计算机网络安全技术丛书 3

Database Scanner

网络数据库安全维护高手

〔美〕John Shum 主编
钱辉 孟国伟 胡敏 编译

本书配套光盘内容包括:
本书配套的电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

计算机网络安全技术丛书 3

Database Scanner

网络数据库安全维护高手

〔美〕John Shum 主编
钱辉 孟国伟 胡敏 编译

本书配套光盘内容包括:
本书配套的电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是“计算机网络安全技术丛书”之一。该书全面系统地介绍了数据库监控工具 Database Scanner 的使用方法和技巧，并对数据库安全性方面的问题进行了详细的讲解。众所周知，随着计算机技术的发展，大型数据库所扮演的角色越来越重要。数据库的安全性就成为一个亟待解决的问题。Database Scanner 正是这样一种维护数据库安全的专用软件。它在扫描数据库时，模拟电脑黑客的思维方式，专门查找数据库的缺陷，就像一名攻击者寻找漏洞一样。用户利用它可以很快找出数据库安全上的缺陷，并采用相应措施堵住漏洞，这样便可防患于未然。

本书由 6 章及 3 个附录组成，内容涵盖了 Database Scanner 所涉及的各个方面的问题，主要包括：Database Scanner 简介，创建、运行一个安全策略，分析安全扫描结果，检查口令可靠性和 Database Scanner 的界面元素。附录部分分别提供了应用 Database Scanner 对 Microsoft SQL Server，Sybase Adaptive Server 和 Oracle 进行安全检测，生成安全扫描报告，并应用安全策略编辑窗口创建安全策略的细节方面的信息。

本书内容新颖，实用性强，条理清晰，实例丰富，深入浅出地阐述了 Database Scanner 的基本知识和使用技巧，并提供了切实可行的解决安全漏洞的方法。本书不仅是数据库开发、设计、管理、维护人员和 Database 服务商必备的参考书，而且也是高等院校相关专业师生和社会相关领域人员不可缺少的教学、自学用书。

本书配套的电子光盘内容包括：与本书配套的电子书。

系　列　书：	计算机网络安全技术丛书 (3)
书　　名：	Database Scanner 网络数据库安全维护高手
文本著作者：	John Shum 主编
文 本 译 者：	钱辉　孟国伟　胡敏　编译
CD 制 作 者：	希望多媒体开发中心
CD 测 试 者：	希望多媒体测试部
责 任 编 辑：	纪红
出版、发行者：	北京希望电子出版社
地　　址：	北京海淀路 82 号　100080
	网址：www.bhp.com.cn　E-mail: lwm@.hope.com.cn
	电话：010-62562329,62541992,62637101,62637102，010-62633308.
	62633309（图书发行，技术支持）
	010-62613322-215（门市）　010-62531267（编辑部）
经　　销：	各地新华书店、软件连锁店
排　　版：	希望图书输出中心
CD 生 产 者：	北京中新联光盘有限责任公司
文本印刷者：	北京广益印刷厂
规格 / 开本：	787×1092　1/16 开本　8.125 印张　172 千字
版次 / 印次：	2000 年 8 月第 1 版　2000 年 8 月第 1 次印刷
印　　数：	0001～3000 册
本 版 号：	ISBN 7-900044-80-9/TP・80
定　　价：	30.00 元(1CD，含配套书)

主编的话

网络安全现在已经成为 IT 业界最为关注的头等大事，如何及时预报和监测计算机病毒、反击黑客入侵、分析病毒特征、设置多重密码、配置代理服务器和双机容错、研制公私密钥、保护企业的资源已成为网络工程人员开发中首要考虑的技术之一。美国 ISS 公司专门从事网络安全技术的研究和网络安全防范工具的研制、开发，它推出的一系列网络安全监控工具反映了最新的网络安全技术，是目前最权威的网络安全防范工具。

