the CENTER for
INTERNET SECURITY

Oracle Database Security Benchmark v1.2
For Oracle Version 8i
Level 1 and Level 2

Agreed Terms of Use

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

1. No network, system, device, hardware, software or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

AGREED TERMS OF USE 3

INTRODUCTION 7

1. RECOMMENDED INSTALLATION & CONFIGURATION 7

1.1. OPERATING SYSTEM AND NETWORK SECURITY 7
1.2. INSTALLATION OF ORACLE SOFTWARE 7
1.3. ORACLE UPDATES AND PATCHES 7

2. RECOMMENDED SETTINGS 9

3. APPENDIX A – ADDITIONAL SETTINGS 39

4. APPENDIX B – DEFAULT USER ACCOUNTS 42

5. APPENDIX C – DISABLED WINDOWS 2000 SERVICES 48

Introduction

This guide provides high-level recommendations to secure an Oracle database. By configuring the database to the new benchmark, a secure baseline configuration is introduced to protect the system from the common "out of the box" vulnerabilities. This document is based in part on the SANS "Securing Oracle Step-by-Step" guide published January 2003[1] and reflects valuable comments provided by Oracle Corporation and other resources[2]. The scope of the document includes Oracle version 8i. Version 2.0 of this document support version 9i and 10g and can be downloaded from http://www.cisecurity.org. The intended audience for this document is the advanced database administrator in a managed enterprise environment. The novice administrator and home user should refer to the previously mentioned guidance documents, which contain detailed descriptions and explanations for hardening an Oracle database before reading this document. It is strongly recommended that these settings be reviewed to comply with local policy and tested on non-production systems before being deployed.

1. Recommended Installation & Configuration

This section presents various steps that can be adopted to securely install, setup, configure, and operate an Oracle database. The security of the Oracle database is a function of the security of the network and operating system that hosts the database.

1.1. Operating System and Network Security

- Implement the CIS Security Benchmarks for the operating system on the database host machine.
- Ensure that the database host machine is protected by a firewall.

1.2. Installation of Oracle Software

- Perform a clean installation on a secure network segment or off the network.
- If installation is on a Windows platform, ensure that the target volume is NTFS.
- Install the database with the minimum options that are required for the environment.
- Installation of the demo database is not recommended.
- Set the $TMP and $TMPDIR environment variables to a protected directory with access given only to the Oracle software owner and the ORA_INSTALL group.

1.3. Oracle Updates and Patches

- Ensure that all relevant security patches have been installed. The appropriate patches depend upon the options installed and the operating system of the database host.

[1] This resource is a copyright by SANS Institute, for information on the purchase of this document, please visit http://store.sans.org/store_item.php?item=80

[2] Other Oracle security resources referenced;

- Oracle Metalink (http://metalink.oracle.com/)
- Pete Finnigan.com (http://www.petefinnigan.com/orasec.htm)

- Subscribe to the Oracle Security mailing list to stay current with the Oracle security bulletins. To subscribe to the list, go to http://otn.oracle.com/deploy/security/alerts.htm and follow the link labeled “Current Alerts (Subscribe to security alerts)” to electronically register for the alerts.

2. Recommended Settings

This section contains recommendations for securing an Oracle database. The recommendations should be implemented with consideration to the particular database and application environment. Some of the suggested security settings may be overridden by local policy. It is important to note that the parameters and their values need to be spelled correctly to ensure the desired policy has been implemented. Many of the parameters and settings, if misspelled, will not cause an error or warning message to be generated. As a convention, the pfile is referred to as init.ora though this file will most likely be named differently in an actual implementation (i.e. init*SID*.ora).

The recommendations are presented in tables with the following columns:

- Configuration Item – specific area that requires configuration or policy recommendation.
- Action/Recommended Parameter – recommendation for specific setting or policy of the configuration item.
- Comments – concise comments pertaining to the recommendation.
- OS VER – denotes whether the setting is applicable to an operating system of Windows (W), Unix (U), or Both (B).
- Score – a Y setting indicates that the recommendation will be scored by the tool. An R setting indicates that the recommendation will be reportable by the tool - that is a numeric score may not be generated, but a report of the configuration can be presented by the tool for review. A scorable item (Y) implies that it is also reportable (R). A setting of N indicates that the recommendation will not be scorable or reportable by a tool.
- Level – The recommendations are divided into three categories: Level 1, Level 2, and Appendix.
  - Level 1 recommendations meet the following criteria:
    - Represent a minimum baseline that is suggested for most environments
    - Easily implemented by someone with minimal background and not likely to break database or application functionality
    - Can be scored with a tool
  - Level 2 recommendations may require an advanced level DBA to implement and/or may break database or application functionality.
  - Appendix items are suggestions rather than recommendations for further hardening of the database environment. These are not likely applicable to most environments or may not be “strictly” within the realm of database security.

Host Files							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
1.01	Files in $ORACLE_HOME/ bin	Verify ownership	Verify that all files in the $ORACLE_HOME/bin are owned by the Oracle software account. In Windows, this account needs to be part of the Administrators group.	8i	B	Y	1
1.02	Files in $ORACLE_HOME/ bin	Permissions set to 0751 or less on Unix systems	Ensure that all files in the $ORACLE_HOME/bin directory have permissions set to 0751 or less.	8i	U	Y	1
1.03	Files in $ORACLE_HOME (not including $ORACLE_HOME/ bin)	Permissions set to 0750 or less on Unix systems	Ensure that all files in $ORACLE_HOME directories (except for $ORACLE_HOME/bin) have permission set to 0750 or less. Users logged into the server who are not members of the dba group will not be able to run applications such as SQL*Plus if this recommendation is followed.	8i	U	Y	1
1.04	Oracle account .profile file	Unix systems umask 022	Ensure the umask value is 022 for the owner of the Oracle software before installing Oracle. Generally, the Oracle .profile account is where the umask will be set, however it could be set in other places. Regardless of where the umask is set, ensure it is set to 022 before installing Oracle.	8i	U	Y	1
1.05	init.ora	Verify permissions	Contains database startup parameters. File permissions should be restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.07	Database datafiles	Verify permissions	File permissions should be restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.08	init.ora	Verify permissions of file referenced by ifile parameter	If the ifile functionality is used, check the permissions and contents of the ifile to ensure validity and to prevent users from reading the file. As with the init.ora file, the file permissions of the referenced ifile should be restricted to the Oracle software owner and the dba group.	8i	B	Y	1
1.09	init.ora	_trace_files_public= FALSE	Prevents users from having the ability to read trace files.	8i	B	Y	1
1.10	init.ora	global_names= TRUE	Ensures that Oracle will check that the name of a database link is the same as that of the remote database.	8i	B	Y	1
1.11	init.ora	max_enabled_roles	This should be limited as much as possible. Typically,	8i	B	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
		=30	SYS gets 20 roles by default.				
1.12	init.ora	remote_os_authent= FALSE	Prevents a connection without a password.	8i	B	Y	1
1.13	init.ora	remote_os_roles= FALSE	Prevents connection spoofing.	8i	B	Y	1
1.15	init.ora	audit_trail parameter set to OS, DB, or TRUE	Ensures that basic audit features are used. Recommend setting audit_trail to OS as it reduces the likelihood of a Denial of Service attack and it is easier to secure the audit trail. OS is required if the auditor is distinct from the DBA. Any auditing information stored in the database is viewable and modifiable by the DBA.	8i	B	Y	1
1.16	init.ora	audit_file_dest parameter settings	Set to a valid directory owned by oracle set with owner read/write permissions only. Default logging of startup, shutdown and privileged connections will be written to this directory. If the audit trail parameter is set to OS on Unix systems, other auditing information will also be written here. Windows systems will log to the Event Viewer if audit trail parameter is set to OS.	8i	U	Y	1
1.17	init.ora	user_dump_dest parameter settings (see comments)	Set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.18	init.ora	background_dump_dest parameter settings	Set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.19	init.ora	core_dump_dest parameter settings	Set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.20	init.ora	control_files parameter settings	Ensure the permissions are restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.21	init.ora	os_authent_prefix="" (A null string)	Setting this ensures that the only way an account can be used externally is by specifying IDENTIFIED EXTERNALLY when creating a user.	8i	B	Y	1
1.22	init.ora	os_roles=FALSE	O/S roles are subject to control outside the database. This separates the duties and responsibilities of DBAs and system administrators.	8i	B	Y	1
1.23	init.ora	Settings for utl_file_dir	Do not use the following settings: "*" – Allows access to any file	8i	B	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
		parameter should avoid certain directories (see comments)	Any trace file directories – Critical information could be read "." – Allows access to the current directory Location of the core dump trace files – Critical information could be read Any other directories where sensitive information might be found.				
1.25	init.ora	log_archive_dest _n parameter settings	Only applicable if archivelog mode is used for database. File permissions should be restricted to the owner of the Oracle software and the dba group. For complex configurations where different groups need access to the directory, suggest using access control lists in Unix. The archive logs should be secured as LogMiner could be used to extract database information from the archive logs. Note: If Oracle Enterprise Edition is installed, and no log_archive_dest_n parameters are set, the deprecated form of log_archive_dest may be used.	8i	B	Y	1
1.26	init.ora	log_archive_duplex_ dest parameter settings	Only applicable if archivelog mode is used for database and the deprecated form of log_archive_dest is used as per the note in Item 1.27. If this parameter is used, set to a valid directory owned by oracle set with owner and group read/write permissions only. For complex configurations where different groups need access to the directory, suggest using access control lists in Unix. The archive logs should be secured as LogMiner could be used to extract database information from the archive logs	8i	B	Y	1
1.27	init.ora	log_archive_start= TRUE	Ensures that archiving of redo logs is done automatically and prevents suspension of instance operations when redo logs fill. Only applicable if archivelog mode is used for database. See note in item 3.38.	8i	B	Y	1
1.28	init.ora	sql92_security= TRUE	This parameter will enforce the requirement that a user must have SELECT privilege on a table in order to be able to excute UPDATE and DELETE statements using WHERE clauses on a given table.	8i	B	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
1.29	listener.ora	Change default name of listener	Avoid calling the listener by the default name – select a distinct name instead.	8i	B	Y	1
1.30	listener.ora	Use IP addresses rather than hostnames	Use IP addresses rather than host names in the listener.ora file to eliminate unnecessary dependencies on a DNS server. From an administrative standpoint DNS is preferable, but from a security standpoint the dependencies on a DNS server are discouraged.	8i	B	Y	1
1.31	listener.ora	Verify permissions	File permissions should be restricted to the owner of the Oracle software and the dba group. If backup copies of the listener.ora file are created (for example when using utilities to modify the listener.ora file) ensure that these backup files are removed or the permissions are also set correctly.	8i	B	Y	1
1.32	tkprof	Remove from system	The tkprof utility is useful in reading trace files and should be removed from production environments. If tkprof must remain on the production system, ensure that it is protected. Set file permissions of 0750 or less on Unix systems. On Windows systems, ensure that only required users have access and that Everyone does not have access.	8i	B	Y	1
1.33	Files in $ORACLE_HOME/ network/admin directory	Verify permissions	Ensure permissions for all files are restricted to the owner of the Oracle software and the dba group. This setting is intended for the database server. Note: If an application that requires access to the database is also installed on the database server, the user the application runs as must have read access to the tnsnames.ora and sqlnet.ora files.	8i	B	Y	1
1.34	webcache.xml	Verify permissions	Contains weakly encrypted passwords. File permissions should be restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.35	snmp_ro.ora	Verify permissions	File permissions should be restricted to the owner of the Oracle software and the dba group. Preferably this service should not be enabled, but if required, set permissions as recommended.	8i	B	Y	1
1.36	snmp_rw.ora	Verify permissions	Contains Intelligent Agent passwords. File permissions should be restricted to the owner of the	8i	B	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			Oracle software and the dba group. Preferably this service should not be enabled, but if required, set permissions as recommended.				
1.37	sqlnet.ora	Verify permissions	File permissions should be restricted to the owner of the Oracle software and the dba group. This setting is intended for the database server. Note: If an application that requires access to the database is also installed on the database server, the user the application runs as must have read access to the sqlnet.ora file.	8i	B	Y	1
1.38	sqlnet.ora	log_directory_client parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. If not set in the sqlnet.ora file, the default is the current working directory and failed connection attempts will generate sqlnet.log entries in these unprotected directories. Setting this parameter will ensure a single log file is created in a known location rather than several log files created in many locations.	8i	B	Y	1
1.39	sqlnet.ora	log_directory_server parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. If not set in the sqlnet.ora file, the default is $ORACLE_HOME/network/log.	8i	B	Y	1
1.40	sqlnet.ora	trace_directory_ client parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. This is the destination directory for client-side trace files. If not set in the sqlnet.ora file, the default is $ORACLE_HOME/network/log.	8i	B	Y	1
1.41	sqlnet.ora	trace_directory_ server parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. This is the destination directory for server-side trace files. If not set in the sqlnet.ora file, the default is $ORACLE_HOME/network/log.	8i	B	Y	1
1.42	listener.ora	admin_restrictions_ *listener_name*=on	Replace *listener_name* with the actual name of your listener(s) for this parameter setting. The listener password can be brute forced and thereby allow a hacker to make modifications to the listener. This restriction prevents run time modification to the	8i	B	Y	1

