

<<Windows 2000 Server中>>

图书基本信息

书名：<<Windows 2000 Server中文版配置手册>>

13位ISBN编号：9787115088826

10位ISBN编号：7115088829

出版时间：2000年12月1日

出版时间：人民邮电出版社

作者：Curt Simmons

页数：343

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<Windows 2000 Server中>>

### 内容概要

本书详细介绍了Windows 2000 Server 中文版的配置方法。

## 书籍目录

第一部分 概述	1
第1章 网络安全简介	3
1.1 攻击、服务和机制	4
1.1.1 服务	5
1.1.2 机制	6
1.1.3 攻击	6
1.2 安全攻击	7
1.2.1 被动攻击	8
1.2.2 主动攻击	8
1.3 安全服务	9
1.3.1 保密性	9
1.3.2 验证	9
1.3.3 完整性	10
1.3.4 不可否认性	10
1.3.5 访问控制	10
1.3.6 可用性	10
1.4 网络安全模型	10
1.5 Internet标准和RFC	12
1.5.1 Internet社团	12
1.5.2 RFC的发布	13
1.5.3 标准化进程	13
1.5.4 非标准跟踪文档	14
1.6 Internet和Web资源	14
1.6.1 本书的Web站点	15
1.6.2 其他网络站点	15
1.6.3 UNENET新闻组	15
1.6.4 推荐读物	16
第二部分 密码术	17
第2章 常规加密和消息的保密性	19
2.1 常规加密原则	19
2.1.1 密码术	20
2.1.2 密码分析	20
2.1.3 Feistel的密码结构	22
2.2 常规加密算法	23
2.2.1 数据加密标准	24
2.2.2 三重DEA	27
2.2.3 高级加密标准	28
2.2.4 其他对称分组密码	29
2.3 密码分组操作方式	31
2.3.1 加密分组的链方式	31
2.3.2 密码反馈方式	33
2.4 加密设备的位置	33
2.5 密钥分布	36
2.6 习题	37
第3章 公钥密码和消息验证	39

## &lt;&lt;Windows 2000 Server中&gt;&gt;

- 3.1 消息验证的方法 39
  - 3.1.1 使用常规加密方法的验证 39
  - 3.1.2 没有加密的消息验证 39
  - 3.1.3 消息验证码 40
  - 3.1.4 单向哈希函数 41
- 3.2 安全哈希函数和HMAC 42
  - 3.2.1 哈希函数的需求 42
  - 3.2.2 简单哈希函数 43
  - 3.2.3 SHA-1安全哈希函数 45
  - 3.2.4 其他安全哈希函数 46
  - 3.2.5 HMAC 48
- 3.3 公钥密码术规则 50
  - 3.3.1 公钥加密的结构 51
  - 3.3.2 公钥密码系统的应用 52
  - 3.3.3 公钥密码的要求 53
- 3.4 公钥密码算法 53
  - 3.4.1 RSA公钥加密算法 54
  - 3.4.2 Diffie-Hellman密钥交换 56
  - 3.4.3 其他公钥密码算法 58
- 3.5 数字签名 59
- 3.6 密钥管理 59
  - 3.6.1 数字证书 60
  - 3.6.2 公钥密码的保密密钥分发 61
- 3.7 习题 61
- 3.8 背景知识—素数和模运算 63
  - 3.8.1 素数和相对素数 63
  - 3.8.2 模运算 65
- 第三部分 网络安全应用 67
- 第4章 身份验证应用 69
  - 4.1 Kerberos 69
    - 4.1.1 动机 70
    - 4.1.2 Kerberos 版本4 71
    - 4.1.3 Kerberos版本5 79
  - 4.2 X.509身份验证服务 83
    - 4.2.1 证书 83
    - 4.2.2 身份验证过程 87
    - 4.2.3 X.509版本3 89
  - 4.3 习题 90
  - 4.4 背景知识--Kerberos加密技术 91
    - 4.4.1 口令到密钥的转换 91
    - 4.4.2 传播密码分组链模式 93
- 第5章 电子邮件安全 95
  - 5.1 PGP 95
    - 5.1.1 表示法 96
    - 5.1.2 操作说明 96
    - 5.1.3 密钥和密钥环 100
    - 5.1.4 公钥管理 106

