GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Covering Your DataBases – An Overview of Database Scanner™
Joseph Rosario

Introduction

Not many people think about databases when you mention the words "Information Security". But if you were to ask where the corporation assets are, people are likely to answer "It's sitting on the XYZ server". So a conversation might take place about protecting the XYZ server. However, unless specifically asked you may never hear that the information you want protect actually is in a database that resides on the server. When you stop and think about it, no matter what industry you may be in, you have information you want to protect. Whether it is client lists, bank accounts, or product information, somebody somewhere can probably benefit by lifting this information from your database. The following is a discussion of basic database technology, topics surrounding scanning databases and an overview of Internet Security System's Database Scanner™.

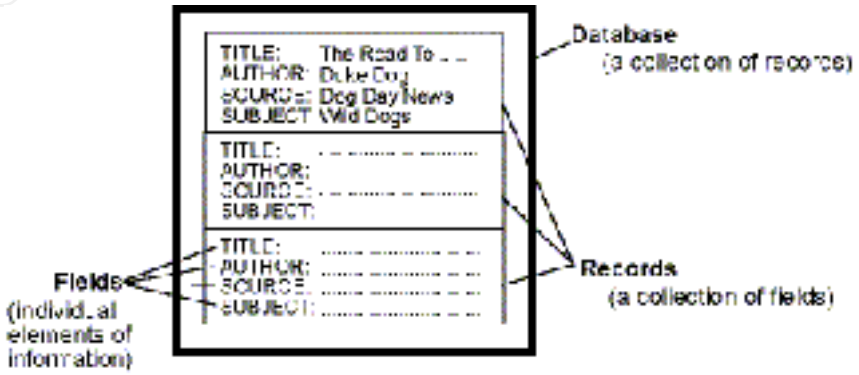
The Database Scanner™ is an automated tool that uncovers database security and to some extent operating system vulnerabilities. The Database Scanner™ can do this for various databases from a single machine. Below you will find notes on installation and the general use of this scanner. Because the subject of database security cannot be discussed without taking into account the security of the underlying operating system, you will be referred to various web-sites that provide further details on that particular subject.

Database Pieces

Before we can begin to talk about securing databases it is useful to understand a little bit about them. So first of all what defines a database? Like most things, the question will elicit different answers. One can simply think about a database as being a collection of data. These data can be just about anything. Several are examples are:

- Expenses
- Bank Accounts
- Human Resource (Salary Information and other personal info.)

Just about any information that you can think of is probably sitting on a database somewhere. The following illustration is helpful in understanding what the basic components of a database look like.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(**Figure 1:** Diagram found at http://www.lib.jmu.edu/library/gold/dbasdef.htm)

Taking this idea to a slightly different format brings us to the idea of a *Table*.

Title	Author	Source	Subject
The Road To..	Duke Dog	Duke Dog News	Wild Dogs

> The organizing principle in a relational database is the table, a rectangular row/column arrangement of data values. The relational database concept was originally developed by Dr. E.F. "Ted" Codd, an IBM researcher. In June 1970 Dr. Codd published an article entitled "A Relational Model of Data for large Shared Data Banks" that outlined a mathematical theory of how data can be stored and manipulated using a tabular structure.

This is very much like the format we see when we open a Microsoft Excel™ spreadsheet. If you were to open up a database (e.g. with Microsoft Enterprise Manager™) you will notice that the database is actually made up of several of these tables.

The following is a partial diagram of the sample database provided with Microsoft SQL. Additional items in the diagram are Stored Procedures, Users and others that we will discuss later. For now this diagram is meant to illustrate the idea of relational database.