Host Files							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
			listener.ora parameters as the listener will refuse to accept SET commands. Changes can be made by modifying the listener.ora file and issuing a RELOAD command.				
1.43	listener.ora	log_file_listener parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. If not set in the listener.ora file, the default is $ORACLE_HOME/network/log/listener.log.	8i	B	Y	1
1.44	listener.ora	logging_listener=ON	If not set in the listener.ora file, the default is ON. However, if the listener logging is turned off, some information that might indicate an attack on the listener will be unavailable.	8i	B	Y	1
1.45	listener.ora	trace_directory_*listener_name* parameter settings	Set to a valid directory owned by oracle set with owner and group read/write permissions only. If not set in the listener.ora file, the default is $ORACLE_HOME/network/trace	8i	B	Y	1
1.46	listener.ora	trace_file_*listener_name* parameter settings	If not set in the listener.ora file, the default is *listener_name*.trc. This file should be owned by oracle set with owner and group read/write permissions only.	8i	B	Y	1
1.47	Redo logs	Mirror	Ensure that on-line redo logs are mirrored and that more than one group exists.	8i	B	Y	1
1.48	Control files	Mirror	Ensure that the control files are mirrored.	8i	B	Y	1
1.49	Archive log files	Backup	If archivelog mode is used, ensure that archive log files are saved to tape or to a separate disk. File permissions should be restricted to the owner of the Oracle software and the dba group. The archive logs should be secured as LogMiner could be used to extract database information from the archive logs.	8i	B	N	1
1.50	svrmgrl	Verify permissions	Ensure the permissions of the binaries for svrmgrl on the server are restricted to the owner of the Oracle software and the dba group. If host based access to the database is not required, disable access to the binaries.	8i	B	Y	1
1.51	sqlplus	Verify permissions	Ensure the permissions of the binaries for sqlplus on the server are restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.52	htaccess	Verify permissions	Contains Apache passwords. File permissions should	8i	B	Y	1

Host Files

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			be restricted to the owner of the Oracle software and the dba group. Preferably this service should not be enabled, but if required, set permissions as recommended.				
1.53	wdbsvr.app	Verify permissions	Contains mod_plsql passwords. File permissions should be restricted to the owner of the Oracle software and the dba group.	8i	B	Y	1
1.54	xsqlconfig.xml	Verify permissions	May contain usersnames and passwords used by HTTP to connect to the database using the XSQL servlet. File permissions should be restricted to the owner of the Oracle software and the dba group. This file is present only if XML/SQL Servlet is installed.	8i	B	Y	1
1.55	otrace	Disable	The otrace utility has been reported to cause performance problems as the .dat files grow in size. Oracle Metalink note 1020763.6 provides detail regarding this. To disable otrace Metalink note 192541.995 suggests the following: Go to the $ORACLE_HOME/otrace/admin directory of your instance and remove or delete the dat files related to otrace. Do this for all *.dat files in this directory.	8i	B	Y	1
1.56	Windows platform	Do not install Oracle on a domain controller	Extreme risk arises if an Oracle server is compromised on a domain controller. Instead, install Oracle on a domain member server or a stand alone server.	8i	W	Y	1
1.57	Windows Services	Disable or remove unnecessary Windows services, e.g., OracleOraHome90HTTPServer.	Limiting services limits exposures to possible unknown vulnerabilities. Refer to Appendix C for recommendations on which Windows 2000 Services to disable.	8i	W	Y	1
1.58	Windows Networking	Remove all unnecessary protocol stacks except TCP/IP.	Limiting protocol stacks limits exposures to possible unknown vulnerabilities.	8i	W	Y	1
1.59	Windows Administrator’s Account	Rename the local computer’s Administrator account	The default name is well known.	8i	W	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
1.60	Windows Oracle Account	Use local administrator account	Run the Oracle services using a local administrator account created specifically for Oracle. Deny Log on Locally to this account. (Note: On Windows, Oracle requires use of an administrator account or System; otherwise, Oracle service errors may occur.)	8i	W	Y	1
1.61	Windows Oracle Domain Account	Use restricted service account (RSA)	If the Oracle services require domain resources, then the server should be a domain server and the Oracle services should be run using a restricted service account (RSA), i.e., restricted domain user account. The account is a domain user account, not a domain administrator account. It should be added to the local administrators group on the server running the Oracle services.	8i	W	Y	1
1.62	Windows Oracle Domain Global Group	Create a global group for the RSA and make it the RSA's primary group	The RSA account is not an account that should have access to resources that all domain users have a need to access. Note: Do not assign any rights to the group.	8i	W	Y	1
1.63	Windows Oracle Account Domain Users Group Membership	Remove the RSA from the Domain Users group	The RSA should have limited access requirements.	8i	W	Y	1
1.64	Windows Oracle Domain Network Resource Permissions	Verify permissions	Give the appropriate permissions to the RSA or global group for the network resources that are required. The RSA should have limited access requirements.	8i	W	N	1
1.65	Windows Oracle Domain Account Logon to… Value	Limit to machine running Oracle services	The RSA has no requirement to log onto domain computers, but must have a workstation set on the domain controller. Configure the RSA to only log on to the computer that is running the Oracle services and on the actual computer deny the right to Log on locally as the RSA.	8i	W	Y	1
1.66	Windows Local Users Group Membership	Remove Domain Users from Users group	If the server is a domain server, then remove the Domain Users group from the local computer's Users group. Only required users and administrators require access to the server.	8i	W	Y	1
1.67	Windows Directory Permissions	Verify permissions	Remove the Everyone Group from the installation drive or partition and give System and local	8i	W	Y	1