有效利用最新技术和工具维护网络安全，对专业人员提出了更专业的知识要求。由此，针对具体应用的知识已被人们充分注意，并被有的放矢地用于工程之中。

“计算机网络安全技术”丛书即是为满足以上社会需求而组织出版的。本丛书第一批图书集中了 ISS 公司最新的并被广泛应用的网络监控工具，给出了工具的防范原理、应用方法，及相关使用技巧，讨论了使用该项技术后的网络维护、应用、开发和管理。本丛书旨在给网络管理、维护、开发、应用人员提供完整的应用网络监控工具的技术指导，以安全、有效地运用工具于网络维护之中。本丛书首批出版以下图书：

- 《**System Scanner 企业网络安全维护高手**》。本书介绍了企业网络监控权威工具之一 System Scanner（SS）的应用。

System Scanner 是监控企业内部主机运行状态的“火眼金睛”。本书由 7 章和 3 个附录组成，内容包括：System Scanner 基础知识，实施风险评估，锁定系统，使用报表，生成警报，管理 System Scanner 环境和使用策略。附录 A 是相关参考资料的查找方法和推荐的参考书目，附录 B 重点讨论了 System Scanner 中应用的各种策略，附录 C 介绍如何配置控制台。本书最后还提供了相关术语的解释，以供读者参考。

- 《**Internet Scanner 互联网安全维护高手**》。本书讨论了维护互联网安全的专用软件：Internet Scanner。Internet Scanner 是目前最快、最易掌握和最有效的网络安全扫描软件。它在扫描网络时，模拟电脑黑客的思维方式，专查找网络的缺陷，就像一名攻击者寻找网络漏洞一样。用户利用它可以很快找出网络安全上的缺陷，并采用相应措施堵住漏洞，防患于未然。在本书的指导下，用户可以很快掌握 Internet Scanner 的使用方法。

本书包括 5 章和 1 个附录。介绍了 Internet Scanner 基本功能，说明了如何扫描网络和查找危害网络安全的隐患，讨论了策略配置，以及利用策略完成符合自己要求的扫描，还讨论了如何将扫描结果制成报表，如何应用数据库，如何把扫描获取的信息存入数据库。附录部分描述了 Internet Scanner 的用户界面，列出了 Internet Scanner 内置的检测任务和外接的（插件）检测任务，启用这些检测任务可以很快找出网络安全的薄弱环节。附录还列出了使用 Internet Scanner 时经常发生的问题，并说明了解决办法，最后介绍了与网络安全相关的参考资料。

- 《**Database Scanner 网络数据库安全维护高手**》。本书介绍了维护网络数据库安全的专用软件——Database Scanner 的使用方法。Database Scanner 是面向 Microsoft SQL Server，Sybase Adaptive Server 和 Oracle 的顶级数据库安全性检测工具，是目前第一个为数据库

的缺陷和隐患进行评估的产品。它的设计思路是通过创建和执行安全策略来保护数据库应用程序。Database Scanner 能够自动地鉴别在数据库系统中存在的安全隐患，能够修正从口令过于简单到 2000 年的特洛伊木马等一系列问题，内置的知识库能够对违背和不遵循安全性策略的做法推荐纠正后的操作，并直接访问知识库提供易于理解的报告。本书讨论了 Database Scanner 应用的方方面面。

藉此丛书付梓之际，我特别要向在本丛书出版过程中一直精诚合作的编译人员表达真诚的谢意。感谢他们的勤奋和热情，在编译本套书的过程中他们把节假日也投入到了编译工作中；在此还要提到的是，他们对某些不很熟悉的知识所表现出的认真和严谨的学习态度，令我印象深刻。

本丛书从选题、编译到出版，历时仅 3 个月。因出版时间紧迫，书中错误在所难免，敬请读者拨冗指正，在此谨先致谢！

John Shum

2000 年 4 月

目　录

1 Data Base Scanner 简介

1.1 介绍

什么是 Database Scanner

面向 Microsoft SQL Server, Sybase Adaptive Server,和 Oracle 的 Database Scanner 是顶级的数据库安全性检测工具。