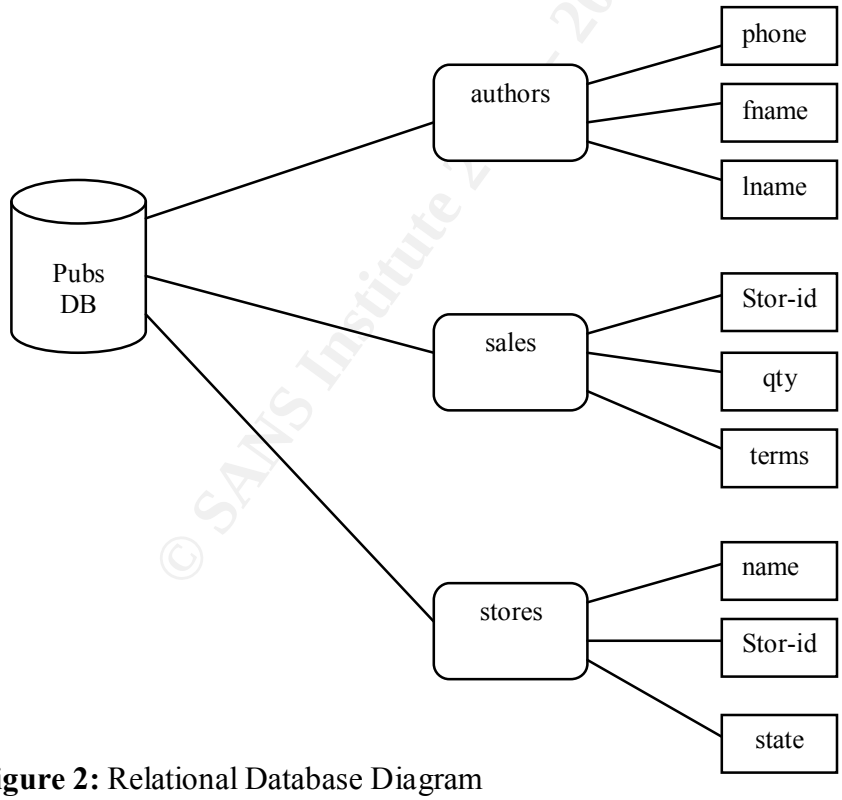


Figure 2: Relational Database Diagram

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DataHomeBase

A very significant point about databases is that these databases reside on platforms that have their own operating systems to be protected. Although databases have their own security controls they also inherit the security or insecurity of the operating systems they run on. As you can expect a weak non-secured operating system can allow a malicious person to copy off your valuable data. Conversely an unsecured database can lead someone right to the operating systems command prompt. So please remember to harden those operating systems as well. Included at the end of this document you will have a reference list that can get you started.

What are Database Vulnerabilities?

When you analyze the particulars of protecting an operating system, then examine what is needed to protect a database, you come to the realization that databases have parallel security controls. Databases have their own connectivity parameters, their own file ownership system control, authentication and so on. So in what security areas can the Database Scanner™ help? These areas are the same ones we have to worry about with an operating system.

- User ids and passwords
- Data Access
- Authentication
- Audits
- Known Vulnerabilities

Generally anything worth protecting should have some control over these areas. Experience will tell you that when it comes to analyzing the security aspects of computer systems and databases that you end up with dozens of detailed listings. For this reason several detailed checklists are referenced at the bottom of this document.

Database Scanner™

Before installing Database Scanner™ or any product, it is always a good idea to check what the requirements are for proper operation. But first how much disk space will you need? The software can be downloaded for evaluation at the link listed below. The file size is about forty-six megabytes.

Installation:

Database Scanner™ will install on Microsoft's Windows 2000™ and Microsoft's Windows NT 4.0™ systems. This is not to be confused with the operating systems that the databases run on. The databases that you may scan can reside on other operating systems. You will need at least sixty (60) megabytes for the actual program to install. However depending on how many databases you plan to scan and how long you want to keep your data, you may require up to two gigabytes of disk space. Check with your legal department and auditors to find out how long you must keep this data around. Because of this you should plan accordingly. Especially if you plan to scan Sybase™ or Oracle™ databases, these require separate driver installations.

© SANS Institute 2000 - 2002, Author retains full rights.

Specifically speaking, Windows NT™ requires service pack 6a at minimum. Windows 2000 will require at least Windows 200 service pack 1. The recommended processor speed is 400 Mhz and 256 Mbytes of installed RAM is recommended.

Database Scanner™ can scan different databases. However each database that you plan to scan needs to be at a certain software or patch revision. Microsoft's SQL Server™ versions are 8.0 with service pack 2 otherwise versions 7.0 or 6.5 can be scanned. The Sybase™ versions are 11.5, 11.9.2 or 12.0. Oracle™ versions are required to be at 7.3, 8.1.7 or 8.0.6. Although intermediate versions can probably be scanned, checking with the vendor is always a good idea.