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			Administrators Full Control. Only required users and administrators require access to the Oracle installation drive or partition. The RSA is part of the local Administrators Group.				
1.68	Windows Program Folder Permissions	Verify permissions	Remove permissions for the Users group from the [OS drive]:\Program Files\Oracle folder. The Oracle program installation folder should allow limited access.	8i	W	Y	1
1.69	Windows Tools Permissions	Verify permissions	Tighten the permission on tools (*.exe) in the WINNT and System32 folders, e.g., only Administrators should have permissions on these files; however, deny access to the Oracle service account. Although the Oracle service account is an administrator account, it should be denied access to executables.	8i	W	Y	1
1.70	Windows HKLM Registry Key Permissions	Remove the Everyone group on the HKLM key.	There is no need for Everyone to be able review registry settings.	8i	W	Y	1
1.71	Windows Oracle Registry Key Permissions	Verify permissions	Give Full Control over the HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE key to the account that will run the Oracle services and remove the local Users group if it's not required. Give read permissions to those users that require it. Access to the Oracle registry key should be limited to those users that require it. Appropriate permissions should be set.	8i	W	Y	1
1.72	Windows Oracle Registry Key Setting	Set OSAUTH_ PREFIX_DOMAIN registry key to TRUE	This setting is only applicable to Windows systems. If externally identified accounts are required, this setting forces the account to specify the domain which prevents spoofing of user access from an alternate domain or local system. This registry key should be created or updated in `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES`	8i	W	Y	1

Database Access							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
2.01	Database Profiles	failed_login_attempts =3	Number of consecutive unsuccessful login attempts before account is locked. Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database. Application accounts should be set for failed_login_attempts=1.	8i	B	Y	1
2.02	Database Profiles	password_life_time= 90	Number of days before a password expires and must be changed. Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.	8i	B	Y	1
2.03	Database Profiles	password_reuse_ max=20	Number of password changes before the current password can be reused. This setting must be set to unlimited if a password_reuse_time value other than unlimited is defined for Oracle versions earlier than 9i. See Metalink DocID 228991.1 to see the Oracle version specific relationship of this setting with the password_reuse_time setting. Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.	8i	B	Y	1
2.04	Database Profiles	password_reuse_ time= 365	Number of days before the current password can be reused. This setting must be set to unlimited if a password_reuse_max value other than unlimited is defined for Oracle versions earlier than 9i. See Metalink DocID 228991.1 to see the Oracle version specific relationship of this setting with the password_reuse_max setting. Local policy may override the recommend setting. This setting may not be applicable for middle tier application accounts that access the database.	8i	B	Y	1
2.05	Database Profiles	password_lock_time= 1	Number of days to lock an account. Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.	8i	B	Y	1

Database Access							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
2.06	Database Profiles	password_grace_time=3	Number of days to permit a password change after the password has expired. Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.	8i	B	Y	1
2.07	Tablespaces	Do not have default_tablespace set to SYSTEM for user accounts	Avoid having user accounts with default tablespace of SYSTEM. Typically, only SYS should have a default tablespace of SYSTEM. May be difficult or impossible to move some objects.	8i	B	Y	1
2.08	Tablespaces	Do not have temporary_tablespace set to SYSTEM for user accounts	Avoid having any account (including SYS) with temporary tablespace of SYSTEM.	8i	B	Y	1
2.10	Tablespaces	Ensure application users have not been granted quotas on tablespaces.	This prevents the possibility of a denial of service type attack by filling up disk space. Consider establishing quotas for developers on shared production/development systems to prevent space resource contention.	8i	B	Y	1
2.11	Any dictionary object	Review access	Check for any user that has access to any dictionary object and revoke where possible.	8i	B	R	1
2.12	Tables	Limit access to SYS.AUD$	Check for any user other than SYS and DBA accounts that have access and revoke where possible. This is only applicable if the audit trail parameter is set to DB or TRUE.	8i	B	Y	1
2.13	Tables	Limit access to SYS.USER_HISTORY$	Revoke access to this table from all users and roles except for SYS and DBA accounts.	8i	B	Y	1
2.14	Tables	Limit access to SYS.LINK$	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.15	Tables	Limit access to SYS.USER$	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.16	Tables	Limit access to SYS.SOURCE$	Check for any user other than SYS and DBA accounts that have access and revoke where possible.	8i	B	Y	1
2.17	Tables	Limit access to PERFSTAT.STATS$SQLTEXT	Check for any user that has access and revoke where possible	8i	B	Y	1

Database Access							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
2.18	Tables	Limit access to PERFSTAT.STATS$ SQL_SUMMARY	Check for any user that has access and revoke where possible	8i	B	Y	1
2.19	Tables	Limit access to any X$ table	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.20	Views	Limit access to any DBA_ view	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.21	Views	Limit access to any V_$ view	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.22	Views	Limit access to ALL_SOURCE	Check for any user other than SYS that has access and revoke where possible.	8i	B	Y	1
2.23	Views	Limit access to DBA_ROLES	Restrict access to this view to all users except SYS and DBAs. If recommendation 2.20 has been implemented, this is superfluous.	8i	B	Y	1
2.24	Views	Limit access to DBA_SYS_PRIVS	Restrict access to this view to all users except SYS and DBAs. If recommendation 2.20 has been implemented, this is superfluous.	8i	B	Y	1
2.25	Views	Limit access to DBA_ROLE_PRIVS	Restrict access to this view to all users except SYS and DBAs. If recommendation 2.20 has been implemented, this is superfluous.	8i	B	Y	1
2.26	Views	Limit access to DBA_TAB_PRIVS	Restrict access to this view to all users except SYS and DBAs. If recommendation 2.20 has been implemented, this is superfluous.	8i	B	Y	1
2.27	Views	Limit access to DBA_USERS	Restrict access to this view to all users except SYS and DBAs. If recommendation 2.20 has been implemented, this is superfluous.	8i	B	Y	1
2.28	Views	Limit access to ROLE_ROLE_PRIVS	Restrict access to this view to all users except SYS and DBAs.	8i	B	Y	1
2.29	Views	Limit access to USER_TAB_PRIVS	Restrict access to this view to all users except SYS and DBAs.	8i	B	Y	1
2.30	Views	Limit access to USER_ROLE_PRIVS	Restrict access to this view to all users except SYS and DBAs.	8i	B	Y	1
2.31	Roles	Limit assignment of roles that have _CATALOG_	Revoke any catalog roles from those roles and users that do not need them. These roles are SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE, DELETE_CATALOG_ROLE, and	8i	B	R	1

Database Access

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			RECOVERY_CATALOG_OWNER.				
2.32	Synonyms	Limit access to any V$ synonym	Check for any user that has access and revoke where possible.	8i	B	Y	1
2.33	Privileges	Restrict system privileges	All system privileges except for CREATE SESSION should be restricted to DBAs, application object owner accounts/schemas (locked accounts) and default Oracle accounts. Developers may be granted limited system privileges as required on development databases.	8i	B	Y	1
2.34	Privileges	Limit granting of privileges that contain the keyword ANY	Check for any user or role that has the “ANY” keyword and revoke this role where possible.	8i	B	Y	1
2.35	Privileges	Limit granting of ALL PRIVILEGES	The GRANT ALL PRIVILEGES statement is similar to granting the DBA role with the addition of UNLIMITED TABLESPACE privileges. There should be no reason to grant these privileges to any user.	8i	B	N	1
2.37	Privileges	Limit granting of privileges that have WITH ADMIN	Check for any user or role that has been granted privileges “with admin” and revoke where possible.	8i	B	Y	1
2.38	Privileges	Limit granting of privileges that have WITH GRANT	Check for any user or role that has been granted privileges “with grant” and revoke where possible.	8i	B	Y	1
2.39	Privileges	Limit granting of privileges that have CREATE	Check for any user that has object creation privileges and revoke where possible.	8i	B	Y	1
2.40	Privileges	Limit granting of CREATE LIBRARY	The CREATE LIBRARY privilege can be used to access operating system files and gain and escalation of privileges on the operating system. Check for any user or role that has this privilege and revoke where possible.	8i	B	Y	1
2.41	Privileges	Limit granting of ALTER SYSTEM	Check for any user or role that has this privilege and revoke where possible.	8i	B	Y	1
2.42	Privileges	Limit granting of CREATE PROCEDURE	Check for any user or role that has this privilege and revoke where possible.	8i	B	Y	1
2.43	Privileges	Limit granting of BECOME USER	Check for any user or role that has this privilege and revoke where possible.	8i	B	Y	1

