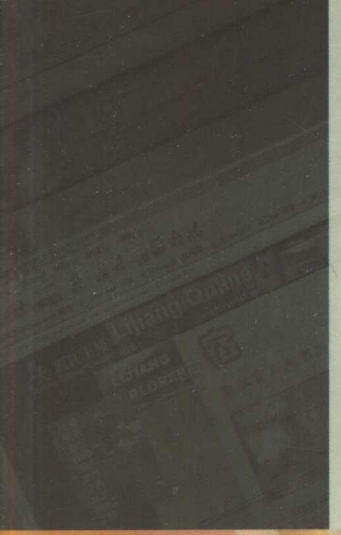

新编计算机网络安全实用丛书

Windows NT 系统安全管理

北京启明星辰信息技术有限公司 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

新编计算机网络安全实用丛书

Windows NT 系统安全管理

北京启明星辰信息技术有限公司　编著

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

内 容 简 介

本书系统讲述了 Windows NT 系统的安全管理，内容包括：Windows NT 安全基础，Windows NT 安全环境，Windows NT 账号安全管理，Windows NT 资源安全管理，Windows NT 网络安全管理，Internet 服务器 IIS 安全管理，Windows NT 安全工具，Windows 2000 安全特征，Windows NT/2000 安全常见问题及解答，评估 Windows NT/2000 的安全性以及 Windows NT/2000 的常见安全漏洞等。

图书在版编目(CIP)数据

Windows NT 系统安全管理/北京启明星辰信息技术有限公司编著 .—北京：电子工业出版社，2002.1
(新编计算机网络安全实用丛书)
ISBN 7-5053-6887-7

Ⅰ.W … Ⅱ.北 … Ⅲ.服务器—操作系统(软件)，Windows NT—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 062124 号

丛 书 名：新编计算机网络安全实用丛书
书　　名：Windows NT 系统安全管理
编　　著：北京启明星辰信息技术有限公司
责任编辑：贾贺　张旭
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京牛山世兴印刷厂
装 订 者：三河市路通装订厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18.5　字数：474 千字
版　　次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
书　　号：ISBN 7-5053-6887-7/TP·3913
印　　数：5000 册　　定价：28.00 元

丛 书 序

全球信息高速公路的建设给整个社会的科学与技术、经济与文化带来了巨大的推动与冲击，同时也给我们带来了许多挑战。Internet/Intranet 的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。随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的是信息安全问题日益突出。在人们对网络的优越性还没有完全接受的时候，黑客攻击开始肆虐全球的各大网站；而病毒制造者们也在各显其能，从 CIH 到爱虫，中毒者不计其数。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三个方面。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。新的攻击手法包括：通过网络监听获取网上用户的账号和密码；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账户进行攻击，如 Telnet Daemon、FTP Daemon、RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 Send Mail，采用 Debug、Wizard、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。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 的瘫痪等。可见我们面临的计算机网络系统的安全威胁日益严重。

那么，黑客攻击等威胁行为为什么经常能够得逞呢？主要原因在于 Internet/Intranet 系统内在的安全脆弱性；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较弱。

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。

这套新版的计算机网络安全实用丛书具有起点高、内容新、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、网络安全工具以及防范黑客攻击手段等内容的详细分析和介绍。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

目　录

第 1 章　Windows NT 安全基础 …… 1

1.1　Windows NT 安全体系 …… 2
1.1.1　Windows NT 安全模型构成 …… 2
1.1.2　登录过程 …… 3
1.1.3　本地安全权威 …… 3
1.1.4　安全账号管理器 …… 4
1.1.5　安全引用监视器 …… 5
1.2　Windows NT 和 C2 级安全 …… 6
1.2.1　C2 级安全及黄皮书 …… 6
1.2.2　Windows NT 的 C2 级安全进展 …… 8
1.2.3　现实世界中的安全问题 …… 9

第 2 章　Windows NT 安全环境 …… 10

2.1　对象和共享资源 …… 11
2.2　Windows NT 文件系统：FAT 和 NTFS …… 12
2.2.1　FAT 文件系统 …… 12
2.2.2　NTFS …… 13
2.2.3　通用 Internet 文件系统 …… 14
2.3　Windows NT 的域和工作组 …… 15
2.3.1　域 …… 15
2.3.2　域和委托 …… 16
2.3.3　工作组 …… 18
2.4　用户账号 …… 19
2.4.1　概览 …… 19
2.4.2　账号类型 …… 19
2.4.3　认证 …… 20
2.4.4　用户管理 …… 21
2.5　用户权利和权限 …… 21
2.5.1　用户权利 …… 21
2.5.2　用户权限 …… 23

