件	438
20.16.1 网络管理的组成	395	22.5.4 通过浏览器申请证书	438
20.16.2 管理信息库	395	22.5.5 安装服务器申请证书	439
20.16.3 SNMP 协议	395	22.5.6 通过 SSL 访问服务器	439
20.17 常见问题	396	22.6 SSL/TIS 在 UNIX/Linux 上的实现	440
第 21 章 IP 层安全协议	398	22.6.1 获取和安装 OpenSSL	440
21.1 IPSec 协议	398	22.6.2 配置 OpenSSL 环境	440
21.2 IETF IPSec 简介	399	22.6.3 获得和安装 Apache+SSL	441
21.3 安全关联	402	22.6.4 建立证书中心	441
21.4 IPSP 验证头	403	22.6.5 产生和安装服务器证书	442
21.5 安全载荷封装	406	22.7 相关问题	443
21.6 密钥管理和交换	408	第 23 章 应用层安全协议	445
21.6.1 Photuris 和 SKEME 密钥管理		23.1 Telnet	445
协议	409	23.1.1 安全的 RPC 认证	446
21.6.2 ISAKMP 密钥管理协议	411	23.1.2 安全 Telnet	447
21.6.3 OAKLEY 密钥决定协议	412	23.2 电子邮件	448
21.6.4 IKE 协议	413	23.2.1 增强保密邮件	449
21.7 Windows 上的 IPSec 实现	414	23.2.2 相当好的保密性 (Pretty	
21.7.1 域和对等通信	415	Good Privacy)	452
21.7.2 远程通信	416	23.2.3 安全 MIME	453
21.7.3 IPSec 配置和管理	418	23.3 WWW 事务	454
21.8 UNIX/Linux 上的 IPSec 实现	422	23.4 其他应用	457
21.8.1 NIST IPSec 项目组	422	23.5 常见问题	458
21.8.2 Free S/Wan 项目组	422	第 24 章 防火墙技术	459
21.8.3 KAMEBSD 上实现 IPSec	422	24.1 防火墙	459
21.9 回顾	423	24.1.1 防火墙的功能	460
第 22 章 传输层安全协议	425	24.1.2 防火墙的缺陷	460
22.1 SSH 协议	425	24.1.3 防火墙常用概念	461
22.1.1 SSH 传输层协议	426	24.1.4 防火墙基本类型	462
22.1.2 SSH 认证协议	428	24.1.5 防火墙构成成本	462
22.1.3 SSH 连接协议	428	24.1.6 防火墙技术发展	463
22.2 安全 Socket 层	429	24.1.7 防火墙主要技术	463
22.2.1 SSL 记录协议	430	24.2 包过滤技术	464
22.2.2 SSL 握手协议	431	24.3 代理服务技术	465

24.4 防火墙其他技术.....	467	25.5 综合应用 CA、PKI 技术.....	519
24.4.1 地址翻译 (NAT) 技术.....	467	第四部分 Cisco 安全篇	
24.4.2 虚拟专用网技术.....	468	第 26 章 AAA 认证、授权和记账.....	
24.4.3 内容检查技术.....	469	26.1 AAA 概要.....	525
24.5 防火墙安全策略.....	470	26.1.1 AAA 安全服务.....	525
24.6 防火墙体系结构.....	471	26.1.2 AAA 配置过程概览.....	526
24.6.1 堡垒主机.....	471	26.2 AAA 认证配置.....	528
24.6.2 堡垒主机原则.....	471	26.2.1 AAA 认证方法列表.....	528
24.6.3 特殊的堡垒主机.....	472	26.2.2 方法列表配置示例.....	528
24.6.4 堡垒主机的物理位置.....	474	26.3 认证配置命令.....	529
24.6.5 堡垒主机服务选择.....	474	26.3.1 aaa authentication arap.....	530
24.6.6 堡垒主机账户管理.....	475	26.3.2 aaa authentication banner.....	530
24.6.7 建立堡垒主机.....	475	26.3.3 aaa authentication enable default.....	531
24.7 双宿主主机结构.....	476	26.3.4 aaa authentication fail-message	531
24.8 屏蔽主机结构.....	477	26.3.5 aaa authentication local-override.....	532
24.9 屏蔽子网结构.....	478	26.3.6 aaa authentication login	532
24.10 防火墙结构变化及组合.....	481	26.3.7 aaa authentication nasi	532
24.11 企业选购防火墙原则.....	489	26.3.8 aaa authentication password- prompt.....	533
24.12 防火墙设计原则.....	491	26.3.9 aaa authentication username- prompt.....	533
第 25 章 加密与认证.....	493	26.3.10 aaa new-model	533
25.1 加密与认证技术基础.....	493	26.3.11 aaa processes.....	533
25.1.1 加密的基本概念.....	493	26.3.12 access-profile	534
25.1.2 加密通信的典型过程.....	494	26.3.13 arap authentication	534
25.1.3 加密主要技术.....	495	26.3.14 clear ip trigger-authentication	535
25.1.4 身份认证简介.....	497	26.3.15 ip trigger-authentication (global configuration)	535
25.1.5 数字证书.....	498	26.3.16 ip trigger-authentication (interface configuration)	535
25.1.6 数字签名.....	500	26.3.17 login authentication.....	536
25.2 PGP 软件.....	502	26.3.18 login tacacs.....	536
25.2.1 PGP 名词解释.....	503	26.3.19 nasi authentication	536
25.2.2 安装 PGP	504	26.3.20 ppp authentication.....	536
25.2.2 生成密钥.....	507	26.3.21 ppp chap hostname.....	537
25.2.3 文件加密与解密.....	508	26.3.22 ppp chap password.....	537
25.2.4 数字签名.....	510	26.3.23 ppp chap refuse	537
25.3 PKI 技术.....	512	26.3.24 ppp chap wait	538
25.3.1 PKI 公开密钥体系.....	513		
25.3.2 PKI 技术在安全体系中的应用	514		
25.4 CA 认证.....	517		
25.4.1 CA 的作用.....	518		
25.4.2 在安全体系中应用 CA 技术.....	518		