Database Scanner 是第一个为数据库的缺陷和隐患进行评估的产品，它的设计思路是通过创建，遵照和执行安全策略来保护数据库应用程序。Database Scanner 能够自动的鉴别在数据库系统中存在的安全隐患，能够修正从口令过于简单到 2000 年顺从性以及特骆伊木马等一系列问题。内置的知识库能够对违背和不遵照安全策略的做法推荐纠正后的操作，并且能够直接访问知识库和提供易于理解的报告。

支持平台

ISS 支持 Database Scanner 在下列数据库平台上进行扫描：

- Oracle 8i,8.0 和 7.3(Unix 或 Windows NT)
- Microsoft SQL Server 6.x 和 7(Windows NT)
- Sybase Adaptive Server 11.x(Unix 或 Windows NT)

ISS 已经通过在下列平台上进行的 Database Scanner 的认证

- Oracle 8.0 和 7.3 在 Solaris, HP/UX，和 Windows NT Server 4.0 上
- Sybase Adaptive Server 11.0,11.5, 和 11.9.2 在 Solaris 和 Windows NT Server 4.0 上
- Microsoft SQL Server 6.0,6.5,和 7 在 Windows NT Server 4.0 上

另外在其他版本的数据库和操作系统平台上也进行了测试，包括 Oracle 8i 和 Windows2000。更多的测试将继续进行。

关于因特网安全系统有限公司

因特网安全系统有限公司（ISS)(NASDAQ-NMS:ISSX) 是网络监控，侦测和为企业的信息系统安全性和完整性提供保护的相应软件的主要提供者。

1.2 文档目录

Database Scanner 3.0 用户指南包含 Database Scanner 的各种功能以及涉及所在公司自身的安全策略部分的功能的信息。

各章节概况

第 1 章：介绍 Database Scanner 介绍 ISS 和 Database Scanner3.0

第 2 章：创建安全策略 提供关于应用 Database Scanner 工业标准安全策略或创建特定的安全策略方面的信息

第 3 章：执行安全性查询 提供关于用 Database Scanner 进行的一个安全性扫描实例方面的信息

第 4 章：分析安全性查询的结果 提供关于一个安全性扫描实例结果分析方面的信息

第 5 章：检查口令的可靠性 提供关于网络上数据库口令的可靠性方面的信息

第 6 章：Database Scanner 界面 提供关于 Database Scanner 的窗口和菜单方面的信息

附录概况

附录 A：Microsoft SQL Server 提供关于 Database Scanner 生成的安全性报告和应用安全策略编辑窗口创建安全策略的细节方面的信息

附录 B：Sybase Adaptive Server 提供关于 Database Scanner 生成的安全性报告和应用安全策略编辑窗口创建安全策略的细节方面的信息

附录 C：Oracle 提供关于 Database Scanner 生成的安全性报告和应用安全策略编辑窗口创建安全策略的细节方面的信息

在线帮助

按 F1 键激活 Database Scanner 窗口的帮助；或者在 Database Scanner 窗口的主菜单，选择 Help/Contents 来显示在线帮助的目录列表。

1.3 Database Scanner 的特点

介绍

发生安全侵害一般是由于系统配置不正确，安全策略没有被建立和执行。应用 Database Scanner，可以建立数据库安全策略，扫描数据库，查找安全漏洞和提交易于理解的安全性检测报告。

可定制的安全策略和执行

由于 Database Scanner 体系结构上的灵活性，可以设置并执行特定的数据库安全策略来控制合法的数据库操作。可以为网络环境中不同的数据库服务器创建多个安全策略。一

旦创建了一个安全策略，Database Scanner 执行彻底的检测并产生一个重要的参照基准，以此基准来估量和控制安全性隐患，并且有助于进行不间断的安全性方面的改进。

全面的安全缺陷检测

Database Scanner 能够迅捷轻松的通过网络扫描数据库，在广泛的范围内检测到数据库细节方面的缺陷。这种全方位的扫描能够对诸如身份认证，用户权限和系统完整性设置方面的安全隐患进行全面的评估。