2.6 用户组 …… 26
2.6.1 全局组 …… 26
2.6.2 本地组 …… 27
2.6.3 特别组 …… 27
2.7 注册表 …… 28
2.7.1 注册表概述 …… 29
2.7.2 注册表中的关键字 …… 30
2.7.3 注册表中的值 …… 31
2.7.4 注册表中关键字的结构 …… 32

第 3 章 Windows NT 账号安全管理 …… 38

3.1 Windows NT 的安装 …… 39
3.1.1 删除不必要的硬件 …… 39
3.1.2 建立 Windows NT 的单纯安装环境 …… 39
3.1.3 避免在同一机器上安装多个 Windows NT 系统 …… 40
3.1.4 进行必要的物理性保护 …… 40
3.1.5 删除 POSIX 和 OS/2 子系统 …… 40
3.1.6 禁止从其他操作系统启动 …… 40
3.1.7 采用 NTFS 文件系统 …… 41
3.1.8 域环境下的安装 …… 41
3.1.9 不要进行简单的拷贝安装 …… 41
3.2 用户账号的安全管理 …… 42
3.2.1 系统管理员账号管理 …… 42
3.2.2 来宾账号管理 …… 43
3.2.3 用户账号管理 …… 44
3.3 组账号的安全管理 …… 47
3.4 账号策略及密码的安全管理 …… 48
3.5 用户权利的安全管理 …… 50

第 4 章 Windows NT 资源安全管理 …… 52

4.1 文件系统与共享资源的安全管理 …… 53
4.1.1 共享文件和目录的安全管理 …… 53
4.1.2 本地文件和目录的安全管理 …… 56
4.1.3 常规和 Web 共享属性 …… 63
4.1.4 审核功能 …… 63
4.2 应用程序和用户主目录的安全管理 …… 65
4.2.1 应用程序的目录安全“管理措施” …… 65
4.2.2 主目录设置中的安全措施 …… 66

4.3 打印机的安全管理 …… 67
4.4 注册表的安全管理 …… 69
4.4.1 注册表的编辑功能 …… 69
4.4.2 注册表的安全管理 …… 71
4.4.3 注册表编辑器的限制使用 …… 77
4.4.4 注册表的审核 …… 78
4.5 审核策略和安全日志 …… 79
4.6 系统策略文件 …… 81
4.7 Windows NT 服务管理 …… 84
4.7.1 Windows NT 提供的基本服务 …… 85
4.7.2 服务的安全管理应注意的事项 …… 86
4.7.3 服务整理分析 …… 87
4.8 病毒与防范 …… 90
4.8.1 推荐的防病毒工具 …… 90
4.8.2 网络病毒防治 …… 92
4.9 备份与容错 …… 94

第 5 章 Windows NT 网络安全管理 …… 95

5.1 域委托关系的安全管理 …… 96
5.2 RAS 的安全管理 …… 97
5.2.1 RAS 的认证方法 …… 98
5.2.2 RAS 服务器的安全性 …… 99
5.2.3 使用回呼安全机制 …… 100
5.2.4 使用数据加密 …… 101
5.2.5 与 PPTP 服务协议一起建立 VPN 服务器 …… 102
5.3 Windows NT 的多协议环境 …… 104
5.4 Microsoft TCP/IP 安全设置 …… 107
5.5 企业级应用的安全性考虑 …… 109
5.5.1 企业级应用的安全保护 …… 109
5.5.2 数据的加密传输技术 …… 112
5.6 代理服务器与防火墙 …… 113
5.7 制定系统安全策略 …… 114
5.7.1 系统安全策略的制定应考虑的问题 …… 114
5.7.2 安全手册的大纲 …… 115
5.7.3 灾难恢复计划 …… 115

第 6 章 Internet 服务器 IIS 的安全管理 …… 117

6.1 IIS 4.0 特性 …… 118

6.1.1 更容易地搭建和管理 Web 服务器 …… 118
6.1.2 符合 Internet 标准的服务 …… 120
6.1.3 简单可靠的 Web 应用开发和发布环境 …… 120
6.1.4 基于标准的数据访问方式 …… 121
6.1.5 集成的认证和安全举措 …… 121
6.1.6 丰富的内容管理和控制 …… 122
6.1.7 灵活的 FTP 服务 …… 123
6.2 IIS 4.0 安全性设置 …… 123
6.2.1 HTTP 服务的安全特征设置 …… 123
6.2.2 FTP 服务的安全特征设置 …… 131
6.3 IIS 4.0 服务器的安全管理—— 一揽子解决方案 …… 134
6.3.1 整理设备系统的信息清单 …… 135
6.3.2 准备工作 …… 135
6.3.3 对 Windows NT 4.0 系统进行安全性设置 …… 136
6.3.4 IIS 4.0 的安全性设置 …… 141
6.3.5 相关的安全措施 …… 147