26.3.25	ppp pap sent-username.....	538	27.2.3	radius-server attribute nas-port extended.....	561
26.3.26	ppp use-tacacs.....	539	27.2.4	radius-server configure-nas.....	561
26.3.27	show ip trigger-authentication	539	27.2.5	radius-server dead-time.....	561
26.3.28	show ppp queues.....	539	27.2.6	radius-server extended-portnames.....	562
26.3.29	timeout login response	540	27.2.7	radius-server host.....	562
26.4	AAA 授权配置.....	540	27.2.8	radius-server host non-standard	562
26.4.1	AAA 授权命名方法列表.....	540	27.2.9	radius-server optional passwords.....	563
26.4.2	命名方法列表授权配置实例.....	542	27.2.10	radius-server key.....	563
26.4.3	TACACS+授权示例.....	544	27.2.11	radius-server retransmit	563
26.4.4	RADIUS 授权示例.....	544	27.2.12	radius-server timeout	563
26.4.5	反向 Telnet 授权示例	545	27.2.13	radius-server vsa send.....	563
26.5	授权配置命令.....	547	27.3	配置 TACACS+.....	564
26.5.1	aaa authorization	547	27.3.1	TACACS+概览	564
26.5.2	aaa authorization config- commands	547	27.3.2	TACACS+操作	565
26.5.3	aaa authorization reverse-acces.....	547	27.3.3	TACACS+配置示例	566
26.5.4	aaa authorizationaaa new-model	548	27.4	配置 Kerberos	569
26.5.5	authorization	548	27.4.1	Kerberos 概览.....	569
26.5.6	ppp authorization	548	27.4.2	使用 Kerberos 命令配置 KDC	570
26.6	AAA 记账配置	548	27.4.3	Kerberos 配置示例.....	571
26.6.1	记账的命名方法列表.....	548	27.5	Kerberos 命令	578
26.6.2	命名方法列表记账配置示例.....	549	27.5.1	clear kerberos creds.....	578
26.7	记账配置命令.....	551	27.5.2	connect	579
26.7.1	aaa accounting.....	551	27.5.3	kerberos clients mandatory	579
26.7.2	aaa accounting suppress null- username	552	27.5.4	kerberos credentials forward.....	579
26.7.3	aaa accounting update	552	27.5.5	kerberos instance map.....	580
26.7.4	accounting.....	552	27.5.6	kerberos local-realm.....	580
26.7.5	ppp accounting	553	27.5.7	kerberos preauth.....	580
26.7.6	show accounting.....	553	27.5.8	kerberos realm.....	580
第 27 章	安全服务器协议.....	555	27.5.9	kerberos server	580
27.1	配置 RADIUS.....	555	27.5.10	kerberos server	581
27.1.1	RADIUS 概览.....	555	27.5.11	kerberos srvtab entry.....	581
27.1.2	RADIUS 操作.....	556	27.5.12	kerberos srvtab remote.....	581
27.1.3	RADIUS 配置任务表.....	556	27.5.13	key config-key	581
27.1.4	RADIUS 配置示例.....	558	27.5.14	show kerberos creds.....	582
27.2	RADIUS 命令	560	27.5.15	telnet.....	582
27.2.1	aaa nas-port extended.....	561	第 28 章	流量过滤与防火墙.....	583
27.2.2	ip radius source-interface	561	28.1	访问控制列表.....	583
			28.1.1	关于访问控制列表.....	583