Database Scanner 在进行安全缺陷检测时的关键区域显示在表 1.1 中：

表 1.1 Database Scanner 安全缺陷检测

安全缺陷检测	描述
口令，登录和用户	自动的执行口令可靠性分析，对能够进行登录的用户进行跟踪，检查用户名的完整性
配置	验证功能上潜在的损坏是否被允许，并对配置选项是否需要更改提出建议，这些配置选项包括： • 复制 • 邮件 • 直接更新 • 登录监察 • 启动存储的过程存在 • 警报和计划任务 • 网络任务 • 跟踪标志 • 不同的网络协议
许可控制	确定谁访问了存储过程，并且当数据库用户对 Windows NT 的文件和资源获得未经授权的许可时，将认为是对数据库的威胁，它将对这种可能的威胁发出警报。对系统内存在的潜在特骆伊木马程序进行检查，这些特骆伊木马会收集获得网络访问权限所需的敏感数据。
2000 年顺从性	对数据库环境进行分析并对数据和存储过程中存在的 2000 年问题做出报告

纠正后的行为和快速消除安全漏洞

当数据库安全监察结束时，Database Scanner 将对系统的安全性能提供专业的分析，这种分析将以图形的方式形成报告。Database Scanner 同时也将提供易于理解的用于消除安全风险的纠正后操作。

2 创建一个安全策略

2.1 介绍

概述

这章提供了关于创建安全策略的信息和操作安全策略的步骤。

此主题包括下列内容：

- 应用一个工业标准安全策略
- 创建一个特定的安全策略
- 删除一个安全策略
- 备份一个安全策略
- 装载一个安全策略

Database Scanner 提供三个内置的安全策略（最大，中等和最小），用户也可以应用安全策略编辑器创建自己特定的安全策略。关于安全策略编辑器界面的详细描述，请参照本书相关章节的描述。

2.2 应用一个工业标准安全策略

概述

数据库编辑器提供了三个内置的安全策略：最大，中等和最小安全策略。可以应用这些策略快速配置安全标准等级，并且 Database Scanner 将依照此标准进行检测。

最大安全策略

最大安全策略是一个非常严紧的策略，主要应用于对安全要求苛刻的数据库。

最大安全策略包括以下内容：

- 消除对数据库遗留安全隐患的功能
- 配置大量的监察
- 初步设计数据库的安全策略

应用最大安全策略将导致数据库功能的减弱和性能方面的下降，所

以除了对安全有极特殊要求的数据库外不要应用此策略。

中等安全策略

中等安全策略是一个较强的安全策略，应用此策略需要修改许多默认的设置，并且将导致对数据库某些功能的限制。中等安全策略提供一个较高的安全等级，对数据库的性能和功能将会产生一定的影响。

最小安全策略

最小安全策略是一个较好的安全策略，应用此策略需要修改许多默认的设置，并且将导致对数据库某些功能的限制。最小安全策略提供一个适中的安全等级，仅对数据库的性能和功能产生轻微的影响。

操作步骤

对 MS SQL Server ,Sybase Adaptive Server 或 Oracle 的工业标准安全策略进行浏览，请遵照如下步骤：

1. 在 Database Scanner 的欢迎窗口中，点击 Set Security Policy 以激活安全策略窗口。
2. 在安全策略名称和服务器类型列表中，选择 Maximum，Medium 或 Minimum 之一。
3. 点击 Open 在安全策略编辑窗口中打开安全策略。
4. 如果要对安全策略进行预览，点击 Preview，则安全策略的详细资料将显示在策略细节窗口内。
5. 在安全策略编辑窗口中，点击 OK 接受安全策略并返回欢迎窗口中。

创建一个自定义的安全策略

操作步骤

创建一个自定义的数据库安全策略，请遵照下列步骤：

1. 在 Database Scanner 的欢迎窗口中，点击 Set Security Policy 以激活安全策略窗口。
2. 从策略名称和服务器类型列表中：

