<<Oracle安全手册>>

图书基本信息

书名：<<Oracle安全手册>>

13位ISBN编号：9787111099857

10位ISBN编号：7111099850

出版时间：2002-4-1

出版时间：机械工业出版社

作者：Marlene Theriault,Aaron Newman

页数：389

<<Oracle安全手册>>

内容概要

本书提供了经过验证的可以保护Oracle环境的技术和策略——涵盖范围从操作系统到网络。
通过阅读本书，你可以一步步地掌握怎样使用Oracle的内置工具开发周全的安全计划。
本书还讲解了如何避免黑客的攻击，以及如何审计和调试整个系统。
由于得到了Oracle公司的官方认可，本书甚至还讨论了Oracle安全实现的部分细节。
本书内容丰富，讲解生动，是Oracle数据库管理人员及Oracle数据库开发人员宝贵的参考资源。

<<Oracle安全手册>>

书籍目录

第一部分基础知识
第1章 安全构架
l. l 安全的发展
l.2 了解面临的威胁
1.2. l 来自内部的威胁
1. 2. 2 外部威胁
1. 2. 3 安全漏洞来自何方
l. 3 确定谁可以做什么
1.3. l 验证
1. 3. 2 授权
1. 3. 3 系统完整性
1. 3. 4 不同授权模型概览
第2章 Oracle安全实现
2.1 Oracle安全背景知识
2.1. 1 关于备份
2. 1.2 向更强壮的安全性发展
2. 1. 3 Oracle 6以及新的安全措施
2. 1. 4 Oracle 7新特性
2. 1. 5 Oracle 8简介
2. 2 Oracle8i和因特网
第3章 安全规划
3. l 定义安全规划
3. 1. l 安全权衡
3. 1. 2 安全规划的角色
3. 1. 3 全局和局部策略
3. 1. 4 分配责任
3. l. 5 过程
3. 2 估量风险
3. 2.1 易受攻击的程度
3. 2. 2 价值评估
3. 2. 3 备用解决方案
3.3 数据库生命周期
3. 3. l 旧系统
3. 3.2 新系统
3. 3. 3 评估数据库软件包
第二部分操作系统的安全
第4章 UNIX操作系统上的数据库安全
4. l 为什么我们需要操作系统
4.2 确保UNIX的安全
4.2. 1 UNIX基本安全特性
4. 2. 2 锁定操作系统
4. 3 保证UNIX上Oracle的安全
4.3. 1 Oracle数据库如何运行
4. 3.2 在UNIX上安装Oracle
4.3. 3 使用安全临时目录

4. 3.4 原始设备的安全
4. 3. 5 SUID位启用的Oracle文件
4. 3.6 OSDBA、OSOPER和 Internal
4. 3. 7 关于使用SQL*Plus的一个警告
4.3. 8 将审计日志写到操作系统中
第5章 Oracle和 Windows NT／2000的安全
5. 1 Windows NT／2000基础知识
5. 2 Windows NT上 Oracle概述
5. 2.1 Windows NT是如何工作的
5. 2. 2 进程和线程
5. 2. 3 查看Oracle线程
5. 2. 4 Oracle和 Windows注册表
5. 3 在Windows NT／2000系统上保护Oracle
第6章 操作系统验证
6. l 配置验证
6. 1.1 设置参数
6. l. 2 TNS协议
6. 2 Windows验证
6.2.1 在网络上发送证书
6. 2. 2 创建 Windows数据库用户
6.2.3 创建 Windows用户
6、2. 4 Windows操作系统角色
6. 3 UNIX操作系统验证
第三部分保护Oracle数据库
第7章 密码和用户
7.1 Oracle密码管理特性
7. 2 默认Oracle用户
7.3 外部和远程用户验证
第8章 特权、授权、角色和视图
8. l 关于对象和特权
8. 2 关于用户
8.2.1 控制用户访问
8.2.2 关于授予特权
8.2.3 如何使用角色
8. 2.4 Oracle提供的角色
8. 2.5 关于用户默认角色
8.3 使用视图
8. 4 关于触发器
第9章 Oracle和数据库链
9.1 基本数据库链架构
9.2 创建数据库链
9.3 数据库链的安全问题
9.4 关于共享数据库链
9. 5 更多关于全局数据库链的信息
9.6 审计数据库链
第10章 安全和开发工具
10.1 应用程序安全性

10.1.1 数据库用户和应用程序用户
10.1.2 将应用程序安全建立进数据库
10.1.3 应用程序设计惯例
10．1．4 Oracle调用接口
10.1.5 监视数据库活动的审计
10.2 虚拟专用数据库
10.2.1 细粒度访问控制
10.2．2 应用程序上下文
10.3 调用者权限和定义者权限
10．3．l 定义者权限
10.3.2 调用者权限
10．4 PL／SQL包
10．4．1 DBMS_0BFUSCATION
T00LKIT
10．4.2 UTL FILE包
第四部分保护网络通信
第11章 网络完整性、验证和加密
11．1 Oracle高级安全选项介绍
11．1．1 侦听和欺骗
11．1.2 劫持连接
11.l．3 保护网络上数据
11.2 OAS固有特性
11．2．l 配置验证
11.2.2 配置完整性
11．2．3 配置加密
11.3 安全套接字层协议
11．3.1 配置SSL
11．3．2 调试SSL连接
11．3．3 企业用户安全
11.4 推荐的协议
第12章 Oracle安全选项
12.1 虚拟专用数据库
12．2 简要介绍Oracle Label Security
12.3 Oracle因特网目录
12.3.1 关于LDAP架构
12.3.2 Oracle因特网目录的实现
第13章 防火墙和Oracle
13.1 防火墙工作机理
13．1.1 防火墙方式
13．1.2 防火墙不能做什么
13.1．3 防火墙的类型
13.2 通过防火墙使用 Oracle
13.2.1 问题
13.2.2 决定连接问题的罪魁祸首是否是防火墙
13.2．3 防火墙代理
13．2.4 监听器服务
13．2．5 连接管理器

13．2．6 防止端口重定向
第14章 Apache HTTP服务器的安全性
14．1 关于Web服务器
14．2 Oracle的Apache实现
14.2.1 Apache的安装和配置
14．2．2 Oracle的 HTTP配置文件
14.2.3 Apache的安全问题
第15章 Oracle Portal安全管理
15．1 Oracle Portal概述
15．2 Portal验证管理
15．3 用户管理
15．3．1 增加用户
15．3．2 编辑用户
15．3．3 自助式用户维护
15．4 配置登录服务器
15．4．1 密码策略管理
15．4．2 验证用户
15．5 对象访问管理
15．5．1 创建用户组
15.5．2 授予用户和用户组访问权限
15．5．3 授予对页面和应用程序的公共访问权限
第五部分黑客和问题解决
第16章 实施审计
16.1 关于审计
16．1．1 要回答的审计问题
16．1．2 自定义数据库审计
16．2 表的审计方法
第17章 使数据库免于黑客攻击
17．1 攻击者
17．1．1 怀恨在心的雇员
17．1．2 职业黑客
17．1．3 破坏者
17．1．4 已授权用户获得多余的特权
17．2 攻击的种类
17.2．1 缓冲区溢出
17．2．2 SQL Injection攻击
17．2．3 报告弱点
17．2．4 独立安全评估
17．3 保护数据库的工具
17.3．1 安全评定
17．3．2 入侵检测
17．3．3 加密
17．3．4 选择产品策略
附录
附录A 词汇表
附录B 安全风险评估检查表
附录C 保护系统安全的步骤

附录D 系统特权和审计选项
附录E Oracle9i安全特性

版权说明