Database Access							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
2.44	Privileges	Limit granting of SELECT ANY TABLE	Check for any user that has access and revoke where possible. If application data is sensitive, and it is possible, revoke this privilege from the DBA accounts as well.	8i	B	Y	1
2.45	Privileges	Limit granting of AUDIT SYSTEM	Review which users have audit system privileges and limit as much as possible to ensure audit commands are not revoked.	8i	B	Y	1
2.46	Privileges	Grant privileges to roles rather than individual user accounts	Granting of privileges to roles rather than individual users may aid in administration. This method ensures that the same privileges are assigned to users performing the same job functions.	8i	B	Y	1
2.47	Privileges	Review privileges granted to PUBLIC	Review all privileges granted to PUBLIC. Limit or revoke unnecessary PUBLIC privileges.	8i	B	R	1
2.48	Roles	Limit assignment of RESOURCE	Revoke the resource role from normal application user accounts. Although the query, “select privilege from sys.dba_sys_privs table where grantee = ‘RESOURCE’;” does not show UNLIMITED_ TABLESPACE, a user granted RESOURCE will have an unlimited quota on SYSTEM even after the quota is set to 0. UNLIMITED_TABLESPACE overrides any explicit tablespace quotas.	8i	B	Y	1
2.49	Roles	Limit assignment of CONNECT	Revoke connect role from normal application user accounts. The CONNECT role is much more than “CREATE SESSION”.	8i	B	Y	1
2.50	Roles	Limit assignment of DBA	Revoke dba role from users who do not require it. Consider creating a sanitized version of the dba role with only those privileges that are necessary.	8i	B	R	1
2.51	Packages	Limit or deny access to UTL_FILE	Revoke the public execute privilege on utl_file as it can be used to access O/S	8i	B	Y	1
2.52	Packages	Limit or deny access to UTL_TCP	Revoke the public execute privilege on utl_tcp as it can write and read sockets.	8i	B	Y	1
2.53	Packages	Limit or deny access to UTL_HTTP	Revoke the public execute privilege on utl_http as it can write content to a web browser.	8i	B	Y	1
2.54	Packages	Limit or deny access to UTL_SMTP	Revoke the public execute privilege on utl_smtp as it can send mail from the database server.	8i	B	Y	1
2.55	Packages	Limit or deny access to DBMS_LOB	Revoke the public execute privilege. The package can be abused and relative paths can be used to	8i	B	Y	1

Database Access							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			access any file in any directory.				
2.56	Packages	Limit or deny access to DBMS_SYS_SQL	Revoke the public execute privilege. Package can be used to run PL/SQL and SQL as the owner of the procedure rather than the caller.	8i	B	Y	1
2.57	Packages	Limit or deny access to DBMS_JOB	Revoke the public execute privilege. The package can be abused to run scheduled jobs on the database.	8i	B	Y	1
2.58	Access to database objects by a fixed user link	Disallow	Fixed user database links which have a hardcoded username and password should be avoided.	8i	B	Y	1
2.59	Listener password	Encrypt the listener password	Set an encrypted password for the listener. The listener does not have a password set. Setting an encrypted password for the listener protects the listener from shutting down the listener, showing the services, or changing the listener settings.	8i	B	Y	1

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
3.01	Oracle alert log file	Review contents	The Oracle alert log file should be regularly reviewed for errors.	8i	B	N	1
3.02	listener.log file	Review contents	Regularly review the listener.log file for failed attempts to connect to the listener. Also periodically roll and archive the listener.log file. On Windows systems, rolling the log file will require stopping and starting the listener. An exceptionally large listener.log file may impact performance due to the log file being opened, appended to, and closed for each connection.	8i	B	N	1
3.03	http://otn.oracle.com/deploy/security/alerts.htm	Review for security alerts	Regularly check the Oracle security alert page on http://otn.oracle.com/deploy/security/alerts.htm.	8i	B	N	1
3.04	v_$resource_limit	Review	Ensure the database is not approaching the limits of the resources allocated.	8i	B	Y	1
3.05	Service or SID name	Non-default	Do not use the default SID or service name of ORCL.	8i	B	Y	1

Policy and Procedure							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
3.06	Database creation scripts on host	Remove or secure	Databases may be created using the Database Configuration Assistant, which can be set to store database creation scripts on the server (by default they will be placed in the $ORACLE_HOME/ assistants/dbca directory). Database creation scripts may also be created via home grown scripts written by the DBA. Database creation scripts may contain username and password combinations. After the database has been created, remove the scripts or at a minimum move them to a safe repository area. NOTE: Scripts may also be created in $ORACLE_BASE/admin/$ORACLE_SID/scripts/	8i	B	Y	1
3.07	Unix root group members on host	Disallow oracle as member of root group	Ensure that the Oracle software owner account is not a member of the root group on Unix systems.	8i	U	Y	1
3.08	Oracle DBA group membership on host	Review	Review the membership of the DBA group on the host to ensure that only authorized accounts are included. This should be limited to users who require DBA access.	8i	B	R	1
3.09	Sensitive information in process list on host	Avoid or encrypt	An enforced policy should exist to ensure that no scripts are running that display sensitive information in the process list such as the Oracle username and password. Suggest using a privileged process to get and decrypt encrypted passwords.	8i	B	N	1
3.10	Sensitive information in cron jobs on host	Avoid or encrypt	An enforced policy should exist to ensure that no cron jobs have sensitive information such as database username and passwords. Suggest using a privileged process to get and decrypt encrypted passwords.	8i	U	N	1
3.11	Sensitive information in AT jobs on host	Avoid or encrypt	An enforced policy should exist to ensure that no AT jobs have sensitive information such as database username and passwords. Suggest using a privileged process to get and decrypt encrypted passwords.	8i	W	N	1
3.12	Sensitive information in environment variables on host	Avoid or encrypt	An enforced policy should exist to ensure that no users have unencrypted sensitive information such as database username and passwords set in environment variables. Suggest using a privileged process to get and decrypt encrypted passwords.	8i	B	N	1
3.13	Sensitive	Avoid or encrypt	An enforced policy should exist to ensure that no	8i	B	N	1

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
	information in batch files on host		batch files have unencrypted sensitive information such as database username and passwords. Suggest using a privileged process to get and decrypt encrypted passwords.				
3.14	Oracle file locations	Separate for performance	Split the location of the Oracle software distribution, redo logs, data files, and indexes onto separate disks and controllers for resilience.	8i	B	Y	1
3.15	Filesystems	Separate Oracle files from non-Oracle files	Only put database files on filesystems exclusively used by Oracle. Ensure that no Oracle files are on the same partition as the operating system, especially in a Windows environment.	8i	B	Y	1
3.16	Optimal Flexible Architecture	Implement	Follow the Oracle Optimal Flexible Architecture guidelines to provide for consistency and ease of administration.	8i	B	N	1
3.17	Checksum PL/SQL code	Implement	Store the checksum results and periodically check for alterations.	8i	B	N	1
3.18	All database objects	Monitor	Store the results of the time stamps of the creation, reload, and compilation of database objects and review the results regularly to ensure no unauthorized changes have occurred.	8i	B	N	1
3.19	Ad-hoc queries on production databases	Avoid	Disallow ad-hoc queries on production databases. This recommendation may not be suitable for all environments, for example, data warehouses.	8i	B	N	1
3.20	Media integrity	Verify	Backup media integrity should be checked regularly.	8i	B	N	1
3.21	Remote shell access on host	Encrypt session	If remote shell access is required, use ssh or a VPN solution to ensure that session traffic is encrypted. In a cluster environment (RAC or OPS) rsh and rcp are required between the nodes for the Oracle software owner. In the case of a cluster environment, the access should be restricted by user and host.	8i	B	N	1
3.22	Applications with database access	Review	Review and control which applications access the database.	8i	B	N	1
3.23	Location of development database	Separate server from production database	Test and development databases should not be located on the same server as the production system.	8i	B	N	1
3.24	Network location of production and	Separate	If possible, place production databases on a different network segment from test and development	8i	B	N	1

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
	development databases		databases.				
3.25	Monitor for development on production databases	Prevent development on production databases	Check for evidence of development occurring on production databases. Auditing can monitor this type of activity. Alternately, the last_ddl_time column of the dba_objects view can be used to check for objects that have changed.	8i	B	N	1
3.26	Access to production databases	Avoid access from development or test databases	Database access from development and test databases to production databases should be prohibited.	8i	B	N	1
3.27	Developer access to production databases	Disallow	Developers should not have direct access to production databases.	8i	B	N	1
3.28	Developer accounts on production databases	Remove	Remove any developer accounts that exist in the production database.	8i	B	N	1
3.29	Databases created from production exports	Change passwords	If test or development databases are created from backups or exports of the production system, ensure that all passwords are changed before granting access to developers or testers.	8i	B	N	1
3.30	Databases created from production systems	Remove sensitive data	If test or development databases are created from backups or exports of the production system, ensure that all sensitive data (such as payroll information) is removed before granting access to developers or testers.	8i	B	N	1
3.31	Account Management	Document and enforce account management procedures	Create and regularly review procedures for account management. This should include the creation of new user accounts, moving a user to a new group or role, and handling of dormant or inactive accounts.	8i	B	N	1
3.32	Change Control	Document and enforce change control procedures	Create and regularly review procedures for new applications that access the database and change control management procedures for releasing development code into production. Monitor the addition of new users and access rights.	8i	B	N	1
3.33	Disaster recovery procedures	Review	Ensure the disaster recovery procedures are fully documented and regularly tested.	8i	B	N	1