- 选择<New Security Policy>为 MS SQL Server ,Sybase Adaptive Server 或 Oracle 建立新的安全策略，并点击 Open。

或

- 以高亮显示 ISS 的工业标准安全策略（最大、中等、最小安全策略）之一，或者高亮显示一个已经定制好的安全策略，作为一个参照基准，然后点击 Copy，在安全策略编辑窗口中显示一个安全策略。

3. Database Scanner 将数据库安全方面的设置划分为三个关键性的安全范畴：身份认证，用户权限和系统完整性。在任何一个范畴中，可以对想要建立的安全策略进行设置。

Oracle 数据库编辑器允许对所选择的帐户、角色(role)和数据表授予特例许可。这些特例许可将通知 Database Scanner 忽略被某些特定的数据库用户视为合法的一些情况。可以在下列设置中授予特例许可：

- 帐户许可

- 角色许可
- 监察表许可
- 数据库链接许可
- PUBLIC 对象许可
- UTL_FILE 许可

对以上的任何一项设置授予特例许可将使上述的所有设置均得到特例许可。

4. 对于 MS SQL Server 和 Sybase Adaptive Server，All 标签中提供了所有的数据库安全策略设置方面的概况。如果要在 All 标签中改变设置，点击下拉列表框或直接键入新值实现要做的改变。

5. 在 Policy 域中，输入安全策略的名称。

6. 点击 Apply 将所作的改变写入安全策略中，并且仍然保持在安全策略编辑窗口中，或者点击 OK 来保存安全策略并退出安全策略编辑窗口。

2.3 删除一个安全策略

操作步骤

从 Database Scanner 中删除安全策略，遵照下列步骤：

1. 在 Database Scanner 的欢迎窗口中，点击 Set Security Policy 以激活安全策略窗口。

2. 从安全策略名称列表中，选择想要删除的安全策略，并点击 Open 打开安全策略编辑窗口。

3. 点击 Delete Policy 来删除安全策略。将出现一个确认窗口，让用户确认是否进行删除。

4. 点击 Yes 删除安全策略后返回 Database Scanner 主窗口。

注意 不能删除缺省的安全策略。

2.4 备份一个安全策略

标准存档文件

将一个安全策略备份到 Database Scanner 的缺省策略文档目录下，请遵照以下步骤：

1. 在 Database Scanner 主窗口中，选择 Scanner →Manage Scans/Policies 来显示 Scan/Policy 管理窗口。

2. 选择 Policy Management 标签。

3. 选择想要备份的一个或多个策略。

4. 如果没有可选择的，选中 Standard Archive 单选按钮并点击 Backup Policy。

5. 点击 Close 返回 Database Scanner 的主窗口。

已存在的存档文件

1. 在 Database Scanner 主窗口中，选择 Scanner →Manage Scans/Policies 来显示

Scan/Policy 管理窗口。

2. 选择 Policy Management 标签。

3. 选择想要备份的一个或多个策略。

4. 选中 Existing File 单选按钮或在 Existing File 字段中键入备份文件的名称。

5. 点击 Backup Policy。

6. 点击 Close 返回 Database Scanner 的主窗口。

新建的存档文件

将安全策略备份到一个新的文件中，请遵照如下步骤：

1. 在 Database Scanner 主窗口中，选择 Scanner →Manage Scans/Policies 来显示 Scan/Policy 管理窗口。

2. 选择 Policy Management 标签。

3. 选择想要备份的一个或多个策略。

4. 选中 New File 单选按钮并且在 New File 字段中键入新的文件名称。

5. 点击 Backup Policy。

6. 点击 Close 返回 Database Scanner 的主窗口。

装载一个安全策略

操作步骤

装载一个安全策略，请遵照如下步骤：

1. 在 Database Scanner 主窗口中，选择 Scanner →Manage Scans/Policies 来显示 Scan/Policy 管理窗口。

2. 选择 Policy Management 标签。

3. 根据备份的安全策略的位置，在 Standard Archive 和 Existing File 二者中选择其一，并且点击 Load Policy 来显示 Load Policies 对话框。