第 7 章 Windows NT 安全工具 …… 152

7.1 Windows NT 安全突破工具 …… 153
7.1.1 NTFSDOS.exe …… 153
7.1.2 NTRecover 和 Remote Recovery …… 153
7.1.3 NTLocksmith …… 155
7.1.4 ERD Commander 2000 …… 155
7.1.5 L0phtCrack …… 155
7.1.6 PWDump Utility Tool/Hack …… 155
7.1.7 PWDump …… 156
7.1.8 NTOMax …… 156
7.1.9 NTOtools …… 157
7.1.10 NT4ALL …… 158
7.1.11 BackOrifice …… 158
7.2 Windows NT 平台上的扫描分析工具 …… 159
7.2.1 ISS SAFEsuite …… 159
7.2.2 Somarsoft …… 160
7.2.3 NTO Scanner …… 160
7.2.4 WSPingPro …… 161
7.2.5 Desktop Sentry …… 162
7.2.6 BLAST …… 162
7.2.7 NetXray 和 Sniffer 协议分析仪和网络监控软件 …… 162

7.2.8 自由软件类协议分析仪：Analyzer 和 Ethereal …… 166
7.2.9 WebBoy，PacketBoy 和 EtherBoy …… 167
7.2.10 WebSense Enterprise …… 167
7.2.11 Kane Security Analyst …… 167
7.3 Windows NT 平台上的入侵检测系统 …… 168
7.3.1 Snort …… 168
7.3.2 Checkpoint RealSecure …… 168
7.3.3 TripWire …… 169
7.3.4 Intact 变更检测系统 …… 169
7.3.5 ISS RealSecure Manager，Network Sensor，OS Sensor 和 Server Sensor …… 169
7.3.6 SecureNet Pro 和 SecureNet Enterprise …… 170
7.3.7 BlackICE Defender …… 170
7.4 Windows NT 的审核追踪工具 …… 171
7.4.1 SENTRY …… 171
7.4.2 EventSLog …… 171
7.4.3 Forensic Toolkit …… 171
7.4.4 NTLast …… 172
7.4.5 WinAuDlog …… 172
7.4.6 PsLogList …… 172
7.5 基于 Windows NT 的防火墙 …… 172
7.5.1 Raptor Eagle …… 173
7.5.2 Firewall-1 …… 173
7.5.3 Microsoft Proxy 2.0 代理服务器 …… 173
7.5.4 TIS Gauntlet 防火墙 …… 174
7.5.5 Guardian 防火墙 …… 174
7.5.6 ZoneLabs 的 ZoneAlarm 防火墙 …… 174
7.5.7 Sygate 防火墙 …… 175

第 8 章 Windows 2000 安全特性 …… 177

8.1 Windows 2000 操作系统简介 …… 178
8.1.1 Windows 2000 专业版的主要特点 …… 179
8.1.2 Windows 2000 服务器版和高级服务器版的特点 …… 181
8.2 Windows 2000 和 Windows NT 的安全特征区别 …… 187
8.3 Windows NT 升迁的安全性考虑 …… 189
8.4 Windows 2000 的安全特性 …… 191
8.4.1 Windows 2000 的活动目录 …… 191
8.4.2 EFS 文件系统 …… 193
8.4.3 Kerberos 认证 …… 194

8.4.4 PKI 体系结构 …… 195
8.5 Windows 2000 的缺省安全访问控制设置 …… 197
8.5.1 Power Users 和 Users 文件系统的默认访问控制 …… 198
8.5.2 Power Users 和 Users 注册表项的默认访问控制 …… 201
8.6 Windows 2000 的缺省用户权利设置 …… 203
8.7 Windows 2000 缺省的组成员 …… 205
8.8 IIS 5.0 的安全配置简介 …… 207
8.8.1 应用 IIS 5.0 的安全配置清单 …… 208
8.8.2 IIS 5.0 的安全配置的额外需求 …… 208
8.8.3 及时获取补丁程序和应用适当的工具 …… 209

