

<<Windows2000安全技术>>

图书基本信息

书名：<<Windows2000安全技术>>

13位ISBN编号：9787302050858

10位ISBN编号：7302050856

出版时间：2002-1

出版时间：清华大学出版社

作者：(美)roberta bragg

页数：398

字数：635

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>

<<Windows2000安全技术>>

内容概要

书从实用的角度出发, 全面地介绍了关于Windows 2000的信息系统安全, 介绍了大量有关Windows 2000安全的工具、特性及结构方面的信息。

全书分四部分, 分别介绍了安全的基本概念与定义、操作系统安全的保护、本地网络安全的保护以及实际网络安全的保护。

内容包括: 密码学简介、相关的安全协议、公钥体系及其建立过程、Kerberos、加密文件系统、NTFS、安全策略及安全工具; 此外, 还介绍了Wi

<<Windows2000安全技术>>

书籍目录

第1部分 概念与定义

第1章 安全的基本概念

1.1 安全的三个“A”

1.1.1 认证

1.1.2 授权

1.1.3 审核

1.2 安全策略

1.3 计算机安全的目标

1.3.1 完整性

1.3.2 控制

1.3.3 可用性

1.4 其他安全术语

1.5 更多的信息

1.6 小结

第2章 密码学介绍

2.1 历史背景

2.2 现代的加密算法

2.2.1 对称密钥密码系统

2.2.2 非对称密钥密码系统

2.2.3 公钥体系

2.2.4 数字签名

2.2.5 数字编码

2.3 常用加密算法

2.3.1 DES

2.3.2 已被提议用来替代DES的算法

2.3.3 Ron Rivest算法

2.3.4 CAST-128

2.3.5 Diffie-Hellman

2.3.6 RSA

2.3.7 散列函数

2.3.8 将来的希望：椭圆曲线密码系统

2.4 攻击方法

2.5 更多的信息

2.6 小结

第3章 新的协议、产品及API

3.1 与Web相关的协议

3.1.1 安全套接字层和HTTPS

3.1.2 传输层安全协议 (RFC 2246)

3.2 远程访问协议

3.2.1 串行线路Internet协议 (RFC 1055)

3.2.2 点到点协议 (RFC 1661)

3.2.3 口令认证协议

3.2.4 质询-握手认证协议 (RFC 1994)

3.2.5 Microsoft-CHAP版本1 (RFC 2433) 和版本2 (RFC 2759)

3.2.6 点到点隧道协议 (RFC 2637)

<<Windows2000安全技术>>

3.2.7 Microsoft点到点加密机制 (MPPE)

3.2.8 第二层隧道协议 (RFC 2661)

3.3 IPSec

3.3.1 密钥管理

3.3.2 安全策略数据库

3.3.3 IP栈实现

3.3.4 通信安全协议：AH与ESP

3.3.5 SA束

3.3.6 性能问题

3.4 DHCP与动态DNS之间的安全通信 (RFC 2535, 2136, 2137)

3.4.1 公钥／私钥的实现 (RFC 2535)

3.4.2 通过Kerberos 5的DHCP认证和使用DHCP的DNS安全更新

3.5 Microsoft独有的API和安全协议

3.5.1 服务器控制的加密系统

3.5.2 CryptoAPI

3.5.3 认证码

3.5.4 安全支持提供者接口 (SSPI)

3.5.5 LM、NTLM、NTLMv2

3.6 更多的信息

3.7 小结

第4章 公钥体系 (PKI)