Of course these varying versions of database systems run on different operating systems. The operating systems on which these databases reside can be Windows NT Server™ with SP4, SP5 or SP6a. The Unix flavors are as follows – Sun's Solaris™ 2.6 through 2.8, Hewlett Packard's HP-UX™ versions 10.20 or 11.0 and Red Hat Linux™ 6.2

- When you run the downloaded file, the program will tell you to run the setup program that it extracts.
- You then type a temp directory where you want the setup program to reside. Let's use dbtemp.
- Go to the dbtemp directory and run the setup program.
- Following the setup prompts is fairly trivial. The setup program however will remind you about the separate driver installation requirements for Sybase™ and Oracle™. If you plan to scan Microsoft SQL™ databases these drivers are automatically installed for you.
- Prepare for reboot. Setup program will prompt for a reboot when it is done.

If you require the Oracle™ driver's you must install SQL*NET or NET8 drivers on the computer that will be running the Database Scanner™. These drivers should have been included with the Oracle software your company purchased. You might want to visit your local database administrator for these.

If it's Sybase™ you are after, then the Sybase™ Adaptive Server OBDC driver and Open client Library drivers need to be installed on the system you plan to run the Database Scanner™. As stated above, you can probably get these from your database administrator.

In order to gain the fullest advantage of the Database Scanner™ you will need to supply the program with a logon user id. This id is the one that will be used to read the access tables, user ids and so on. You might think that this is "cheating". Well actually it is not. Remember that the goal here is to assess the vulnerabilities of the database. Although the program has a "penetration" mode, the main goal of any vulnerability scanner is to be able to identify all security holes that it was programmed to identify so that you can fix them!

Product Requirements can be found at
http://documents.iss.net/literature/DatabaseScanner/dbs_sysreq.pdf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Starting:

You will find the application under the menu "Programs->Iss->Database 4.2". The evaluation period is for fifteen (15) days. Click on the "I am in compliance with the License Agreement" bar.

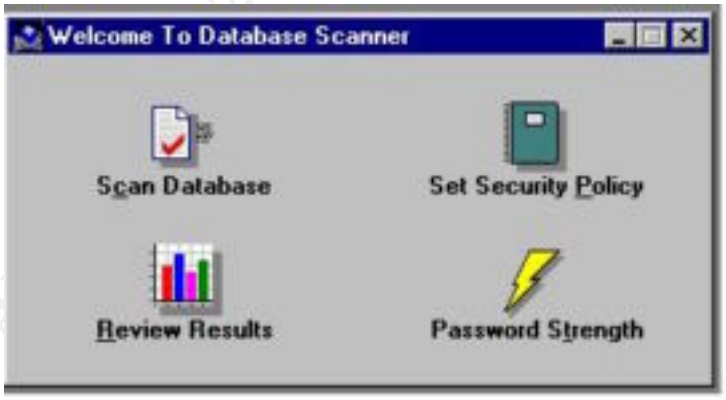
Now before we start anything let's make sure that we are using sample data. The "Sample Data" feature allows you to view sample reports without having to actually find a database that you can scan. As with any scanning software you may use, make sure you make appropriate arrangements with your company or client before scanning a live database. Verify and confirm that the folks that manage the database, your management, and other database administrators know about your intentions. Do you have a contingency plan in place?

To verify you are using sample data follow the steps outlined below.

1. Click on the "Scanner" pull-down menu and select options.
2. Then select "Sample Data". You will select "Show Live Data" once you decide to scan a real database. Otherwise you will see that "Show Sample Data" is selected.
3. Click "Ok".

The four main options on the screen are:

- Scan Database
- Set Security Policy
- Review Results
- Password Strength



Database Scanner's™ Main Menu

Before we discuss scanning databases, we should talk about what you should have in order to start. First you will need a license key from Internet Security Systems (ISS). This can be obtained by calling an 800 number or sending an email.

Secondly and perhaps more important is the fact that you should have a policy in place. A policy that says, that not only can you run this scanner, but also addresses the following areas.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Who is allowed to use the scanner?
- What is the proper use of the scanner?
- Who is authorized to grant access and approve usage?
- Who may have system administration privileges?
- What are the user's rights and responsibilities?
- What are the rights and responsibilities of the system administrator vs. those of the user?
- What do you do with sensitive information?

Other areas that of concern are:

- At what time can it be run and at what frequency?
- Who owns the information from the scanner?
- Who is authorized to view the reports?
- Who will fix the problems and by when?

The answers to these questions will help define how you are going to use the scanner as well as what database security policy will be placed on the product. When you speak of policy and scanners you should be aware that there are two different things we are talking about here. A policy within a scanner defines what to look for and sometimes the response. The other type of policy is your own corporate policy that defines people, procedures, practices etc.