Policy and Procedure

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
3.34	Backdoors	Eliminate	Tight change control management procedures and checksums of the source code can help prevent backdoors into the database.	8i	B	N	1
3.35	Public dissemination of database information	Disallow	There is great risk in posting database information such as SIDs, hostnames, and IP addresses to newsgroups and mailing lists.	8i	B	N	1
3.36	Screen saver	Set screen saver/lock with password protection of 15 minutes.	If an organizational policy does not exist, 15 minutes is recommended.	8i	B	N	1
3.37	Distribution of tnsnames.ora files to clients	Include only necessary tnsnames.ora when distributing to clients	If clients connect to the database using tnsnames.ora files, ensure that only necessary entries are included in the file when distributing to clients. Extraneous information in the tnsnames.ora file may be used as leverage by an attacker.	8i	B	N	1
3.38	Put database in archivelog mode (if appropriate to database function).	If the database was not created in archivelog mode, start the database in mount mode, and issue: alter database achivelog;	Point in time recovery not possible unless database is in archivelog mode. In many cases, the database function may not warrant archivelog mode (such as a database that holds read-only or static data) and this setting can be ignored. If archive log mode is used, transmission of archive logs should be secured as LogMiner could be used to extract database information from the archive logs.	8i	B	Y	1
3.39	Windows Event Log	Monitor	The Windows Event Log should be regularly monitored for errors related to the Oracle database.	8i	W	N	1

Host Files

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
4.01	init.ora	remote_login_ passwordfile=none	Prevents remote privileged connections to the database. This suggests that remote administration	8i	B	Y	2

Host Files

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			should be performed by remotely logging into the database server via a secured connection. Alternately, an administrative listener could be created, the remote_login_passwordfile set to exclusive, and logging of the administrative listener implemented. See tables below for detailed configuration recommendations. Also refer to item 6.41 regarding administrative listener setup.				

Remote Administration of Oracle via Host

	Admin Listener	remote_login_passwordfile setting	SSH or other Secure Method	Terminal Server via IPSec
Unix	N/A	none	Implement	N/A
Windows	N/A	none	N/A	Implement

Remote Administration of Oracle via Administrative Listener

	Admin Listener	remote_login_passwordfile setting	Admin Listener Logging	Client Listener Logging
Unix	Required	exclusive	Required	Strongly Encouraged
Windows	Required	exclusive	Required	Strongly Encouraged

Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
4.02	init.ora	o7_dictionary_ accessibility= FALSE	Prevents users or roles granted SELECT ANY TABLE from accessing the data dictionary. This may cause some applications to stop working – especially 3rd party applications.	8i	B	Y	2
4.05	$ORACLE_HOME/ bin/extproc	Remove binary from host	ExtProc functionality allows external C and Java functions to be called from within PL/SQL. If extproc functionality is not required, remove this binary. Strongly recommend removing extproc binary from Windows systems as this is run as with admin or system privileges on Windows. If extproc functionality is required, refer to Oracle Metalink note 175429.1 for instructions on securing extproc.	8i	B	Y	2
4.06	tnsnames.ora	Remove extproc entry	ExtProc functionality allows external C and Java functions to be called from within PL/SQL. If extproc functionality is not required, remove this entry. If extproc functionality is required, refer to	8i	B	Y	2

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			Oracle Metalink note 175429.1 for instructions on securing extproc. In short a separate listener should be created running as a non-privileged user and the tnsnames.ora file will need to be modified to reflect the correct port for the new Oracle listener.				
4.07	listener.ora	Remove extproc entry	ExtProc functionality allows external C and Java functions to be called from within PL/SQL. If extproc functionality is not required, remove this entry. If extproc functionality is required, refer to Oracle Metalink note 175429.1 for instructions on securing extproc. In short, create a new listener specifically for extproc. This listener should run as an unprivileged OS user. On Unix this might be the “nobody” account, on Windows, it should not be a Windows LOCAL SYSTEM user and should have the “Logon as a service” privilege.	8i	B	Y	2
4.08	listener.ora	Change standard ports	Avoid running the listener on their normal ports such as 1521 and 1526.	8i	B	Y	2
4.10	listener.ora	connect_timeout_*listener*=10	This is the time in seconds that a client is allowed to complete a connection request to the listener after the network connection has been established. If not set in the listenter.ora file, the default is none (there is no limit). Suggestion is to set to a low initial value and adjust upward if normal clients are unable to connect within the time allocated.	8i	B	Y	2
4.11	protocol.ora	tcp.validnode_checking= YES	Set this parameter in the $ORACLE_HOME/network/admin/protocol.ora file.	8i	B	Y	2
4.12	protocol.ora	Set tcp.invited_nodes to valid values	Use IP addresses of authorized hosts to set this parameter in the protocol.ora file.	8i	B	R	2
4.13	protocol.ora	Set tcp.excluded_nodes to valid values	Use IP addresses of unauthorized hosts to set this parameter in the protocol.ora file. Note: if the tcp.invited_nodes is set, the tcp.excluded_nodes values are ignored.	8i	B	R	2
4.18	sqlnet.ora	sqlnet.expire_time= 10	This is the time interval in minutes to send probes for dead connection detection. Idle connections do not get disconnected, but dead connections do. If this is not set in the sqlnet.ora file, the default is	8i	B	Y	2

Host Files							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			never to expire.				
4.19	All associated application files	Verify permissions	Check the file permissions for all application files for proper ownership and minimal file permissions. This includes all 3rd party application files on the server that access the database. Any 3rd party applications should be installed on a separate server from the database. If this is not possible in the environment, ensure that the 3rd party applications are installed on separate partitions from the Oracle software and associated datafiles.	8i	B	N	2
4.20	tnsnames.ora	server=dedicated	Random port reassignment is generally undesirable from a security standpoint. On Unix platforms prior to 9i, if MTS is used, communication by default is redirected to random ports above 1024. Setting server=dedicated in the $ORACLE_HOME/network/admin/ tnsnames.ora file prevents the random reassignment of ports. Alternately, the port reassignment can be limited by placing entries similar to the following in the init.ora file: mts_dispatchers="(address=(protocol=tcp) (host=*hostname*) (port=*port*)) dispatchers=1)" OR local_listener="(address_list = (address= (protocol=tcp) (host=*hostname*)(port=*port*)) (address=(protocol=tcp)(key= *hostname*)))"	8i	U	Y	2
4.21	Windows registry	use_shared_socket= TRUE	On Windows systems, the port used to establish a connection is automatically reassigned to a random port number. Add this to the HKEY_LOCAL_MACHINE\ SOFTWARE\ORACLE\HOME<#> registry key if random port reassignment is undesired, such as if there is a need to pipe through a firewall. See Oracle Metalink note 124140.1 for details.	8i	W	Y	2

Host Files							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
4.22	Oracle software owner host account	Lock account	On Unix systems, lock the Oracle software owner account. If the account cannot be locked, use a very strong password for the account. Account can be unlocked if system maintenance is required. This is not recommended for Windows environments.	8i	U	Y	A

Database Access							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
5.01	Default Accounts (created by Oracle)	The following actions are recommended in order of preference for default accounts: 1. Drop the user 2. Lock the user account 3. Change the default password	A list of default accounts and passwords that may be created depending upon the Oracle version and options installed is included in Appendix B. Depending upon the particular database and application environment, these accounts should be protected by one of these methods. A specific example is the CTXSYS account. Oracle ConText (formally Intermedia) functionality allows access to external files. Lock the CTXSYS account if ConText is required or drop the CTXSYS user with the cascade option if ConText is not required.	8i	B	Y	2
5.02	Third party default passwords	Set all default account passwords to non-default strong passwords	Some third party applications create well known default accounts in an Oracle database. If possible, the default password for these accounts should be changed or the account should be locked. Appendix B contains some default accounts created by some 3rd party applications.	8i	B	N	2
5.03	Accounts	Lock account access for application schema owners	If possible, lock the account for the application schema owner. Users should not connect to the database as the application owner.	8i	B	R	2
5.04	Database Profiles	Review accounts	Check and review any user who has	8i	B	R	2

Database Access							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
		where PASSWORD= 'EXTERNAL'	password='EXTERNAL'. Do not allow remote OS authentication to the database.				
5.05	Database Profiles	Set password_verify_ function to a verification function	Allows password verification function to be called when passwords are changed. This always works for password changes via the "password" command at an SQL prompt. It may or may not work with the ALTER USER command. This setting may not be applicable for middle tier application accounts that access the database. Oracle provides utlpwdmg.sql which can be used to create a password verification function. If using this script to create a password verification function, suggest making the following changes at the bottom of the utlpwdmg.sql file: PASSWORD_GRACE_TIME 3 (Item #2.06) PASSWORD_REUSE_TIME 365 (Item #2.04) PASSWORD_REUSE_MAX 20 (Item #2.03) FAILED_LOGIN_ATTEMPTS 3 (Item #2.01) PASSWORD_LOCK_TIME 1 (Item #2.05) Also suggest modifying the line: IF length(password) < 4 by changing the minimum password length to 8. These settings are in accordance with the recommendations in this document. Local policy may override these recommendations and the values in the utlpwdmg.sql file should be modified accordingly.	8i	B	Y	2
5.06	Database Profiles	Set CPU_PER_ SESSION as appropriate	Ensure that users profile settings have appropriate values set for the particular database and application.	8i	B	R	2
5.07	Database Profiles	Set PRIVATE_SGA as appropriate	Ensure that users profile settings have appropriate values set for the particular database and application. This only applies when shared/multi-threaded server is in use.	8i	B	R	2
5.08	Database Profiles	Set LOGICAL_READS_ PER_SESSION as	Ensure that users profile settings have appropriate values set for the particular database and application.	8i	B	R	2