第 9 章 Windows NT/2000 安全常见问题及解答 …… 210

9.1 安全基础 …… 211
9.1.1 服务包 …… 211
9.1.2 伪装 …… 211
9.1.3 SID，Permissions，ACE，ACL，SRM，LSA，SAM …… 211
9.1.4 访问令牌 …… 211
9.1.5 Active Directory，PKI，Kerberos …… 212
9.1.6 IPSec …… 212
9.1.7 安全通道 …… 212
9.1.8 使 Windows NT 计算机达到 C2 级安全 …… 212
9.1.9 有否基于 Windows NT 的病毒，Windows NT 对其他病毒是否敏感 …… 213
9.1.10 使客户机更安全而不受到用户的入侵 …… 214
9.1.11 页文件是否能包含敏感数据 …… 214
9.1.12 Windows NT 的口令是否安全 …… 214
9.1.13 特洛伊木马病毒 …… 215
9.2 文件系统和共享的安全性 …… 215
9.2.1 刚安装一个服务包，文件权限就被改变的原因 …… 216
9.2.2 没有授权的用户可删除文件的原因 …… 216
9.2.3 能否从其他操作系统中读或写数据到 NTFS 磁盘 …… 216
9.2.4 CIFS …… 216
9.2.5 能否使默认共享资源不共享 …… 216
9.2.6 文件共享是否存在错误 …… 216
9.2.7 空会话 …… 217
9.2.8 控制用户使用的磁盘空间 …… 217
9.3 注册表的安全性 …… 217
9.3.1 HKEY_LOCAL_MACHINE 键的设置 …… 217
9.3.2 在网络上是否可访问注册表 …… 217

9.3.3 意义重大的键值 …… 217
9.4 Windows NT 的网络安全 …… 218
9.4.1 Windows NT 是否易受 SYN Flood 袭击 …… 218
9.4.2 Windows NT 机器有没有可能利用包过滤 …… 218
9.4.3 让 NBT 通过防火墙必须使用的端口 …… 218
9.4.4 认证代码 …… 219
9.4.5 使用 SNMP 应考虑的因素 …… 219
9.4.6 显示与 Windows NT 系统联接的服务程序的 TCP/ UDP 端口 …… 219
9.4.7 用 Ping 攻击 Windows NT 系统是否容易 …… 219
9.4.8 RPC 服务程序的漏洞 …… 220
9.4.9 DHCP …… 220
9.4.10 OOB 攻击 …… 220
9.4.11 Windows NT 处理被分割的 IP 数据包 …… 220
9.4.12 远程访问服务器安全性 …… 220
9.4.13 开放式数据库互联安全性 …… 221
9.5 日志和审核功能 …… 221
9.5.1 Windows NT 上的系统日志功能 …… 221
9.5.2 能否把日志移到另外的分区上 …… 221
9.5.3 能否给其他人授权来查看或改变日志文件 …… 221
9.5.4 所有用户能进行的操作不全显示在日志中的原因 …… 221
9.6 Windows NT 中的加密 …… 222
9.6.1 Crypto API …… 222
9.6.2 在美国范围之外能否使用美国境内使用的密码 …… 222
9.6.3 Windows 2000 提供的加密措施 …… 222
9.7 Service Packs 对安全性的修正 …… 222
9.7.1 Windows NT SP4 的增强的安全性 …… 222
9.7.2 Windows NT SP6a 和 PostFix 的安全性的修正 …… 223
9.7.3 C2 Update 安全性修正 …… 223
9.8 Windows NT/2000 安全性问题综合问答 …… 224
9.8.1 在远程服务的安装过程中，如何确保用户设置管理员密码 …… 224
9.8.2 计算机从睡眠状态中返回时不会提示输入密码的原因 …… 224
9.8.3 用户从命令行修改密码的方法 …… 225
9.8.4 恢复 NT 结构的缺省许可控制 …… 225
9.8.5 安全事件 ID 的定义列表 …… 226
9.8.6 阻止 Windows 2000 升级覆盖某些特定的安全设置 …… 228
9.8.7 改变 Kerberos 的票证的生存周期 …… 229
9.8.8 密钥分配中心与客户之间的长期密钥的分配 …… 231
9.8.9 安全配置和分析管理单元的使用 …… 231