Once a corporate policy is established that addresses the scanning of databases we can turn our attention towards the Database Scanner™ Security Policy tab.

In order to create or edit a security policy for the scanner, simply click on the "Set Security Policy" tab. This action will display a list of pre-configured policies labeled "Security Level 2 through 7. This is extremely convenient as it gives the user a starting point. You may consider starting with "Security Level 2" for a couple of reasons. You need to understand how the scanner will affect the performance of your database server and you don't want to be overwhelmed with items to fix. Below is how the product defines these levels.

Policy	This policy tests..
Level 2	The risk of compromise from simple attacks from unsophisticated external attackers
Level 3	Susceptibility to external system compromise from automated attack tools
Level 4	Resistance to password cracking and susceptibility to external compromise from very knowledgeable attackers
Level 5	Resistance to local users gaining enhanced or system administrator privilege to access unauthorized or restricted information.
Level 6	The integrity of the underlying operating system configuration on which the database is installed.
Level 7	The integrity of application data and customer specific application configurations against accidental or malicious changes.

The Levels are defined in "Database Scanner™ 4.2 Frequently Asked Questions"

There are three major areas that the Database Scanner™ addresses. These are Authentication, Authorization and System Integrity. Under Authentication section will find items like:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Stale Logins
- Guest User Ids
- Blank sa passwords

Examples of Authorization checks are:

- Allow Updates to System Tables
- Extended Stored Procedures

  Note: Extended stored procedures allow Microsoft SQL Server user to run external to SQL server. Other databases have similar problems with access to "cmdshell" (command shell) types of procedures.

- Logon Hours Violations

System Integrity checks include:

- Database Backups
- Auditing Levels
- Microsoft SQL Server™ Service Packs

The checks are detailed within the product itself. However a complete listing can be found at http://documents.iss.net/literature/DatabaseScanner/dbs_ps.pdf

Once you gain some experience with this you can then start tweaking the policy to fit your organizational needs. **Note:** Using the "Set Security Policy" tab allows you to edit or create a policy. It does not actually set or does it associate the policy for a given scan. You set the policy for a scan when you actually run the scan.
A particularly nice feature of the Database Scanner™ is that it can find existing databases for you. If you want, you can always manually define the database you want to scan. When you are ready to scan select the "Scan Database" tab. Selecting this will then present you with a menu that contains a *Network Neighborhood* expansion tree. Expanding this will show the following databases for selection: Microsoft SQL Server™, Sybase™ and Oracle™.

Within this context is where you actually select the policy you want run with a particular

© SANS Institute 2000 - 2 ...hor retains full rights.

database.

Policy Selection

When you have made your selection click on "Start Scan". When the scan has completed you can select "Review Results". The menu that opens for you allows you to select the database and the scan report for viewing. The nice thing here is that you can preview the report contents separately. So for example, you can see what the table of contents will look like independent from all of the other pages. This feature can save you a lot of time and paper.

To give you an idea of what is include in a standard report below are the table of contents.

- Executive Summary
- Summary of Violations
- Violation Details
- Differences
- Trend Analysis
- Check Status
- Policy Details
- Active Logins
- Audit Configurations
- Backups
- Configuration Options
- Database Summary
- Explicit Object Permissions
- Explicit User Permissions
- Extended Stored Procedures
- File Permissions
- Roles/Users
- Integrated Logins
- Logins
- Login Hours Violations
- Modified System Stored Procedures
- Password Aging
- Password Attacks
- Password Strength Analysis
- Stale Logins
- Statement Permissions

Table of Contents Report directly from Database Scanner™

Quite of few of these are self-explanatory. Others might not have an obvious definition. Listed below are ones worth defining.

Check Status: The "check' in check status refers to whether or not a particular security policy item failed, passed, or was not performed.

© SANS Institute 2000 - 2002, Author retains full rights.

Audit Configurations: This particular item tells you if the database you are scanning has the proper auditing parameters set. These parameters are tested against what you have defined in the security policy setting. It will also show you whether the database is set to audit anything at all. In other words is auditing turned on?

Integrated Logins: This section of the report lists those login ids that were shown to have been coming from an NT login. These are considered integrated from an operating system point of view.

Password Attacks: If you have this checked in your security policy the scanner will indicate whether or not there have been failed attempts at login in a short time. What's a short time? The time indicated is one minute.