Database Access							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
		appropriate					
5.09	Database Profiles	Set SESSIONS_PER_ USER as appropriate	Ensure that users profile settings have appropriate values set for the particular database and application.	8i	B	R	2
5.10	Database Profiles	Set CONNECT_TIME as appropriate	Ensure that users profile settings have appropriate values set for the particular database and application.	8i	B	R	2
5.11	Database Profiles	Set IDLE_TIME as appropriate	Ensure that users profile settings have appropriate values set for the particular database and application.	8i	B	R	2
5.12	Tables	Do not store passwords in clear text in Oracle tables	Passwords stored by applications in the database tables should be encrypted. Access to these tables should be limited.	8i	B	N	2
5.13	Tables	Encrypt critical data	Critical data should be encrypted to prevent the DBA from accessing it. Alternately, audit key tables. This does not prevent the DBA from viewing the data, but would create a record of the activity. Management of the encryption key must be done carefully as exposure of the key will render the encryption moot.	8i	B	N	2
5.14	Views	Revoke public access to all public views that start with ALL_	Revoke access to these views when possible. This may interfere with some applications.	8i	B	Y	2
5.15	Roles	Password protect roles	Role passwords are useful when an application controls whether or not a role is turned on. This prevents a user directly accessing the database via SQL (rather than through the application) from having enabling the privileges associated with the role.	8i	B	Y	2
5.16	Packages	Limit or deny access to dbms_backup_ restore	Provides file system functions such as copying files, altering control files, accessing devices, and deleting files.	8i	B	Y	2
5.17	Packages	Limit or deny access to DBMS_RANDOM	Revoke the public execute privilege. It is used to generate random numbers but the numbers generated are known to not be sufficiently random. Also, DBMS_RANDOM could be used to weakly encrypt data by users who should not be storing	8i	B	Y	2

Database Access							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
			encrypted data.				
5.18	OEM objects	Remove if OEM not used (see comments)	Execute $ORACLE_HOME/rdbms/admin/ catnsnmp.sql to remove all the objects and delete the file $ORACLE_HOME/bin/dbsnmp.	8i	B	Y	2

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
6.01	Oracle Installation	Oracle software owner account name NOT oracle	Do not name the Oracle software owner account oracle as it is very well known.	8i	B	Y	2
6.02	Oracle SID for 3rd party applications	Non-default SID	Change the default SID of the third party application to avoid using the well known SID. This also applies to the user accounts and passwords installed by these applications. The idea is that any application that creates a database or user accounts should have the default name changed. If the default names are used and well known, this can be used as leverage for an attack.	8i	B	N	2
6.03	Oracle Installation	Separate users for different components of Oracle	For Unix systems, create unique user accounts for each Oracle process/service in order to differentiate accountability and file access controls. Separating the user for the intelligent agent, the listener, and the database is recommended. This is not recommended for Windows environments.	8i	U	Y	2
6.04	Auditing	Audit ALTER ANY TABLE	Audit the use of ALTER ANY TABLE.	8i	B	Y	2
6.05	Auditing	Audit ALTER USER	Audit the use of ALTER USER.	8i	B	Y	2
6.06	Auditing	Audit any CREATE statement	Audit the use of any CREATE statement.	8i	B	Y	2
6.07	Auditing	Audit CREATE ROLE	Audit the use of CREATE ROLE.	8i	B	Y	2
6.08	Auditing	Audit CREATE USER	Audit the use of CREATE USER.	8i	B	Y	2
6.09	Auditing	Audit CREATE	Audit the use of CREATE SESSION for successful	8i	B	Y	2

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
		SESSION	or unsuccessful operations.				
6.10	Auditing	Audit any DROP statement	Audit the use of any DROP statement.	8i	B	Y	2
6.11	Auditing	Audit DROP ANY PROCEDURE	Audit the use of DROP ANY PROCEDURE.	8i	B	Y	2
6.12	Auditing	Audit DROP ANY TABLE	Audit the use of DROP ANY TABLE.	8i	B	Y	2
6.13	Auditing	Audit GRANT ANY PRIVILEGE	Audit the use of GRANT ANY PRIVILEGE.	8i	B	Y	2
6.14	Auditing	Audit GRANT ANY ROLE	Audit the use of GRANT ANY ROLE.	8i	B	Y	2
6.15	Auditing	Audit INSERT failures	Audit INSERT failures attempted into critical data objects.	8i	B	Y	2
6.16	Auditing	Logon, logoff, database start or stop, and other information.	Create triggers against all tables and system events that are meaningful to the database and application.	8i	B	N	2
6.17	Auditing	Use triggers to implement row level auditing	Use triggers to enforce row level auditing for important data.	8i	B	N	2
6.19	Auditing	Review procedures and reports to review audit logs	Regular, timely reviews of the collected audit information is encouraged.	8i	B	N	2
6.20	Auditing	Set AUDIT ALL ON SYS.AUD$ BY ACCESS	By setting AUDIT ALL ON SYS.AUD$ BY ACCESS, attempts to alter the audit trail will be audited. Only applicable if the audit trail parameter is set to DB or TRUE.	8i	B	Y	2
6.21	Auditing	Regularly purge the audit trail	Review the purging procedures to ensure that the audit trail is purged regularly.	8i	B	N	2
6.22	Alerts on high priority incidents	Create processes to alert	Create processes to monitor and alert of high priority incidents.	8i	B	N	2
6.23	Any remote access to host	Controlled	All remote access to the database should be through an application gateway firewall that supports Oracle network firewall proxy.	8i	B	N	2
6.24	Intelligent agent	Do not use	If the database server is accessible via the Internet, do not use the Intelligent Agent. This may not be practical for OEM or SNMP monitored databases.	8i	B	Y	2

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
6.25	Application PL/SQL code	Wrap	The wrap program provided by Oracle encodes the PL/SQL source code but does not encrypt it. This makes the source code unreadable.	8i	B	Y	2
6.26	PL/SQL code variables and constants	Obscure	The wrap program does not encode variables and constants. One way to obscure these is to build strings from concatenated parts in code.	8i	B	N	2
6.27	Hard coded data in PL/SQL code	Avoid or encrypt	Do not use unencrypted hard coded usernames, passwords, or other critical data in the PL/SQL code.	8i	B	N	2
6.28	Decommissioned applications	Remove all components	Ensure that all associated binaries, users, batch process, and access rights are removed when applications are decommissioned.	8i	B	N	2
6.29	Usernames and passwords	Do not hardcode in application source code	Do not hard code usernames and passwords in application source code. Recommend setting username and passwords in an encrypted external file or database table.	8i	B	N	2
6.30	DDL statements in application	Disallow	Applications should not alter the database schema.	8i	B	N	2
6.31	Reporting tool interface and authentication	Review	Any administrative access to the database host should be controlled by an application level firewall.	8i	B	N	2
6.32	Enabling of batch process account	Time enabled	The account that is used to run batch processes should be enabled only during the time that the batch processes run. If batch processing is process dependent rather than time dependent, it may be possible to establish a window to enable the account.	8i	B	N	2
6.33	Passwords for batch processes	Secure	Passwords for batch processes should not be a command line parameter or an environment variable.	8i	B	N	2
6.34	External account access for batch processes	Disallow	External accounts used for batch processes allow a simple way to access the database.	8i	B	N	2
6.35	Object and table owners	Review	Identify the owner of all objects and tables that are used by third party applications.	8i	B	R	2
6.36	Data in development	Protect	If data is imported from a production database to development or test databases, ensure that any	8i	B	N	2

Policy and Procedure							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
	database		sensitive data (i.e. payroll information) is not accessible to users of the development or test databases. This can be done by either deleting, encrypting, or otherwise protecting the sensitive data.				
6.37	Database links to production databases	Avoid links from development database	Database links from development and test databases to production databases should be forbidden.	8i	B	N	2
6.38	User permissions	Review	Review and test development databases for users with excess permissions not granted in production.	8i	B	N	2
6.39	Procedures for backup tape retrieval	Review	Ensure the procedures for backup tape retrieval are documented and are adequate to prevent social engineering attacks to steal data.	8i	B	N	2
6.40	Intrusion detection system on host	Utilize	Use a host based Intrusion Detection System on the server hosting the Oracle database.	8i	B	N	2
6.41	Multiple listeners	Create separate listeners for clients and administration. Protect the administrative listener with IPSec ESP or OAS SSL and a personal firewall.	An administrative listener, protected by IPSec, could allow administrators access to the server if the client listener(s) are taken down. Preference of implementation is IPSec ESP, otherwise SSL and personal firewall. If SSL is not possible, use OAS native encryption/integrity with a personal firewall, otherwise use a personal firewall. Access should be limited to specific administrative workstations.	8i	B	N	2
6.42	Remote Administration of Listener	Configure listener to have an SSL port.	If remote administration of a listener via the listener utility is required, e.g., no administration through SSH or MS Terminal Server, configure the listener to have a TCPS (SSL) port. If the listener is configured to use multiple protocols, set the SSL protocol as the first protocol in listener.ora.	8i	B	N	2

3. Appendix A – Additional Settings

This section contains additional settings to consider. Unlike the Level 1 and Level 2 settings which are strongly recommended, the settings in this section may be version specific, extremely difficult to implement, or intended only for environments where security is especially stringent.