4.1 证书颁发机构

4.2 注册颁发机构

4.3 证书与密钥

4.3.1 X.509证书

4.3.2 简单公钥体系

4.3.3 PGP

4.3.4 证书验证

4.4 证书仓库

4.5 证书吊销列表

4.5.1 吊销列表的选项

4.6 证书信任模型

4.6.1 层次型信任模型

4.6.2 分布式信任

4.6.3 Web信任

4.6.4 用户信任

4.6.5 交叉证明

4.7 客户与客户软件

4.8 PKI过程

4.8.1 时间问题

4.8.2 密钥／证书生存周期

4.8.3 产生

4.9 更多的怕息

4.10 小结

第5章 Kerberos基础

5.1 Kerberos基础

5.1.1 登录认证：认证服务交换

<<Windows2000安全技术>>

- 5.1.2 获得一个票证：票证授予服务交换
- 5.1.3 访问资源：客户／服务器认证交换
- 5.2 Kerberos组成和算法
 - 5.2.1 组件
 - 5.2.2 Kerberos算法
- 5.3 Kerberos信任路径
- 5.4 加密和校验和
- 5.5 更多的信息
- 5.6 小结
- 第2部分 保护操作系统的安全
- 第6章 从头开始考虑安全
 - 6.1 用户和组
 - 6.1.1 独立系统上的用户和组
 - 6.1.2 隐式的用户权限
 - 6.2 活动目录介绍
 - 6.2.1 活动目录结构
 - 6.2.2 域模式
 - 6.2.3 组作用域
 - 6.2.4 域中默认的组
 - 6.2.5 隐式组或系统组
 - 6.3 权限和特权
 - 6.3.1 用户和组管理工具
 - 6.4 Windows 2000 NTFS
 - 6.4.1 文件权限
 - 6.4.2 默认安全设置
 - 6.4.3 资源访问
 - 6.4.4 特殊权限
 - 6.4.5 与以前NTFS版本的区别
 - 6.4.6 共享文件夹的发布：模糊中会有安全性吗？
 - 6.5 默认注册表权限
 - 6.6 软保护和Windows文件保护
 - 6.6.1 软保护
 - 6.6.2 Windows文件保护
 - 6.7 Windows 2000加密文件系统
 - 6.7.1 EFS基础
 - 6.7.2 加密文件系统如何工作
 - 6.7.3 提供证书颁发机构的好处
 - 6.7.4 Cipher命令
 - 6.7.5 恢复策略和EFS管理
 - 6.8 最佳操作
 - 6.9 更多的信息
 - 6.10 小结
- 第7章 用户认证
 - 7.1 LM与NTLM认证
 - 7.2 Windows 2000中的Kerberos
 - 7.2.1 Kerberos对Windows 2000的益处

<<Windows2000安全技术>>

- 7.2.2 活动目录的作用
- 7.2.3 认证的第1步：获取登录会话密钥
- 7.2.4 认证的第2步：TGS交换——获取特定服务器的票证
- 7.2.5 认证的第3步：使用会话票证来获准进入——CS交换
- 7.2.6 票证
- 7.2.7 DNS名字解析
- 7.2.8 域间的活动
- 7.2.9 Kerberos与WinLogon服务的集成
- 7.2.10 使用Kerberos票证来得到访问控制信息
- 7.2.11 Kerberos与服务账号的集成
- 7.2.12 公钥的Kerberos扩展
- 7.3 网络登录的过程
- 7.4 在Windows 2000中使用智能卡
 - 7.4.1 Microsoft的方法
 - 7.4.2 基本组件
 - 7.4.3 安装与使用智能卡
 - 7.4.4 使用智能卡进行Windows 2000登录
 - 7.4.5 智能卡与远程访问
- 7.5 更多的信息
- 7.6 小结
- 第8章 生存周期选择
 - 8.1 为了改进安全性而在安装时的注意事项
 - 8.1.1 升级与全新安装之间的区别
 - 8.1.2 保护升级安装的安全
 - 8.1.3 已升级的Windows NT主域控制器（PDC）上的活动目录
 - 8.2 维护
 - 8.2.1 选择安全的应用程序：Windows 2000应用程序标志的标准
 - 8.2.2 使用和维护安全策略
 - 8.2.3 备份
 - 8.3 系统恢复：修复概述
 - 8.3.1 在安全模式中启动
 - 8.3.2 紧急修复过程
 - 8.3.3 使用最后一次正确配置
 - 8.3.4 使用Windows 2000修复控制台
 - 8.3.5 系统文件检查器
 - 8.4 死亡与分解
 - 8.5 最佳操作
 - 8.6 更多的信息
 - 8.7 小结
- 第9章 安全工具
 - 9.1 使用安全配置和分析工具集
 - 9.1.1 安全模板
 - 9.1.2 安全配置和分析
 - 9.1.3 使用secedit工具
 - 9.1.4 使用安全配置工具集进行审核
 - 9.2 组策略
 - 9.2.1 组策略工具

