<<Oracle安全实践>>

图书基本信息

书名：<<Oracle安全实践>>

13位ISBN编号：9787030229632

10位ISBN编号：7030229630

出版时间：2009-1

出版时间：科学出版社

作者：Josh Shaul Aaron Ingram

页数：165

<<Oracle安全实践>>

内容概要

随着计算机和信息技术的迅速发展，信息安全日益引起人们的重视，而数据库安全是保证信息安全的重要环节。

本书旨在创建实践程序来保证Oracle数据库安全，深入讨论了文件系统、TNS侦听、管理员PUBLIC权限、口令控制，详细介绍了如何管理默认账户、监测数据库运行、制定安全计划等内容。适合与数据库安全、审计、信息安全专业或领域的相关人员阅读。

作者简介

Josh Shaul，1997年进入safeNet公司，开始安全领域的工作，参与本行业第一块完整的IPsec加速器芯片的研发工作。
在担任SafeNet开发人员的5年里，Josh为广泛范围的应用程序进行设计、开发和增强SafeNet的嵌入式安全解决方案。
在最近的4年里，Josh主要关注于安装工程，帮助公司在各种网络设施、芯片系统（SoCs）和处理平台上部署安全软件及硬件。
他是安全协议和标准、可信性计算及应用程序等级安全方面的专家。
最近，Josh专注于数据库安全，帮助大企业研发恰当的深人防范的策略来保证敏感数据源头的安全。
Josh目前在Application Sectlrity公司负责Worldwide Sys—tems Engirleering项目。

<<Oracle安全实践>>

书籍目录

致谢作者简介技术编辑第1章 Oracle安全概述 引言 Oracle安全特性的历史简介 权限控制 网络 审计 口令管理 数据分区 Oracle 10g和更高版本 管理环境驱动的数据库安全 主要的数据窃取事件 CardSysteins SOlutions——2005年6月 ChoicePoint——2005年2月 TJX——2007年1月 退伍军人事务部——2006年5月 渐进地保证Oracle安全 对每个种类数据库系统合适的安全 小结 快速解决方案 常见问题第2章 文件系统 引言 了解文件 数据 日志 软件 检查推荐的许可 操作系统基础 软件许可 非软件许可 管理变更 小结 快速解决方案 常见问题第3章 TNS监听器安全 引言 TNS监听器介绍 监听器组件 监听器命令 Oracle 10g监听器变更 监听器可能是攻击缺陷的主要来源 由于设计导致的监听器缺陷 不存在账号停用 以明文传输的口令 使用口令或者哈希口令的验证 通过应用Oracle补丁集和CPU来修补监听器缺陷 监听器DoS攻击 监听器缓存区溢出攻击 保证监听器配置安全 监听器安全/监听器口令 ADMIN—RESTRICTIONS 监听器日志和跟踪 ExtProc 有效的节点检查 小结 快速解决方案 常见问题第4章 管理默认账号 引言 从9i到10g的Oracle默认账号角色 默认账号 锁定账号和中止默认口令 配置强口令 解除账号锁定和配置强口令 Oracle的哈希口令算法 定义强口令 配置强口令 自动控制鉴别默认账号的过程 创建自己的默认口令扫描脚本 使用一种免费可用的默认口令扫描器 使用一种商业化的数据库缺陷扫描器 小结 快速解决方案 常见问题第5章 PUBLIC特权 引言 PUBLIC组 简单介绍：Oracle特权和角色 授予PUBLIC的角色 敏感函数上的默认特权 DBMS RANDOM UTL—FILE UTL—HTTP UTL—SMTP UTL—TCP 从来不应该授予PUBUC的特权 系统特权 SYS模式中的对象特权 使用一般的意义 小结 快速解决方案 常见问题第6章 软件升级 引言 理解Oracle的软件补丁思想 安全 成本 平台 检查CPU 评估风险矩阵 作用于安全顾问 安装关键的补丁升级 计划 测试和配置 评估安全警告 小结 快速解决方案 常见问题第7章 口令和口令管理第8章 数据库事件监测第9章 执行指南

章节摘录

第1章 Oracle安全概述引言一位就职于世界上最大的银行之一的数据库高级管理人员告诉我，保证Oracle安全的最好方式是“ 把网线拔掉 ”……可能他是对的。
事实上，几乎对所有的网络应用程序来说，这个结论是成立的。
不幸的是，对多数人而言，关闭数据库是不可行的；我们必须寻找另外的方法来确保系统的安全。
新的技术和服务为商业带来收入，尤其是那些为客户提供定制信息的系统。
这些系统需要频繁地进行存储、处理及对个人数据提供访问。
存储商业机密或财务信息的系统也是一样。
很多存储的数据是非常敏感的，虽然如此，这些数据都必须快速且容易地被访问。
这些构成了对数据安全的重大挑战，也是我们将在本书中自始至终详细讨论的内容。
本书的目的是帮助读者建立针对Oracle数据库系统的实用安全方案。
我们将创建一种方法来度量和评价数据库安全性能，并且提供工具为每个Oracle数据库创建一张安全性能计分卡。
本书并非一本数据库管理员（DBA）手册一差别很大。
我们写作的目的是针对整个数据库安全团体，不但包括DBA，还包括信息技术（InformationTechnology，IT）安全人员、审计人员，甚至信息安全官（ChiefInformationSecurityOfficer，CISO）。
目前，Oracle是世界上应用最广泛的数据库管理系统。
它几乎是现存的各个主要行业关键系统的核心部件。
在金融、医疗、电信、制造、政府，甚至军队里，数据库和数据库中的数据就意味着业务的全部。
在过去的几年里，数据库已经成为计算机频繁攻击的对象。
最初，攻击的主要意图是造成业务的崩溃和在黑客社区中获得臭名昭著的效果；伴随着数据库攻击行为的不断增长，这种情况已发生了显著的改变，攻击者更关注于从数据库系统中提取敏感的和有价值的信息，以此谋取金钱利益。
如窃取个人信息进行身份欺骗、窃取信用卡口令来随意消费、窃取商业机密以期获得其竞争者的回报，这些都是隐藏在数据库攻击后面的驱动力。

编辑推荐

《Oracle安全实践:来自第三方的关系型数据库安全指南》为21世纪信息安全大系丛书之一，由科学出版社出版。

版权说明