9.8.10 保护密码不受密码监视、分析等攻击工具的威胁 …… 232
9.8.11 在 Null 会话访问、远程过程调用和进程间通信中信息的列举 …… 232
9.8.12 检测被破解的用户密码 …… 233
9.8.13 可以及时了解最新安全信息的安全邮件列表 …… 234
9.8.14 系统密钥保护用户的密码 …… 235
9.8.15 拷贝文件使之保持原有的安全和许可控制权限的方法 …… 236
9.8.16 使系统在安全日志满时停止运行 …… 236
9.8.17 在关闭系统时清理 Pagefile.sys 文件的方法 …… 236
9.8.18 加强对密码过滤，促使用户使用安全密码 …… 237
9.8.19 跟踪在系统崩溃时发生的事情 …… 237
9.8.20 使系统在崩溃之后自动重启 …… 238
9.8.21 启用对 SAM 的审计 …… 238
9.8.22 对共享系统的对象加强保护 …… 239
9.8.23 限制匿名账户对对象的访问 …… 239
9.8.24 启用 SMB 签名 …… 239
9.8.25 加强 Internet 的访问控制策略 …… 240
9.8.26 启用审核功能 …… 240
9.8.27 查阅、清除安全日志 …… 240
9.8.28 得到关于事件查看器的更多信息 …… 241
9.8.29 得到更多关于 NT 安全问题的信息 …… 241

第 10 章 Windows NT/2000 的安全性评估 …… 242

10.1 C2 级安全标准 …… 243
10.1.1 安全系统标准：C2 …… 243
10.1.2 C2 级安全性需求定义 …… 244
10.1.3 Windows NT 的 C2 级安全性 …… 244
10.1.4 解决现实世界的问题 …… 245
10.1.5 Windows NT 系统环境的安全设计 …… 246
10.2 审核系统 C2 级安全兼容性 …… 246
10.3 C2 级标准评估 …… 247
10.3.1 账号策略和限制 …… 247
10.3.2 用户账号 …… 248
10.3.3 组策略 …… 248
10.3.4 管理员账号和管理员组 …… 249
10.3.5 来宾账号和一般用户组 …… 250
10.3.6 用户权限 …… 250
10.3.7 文件系统的访问许可权限和共享 …… 251
10.3.8 Windows NT 病毒和特洛伊木马控制程序 …… 252

10.3.9 审核和事件日志 …… 252
10.3.10 容错、备份和不间断电源 …… 253
10.4 Windows 2000 的安全性标准评估 …… 253

附录 A Windows NT/2000 的常见安全漏洞 …… 255

A.1 Windows NT 的部分安全漏洞 …… 256
A.1.1 SAM 复制问题 …… 256
A.1.2 紧急修复盘与 SAM 复制 …… 257
A.1.3 SAM 与 SMB 问题 …… 257
A.1.4 特洛伊木马与 SAM …… 258
A.1.5 获得 Administrator 级别的访问权问题 …… 258
A.1.6 另一个 Administrator 级别的访问权 …… 258
A.1.7 某些系统程序的不适当使用 …… 259
A.1.8 所有用户可能联接管理系统的共享资源 …… 259
A.1.9 无限制尝试联接 …… 259
A.1.10 账户的加锁问题 …… 259
A.1.11 自动解锁问题 …… 259
A.1.12 最近一次注册的用户名显示问题 …… 260
A.1.13 口令问题 …… 260
A.1.14 Windows NT 口令可能被非 NT 平台更改 …… 260
A.1.15 管理员有能力从非安全的工作站上进行远程登录 …… 260
A.1.16 NT 的注册表的默认权限设置有很多不当之处 …… 261
A.1.17 有可能远程访问 NT 平台上的注册表 …… 261
A.1.18 NT 机器允许在安装时输入空白口令 …… 261
A.1.19 通过访问其他的并存操作系统有可能绕过 NTFS 的安全设置 …… 261
A.1.20 文件句柄可能从内存中被读取到，用来访问文件，而无需授权 …… 262
A.1.21 默认权限设置问题 …… 262
A.1.22 打印机问题 …… 262
A.1.23 通过 FTP 有可能进行无授权的文件访问 …… 262
A.1.24 基于 NT 的文件访问权限对于非 NT 文件系统不可读 …… 262
A.1.25 Windows NT 文件安全权限的错误设置带来的潜在的危险 …… 263
A.1.26 标准的 NTFS “读”权限意味着可以同时“读”和“执行” …… 263
A.1.27 Windows NT 总是不正确地执行“删除”权限 …… 263
A.1.28 默认组的权利问题 …… 263
A.1.29 NT 的进程定期处理问题 …… 263
A.1.30 账户组资格问题 …… 264
A.1.31 Everyone 组的默认权利问题 …… 264
A.1.32 事件管理器中 Security Log 的设置问题 …… 264