<<Windows2000安全技术>>

- 9.2.2 GPO组件
- 9.2.3 与组策略编辑器一起使用安全配置和分析
- 9.3 支持工具
- 9.4 Resource Kit工具
- 9.4.1 与审核相关的工具
- 9.4.2 组策略工具
- 9.4.3 用户管理工具
- 9.4.4 管理工具
- 9.4.5 注册表工具
- 9.4.6 DACL
- 9.5 选择要使用的工具
- 9.6 最佳操作
- 9.7 更多的信息
- 9.8 小结
- 第10章 保护Windows 2000 Professional的安全
- 10.1 建立和保护用户和组数据库
- 10.1.1 安全模型
- 10.1.2 管理本地账号数据库中的账号和组
- 10.1.3 保护账号数据库
- 10.2 Windows NT 4.0域中的Windows 2000 Professional
- 10.2.1 Windows NT 4.0域中的认证
- 10.2.2 Windows NT域中的授权
- 10.3 使用组策略管理本地安全设置
- 10.3.1 账号策略
- 10.3.2 本地策略
- 10.3.3 策略设置
- 10.4 使安全设置与用户能力匹配
- 10.5 策略的实现和实施
- 10.5.1 密码策略
- 10.5.2 账号锁定
- 10.5.3 审核策略
- 10.5.4 用户权限
- 10.5.5 安全选项
- 10.5.6 事件日志设置
- 10.6 保护无线连接的安全
- 10.6.1 无线连接：计算机与计算机
- 10.6.2 无线连接：红外网络连接
- 10.7 安全数据和应用程序访问的协议与进程
- 10.8 使用Windows 2000 Professional管理Windows 2000域
- 10.8.1 可用的工具
- 10.9 最佳操作
- 10.10 更多的信息
- 10.11 小结
- 第11章 保护Windows 2000 Server的安全
- 11.1 Server的角色
- 11.1.1 Server的关系
- 11.1.2 Server的作用

<<Windows2000安全技术>>

11.2 安装默认的安全项

11.2.1 用户和组

11.2.2 本地安全策略

11.3 策略设置

11.4 Server安全模板

11.5 使用和保护终端服务

11.5.1 登录权限

11.5.2 应用程序问题

11.5.3 终端服务配置工具

11.5.4 数据加密

11.6 保护互操作服务

11.6.1 Macintosh服务

11.6.2 Unix服务

11.7 最佳操作

11.8 更多的信息

11.9 小结

第3部分 保护Microsoft本地局域网的安全

第12章 域级安全

12.1 活动目录概念介绍

12.1.1 活动目录层次

12.1.2 全局编录

12.1.3 信任关系

12.1.4 数据存储和复制

12.1.5 混合模式，本机模式

12.1.6 LDAP

12.2 动态DNS

12.2.1 动态DNS是怎样工作的

12.2.2 保护动态DNS

12.3 分布式安全服务介绍

12.3.1 IPSec策略

12.3.2 Kerberos策略

12.4 网络认证服务的比较：Kerberos和NTLM

12.5 最佳操作

12.6 更多的信息

12.7 小结

第13章 保护传统Windows客户的安全

13.1 改善认证措施

13.1.1 下级客户的登录

13.1.2 实现NTLMv2：第一步——下级客户

13.1.3 实现NTLMv2：第二步——在Windows 2000域控制器上要求使用NTLMv2

13.2 保护网络通信

13.2.1 SMB签名

13.2.2 使用经协商的NTLMv2会话安全

13.3 改善基本的系统安全

13.3.1 系统策略编辑器

13.3.2 安全配置管理器

13.4 最佳操作

<<Windows2000安全技术>>

13.5 更多的信息

13.6 小结

第14章 保护分布式文件系统的安全

14.1 理解DFS

14.1.1 定义、组件和概念

14.1.2 DFS的工作方式

14.1.3 DFS的使用

14.1.4 DFS客户端

14.2 理解文件复制服务

14.2.1 定义FRS功能

14.2.2 在DFS中使用FRS

14.2.3 管理DFS复制计划

14.3 保护DFS的安全

14.3.1 保护DFS拓扑结构

14.3.2 保护文件和文件夹

14.3.3 保护文件复制策略

14.3.4 规划安全的DFS架构

14.3.5 实现和维护

14.3.6 审核DFS的安全性

14.4 最佳操作

14.5 小结

第4部分 保护现实世界网络的安全

第15章 安全远程访问选项

15.1 路由和远程访问服务

15.1.1 网络地址转换和Internet连接共享

15.1.2 远程访问服务 (RAS)