28.1.2 访问列表配置概述.....	584	29.2.4 定义加密映射并分配给接口.....	630
28.2 Cisco IOS 防火墙	587	29.2.5 生成 DSS 公钥及私钥示例	632
28.2.1 Cisco IOS 防火墙解决方案	587	29.2.6 交换 DSS 密钥示例	633
28.2.2 创建专用的防火墙.....	587	29.2.7 使 DES 加密算法有效示例	634
28.2.3 配制防火墙的其他指导原则.....	589	29.2.8 加密映射应用到接口示例.....	635
28.3 配置锁定和密钥的安全性（动态访问 列表）	590	29.2.9 改变加密访问列表限制示例.....	639
28.3.1 关于锁定和密钥.....	590	29.2.10 对 GRE 隧道加密配置示例.....	639
28.3.2 地址欺诈对锁定和密钥的威胁.....	591	29.2.11 对指定 ESA 进行加密配置.....	642
28.3.3 锁定和密钥对路由器性能影响.....	592	29.2.12 删除 DSS 密钥示例	644
28.3.4 配置锁定和密钥的前提条件.....	592	29.2.13 测试加密连接示例.....	646
28.3.5 配置锁定和密钥.....	592	29.3 配置 IPSec 网络安全	647
28.3.6 锁定和密钥配置技巧.....	593	29.3.1 IPSec 工作过程概述	648
28.3.7 检验锁定和密钥配置.....	594	29.3.2 IPSec 配置任务列表	649
28.3.8 锁定和密钥的维护.....	595	29.3.3 IPSec 配置示例	653
28.3.9 配置锁定和密钥示例.....	595	29.4 配置身份认证互操作性.....	654
28.3.10 锁定和密钥命令.....	597	29.4.1 CA 互操作性概述.....	654
28.4 配置 IP 会话过滤（反射访问列表）	599	29.4.2 CA 互操作性配置任务列表.....	654
28.4.1 关于反射访问列表.....	599	29.4.3 CA 互操作性配置示例.....	656
28.4.2 配置反射访问列表前的准备.....	601	29.5 配置 IKE 安全协议	660
28.4.3 配置反射访问列表.....	602	29.5.1 IKE 配置任务列表.....	661
28.4.4 配置反射访问列表示例.....	604	29.5.2 清除和诊断 IKE 连接.....	664
28.4.5 反射访问列表命令.....	607	29.5.3 IKE 配置示例	665
28.5 配置 TCP 截取（防止 DoS 攻击）	608	第 30 章 网络设备安全.....	667
28.5.1 关于 TCP 截取	608	30.1 探查目标.....	667
28.5.2 TCP 截取的配置任务列表	609	30.1.1 dig 工具	668
28.5.3 TCP 截取的配置范例	611	30.1.2 traceroute 工具.....	669
28.6 配置基于上下文的访问控制.....	611	30.1.3 IP 地址查询.....	670
28.6.1 CBAC 概述.....	611	30.2 自治系统查询（AS 查询）	671
28.6.2 CBAC 配置任务.....	615	30.2.1 traceoute 命令输出.....	671
28.6.3 CBAC 配置示例.....	619	30.2.2 ASN 信息 traceroute 输出.....	672
第 29 章 IP 安全和加密技术.....	625	30.2.3 show ip bgp 命令	672
29.1 IP 安全和加密技术概述	625	30.3 公共新闻组.....	673
29.1.1 安全特性.....	625	30.4 对网络服务进行探测.....	674
29.1.2 IPSec 和 Cisco 加密技术对比	626	30.4.1 nmap 工具.....	674
29.2 配置 Cisco 加密技术.....	627	30.4.2 识别操作系统.....	678
29.2.1 配置生成 DSS 公钥及私钥	627	30.4.3 响应信息识别 Cisco 产品	678
29.2.2 交换 DSS 公钥	628	30.5 OSI 模型第一层	679
29.2.3 启用 DES 加密算法	629	30.6 OSI 模型第二层	680
		30.7 对开关阵列网络进行嗅探.....	681

30.7.1	ARP 重定向	681	30.9.1	对 MIB 信息块的读/写	696
30.7.2	对广播通信进行嗅探	684	30.9.2	Cisco 设备口令弱加密算法	698
30.7.3	VLAN 跳跃	688	30.9.3	TFTP 下载	699
30.7.4	IRPAS 工具包和 CDP 工具	690	30.10	对路由分配协议的攻击手段	699
30.7.5	STP 扩散树协议攻击	691	30.10.1	RIP 欺诈	700
30.7.6	VTP,VLAN 主干协议攻击	691	30.10.2	IGRP 内部网关路由协议	702
30.8	OSI 模型的第三层	692	30.10.3	OSPF 先打开最短路径	703
30.8.1	tcpdump 嗅探器	693	30.10.4	BGP	704
30.8.2	dsniff 嗅探器	694	30.10.5	注射假造的 BGP 数据包	705
30.8.3	Ettercap 工具	696	30.11	用网络管理协议发动的攻击	708
30.9	配置失误	696	30.12	总结	709

第一部分

Windows 安全篇

本部分内容由 13 章组成，主要讨论应用最为广泛的 Windows 操作系统的安全问题。

Windows 操作系统最容易上手，但其存在的问题多多，无论是系统本身的漏洞，还是其提供的各种服务：上网有问题，打印有问题，输入有问题，开、关机有问题……但本书不准备讲这些，而是另辟蹊径，首先简单讨论一下 Windows 的安全及其防护，接着转移目标，讲如何攻击这个穷寇。

基于 Windows 系统网络方面的安全问题，主要从以下方面进行讨论：

- Windows 安全结构及其防御。
- 踩点、嗅探、扫描。
- 获取控制权。
- 服务攻击——IIS、SQL Server、Web。
- 扩大攻击范围。
- 后门处理。
- DoS 攻击。

SECTION 1