Appendix A							
Item #	Configuration Item	Action / Recommended Parameter	Comments	ORA VER	OS VER	Score	Level
7.01	OAS - General	Review requirement for integrity and confidentiality requirements.	Only implement OAS if a local integrity/encryption policy does not already exist, e.g., IPSec or other means for providing integrity/confidentiality services.	8i	B	Y	A
7.02	OAS – Oracle Wallet Owner Permissions	Set configuration method for Oracle Wallet. Ensure only the appropriate Oracle user account has access to the wallet.	The Oracle service account must have access to the wallet.	8i	B	Y	A
7.03	OAS – Oracle Wallet Trusted Certificates	Remove certificate authorities (CAs) that are not required.	Trust only those CAs that are required by clients and servers.	8i	B	Y	A
7.04	OAS – Oracle Wallet Trusted Certificates Import	When adding CAs, verify fingerprint of CA certificates.	When adding CA certificates via out-of-band methods, fingerprints should be used to verify the certificate.	8i	B	N	A
7.05	OAS – Certificate Request Key Size	Request the maximum key size available.	The largest key size available that is compatible with the network environment should be selected.	8i	B	Y	A
7.06	OAS – Server Oracle Wallet Auto Login	Allow Auto Login for the server's Oracle Wallet	For Windows Oracle database servers, SSL will not work unless Auto Login is set.	8i	W	Y	A
7.07	OAS – SSL Tab	SSL is preferred method. If PKI not possible, use OAS Integrity/Encryption.	OAS Integrity/Encryption should only be used if required because of non-SSL clients.	8i	B	R	A
7.08	OAS – SSL Version	Set SSL version. SSL_VERSION = 3.0	Any should not be used.	8i	B	Y	A

Appendix A							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
7.09	OAS – SSL Cipher Suite	Set SSL Cipher Suite. SSL_CIPHER_ SUITES = SSL_ RSA_ WITH_3DES_ EDE_ CBC_SHA)	At a minimum, triple DES should be supported. Add SSL_RSA_WITH_RC4_128_SHA or SSL_RSA_WITH_RC4_128_MD5 only if clients don't support the recommended value.	8i	B	Y	A
7.11	OAS – SSL Client Authentication	SSL_CLIENT_ AUTHENTICATION= TRUE	If client certificates are not supported in the enterprise, then set to FALSE.	8i	B	Y	A
7.12	OAS – Encryption Tab	Use OAS encryption only if SSL is not feasible.	OAS Integrity/Encryption should only be used if required because of non-SSL clients.	8i	B	R	A
7.13	OAS – Encryption Type	Set encryption type to required. SQLNET. ENCRYPTION_ SERVER = REQUIRED	Using required will ensure that OAS encryption takes place.	8i	B	Y	A
7.14	OAS – Encryption Seed	Set a different seed on each client and server and a seed size of 70 characters. SQLNET.CRYPTO_ SEED = some70charValue	Avoid using reserved characters, i.e., single quote, double quote, space, number sign, equal sign, right or left parenthesis, comma, and backslash	8i	B	Y	A
7.15	OAS – Encryption Method	Set SQLNET. ENCRYPTION_ TYPES_SERVER= (3DES168, 3DES112)	At a minimum, triple DES should be supported. Add RC4_256 or RC4_128 only if clients don't support the recommended values.	8i	B	Y	A
7.16	OAS – Integrity Checksum	Set SQLNET. CRYPTO_ CHECKSUM_ SERVER= REQUIRED	If IPSec, SSL 3.0, or similar integrity checking is not implmented, but integrity services are required, then use OAS Integrity.	8i	B	Y	A
7.18	RAID file systems	Implement	File systems holding the Oracle data should be on RAID volumes for resilience.	8i	B	N	A
7.19	Magnetically wipe	Implement	Magnetically wipe old, no longer used, or failed	8i	B	N	A

Appendix A							
Item #	**Configuration Item**	**Action / Recommended Parameter**	**Comments**	**ORA VER**	**OS VER**	**Score**	**Level**
	failed disks		disks. This issue is most likely handled by system administrators.				
7.20	Backups on system disks	Verify permissions	In many environments, database backups are written to system disks. In this type of environment, ensure that the backup files are protected. Files should be owned by oracle software owner set with owner read/write permissions only.	8i	B	N	A
7.21	Off site backup storage	Implement	Implement off site backup storage procedures.	8i	B	N	A
7.22	Recovery procedures	Document and Test	Ensure that database recovery procedures are fully documented and regularly tested.	8i	B	N	A
7.23	Backup and restore procedures	Document and Test	Ensure that database backup and restore procedures are fully documented and regularly tested.	8i	B	N	A
7.24	Screening router	Implement to restrict access to database host	Implement a screening router to restrict access to the database host.	8i	B	N	A
7.25	Personal fiirewall	Implement on database administration machines	Use a personal firewall on all computers used to administer databases.	8i	B	N	A

Note: User communities that are required to configure their database to comply with FIPS should refer to the Oracle Advanced Security FIPS 140-1 Settings in the Oracle Advanced Security Administrator's Guide; however, the benchmark's encryption, integrity and protocol settings are the preferred settings.

4. Appendix B – Default User Accounts

Appendix B contains a list of default accounts that may be created during the installation of Oracle products and some select 3rd party products. The actual accounts that are created depend upon the version of Oracle installed and the specific options chosen during the installation. This is intended as a guide to be used with recommendation 5.01 and 5.02 in removing, disabling, or modifying the password for the default accounts created.

Username	Identified by	HashVal
ADAMS	WOOD	72CDEF4A3483F60D
ADLDEMO	ADLDEMO	147215F51929A6E8
ADMIN	JETSPEED	CAC22318F162D597
ANONYMOUS	values 'anonymous'	anonymous
APPLSYS	FND	0F886772980B8C79
APPLYSYSPUB	PUB	A5E09E84EC486FC9
APPS	APPS	D728438E8A5925E0
APPUSER	APPPASSWORD	7E2C3C2D4BF4071B
AQ	AQ	2B0C31040A1CFB48
AQDEMO	AQDEMO	5140E342712061DD
AQJAVA	AQJAVA	8765D2543274B42E
AQUSER	AQUSER	4CF13BDAC1D7511C
AUDIOUSER	AUDIOUSER	CB4F2CEC5A352488
AURORA$JIS$UTILITY$	INVALID	E1BAE6D95AA95F1E
AURORA$ORB$UNAUTHENTICATED	INVALID	80C099F0EADF877E
BC4J	BC4J	EAA333E83BF2810D
BLAKE	PAPER	9435F2E60569158E
CATALOG	CATALOG	397129246919E8DA
CDEMO82	CDEMO82	7299A5E2A5A05820
CDEMOCOR	CDEMOCOR	3A34F0B26B951F3F
CDEMORID	CDEMORID	E39CEFE64B73B308
CDEMOUCB	CDEMOUCB	CEAE780F25D556F8
CENTRA	CENTRA	63BF5FFE5E3EA16D
CIDS	CIDS	AA71234EF06CE6B3
CIS	ZWERG	AA2602921607EE84

Username	Identified by	HashVal
CISINFO	ZWERG	BEA52A368C31B86F
CLARK	CLOTH	7AAFE7D01511D73F
COMPANY	COMPANY	402B659C15EAF6CB
COMPIERE	COMPIERE	E3D0DCF4B4DBE626
CQSCHEMAUSER	PASSWORD	04071E7EDEB2F5CC
CSMIG	CSMIG	09B4BB013FBD0D65
CTXDEMO	CTXDEMO	CB6B5E9D9672FE89
CTXSYS	CTXSYS	24ABAB8B06281B4C
DBI	MUMBLEFRATZ	D8FF6ECEF4C50809
DBSNMP	DBSNMP	E066D214D5421CCC
DEMO	DEMO	4646116A123897CF
DEMO8	DEMO8	0E7260738FDFD678
DEMO9	DEMO9	EE02531A80D998CA
DES	DES	ABFEC5AC2274E54D
DSGATEWAY	DSGATEWAY	6869F3CFD027983A
DSSYS	DSSYS	E3B6E6006B3A99E0
EJSADMIN	EJSADMIN_PASSWORD	313F9DFD92922CD2
EMP	EMP	B40C23C6E2B4EA3D
ESTOREUSER	ESTORE	51063C47AC2628D4
EVENT	EVENT	7CA0A42DA768F96D
FINANCE	FINANCE	6CBBF17292A1B9AA
FND	FND	0C0832F8B6897321
FROSTY	SNOWMAN	2ED539F71B4AA697
GPFD	GPFD	BA787E988F8BC424
GPLD	GPLD	9D561E4D6585824B
HCPARK	HCPARK	3DE1EBA32154C56B
HLW	HLW	855296220C095810
HR	HR	4C6D73C3E8B0F0DA
IMAGEUSER	IMAGEUSER	E079BF5E433F0B89
IMEDIA	IMEDIA	8FB1DC9A6F8CE827
INTERNAL	ORACLE	???
JMUSER	JMUSER	063BA85BF749DF8E
JONES	STEEL	B9E99443032F059D
L2LDEMO	L2LDEMO	0A6B2DF907484CEE