## &lt;&lt;Windows 2000 Server中&gt;&gt;

- 5.2 S/MIME 109
  - 5.2.1 RFC 822 110
  - 5.2.2 多用Internet邮件扩展 110
  - 5.2.3 S/MIME的功能 116
  - 5.2.4 S/MIME的消息 118
  - 5.2.5 S/MIME证书处理 122
  - 5.2.6 增强的安全服务 123
- 5.3 使用ZIP压缩数据 124
  - 5.3.1 压缩算法 125
  - 5.3.2 解压缩算法 126
- 5.4 基数64转换 126
- 5.5 PGP随机数生成 127
  - 5.5.1 真随机数 128
  - 5.5.2 伪随机数 128
- 5.6 习题 130
- 第6章 IP安全 131
  - 6.1 IP安全概况 131
    - 6.1.1 IPSec的应用 132
    - 6.1.2 IPSec的优势 132
    - 6.1.3 路由应用 133
  - 6.2 IP安全体系结构 133
    - 6.2.1 IPSec文档 134
    - 6.2.2 IPSec服务 135
    - 6.2.3 安全关联 135
    - 6.2.4 传输和隧道模式 138
  - 6.3 验证报头 139
    - 6.3.1 反重放服务 140
    - 6.3.2 完整性检查值 140
    - 6.3.3 传输和隧道模式 141
  - 6.4 封装安全有效载荷 143
    - 6.4.1 ESP格式 143
    - 6.4.2 加密和验证算法 144
    - 6.4.3 填充 144
    - 6.4.4 传输和隧道模式 144
  - 6.5 组合式安全关联 147
    - 6.5.1 验证加保密性 148
    - 6.5.2 SA的基本组合 148
  - 6.6 密钥管理 150
    - 6.6.1 Oakley密钥确定协议 150
    - 6.6.2 ISAKMP 153
  - 6.7 习题 157
  - 6.8 背景知识--网络互连和Internet协议 158
    - 6.8.1 IP的作用 158
    - 6.8.2 IPv4 160
    - 6.8.3 IPv6 161
    - 6.8.4 IPv6报头 161
- 第7章 Web安全 165

## &lt;&lt;Windows 2000 Server中&gt;&gt;

- 7.1 Web安全问题 165
  - 7.1.1 Web安全威胁 166
  - 7.1.2 Web通信流安全的实现 166
- 7.2 安全套接层和传输层安全 167
  - 7.2.1 SSL体系结构 167
  - 7.2.2 SSL记录协议 169
  - 7.2.3 改变密码规格协议 171
  - 7.2.4 警告协议 172
  - 7.2.5 握手协议 172
  - 7.2.6 密码计算 177
  - 7.2.7 传输层安全 178
- 7.3 安全电子交易 182
  - 7.3.1 SET 概述 182
  - 7.3.2 双重签名 184
  - 7.3.3 支付过程 186
- 7.4 习题 190
- 第8章 网络管理安全 191
  - 8.1 SNMP的基本概念 191
    - 8.1.1 网络管理体系结构 191
    - 8.1.2 网络管理协议体系结构 192
    - 8.1.3 代理 194
    - 8.1.4 SNMPv2 194
  - 8.2 SNMPv1的共同体机制 198
    - 8.2.1 共同体和共同体名称 198
    - 8.2.2 验证服务 199
    - 8.2.3 访问策略 199
    - 8.2.4 代理服务 200
  - 8.3 SNMPv3 200
    - 8.3.1 SNMP体系结构 201
    - 8.3.2 消息处理和用户安全模型 207
    - 8.3.3 基于视图的访问控制 215
  - 8.4 习题 219
- 第四部分 系统安全 223
- 第9章 入侵者和病毒 225
  - 9.1 入侵者 225
    - 9.1.1 入侵技术 226
    - 9.1.2 口令保护 228
    - 9.1.3 口令的弱点 228
    - 9.1.4 访问控制 231
    - 9.1.5 口令选择策略 232
    - 9.1.6 入侵检测 236
  - 9.2 病毒和相关威胁 243
    - 9.2.1 恶意程序 244
    - 9.2.2 病毒的性质 247
    - 9.2.3 病毒的类型 250
    - 9.2.4 宏病毒 251
    - 9.2.5 反病毒方法 252

9.2.6 反病毒高级技术	253
9.3 习题	255
第10章 防火墙	257
10.1 防火墙设计原则	257
10.1.1 防火墙的特点	258
10.1.2 防火墙的种类	259
10.1.3 防火墙配置	263
10.2 可信系统	265
10.2.1 数据访问控制	265
10.2.2 可信系统的概念	266
10.2.3 防御特洛伊木马程序	268
10.3 习题	270
附录A 本书引用的RFC	271
附录B 网络安全课程教学计划	273
B.1 研究计划	273
B.2 编程计划	274
B.3 读书/报告作业	274
附录C 术语表	275

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>