4. 从 Policy 列表中，选择想要打开的安全策略并点击 OK。如果安全策略在标准存档文件中没有被列出，则点击...按钮来查找存档文件，或者在 Existing File 字段中键入存档文件的位置。所要装载的安全策略就会显示在 Scan/Policy 管理窗口的 Policy Management 标签中。

3 运行一个安全扫描

3.1 介绍

概述

本章提供了运行一个全面的数据库安全扫描和分析方面的信息和操作步骤。此主题包括下列内容：

- 运行一个安全扫描
- 进行安全扫描期间增加额外的数据库
- 进行安全扫描期间删除数据库

3.2 运行一个安全扫描

概述

在正确安装 Database Scanner 后，就可以立即应用 Database Scanner 提供的工业标准安全策略或者用户自己定义的安全策略来运行一个安全扫描以验证数据库是否符合安全要求。（关于“创建自定义安全策略”请参考本书的相关内容）。

安全风险

进行数据库扫描时，Database Scanner 识别任何安全风险，并在下列范围内揭示出来：

- 身份认证——在数据库范围内验明用户的身份。
- 用户权限——在系统范围内验证合法用户如何使用特定的资源。
- 系统完整性——将注意的焦点集中于数据库系统资源的协调，控制和 2000 年问题上。

重要信息 在通过网络运行扫描前，必须确认已经配置了一个客户机的连接。关于配置客户机连接的具体信息，请参考本书相关章节。

操作步骤

运行安全扫描，请遵照如下步骤：

1. 在 Database Scanner 的欢迎窗口中，点击 Scan Database 来显示数据库扫描窗口。

2. 在 Double click a server to add it to the list 字段中，展开 Network Neighborhood 树形结构并选择想要扫描的数据库。在选择的服务器下面将显示网络上的数据库列表。

—或—

在 To add a server to the list，enter database name and click Add Database 列表字段中直接键入想要扫描的服务器的名称。

注意 Database Scanner 的扫描授权是基于运行扫描时所用到的逻辑名。一旦使用某个逻辑名对一个服务器进行了一次扫描，那么就必须在后续的扫描过程中使用相同的逻辑名，这样可以防止授权的增加。

3. 将服务器加入到 Run scan for these databases 表格(grid)时，双击 Network Neighborhood 树形结构中的数据库并单击 Add Database。

推荐 对于 Microsoft SQL Server，当通过网络运行安全扫描时，ISS 推荐应用加密的连接登录 ID，口令和数据。Microsoft SQL Server 需要使用经过加密的 Multi-Protocol Net-Library。

4. 数据库将出现在 Run scan for these databases 表格中。可以在表格中改变下列设置：

表 3.1 数据库扫描选项设置

设置	描述
Server	进行扫描的服务器的名称
Trusted（仅限于 MS SQL）	选择是否在连接的时候使用 Windows NT 身份认证
Account	通过标准身份认证连接到服务器的帐户
Password	通过标准身份认证连接到服务器的帐户口令
Policy	扫描数据库所用的安全策略（最大、中等、最小和特定策略）
Type	关于扫描的服务器类型的描述（Microsoft SQL Server，Oracle 或 Sybase Adaptive Server）
Host Address（仅限于 Oracle）	Unix 网络的地址
Host User Name（仅限于 Oracle）	Unix 帐户（Oracle 的安装用户）
Host Password（仅限于 Oracle）	主机用户名的口令

5. 重复步骤 2 和步骤 3 以增加更多的服务器，或参考本章的相关部分。

6. 点击 Start Scan 开始扫描数据库来查找安全漏洞和隐患。对每一个被扫描的服务器都将打开一个新的窗口，在窗口中显示扫描的进程。

3.3 进行安全扫描期间增加额外的数据库

可以通过下列两种操作方法中的任何一种从数据库扫描窗口添加额外的数据库：

- 在 Network Neighborhood 树形结构的服务器列表中双击一个服务器，将其加入到