Username	Identified by	HashVal
LBACSYS	LBACSYS	AC9700FD3F1410EB
LIBRARIAN	SHELVES	11E0654A7068559C
MASTER	PASSWORD	9C4F452058285A74
MDDEMO	MDDEMO	46DFFB4D08C33739
MDDEMO_CLERK	CLERK	564F871D61369A39
MDDEMO_MGR	MGR	B41BCD9D3737F5C4
MDSYS	MDSYS	72979A94BAD2AF80
MFG	MFG	FC1B0DD35E790847
MGWUSER	MGWUSER	EA514DD74D7DE14C
MIGRATE	MIGRATE	5A88CE52084E9700
MILLER	MILLER	D0EFCD03C95DF106
MMO2	MMO2	AE128772645F6709
MMO2	MMO3	A0E2085176E05C85
MODTEST	YES	BBFF58334CDEF86D
MOREAU	MOREAU	CF5A081E7585936B
MTS_USER	MTS_PASSWORD	E462DB4671A51CD4
MTSSYS	MTSSYS	6465913FF5FF1831
MXAGENT	MXAGENT	C5F0512A64EB0E7F
NAMES	NAMES	9B95D28A979CC5C4
OAS_PUBLIC	OAS_PUBLIC	A8116DB6E84FA95D
OCITEST	OCITEST	C09011CB0205B347
ODS	ODS	89804494ADFC71BC
ODSCOMMON	ODSCOMMON	59BBED977430C1A8
OE	OE	D1A2DFC623FDA40A
OEMADM	OEMADM	9DCE98CCF541AAE6
OEMREP	OEMREP	7BB2F629772BF2E5
OLAPDBA	OLAPDBA	1AF71599EDACFB00
OLAPSVR	INSTANCE	AF52CFD036E8F425
OLAPSYS	MANAGER	3FB8EF9DB538647C
OMWB_EMULATION	ORACLE	54A85D2A0AB8D865
OPENSPIRIT	OPENSPIRIT	D664AAB21CE86FD2
ORACACHE	ORACACHE	5A4EEC421DE68DDD
ORACLE	ORACLE	38E38619A12E0257
ORAREGSYS	ORAREGSYS	28D778112C63CB15

Username	Identified by	HashVal
ORDPLUGINS	ORDPLUGINS	88A2B2C183431F00
ORDSYS	ORDSYS	7EFA02EC7EA6B86F
OSE$HTTP$ADMIN	INVALID	05327CD9F6114E21
OSP22	OSP22	C04057049DF974C2
OUTLN	OUTLN	4A3BA55E08595C81
OWA	OWA	CA5D67CD878AFC49
OWA_PUBLIC	OWA_PUBLIC	0D9EC1D1F2A37657
PANAMA	PANAMA	3E7B4116043BEAFF
PATROL	PATROL	0478B8F047DECC65
PERFSTAT	PERFSTAT	AC98877DE1297365
PLSQL	SUPERSECRET	C4522E109BCF69D0
PM	PM	C7A235E6D2AF6018
PO	PO	355CBEC355C10FEF
PO7	PO7	6B870AF28F711204
PO8	PO8	7E15FBACA7CDEBEC
PORTAL30	PORTAL31	D373ABE86992BE68
PORTAL30_DEMO	PORTAL30_DEMO	CFD1302A7F832068
PORTAL30_PUBLIC	PORTAL30_PUBLIC	42068201613CA6E2
PORTAL30_SSO	PORTAL30_SSO	882B80B587FCDBC8
PORTAL30_SSO_PS	PORTAL30_SSO_PS	F2C3DC8003BC90F8
PORTAL30_SSO_PUBLIC	PORTAL30_SSO_PUBLIC	98741BDA2AC7FFB2
POWERCARTUSER	POWERCARTUSER	2C5ECE3BEC35CE69
PRIMARY	PRIMARY	70C3248DFFB90152
PUBSUB	PUBSUB	80294AE45A46E77B
PUBSUB1	PUBSUB1	D6DF5BBC8B64933E
QS	QS	4603BCD2744BDE4F
QS_ADM	QS_ADM	3990FB418162F2A0
QS_CB	QS_CB	870C36D8E6CD7CF5
QS_CBADM	QS_CBADM	20E788F9D4F1D92C
QS_CS	QS_CS	2CA6D0FC25128CF3
QS_ES	QS_ES	9A5F2D9F5D1A9EF4
QS_OS	QS_OS	0EF5997DC2638A61
QS_WS	QS_WS	0447F2F756B4F460
RE	RE	933B9A9475E882A6

Username	Identified by	HashVal
REP_MANAGER	DEMO	2D4B13A8416073A1
REP_OWNER	DEMO	88D8F06915B1FE30
REP_OWNER	REP_OWNER	BD99EC2DD84E3B5C
REPADMIN	REPADMIN	915C93F34954F5F8
RMAIL	RMAIL	DA4435BBF8CAE54C
RMAN	RMAN	E7B5D92911C831E1
SAMPLE	SAMPLE	E74B15A3F7A19CA8
SAP	SAPR3	BEAA1036A464F9F0
SCOTT	TIGER	F894844C34402B67
SDOS_ICSAP	SDOS_ICSAP	C789210ACC24DA16
SECDEMO	SECDEMO	009BBE8142502E10
SERVICECONSUMER1	SERVICECONSUMER1	183AC2094A6BD59F
SH	SH	54B253CBBAAA8C48
SITEMINDER	SITEMINDER	061354246A45BBAB
SLIDE	SLIDEPW	FDFE8B904875643D
STARTER	STARTER	6658C384B8D63B0A
STRAT_USER	STRAT_PASSWD	AEBEDBB4EFB5225B
SWPRO	SWPRO	4CB05AA42D8E3A47
SWUSER	SWUSER	783E58C29D2FC7E1
SYMPA	SYMPA	E7683741B91AF226
SYS	CHANGE_ON_INSTALL	D4C5016086B2DC6A
SYSADM	SYSADM	BA3E855E93B5B9B0
SYSMAN	OEM_TEMP	639C32A115D2CA57
SYSTEM	MANAGER	D4DF7931AB130E37
TAHITI	TAHITI	F339612C73D27861
TDOS_ICSAP	TDOS_ICSAP	7C0900F751723768
TESTPILOT	TESTPILOT	DE5B73C964C7B67D
TOAD	TOAD	4759257F78A8B5A3
TRACESVR	TRACE	F9DA8977092B7B81
TRAVEL	TRAVEL	97FD0AE6DFF0F5FE
TSDEV	TSDEV	29268859446F5A8C
TSUSER	TSUSER	90C4F894E2972F08
TURBINE	TURBINE	76F373437F33F347
ULTIMATE	ULTIMATE	4C3F880EFA364016

Username	Identified by	HashVal
USER	USER	74085BE8A9CF16B4
USER0	USER0	8A0760E2710AB0B4
USER1	USER1	BBE7786A584F9103
USER2	USER2	1718E5DBB8F89784
USER3	USER3	94152F9F5B35B103
USER4	USER4	2907B1BFA9DA5091
USER5	USER5	6E97FCEA92BAA4CB
USER6	USER6	F73E1A76B1E57F3D
USER7	USER7	3E9C94488C1A3908
USER8	USER8	D148049C2780B869
USER9	USER9	0487AFEE55ECEE66
UTLBSTATU	UTLESTAT	C42D1FA3231AB025
VIDEOUSER	VIDEOUSER	29ECA1F239B0F7DF
VIF_DEVELOPER	VIF_DEV_PWD	9A7DCB0C1D84C488
VIRUSER	VIRUSER	404B03707BF5CEA3
VRR1	VRR1	811C49394C921D66
VRR1	VRR2	3D703795F61E3A9A
WEBCAL01	WEBCAL01	C69573E9DEC14D50
WEBDB	WEBDB	D4C4DCDD41B05A5D
WEBREAD	WEBREAD	F8841A7B16302DE6
WKPROXY	WKPROXY	AA3CB2A4D9188DDB
WKSYS	WKSYS	545E13456B7DDEA0
WWW	WWW	6DE993A60BC8DBBF
WWWUSER	WWWUSER	F239A50072154BAC
XDB	XDB	FD6C945857807E3C
XPRT	XPRT	0D5C9EFC2DFE52BA

5. Appendix C – Disabled Windows 2000 Services

Appendix C contains a list of services that, if not needed should be disabled on a Windows 2000 server running Oracle. This is intended as a guide to be used with recommendation 1.58 in disabling Windows services.

Windows 2000 Service
Alerter
ClipBook Server
Computer Browser
DHCP Client
Distributed File System
Fax Service
Internet Connection Sharing
IPSEC Policy Agent (Disable unless IPSEC policies will be used.)
License Logging Service
Logical Disk Manager Administrative Service
Messenger
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
OracleOraHome90HTTPServer (Disable unless iSQL or other web resource is required.) Note: may have a different name.
Print Spooler
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Registry Service (Disable unless running hfnetchk or similar utilities.)
Removable Storage
RunAs Service
Smart Card
Smart Card Helper
Telephony
Telnet
Windows Installer
Workstation (Disable unless the server will be part of a domain.)