15.1.3 虚拟专用网络

15.2 Internet认证服务

15.2.1 Internet认证服务的配置和放置

15.2.2 IAS策略

15.2.3 和IAS一起使用VPN

15.2.4 什么时候使用IAS, 什么时候使用RRAS

15.3 终端服务

15.3.1 向用户提供远程访问

15.3.2 为管理员提供远程访问

15.4 保护远程管理访问的安全

15.4.1 使用策略控制访问

15.4.2 使用telnet

15.5 最佳操作

15.6 更多的信息

15.7 小结

第16章 使用分布式安全服务保护网络的安全

16.1 活动目录操作

16.1.1 活动目录复制

16.1.2 保护活动目录

16.1.3 恢复活动目录

16.2 使用组策略对象控制计算机和用户

<<Windows2000安全技术>>

- 16.2.1 组策略处理
- 16.2.2 组策略继承
- 16.2.3 组策略管理的其他项目
- 16.2.4 组策略对象的复制和管理
- 16.2.5 策略应用
- 16.2.6 混合的Windows操作系统网络中的策略
- 16.2.7 组策略对象的权限委派
- 16.3 更多的信息
- 16.4 小结
- 第17章 企业公钥体系
- 17.1 Windows 2000证书服务结构
 - 17.1.1 证书颁发机构
 - 17.1.2 证书层次
 - 17.1.3 证书和证书模板
 - 17.1.4 证书吊销列表
 - 17.1.5 钥策略
 - 17.1.6 证书存储
 - 17.1.7 加密服务提供者
 - 17.1.8 证书信任列表
- 17.2 证书生存期
 - 17.2.1 当安装根CA时，颁发一份根CA证书
 - 17.2.2 如果受到请求，根CA可以为从属CA颁发证书
 - 17.2.3 从属CA可以为别的从属CA颁发证书
 - 17.2.4 周期性的发布证书吊销列表
 - 17.2.5 根CA证书必须在过期之前或者整个证书服务结构失效之前重新颁发
 - 17.2.6 从属CA证书在过期之前或者它颁发的任何证书失效之前重新颁发
 - 17.2.7 证书请求放置在队列中等待管理员同意／拒绝
 - 17.2.8 基于公钥体系的应用程序使用的证书
 - 17.2.9 证书可以被吊销
 - 17.2.10 证书可以被更新
 - 17.2.11 证书可以失效
- 17.3 公钥体系的组策略
 - 17.3.1 企业信任（用户和计算机配置）
 - 17.3.2 加密数据恢复代理
 - 17.3.3 自动的证书请求设置
 - 17.3.4 受信任的根CA
- 17.4 证书服务的其他安全实践
 - 17.4.1 创建安全的CA层次
 - 17.4.2 CA自由访问控制列表
 - 17.4.3 第三方信任
 - 17.4.4 备份和恢复过程和建议
 - 17.4.5 允许Netscape兼容的基于Web的吊销检查
 - 17.4.6 修改默认的证书模板自由访问控制列表
- 17.5 基于证书／公钥体系的应用程序
- 17.6 最佳操作
- 17.7 更多的信息
- 17.8 小结

<<Windows2000安全技术>>

第18章 协同工作

18.1 与UNIX协同工作

18.1.1 原有功能

18.1.2 Services for Unix 2.0

18.1.3 Kerberos互操作性

18.2 PKI互操作性

18.2.1 共存

18.2.2 商业合作伙伴访问

18.2.3 只使用第三方PKI

18.2.4 基于第三方PKI的应用程序

18.3 Macintosh

18.3.1 文件共享

18.3.2 控制打印机访问

18.3.3 Microsoft提供的用户认证模块 (MS—UAM)

18.4 Novell

18.4.1 Windows 2000和NetWare网络间协同工作

18.4.2 在NetWare网络中集成Windows 2000 Professional系统

18.5 IBM Mainframe和AS400

18.6 单一登录

18.6.1 扩展环境

18.6.2 详细情况

18.6.3 不使用SSO的情况

18.7 目录集成：元目录

18.8 最佳操作

18.9 更多的信息

18.10 小结

第19章 Web安全

19.1 保护Windows 2000 Server

19.1.1 配置硬件

19.1.2 升级操作系统

19.1.3 删除或禁用不必要的组件

19.1.4 检查和设置组策略

19.1.5 理解并限制登录和用户权限

19.1.6 增强文件系统的安全性

19.2 保证Web站点的安全

19.2.1 基本属性和站点配置

19.2.2 匿名用户账号

19.2.3 认证

19.2.4 虚拟目录安全

19.2.5 文件访问

19.2.6 安全凭据委派

19.2.7 使用SSL

19.3 工具

19.3.1 随产品一起发布的安全工具和服务

19.3.2 Internet服务器安全配置工具

19.3.3 Web安全模板

19.4 监视，测量和维护

<<Windows2000安全技术>>

- 19.4.1 安全开销
- 19.4.2 什么是可疑的活动
- 19.5 最佳操作
- 19.6 更多的信息
- 19.7 小结
- 第20章 案例研究：分布式合作伙伴
- 20.1 商业模式
 - 20.1.1 根本原因
 - 20.1.2 服务
- 20.2 网络基本设施的安全
 - 20.2.1 逻辑综述
 - 20.2.2 物理网络
- 20.3 活动目录架构主干
- 20.4 认证和授权
 - 20.4.1 公钥体系 (PKI)
 - 20.4.2 商业功能网络的认证
 - 20.4.3 授权
- 20.5 公共和私有接口处理
- 20.6 小结
- 附录 资源
- 参考书
- Microsoft 站点信息
- 其他Web 站点
- 白皮书

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>