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

Run scan for these databases 表格中。

- 点击 Network Neighborhood 树形结构的服务器列表中的一个服务器，将其加入到 To add a server to the list，enter database name and click Add Database 列表中，然后点击 Add Database 将服务器加入到 Run scan for these databases 表格中。

重复上述二者中的任何一个过程，直到为这次扫描选择到所有期望的数据库。关于运行扫描方面的介绍，请参考本书的相关内容。

3.4 进行安全扫描期间删除数据库

操作步骤

在进行安全扫描期间删除数据库，请参照下列步骤：

1．在数据库扫描窗口中，找到 Run scan for these databases 表格并选择想要删除的数据库。

2 点击 Remove ，则在这次扫描期间，此数据库被删除。

3 在扫描期间删除其他的数据库，重复步骤 1 和 2。

4 安全扫描结果分析

4.1 介绍

概述

本章提供了关于安全扫描结果分析方面的信息。本主题包括下列内容：

- 回顾安全扫描结果
- 更改安全策略进行安全扫描
- 备份安全扫描结果

4.2 回顾安全扫描结果

概述

安全扫描被执行完后，Database Scanner 通过数据分析引擎将扫描结果进行组织，并生成易于理解的数据库安全扫描报告。用户将在下列的安全范畴内得到安全扫描的分析结果。

- 身份认证
- 用户权限
- 系统完整性

操作步骤

回顾安全性扫描结果和报告，请遵照下列步骤：

1. 在 Database Scanner 的欢迎窗口内，点击 Review Results 来显示回顾结果窗口。

2. 在 Server Name 列表中，选择需要回顾的服务器。服务器选择完毕后，对数据库进行的各项扫描结果就会显示在 Scan Data 窗口内。

3. 在 Scan Date 列表中，选择一项安全扫描结果。所有的扫描结果是按照扫描的日期和时间进行组织的。

4. 选择需要回顾的报告。当大多数的报告被选择到后，将出现一些参数。应用这些参数来过滤报告中的数据。选择报告时，在 Reports

列表中的复选框中进行选择。关于每种报告及其参数的详细描述，请参阅本书的相关章节。

5. 对所选择的报告进行回顾，点击 Print Reports 将所需要的报告直接发送到打印机上。

—或—

点击 Preview Reports，在屏幕上对报告进行预览。

4.3 更改安全策略进行安全扫描

概述

对于 Microsoft SQL Server 和 Sybase Adaptive Server，Database Scanner 允许改变安全扫描时所用的策略以比较不同的策略下服务器的安全性。由于这种强大的功能，可以在对 Oracle 数据库扫描时打开或关闭一些特殊的检测，但是 Oracle 数据库并不提供改变策略进行扫描的特性。

操作步骤

改变安全策略进行扫描以得到结果，请遵照如下步骤：

1. 在 Database Scanner 的欢迎窗口内，点击 Review Results 来显示回顾结果窗口。

2. 在 Server Name 列表中，选择需要回顾的服务器。服务器选择完毕后，对数据库进行的各项扫描结果就会显示在 Scan Data 窗口内。

3. 在 Scan Data 列表中，选择一项安全扫描结果。所有的扫描结果是按照扫描的日期和时间进行组织的。

4. 点击 Change Policy。将弹出选择安全策略对话框。

5. 选择进行安全扫描时所应用的策略，点击 OK。

6. 选择需要回顾的报告。当大多数的报告被选择到后，将出现一些参数。应用这些参数来过滤报告中的数据。选择报告时，在<:Server type>Reports 列表的复选框中进行选择。关于每种报告及其参数的详细描述，请参阅本书相关章节的内容。

7. 对所选择的报告进行回顾：

- 在扫描结果回顾窗口中，点击 Print Reports 将所需要的报告直接发送到打印机上。

—或—

- 在扫描结果回顾窗口中，点击 Preview Reports，在屏幕上对报告进行预览。

4.4 备份安全扫描结果

标准存档文件

将一个安全扫描结果备份到 Database Scanner 的缺省扫描结果文档目录下，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 Scan Management 标签。

3．在 Machines和 Scans列表中，选择进行备份的计算机和安全扫描结果。

4．选中 Standard Archive 单选按钮。

5．在备份安全扫描结果后如要删除源文件，请选择 Remove Scans。

6．点击 Backup Scan。

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 Scan Management 标签。

3.在 Machines 和 Scans 列表中，选择进行备份的计算机和安全扫描结果。

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 Scan。

新建的存档文件

将安全扫描结果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 Scan Management 标签。

3．在 Machines 和 Scans 列表中，选择进行备份的计算机和安全扫描结果。

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 Scan。

4.5 装载一个安全扫描结果

操作步骤

从存档文件中装载一个安全扫描结果，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 Scan Management标签。