Statement Permissions: What are these things? These items are very important to the security of your database. This report can indicate to you the permissions or "access rights" users have to Create a database, table, stored procedure and especially if the user has the permission to backup the database. Pay close attention to these items.

Remember that each of these items listed above can be selected or deselected for printing.

Password Strength

The "Password Strength" tab is essentially a built-in password cracker. With proper access to the users table from a database can be read and passwords attempted. All of the default password files are in the product's root directory. Most of these passwords are alpha. So if you want to try something fancy you need either to edit the existing file or create your own.

For The Privileged

To gain an appreciation to what the Database Scanner™ automatically discovers for you, let's examine the area of privileges. Privileges within this context can be compared to access rights. These rights or privileges in general are the ability to view, create, modify and run SQL commands. These translate to the following:

The **Select** privilege allows you to retrieve data from a table.

The **Insert** privilege allows you to insert new rows into a table.

The **Delete** privilege allows you to delete rows of data from a table

The **Update** privilege allows you to modify rows of data in a table.

Note: Your particular database may have variations and additional privileges. The privileges listed here are basic ones that most databases should allow you to define.

How does one provide access rights to users? In order for you to allow access to a database, you must be either the original owner/creator or you may have been given this right by the owner.

© SANS Institute 2000 - 2002, Author retains full rights.

You can use the database administration program (e.g. Microsoft Enterprise Manager™) or Structured Query Language (SQL)'s GRANT command to accomplish your individual assignment. No matter how you do it the process takes some work to complete. Now that you have finished you need to check you assignments once in a while as part of your security assessment cycle.

Even if your database supports the "Group" concept for access rights you can imagine that it would take a considerable amount of time manually checking these rights for hundreds of users on several databases. Luckily the Database Scanner™ has a report entitled "Explicit Object Permissions". Not only will the program automatically show you the privileges associated with users/groups and objects; it will also show where there are violations. How does it know that there exists a violation? You have to set this up in the Security Policy before hand. Recall the policy discussion above.

This was an example of access rights. You can only imagine the effort to manually check stale logins, weak passwords, patch levels on multiple platforms for many users.

Notice the violations listed in this sample report.
Source: Explicit Object Permissions; Sample report from Database Scanner™

Object Name: Orders **Owner:** dbo

	User ID/Group	Action	Type	Grantor
Violation	public	References	Grant	dbo
	public	Select	Grant	dbo
Violation	public	Insert	Grant*	dbo
Violation	public	Delete	Grant*	dbo
Violation	public	Update	Grant	dbo

Command Line Options

There will be times that running the graphical user interface will not be practical. For example you may be required to run a scan at midnight on a Sunday. You might want to automate scans for this purpose. Open up a DOS command window and change to the following directory: "Program Files\ISS\DBScan42". From here you will find the program "scan.exe". If you just run the program without any parameters then it will indicate to you what the parameters are for the command line. The program responds with: Usage: scan /S<server> /Y<server type> /C<policy> {/L<login> /P<password> | /T} [/H<host> /R<host account> /W<host password>]

The *server* is the database server name. The program will not accept a server name without the *server type*. The server types have been defined as "M" for Microsoft, "O" for Oracle and "S" for Sybase. The command line does not care if you use upper or lower case. An actual command line can look like this:

c:\program files\iss\dbscan42\scan /s**gh** /y**m** /c**security level 2** /l**sa** /p**password**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Where **gh** is the database server name, **security level 2** is the security policy you want run, **sa** is the system administrator's account name, and **password** is the "sa" password. Notice that without the database type in the command line, there is no way to distinguish the "security level 2" policy for Oracle vs. Sybase etc. As shipped, the scanner has identical security policy names for each type of database supported.

For a complete reference on the command line options see Database Scanner User's Guide

Penetration Mode

As mentioned earlier the idea of having the administrator's password is to gain a full perspective of the security controls that are lacking or in place. The idea of the penetration mode is to attempt to gain access to the database without the benefit of the administrator's password. You might think of this as being the state of security for the database from an outsider's point of view. The outsider could be anyone not authorized to access the database, this includes current employees. Although you need a separate license to run Internet Security's Internet Scanner, the Database Scanner can join forces with the Internet Scanner and give you a complete picture of your security posture. While the Internet Scanner main focus is operating system's vulnerabilities the two product's combined view allows you to fully understand how vulnerable your computer is from either the database point of view or the database point of view. Remember a vulnerability in either area can compromise the other.