A.1.33 审计文件是不完全的 …… 264
A.1.34 Security Log 不是全部集成的 …… 265
A.1.35 屏幕保护程序问题 …… 265
A.1.36 查询已注册用户名的问题 …… 265
A.1.37 SATAN 扫描崩溃 …… 265
A.1.38 Red Button …… 265
A.1.39 Ping Death 现象 …… 266
A.1.40 Out-of-Band 问题 …… 266
A.1.41 与浏览器和 NT 机器有关的安全漏洞 …… 267
A.2 Windows 2000 的部分安全漏洞 …… 267
A.2.1 ActiveX 参数验证漏洞 …… 267
A.2.2 NetMon 协议分析漏洞 …… 267
A.2.3 HyperTerminal 缓冲区溢出漏洞 …… 268
A.2.4 非法 RPC 数据包漏洞 …… 268
A.2.5 LPC 和 LPC 端口溢出漏洞 …… 268
A.2.6 NetMeeting 桌面共享漏洞 …… 268
A.2.7 简体中文输入法编辑器识别漏洞 …… 268
A.2.8 静态映像权限（Still Image Privilege）提升漏洞 …… 269
A.2.9 Telnet 客户端 NTLM 认证漏洞 …… 269
附录 B 术语表 …… 270
附录 C Windows NT 安全资源链接 …… 274
附录 D 缩略语参考对照表 …… 276

第 1 章

Windows NT 安全基础

本章概要：

- 介绍 Windows NT 的安全体系结构，阐述登录过程、本地安全权威、安全账号管理器和安全引用监视器等安全组件；
- 介绍 Windows NT 的 C2 级安全性兼容状况以及黑客常用的网络攻击手段。

Windows NT 4.0 大体上分为两个版本：工作站版（Workstation）和服务器版（Server 和 Server Enterprise Edition）。两者具有同样的核心特性、安全系统和网络设计。服务器版侧重于网络文件、数据库的服务和应用，其特殊结构也是为多用户设计的；工作站版是完全 32 位的操作系统，可以给某些高级用户提供更优越的处理能力来克服 Windows 95 和 Windows 98 的一些缺陷。在 Windows NT 的安全子系统中，Windows NT 服务器版和 Windows NT 工作站版的主要区别是：Windows NT 服务器版的用户账户数据库可用于 Windows NT 的整个域，而 Windows NT 工作站版的账户数据库只能本地使用。在讨论安全问题时，我们主要以 Windows NT Server 为目标，Windows NT Workstation 在很多方面可借鉴于此。

1.1 Windows NT 安全体系

Windows NT 具有模块化的设计结构。Windows NT 的操作系统由一组软件模块构成，它们被称为执行程序服务（Executive Service），运行在内核模式（Kernel Mode）下。在内核模式之上是用户模式，用户模式由非特权的服务组成，称为保护子系统（Protected Subsystem），它们的启动由用户来决定。

基本上，内核模式组件是必需的，并且能够组成一个自成体系的操作系统；用户模式组件运行在核心之上，可利用它的服务。这就是业界常说的微内核（Microkernel）结构。

Windows NT 的安全性根植于 Windows NT 的核心（Kernel）层，它在各层次提供一致的安全模型。Windows NT 安全模型是 Windows NT 操作系统中密不可分（Integral）的子系统，它影响着整个 Windows NT 操作系统，安全子系统控制着对象的访问（如文件、内存、打印机、驱动器乃至窗口等）。在 Windows NT 中，对象实质是指一系列信息集合体，与程序设计上的概念类似，它封装了数据及处理过程，使之成为一个可广泛引用的整体。当对象用于网络环境中时，称之为资源；当对象在网络上共享时，称之为共享资源。

1.1.1 Windows NT 安全模型构成

Windows NT 的安全系统提供了对事件的审核和详细的跟踪（Auditing And Logging）手段来监控网络上资源的访问和应用。从一定的角度来讲，Windows NT 应该比其他流行的操作系统更安全，当然前提是你了解 Windows NT 的安全体系与规范，并付诸实践。

Windows NT 的安全模型由几个关键性的部分构成，每一个部分在整个安全模型中都不可或缺。它们是：登录过程（Logon Process，LP）、本地安全权威（Local Security Authority，LSA）、安全账号管理器（Security Account Manager，SAM）和安全引用监视器（Security Reference Monitor，SRM），它们一起耦合成了 Windows NT 的安全子系统。下面分别对各个部分予以扼要的介绍。