3．根据备份的安全扫描结果的位置，在 Standard Archive 和 Existing File 二者中选择其一。

4．点击 Load Scan来显示 Load Scans对话框。

5．在 Machines 和 Scans 列表中，选择想装载的安全扫描结果。

6．在 Scan Management 标签中点击 OK，进行安全扫描结果的装载。

7．点击 Close 以返回 Database Scanner 主窗口。

5 检查口令的可靠性

5.1 介绍

概述

本章提供关于运行口令可靠性检测程序方面的信息，口令可靠性检测可以防止数据库帐户被侵袭。此主题包括下列内容：

- 运行口令可靠性检测程序
- 选择一个口令文件
- 定制口令字典

5.2 运行口令可靠性检测程序

操作步骤

运行口令可靠性检测程序，请遵照如下步骤：

1．在 Database Scanner 的欢迎窗口中，点击 Password Strength 来显示口令可靠性检测窗口。

2．可以通过下列三种方式选择要访问的服务器：

- 在 Check password strength on server 字段中，键入数据库服务器的名称。
- 在 Network Neighborhood 树形结构中选择一个数据库服务器。
- 在 Check password strength on server 下拉列表中选择一个数据库服务器。

3．在 Server Type 下拉列表框中，选择一个服务器。

4．对于 MS SQL Server ，选中 Trusted Connection 复选框以应用 Windows NT 的安全措施来验证数据库的登录。如果使用数据库帐户进行登录，则清除 Trusted Connection 复选框并键入有效的帐户名和口令。

5．选择一个口令文件来进行口令可靠性的测试。可以通过在 Password File 列表中选择一个口令字典，来使用 Database Scanner 中内置的包含较易被猜测到的口令的口令字典之一。如果希望应用自己的口令字典，点击 Browse 按钮，选择希望应用的字典文件。关于创建口令

字典方面的信息，请参考“创建一个口令字典”部分。

6. 点击 Check Passwords 开始测试口令可靠性。屏幕上将出现一个状态条来显示口令测试的进程。当测试评估过程结束后，将出现以图形方式显示的口令文件可靠性的测试结果。

5.3 选择一个口令文件

概述

Database Scanner 提供了一个内置的含有 30,000 较易被猜到的口令的口令字典，应用此口令文件可以对所希望进行的各等级的评测提供方便。当然，也可以应用自己创建的口令字典。

操作步骤

为口令可靠性测试选择一个口令文件，请遵照下列两种方式中的任一种：

在 Password file 下拉列表框中，选择一个口令文件：

表 5.1 口令字典描述

口令文件	描述
<Use larger password dictionary>	Database Scanner 的扩展口令字典
<Use faster password dictionary>	简化口令字典以进行更有效的口令可靠性的评估
<Use Sybase dictionary>	Sybase Adaptive Server 不允许口令的长度少于 6 个字符(此口令字典是特别为 Sybase Adaptive Server 进行配置的)
<Use names only>	仅仅对应用正确用户名帐户进行口令可靠性检查
<Use non-names only>	对应用正确用户名之外的帐户进行口令可靠性的检查
<Do not use dictionary>	执行默认的口令可靠性测试 • 口令不存在 • 口令和帐户相同 • 口令为帐户名后接数码 1－9 (MS SQL Server) • 口令为帐户名后接数码 1－100 (Oracle) • 口令为帐户名后接数码 1（Sybase Adaptive Server） • 口令为帐户名的翻转 • 口令和服务器名相同（Oracle）

一或 –

2. 点击 Browse 以显示 Open 对话框。打开一个口令文件或在 File Name 字段中键入一个口令文件名，然后点击 Open。

5.4 定制口令字典

概述

一些私人的口令，比如公司名称，可以并且应当被加入到口令字典中。这些口令字典文件将以文本文件的格式存储在相应的目录中。

操作步骤

修改口令字典，请遵照如下步骤：

1．在桌面上，点击 Start 菜单，选择 Programs→Accessories→Notepad 或 Programs→Accessories→WordPad。

2．根据所要进行添加口令的口令库的不同，打开下列文件：

表 5.2 口令库文件

口令库	对应的文本文件
<Use faster password dictionary>	fasterpw.txt
<Use larger password dictionary>	largepw.txt
<Use Sybase dictionary>	Sybasepw.txt
<Use names only>	namespw.txt
<Use non-names only>	nonnamepw.txt
<Do not use dictionary>	blank.txt

3．在此文本文件的开头，在单独的一行上输入一个口令后，按 Enter 键。

4．重复步骤 3，将所希望添加的口令添加到口令字典中。

5．在 File 菜单中选择 Save 命令保存文本文件。

6．在 File 菜单中选择 Exit 命令退出 Notepad 或 WordPad。

5.5 创建一个口令文件字典

概述

Database Scanner 允许创建自己的口令字典。一些私人的口令，比如公司名称，可以并且应当被加入到所使用的 Database Scanner 的口令字典中。此字典文件也将以文本文件的形式进行存储。

操作步骤

创建一个口令字典，请遵照如下步骤：

1．在桌面上，点击 Start 菜单，选择 Programs→Accessories→Notepad 或 Programs→Accessories→WordPad。

2. 在此文本文件的开头，在单独的一行上输入一个口令后，按 Enter 键。
3. 重复步骤 2，将所希望添加的口令添加到口令字典中。
4. 在 File 菜单中选择 Save 命令保存文本文件。
5. 在 File 菜单中选择 Exit 命令退出 Notepad 或 WordPad。