You can access the penetration mode via the Scan Tab as pictured in the figure above. Along side the regular Scan you will see what is called the Penetration Test tab. You then proceed as if it were a regular scan. Select the server and the policy to run. Additional options are to run a full audit if access is gained and whether or not to perform a dictionary attack.

Conclusion

Database security continues to be one area that requires careful planning and understanding. User ids, access control, auditing and operating system security are areas that need to be addressed when looking to secure a database. Database Scanner™ assists in automating the identification of security violations within the database itself. In addition the Database Scanner™ has checks for the underlying operating system, patch levels, file protection and so on. Realize that when attacks are made for the purpose of stealing information a lot of this information is sitting on a database somewhere. Just recently InfoSecNews released the following piece on database security:

> Database Server Security Vulnerabilities Exposed
> "Research recently completed by Evans Data Corp. has found that database servers plugged into the Internet are highly vulnerable to security breaches.
> http://www.infosecnews.com/sgold/news/2002/01/30_05.htm

Overall the Database Scanner™ product is easy to install and run. It provides an easy to use menu system and it is not difficult to configure. The more difficult areas are establishing

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

corporate policies and controls for the proper use of this or any other scanning software. Other products that may be of interest are:

Database Security Manager from BrainTree
http://www.sqlsecure.com/Products/DSM/dsm.html

AppDetective by Application Security Inc.
http://www.appsecinc.com/

bv-Control for Microsoft SQL Server by Bindview
http://www.bindview.com/products/control/sql.cfm

BIBLOGRAPHY

Grodd, James R. and Weinberg, Paul N. The Complete Reference SQL. Berkeley: Osborne/McGraw Hill, 1999. 429 – 454.

Microsoft Corporation. Microsoft SQL Server - Administrator's Companion. 1995

Cooper, Frederic J., Goggans, Chris., Halvey, John K., Hughs, Larry., Morgan, Lisa., Karanjit, Holbrook, Paul J., Siyan., Stallings, William., Stephenson, Peter. Implementing Internet Security. Indianapolis: New Riders, 1995. 273 – 363.

Cameron, Lynn. James Madison University. "What is a Database?" URL: http://www.lib.jmu.edu/library/gold/dbasdef.htm (19 Jan. 2002)

Carnegie Mellon University. "Windows NT Security and Configuration Resources." 17 April 2000. URL: http://www.cert.org/tech_tips/win-resources.html (21 Jan 2002)

Carnegie Mellon University. "UNIX Security Checklist v2.0." 8 Oct. 2001. URL: http://www.cert.org/tech_tips/usc20_full.html (21 Jan 2002)

Spitzner, Lance. "Armoring Linux." 19 Sept. 2001. URL: http://www.enteract.com/~lspitz/linux.html (21 Jan 2002)

Internet Security Systems. "Useful Sites". URL: http://www.iss.net/security_center/useful_sites/ (21 Jan 2002)

Andrews, Chip. "SQL Server Security Checklist" 25 Nov. 2001. URL: http://www.sqlsecurity.com/ (23 Jan 2002)

Finnigan, Pete. "Oracle Security White Paper Series, Exploiting and Protecting Oracle". 24 Aug. 2001. URL: http://www.pentest-limited.com/oracle-security.htm (23 Jan 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Application Security Inc. “AppDetective™ for Oracle Security Audit Categories”. URL: http://www.appsecinc.com/products/appdetective/oracle/audit.html (23 Jan 2002)
Internet Security Systems. “Evaluation Form” URL: https://www.iss.net/cgi-bin/download/evaluation/evaluation-select.cgi (29 Jan 2002)

Internet Security Systems. “Database Scanner Product Specifications.” URL: http://documents.iss.net/literature/DatabaseScanner/dbs_sysreq.pdf (29 Jan 2002)

Internet Security Systems. “Database Scanner 4.2 Frequently Asked Questions.” October 2001. URL: http://documents.iss.net/literature/DatabaseScanner/dbs_faq.pdf (31 Jan. 2002)

Internet Security Systems. “Database Scanner User Guide 4.2.” September 2001. URL: http://documents.iss.net/literature/DatabaseScanner/DBS42_ug.pdf (28 Jan 2002)

Internet Security Systems. “Database Scanner”. URL: http://documents.iss.net/literature/DatabaseScanner/dbs_ps.pdf (28 Jan 2002)

© SANS Institute 2000 - 2002, Author retains full rights.